UACM

Universidad Autónoma
de la Ciudad de México

NADA HUMANO ME ES AJENO

COLEGIO DE CIENCIA Y TECNOLOGÍA

LICENCIATURA EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

Ingeniería inversa de la red tipo "WAN" de una empresa de suministros médicos

T E S I S

QUE PARA OPTAR POR EL TÍTULO DE

LICENCIADA EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

P R E S E N T A

LESLIE SAHARY HERNÁNDEZ CABALLERO

D I R E C T O R

MTRO. JOSÉ IGNACIO CASTILLO VELÁZQUEZ

Ciudad de México, agosto de 2024.

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

CA Coordinación Académica

SISTEMA BIBLIOTECARIO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO
COORDINACIÓN ACADÉMICA

RESTRICCIONES DE USO PARA LAS TESIS DIGITALES

DERECHOS RESERVADOS©

La presente obra y cada uno de sus elementos está protegido por la Ley Federal del Derecho de Autor; por la Ley de la Universidad Autónoma de la Ciudad de México, así como lo dispuesto por el Estatuto General Orgánico de la Universidad Autónoma de la Ciudad de México; del mismo modo por lo establecido en el Acuerdo por el cual se aprueba la Norma mediante la que se Modifican, Adicionan y Derogan Diversas Disposiciones del Estatuto Orgánico de la Universidad de la Ciudad de México, aprobado por el Consejo de Gobierno el 29 de enero de 2002, con el objeto de definir las atribuciones de las diferentes unidades que forman la estructura de la Universidad Autónoma de la Ciudad de México como organismo público autónomo y lo establecido en el Reglamento de Titulación de la Universidad Autónoma de la Ciudad de México.

Por lo que el uso de su contenido, así como cada una de las partes que lo integran y que están bajo la tutela de la Ley Federal de Derecho de Autor, obliga a quien haga uso de la presente obra a considerar que solo lo realizará si es para fines educativos, académicos, de investigación o informativos y se compromete a citar esta fuente, así como a su autor ó autores. Por lo tanto, queda prohibida su reproducción total o parcial y cualquier uso diferente a los ya mencionados, los cuales serán reclamados por el titular de los derechos y sancionados conforme a la legislación aplicable.

PRÓLOGO

En la UACM, los primeros egresados titulados de ISET se lograron en 2012 en el plantel Casa Libertad. El ADVNETLAB (Advanced Networking Laboratory) en la UACM fue fundado en 2013 en el campus San Lorenzo Tezonco por quien suscribe, José Ignacio Castillo Velázquez, con recursos propios. Una vez que hubo masa crítica de egresados de ISET en el citado campus e interés sobre el tema de redes. Con base en mi experiencia en universidades públicas y privadas (UTM, UPAEP, BUAP, UAM, UDEFA, UACM) y empresas públicas y privadas (DICINET, IFE, REDUNO-TELMEX, Data Center Dynamics) desarrollé la metodología ADVNETLAB, la cual está en constante reajuste y con la que se dirigen las tesis y otros proyectos.

Desde 2015, desde ADVNETLAB, a la fecha hemos producido 18 tesis, tal que se han titulado 20 estudiantes de telecomunicaciones; tal que 16 de ellos licenciatura de la UACM México, 3 de licenciatura la UNAS Perú y 1 de maestría de la UPS Ecuador.

La calidad de los trabajos desarrollados en el laboratorio ha permitido que se publiquen 37 artículos indexados en SCOPUS, tanto en redes avanzadas como en seguridad informática, software y educación; 20 de tales publicaciones se han realizado con los ahora ingenieros. Se desarrolló UTILCON, un sistema de gestión de congresos o seminarios u otro tipo de eventos académicos gratuito en línea y en español, registrado ante el Instituto Nacional de Derechos de Autor, ya que en México los sistemas de software no son patentables como sí lo son en otros países.

En ADVNETLAB se ha abordado la conectividad y gestión para las redes avanzadas CUDI, CLARA, Internet2, CANARIE, REUNA, GEANT, AFRICACONNECT, CEDIA y Pacific Wave, bajo protocolos IPv4, IPV6 y SDN, así como la ingeniería inversa.

En esta ocasión se presenta Leslie Sahary Hernandez Caballero (ANL20) con el trabajo Ingeniería inversa de la red tipo “WAN” de una empresa de suministros médicos, bajo una topología real y para la cual se abordan además de la conectividad y gestión de red, aspectos relacionados con la seguridad informática. Mis felicitaciones a Leslie Hernández por el trabajo concluido este agosto de 2024, mismo que iniciamos en febrero de 2023.

M. en C. José Ignacio Castillo Velázquez

Director de tesis - Agosto de 2024

ADVNETLAB UACM-SLT

RESUMEN

En la actualidad, las empresas se encuentran en una era digital con avances tecnológicos rápidos e impredecibles, las redes WAN, MAN y LAN realizan un papel importante en la conectividad y el intercambio de información. Dado que la innovación tecnológica es un proceso continuo, los equipos y software se vuelven obsoletos y vulnerables rápidamente. Por este motivo, es forzoso contar con dispositivos y sistema a la vanguardia y actualizados para garantizar un óptimo desempeño.

Este estudio se centra en analizar la red WAN de una empresa que provee suministros médicos para obtener una visión detallada de la infraestructura de red de una empresa, con el fin de identificar su topología, evaluar la seguridad de la red inalámbrica (WLAN) y analizar los anchos de banda contratados con los proveedores de servicios de internet (ISP).

Para llevar a cabo este estudio y comprender funcionamiento de la red, se llevó a cabo un análisis mediante ingeniería inversa, comenzando por un inventario físico detallado y culminando en la construcción de un modelo simulado que me permitió crear y experimentar con redes virtuales de forma segura y sin riesgo de afectar la red real.

Para evaluar el rendimiento de la red se hace uso de herramientas en línea para medir las velocidades de conexión a internet de cada sucursal y comprobar si la conexión coincide o se acerca a la que ofrecen el proveedor de internet. Por último, mediante la revisión en la configuración de los *Access Point* se pudo identificar la seguridad con la que cuenta la red inalámbrica de la empresa.

A partir del análisis realizado se identifican vulnerabilidades y oportunidades de mejora para la infraestructura de red. Se realizan sugerencias y propuestas que permitirán mejorar la seguridad, el rendimiento y la fiabilidad de la red, alineando la infraestructura con las necesidades actuales y futuras de la empresa.

ABSTRACT

Today, companies are in a digital era with rapid and unpredictable technological advances, and WANs, MANs and LANs play an important role in connectivity and information exchange. As technological innovation is a continuous process, equipment and software quickly become obsolete and vulnerable. For this reason, it is imperative to have state of the art and up to date devices and systems to ensure optimal performance.

This study focuses on analyzing the WAN network of a company that provides medical supplies to obtain a detailed view of the network infrastructure of a company, in order to identify its topology, evaluate the security of the wireless network (WLAN) and analyze the bandwidths contracted with Internet Service Providers (ISPs).

To carry out this study and understand how the network works, a reverse engineering analysis was carried out, starting with a detailed physical inventory and culminating in the construction of a simulated model that allowed me to create and experiment with virtual networks safely and without the risk of affecting the real network.

To evaluate the performance of the network, online tools are used to measure the internet connection speeds of each branch and check if the connection matches or is close to the one offered by the internet provider. Finally, by reviewing the configuration of the Access Points, it was possible to identify the security of the company's wireless network

Based on the analysis performed, vulnerabilities and improvement opportunities for the network infrastructure are identified. Suggestions and proposals are made to improve the security, performance and reliability of the network, aligning the infrastructure with the current and future needs of the company.

CONTENIDO

CAPÍTULO I

INTRODUCCIÓN

1.1 ESTRUCTURA DE LA TESIS

Esta tesis se compone de 4 capítulos que se describen a continuación:

En el capítulo 1 “Introducción”. Se realiza la descripción de ingeniería inversa y su aplicación. En el capítulo 2 “Redes y protocolos” se describen los protocolos de conectividad y gestión y se mapea a cada capa del modelo ISO/OSI en la que operan. En este capítulo se incluirá la descripción de los tipos de autentificación mediante claves compartidas WEP, WPA, WPA2 y Enterprise. En el capítulo 3 “Metodología” se realiza la simulación de las redes y se válida la seguridad la red empresarial vs red casera. En el capítulo 4 se indican los “Resultados y conclusiones”.

Para el manejo de citas se usará el estilo empleado por el Institute of Electrical and Electronics Engineers (IEEE) y para el manejo de acrónimos el tipo PPP (Inglés- español)

1.2 INGENIERÍA INVERSA

La búsqueda de métodos para crear nuevos productos en el mercado con el fin de satisfacer la oferta y demanda, así como comprender los componentes de un objeto, ha permitido que las empresas utilicen la ingeniería inversa para satisfacer las necesidades particulares, así como utilizar su metodología para mejorar o reconstruir productos. Actualmente nos encontramos en un entorno digital avanzado que conlleva desafíos para la detección de problemas de interoperabilidad entre aplicaciones o fallas en software y hardware en donde está presente la ingeniería inversa.

La ingeniería inversa no tiene una fecha concreta de su comienzo, se mencionan fechas como en la época de la revolución industrial, la primera guerra mundial, sin llegar a tener un acuerdo del inicio de este tipo de ingeniería. Se ocupa de forma cotidiana en diferentes áreas tecnológicas, medicina, social, cultural, educación, políticas y manufactura. El método se utiliza cuando se cuenta con un modelo ya existente, el proceso de ingeniería inversa nos permite la reconstrucción de cualquier sistema con el fin de observar su estructura y componentes para entender el funcionamiento y con base en un análisis poder mejorarlo.

Existen diferentes definiciones de la ingeniería inversa y cada una tiene su metodología por ejemplo Chifofsky lo define como: *El análisis de un sistema para identificar sus componentes actuales y las dependencias entre ellos, para extraer y crear abstracciones de dicho sistema e información de su diseño*. [1]

Para poder aplicar la ingeniería inversa es necesario tener un modelo construido con base en la ingeniería progresiva/avanzada utilizando etapas estructuradas, requisitos, diseño e implementación como se muestra en la figura 1.

- Requisitos: Especificaciones del problema que se pretende resolver, objetivos, restricciones y normas empresariales.
- Diseño: Especificaciones de la solución.
- Implementación: Codificación, pruebas y entrega. [1]

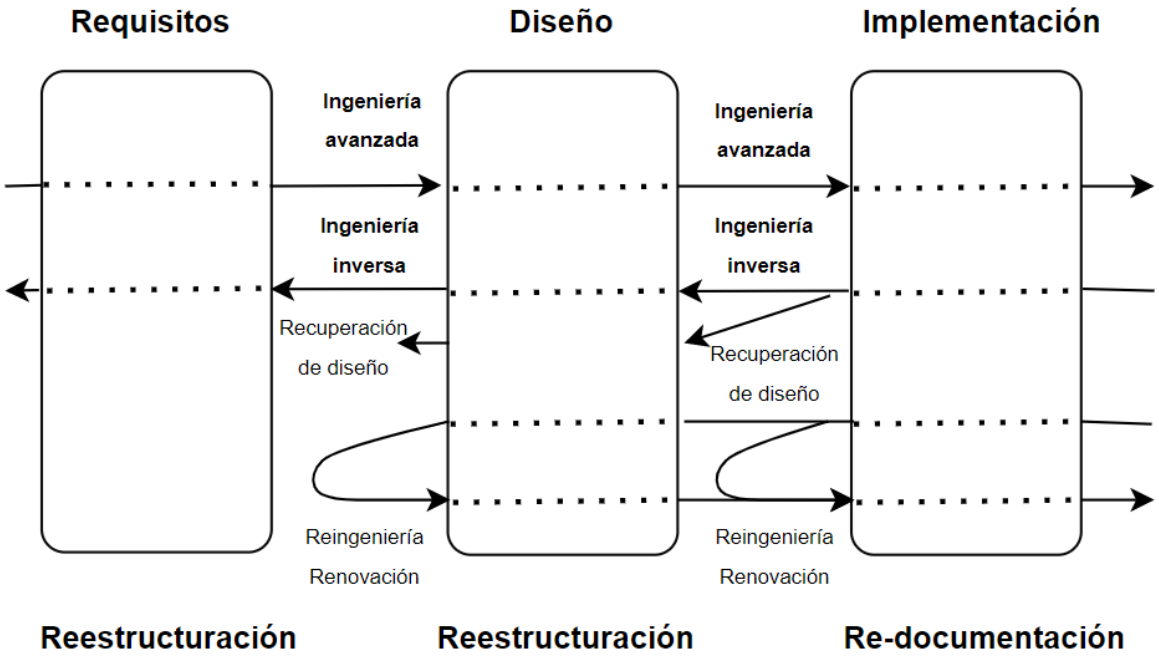


Figura 1 Ciclo de ingeniería avanzada & Ingeniería inversa [1]

La “ingeniería avanzada” utiliza el adjetivo “*Hacia adelante*” que sigue una secuencia desde el requerimiento hasta la entrega de un sistema, mientras que la “ingeniería inversa” a través de la comprensión y complejidad permite descubrir el funcionamiento y operación del sistema, utilizado información técnica para recuperar o restructurar un diseño sin alterar su funcionamiento, esto depende del objetivo que se requiera del sistema u objeto en estudio [1], como, por ejemplo:

- Re- documentación: *Documentación retrospectiva de un sistema u objeto que tiene como finalidad ayudar a conocer el objeto*, en algunos casos se utiliza para recuperar documentación pérdida o inexistente, conociendo los niveles de abstracción que dependen de la complejidad y características físicas del sistema (sistemas, programas, componentes y configuraciones)

- Recuperación de diseño: Se utiliza para recuperar y reproducir el sistema en estudio. Utilizando la siguiente pregunta: ¿Cómo lo hace? y ¿Por qué?

- Reestructuración: *La trasformación desde una forma de representación a otra en el mismo nivel de abstracción, preservando las características externas del sistema (Funcionalidad y Semántica)* [1]. Es decir, cambiar la estructura sin afectar su funcionamiento.

- Reingeniería: Implementar el nuevo diseño realizando alteraciones para reconstruirlo en su nueva forma. Puede utilizar tanto la ingeniería directa e inversa para su aplicación.

En la tabla 1 se presenta un breve resumen de casos prácticos de la industria de las telecomunicaciones donde se utilizó la ingeniería inversa, se indican empresas, método y una breve descripción.

Empresas	Método	Descripción
1980. Phoenix Tecnologies Ltd	Ingeniera inversa en desarrollo	Producir el BIOS patentado por IBM, sin utilizar el código propiedad de IBM.
1992. Cyrix Corp y Advanced Micro Device INC	Ingeniera inversa para fabricación	Fabricación de microprocesadores compatibles con Intel de bajo costo.
2007. W. Cui, V.Paxson, N. C.Weaver – Discoverer	Ingeniería inversa de protocolos automatizado (En redes- con base en mensajes capturados)	Extracción de mensajes entre cliente y servidor a partir de trazas.
2007. J. Caballero, H. Yin, z. Liandg, D. Song – Polyglot.	Ingeniería inversa de protocolos (Hibrido)	Análisis de vulnerabilidades de seguridad.
2009. Yongjun He, Hui Shu, Xiaobing Xiobing Xiongc - DynamoRIO	Ingeniería inversa de protocolos (Basado en análisis de flujo de datos)	Extracción de protocolos desconocidos.
2010. Zhinqiang Lin – Reward.	Ingeniería inversa de protocolos (Basado en programas- análisis binario)	Reconstrucción de datos y detección de vulnerabilidades.
2013. José-Ignacio Castilo-Velázquez, Noe Galicia-Gutierrez, Juan-Arnulfo López-Ruiz	Ingeniería inversa (Reconstrucción)	Simulación de infraestructura de redes de datos
2018 Jose-Ignacio Castillo-Velazquez; Manuel-Israel Trigueros-Galicia	Ingeniería inversa (Reconstrucción)	Sistema de gestión de congresos.

Tabla 1. Ingeniería inversa en las telecomunicaciones [2, 3, 4, 5, 6, 7, 8]

El uso de la ingeniería inversa es común en la actualidad, en donde se busca innovar o mejorar productos e inclusive es utilizado para analizar productos de competencia y exploración de vulnerabilidades.

La ingeniería inversa está legalmente aprobada si se utiliza sin fines maliciosos.

1.3 OBJETIVO GENERAL

Conocer el funcionamiento de una red WAN en una empresa que provee suministros médicos en diferentes ciudades de México, con el fin de realizar mejoras en la empresa para operar en condiciones óptimas.

1.4 OBJETIVOS ESPECÍFICOS

1: Identificar la topología real de la red empresarial y sus anchos de banda contratados con el ISP.
2: Desarrollar las habilidades de un administrador de red LAN y MAN para lo cual se analizarán, configurarán y monitorearán las funciones básicas de conectividad y gestión bajo IPv4
3: Conocer el nivel de seguridad configurado en la red empresarial
4: Sugerir una propuesta que permita a la red de la empresa operar de manera funcional y segura.

1.5 JUSTIFICACIÓN

La empresa de suministros médicos en la cual se va desarrollar el estudio, implementó un proyecto de infraestructura a través de una empresa externa colocando hardware de dos marcas. Cuando se llevó a cabo la implementación la empresa proveedora de Internet ISP (*Internet Service Provider*- Proveedor de servicios de Internet) externa no entregó la documentación de forma detallada ni mapas de conexión, sólo entregó diagramas generales. El monitoreo y gestión de la infraestructura de comunicaciones de Internet y VoIP (*Voice Over Internet Protocol*- Voz sobre protocolo de Internet) lo realiza la empresa ISP externa. Por otro lado, el monitoreo de la seguridad de cada red LAN (*Local area network*- Red de área local) está a cargo del área de sistemas de la empresa en estudio, es por ello que a través del uso de ingeniería inversa se busca conocer el alcance de la infraestructura y la seguridad a fin de detectar vulnerabilidades y mejoras. Por políticas y seguridad de la empresa no se describirán los modelos de los componentes de infraestructura, únicamente se mencionarán las características de ellos. Esta investigación busca aplicar la metodología de ingeniería inversa para obtener la distribución de la infraestructura de la red de datos de una empresa comercial con alcance nacional a partir de su inventario físico de *switches*, SFP (*Small Form-factor Pluggable Transceiver* - Transceptor enchufable de pequeña forma), *Firewa*lls (corta fuego), la inspección física de la telefonía VoIP y computadoras de usuario instaladas. La red WAN (*Wide area network*- red de área amplia) se encuentra distribuida en cuatro ciudades una en el Estado de México, tres en la Ciudad de México, una en Guadalajara y una en Monterrey. Por tanto, se usará ingeniería inversa para replicar el funcionamiento de la red, utilizando el simulador Cisco Packet Tracer, versión 6.2.

Una de las políticas de la empresa prohíbe difundir cualquier IP pública y privada, marcas y modelos, por lo tanto, en este trabajo se utilizarán dispositivos equivalentes a Cisco. Se tomarán los esquemas y diagramas de la red empresaria para las pruebas en el simulador de packet tracer Cisco

CAPÍTULO 2
REDES Y PROTOCOLOS

Antes de comenzar a identificar los distintos tipos de redes debemos saber qué es una red. Una red es un conjunto de equipos tales como: computadoras, tabletas, *smartphones* entre otros componentes de comunicaciones que se encuentren interconectados de forma alámbrica o inalámbrica y que nos permiten trasportar o compartir recursos o servicios.

Los dispositivos que conforman la red se dividen en dos grupos:

- Dispositivos de usuario final: Impresoras, PC, laptop, servidores, equipos de almacenamientos, telefonía VoIP, teléfono móvil, Tableta, cámaras de seguridad, etc.
- Dispositivos de red
    - Pasivos (Para su funcionamiento no es necesario una fuente de alimentación externa y se utiliza para interconectar enlaces): Cables, fibra óptica, *patch panel* (panel de conexiones), conectores, canaletas,
    - Activos (Se encargan de distribuir la información a través de la red): AP (*Access point*- Punto de acceso*) , Router, Switch*, Modulo óptico SFP, *firewall*, etc

En la actualidad las redes nos permiten comunicarnos e intercambiar información de forma local o internacional, algunas funciones son:

- Comunicación vía telefonía VoIP
- Video conferencias
- Transferencia de información
- Uso de correos electrónicos
- Conexión con bases de datos
- Conexión con aplicaciones Web
- Consulta de información

2.1 TIPOS DE REDES

Se clasifican dependiendo la cobertura y el tamaño de la red.

2.1.1. LAN (*LOCAL AREA NETWORK* -RED DE ÁREA LOCAL)

La red de área local permite un intercambio de datos a alta velocidad entre dispositivos digitales situados en un área geográfica de tamaño moderado [9]. Esta tecnología funciona en la capa 2 (enlace de datos), es decir, la comunicación se realiza a través de direcciones MAC, las IP son necesarias cuando se enrutan a través de segmentos de LAN. Pueden ser alámbricas o inalámbricas y se encuentran dentro de casa, oficinas y edificios.

Las LAN operan actualmente entre los 10 Mbps (Ethernet) y 1 Gbps (Giga Ethernet). Como las tecnologías LAN cubren distancias cortas, ofrecen menor retardo que las WAN. El retardo en una LAN puede ser de unas décimas de milisegundo o hasta 10 milisegundos. [10]

Regularmente las redes LAN se interconectan por cable de par trenzado y su efectividad pueden variar dependiendo de su categorización. Utiliza protocolos de red que permiten la comunicación por ejemplo TCP/IP, Ethernet, FTP, SMTP, entre otros.

2.1.2 MAN (*METROPOLITAN AREA NETWORK* -RED DE ÁREA METROPOLITANA)

La red de área metropolitana interconecta más de 2 redes LAN. Una red de área metropolitana se distingue de otros tipos de redes de datos por su limitación a un área geográfica, como una ciudad. El canal de comunicaciones de una MAN tiene una tasa de datos de moderada a alta y una tasa de error constantemente baja. [11]

2.1.3 WAN (WIDE ÁREA NETWORK- RED DE ÁREA AMPLIA)

La red de área amplia tiene una cobertura extensa abarcando estados o países, permiten interconectar subredes LAN o MAN y emplea enlaces punto a punto. La administración de este tipo de redes es de alta demanda por la cantidad de información que se transmite y en el caso de los proveedores, las redes son conocidas como dorsales (backbone). Las WAN son muy usadas a nivel mundial, por ejemplo: Internet comercial e Internet 2

En la figura 2 se muestra la representación de una red LAN, MAN Y WAN

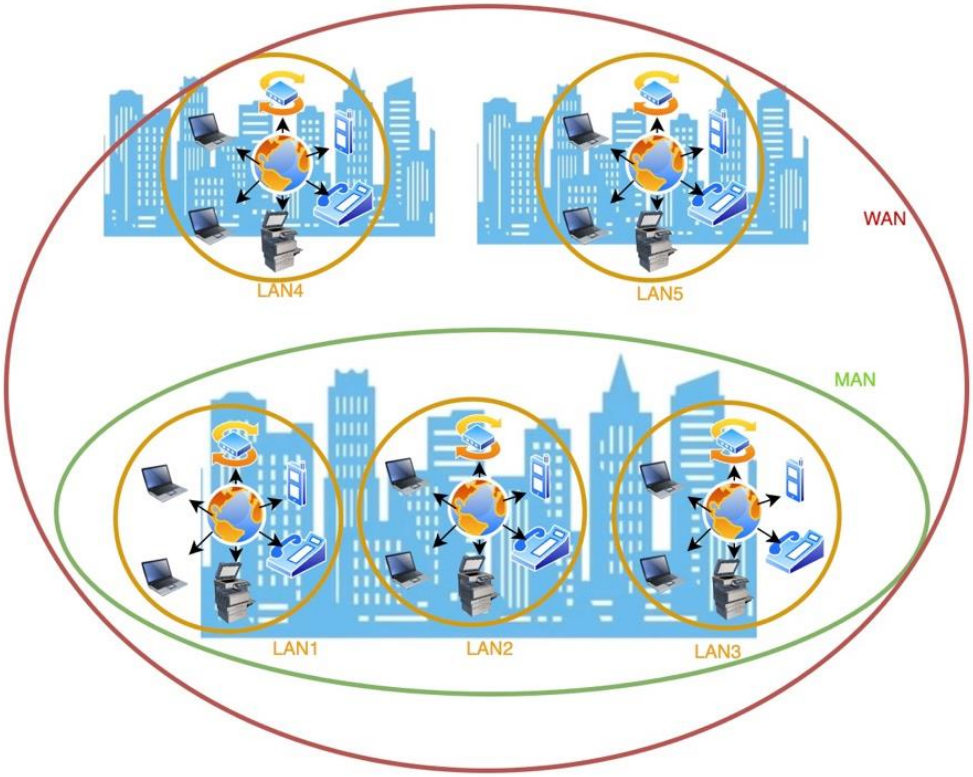


Figura 2 Redes y coberturas LAN, MAN, WAN (Propia)

2.2 TOPOLOGÍAS DE RED

La topología de red es básicamente la configuración física de una red y nos permite interconectar diferentes dispositivos. La velocidad de transmisión, número de dispositivos, dimensión de ubicación intervienen en la elección de la topología. Las topologías incluyen estructura física y lógica: La “topología física” nos indica cómo está diseñada la red, así como la distribución de componen, por ejemplo: nodos, conectores, cables, ordenadores y otros dispositivos físicos; mientras que la “topología lógica” se refiere a la forma de cómo las computadoras se comunican dentro de la red. Es decir, de todos los caminos físicos posibles, la topología lógica nos muestra el camino que siguen en la práctica los paquetes a partir de las distintas opciones. [12]

2.2.1 CLASIFICACIÓN DE TOPOLOGÍAS DE REDES

2.2.1.1 Topología de Bus

Esta topología de bus comparte el mismo medio para transferir información, es decir, cada nodo está conectado al mismo cable. Una transmisión desde cualquier estación se propaga a través del medio en ambos sentidos y es recibida por el resto de las computadoras, el problema que existe para esta topología es la congestión y pérdida de datos ya que la transmisión de información comparte un solo canal. [13]

2.2.1.2 Topología de anillo

En esta topología la conexión debe terminar donde inicio formando básicamente un círculo. Los enlaces son unidireccionales, es decir, los datos se transmiten en un solo sentido, de modo que estos circulan alrededor del anillo, un solo cable conectado al switch puede distribuir a “n” equipos. Los datos se transmiten en tramas y una trama que circula por el anillo pasa por las demás computadoras de modo que la computadora destino reconoce su dirección y copia de la trama. No es recomendable ya que depende

de la funcionalidad de las computadoras de trabajo, si falla una computadora, la comunicación en las demás computadoras se pierde.[13]

2.2.1.3 Topología de estrella

Cada computadora está conectada a un nodo central través de enlaces punto a punto. cada conexión de dispositivos termina en el nodo central, este diseño reduce el riesgo de pérdida total de la red. El nodo central puede ser un switch, si éste falla todo el segmento de red puede fallar. Sin embargo, es mucho más sencillo detectar los errores. La topología estrella es mejor para distancias cortas y puede ofrecer velocidades elevadas a un número pequeño de dispositivos.[13]

El la figura 3 se muestra la topología estrella, donde seis computadoras están conectadas a un switch central y toda la comunicación se realiza a través de éste punto central.

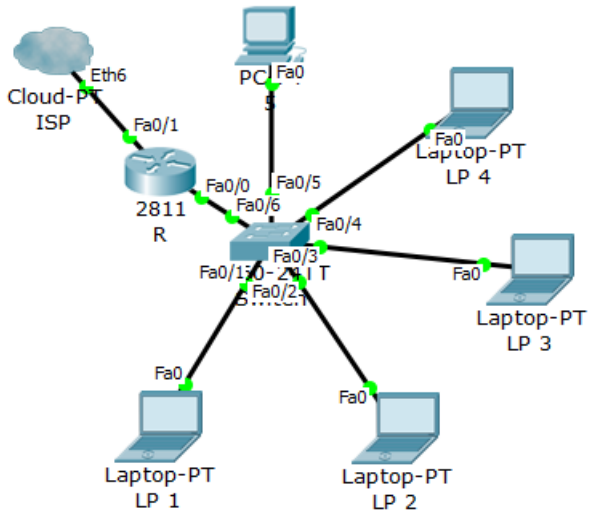


Figura 3. Topología Estrella (imagen propia)

2.2.1.4 Topología de árbol

Es la topología más usada hoy en las empresas ya que da la posibilidad de realizar conexiones punto a punto y requiere añadir switches adicionales para realizar conexión alámbricas o inalámbricas por ejemplo conectar los AP *(Acces Point - Punto de acceso)* que distribuyen la red Wifi (*Wireless Fidelity*- Fidelidad inalámbrica) en una determinada área, puede verse como una combinación de la topología estrella como se muestra en la figura 4.

Una ventaja de usar redes de árbol es que las expansiones son relativamente simples. Las redes no son normalmente afectadas si uno de los nodos falla. Pero si el conmutador falla, las computadoras conectadas a ese conmutador no podrán comunicarse. [14]

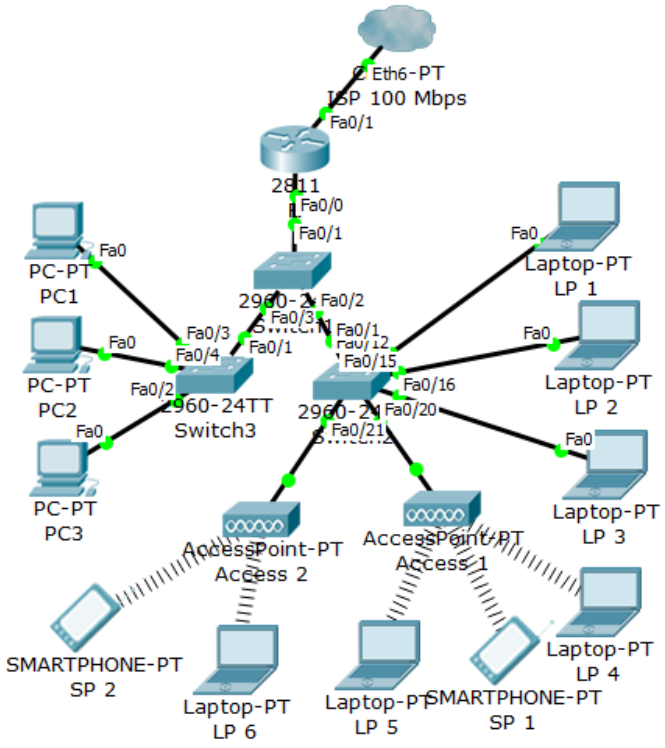


Figura 4. Topología árbol (imagen propia)

2.2.1.5 Topología de malla

Proporciona múltiples enlaces entre los nodos de la red asegurando redundancia. Este tipo de topología asegura la ruta más conveniente y si una conexión es terminada o interrumpida, otra conexión podrá elegirse para transferir información a su nodo de destino, en la figura 5 se realiza una representación gráfica. [14]

La topología de malla permite una comunicación robusta de múltiples saltos y una red más flexible, pero induce una complejidad adicional para proporcionar una conectividad de extremo a extremo entre todos los dispositivos de la red [15], la desventaja de esta configuración es su alto costo

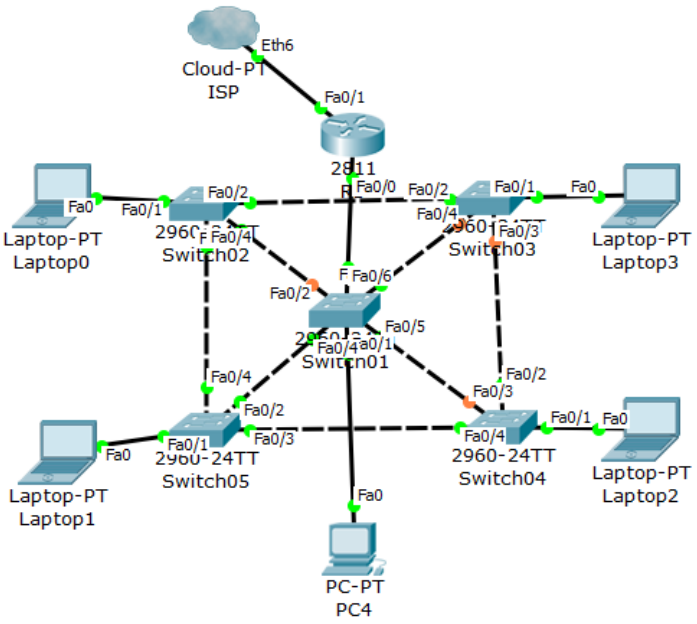


Figura. 5. Topología Malla (imagen propia)

2.3 MODELO OSI Y TCP/IP

En 1984 ISO (Internacional Organization for Standardization- Organización Internacional de Normalización) propuso el modelo OS I(Open Systems Interconnection- Interconexión de sistemas abiertos), el cual buscó asegurar la compatibilidad entre distintas tecnologías de redes y estandarizar los protocolos de datos, este modelo se desarrolló sobre un conjunto de siete capas en donde indica cómo se transporta la información desde la computadora, a través de los medios de red hacia una aplicación que corre en otra computadora. En cada capa se realiza un encapsulamiento y desencapsulamiento de datos. [12]

2.3.1 CAPAS DEL MODELO OSI

2.3.1.1 Capa 7. **Aplicación**

Proceso de red a las aplicaciones. Esta capa permite a los programas de aplicación de nuestro sistema operativo un medio para que interactúen a través de la red, por ejemplo, los portales de navegación web, redes sociales, correo electrónico entre otros, con el objetivo de que los datos puedan viajar de un lugar a otro de la red. En esta capa se lleva a cabo el procesamiento final de la información a intercambiar, es la capa cercana al usuario.

2.3.1.2 Capa ***6. Presentación***

Representación de datos, Realiza la encriptación, codificación y conversión de datos en un lenguaje estándar para que puedan ser interpretados por la computadora. Es decir, permite interpretar el lenguaje de alto nivel como caracteres (palabras, números, caracteres) en código binario bajo ASCII.

2.3.1.3 Capa ***5. Sesión***

Comunicación entre computadores. Establece, administra y termina comunicación entre dos computadoras. Se caracteriza por sincronizar el diálogo entre las capas de presentación de las dos computadoras y administra el intercambio de datos entre ellas [12]. Por ejemplo, cuando existe una conexión inactiva durante un período, el protocolo de la capa de sesión puede cerrarla o volver a abrirla.

2.3.1.4 Capa ***4. Transporte****:*

Conexión extremo a extremo (*end to end*), Establece, mantiene y cierra los circuitos virtuales entre aplicaciones [12]. Su principal función es aceptar los datos de la capa de sesión y segmentarlos en unidades pequeñas y pasarlos a la capa de red reduciendo los errores de transmisión y recepción, asegurando que todos los segmentos lleguen al destino final, donde realiza un proceso de ensamblaje de todos los segmentos con la finalidad de que los datos lleguen de forma fluida y sin saturar la red.

2.3.1.5 Capa 3. **Red**

Direccionamiento y enrutamiento. Esta capa se encarga de que sea posible la comunicación entre dispositivos, cada equipo tiene una dirección lógica, esta dirección forma parte del control de la capa de red, es decir, cuando enviamos paquetes la capa de red agrega al mensaje la dirección IP al equipo emisor y receptor, mientras que el enrutamiento determina las mejores rutas a los diferentes destinos.

2.3.1.6 Capa 2. **Enlace de datos**

Define como se formatean los datos y como se controla el acceso al medio físico, incluye la detección de errores logrando una comunicación confiable entre equipos a través de tramas en donde se indica la dirección MAC (*Media Access Control* - Control de Acceso al Medio) origen y destino *[12]*
Se divide en dos subcapas

LLC (*Logical Link Control* -Control Lógico de Enlace): Es la interfaz entre la MAC y la capa de red, se encarga de comunicar el software de la red con el hardware mediante la tarjeta de red (NIC) una vez que establece comunicaciones son enviados a la subcapa MAC

MAC: Se encarga de agregar direccionamiento físico. A diferencia de las direcciones IP que nos indican en qué red del mundo se encuentra nuestros dispositivos, la dirección MAC nos indica cuál es el dispositivo dentro de una red

2.3.1.7 Capa 1. **Física**

Trasmisión binaria. Es la capa donde se especifica el medio por el cual se trasmiten los datos utilizando codificación y señalización, es decir, los datos son convertidos de código binario a señales de luz, ondas o señales eléctricas mediante un medio que puede ser fibra óptica, UTP u ondas en caso de utilizar Wifi, esta codificación la realiza la NIC o tarjeta de red, enviados de host a host.

Define características mecánicas (propiedades físicas como conectores (RS-232) o adaptadores), eléctricas (niveles de voltaje, velocidades de transmisión), las funcionales define que terminal mecánica o física corresponde a cada terminal eléctrica y de procedimientos (secuencia de eventos) de la capa física. [12]

En 1980 el departamento de la defensa liberó TCP/IP proceso que tardó en madurar desde 1978 a 1983, este modelo combina capas del modelo OSI. TCP/ IP es el protocolo estándar para conectarse a internet y a los servidores web. Por ejemplo, algunas empresas utilizan TCP/IP para interconectar todas las redes de su empresa, aunque ésta no esté conectada a redes externas. Otros grupos utilizan TCP/IP para la comunicación entre sitios geográficamente distantes. [21]

Cada capa tiene asociados uno o más protocolos, como se muestra en la figura 6, donde se indica el mapeo del modelo ISO al modelo TCP/ IP, adicionalmente se muestran algunos protocolos empleados en cada capa

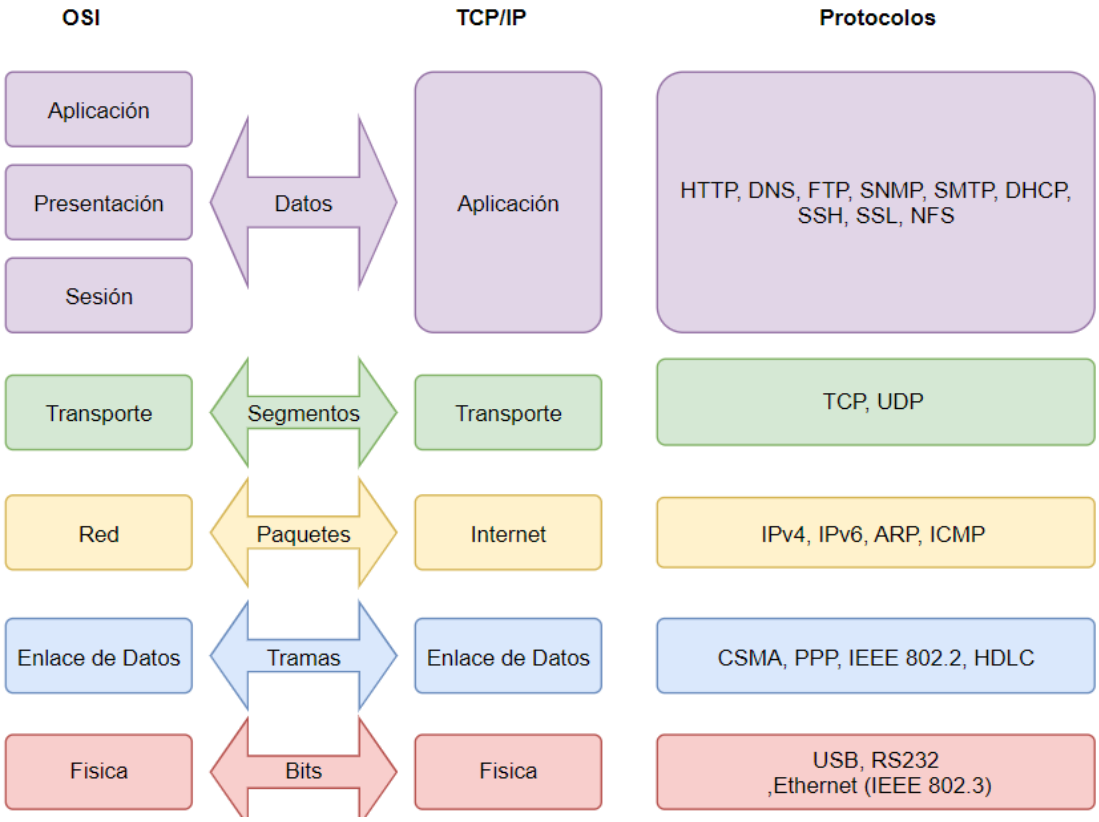


Figura 6. Modelo OSI y su mapeo a TCP/IP

2.4 PROTOCOLOS

La comunicación entre computadoras se rige mediante normas estandarizadas que determinan cómo se transmiten los datos, garantizan y simplifican la comunicación a través de la red, llamados protocolos. En la década de los 70 se desarrollaron varios protocolos propietarios de las distintas compañías que producían computadoras y que también competían en la industria de las redes de datos. Entre ellos funcionan en las capas de comunicación del modelo OSI/ TCP IP. [12]

2.4.1 CAPA DE FÍSICA

Especifica protocolos de *hardware*, Ethernet y conectores que contienen diversas capacidades para transportar datos.

El Estándar **RS- 232** (*Recommended Standard 232*- Estándar Recomendado 232) fue desarrollado por EIA (*Electronic Industries Alliance*- Alianza de Industrias Electrónicas) en 1962, utilizado en distancias cortas y sólo conexiones punto a punto entre dos dispositivos ya sea usando el conector DB9 o DB25 con un cable tipo *null*. Se genero para intercambiar datos binarios entre dispositivos DTE (Equipo terminal de datos ejemplo: PC) y un DCE (Equipos de comunicación de datos ejemplo: Módem), sin embargo, no existe restricción de comunicación entre dos DTE. Posteriormente fueron remplazados por el estándar **USB (*Universal Serial Bus* - Bus Universal en Serie)** en 1996, protocolo de comunicación serial asíncrono que permite conectar y desconectar en cualquier momento los periféricos como impresoras, teléfonos móviles, VoIP, *pendrives*, discos duros externos, por nombrar algunos. Usando el modelo *hub-root-host*, USB es un bus punto a punto dado que requiere un host de partida y un destino. [12,13]

Como se observa en la siguiente tabla 2, USB ha tenido una evolución notable de la versión 4.0 a la 4.2 duplicando la velocidad de transferencia hasta 80 Gbps. utilizando cableado de alta velocidad que permiten el rendimiento de datos.

Versión	Años de liberación	Ancho de banda
USB 1.1	1996	12 Mbps
USB 2.0	2000	480 Mbps
USB 3.0	2008	4.8 Gbps
USB 3.1	2013	5/10 Gbps
USB 3.2	2017	10/20 Gbps
USB 4.0	2019	40 Gbps
USB 4.2	2022	80 Gbps

Tabla 2. Anchos de banda soportando en las versiones de USB [12,16]

Ethernet

En 1977 Xerox creó y patentó Ethernet con el fin de comunicar computadoras y redes de computadoras, esto se realiza a través de cables de redes, el protocolo de Ethernet permite establecer conexión para el intercambio de paquetes de datos sobre cable ya sea coaxial, fibra óptica o par trenzado, éste último es el más utilizado en las empresas. En 1991 se definen estándares para el cableado estructurado por la TIA/EIA (*Telecommunications Industry Association/ Electronic Alliance*- Asociación de la Industria de Telecomunicaciones). [12]

Categoría	Ancho de banda	Ancho de banda de señal	Estándar
5	1,000 Mbps 1 Gbps	100 Mhz	10BASE-T, 100 BASE-TX [IEEE 802.3u], 1000BASE-T [IEEE 802.3ab] (1999)
5e	3,000 Mbps 3 Gbps	350Mhz	Mismos cables que cat 5, distancia máxima 100m 10BASE-T y 100BASE-TX Reduce Crosstalk
6	10,000 Mbps 10 Gbps	250 Mhz	10BASE-T, 100BASE-TX, 1000BASE-T 10GBASE-T[IEEE 802.3an](2006). Se limita la distancia a 55m
6ª	10 Gbps	500 Mhz	Igual que categoría 6 pero mayor frecuencia y mejoras en la reducción de interferencia y crosstalk

Tabla 3. Muestra la categoría de cable UTP(Un-Shielded Twisted Pair - Par Trenzado No-Blindado) más usada [12 ,16].

Los datos que se trasmiten viajan de tres maneras. El modo *simplex*, también denominado unidireccional, es una transmisión en una sola dirección. Se le llama *half duplex* cuando los datos circulan en una sola dirección por vez, el canal de comunicaciones permite alternar la transmisión en dos direcciones. Se le denomina *full dúplex* cuando los datos circulan en ambas direcciones a la vez [17]

2.4.2 CAPA DE ENLACE DE DATOS

En todo momento las personas solicitamos y recibimos información a través de la red, esta información viaja a través de un medio que es la vía por la cual se transporta los datos, durante el proceso de envió de información se usan protocolos que nos permiten recibirla la información sin errores.

CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*- Acceso Múltiple por Detección de Portadora con Detección de Colisiones) Su funcionamiento está diseñado

para redes que comparten el medio, básicamente detecta si un medio transporta señal y evita colisiones, esto significa que todos las estaciones puede transmitir y recibir a la vez. Al transmitirse las tramas, primero verifica si la línea está transmitiendo, si esta inactiva puede trasmitir, en caso de estar ocupada, espera e intenta transmitir otra vez hasta que la línea esta desocupada. Es probable que si dos estaciones transmiten al mismo tiempo pueden desencadenar una colisión. Si detecta que la trama recibida no es válida, la estación receptora simplemente ignorará la trama y la estación de envío espera un período de tiempo aleatorio y luego reanuda la transmisión de datos [12, 13]

La transmisión de información se realiza mediate el control al medio físico por conmutación de circuitos o de paquetes

- Conmutación de circuito: Método de comunicación en el que se establece un camino de comunicación entre dos dispositivos a través de uno o más nodos de conmutación intermedios. A diferencia de la conmutación de paquetes, los datos digitales se envían como una secuencia continua de bits. El ancho de banda está garantizado y el retardo está limitado esencialmente al retardo de propagación. El sistema telefónico utiliza conmutación de circuitos.
- Conmutación de paquetes: Método de transmisión de mensajes a través de una red de comunicación en la que los mensajes largos se subdividen en pequeños paquetes. Los paquetes se transmiten después como en conmutación de mensajes. [13]
- Conmutación de mensajes: Esta técnica es la más antigua, usada en sistemas telegráficos. Para transmitir un mensaje el emisor debe enviar el mensaje completo a un nodo intermedio el cual lo deja en cola donde almacena varios mensajes que son enviados por otros nodos. Luego, cuando es el turno del mensaje lo envía al receptor. El nodo temporal debe tener una gran capacidad de almacenamiento.

PPP (*Point-to-Point Protocol*-Protocolo punto a punto). Protocolo de encapsulamiento que permite que más de un protocolo de la capa de red funcione simultáneamente en el mismo enlace de comunicación. El Protocolo punto a punto

proporciona un método para transmitir datagramas sobre enlaces seriales punto a punto. PPP se compone de tres componentes principales:

1. Un método para encapsular datagramas sobre enlaces seriales.

2. Un LCP (*Link Control Protocol*- Protocolo de Control de Enlace) para establecer, configurar, y probar la conexión de enlace de datos.

3. Un conjunto de NCP (*Network Control Protocols*- Protocolos de Control de Red) para establecer y configurar diferentes protocolos de capa de red. [18]

2.4.3 CAPA DE RED

Los protocolos utilizados en esta capa se utilizan para incluir y trasportar los datos de usuarios a través de la red, como, por ejemplo:

IPV4 (*Internet Protocol version 4* - Protocolo de Internet, versión 4). Permite dar direcciones IP a los equipos, estas direcciones lógicas son de 32 bits de cuatro octetos. Las direcciones IP nos indican en qué red del mundo se encuentra nuestro dispositivo

IPV6 (*Internet Protocol version 6* - Protocolo Internet, versión 6). La versión 6 es la nueva versión del Protocolo Internet y sucesor de la versión 4, sus principales cambios son los siguientes:

- Capacidades de Direccionamiento Extendida: El IPv6 incrementa el tamaño de la dirección IP de 32 bits a 128 bits, soporta más niveles de jerarquías de direccionamiento y más nodos direccionables.

- Simplificación del formato del encabezado. Algunos campos del encabezado de IPv4 se eliminan o se hacen opcionales
- Soporte mejorado para extensiones y opciones. Cambios en la manera que se codifican las opciones del encabezado.

- Capacidades de autenticación y privacidad: Extensiones para utilizar autenticación, integridad de los datos, y (opcional) confidencialidad de los datos [19]

ARP (*Address Resolution Protocol*- Protocolo de Resolución de Direcciones). Realiza un mapeo y relación dinámico de las direcciones IP de la capa 3 a las direcciones MAC de la capa 2. [12]

ICMP (*Internet Control Message Protocol* - Protocolo de Control de Mensajes de Internet): Como su nombre lo indica este protocolo controla y notifica los errores de procesamiento de datagramas del protocolo de Internet, además informa a la fuente original con el fin evitar y corregir los errores. [20]

2.4.4 CAPA DE TRANSPORTE

En la capa de transporte se establece, mantiene y cierra los circuitos virtuales entre aplicaciones usando puertos de comunicación. Tanto UDP(*User Datagram Protocol* - Protocolo de Datagrama de Usuario) como TCP (*Transmission Control Protocol*- Protocolo de control de transmisión) envían información segmentada desde la computadora emisora con el objetivo de reducir errores y la computadora que receptora ensambla la información. Para que estos protocolos puedan transportar información interactúan con las aplicaciones de los usuarios de la capa de aplicación y por otro lado funcionan con el protocolo inferior sobre el protocolo IP de la capa de red, como se muestra en la figura 7. [12]

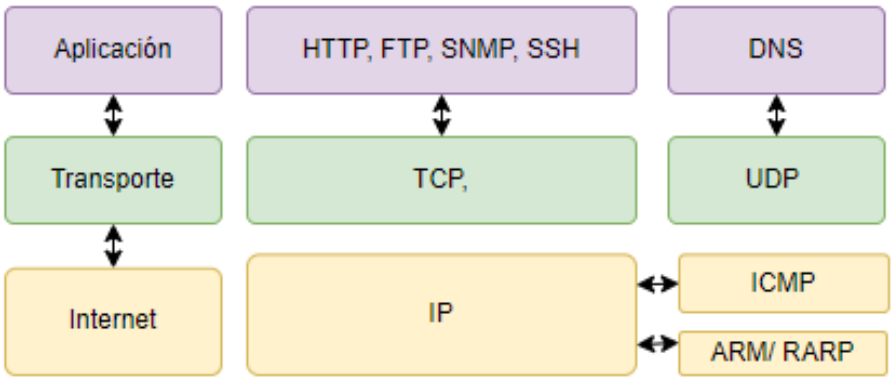


Figura 7. Muestra la comunicación de UDP/TCP con los protocolos de las capas 3 y 5 de modelo TCP/IP [12]

UDP Permite la transmisión de datagramas sin conexión para los procedimientos de la capa de aplicación en redes basadas en IP, los paquetes se envían en direcciones diferentes entre el emisor y el receptor, lo que no garantiza la entrega de datagramas UDP. Sin embargo, UDP permite al remitente especificar números de puerto de origen y destino para el mensaje y calcula la suma de comprobación de los datos y la cabecera [22]. A diferencia de TCP que valida y envía una numeración secuencial.

UDP envía múltiples datagramas en un menor tiempo, por ejemplo, una llamada por Internet (voz/video), es ideal para programas que requieren mayor velocidad, ya que este protocolo no verifica la información. Por ejemplo, en una video conferencia, la perdida de datos se interpreta en distorsión.

TCP está diseñado para ser utilizado como un protocolo confiable entre computadoras en múltiples redes, orientado a la conexión. Reconoce y garantiza que la entrega de datos no contenga errores y respeta el orden de transmisión, así como reenvía datos perdidos.

El TCP es capaz de transferir un flujo continuo de datos y lo logra dividiendo en segmentos la información, a estos segmentos se les inserta un identificador con el número de secuencia y requiere un acuse de recibo positivo ACK (Acknowledgment-Reconocimiento). Si no se recibe el ACK dentro de un intervalo de tiempo de espera, los datos se retransmiten. Después de ensamblar los segmentos de forma ordenada para la entrega a destinatario. Un ejemplo es el envío de imágenes, documentos y archivos. Para finalizar la conexión cliente- servidor se envía un mensaje de confirmación y fin. [23]

Las banderas que utiliza para el envío de segmentos son:

- SYN y FIN Apertura y el cierre de la conexión
- ACK: Acuse de recibido
- RST (*Reset*): Reiniciar

TCP nos garantiza la entrega de información sin errores basados en su procedimiento y cierre de conexión mientras UDP garantiza mayor velocidad

2.4.5 CAPA DE APLICACIÓN

Los protocolos de la capa de aplicación proporcionan servicios al usuario como trasferencia de datos, navegación en internet, correo electrónico y administración de red. En la tabla 4 podemos ver algunos protocolos que interactúan en la capa 5 del modelo TCP/ IP.

Protocolo	Puerto	Nombre	Descripción
HTTP	80	*Hypertext Transfer Protocol* - Protocolo de transferencia de hipertexto	Se utiliza para transferir y visualizar documentos de hipertexto y XML(*Extensible Markup Language*- Lenguaje de Marcado Extensible) via WWW (World Wide Web- Red Mundial)
DNS	53	*Domain Name System protocol*- Protocolo de Sistema de Nombres de Dominio	Gestiona nombre de sistemas principales y sus direcciones IP asociadas. Con ello se utilizan los nombres simples como www.prueba.com en lugar de 192.168.l.254 IPv4 .
FTP	20/21	*File Transfer Protocol* - Protocolo de transferencia de archivos	Protocolo de red para intercambio de archivos, diseñado para ser utilizados por programas
SNMP	161/162	*Simple Network Management Protocol*- Protocolo simple de gestión de red	Protocolo para la gestión de red, permite el monitoreo de los dispositivos de la red (*firewall, switch, router* o cualquier dispositivo con una IP y un agente SNMP)
SMTP	25	*Simple Mail Transfer Protocol*- Protocolo simple de transferencia de correo	El objetivo es transferir correos electrónicos y archivos adjuntos de forma confiable y eficiente. Se caracteriza por transportar correos a través de varias redes
DHCP	67/68	*Dynamic Host Configuration Protocol*- Protocolo de Configuración Dinámica de Host	DHCP asigna una dirección IP permanente a un cliente. En "asignación dinámica", DHCP asigna una dirección IP a un cliente por un período de tiempo limitado (o hasta que el cliente explícitamente renuncia a la dirección). En "asignación manual", el administrador de la red asigna la dirección IP y se usa DHCP simplemente para transmitir la dirección asignada al cliente

Tabla 4. Protocolos utilizados en la capa de aplicación de TCP/IP [24, 25,26, 27]

2.5 CABLEADO ESTRUCTURADO

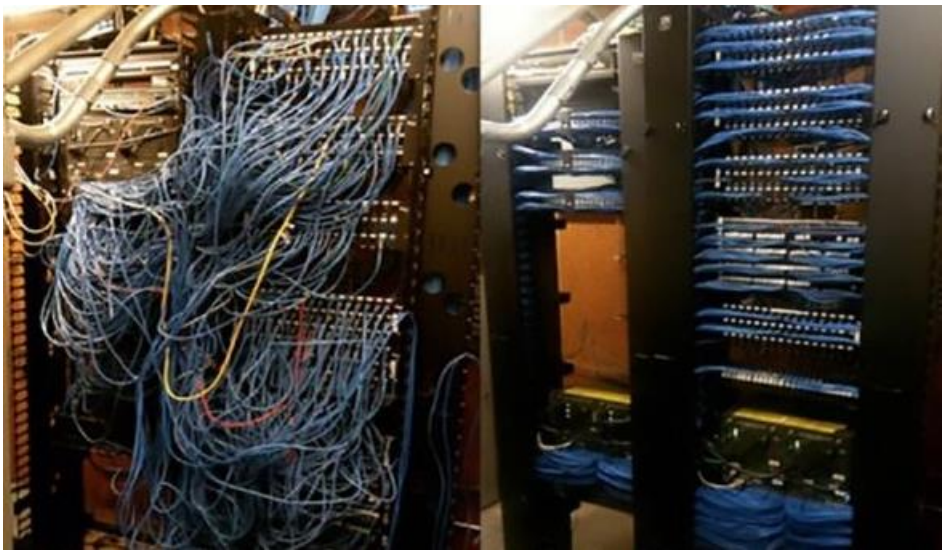
El cableado estructurado se concentra en la capa física y nos permite organizar, identificar e interconectar dispositivos de diferentes tecnologías, como hardware, cables, canaletas, conectores, con el fin de integrar sistemas de telecomunicación para la transferencia y control de voz, datos, video y/o conexiones inalámbricas.

En 1991 la TIA/EIA (*Telecommunications Industry Association/ Electronic Alliance*) definen el estándar para el cableado estructurado TIA/EIA-568-A y fue actualizado en 1995 por TIA/EIA-568-B derivado del avance tecnológico.

Tener un cableado estructurado en cualquier lugar de trabajo o sucursal tiene beneficios como:

- Reducir el mantenimiento continuo
- Facilitar futuros cambios de equipos y servicios
- La detención de errores
- Fallas en la red.
- Permite integrar nuevos sistemas de telecomunicaciones

En la figura 8 se muestra un sitio de datos con cableado sin organizar y un estructurado



(a) (b)

Figura 8. Comparativo de cableado (a) sin organización (b)Cableado estructurado [28]

La arquitectura del cableado estructurado de telecomunicaciones está integrada por diversos componentes que a continuación se indican:

2. Cableado horizontal: Une el área de trabajo con el cuarto de telecomunicaciones, debe estar diseñada para: Voz, datos, LAN, Video, sistemas de señalización (incendios, seguridad, otros)
3. Cableado vertical o troncal *(backbone):* Interconecta todos los cuartos de telecomunicaciones
4. Área de trabajo (WA- *Work Area):* Es donde se encuentran los nodos de trabajo: computadoras, impresoras, teléfonos, terminales de datos y computadoras
5. Cuarto de telecomunicaciones: Es el lugar donde se encuentra los dispositivos de comunicación, proporciona la administración y el enrutamiento de los cables de los equipos secundarios.
6. Cuarto de equipos: Proporciona un entorno controlado para alojar equipos de telecomunicaciones, flujo de aire, sistema de protección (*Data center*).
7. Instalación de entrada: Es la entrada de los servicios del ISP, acceso por donde se interconectan las sucursales y los dispositivos de protección
8. Administración: Mediante planos facilita a los administradores el manejo de los servicios conectados, identificando cada componente del cableado estructurado [29]

2.6 CENTRO DE DATOS

Un centro de datos debe estar planificado para poder distribuir diferentes servicios de comunicación, la norma TIA-942-A especifica los requisitos mínimos para la creación de centros de datos, a continuación. Se muestra algunos requisitos mínimos [30]:

- Altura: Altura minina de cuarto de comunicaciones 2.6 m desde el suelo hasta el techo, requisitos para los armarios/ racks 2,13 m
- Lugar: el cuarto de comunicaciones debe considerar:
  1. No debe contar con ventanas exteriores ya que aumentan la carga térmica y reducen la seguridad.
  2. Lejos de tuberías que ocasionen filtraciones de agua
  3. Prevenir un medio de evacuación.
  4. Evitar ubicaciones restringidas que limiten la expansión, como ascensores, el núcleo del edificio, paredes exteriores u otras paredes fijas del edificio.
  5. Fuera de lugares que puedan ser inundados
  6. De preferencia el cuarto de telecomunicaciones se ubicará en un lugar central a las estaciones de trabajo.
  7. Calefacción y ventilación funcionará las 24 horas de los 365 días
  8. Protección contra incendios y extintores deben cumplir normas
  9. Iluminación: Las luminarias deben situarse sobre los pasillos, y contener alumbrado de emergencia
  10. Puerta: La puerta deberá ser de un ancho mínimo de 1 metro y altura de 2.13 metros libres sin marco. La puerta puede ser desmontable para facilitar el acceso a equipos grandes. La puerta del cuarto de comunicaciones se deberá abrir siempre hacia fuera
  11. Señalización: Se debe desarrollar bajo las condiciones de la sucursal.
  12. Parámetros operativos como humedad y temperatura

La norma define una serie de elementos para el diseño y construcción de un centro de datos, en la figura 9 se muestran estos subsistemas que se deben contemplar para una certificación TIER que cumpla con la disponibilidad, redundancia y tolerancia a fallas.

Cuadro 1.

Telecomunicaciones	Arquitectura	Eléctrica	Mecánica
Cableado de racks	Selección del sitio	Cantidad de accesos	Sistemas de climatización
Accesos redundantes	Tipo de construcción	Puntos únicos de falla	Presión positiva
Cuarto de entrada	Protección ignífuga	Cargas críticas	Cañerías y drenajes
Área de distribución	Requerimientos NFPA 75	Redundancia de UPS	Chillers
Backbone	Barrera de vapor	Topología de UPS	CRAC´s y condensadores
Cableado horizontal	Techos y pisos	PDU's	Control de HVAC
Elementos activos redundantes	Área de oficinas	Puesta a tierra	Detección de incendio
Alimentación redundante	NOC	EPO (Emergency Power Off)	Sprinklers
Patch panels	Sala de UPS y baterías	Baterías	Extinción por agente limpio (NFPA 2001)
Patch cords	Sala de generador	Monitoreo	Detección por aspiración (ASD)
Documentación	Control de acceso	Generadores	Detección de líquidos
	CCTV	Transfer switch	

Tabla 5. Subsistemas que deben contemplarse para una certificación de centro de datos [30, 31]

2.7 PATCH PANEL

Un patch panel es un dispositivo de red eficaz y flexible que permite mantener organizado una red LAN y se encarga de recibir por la parte posterior el cableado horizontal en los bloques IDC *(Insulation-Displacement Connector)* e interconectar a los equipos centrales como routers, switches por la parte frontal, conectándolos con RJ45.

En la tabla 6 se indican tres diferentes patch panel y sus características básicas.

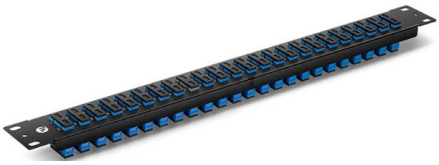
Tipo	Descripción	Imagen
***Patch panel* de cobre**	Para interconectar cableado Ethernet Cat 5e, Cat 6 o Cat 6ª.	
***Patch panel* de fibra óptica**	Admiten conectores de fibra óptica, incluidos el conector lucent (LC), el conector de suscriptor (SC) y los conectores de punta recta (ST)	
***Patch panel* coaxial**	Patch panel coaxial. Se utilizan para instalaciones audiovisuales, en lugar de LAN	

Tabla 6 Tipos de patch panel (existen presentaciones de 12 a 96 puerto) [32]

2.8 RACK

Estructura metálica diseñada para alojar equipos de comunicaciones y los diferentes elementos para el cableado estructurado. Tiene como objetivo organizar todos los dispositivos de telecomunicaciones como: switches, servidores, sistemas de redes, telefonía o firewalls. Su uso es básico para la instalación de equipos ya que son atornillados por los laterales y tienen beneficios como: mejorar la organización de equipos, permiten el flujo de aire y les dan seguridad a los equipos

En la siguiente tabla se muestran los diferentes tipos de rack, su capacidad y dimensiones dependen modelo y marca.

Rack	Característica	Imagen
Soporte de pared	Diseñado para soluciones pequeñas, peso soportado hasta 40kg , capacidad para 4UR UR: Unidades *Rack*	
***Rack* abierto de pared**	Diseñado para espacios muy pequeños son una solución rápida ya que son de fácil instalación, capacidad 6 hasta 24 UR.	
Gabinete compacto	Ideal para soluciones pequeñas, peso soportado hasta 60 kg , capacidad para 9UR.	
***Rack* abierto de piso**	Sirven para organizar cualquier sistema de cableado, equipamiento activo y equipamiento estructural. Soporta hasta 900Kg, capacidad hasta 42 UR	
***Rack* cerrado de piso**	Sirve para guardar los servidores de gran capacidad, soporta hasta 1700Kg, capacidad hasta 42 UR	

Tabla 7. Tipos de *rack*

2.9 CONCEPTOS PARA EL DIAGNÓSTICO DE LA SEGURIDAD WLAN

Las redes WLAN (*Wireless Local Area Network*- Red de área local inalámbrica *)* han evolucionado y continuarán desarrollándose con el fin de proporcionar mejores anchos de bandas, la conexión inalámbrica ha brindado beneficios en la comunicación entre personas permitiendo incrementar la productividad en los corporativos y en el ámbito educativo, Actualmente es la red más utilizada y con mayor posibilidad de conexión tanto en redes públicas como privadas, sin embargo, esto implica ataques a causa de vulnerabilidades para cualquier dispositivo donde puede comprometer la seguridad personal o de corporativos, cualquier tipo de sistema operativo no se encuentra exento (Android, IOS, Linux, macOs, Windows)

De acuerdo a Cisco el *"*62% de los ciberataques tienen como principal foco las pequeñas y medianas empresas, en alrededor de 4000 incidentes al día a nivel mundial. Cuando una empresa permite conectividad inalámbrica en sitio abierta a empleados, clientes o cualquier visitante externo, el campo de ataque potencial se amplía exponencialmente debido a los distintos usuarios y dispositivos tienen acceso a la red" [33]. Lo que indica que se debe contar con redes inalámbricas seguras.

Los principales riesgos de seguridad son:

- Ataques de denegación de servicios (DoS- *Denial of service)* y denegación de servicios de tipo distribuidos (DDoS- Distributed denial of service). Son ataques destinados a una maquina o red, el atacante realiza envío masivo de tramas inundando de tráfico la red, lo cual desencadena un bloqueo o saturación de servicio que posteriormente hace que se detenga totalmente.

  En la figura 9 se muestra un ejemplo de un ataque DDoS mediante solicitudes a un servidor DNS, utilizando la dirección IP falsificada del remitente, luego el servidor DNS envía su respuesta al servidor cliente, esto cuando se hace masivo las respuestas de DNS causan estragos en el servidor destino [34]

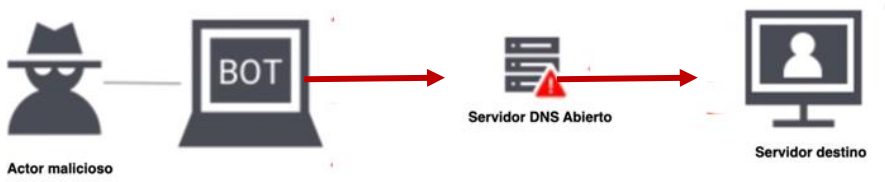


Figura 9. Ejemplo de un ataque DDoS imagen tomada de [34]

Estos ataques de denegación de servicio son el resultado de los siguientes escenarios [35]:

a) Equipos mal configurados: un router mal configurado puede ser el causante de que un usuario malintencionado realice un ataque de DoS. Los ataques pueden ser difícil de distinguir, sin embargo, existen algunas alertas que deben considerarse, por ejemplo, ya sea que una computadora, un sitio web o la red se vuelve más lenta o no responde, por lo tanto debe identificarse si se trata de un ataque mediate el monitoreo de trafico de la red, posteriormente se debe identificar la IP del atacante o la computadora con el comportamiento irregular, finalmente se debe mitigar la situación con algunas medidas, por ejemplo:
    a. Coordinar con el ISP el filtrado de tráfico malicioso
    b. Configurar reglas en el firewall para bloquear el tráfico malicioso
    c. Realizar monitoreo de tráfico y análisis de registro de eventos para registrar el avance del ataque y realizar mejoras en las medidas preventivas para mitigar ataques

    A continuación, se enlistan algunas recomendaciones:

    I. Mantener actualizado el sistema operativo de los equipos de cómputo con un antivirus actualizado
    II. Crear políticas para equipos de usuario final y de red
    III. Cambiar la configuración de fábrica y utilizar contraseñas fuertes en los router y firewalls
    IV. Uso de listas blancas, es decir, un listado de direcciones MAC que serán las únicas que estarán autorizadas para conectarse a la red

V. Implementar en las aplicaciones web un WAF (firewall de aplicación web)

b) Usuarios malintencionados interfiere en la comunicación inalámbrica intencionalmente

c) El uso de funciones vulnerables en la programación de una aplicación puede provocar que un atacante realice una inyección de SQL que consiste en colocar código malicioso en una sentencia al realizar una consulta a través de una página web, por ejemplo, el atacante modifica una consulta SQL, de manera tal que el servidor aumente considerablemente su carga y tiempo de respuesta hasta lograr el esperado servicio de denegación. Recomendaciones: deben incorporar seguridad en cada paso del ciclo de vida de desarrollo del software, planificar las posibles amenazas a la seguridad desde el principio y probar, escanear, auditar y revisar el código durante todo el desarrollo, además se puede incluir herramientas y automatizar las comprobaciones de seguridad en casi todas las fases del desarrollo, por ejemplo, incluir:

I. Kali Linux que es una caja de herramientas orientada para realizar investigación de seguridad, ciencia forense, ingeniería inversa y pruebas de penetración

II. Nmap es un escáner de red de código abierto que se utiliza para descubrir servicios de alojamiento y redes informáticas, en donde se puede realizar un análisis activo que indicará qué puertos están abiertos y qué servicios se están publicando

- Espionaje corporativo: Robo de información sensible como datos comerciales o de estrategia. Los principales actores son: Trabajadores activos, inactivos o un incorrecto procedimiento para el borrado de datos en los equipos de cómputo o servidores, lo que puede ocasionar que una persona externa con conocimientos informáticos pueda recuperar la información, la mejor recomendación es realizar el

borrado seguro. Actualmente existen software certificados que te permiten realizar dicha acción un de ellos se llama Blancco.

- Acceso a dispositivos: Acceso a personas externas a la red corporativa.
- Infección a la red o dispositivos con virus o malware: Un malware o ransomware realiza un secuestro de información, con esto, impide a los usuarios acceder a su sistema o archivos y solicita el pago de rescate para volver acceder a ellos.
- Instalación de aplicaciones no autorizadas o sin licencia.

2.9.1 ESTÁNDARES DE REDES INALÁMBRICAS WLAN

A mediados de la década de los 80 la FCC (*Federal Communications Commision*- Comisión Federal de Comunicaciones) asigna la banda de frecuencia ISM (*Industrial Scientific and Medical*- Banda de frecuencia industrial, científica y médica) mientas la ITU (International Telecommunication Union - Unión internacional de Telecomuncaciones) gestiona y garantiza la utilización del espectro de RF para aplicaciones y tareas industriales, científicas y médicas. Con el desarrollo de productos y la evolución de la comunicación inalámbrica y aplicaciones multimedia se hizo popular utilizar la banda ISM para sistemas de comunicación de corto alcance y baja potencia como, teléfonos inalámbricos, WiFi, Bluethooth, enlaces punto a punto, entre otras aplicaciones. La desventaja de ISM es la falta de protección contra interferencia en equipos analógicos, para garantizar la comunicación utilizan la transmisión de espectro ensanchado donde ocupa un espectro de frecuencia amplio, excepto para aplicaciones de potencia baja, ofreciendo cierta protección tanto para los usuarios de banda estrecha en los rangos asignados por la ISM. Sin embargo, la FCC permite el uso de técnicas de modulación de banda estrecha [36].

En la figura 10 Se muestra el espectro de frecuencia y se indica la localización de las WLAN

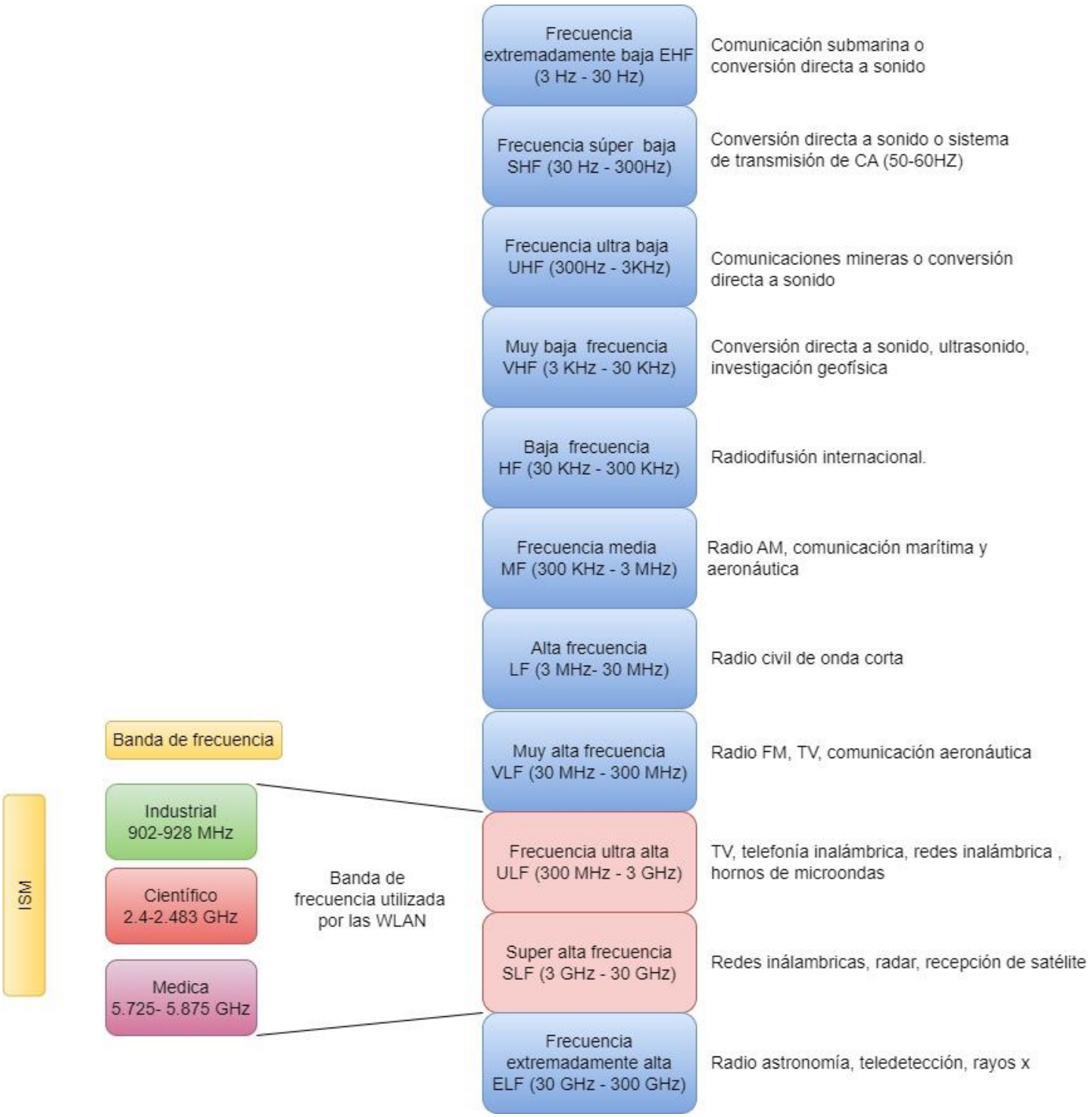


Figura 10. Banda de frecuencia ISM. Imagen propia.

La diferencia en los rangos para 2.4Ghz y 5.0 Ghz se encuentra en la velocidad máxima y RF (*Radio frequency*- Radio de frecuencia) que la red que puede alcanzar, por ejemplo, en la figura 11 nos indica que para la frecuencia 5 GHz nos proporciona mayor velocidad de conexión, menor alcance de red y menor interferencia a comparación de la frecuencia 2.4 que proporciona mayor interferencia, capacidad de penetrar paredes, menor velocidad de conexión y mayor rango de red

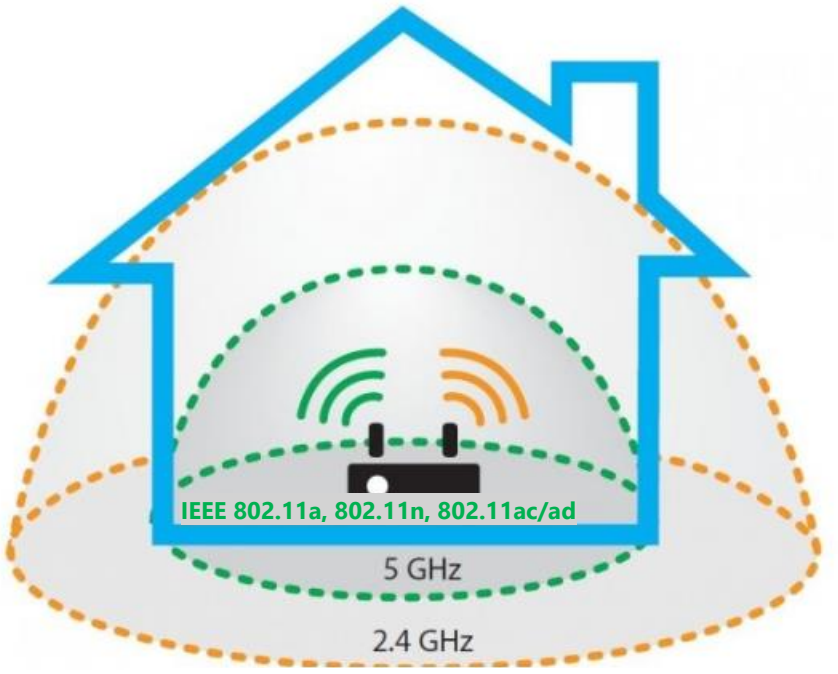


Figura 11 alcance de la red y estándares relacionados, propia con base en [37]

La IEEE (Institute of Electrical and Electronics Engineer- Instituto de Ingenieros Eléctricos y Electrónico) creó el estándar 802.11 para redes inalámbricas conocido como WLAN con el fin de permitir establecer conexión inalámbrica mediante reglas y especificaciones mínimas que permiten conectar cualquier dispositivo compatible con WiFi, trabaja en la capa física, control de acceso al medio y la subcapa MAC y ha tenido una evolución como se muestra en la tabla 8.

Estándar	Frecuencia	Velocidad máxima	Año de lanzamiento	Descripción
802.11	2.4 GHz	1 a 2 Mbps	1997	
802.11a	5.0 GHz	54Mbps	1999	
802.11b	2.4 Ghz	11 Mbps	1999	Los dispositivos que implementan este estándar tienen un mayor alcance y pueden penetrar mejores paredes. No tiene compatibilidad con los dos anteriores.
802.11g	2.4 GHz	54Mbps	2003	Es compatible con el estándar anterior 802.11b. Sin embargo, cuando admite un cliente 802.11b, se reduce el ancho de banda general.
802.11n	2.4 y 5.0 GHz	150-600Mbps	2009	El estándar 802.11n es compatible con dispositivos 802.11a/b/g anteriores.
802.11ac	5 GHz	450 Mbps-1.3 Gpbs	2013	El estándar 802.11ac es compatible con dispositivos 802.11a/n anteriores
802.11ad	2.4, 5Ghz, 60 Ghz	Hasta 7 Gbps	2014	la banda de 60 GHz es una tecnología de línea de vista y, por lo tanto, no puede penetrar las paredes. Cuando un usuario se mueve, el dispositivo cambia a las bandas más bajas de 2,4 GHz y 5 GHz. Compatible con 802.11 a/b/g/n/ac

Tabla 8. Evolución del estándar 802.11 [38]

2.9.2 REDES INALÁMBRICAS

Las redes inalámbricas nos permiten transmitir y recibir información desde cualquier dispositivo mediante AP (*Acces Point*- puntos de acceso) en un área determinada, sin necesidad de conectarlo vía alámbrico. En la tabla 9 se describen los tipos de redes inalámbricas.

TIPO	Alcance	Estándar	Tecnologías
WPAN (Redes de área personal inalámbrica)	<30m	802.15	Bluetooth y Wi-Fi Direct
WLAN (Red de área local inalámbrica)	Hasta 30 m	802.11 a/b/g/n/ac/ad	Wifi: Permite incluir tráfico de datos, voz y video
WWAN (Redes de área extensa inalámbrica)	Hasta 50 Km	802.16	Conexiones de banda ancha por cable y DSL. Se agregó la movilidad a WiMAX en 2005,

Tabla 9. Clasificación de redes inalámbricas [39]

2.9.3 ELEMENTOS TEÓRICOS- AUTENTIFICACIÓN

La gran mayoría de las WLAN utilizan una configuración de seguridad y ésta, define el método de autentificación y encriptación de los datos. Wi-Fi Alliance creó protocolos de seguridad que promueven y garantizan la conexión inalámbrica, interoperabilidad y seguridad. En 1999 se lanzó WEP (*Wired Equivalent Privacy*- Privacidad equivalente por cable) como la primera generación de métodos de autentificación con el objetivo de agregar seguridad a las redes inalámbricas mediante la encriptación de datos. Sin embargo, a medida que la tecnología evolucionó presentó un aumento de vulnerabilidades por lo que fue sustituido por WPA (Wi-Fi Protected Access – Acceso protegido Wi-Fi) en 2003, que compartía similitudes con WEP y adicionaron mejoras en la generación de claves para cada paquete, autorización de autentificación y se incluyó la comprobación de mensajes. Esto no fue suficiente por lo que en el 2004 lanza WPA2 (Wi-Fi Protected Access v2 – Acceso protegido Wi-Fi versión 2), la segunda generación mejorada de WPA el cual utiliza métodos de encriptación más avanzados. En el 2018 se lanzó la última versión WPA3 (Wi-Fi Protected Access versión 3 – Acceso protegido Wi-Fi versión 3), la cual incluye encriptado de datos individualizados, seguridad fuerte, configuraciones simples, actualmente no se a adoptado por la incompatibilidad de los dispositivos y su alto costo de implementación [40].

En la tabla 10 se indica la información relacionada con los protocolos y se hace mención del tipo de cifrado, integridad y la seguridad a los datos que son transmitidos [41, 42, 43].

Protocolos de autentificación	Método de cifrado	Integridad de datos	Estándar	Gestión de Claves
WEP (*Wired Equivalent Privacy*- Privacidad equivalente por cable) 1999	RC4	CRC-32 (Comprobación de redundancia cíclica)	802.11b Bajo	Cifrado de clave asimétrica Usa una clave de 64 y 128
WPA(Wi-Fi Protected Access – Acceso protegido Wi-Fi) 2003	WEP con cifrado TKIP (*Temporal Key Integrity Protocol*- Protocolo de integridad de clave temporal)	MIC (Message Integrity Codes - Comprobación de integridad del mensaje)	802.11g Moderado	WPA+PSK PSK *(Phase Shift Keying*- Codificación por desplazamiento de fase) Usa una clave de 128 a 256 bits para el cifrado
IEEE 802.11i/WPA2 (Version 2) 2004	AES (Advanced Encryption Standard- Estándar de cifrado avanzado)	CCMP	802.11i Seguro	PMK + PSK PMK (Pairwise Master Key- Clave Maestra por Pares) Usa una clave de 128 a 256 bits para el cifrado
WPA 3 (Version 3) 2018	AES- CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol- Protocolo de código de autenticación de mensajes en modo contador con encadenamiento de bloques de cifrado.) AES- GCMP (Galois/Counter Mode Protocol- Protocolo de modo contador de Galois)	SHA-2	IEEE 802.11ax Muy seguro	WPA2+WPA3 Usa una clave de 192/256/384 bits para el cifrado

Tabla 10. Características principales y evolución de los protocolos de autentificación

WPA, WPA2 y WPA3 tienen dos versiones de autentificación:

- Personal: Los usuarios se autentican mediante una clave previamente compartida PSK. Está diseñada para las redes domésticas o de oficinas pequeñas.
- Empresarial: Utiliza el estándar 802.1x, con cifrado de clave TKIP para evitar el acceso no autorizado a la red mediante la verificación de los usuarios, requiere un servidor de autenticación RADIUS (Remote Authentication Dial-In User Service- Protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP). Su configuración es más complicada, proporciona control individualizado, centralizado sobre el acceso a la red inalámbrica [44].

Operación de servidor RADIUS

1. El cliente solicita acceso al servidor RADIUS a través de la red. Si la solicitud no es atendida en un lapso de tiempo, es reenviada.
2. Recepción de la solicitud de servidor RADIUS, si el cliente es válido, el servidor RADIUS consulta la base de datos para verificar en nombre del usuario y contraseña

   Si existen condiciones no válidas, el servidor envía un “Acceso denegado”, si las condiciones se cumplen envía una verificación de identidad al que el usuario debe responder [45]

WEP. La privacidad equivalente por cable del estándar IEEE 802.11, proporciona integridad en los datos asegurándose que no sean modificados y detecta errores, esto lo realiza con el protocolo CRC-32 (*Cyclic Redundancy Checking*- Verificación por redundancia cíclica) y ofrece un algoritmo de cifrado con RC4 (*Rivest Cipher 4*- Cifrado Rivest 4) tenido como acrónimo Ron´s Code 4, funciona en la capa de enlace de datos. WEP cifra el tráfico con una clave estática hexadecimal de 64 o 128 bits, que se compone de la siguiente forma [46]

- 64 bit (24 IV + 40 Clave)
- 128 bit (24 IV + 104 clave)

Donde IV es el Vector de inicialización (Contador)

Para RC4 su función es muy básica y consiste en cifrar un mensaje mediante una operación XOR y una secuencia de clave, que cambian dinámicamente durante la secuencia cifrante, esto se realiza mediante dos algoritmos conocidos como KSA (Key Scheduling Algorithm) para la encriptación de paquetes y PRGA (*Pseudo- Random Generation Algorithm*- Generador pseudoaleatorio de números es un algoritmo) para la desencriptación de paquetes.

WAP continúa utilizando RC4 e incorpora el cifrado TKIP que proporciona una combinación de claves por paquete, una comprobación de la integridad del mensaje (MIC) y un mecanismo de regeneración de claves. TKIP garantiza que cada paquete de datos se envíe con su propia clave de cifrado única, considerando a TKIP más seguro que WEP [46]

WPA2 utiliza una técnica de cifrado y autentificación más avanzada llamada AES y CCMP [46].
AES es un cifrado de bloques de datos de 128 bits a la vez. WAP2 crea nuevas claves de sesión en cada cliente, estas claves son únicas y específicas. Cada paquete que se envía se cifra con una clave única y no existe reutilización de claves por ello WAP2 se considera más seguro que WAP.

WAP3, Ofrece autenticación y encriptación mejoradas. Utiliza el estándar 802.11ax, WPA3 será obligatorio con Wi-Fi 6 que requiere mayor seguridad. Utilizando WPA3 el tráfico del extremo se cifra hasta que el otro extremo sea autentificado

Ejemplo: Estás en cualquier establecimiento conectado a su red utilizando WPA2, cualquier atacante en el mismo lugar puede realizar un ataque Man-in-the-Middle hacia tu dispositivo mediante un ataque de fuerza bruta, en donde el hacker intenta adivinar la contraseña a través de una lista de palabras, combinaciones numéricas de uso frecuente, esto se previene con WPA3 [46].

Para WPA3-Personal la autenticación de contraseñas es más resistente, incluso cuando los usuarios eligen contraseñas que no cumplen con las recomendaciones de complejidad típicas. WPA3 aprovecha la autenticación simultánea de iguales (AES), un protocolo seguro que establece claves entre dispositivos, para proporcionar protecciones más sólidas a los usuarios contra intentos de adivinación de contraseñas por parte de terceros. Para WPA3-Enterprise, ofrece cifrado con base en claves de 192 bits, brindando protecciones adicionales para redes que transmiten datos confidenciales, ejemplo: Áreas de gobiernos o finanzas. [43]

En la tabla 11. se muestra las diferentes opciones de seguridad que existen:

Seguridad	Descripción
Abierta	Sin contraseña
WEP 64	Opción obsoleta e insegura
WEP 128	Opción obsoleta e insegura
WPA-PSK (TKIP)	Opción obsoleta
WPA-PSK (AES)	La información del usuario queda protegida y sólo los usuarios autorizados pueden acceder a la red
WPA2-PSK (TKIP)	Compatible con dispositivos antiguos
WPA2-PSK (AES)	Opción más segura, es un potente estándar de encriptación autorizado por Wi-Fi Alliance
WPA2-PSK (TKIP/AES)	Mayor riesgo de vulnerabilidad por la compatibilidad con equipos obsoletos
WPA3	Mayor protección ante ataques, cifrado de tráfico entre dispositivos y AP

Tabla 11. Opciones de seguridad

La tecnología WiFi es de uso común en los corporativos y los SOHO (Small Office, Home Office), en México se hizo común realizar home office a partir del año 2019 como un método de trabajo. La seguridad es fundamental en cualquier red inalámbrica ya que mantiene la confiabilidad, escalabilidad y eficiencia operacional, hoy en día es un tema crítico a nivel mundial de gran importancia ya que día a día nos exponemos a diversas vulnerabilidades. Un ejemplo claro es la fácil conectividad a las redes públicas por ejemplo en cafeterías, restaurantes, centros comerciales, aeropuertos, hoteles, parques o avenidas principales, de acuerdo a la información emitida por el gobierno de la Ciudad de México, la CDMX cuenta con 31,037 puntos de acceso que conectan hasta 1,082,599 usuarios simultáneos los cuales pueden acceder a redes abiertas [47]. Sin embargo, el método de autentificación abierta no es una opción confiable y que invariablemente repercute en la seguridad de datos. La responsabilidad de contar con sistemas de autentificación de clave compartida minimiza el riesgo de cualquier vulnerabilidad, además la seguridad de las WLAN no solo depende de herramientas seguridad, sino que conlleva un proceso de concientización de usuarios y políticas.

CAPÍTULO 3

METODOLOGÍA

INGENIERÍA INVERSA PARA LA CONFIGURACIÓN Y GESTIÓN

3.1 ANTECEDENTES

La empresa comercializadora de suministros médicos tiene una antigüedad mayor a 30 años en el mercado y opera de forma nacional e internacional, cuenta con un catálogo amplio de productos especializados en el ámbito médico

Actualmente cuenta con 165 empleados distribuidos en 6 sucursales, las sucursales se nombrarán en este trabajo como: sucursal principal 1, 2, 3, 4, 5, 6, en la figura 12 se marcará la ubicación geográfica en donde se encuentra cada sucursal.

Figura 12. Ubicación de las seis sucursales

3.2 RED DE EMPRESA

Cada sucursal tiene su propio centro, en la tabla 11 se muestra la distribución del personal y la topología en cada sitio.

Actualmente con el trabajo remoto y con el personal de campo (servicio al cliente) las sucursales no tienen la operación en un 100%. En la tabla 12 se muestran las sucursales con el número de personas en un escenario de operación del 100%.

Sucursal	Topología	# Personas
1 (CDMX)	Árbol	51 personas
2 (CDMX)	Estrella	59 personas
3(CDMX)	Estrella	12 personas
4 (EDO MEX)	Estrella	15 personas
5 (GDL)	Estrella	14 personas
6 (MTY)	Estrella	7 personas

Tabla 12. Topología de la red y distribución de personal

3.3 METODOLOGÍA

Para la realización de este proyecto de investigación se utilizó la metodología de ingeniería inversa, en la figura 13 se muestra las etapas para la creación del proyecto de tesis [48].

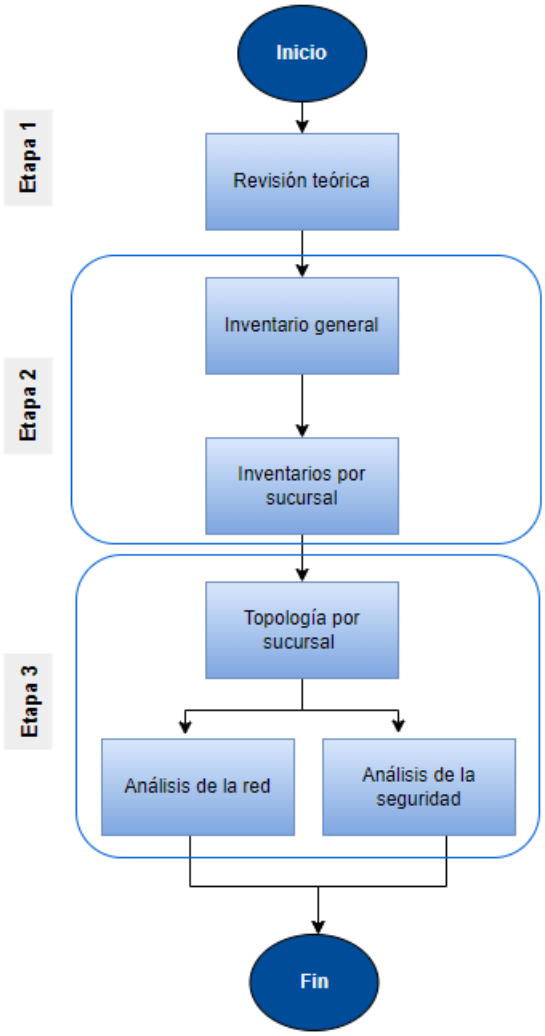


Figura 13. Etapas para el proyecto de tesis usando metodología ADVNETLAB

El la figura 14 muestra el diagrama general de la metodología de ingeniería inversa y se relaciona con las etapas para la creación del proyecto.

Etapa 1. Revisión teórica (3): Se realiza la recopilación de información, conceptos, objetivos y antecedentes de proyecto.
Etapa 2. Inventario físico (3): Se realiza una revisión física para la recopilación de cantidades, marcas, modelos y características de los dispositivos, para posteriormente segmentarlo para la reconstrucción de la red de cada sucursal.
Etapa 3. Topología (2) Con base en los diagramas proporcionados por el proveedor y la inspección física, se realiza el diseño y simulación de la topología por sucursal.

- Análisis de la red (1): Funcionamiento y características físicas del sistema (sistemas, programas, componentes y configuraciones)
- Análisis de la seguridad (1): Conocer el nivel de seguridad

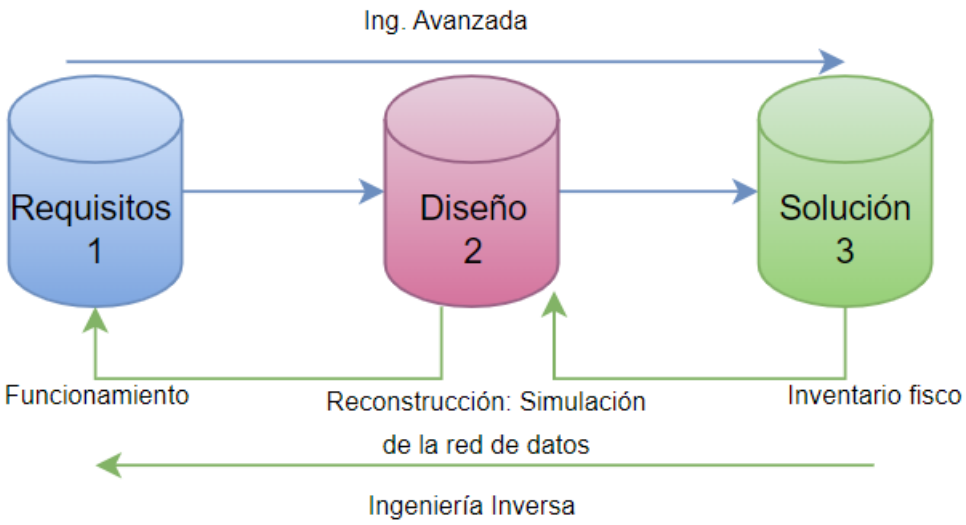


Figura 14. Diagrama de la metodología inversa aplicada para la reconstrucción de la red

En el presente capítulo se indicará el inventario físico de los equipos de comunicación utilizados en la empresa, indicando el equipo equivalente de Cisco.

3.4 TOPOLOGÍA DE CADA LAN

Analizando la figura 13 del diagrama de la sucursal principal, podemos observar los componentes que integran la red de comunicación:

- SFP permite conectar a través de fibra óptica la red pública a la red privada realizando la conversión de señal óptica a eléctrica y viceversa, funcionando en la capa física.
- Firewalls
    - El Firewall principal FW1, FW2 yFW3 realiza diferentes funciones como, por ejemplo:
        - Seguridad perimetral mediante políticas de seguridad basado en permisos
        - Control de aplicaciones
        - Se encuentra configurado como servidor de DHCP(*Dynamic Host Configuration Protocol*- Protocolo de configuración dinámica de host)
        - Enrutamiento del tráfico de datos, configuración de las VPN (Virtual Private Network- (Red privada virtual) para comunicación de usuarios y entre organizaciones,
    - El FW4 lo utiliza el ISP para el monitoreo del equipo de comunicaciones y supervisión de la VLAN (*Virtual Local Area Network* -Red de área local virtual) de Voz
    - SW1: Este switch funciona como conmutador y enrutador, de esta forma permiten separa las VLAN y realizar el enrutamiento entre ellas. Funcionan en la capa 3 y soportan protocolos RIP(*Routing Information Protocol*- Protocolo de Información de Enrutamiento), OSPF(Open Shortest Path First- El Camino Más Corto Primero). En este caso, este switch es el CME (*Call Manager Express- Administrador de llamadas*)
- SW2: Nos permiten la conexión de los dispositivos usando las direcciones MAC, funcionan en la capa 2 enlace de datos.

La figura 15 muestra el diagrama general de las sucursales y se utilizara como modelo para la simulación de las seis sucursales ya que son similares.

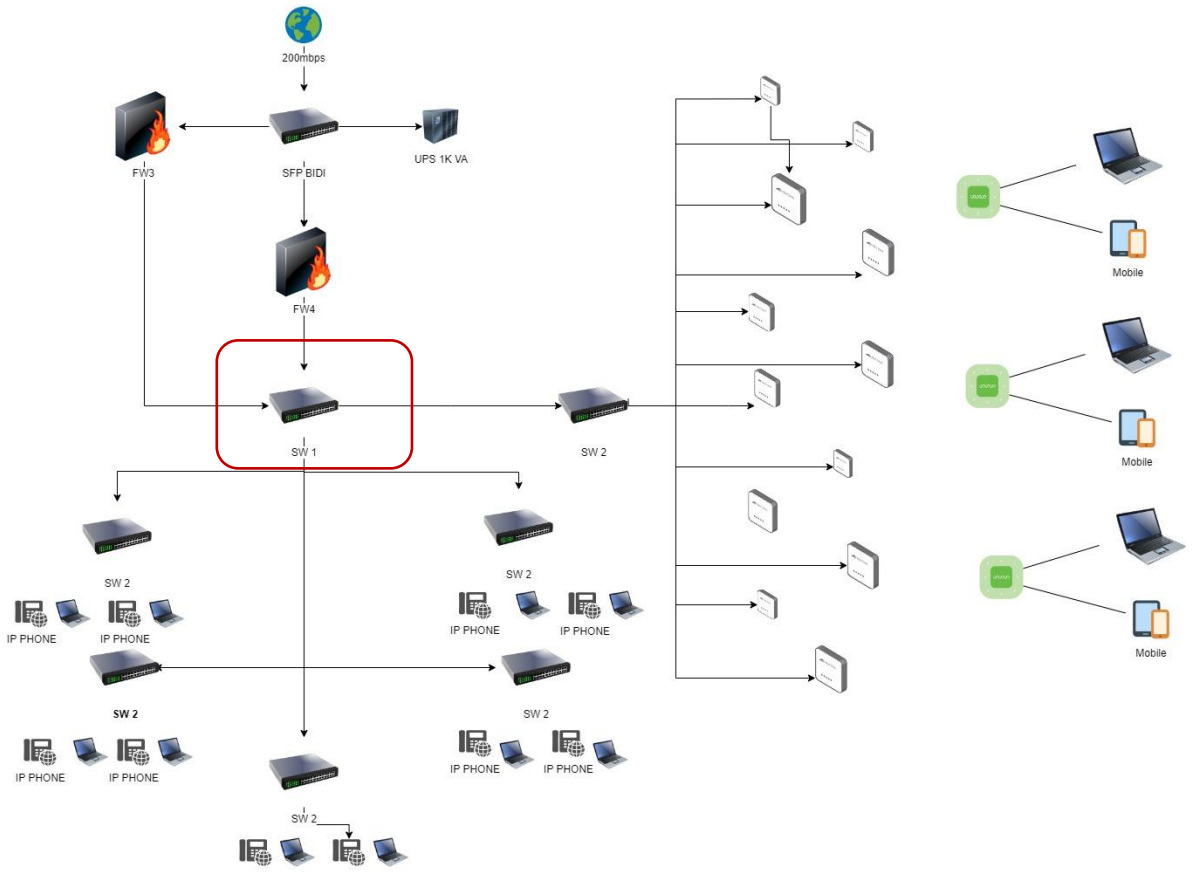


Figura 15. Diagrama general de la red

3.5 ESPECIFICACIONES TÉCNICAS DE LOS COMPONENTES DE LA RED

Los firewalls son dispositivos de seguridad de una red que tienen la finalidad de supervisar, filtrar tráfico de entrada y salida definido mediante reglas de seguridad para evitar amenazas o datos maliciosos de las redes exteriores.

En la tabla 13 se presentan las especificaciones de los equipos instalados en la red empresarial, mientras en la tabla 14 se realiza la equivalencia a con la marca Cisco

	Firewalls real - Marca 1			**Firewall real - Marca 2**
Serie del equipo real	FW1	FW2	FW3	FW4
Capacidad del cortafuegos	2.0 Gbps	1.7 Gbps	3.7 Gbps	1.5Gbps
Capacidad VPN	720Mbps	300Mbps	1.1 Gbps	1.0 Gbps
Capacidad IPS	600Mbps	500Mbps	1.2 Gbps	200 Mbps
NGFW	400Mbps	550Mbps	1.0 Gbps	
Rendimiento de protección contra amenazas	308 Mbps	480Mpbs	900Mbps	
Sesiones simultáneas	80,000	100,000	25,000	500,000
Nuevas sesiones	8,000	9,000	10,000	3,200
Factor de forma	Desktop	Desktop	Desktop	Desktop
Conmutador integrado			8- port	
Punto de acceso Wi- Fi	Si	Si	Si	
RAM[Gb]	4	4	4	
Almacenamiento interno (GB)	80	100	80	16
Equivalencia a Cisco	1010 / 1010E	1120	1140	1120

Tabla 13. Especificaciones reales de firewall usados en la organización

Por acuerdo confidencial con la empresa se editan las marcas y modelos.

Serie 1000 Categorizado para pequeñas empresas y sucursales				**Serie usado en la simulación**
Serie Cisco equivalente	**1010 / 1010E**	**1120**	**1140**	**Cisco ASA 5505**
Capacidad del cortafuegos	890 Mbps	2.3 Gbps	3.3 Gbps	
Capacidad VPN	400 Mbps	1.2 Gbps	1.4 Gbps	100Mbps
Capacidad IPS	900 Mbps	2.6 Gbps	3.5 Gbps	75 Mbps
NGFW				
Sesiones simultáneas	100,000	200000	400000	10,000; 25,000
Nuevas sesiones	25,000	75,000	100,000	4,000
Factor de forma		Montaje en bastidor, 1U	Montaje en bastidor, 1U	Desktop
Punto de acceso Wi- Fi				
RAM[Gb]	8- GB	16-GB	16-GB	512 MB
Almacenamiento interno (GB)	200 GB	200 GB	200 GB	
Serie del equipo real	FW1/FW4	FW2	FW3	Cisco ASA 5505

Tabla 14. Especificaciones reales de la serie equivalente

Dada las especificaciones de los firewalls y comparando la equivalencia de Cisco, la gama usada está categorizada para pequeñas empresas y sucursales. Lo anterior se debe tomar en cuenta para futuras actualizaciones o el crecimiento de la infraestructura cuando se busque migrar a una tecnología con mayor capacidad.

Un SFP es un dispositivo que trabaja en la capa física, su función es convertir señales ópticas a eléctricas y viceversa. En la tabla 15 se muestran las especificaciones del módulo óptico.

Módulo optico SFP		
Artículo	**Descripción**	**Equivalente a cisco**
Nombre del módulo	SFP usado	Cisco GLC-LH-SM
Factor de forma	eSFP	
Estándar de aplicación	1000BASE-BX	1000BASE-LX/LH
Tipo de conector	LC	LC
Tipo de fibra óptica	SMF	SMF
Temperatura de la caja de trabajo [°C(°F)]	De 0 °C a 70 °C (de 32 °F a 158 °F)	De 0 °C a 70 °C (de 32 °F a 158 °F)
Opciones de DDM	Soportado	
Velocidad de transmisión [bit/s]	1Gbit/s	1 Gbps
Distancia de transmisión objetivo [km]	Fibra monomodo: 10 km	550m a hasta 10km
Características ópticas del transmisor		
Longitud de onda central [nm]	1310(RX) 1490(TX)	
Potencia óptica máxima Tx [dBm]	-3,0 dBm	(-)3,0 dBm
Potencia óptica Tx mínima [dBm]	-9,0 dBm	(-)9,5 dBm
Tasa mínima de extinción [dB]	6,0 dB	
Características ópticas del receptor		
Sensibilidad Rx [dBm]	-19,5 dBm	
Potencia de sobrecarga [dBm]	-3,0 dBm	

Tabla 15. Especificaciones técnicas de módulo óptico usado y equivalencia Cisco

Los AP o puntos de acceso son dispositivos que nos permiten crear una red de área local inalámbrica. En la tabla 16 se describen las características de los AP instalados en la empresa, mientas que en la tabla 17 se indican los AP de la marca Cisco.

ACCESS POINT						
Serie real	**AP1**	**AP2**	**AP3**	**AP4**	**AP5**	**AP6**
Ambiente	*Interior*	Interior	Interior/ Exterior	Interior/ Exterior	Interior	Interior
Rango de frecuencia 2.4 Ghz	300Mbps	300Mbps	450Mbps	600Mpbs	150 Mbps	400 Mbps
Rango de frecuencia 5 Ghz	867Mbps	867Mbps	1300Mbps	2400Mbps		867 Mbps
PoE	802.3at PoE+	802.3af/A PoE 24V Passive PoE	802.3af PoE 802.3at PoE+	PoE+	PoE	
Techo		si	si	si		
Pared	si	si	si	si	Si	
Certificación DFS (selección dinámica de frecuencia)	si	si	si		Si	
Clientes simultáneos	250+	250+	125+	300+	100+	100
Estandar Wi Fi	802.11 a/b/g/n/r/k/v/ac	802.11 a/b/g/n/r/k/v/ac	802.11 a/b/g/n/r/k/v/ac	802.11a/b/g WiFi 4/WiFi 5/WiFi 6	802.11 b/g/n	IEEE 802.11ac/n/a 5 GHz IEEE 802.11n/b/g 2.4 GHz
Seguridad inalámbrica	WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)	WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)	WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)	WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3)	WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)	WPA-Personal WPA2-Personal

Tabla 16. Especificaciones reales de los *Access Point* usados en la organización.

Serie Cisco	145AC	150AX	240AC
Ambiente	Indoor	Indoor	Indoor
Rango de frecuencia 2.4 Ghz	300 Mbps	300 Mbps	600 Mbps
Rango de frecuencia 5 Ghz	867 Mbps	867 Mbps	1733 Mbps
PoE	802.3at PoE+	802.3af/at	802.3af/at
Techo	si	Si	
Pared	si	Si	
Clientes simultáneos	200+	200+	200+
Estandar Wi Fi	802.11a/b/g/n/h/d/ac	IEEE 802.3/ab/af/at/a/b/g/n/ac/ax IEEE 802.11h/d	IEEE 802.3 /ab/af/at IEEE 802.11a/b/g/n/ac/h,/d
Seguridad inalámbrica	802.11i, WPA2, WAP3, WPA,802.1X ,AES	802.11i, WPA2, WPA2-Enterprise, WAP3, WPA,802.1X ,AES	802.11i, Wi-Fi Protected Access 2 (WPA2), WAP3 (futuro), WPA, 802.1X, Estándares de cifrado avanzado (AES)

Tabla 17. Especificaciones reales de los AP mapeados a la serie Cisco

Un switch es un sistema que conecta dispositivos como computadoras, impresoras, servidores, etc. y permite transferir datos. Las especificaciones usadas se muestran en la tabla 18.

Switch		
Serie real	Marca 1 SW 1	Marca 2 SW2
Número de puertos	24 10/100Base-T	24 10/100/1000
Estándares	Auto MDI/MDIX, Alimentación a Través de Ethernet, IEEE 802.1 p (etiquetas de Prioridad), IEEE 802.1 p (VLAN)	Auto MDI/MDIX, Alimentación a Través de Ethernet, IEEE 802.1 p (etiquetas de Prioridad), IEEE 802.1 p (VLAN)
Soporte De IPv6	Si	Si
Interna de ancho de banda	64 Gb/s	52 Gb/s
El tamaño de la tabla de direcciones MAC	16 k	8K
Protocolos de administración de grupos de Internet	IGMP v1, IGMP v2, IGMP v3	IGMP v1, IGMP v2, IGMP v3
Los protocolos de enrutamiento dinámico (L3)	RIP v1, RIP v2, OSPF	

Tabla 18. Especificaciones reales de los switches

Cisco	IE-3010-24TC	SG220-26
Número de puertos Gigabit Ethernet	24 puertos 10/100BASETX y dos puertos de enlace ascendente Gigabit Ethernet de doble propósito. (cada puerto de enlace ascendente de doble propósito tiene un puerto Ethernet 10/100/1000 y un puerto Gigabit Ethernet basado en SFP, un puerto activo)	Gigabit Ethernet 24 puertos 10/100/1000 2 puertos combinados Gigabit RJ45/SFP
Protocolos de administración de grupos de Internet	IGMP v1, IGMP v2, IGMP v3	IGMP v1, IGMP v2, IGMP v3
Tiene PoE: no Power over Ethernet(Alimentación através de Ethernet)	Si	Si
El tamaño de la tabla de direcciones MAC		
Los protocolos de enrutamiento dinámico (L3)	RIP v1, RIP v2, OSPF, EIGRP,BGPv4, PIM	

Tabla 19. Especificaciones reales de los SW mapeados a la serie Cisco

3.6 INVENTARIO DE LA INFRAESTRUCTURA DE CADA LAN

En las siguientes tablas se indica el inventario de los componentes que integran la red de cada sucursal.

CANTIDAD	MODELO	TIPO
1	AP4	ACCESS POINT
3	AP1	ACCESS POINT
1	AP2	ACCESS POINT
5	AP3	ACCESS POINT
2	AP5	ACCESS POINT
1	SFP	SWITCH
1	SW1	SWITCH
5	SW2	SWITCH
1	FW4	FIREWALL
1	1K VA	UPS
1	FW3	FIREWALL
3	2KVA	UPS
4	24P	PACH PANEL

Tabla 20. Inventario del equipo de comunicación de la sucursal 1

CANTIDAD	MODELO	TIPO
7	AP1	ACCESO POINT
1	SFP	SWITCH
1	SW1	SWITCH
2	SW2	SWITCH
1	FW4	FIREWALL
1	1K VA	UPS
1	SG300-28PP-K9	SWITCH
1	FW2	FIREWALL
1	750VA	UPS
3	24P	PACH PANEL

Tabla 21. Inventario del equipo de comunicación de la sucursal 2

CANTIDAD	MODELO	TIPO
5	AP5	ACCESS POINT
1	SFP	SWITCH
1	SW1	SWITCH
1	FW4	FIREWALL
1	1K VA	UPS
1	FW1	FIREWALL
1	450VA	UPS
1	24P	PACH PANEL

Tabla 22. Inventario del equipo de comunicación de la sucursal 3

CANTIDAD	MODELO	TIPO
2	AP2	ACCESS POINT
1	SFP	SWITCH
1	SW1	SWITCH
1	SW2	SWITCH
1	FW4	FIREWALL
1	1K VA	UPS
1	FW1	FIREWALL
1	1.2 KVA	UPS
2	24P	PACH PANEL

Tabla 23. Inventario del equipo de comunicación de la sucursal 4

CANTIDAD	MODELO	TIPO
2	AP6	ACCESS POINT
1	SFP	SWITCH
1	SW1	SWITCH
1	SW2	SWITCH
1	FW4	FIREWALL
1	1K VA	UPS
1	24P	PACH PANEL

Tabla 24. Inventario del equipo de comunicación de la sucursal 5

CANTIDAD	MODELO	TIPO
2	AP6	ACCESS POINT
1	SFP	SWITCH
1	SW1	SWITCH
1	SW2	SWITCH
1	FW4	FIREWALL
1	1K VA	UPS
1	24P	PACH PANEL

Tabla 25. Inventario del equipo de comunicación de la sucursal 6

3.7 SIMULACIÓN

En la simulación se utiliza el software de Cisco Packet Tracer y se usan los siguientes equipos:

1. Firewall 5505
2. Router 2811: Permite integrar el servicio telefónico a diferencia de otro routers
3. Switch 2960
4. Laptop
5. Teléfonos IP

Para reproducir el comportamiento del SW1 capa 3, se utilizar dos equipos: el router 2811 para intercomunicar las VLAN y el switch 2960 capa 2 que básicamente reenvía los paquetes entre equipo que pertenecen a la misma red.

En la figura 16 se muestra los dispositivos usados para simular el CME de la red real, en donde el router 2811 nos permite el procesamiento de llamadas para los teléfonos IP.

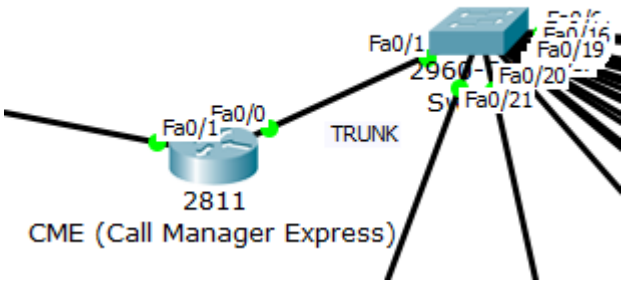


Figura 16. CME, simulación el Switch capa 3 de la red real

Para garantizar la calidad de transmisión de datos y voz es necesario la creación de VLANs, por lo que a continuación se indica como fueron creadas.

3.7.1 CREACIÓN DE VLANS

Paso 1. Se crean las VLAN en el SW 1 con el fin de separar el tráfico de voz y datos como ese encuentra segmentada en la empresa, como se muestra en la figura 17.

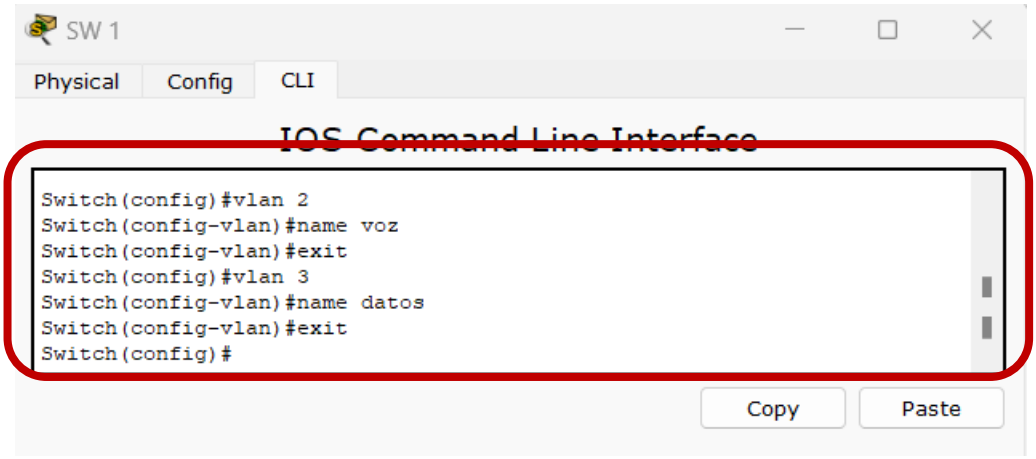


Figura 17. Código usado para la creación de las VLAN en cada SW1

Paso 2. En el mismo SW1 se asigna los puertos troncales de las interfaces FastEtherne0/1 al puerto FastEtherne0/6 en el switch SW1, en la figura 18 muestra la asignación.

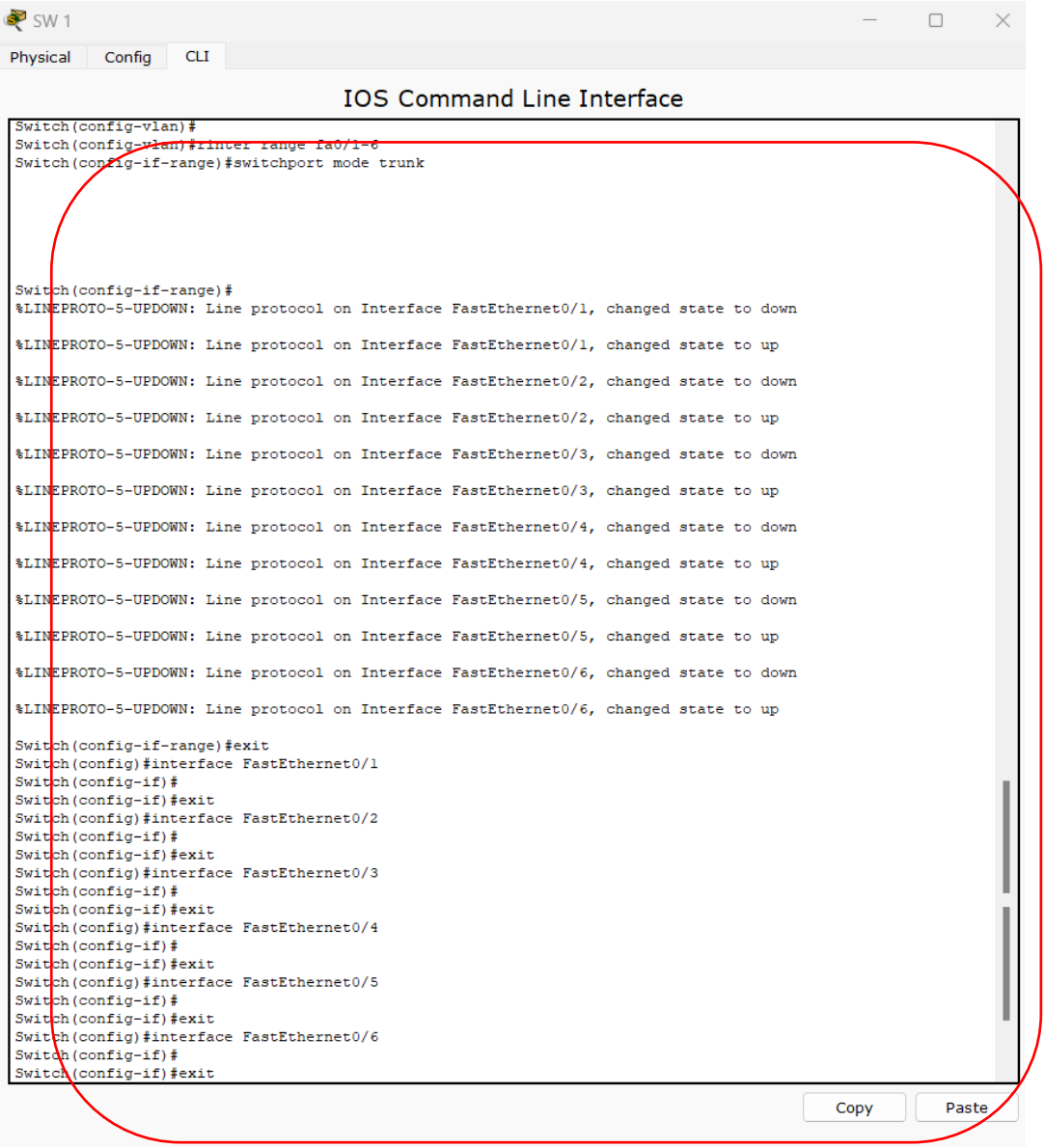


Figura 18. Asignación de troncales

Paso 3. En la figura 19 se muestra la creación de las VLAN en los switches de acceso en donde se tiene conectador los equipos de usuario final.

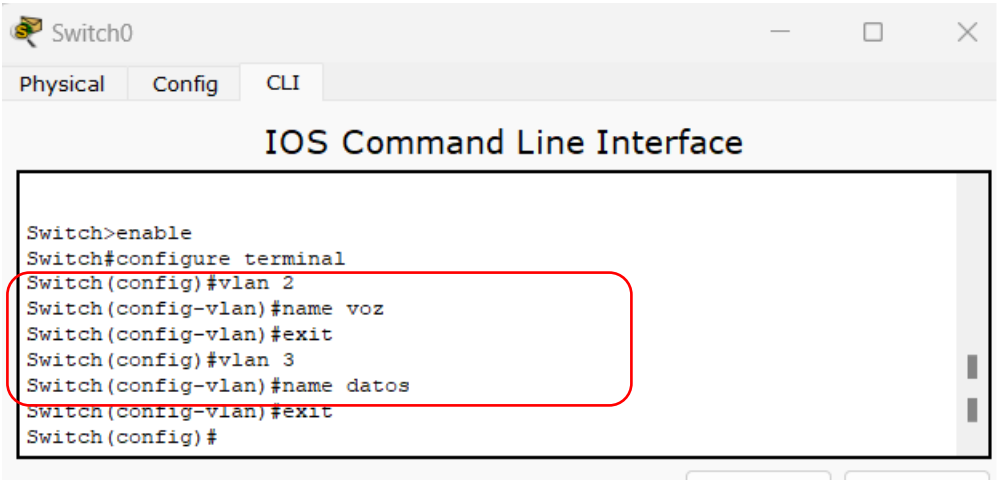


Figura 19. Configuración de VLAN en el switch

Paso 4. Se asignan los puertos de las respectivas VLAN, por limitantes con la versión del simulador se está asignando puertos independientes a los teléfonos IP y las computadoras como se indica en la figura 20, a diferencia de la configuración real en donde a un puerto se pueden asignar la VLAN de datos y la de voz.

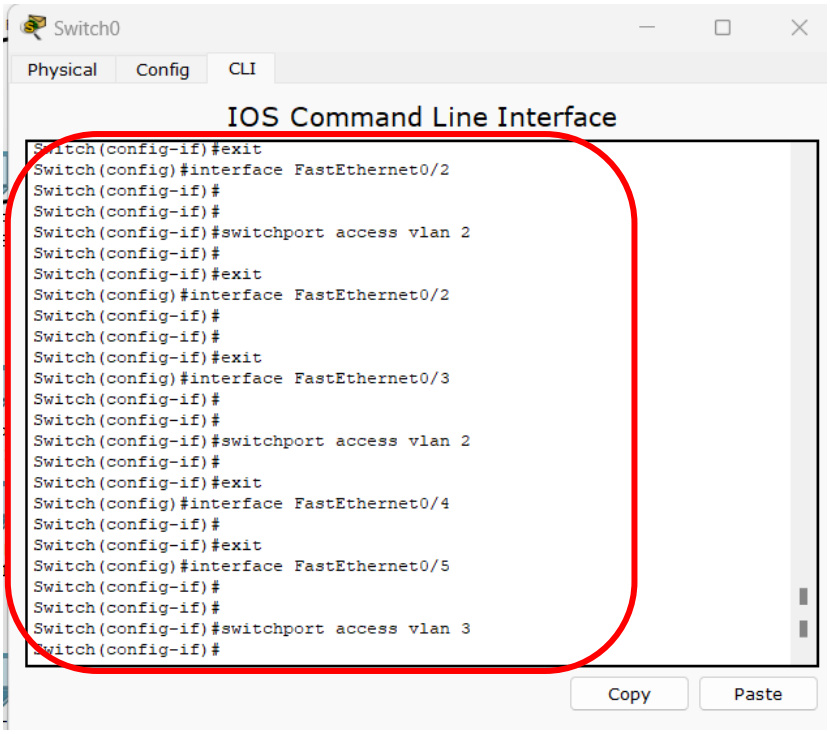


Figura 20. Asignación de puertos a cada VLAN

Paso 5. En la figura 21 se muestra cómo se asignan los puertos a las VLAN

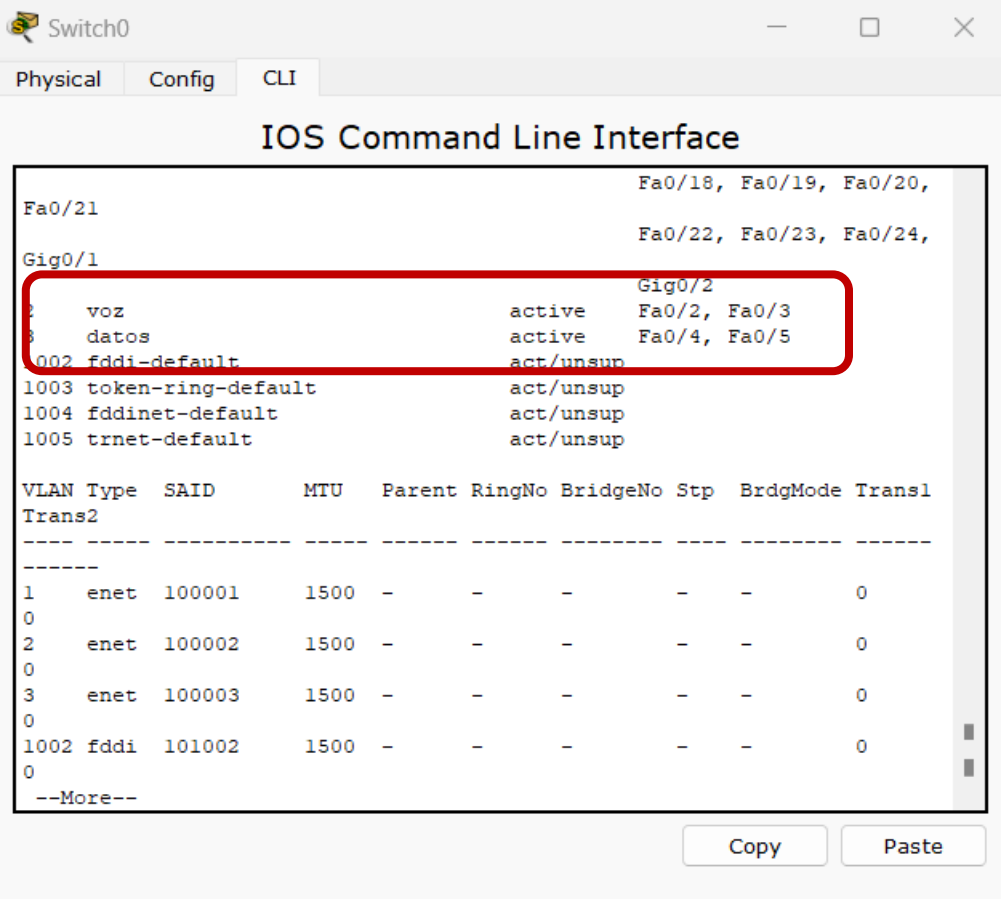


Figura 21. Vista de asignación de puertos respecto a la VLAN

Paso 6. Se realiza la configuración del router para agregar las subinterfaces, estas subinterfaces permitirán crear múltiples segmentos virtuales sobre una conexión física Fa0/0, esto nos va a permitir la conectividad de las VLAN, se muestra en la figura 22 y 23.

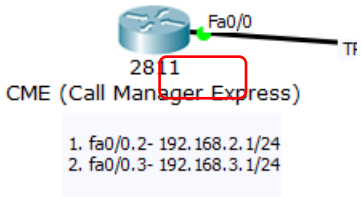


Figura 22. Creación de subinterfaces

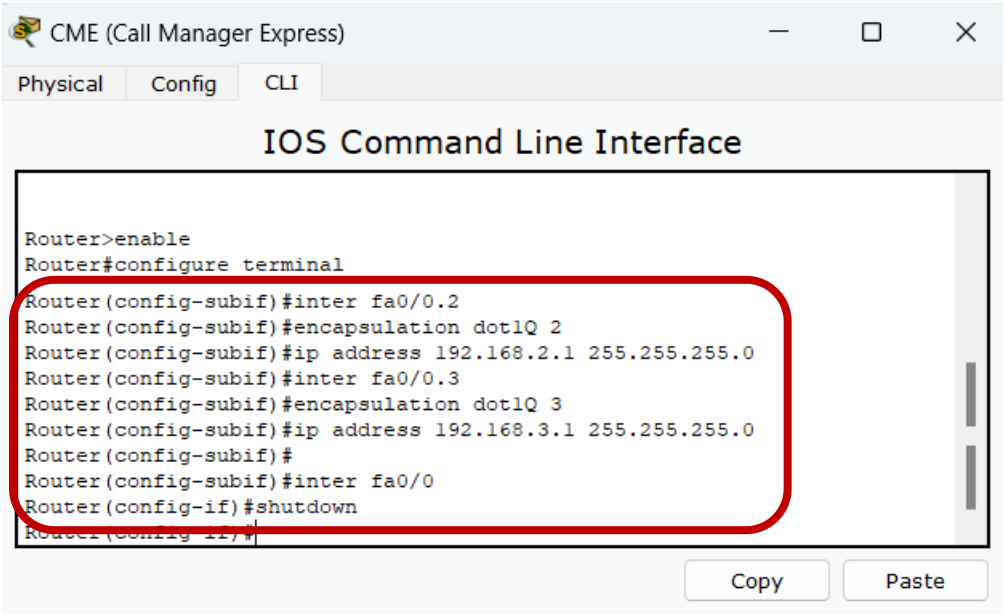


Figura. 23 creación de subinterfaces.

Paso 7. Se realiza la configuración de los teléfonos desde el CME. En la figura 24 se muestra la creación del servidor de DHCP, el rango de direcciones que el DHCP puede utilizar la máscara y la puerta de enlace que no usará el servidor DHCP.

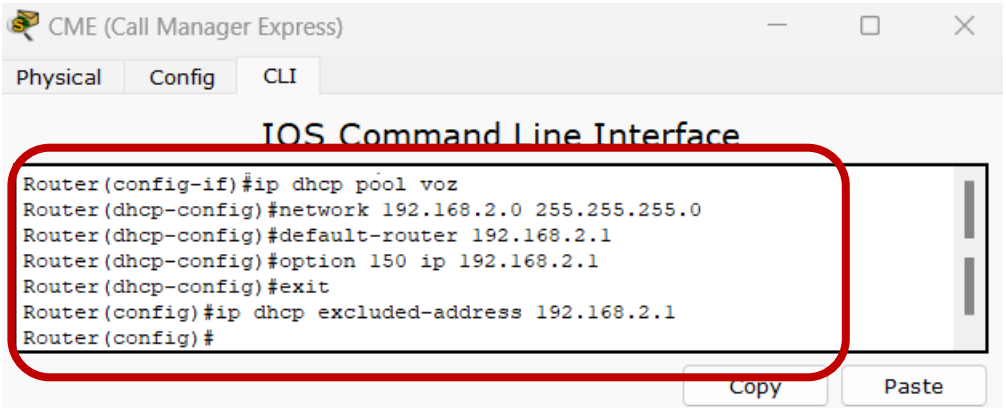


Figura 24. Asignación del rango de direcciones IP y la puerta de enlace

El comando “Option 150” permite descargar la configuración de los servidores TFTP a los teléfonos para que puedan funcionar, es requerido para los equipos Cisco.

Paso 8. Se habilita el CME y se asignan el número máximo de directorios, teléfonos y el puerto predeterminado 2000, este puerto se utiliza para el registro de teléfonos IP. En la figura 25 se muestra la configuración de CME.

Para poder determinar que un router soporta telefonía debe de acepta el comando telephony- service de lo contrario marca error.

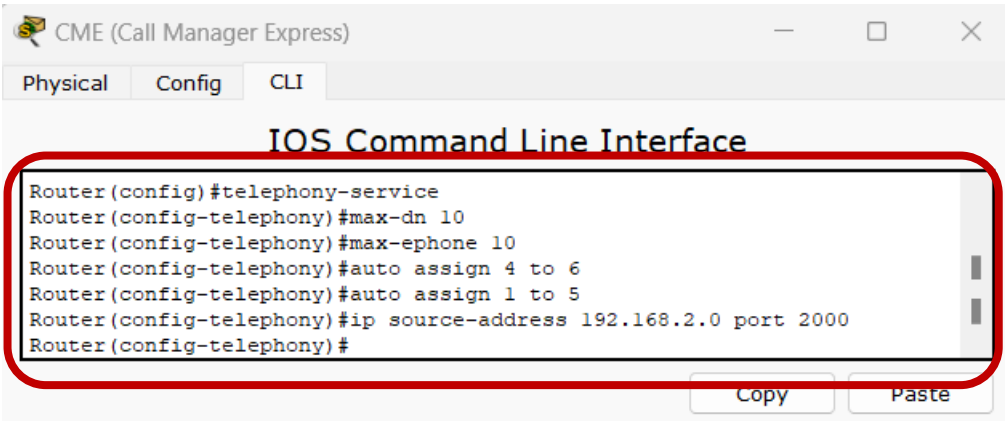


Figura 25. Asignación del rango de direcciones IP y la puerta de enlace

Paso 9. Por último, se agregan las extensiones de los teléfonos desde el CME con las siguientes instrucciones:

#ephone-dn 1

#number 400

#ephone-dn 2

#number 401

CAPÍTULO 4
RESULTADOS Y CONCLUSIONES

4.1 SIMULACIÓN DE LA TOPOLOGÍA DE CADA LAN POR SUCURSAL

A continuación, se muestran los resultados de simular la infraestructura de cada LAN ubicada en cada una de las sucursales. Para cada sucursal se prueba la conectividad entre cada uno de los elementos de la red y se revisa el funcionamiento correcto de cada VLAN, finalmente se revisa la seguridad habilitada en cada una de las topologías. En la tabla 19 se indicaron los componentes de la sucursal 1 y en la figura 26 se muestra la simulación aproximada de la topología de sucursal principal. En ella se puede observar a dos firewalls, el FW4 es el que usa el proveedor de Internet para realizar el monitoreo a los equipos de comunicaciones del cual es propietario y el otro lo utiliza la empresa para la seguridad de la red.

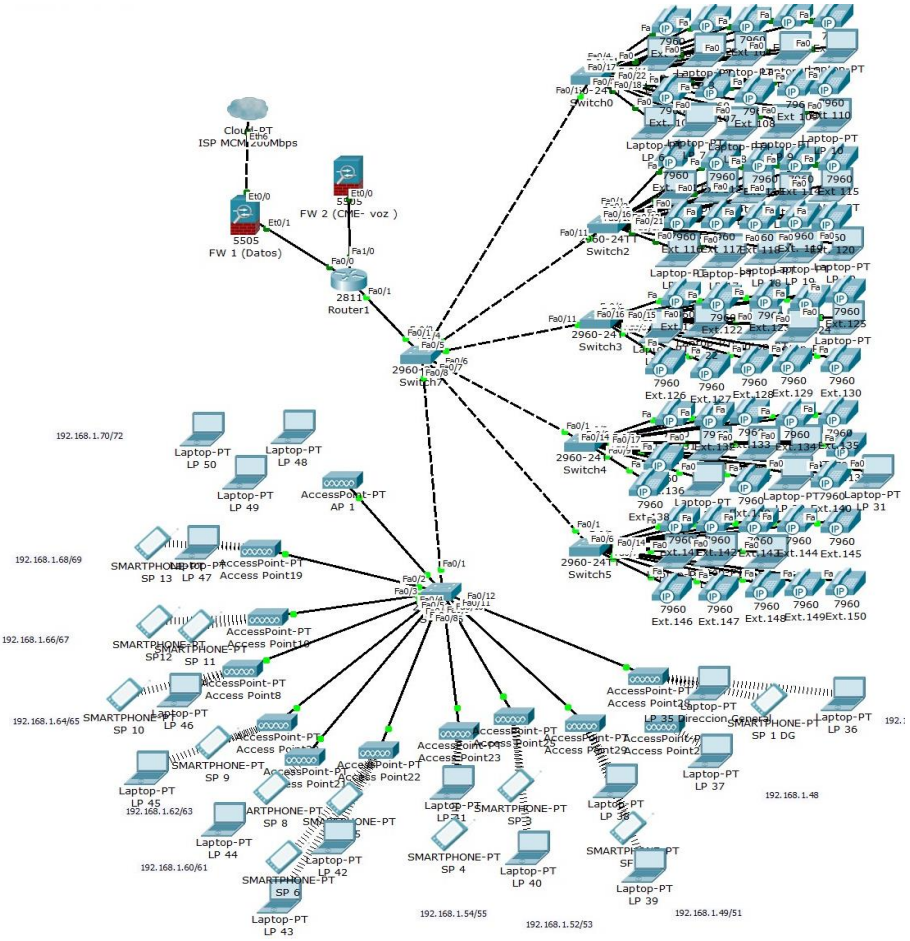


Figura 26. Topología de la sucursal 1 simulando 96 equipos

En esta sucursal 1 laboran alrededor de 51 personas, sin embargo, con la nueva modalidad de *home office,* nos encontramos ocupando la red en un 60%.

En el inventario de la tabla 20 se indican el inventario de la sucursal 2 y en la figura 27 se muestra la simulación aproximada. Al igual que la sucursal principal tiene dos *firewalls*. El FW4 es el que usa el proveedor de Internet para realizar el monitoreo a los equipos de comunicaciones del cual es propietario y el otro lo utiliza la empresa para la seguridad de la red. El número de empleados destinado en la sucursal es de 59, dado que es un área de soporte a clientes solo el 45 % se encuentra operando en la sucursal.

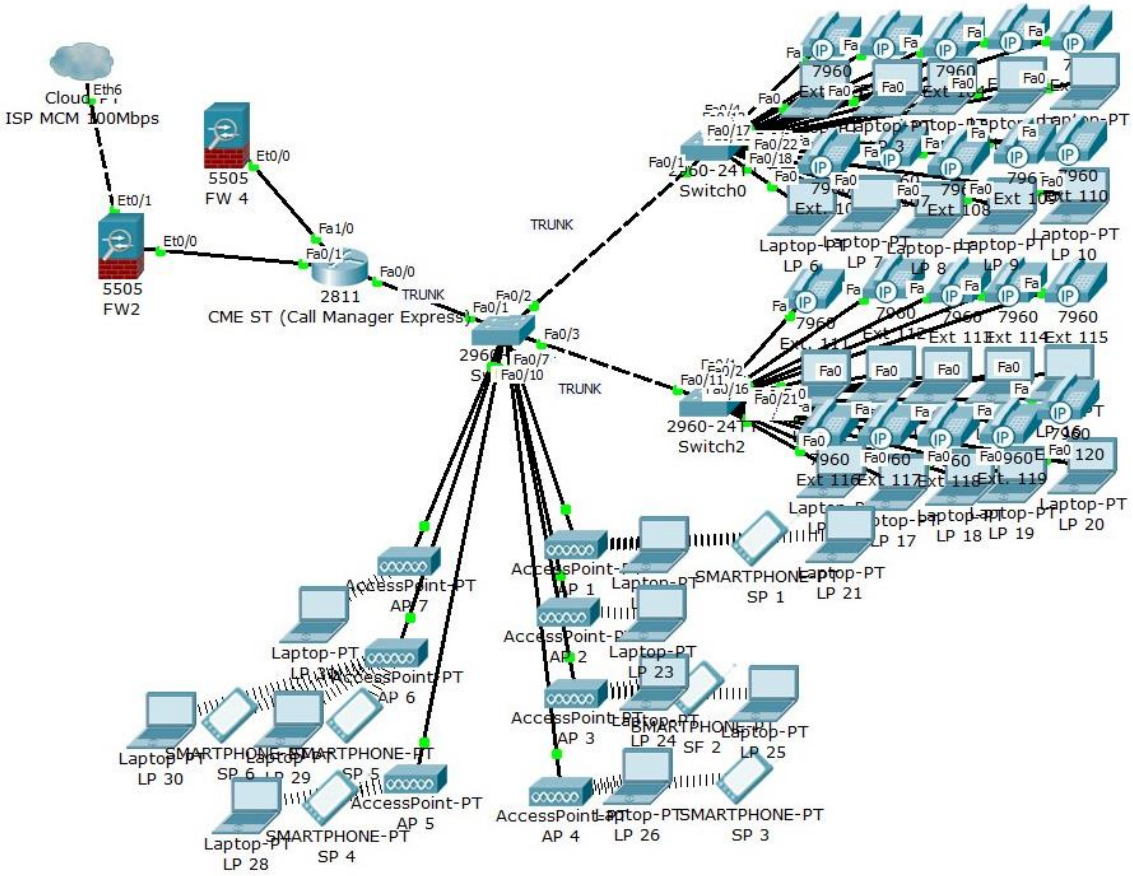


Figura 27 Topología de la sucursal 2, simulando 69 equipos

En la tabla 21 se muestra el inventario de la sucursal 3 y en la figura 28 se muestra la simulación aproximada, cuya topología es la misma que la sucursal 1 y 2 pero con

características diferentes en los AP. El número de usuarios destinado en la sucursal es de 12 pero el porcentaje de operación es del 16% aproximadamente.

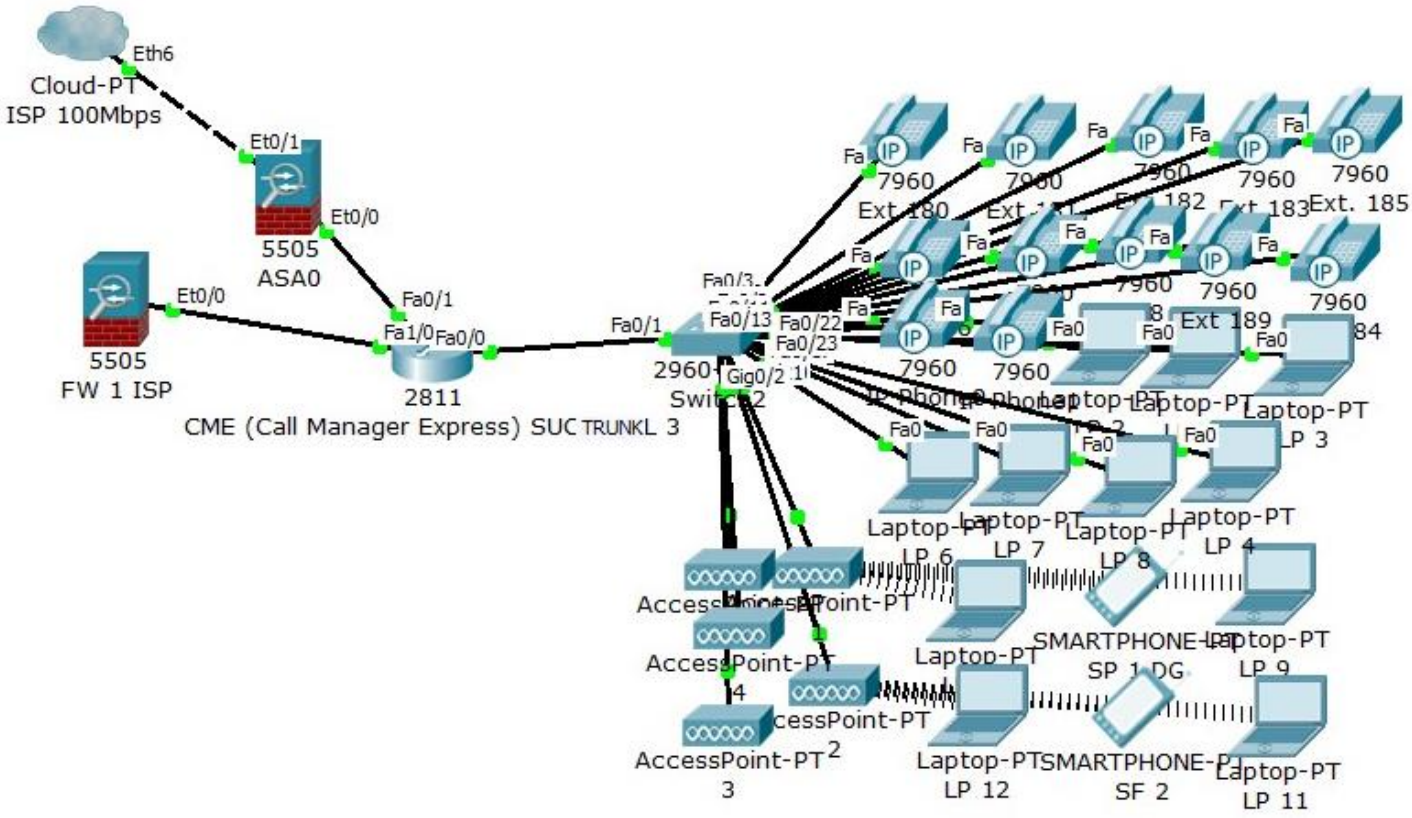


Figura 28. Topología de la sucursal 3, simulando 33 equipos

La sucursal 4 tiene características similares que la sucursal 3, la diferencia está en el número de AP y el porcentaje operacional para esta sucursal, en la figura 29 se puede observar que tiene dos AP para conectar a 12 usuarios y teléfonos móvil de forma inalámbrica, el inventario se puede observar en la tabla 23, su porcentaje operacional es de 100%.

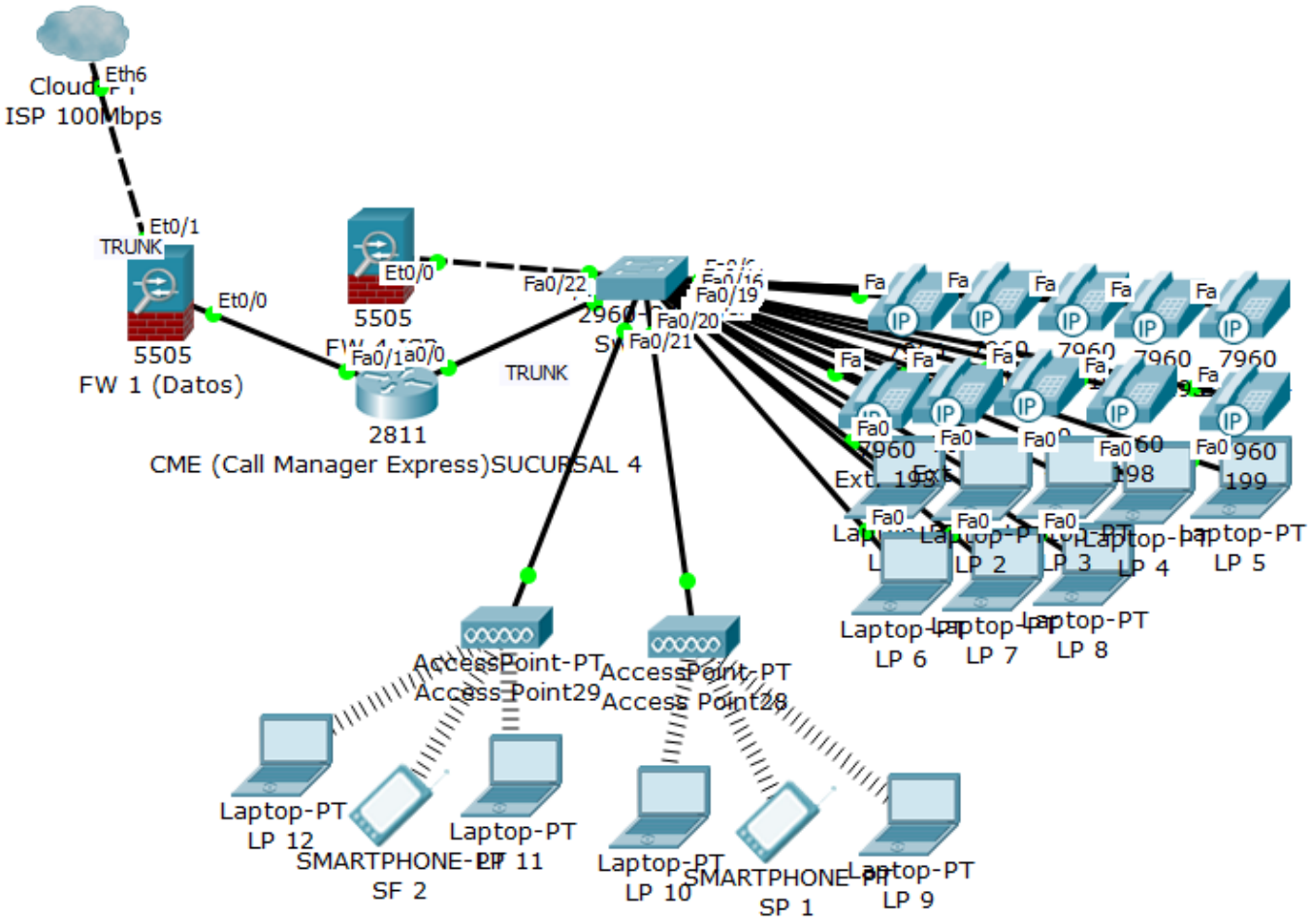


Figura 29. Topología de la sucursal 4, simulando 30 equipos

La sucursal 5 solo cuenta con el FW4 propiedad del ISP con características limitadas para el monitoreo del equipo de comunicaciones y supervisión de la VLAN voz, el número máximo de usuario que operan son 14. Esta red se encuentra sin seguridad perimetral y su porcentaje operacional es variable.

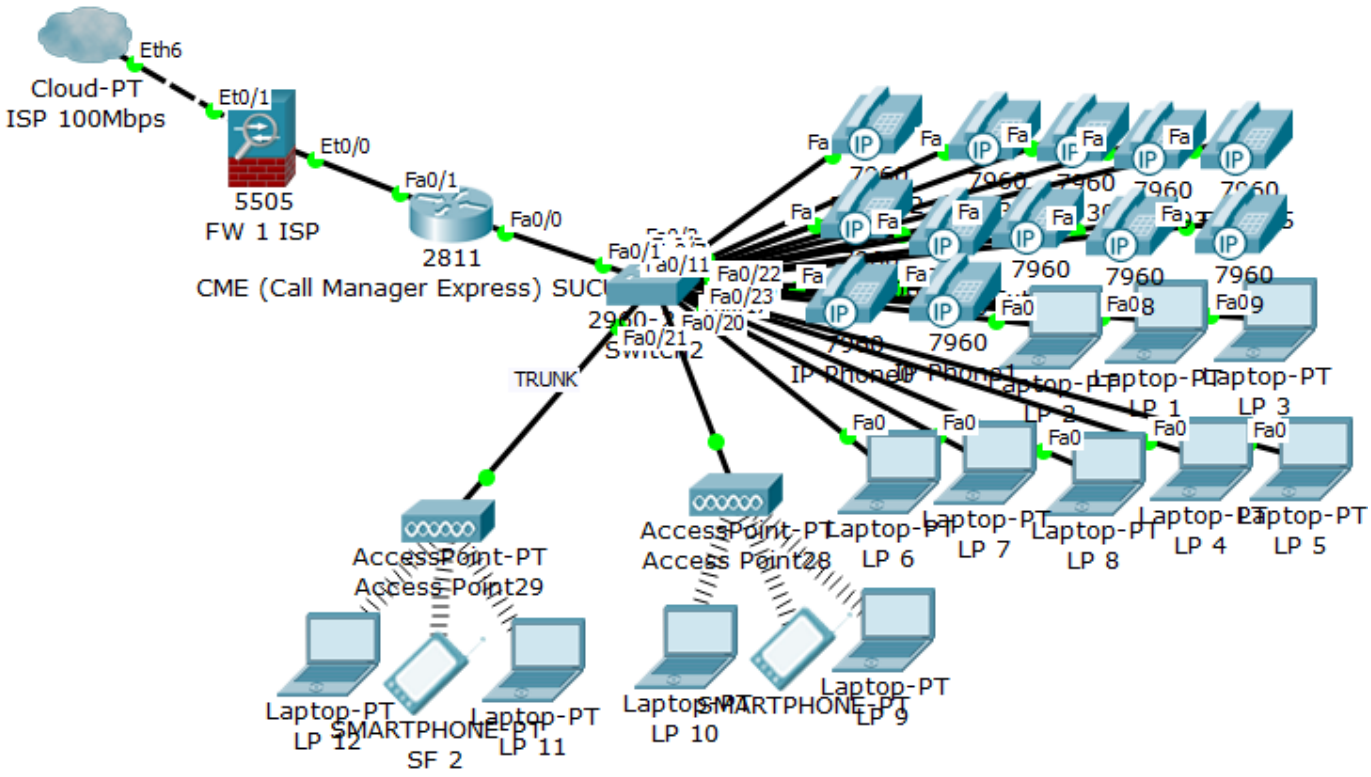


Figura 30. Topología de la sucursal 5, simulando 31 equipos

La sucursal 6 solo cuenta con el FW4 propiedad del ISP con características limitada para el monitoreo del equipo de comunicaciones y supervisión de la VLAN voz, el número máximo de usuario que operan son 7. Esta red se encuentra sin protección perimetral y su porcentaje operacional es variable.

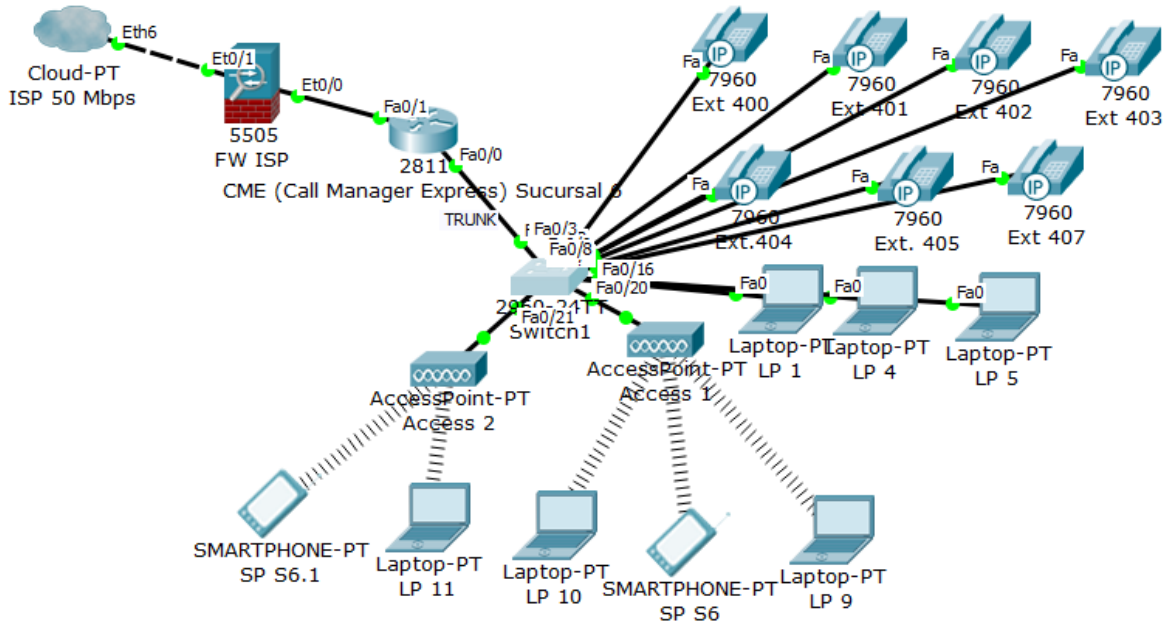


Figura 31. Topología de la sucursal 6, simulando 20 equipos

4.2 PRUEBAS DE CONECTIVIDAD ENTRE COMPUTADORAS

A continuación, se muestran las pruebas de conectividad, se tomó la sucursal 6 ya que todas tiene características similares.

En la figura 32 se observa la simulación de una red de datos configurada para 15 dispositivos conectados a la red.

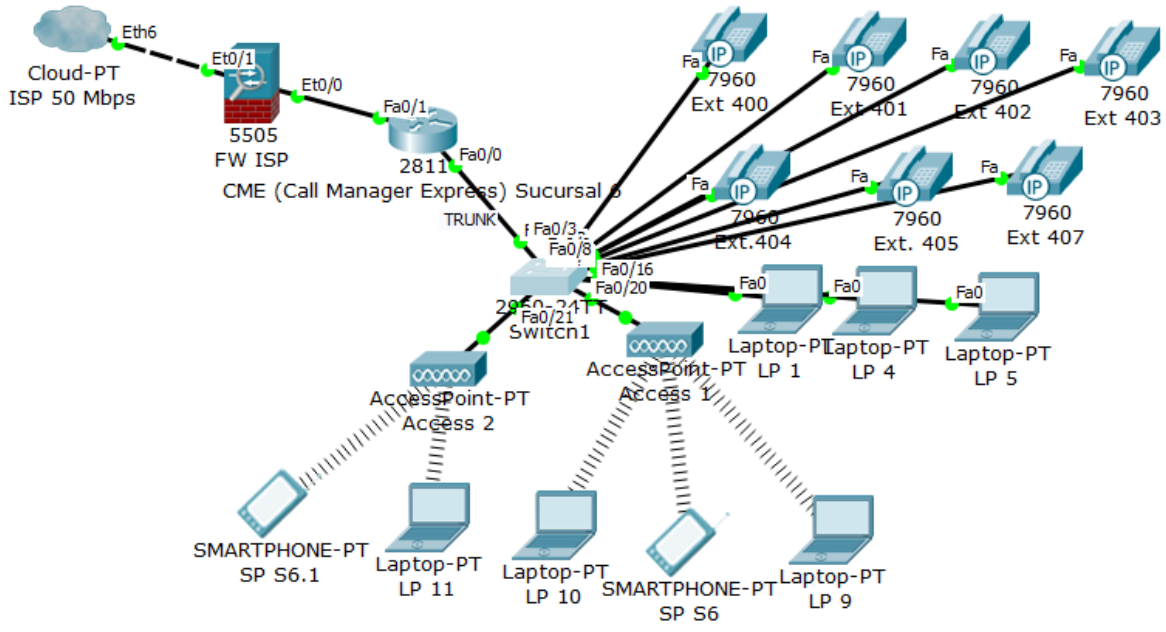


Figura 32. Topología de LAN de la sucursal 6, que se usara para probar la conectividad

En la figura 33 se realiza la validación de la comunicación en la VLAN de datos para las computadoras L3 y L5, mientras se observar el redireccionamiento de paquetes mediante el protocolo ICMP en la figura 34.

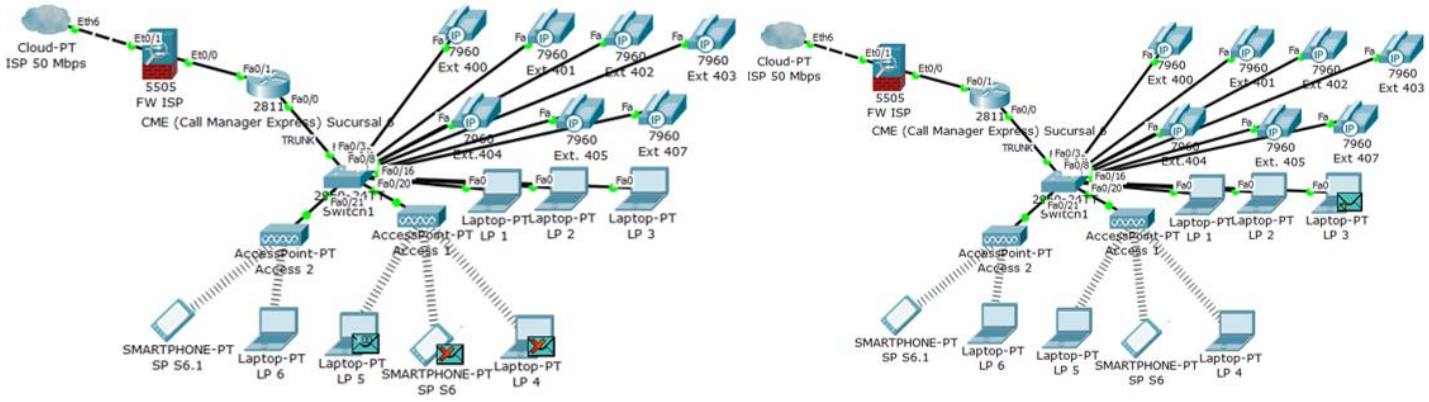


Figura 33. Simulación de la conectividad para las 6 sucursales

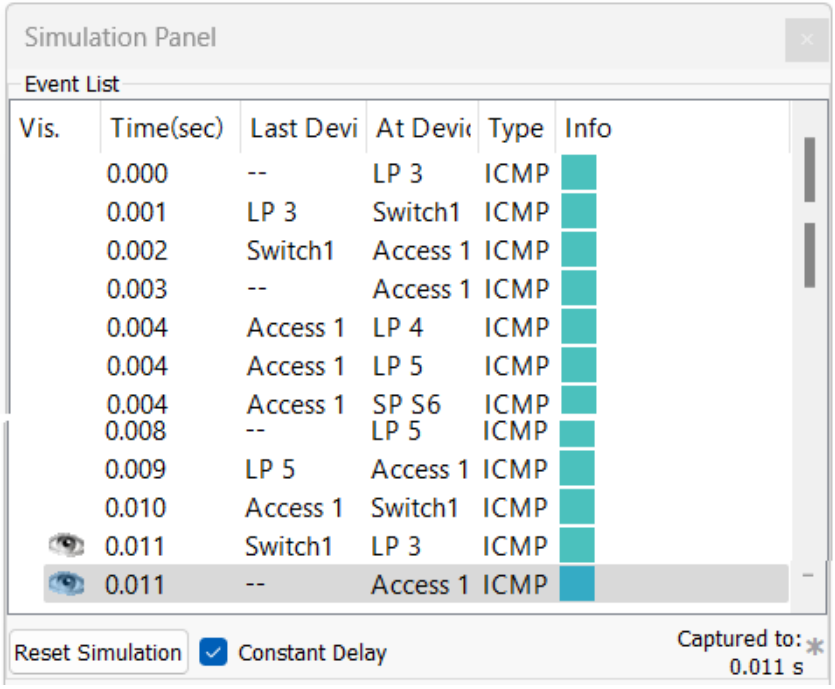


Figura 34. Redireccionamiento de paquetes ICMP

4.3 PRUEBAS DE CONECTIVIDAD ENTRE TELÉFONOS

En la figura 35 se comprueba el funcionamiento de la comunicación de la telefonía.
En el teléfono de la izquierda representado por la extensión 400 se indica la leyenda de *Ring Out,* que es de donde se está originando la llamada y el teléfono de la derecha es la extensión destinatario “403” en donde indica *From*: 400 la cual es el número de la extensión de donde se está realizando la llamada

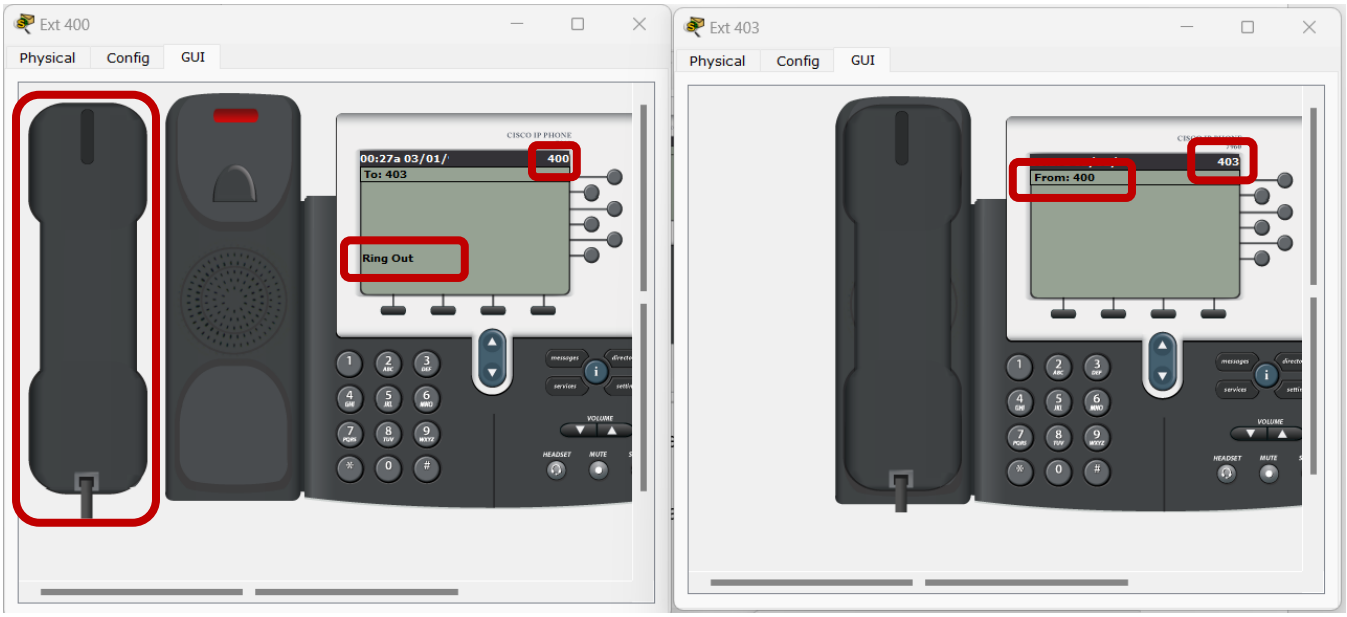


Figura 35. Tono de marcado y procedencia de la llamada

En la figura 36, se observa que al contestar la llamada de la extensión 400 se completa la conectividad

Figura 36. Llamada contestada

En este capítulo se realiza la comprobación de la VLAN de datos enviando paquetes entre la red LAN y WLAN, además se confirma la correcta configuración de la VLAN de voz.

4.3 DIAGNÓSTICO DE LA SEGURIDAD

Con la finalidad de medir el nivel de seguridad con la que cuenta cada sucursal se realiza la revisión de cada Access point y como comparativo se contrasta con el nivel de seguridad de una red residencial.

4.3.1 SEGURIDAD EN SUCURSALES

En la figura 37 se puede observar que dentro de la configuración de un AP se tiene WPA personal, enfocada principalmente a redes domésticos o empresas pequeñas. ésta se caracteriza por ofrecer seguridad a través de una contraseña. Para una mayor seguridad la empresa deberá migrar a WPA 2 Enterprise o WPA 3, en donde cada usuario debe autentificarse con un usuario y contraseña personalizada. La gestión de los AP se realiza a través de un servidor asociado al switch número 4 en la simulación de la sucursal principal y para la sucursal 2, 3,4, 5 y 6 se encuentra asociado al switch número 1, además de que controlan el DVR (*Digital Video Recorder*-Grabador de video digital) para las sucursales 1 a la 5. En la figura 38 también se observa que el controlador de AP no soporta WPA2 por lo que se sugiere tecnología que soporte más nivel de seguridad.

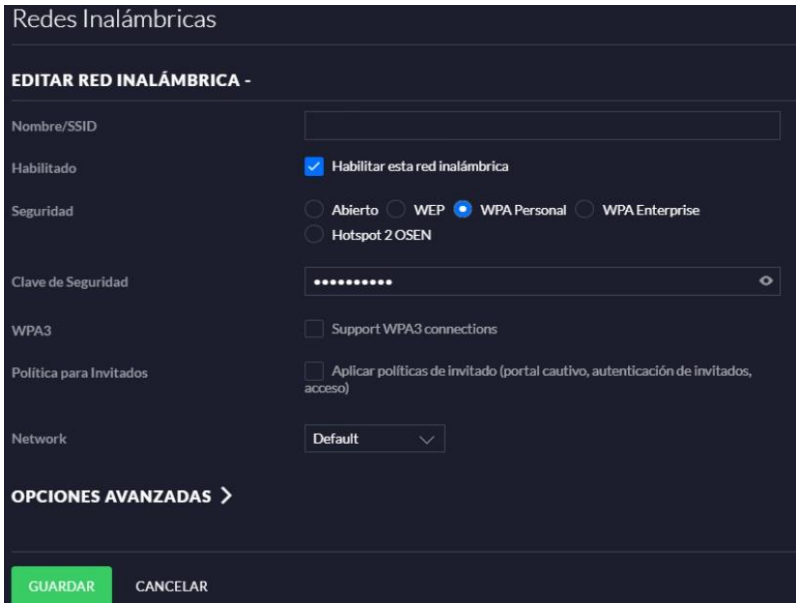


Figura 37. Nivel de seguridad en cada una de las sucursales

4.3.2 SEGURIDAD DE UNA RED CASERA

En la figura 38 vemos un diagrama básico de una red casera, en esta se muestra cómo se conecta diferentes dispositivos vía alámbrica y inalámbrica.

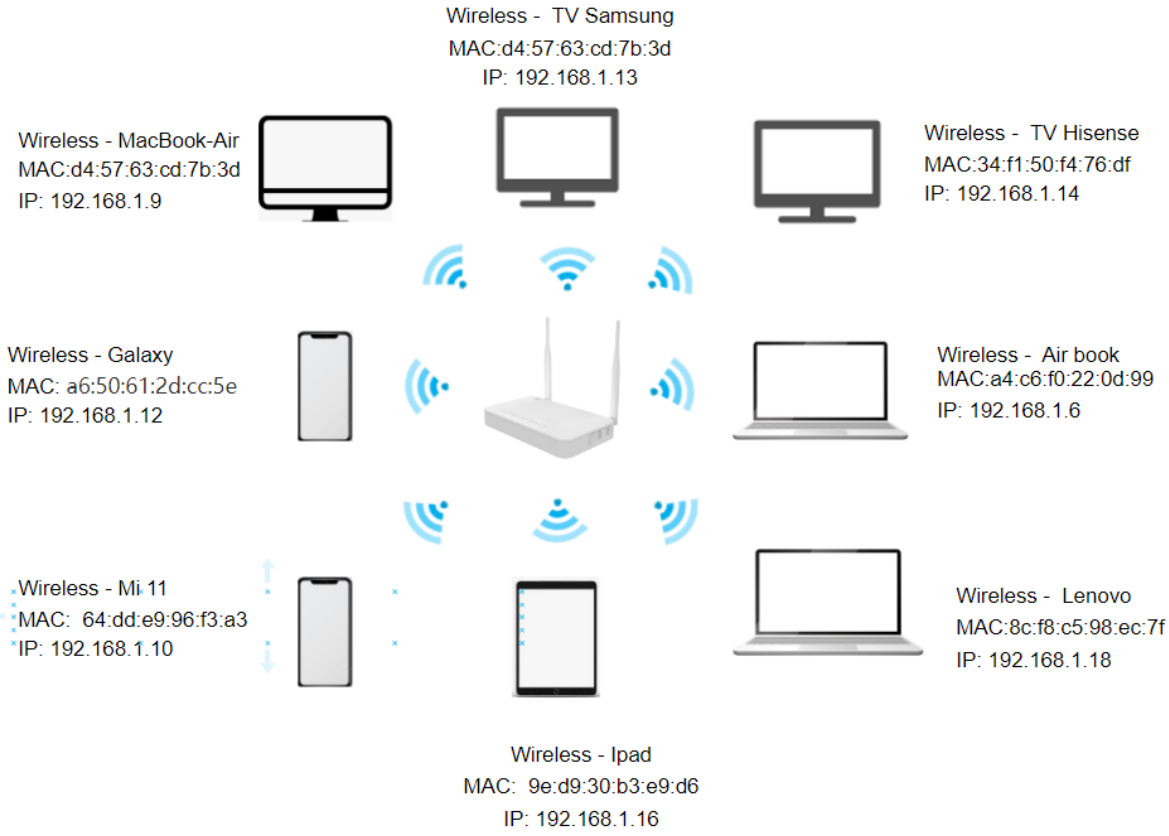


Figura 38. Topología de una red casera

En este caso el equipo que provee conexión inalámbrica se considera un *router, switch, firewall, access point (RSFA)* y corresponde al modelo ZTE ZXHN F670L que se usó para revisar la seguridad en la red domésticas cuyo ancho de banda contratado de 150 Mbps. El tipo de encriptación configurada es WPA2- PSK-AES y como se indicó en la tabla 10 es la opción más segura para este equipo. También puede observarse que aparece la encriptación WPA/WPA2-PSK-TKIP/AES, la cual es compatible con tecnologías obsoletas, sin embargo, es más insegura

En la figura 39 se muestra los niveles de seguridad del RSFA para una red doméstica.

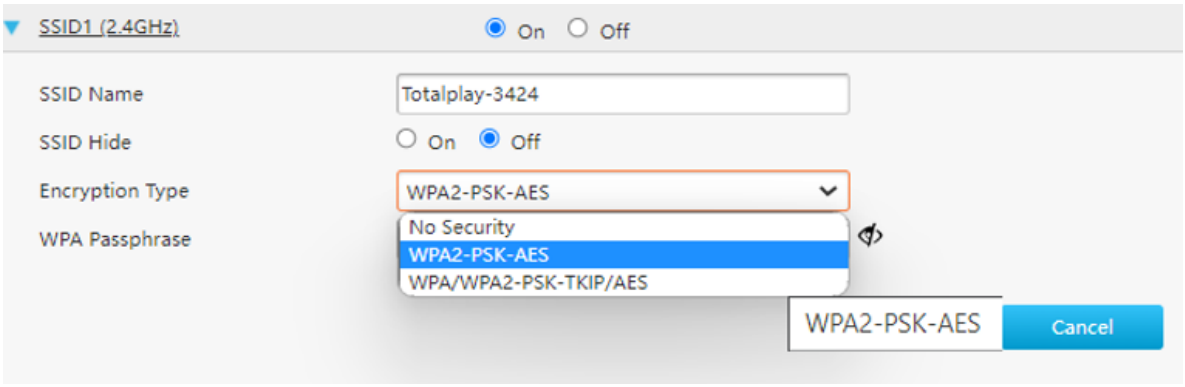


Figura 39. Nivel de seguridad y tipo de encriptación para una red casera

Como podemos observar la red casera cuenta con un nivel de seguridad WPA2, la cual es superior a WPA que se usa en las 6 sucursales, por tanto, es necesario incrementar drásticamente el nivel de seguridad en las sucursales.

De acuerdo a un estudio las WLAN que usan WEP, WPA y WPA2 son vulnerables para la detección de contraseñas y ataque de fuerza bruta, la recomendación para endurecer el nivel de seguridad es WPA2- Enterprise, mientras se hace accesible el WPA 3. [49]

WPA3 busca mejorar la protección vía inalámbrica para las redes personales y empresariales permitiendo la autentificación y encriptación más sólida y altamente confidencial dondequiera que los usuarios se conecten. Las redes WPA3 utilizan los métodos de seguridad más recientes y no permiten protocolos heredados u obsoletos.

En la tabla 26 Se muestran modelos y precios aproximados de los AP que soportan WPA 3 y WiFi 6 ofrecidos por diferentes empresas

Marca	Modelo	Precio
Cisco	Cisco Catalyst 9105/9115	$17,00.00 a 18,000 MXN
TPLINK	EAP690E HD	$10,200.00 a 11,000.00 MXN
TPLINK	EAP670	$4,000 a $5,000.00
UBIQUITI NETWORKS	U6-PRO	$4,000.00 a $5,000.00

Tabla 26. Lista de costos aproximados de AP que ofrecen Wifi 6 y WPA3

Costos actualizados al 10/10/2023, cuyas especificaciones se muestran en el apéndice A3.

4.4 PRUEBAS DE ANCHO DE BANDA

Se realiza la medición de los anchos de banda y se identifica las conexiones entre una red empresarial y una red casera

4.4.1 ANCHO DE BANDA EN SUCURSALES

A continuación, se realizará la medición del ancho de banda y latencia de cada sucursal, lo cual permitirá conocer el rendimiento de la red. Las pruebas se realizaron con Google, IFT (Instituto Federal de Telecomunicaciones) y Megacable. Estos medidores de velocidad utilizan un archivo y realizan la carga o descarga para comprobar el tiempo (ms) y cantidad de datos (bits) que se transmiten. Para realizar la revisión se comparará con los siguientes listados estándar:

La latencia permitirá medir el tiempo total que tarda un paquete de datos en viajar de un nodo origen a un servidor destino. Si la latencia es elevada provocará un rendimiento inadecuado o bien tiempos de carga lentos.

Estándar	ms
Excelente	0 – 20
Bueno	20 – 60
Aceptable	60 – 100
Malo	100 – 250

Tabla 27. Escala de valoración para latencia

El ***jitter*** o fluctuación mide el tiempo de retraso entre la trasmisión de datos y su recepción a través de una conexión de red, estos retrasos tienen que ver con la interrupción en el proceso de envío de paquete de datos, por ejemplo, si una fluctuación es alta, en una video conferencia puede provocar ruido, distorsión de audio o video.

Estándar	ms
Excelente	0 – 10
Bueno	10 - 20
Aceptable	20 - 30
Malo	Mayor a 30

Tabla 28. Escala de valoración de jitter

La **velocidad de carga** es la rapidez con la que podemos enviar nuestros archivos a través de internet, ejemplo: realizar video llamadas, subir fotos a redes sociales o enviar

correos electrónicos y la **velocidad de descarga** es la rapidez con la que se puede recibir datos de un servidor, por ejemplo, navegar por páginas web, escuchar música y videos.

Estándar	Velocidades Mbps	Actividades que se pueden hacer
Muy rápido	Mayor a 100	Transmisiones de alta calidad
Rápido	40 - 100	Descarga de archivos grandes, Videoconferencias, transmisión de video en alta definición
Moderado	5 - 40	Transmisión de video en calidad estándar, videollamadas
Lento	0 – 5	Correo electrónico, búsqueda en navegadores, llamadas (VoIP)

Tabla 29. Escala de valoración para la velocidad de carga y descarga

En el apéndice A4 se muestran las figuras con los resultados de cada probador de velocidad por sucursal, se realiza la comparación de datos con los parámetros estándar indicados en las tablas 27, 28 y 29.

Para verificar el riesgo que puede comprometer el rendimiento de la red se hará uso de la tabla 30.

Estándar	Impacto	Nivel de Riesgo
Muy rápido/Excelente	Muy aceptable	Muy bajo
Rápido/ Bueno	Aceptable	Bajo
Moderado/Aceptable	Tolerable	Medio
Malo/ Lento	No deseable	Alto

Tabla 30. Nivel de riesgo entre latencia y ancho de banda

En la **sucursal 1** se tiene un ancho de banda contratado de 200Mbps, en la tabla 31 se pueden observar los detalles de las pruebas tomadas de forma inalámbrica y vía Ethernet mediante los teléfonos VoIP.

	Latencia (ms)	Jitter (ms)	Descarga (Mbps)	Carga (Mbps)	Modo
Google	31		178.7	182.2	WiFi
Megacable	16	1	158.8	186.0	WiFi
IFT	5	1	188.7	187.8	WiFi
Google	99		74.2	87.3	Ethernet
Megacable	35	2	91.4	94.5	Ethernet
IFT	2	1	94.4	94.2	Ethernet

Tabla 31. Medición de velocidades contratadas con el ISP para la sucursal 1

Como se puede observar en las tablas 32 a 33, las pruebas realizadas vía inalámbrica el impacto y nivel de riesgo es **muy bajo** por lo que no compromete el rendimiento de la red. En cambio, en conexión vía Ethernet el indicador de Google indica un impacto **medio**, esta diferencia de parámetros entre WiFi y Ethernet se deriva del hardware usado para la conexión vía Ethernet, ya que el aprovisionamiento de los teléfonos VoIP se basa en el estándar 10/100Base-TX (Fast Ethernet).

WiFi					
Riesgo		Alto	Medio	Bajo	Muy bajo
Impacto	No deseable				
	Tolerable				
	Aceptable				Google
	Muy aceptable				Megacable/ IFT

Tabla 32. Matriz de riesgo

Ethernet					
Riesgo		Alto	Medio	Bajo	Muy bajo
Impacto	No deseable				
	Tolerable			Google	
	Aceptable			Megacable	
	Muy aceptable			IFT	

Tabla 33. Matriz de riesgo

El probador de Google muestra latencias mayores a comparación de los otros probadores, esto es un comportamiento normal ya que cada probador hace la medición de diferentes formas. Algunos procesan diferentes fragmentos de datos durante la prueba, normalmente el ping se hace en el servidor mas cercano, pero esto no siempre se cumple y, al realizar la prueba, toma cualquier servidor, Google no permite seleccionar el servidor mas cercano. Existen otros factores como: Que tan saturada se encuentre la red, las características de equipo o saturación de programas de equipo que se usa para generar dichas pruebas.

En la **sucursal 2** se tiene un ancho de banda contratado de 100Mbps, en la tabla 34 se puede observar los detalles de las pruebas tomadas de forma inalámbrica y vía Ethernet mediante los teléfonos VoIP:

	Latencia (ms)	Jitter (ms)	Descarga (Mbps)	Carga (Mbps)	Modo
Google	96		72.3	21.8	WiFi
Megacable	15	1	72.4	88.7	WiFi
IFT	4	5	79.6	90.6	WiFi
Google	58		53	41.2	Ethernet
Megacable	13	3	67.5	89.2	Ethernet
IFT	8	4	59.6	91.3	Ethernet

Tabla 34. Medición de velocidades contratadas con el ISP para la sucursal 2

En las tablas 35 y 36 se indican un impacto y nivel de riesgo **bajo** por lo que no compromete el rendimiento de la red de acuerdo al ancho de banda que tiene la sucursal en cualquiera de los dos modos de conexión.

WiFi					
Riesgo		Alto	Medio	Bajo	Muy bajo
Impacto	No deseable				
	Tolerable			Google	
	Aceptable				
	Muy aceptable			Megacable/ IFT	

Tabla 35. Matriz de riesgo

Ethernet					
Riesgo		Alto	Medio	Bajo	Muy bajo
Impacto	No deseable				
	Tolerable				
	Aceptable			Google	
	Muy aceptable			Megacable/ IFT	

Tabla 36. Matriz de riesgo

En la **sucursal 3** se tiene un ancho de banda contratado de 100Mbps, en la tabla 37 se puede observar los detalles de las pruebas tomadas de forma inalámbrica y vía Ethernet mediante los teléfonos VoIP:

	Latencia (ms)	Jitter (ms)	Descarga (Mbps)	Carga (Mbps)	Modo
Megacable	13	1	94.8	77.1	WiFi
IFT	3	1	94.8	89.2	WiFi
Google	3		91.3	77.6	WiFi
Google	102		84.4	88.4	Ethernet
Megacable	34	3	93.4	94.4	Ethernet
IFT	2	2	94.8	94.5	Ethernet

Tabla 37. Medición de velocidades contratadas con el ISP para la sucursal 3

En la tabla 35 y 36 se indican un impacto y nivel de riesgo **bajo** por lo que no compromete el rendimiento de la red de acuerdo al ancho de banda que tiene la sucursal en cualquiera de los dos modos de conexión.

WiFi					
Riesgo		Alto	Medio	Bajo	Muy bajo
Impacto	No deseable				
	Tolerable				
	Aceptable				
	Muy aceptable			Megacable/IFT/Google	

Tabla 38. Matriz de riesgo

Ethernet					
Riesgo		Alto	Medio	Bajo	Muy bajo
Impacto	No deseable			Google	
	Tolerable				
	Aceptable			Megacable	
	Muy aceptable			IFT	

Tabla 39. Matriz de riesgo

Para la **sucursal 4** se tiene un ancho de banda contratado de 100Mbps, en la tabla 40 se puede observar los detalles de las pruebas tomadas de forma inalámbrica.

	Latencia (ms)	Jitter (ms)	Descarga (Mbps)	Carga (Mbps)	Modo
Google	99		59.8	89.2	Inalámbrico
Megacable	35	2	74.1	82.8	Inalámbrico
IFT	4	0	81.1	94	Inalámbrico
Google	105		69.4	62.4	Ethernet

Tabla 40. Medición de velocidades contratadas con el ISP para la sucursal 4

En la tabla 35 y 36 se indican un impacto y nivel de riesgo **bajo** por lo que no compromete el rendimiento de la red de acuerdo al ancho de banda que tiene la sucursal en cualquiera de los dos modos de conexión.

WiFi					
Riesgo		Alto	Medio	Bajo	Muy bajo
Impacto	No deseable				
	Tolerable			Google	
	Aceptable			Megacable	
	Muy aceptable			IF	

Tabla 41. Matriz de riesgo

Ethernet					
Riesgo		Alto	Medio	Bajo	Muy bajo
Impacto	No deseable				
	Tolerable			Google	
	Aceptable				
	Muy aceptable				

Tabla 42. Matriz de riesgo

Para la **sucursal 5** se tiene un ancho de banda contratado de 100Mbps, en la tabla 43 se puede observar los detalles de las pruebas tomadas de forma inalámbrica y vía Ethernet:

	Latencia (ms)	Jitter (ms)	Descarga (Mbps)	Carga (Mbps)	Modo
Megacable	42	1	48.4	50.2	WiFi
Google	40		45.8	41.3	WiFi
IFT	11	1	44.9	51.4	WiFi
Google	44		53.8	47.8	Ethernet
Megacable	42	1	51	43.4	Ethernet
IFT	9	1	54.5	51.4	Ethernet

Tabla 43. Medición de velocidades contratadas con el ISP para la sucursal 5

En la tabla 44 y 45 se indican un impacto y nivel de riesgo **bajo** por lo que no compromete el rendimiento de la red de acuerdo al ancho de banda que tiene la sucursal en cualquiera de los dos modos de conexión.

WiFi					
Riesgo		Alto	Medio	Bajo	Muy bajo
Impacto	No deseable				
	Tolerable				
	Aceptable			Megacable/Google	
	Muy aceptable			IFT	

Tabla 44. Matriz de riesgo

Ethernet					
Riesgo		Alto	Medio	Bajo	Muy bajo
Impacto	No deseable				
	Tolerable				
	Aceptable			Megacable/Google	
	Muy aceptable			IFT	

Tabla 45. Matriz de riesgo

Para la **sucursal 6** se tiene un ancho de banda contratado de 50 Mbps, en la tabla 46 se puede observar los detalles de las pruebas tomadas de forma inalámbrica y vía Ethernet:

	Latencia (ms)	Jitter (ms)	Descarga (Mbps)	Carga (Mbps)	Modo
Megacable	57	2	46.2	38.0	WiFi
Google	54		41.1	24.2	WiFi
IFT	26	3	43.6	43.5	WiFi
Megacable	56	1	49.5	51.3	Ethernet
Google	40		53.2	48.5	Ethernet
IFT	24	1	53.5	53.3	Ethernet

Tabla 46. Medición de velocidades contratadas con el ISP para la sucursal 6

En la tabla 47 y 48 se indican un impacto y nivel de riesgo **bajo** por lo que no compromete el rendimiento de la red de acuerdo al ancho de banda que tiene la sucursal en cualquiera de los dos modos de conexión.

WiFi					
	Riesgo	Alto	Medio	Bajo	Muy bajo
Impacto	No deseable				
	Tolerable				
	Aceptable			Megacable/ Google/IFT	
	Muy aceptable				

Tabla 47. Matriz de riesgo

Ethernet					
	Riesgo	Alto	Medio	Bajo	Muy bajo
Impacto	No deseable				
	Tolerable				
	Aceptable			Megacable/ Google/IFT	
	Muy aceptable				

Tabla 48. Matriz de riesgo

4.4.2 ANCHO DE BANDA EN UNA RED CASERA

El contrato con el ISP Total play para una red casera establece la entrega de 150Mbs, con un precio mensual de $629.00 MXN

- En este caso podemos ver que la conexión es asimétrica, los ISP para hogar ofertan velocidades de descarga mayor a la de carga como lo podemos apreciar en la tabla 49.
- Los indicadores muestran un impacto y nivel de riesgo **muy bajo** por lo que no compromete el rendimiento de la red en descarga, tabla 50.

	Latencia (ms)	Jitter (ms)	Descarga (Mbps)	Carga (Mbps)	Tipo
Google	34		171.4	28.5	Inalámbrico
IFT	4	5	156.8	30.6	Inalámbrico
Megacable	41	4	159.8	30.3	Inalámbrico

Tabla 49. Medición de velocidades contratadas con el ISP para red casera

WiFi					
Riesgo		Alto	Medio	Bajo	Muy bajo
Impacto	No deseable				
	Tolerable				
	Aceptable		Google/Megacable (Carga)		Megacable/Google (Descarga)
	Muy aceptable		IFT (Carga)		IFT (Descarga)

Tabla 50. Matriz de riesgo red casera

4.5 CONCLUSIONES

Con base en el estudio de la red empresarial se presentan las siguientes conclusiones técnicas y no técnicas:

- Se realizó el mapeo y validación de la topología de las sucursales usando el inventario de cada centro de datos, se indica en el apéndice A2. En la simulación de cada sucursal se realizó el estudio, análisis y configuración del router y switch con el fin de conocer el funcionamiento de la red de comunicación de la LAN y VLAN de voz y datos.

Sucursal	N° de equipos simulados	Sugerencias adicionales
1	96	Es recomendable contar con una conexión redundante, ya que la disponibilidad y estabilidad de la red es un tema de suma importancia para la organización.
2	69	Es recomendable contar con una conexión redundante
3	33	Es necesario realizar cambio del controlador de los AP ya que eventualmente ocasiona la desconexión de los equipos que se conectan vía Wifi.
4	30	Realizar actualización en el firewall
5	31	Solo cuenta con un firewall (FW4) propiedad del ISP y solo se usa para el monitoreo del equipo de comunicaciones y supervisión de las VLAN de voz. Se debe incluir el firewall de protección para dichas sucursales y que, además, funcionará para la supervisión centralizada desde la sucursal principal mediante conexión remota por VPN.
6	20	

Tabla 51. Numero de equipos simulados y recomendaciones

- Con base en las pruebas de velocidad de los tres verificadores (Google, IFT, Megacable) se logró conocer los anchos de banda y además verificar el rendimiento de cada sucursal con base en la medición de ancho de banda y latencia. Estas pruebas se realizar en horas de mayor concurrencia.

Sucursal	Riesgo
1	Muy bajo
2	Bajo
3	Bajo
4	Bajo
5	Bajo
6	Bajo

Tabla 52. Nivel de riesgo de las sucursales

.

Para la sucursal 4. Se omitieron las pruebas en modo Ethernet ya que al realizar la validación se interrumpía la conexión con el servidor, es urgente realizar la actualización del firewall.

La arquitectura de la red se ha adecuado conforme las necesidades de la empresa, sin embargo, la cantidad de nodos es limitado y por ello se hace uso de los teléfonos VoIP para conecta el cable Ethernet hacia una computadora. Tomando en cuenta que los enlaces de fibra óptica contratados se encuentran entre los 100-200 Mbps para las sucursales 1, 2,3,4 y 5 y que los teléfonos VoIP tienen una capacidad máxima de 100Mbps, se deduce que esto interfiere en la capacidad de transferencia dando como resultado velocidades por debajo de los 100Mbps. Para mejorar la velocidad de transferencia y rendimiento en modo Ethernet conectados desde los teléfonos VoIP, es necesario considerar en la próxima renovación de equipos de telefonía el cambio de versiones a Gigabit.

Otras sugerencias para aumentar la velocidad y/o detectar errores que comprometan la velocidad se recomienda lo siguiente:

- Revisar características de los equipos en uso y nuevas adquisiciones
- Revisión de nodos y cableado
- Monitoreo red
- Programas en segundo plano (que consuma ancho de banda)
- Fallos de ISP

- Comprobar el estado de la tarjeta de red de los equipos

- Existe una diferencia notable entre las conexiones de las sucursales y la red casera, para las sucursales son simétricas mientras que para la casera es totalmente asimétrica; la velocidad de carga para las sucursales es estables.

- Se exploran los niveles de seguridad de la red, tanto para WEP como WPA personal, el nivel de seguridad es muy vulnerable; es recomendable como primera solución, realizar el cambio a WPA Enterprise, para tener el control de acceso mediante el servidor de autentificación RADIUS y posteriormente incluir un cambio a tecnologías con WPA2 – Enterprise. Sin embargo, desde el 2023 ya es recomendable el uso de WPA3, ya sea en su nivel personal o enterprise. Es prioritario realizar un cambio urgente y seguir evolucionando a tecnologías que ofrezcan mejor seguridad ante nuevas amenazas. En la tabla 53 se muestra la propuesta de inversión por sucursal. Se toma como base la misma cantidad de AP instalados actualmente.

Sucursal	Numero de AP	Marca /Modelo	Precio Unitario	Total
1	12	Cisco Catalyst 9105/9115	$18,000.00	$216,000.00
		TPLINK -EAP670	$5,000.00	$60,000.00
2	7	Cisco Catalyst 9105/9115	$18,000.00	$126,000.00
		TPLINK -EAP670	$5,000.00	$35,000.00
3	5	Cisco Catalyst 9105/9115	$18,000.00	$90,000.00
		TPLINK -EAP670	$5,000.00	$25,000.00
4	2	Cisco Catalyst 9105/9115	$18,000.00	$36,000.00
		TPLINK -EAP670	$5,000.00	$10,000.00
5	2	Cisco Catalyst 9105/9115	$18,000.00	$36,000.00
		TPLINK -EAP670	$5,000.00	$10,000.00
6	2	Cisco Catalyst 9105/9115	$18,000.00	$36,000.00
		TPLINK -EAP670	$5,000.00	$10,000.00

Tabla 53. Propuesta para cambio de AP

- Al usar la versión del simulador académico *packet tracer* se puede generar la simulación, pero también existe la limitante para la configuración de los teléfonos VoIP y las computadoras, ya que no se puede asignar en un puerto la VLAN de voz y datos, por ello se asignan puertos independientes para cada dispositivo.

4.5.1 RECOMENDACIONES ADICIONALES

A continuación, se muestra recomendaciones adicionales

1. Los centros de datos fueron adaptados a las condiciones de las oficinas que no cubren los requisitos mínimos solicitados por la norma TIA-942-A. Para una certificación se deberá valorar una inversión para cumplir con los 4 subsistemas (Telecomunicaciones, Arquitectura, Sistema eléctrico, Sistema mecánico)
2. Como reforzamiento de medidas preventivas deberá crearse campañas y políticas sobre el uso de dispositivos y conexión a sitios, ya que la seguridad de las WLAN no solo depende de herramientas seguridad, sino que conlleva un proceso de concientización de usuarios.

- Uso de aplicaciones móviles
- Uso de aplicaciones bajo licenciamiento
- Uso de redes caseras o publicas
- Políticas de seguridad y planes de respuesta a incidentes.

Por políticas y seguridad de la empresa se omiten datos de la empresa y nombres de la estructura organizacional, la publicación de marcas y modelos de los componentes de infraestructura, IP públicos y privados. Se permite mencionan las características de los componentes de la infraestructura.

4.6 EPÍLOGO

Durante el proceso de elaboración de la tesis tuve que poner en práctica las habilidades cognitivas que desarrollé durante mi formación profesional y laboral: tuve que poner **atención** para poder recabar los antecedentes en las diversas fuentes que tuve disponibles, posterior a ello tuve que **elaborar** la traducción de lo investigado para poder plasmarlo conforme a mi entendimiento, realizando una tarea de **comprensión**. Si bien no todo lo investigado lo retuve en su totalidad, pero si me permite tener una **recapitulación** de **conocimientos** que utilicé mientras me encontraba estudiando la licenciatura.

Este trabajo no hubiera sido posible sin el apoyo de personas claves en mi desarrollo profesional:

El presente trabajo quiero dedicarlo a mi mamá, que siempre me ha brindado su apoyo incondicional, por ser mi inspiración de todo lo que hago, sus consejos y por estar en los momentos buenos y ser mi mayor fuente de fortaleza en los momentos difíciles. Gracias por ser la mujer más increíble que conozco.

A la persona más valiosa que tengo en la vida, a mi hija hermosa, mi alegría, gracias por tu comprensión, por adaptarte a mis horarios y por ser tan paciente conmigo durante los momentos en los que me encontraba dedicada a la tesis. Eres mi mayor motivación y mi fuente de inspiración para seguir luchando por mis sueños.

A mi esposo, gracias por tu paciencia infinita, siempre estás ahí para animarme, motivarme y recordarme que todo se puede aun cuando sean momentos difíciles. Tu comprensión y sacrificio han sido invaluables para mí. Gracias por comprender mis horas de estudio y por hacerte cargo de las tareas del hogar para que yo pudiera concentrarme en mi tesis. Eres parte fundamental de mi éxito y te agradezco de todo corazón por estar siempre a mi lado.

A usted, Ing. BJB, le agradezco profundamente por su confianza y apoyo en mi desarrollo profesional. Por permitirme conciliar mi trabajo con mis estudios, por brindarme la flexibilidad necesaria para poder desarrollar mi tesis y por permitirme formar parte de su equipo de trabajo. Su apoyo y comprensión ha sido fundamental para alcanzar este logro.

De manera especial, quiero agradecer a la Lic. DJ por la confianza que ha depositado en mí, por darme la oportunidad de asumir nuevos retos y responsabilidades.

A mi jefe directo por la confianza desde que llegué a la empresa. Agradezco especialmente su alta exigencia, la cual me ha permitido desarrollar mi capacidad para trabajar bajo presión y cumplir con plazos ajustados. Sus constantes desafíos me han motivado a salir de mi zona de confort y aprender cosas nuevas, y su retroalimentación honesta y constructiva me ha ayudado a identificar áreas de mejora y a perfeccionar mis habilidades.

A mi director de tesis el M. en C. José Ignacio Castillo Velázquez, le expreso mi más sincero agradecimiento por su guía y apoyo durante la realización de mi tesis. Por su paciencia, consejos y por compartir conmigo sus conocimientos y experiencia. Agradezco especialmente su constante seguimiento y presión, los cuales me han permitido mantenerme enfocada y avanzar en mi tesis a pesar de los desafíos.

Al Dr. Adolfo Horacio Escalona Buendía, el Ing. José Miguel Vargas Pliego y el Ing. Ricardo Galindo Reyes, les agradezco profundamente su valiosa colaboración y sus aportaciones a mi tesis. Gracias por su tiempo, por su disposición y por compartir conmigo sus conocimientos. Su asesoría ha sido decisiva para mejorar la calidad de mi trabajo y para lograr un resultado final satisfactorio.

Y a todas aquellas personas que son importantes en mi vida y que no menciono sus nombres pero que de una u otra manera han contribuido a mi formación y a la realización de este proyecto de investigación, les expreso mi más sincero agradecimiento.

5. REFERENCIAS

[1] E. J. Chikofsky and J. H. Cross, "Reverse engineering and design recovery: a taxonomy," in IEEE Software, vol. 7, no. 1, pp. 13-17, Jan. 1990, doi: 10.1109/52.43044.

[2] X. Li and L. Chen, "A Survey on Methods of Automatic Protocol Reverse Engineering," 2011 Seventh International Conference on Computational Intelligence and Security, Sanya, China, 2011, pp. 685-689, doi: 10.1109/CIS.2011.156.

[3] Y. He, H. Shu and X. Xiong, "Protocol Reverse Engineering Based on DynamoRIO," 2009 International Conference on Information and Multimedia Technology, Jeju, Korea (South), 2009, pp. 310-314, doi: 10.1109/ICIMT.2009.26.

[4] J.I Castillo, N Galicia, J. A López, “Ingeniería inversa parcial y simulación de la infraestructura de una red de datos MAN”, Ingeniería en Sistemas Electrónicos y Telecomunicaciones, Universidad Autónoma de la Ciudad de México, ,2013, pp 1- 5.

[5] Schwart. Mathew, Reverse - Engineering, 2001, Available from [https://www.computerworld.com/article/2585652/reverse-engineering.html]

[6] J. -I. Castillo-Velazquez and M. -I. Trigueros-Galicia, "UTILCON 1.0: A Conference Management System trainer in Spanish with strict refereeing control," 2019 IEEE XXVI International Conference on Electronics, Electrical Engineering and Computing (INTERCON), Lima, Peru, 2019, pp. 1-4, doi: 10.1109/INTERCON.2019.8853831.

[7] M. -I. Trigueros-Galicia , “Útilcon”, versión 1.0, 2018, Available from: [http://utilcon.esy.es/]

[8] EasyChair Ltd, “EasyChair”, 2002-2023, Available from: [https://easychair.org/]

[9] Digital Equipment corporation, The Ethernet, a Local Area Network and Physical Layer Specifications, Version 2.0, nov. 1982 Pag. 1, Available from [http://decnet.ipv7.net/docs/dundas/aa-k759b-tk.pdf/]

[10] Commer, Douglas E., “Internetworking with TCP/IP”, Vol I Principles, Protocols, and Architecture. Prentice Hall Inc., Pag. 19, 1995

[11] IEEE, “FUNCTIONAL REQUIREMENTS”, Version 5.4, Oct.1981, Available from: [https://www.ieee802.org/802_archive/fureq6-8.html]

[12] Castillo Velazquez, Jose Ignacio, “Redes de datos” contexto y evolución” Tercera edición. Samsara, 2019. Pag [87-163].

[13] Stallings, William, “Comunicaciones y Redes de Computadores”. Sexta Edición. Prentice Hall Inc., 2004. pp 200, 484-489 ,516

[14] Perpinan, Antonio, “ADMINISTRACION DE ES GNU/LINUX”, Fundación Código Libre Dominicano, 2004, pp 13-16

[15] S. R. Lee, J. -S. Back, J. -S. Oh and M. -A. Jeong, "A mesh topology formation scheme for IEEE 802.15.4 based wireless sensor networks," 2015 Seventh International Conference on Ubiquitous and Future Networks, Sapporo, Japan, 2015, pp. 150-152, doi: 10.1109/ICUFN.2015.7182523.

[16] USB Implementers Forum, Inc. Available from: [www.usb.org]

[17] Cisco, “Transmisión de datos en la red”. 2011, Available from: [http://www.cca.org.mx/profesores/abc/pdfs/cisco/cisco_0.pdf]

[18] DARPA, RFC 1661, The Point-to-Point Protocol (PPP),1994

[19] DARPA, rfc 2460, Internet Protocol, Version 6 (IPv6) ,1998

[20] DARPA, RFC 792, Internet Control Message Protocol,1981

[21] Stevens, Richard, “TCP/IP Illustrated, Volume 1: The Protocols”, Addison Wesley, 1994 pp 2.

[22] IBM, Documentación, User Datagram Protocol, 2021, Available from: [https://www.ibm.com/docs/es/aix/7.1?topic=protocols-user-datagram-protocol]

[23] DARPA, RFC 793, Transmission control protocol, 1981

[24] IBM, IBM Documentation, 2021, Available from: [https://www.ibm.com/docs/en]

[25] DARPA, RFC 959, File Transfer protocol, 1985

[26] DARPA, RFC 5321, Simple Network Management Protocol, 2008

[27] DARPA, RFC 2131, Dynamic Host Configuration Protocol,1997

[28]Gladford technologies Ltd, “Cable-management”, Available from: [https://gladford.com.ng/cable-management/]

[29] ANSI/TIA/EIA-568-B.1 , Commercial Building Telecommunications Cabling Standard, 2001.

[30] ANSI/TIA-942-A, Telecommunications Infrastructure Standard for Data Centers, 2012.

[31] Ventas de seguridad, “Tecnología de la información, El standard TIA 942” , 2007, Available from: [http://www.areadata.com.ar/pdf/El%20standard%20TIA%20942%20-vds-11-4.pdf]

[32] Foro Huawei ,Patch Panel, 2022, Available from: [https://forum.huawei.com/enterprise/es/%C2%BFqu%C3%A9-es-un-patch-panel/thread/1028040-100237]

[33] Mendez, Leobardo, Blog Cisco Latinoamérica , “4 formas de proteger la red WiFi de tu empresa”, 2018, Available from: [https://gblogs.cisco.com/la/en-leobardo-4-formas-de-proteger-la-red-wifi-de-tu-empresa/]

[34] Onelogin, What is a DDoS Attack? , Available from: [https://www.onelogin.com/learn/ddos-attack]

[35] Cisco Network Academy, “Amenazas de WLAN”, Available: [https://www.sapalomera.cat/moodlecf/RS/3/course/module4/4.3.1.2/4.3.1.2.html#:~:text=Un%20usuario%20malintencionado%20interfiere%20en,leg%C3%ADtimo%20pueda%20acceder%20al%20medio.]

[36] Wireless Communication, Network Concepts and Standard, 1994 , Available from: [http://www.wirelesscommunication.nl/reference/chaptr01/dtmmsyst/ism.htm]

[37] thuthuattienich ,”2.4 Ghz và 5 Ghz là gì? Sự khác nhau giữa Wi-Fi 2.4 Ghz và 5 Ghz?”, Available from: [https://thuthuattienich.com/wiki/2-4ghz-vs-5ghz/]

[38] Cisco Network Academy, “Conceptos de tecnología inalámbrica”, Available from: [https://www.sapalomera.cat/moodlecf/RS/3/course/module4/index.html#4.1.1.5]

[39] Cisco Network Academy, “Introducción a la tecnología inalámbrica”, Available from: [https://www.sapalomera.cat/moodlecf/RS/3/course/module4/index.html#4.1.1.3]

[40] John L. MacMichael ”Auditing Wi-Fi Protected Access (WPA) Pre-Shared Key Mode” , 2005, Available from : [https://www.linuxjournal.com/article/8312]

[41] Cisco “What Is Wi-Fi Security?” , Available from: [https://www.cisco.com/c/en/us/products/wireless/what-is-wi-fi-security.html#~protocols]

[42] AVAST “Wi-Fi Security: WEP vs WPA or WPA2”, 2022, Available from:, [https://www.avast.com/c-wep-vs-wpa-or-wpa2]

[43] Wi- Fi Alliance, WAP3 Specification, 2022, Available from: [https://www.wi-fi.org]

[44] Cisco “Protección de WLAN” , Available from: , [https://www.sapalomera.cat/moodlecf/RS/3/course/module4/4.3.2.4/4.3.2.4.html]

[45] DARPA, RFC 2865, Remote Authentication Dial In User Service (RADIUS)

[46] IPCisco,” Wireless Security Protocols”, Available: [https://ipcisco.com/lesson/wireless-security-protocols/]

[47] Gobierno de la Ciudad de Mexico, Wifi gratuito en la Ciudad de Mexico , Available from: [https://internetparatodas.cdmx.gob.mx/puntos-wifi/escuela_publica]

[48] J. -I. Castillo-Velazquez and R. -B. Silva-Lopez, "Tuning to ADVNETLAB Methodology for thesis advisory in science and engineering for ICT," 2018 IEEE XXV International Conference on Electronics, Electrical Engineering and Computing (INTERCON), Lima, Peru, 2018, pp. 1-4, doi: 10.1109/INTERCON.2018.8526417.

[49] J. -I. Castillo-Velazquez, M. A. Garcia and D. J. Serrano Martinez, "Hardening as a best practice for WLAN Security Meanwhile WPA3 is released," 2019 IEEE 39th Central America and Panama Convention (CONCAPAN XXXIX), Guatemala City, Guatemala, 2019, pp. 1-5, doi: 10.1109/CONCAPANXXXIX47272.2019.8977073.

APÉNDICE

A1.-INVENTARIO POR SUCURSAL

CANTIDAD	MODELO	TIPO
1	AP4	ACCESS POINT
3	AP1	ACCESS POINT
1	AP2	ACCESS POINT
5	AP3	ACCESS POINT
2	AP5	ACCESS POINT
1	SFP	SWITCH
1	SW1	SWITCH
5	SW2	SWITCH
1	FW4	FIREWALL
1	1K VA	UPS
1	FW3	FIREWALL
3	2KVA	UPS
4	24P	PACH PANEL

Inventario del equipo de comunicación de la sucursal principal

CANTIDAD	MODELO	TIPO
7	AP1	ACCESO POINT
1	SFP	SWITCH
1	SW1	SWITCH
2	SW2	SWITCH
1	FW4	FIREWALL
1	1K VA	UPS
1	SG300-28PP-K9	SWITCH
1	FW2	FIREWALL
1	750VA	UPS
3	24P	PACH PANEL

Inventario del equipo de comunicación de la sucursal 2

CANTIDAD	MODELO	TIPO
5	AP5	ACCESS POINT
1	SFP	SWITCH
1	SW1	SWITCH
1	FW4	FIREWALL
1	1K VA	UPS
1	FW1	FIREWALL
1	450VA	UPS
1	24P	PACH PANEL

Inventario del equipo de comunicación de la sucursal 3

CANTIDAD	MODELO	TIPO
2	AP2	ACCESS POINT
1	SFP	SWITCH
1	SW1	SWITCH
1	SW2	SWITCH
1	FW4	FIREWALL
1	1K VA	UPS
1	FW1	FIREWALL
1	1.2 KVA	UPS
2	24P	PACH PANEL

Inventario del equipo de comunicación de la sucursal 4

CANTIDAD	MODELO	TIPO
2	AP6	ACCESS POINT
1	SFP	SWITCH
1	SW1	SWITCH
1	SW2	SWITCH
1	FW4	FIREWALL
1	1K VA	UPS
1	24P	PACH PANEL

Inventario del equipo de comunicación de la sucursal 5

CANTIDAD	MODELO	TIPO
2	AP6	ACCESS POINT
1	SFP	SWITCH
1	SW1	SWITCH
1	SW2	SWITCH
1	FW4	FIREWALL
1	1K VA	UPS
1	24P	PACH PANEL

Inventario del equipo de comunicación de la sucursal 6

A2.- ANCHO DE BANDA POR LOCALIDAD

UBICACIÓN	ANCHO DE BANDA INCLUIDO
Sucursal principal	200 Mbps
Sucursal 2	100 Mbps
Sucursal 3	100 Mbps
Sucursal 4	100 Mbps
Sucursal 5	100 Mbps
Sucursal 6	50 Mbps

Anchos de banda

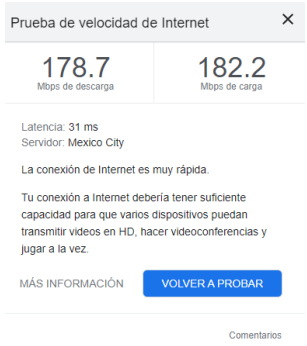
A3.- ESPECIFICACIONES PARA LOS AP

- Cisco Catalyst 9115 Series Wi-Fi 6 Access Points
- EAP690E HD Access Points Wi-Fi 6E AXE11000
- EAP670 AX5400 Multi-Gigabit Ceiling Mount WiFi 6 Access Point | TP-Link
- Access Point U6 Pro

	Cisco Catalyst 9115	EAP690E HD	EAP670	U6-PRO
Marca	Cisco	Tplink	Tplinkl	Ubiquiti
Tasa de transferencia (máx)		2.4Ghz 1148 Mbps 5.0 Ghz 4804 Mbps	2.4Ghz 574 Mbps 5.0 Ghz 4804 Mbps	4800Mbit/s
Velocidad	2500 Mbit/s	11000 Mbit/s	2500 Mbit/s	1000Mbit/s
PoE Mode	802.3at PoE+	802.3bt PoE+	802.3at PoE+	PoE+
Clientes concurrentes		2000	300+	300+
Estandar Wi Fi	IEEE 802.3, 3ab, 3af/at, 11 a/b/g/n/ ac/ax, 11h, 802.11 d	IEEE 802.11 a/b/g/n/ac/ax	802.11a/b/g WiFi 4/WiFi 5/WiFi 6	802.11a/b/g WiFi 4/WiFi 5/WiFi 6
Seguridad inalámbrica	802.11i, Wi-Fi Protected Access 3 (WPA3), WPA2, WPA, 802.1X, Advanced Encryption Standard (AES)	WPA-Personal/Enterprise, WPA2-Personal/Enterprise, WPA3-Personal/Enterprise, OWE	WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3)	WPA-PSK, WPA-Enterprise (WPA/WPA2/WPA3)

A4.- MEDICIÓN DE VELOCIDAD

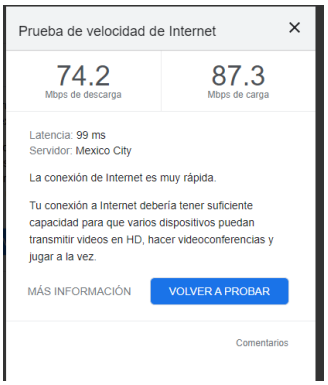
Sucursal principal



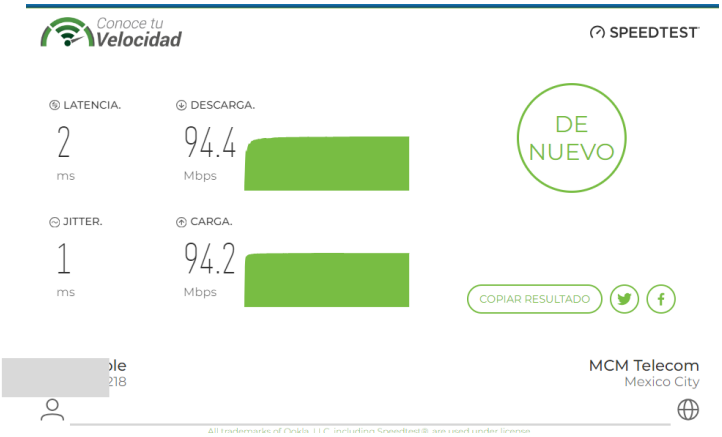
(a)Test inalámbrica realizado con Google

(b)Test inalámbrica realizado con IFT

(c)Test inalámbrica realizado con Megacable



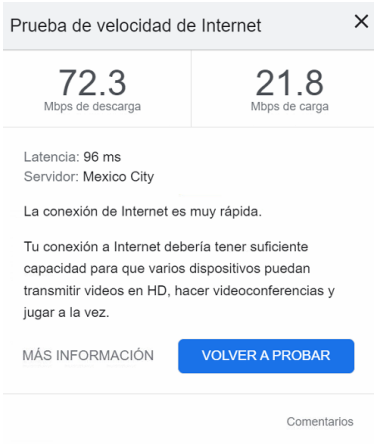
(a)Test modo Ethernet realizado con Google



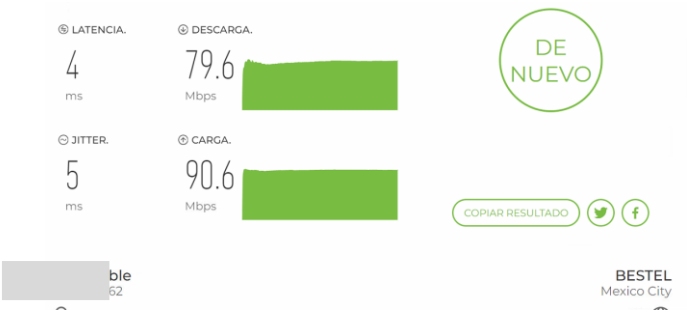
(b)Test modo Ethernet realizado con IFT

(c)Test inalámbrica realizado con Megacable

Sucursal 2

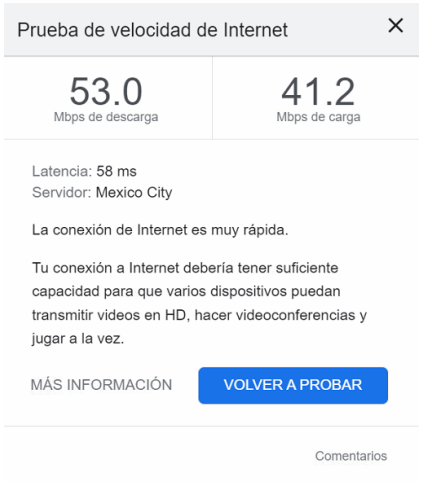


(a)Test modo inalámbrica realizado con Google



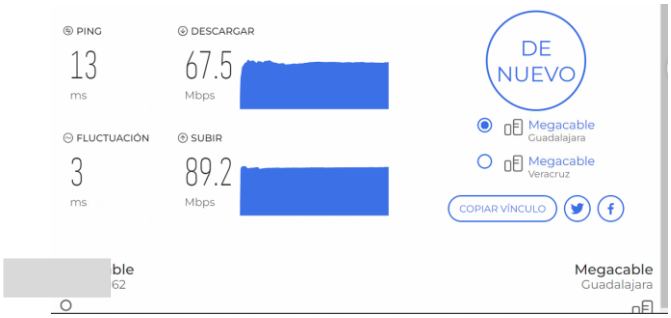
(b)Test modo inalámbrica realizado con IFT

(c)Test modo inalámbrica realizado con Megacable



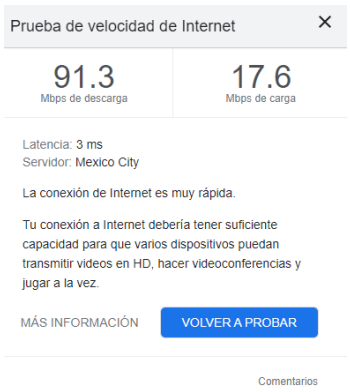
(a)Test modo Ethernet realizado con Google

(b)Test modo Ethernet realizado con IFT

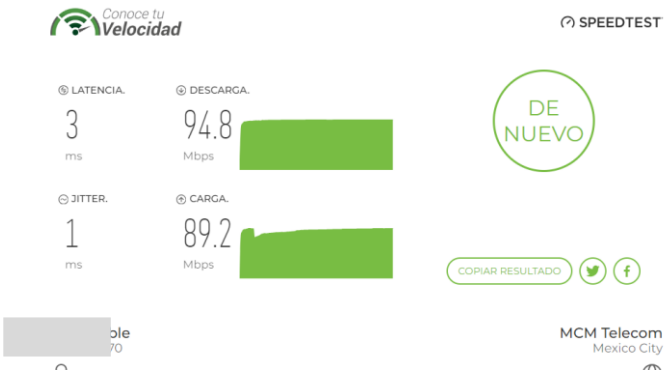


(c)Test inalámbrica realizado con Megacable

Sucursal 3

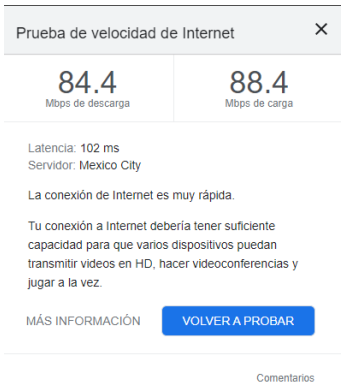


(a)Test modo inalámbrica realizado con Google



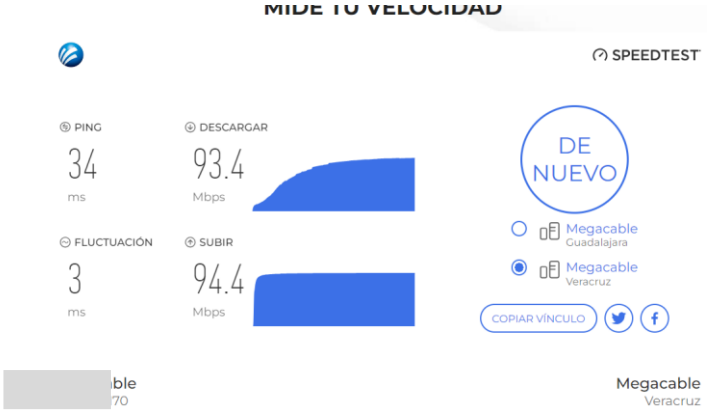
(b)Test modo inalámbrica realizado con IFT

(c)Test modo inalámbrica realizado con Megacable



(a)Test modo Ethernet realizado con Google

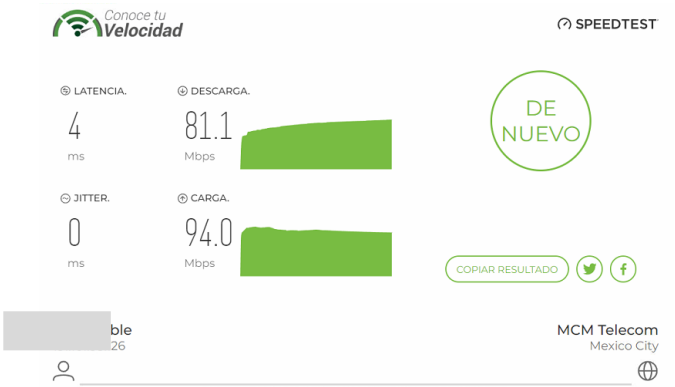
(b)Test modo Ethernet realizado con IFT



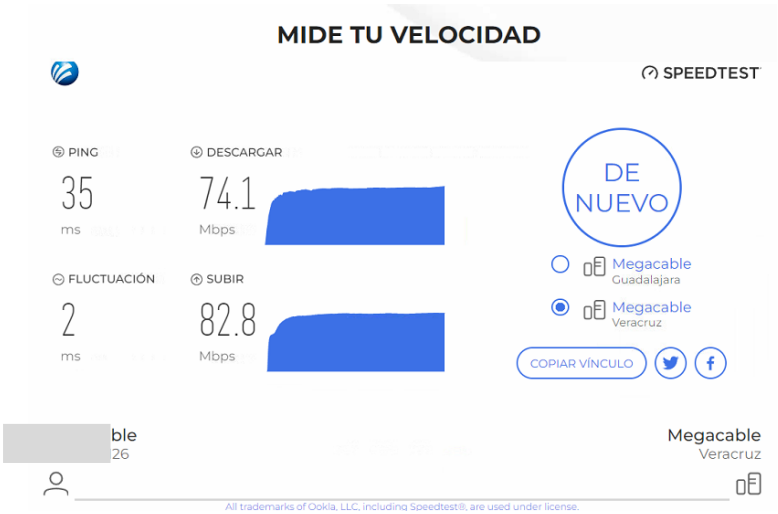
(c)Test inalámbrica realizado con Megacable

Sucursal 4

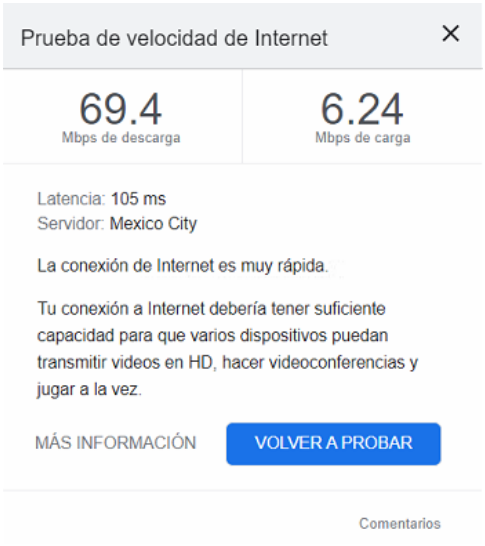
(a)Test modo inalámbrica realizado con Google



(b)Test modo inalámbrica realizado con IFT

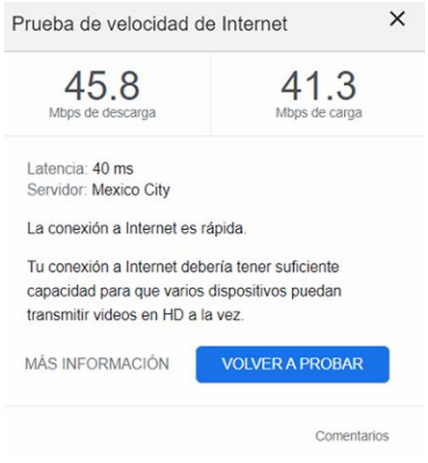


(c)Test modo inalámbrica realizado con Megacable

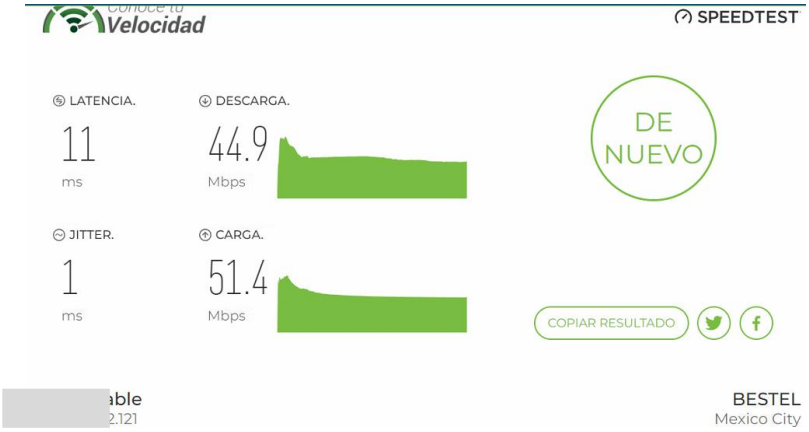


(a)Test modo Ethernet realizado con Google

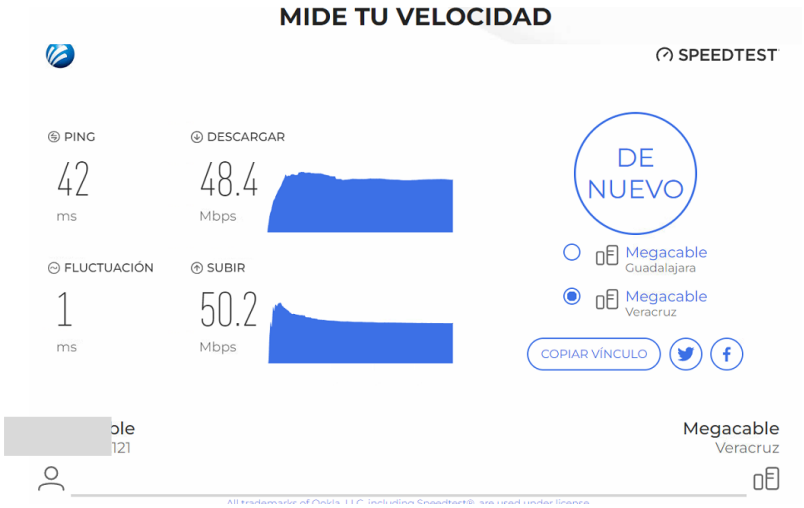
Sucursal 5



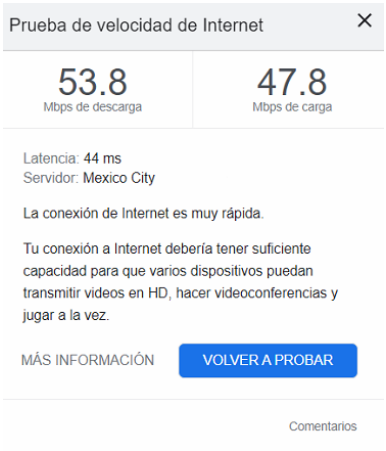
(a)Test modo inalámbrica realizado con Google



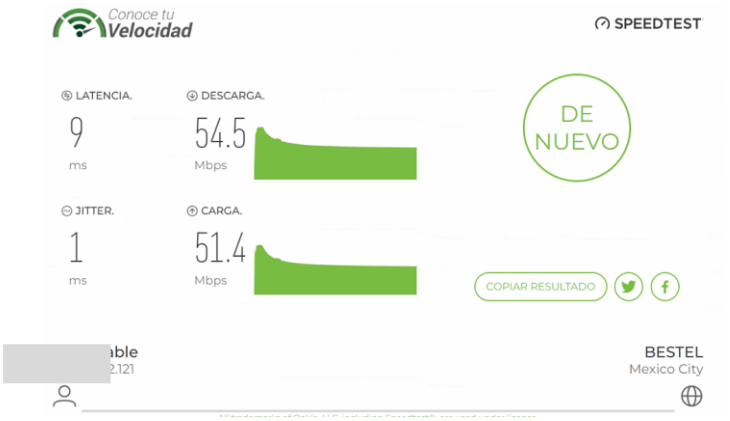
(b)Test modo inalámbrica realizado con IFT



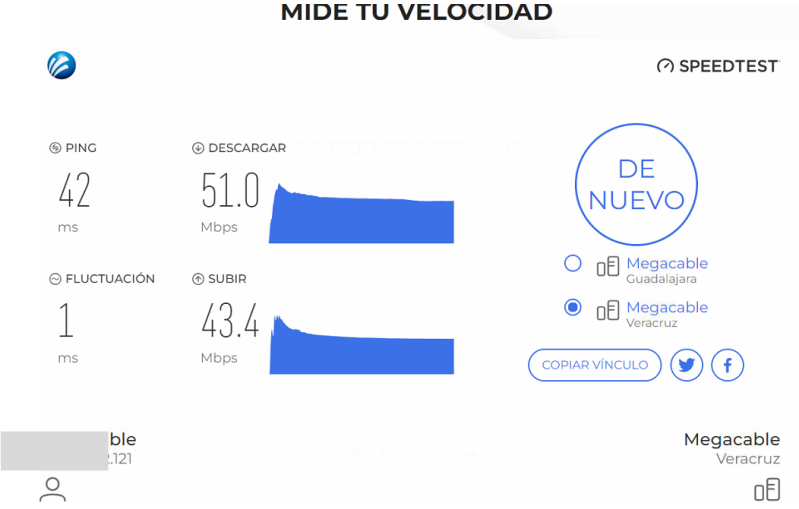
(c)Test modo inalámbrica realizado con Megacable



(a)Test modo Ethernet realizado con Google



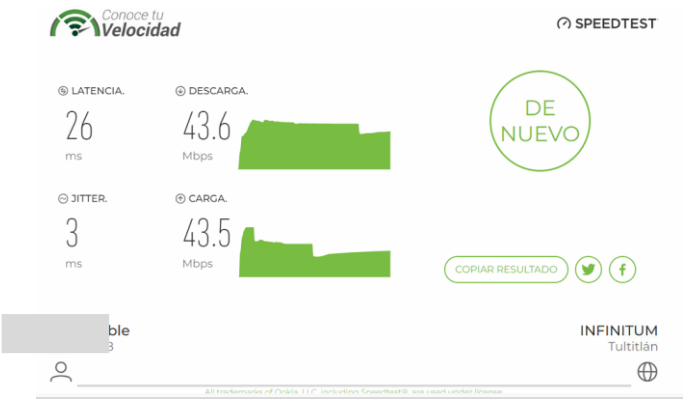
(b)Test modo Ethernet realizado con IFT



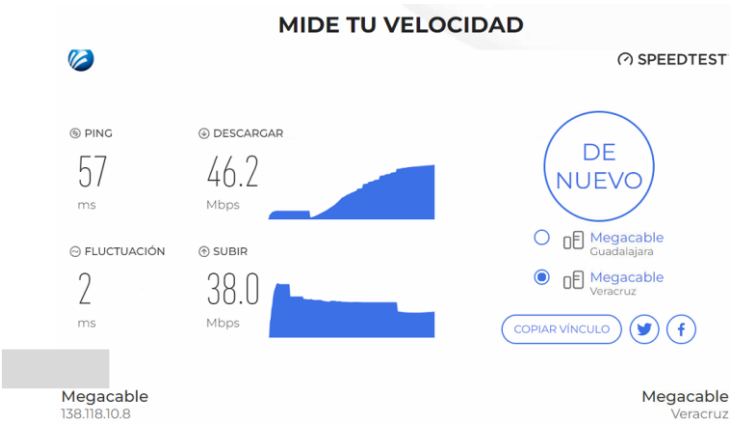
(b)Test modo Ethernet realizado con IFT

Sucursal 6

(a)Test modo inalámbrica realizado con Google



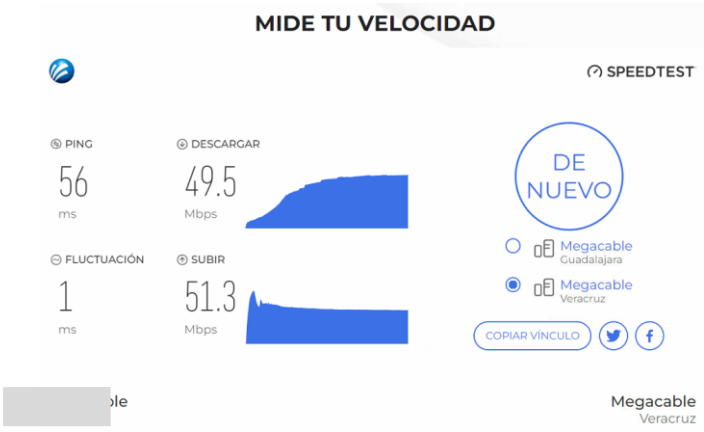
(b)Test modo inalámbrica realizado con IFT



(c)Test modo inalámbrica realizado con Megacable

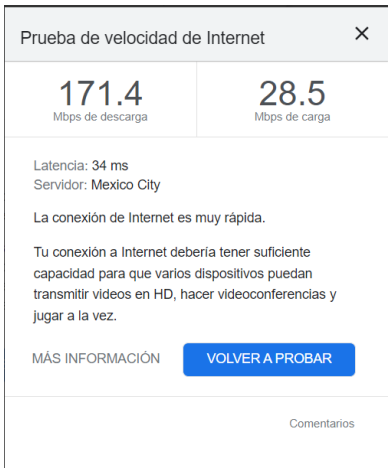
(a)Test modo Ethernet realizado con Google

(b)Test modo Ethernet realizado con IFT

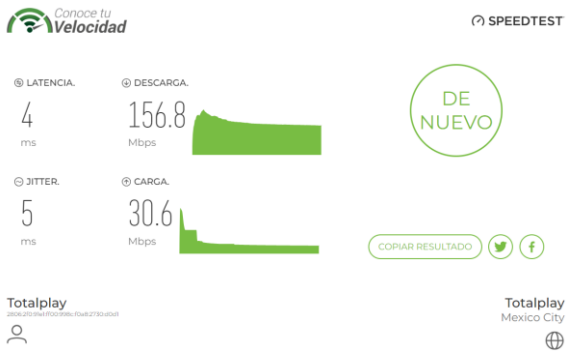


(c)Test inalámbrica realizado con Megacable

Red casera



(a)Test modo inalámbrica realizado con Google



(b)Test modo inalámbrica realizado con IFT

(c)Test modo inalámbrica realizado con Megacable

LISTA DE ACRÓNIMOS

ACK- Acknowledgment / Reconocimiento

AES- Advanced Encryption Standard / Estadar de cifrado avanzado

AP- *Acces Point / Punto de acceso*

ARP - *Address Resolution Protocol* /Protocolo de resolución de direcciones

ASCII - American Standard Code for Information Interchange / Código Estándar estadounidense para el Intercambio de Información

Backbone- Cableado vertical o troncal

CCMP- Counter Cipher Mode with Block Chaining Message Authentication Code Protocol/ Protocolo de código de autenticación de mensajes de encadenamiento de bloques de cifrado en modo contador

CRC-32 -*Cyclic Redundancy Checking/* Verificación por redundancia cíclica

CSMA/CD - *Carrier Sense Multiple Access with Collision Detection*/ Acceso Múltiple por Detección de Portadora con Detección de Colisiones)

DCE - Data Circuit Terminating Equipment / Equipo de comunicación de datos

DDoS- Distributed denial of service/ Denegacion de servicios de tipo distribuidos

DHCP- Dynamic Host Configuration Protocol- Protocolo de configuración dinámica de host

DNS- Domain Name System protocol- Protocolo de Sistema de Nombres de Dominio

DoS- *Denial of service/* Denegación de servicios

DTE - Data Terminal Equipment / Equipo terminal de datos

DVR - Digital Video Recorder / Grabador de video digital

EIA -Electronic Industries Alliance/ Alianza de Industrias Electrónicas

FCC - Federal Communications Commission / Comisión Federal de Comunicaciones

FCC- *Federal Communications Commision* / Comisión Federal de Comunicaciones

FTP- File Transfer Protocol - Protocolo de transferencia de archivos

Gbps - Giga bits por segundo

HTTP- Hypertext Transfer Protocol - Protocolo de transferencia de hipertexto

ICMP - *Internet Control Message Protocol* / Protocolo de control de mensajes de Internet

IDC - *Insulation-Displacement Connector/* Conector de desplazamiento de aislamiento

IEEE - Institute of Electrical and Electronics Engineer / Instituto de Ingenieros Eléctricos y Electrónicos

IPV4- Internet Protocol / Protocolo de Internet, versión 4

IPV6- Internet Protocol / Protocolo de Internet, versión 6

ISM- *Industrial Scientific and Medical*- Banda de frecuencia industrial, científica y medica

ISP- Internet Service Provider / Proveedor de servicios de Internet

ITU – International telecommunication Union / Union internacional de Telecomuncaciones

KSA - Key Scheduling Algorithm/ Algoritmo de programacion de claves

LAN - Local Área Network / Red de Área Local

LCP - *Link Control Protocol/* Protocolo de control de enlace

LLC- Logical Link Control/ Control Lógico de Enlace

MAC- Media Access Control / Control de acceso al medio

MAN: Metropolitan Area Network/ Red de área metropolitana

Mbps- Mega bits por segundo

MIC- Message Integrity Codes / Códigos de integridad de mensajes

NCP- *Network Control Protocols* / Protocolos de control de red

NIC - Network Interface Card / Tarjeta de interfaz de red

OSI - Open Systems Interconnection / Sistemas abiertos de interconexión

PBX- Private Branch Exchange

Pendrives: Dispositivo portátil de almacenamiento

PoE: Power over Ethernet / Alimentación a traves de Ethernet

PPP - Point-to-Point Protocol- Protocolo punto a punto

PRGA - Pseudo- Random Generation Algorithm / Algoritmo de generación aleatorio

RADIUS- Remote Authentication Dial-In User Service/ Protocolo estándar de internet que proporciona servicios centralizados de gestion de autentificación.

RC4 - *Rivest Cipher 4/ Cifrado Rvest 4*

RF- Radio frequency / Radio frecuencia

RS- 232 Recommended Standard 232 / Estándar Recomendado 232

RST – *Reset* / Reiniciar

SFP - Small Form-factor Pluggable Transceiver /Ffactor pequeño de forma conectable

SMTP- Simple Mail Transfer Protocol- Protocolo simple de transferencia de correo

SNMP- Simple Network Management Protocol- Protocolo simple de gestión de red

SOHO - Small Office, Home Office/ Oficina pequeñas, Oficina en casa

SYN- Synchronization / Sincronización

TCP - *Transmission Control Protocol* / Protocolo de control de transmisión

TIA/EIA - Telecommunications Industry Association/ Electronic Industries Alliance/ Asociación de la industria de las telecomunicaciones// Alianza de Industrias Electrónicas

TKIP - Temporal Key Integrity Protocol/ Protocolo de integridad temporar del claves

UDP - *User Datagram Protocol* / Protocolo de datagrama de usuario

UR: Unidades *Rack*

USB - Universal Serial Bus / Bus universal en serie

UTP- Unshielded Twister Pair / Par trenzado no blindado

VoIP - Voice over IP/ Voz sobre protocolo de internet

WA- Wor*k Area /Area de trabajo*

WAN: Wide Area Network/ Red de Area Amplia

WPA- Wi-Fi Protected Access / Acceso protegido Wi-Fi

WPA2 - Wi-Fi Protected Access v2 / Acceso protegido Wi-Fi version 2

WPA3 - Wi-Fi Protected Access v3/ Acceso protegido Wi-Fi version 3

WEP - *Wired Equivalent Privacy*/ Privacidad equivalente por cable

WiFI - Wireless Fidelity / fidelidad sin cables o inalámbrica

WiMAX- Worldwide Interoperability for Microwave Access/ Interoperabilidad Mundial para Acceso por Microondas

WLAN - *Wireless Local Area Network/* Red de área local inalámbrica

WLAN - Wireless Personal Area Network / Red de área local inalámbrica

WPAN - Redes de área personal inalámbrica

WWAN - Wireless Local Area Network / Redes de área extensa inalámbrica

WWW - World Wide Web/ Red Informática Mundial