UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE TECNOLOGÍA
CARRERA DE ELECTRÓNICA Y TELECOMUNICACIONES

APLICACIÓN DE UN SISTEMA DE SEGURIDAD EN LA RED (Internet) UTILIZANDO EL TUNNEL GRE DE CISCO SOBRE IPV6 EN LA INSTITUCION FINANCIERA "PRENDAMAS"

Proyecto de Grado presentado para obtener el Grado de Licenciatura

POR: Jhamir Jesus Quispe Chavez

TUTOR: Lic. Julia Torrez Soria

La Paz – Bolivia

2022

Agradecimientos

Doy las gracias a Dios por haberme dado la vida y la inteligencia para poder desarrollar este proyecto. A mi tutora Licenciada Julia Torrez Soria por su apoyo, comprensión, confianza y sobre todo su contribución oportuna en la revisión del presente proyecto.

DEDICATORIA

Dedicado a mi madre Maritza Angela Chavez Choque quien siempre me apoyo incondicionalmente y me mostro el mejor camino que podría tomar mi vida.

Ella es la persona que me daba fuerza para no dejar a medio camino mi formación académica y me apoyaba en todo sentido, por eso le debo mucho. Y una mención a mi abuelita Nicolasa que se fue al cielo por culpa de la pandemia, se que desde el cielo esta feliz por este logro.

INDICE

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN DEL PROYECTO

El presente proyecto de grado trata de la implementación de un sistema de seguridad en la red internet cuyo objetivo principal es el de brindar seguridad en la transmisión de datos por medio de una red insegura como es el internet entre sucursales de la Institución Financiera Prendamas. En la actualidad la Institución Financiera Prendamas tiene una red privada WAN (Wide Área Network) “Red de Área Amplia” la cual es el medio por donde viaja su información entre sus diferentes sucursales de la ciudad de La Paz, esta red privada WAN representa un costo elevado para el tipo de información que se maneja en esta Institución Financiera “Prendamas” y al no tener otras opciones de sistemas de seguridad acorde al tipo de información que manejan están obligados a seguir utilizando esta red privada.

Lo que se realizara será la migración de IPv4 a IPv6 cuyo es requisito para la implementación de este sistema de seguridad en la red LAN(Local Área Network) “Red de Área Local” de la Institución Financiera Prendamas la cual permitirá que su información viaje a través de la red internet el cual es un conjunto descentralizado de redes de comunicaciones interconectadas, que utilizan la familia de protocolos TCP/IP, lo cual garantiza que las redes físicas heterogéneas que la componen constituyen una red lógica única de alcance mundial cuya finalidad es permitir el intercambio libre de información entre todos sus usuarios. Este sistema de seguridad que se implementará lleva el nombre de Tunnel Gre de Cisco, el cual permitirá la transmisión de datos en la red internet realizando la encriptación de los mismos extremo a extremo, este sistema de seguridad encapsula una amplia variedad de tipos de paquete de protocolo dentro de túneles IP, lo que crea un enlace punto a punto virtual a los routers Cisco en puntos remotos.

CAPITULO I

ANTECEDENTES DEL PROYECTO

1.1 Introducción

En el siguiente perfil de proyecto se observará la temática en el ámbito de la Seguridad en la Red (Internet), se podría denominar a Internet como una red insegura, internet es una colección mundial de redes interconectadas (abreviado: internet Works o internet) que colaboran para intercambiar información sobre la base de estándares comunes. A través de cables telefónicos, cables de fibra óptica, transmisiones inalámbricas y enlaces satelitales, los usuarios de internet pueden intercambiar información de diversas formas. Internet es un conglomerado de redes que no es propiedad de ninguna persona ni de ningún grupo.

En la actualidad cualquier institución que maneje información confidencial como por ejemplo podemos mencionar una entidad bancaria, empresas privadas o públicas, ministerios de estado, etc. Este tipo de información confidencial que manejan estas instituciones ya mencionadas no se les ocurre ni por un momento mandarla por internet por el tema de la inseguridad en la red ya que se ponen vulnerables a que su información sea intervenida.

Este tipo de información confidencial tiene un sistema de seguridad el cual es enviar su información en una Red Privada WAN la ventaja que tiene esta Red es el ser seguro, es controlado, pero su única desventaja que se podría mencionar es un alto costo. Al ser un alto costo algunas empresas, instituciones, universidades, unidades educativas que requieran seguridad en su información no podrían acceder a ese servicio de seguridad en una Red Privada (WAN).

El Sistema de Seguridad en la Red (internet) que se quiere aplicar con la tecnología de Tunnel Gre propietario de Cisco es de beneficio para estas instituciones, empresas, unidades educativas, etc.

Esta tecnología nos permitirá manejar información confidencial usando la red de internet en forma segura, es decir que la información viajara a través de internet (extremo a

extremo) sin ser interceptado por equipos intermedios, otras de las ventajas que podemos mencionar es que los costos bajaran considerablemente debido a que internet es un conglomerado de redes que no es propiedad de ninguna persona o agrupación. Esta tecnología denominada Tunnel Gre que se quiere aplicar como Sistema de Seguridad en la Red internet se realizara con la programación en los Routers de la Institución Financiera Prendamas, también se hará la respectiva migración de Ipv4 a Ipv6 a todos los equipos, toda la configuración se realizara en Ipv6 para aumentar la seguridad y brindar un buen servicio a un bajo costo.

1.2 PLANTEAMIENTO DE PROBLEMAS

1.2.1 DESCRIPCION DEL PROBLEMA

El problema que da origen por desarrollar el proyecto es la "Limitada capacidad Tecnológica de Seguridad en la Red (Internet) para la Institución Financiera Prendamas ubicada en la ciudad de La Paz" y se fundamenta en los siguientes elementos:

En la actualidad la Institución Financiera Prendamas, recibe un servicio de Seguridad en una Red Privada (WAN) es por esta Red donde envía su información, la cual implica un alto costo por el servicio que recibe.

La Institución Financiera Prendamas teniendo el conocimiento de las características que tiene la Red (Internet) como ser una red insegura y nada confiable, ni se imagina enviar su información por este medio (Internet).

Al estudiar el tipo de información que maneja la Institución Financiera Prendamas y hacer una comparación con el tipo de información que maneja por ejemplo una Entidad Bancaria. Haciendo esta comparación pudimos diferenciar un Nivel de Seguridad que requiere para su información cada institución el cual para una Entidad Bancaria necesita un Nivel de Seguridad muy alta por el tipo de información que maneja como ser: transacciones financieras, datos confidenciales del cliente, números de cuentas, contraseñas, cuentas de ahorro. Mientras que la Institución Financiera Prendamas

requiere un Nivel de Seguridad Medio por el tipo de información que maneja como ser: datos del cliente, cantidad de dinero que se prestó al cliente, características de la prenda (joya en oro) que se dejó como garantía, este tipo de información también requiere seguridad por ese motivo la Institución Financiera Prendamas en la actualidad maneja su información de forma confidencial en la Red Privada WAN.

La Institución Financiera Prendamas brinda sus servicios de préstamos prendarios diferenciándose de las alternativas del mercado especializándose en joyas de oro por el cual tiene otro nivel de información y no cumple las funciones que realiza por ejemplo una Entidad Bancaria que necesita otro nivel de seguridad.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Implementar la Tecnología (Tunnel Gre) que permita la Seguridad en la Red (Internet) para el manejo de la información en la Institución Financiera “Prendamas” ubicado en la ciudad de La Paz en la gestión 2021.

1.3.2 OBJETIVOS ESPECIFICOS

- Realizar un estudio al servicio que ofrece a la sociedad la Institución Financiera “Prendamas” para luego poder analizar qué tipo de información que maneja actualmente en su Red privada (WAN).
- Investigar el costo aproximado del servicio de la Red privada (WAN) que tiene actualmente como sistema de seguridad la Institución Financiera Prendamas y así poder identificar el nivel de información de confidencialidad (Alto, Medio, Bajo).
- Realizar la migración de Ipv4 a Ipv6 en las computadoras de cada agencia, también realizar la programación en los Routers para aplicar la seguridad en la Red (Internet) con la tecnología del Tunnel Gre.

- Analizar las ventajas que le ofrece este Servicio de Seguridad en la Red (Internet) denominado Tunnel Gre que le permitirá bajar sus costos comparados con los servicios que recibe actualmente en la Red Privada (WAN).
- Elaborar manual de funcionamiento y configuración del Tunnel Gre

1.4 JUSTIFICACION

1.4.1 JUSTIFICACION TECNOLOGICA

La tecnología en nuestra sociedad y contexto ha realizado varios cambios y aporte en nuestra sociedad es necesario tomar en cuenta que al aplicar este sistema de Seguridad en la Red (Internet) con la tecnología denominada Tunnel Gre que permitirá a la Institución Financiera Prendamas poder manejar su información confidencial de manera segura en la red internet.

1.4.2 JUSTIFICACION SOCIAL

La presente propuesta de proyecto es justificada como una alternativa de Seguridad en la Red (Internet), por el tipo de información que maneja la Institución Financiera Prendamas y por lo tanto el nivel de seguridad que requiere esta institución específicamente, se podrá brindar el servicio de seguridad en la Red (Internet) aplicando la tecnología Tunnel Gre de Cisco en la Institución Financiera Prendamas que nos permitirá manejar la información de esta institución de forma segura (extremo-extremo), al aplicar esta tecnología nos permitirá también poder bajar los costos de servicio de seguridad que recibe actualmente en la Red Privada WAN para el manejo de su información.

1.4.3 JUSTIFICACION ACADEMICA

El presente perfil de proyecto permite aplicar y poner en práctica conocimientos, competencias y habilidades adquiridas en la carrera de Electrónica y Telecomunicaciones de las materias de sistemas digitales I, sistemas digitales II en estas

materias pudimos aprender lo más importante del mundo de las Redes que es inmensa, entre lo más importante que podemos mencionar es la manipulación y configuración de los equipos como ser el Router, Switch, computadoras, etc.

1.4.4 JUSTIFICACION ECONOMICA

Aplicar la tecnología Tunnel Gre en la Institución Financiera Prendamas para la Seguridad en la Red (Internet), así la Institución podrá manejar su información de manera segura en la red, a comparación del servicio de seguridad que recibe actualmente en la Red Privada WAN, el precio de esta tecnología (Tunnel Gre) será por debajo del precio de la Red Privada WAN.

1.5. DELIMITACION DEL PROYECTO

1.5.1 TEMPORAL

La Tecnología (Tunnel Gre), es un Sistema de Seguridad en la Red (Internet), la función que desempeñara este sistema de seguridad es proteger la información que viajara a través de la red de internet para la Institución Financiera “Prendamas” en la gestión 2021, de esta manera se podrá obtener un trabajo final en un lapso de tiempo de 6 meses garantizando el buen funcionamiento de este sistema de seguridad.

1.5.2 ESPACIAL

Esta aplicación de la Tecnología (Tunnel Gre), es un Sistema de Seguridad en la Red (Internet), la cual permitirá manejar su información de forma segura en la red internet, este sistema de seguridad se aplicará en la Institución Financiera “Prendamas” en la Ciudad de La Paz.

1.5.3 TEMATICA

Los parámetros fundamentales para que este sistema de seguridad en la red de internet tenga un óptimo funcionamiento es la programación del Tunnel Gre en los Routers de cada Red LAN y la respectiva migración de IP (Internet Protocol) es decir de Ipv4 a Ipv6 en los diferentes equipos de la Red LAN en la Institución Financiera Prendamas,

con esta tecnología la información viajara de forma segura a través de internet sin ser intervenido por los equipos intermedios en esta red, viajara extremo a extremo.

CAPITULO II

MARCO METODOLOGICO

2.1 Definición de la investigación aplicada

La Investigación Aplicada tiene por objetivo resolver un determinado problema o planteamiento específico, enfocándose en la búsqueda y consolidación del conocimiento para su aplicación y, por ende, para el enriquecimiento del desarrollo cultural y científico. (ZRV Cordero, 2009)

Figura N°1
Diagrama en Bloques de la Investigación Aplicada

Fuente: http://www.duoc.cl/biblioteca/crai/definicion-y-proposito-de-la-investigacion-aplicada

2.2 Diseño de la Investigación

En este caso se quiere aplicar una tecnología que permita la seguridad en la red de internet. Por consiguiente, el tipo de ámbito al que se aplica es muy específico y bien delimitado, ya que no se trata de explicar una amplia variedad de situaciones, sino que más bien se intenta abordar un problema específico.

Esta investigación aplicada busca la generación de conocimiento con aplicación directa a los diferentes problemas, se basa fundamentalmente en los hallazgos tecnológicos de la investigación básica, ocupándose del proceso de enlace entre la teoría y el producto.

2.3 Actividad y Tarea

- Realizar la migración de IP (Internet Protocol) de Ipv4 a Ipv6 a los equipos de la Red LAN de la Institución Financiera Prendamas
- Escoger el enrutamiento adecuado para la programación en los routers
- Realizar la programación en los routers respectivos para generar el Tunnel Gre
- Realizar el respectivo funcionamiento de este sistema seguridad entre dos agencias diferentes de la misma Institución Financiera Prendamas
- Elaboración del manual de funcionamiento del sistema de seguridad (Tunnel Gre)

2.4 Métodos y Técnicas

De acuerdo al planteamiento del problema, se tomó en cuenta el tipo de estudio aplicativo; es decir, una investigación centrada en encontrar mecanismos o estrategias que permitan lograr un objetivo concreto, como conseguir un elemento o bien que pueda ser de utilidad.

Frecuentemente el propósito del investigador es describir situaciones y eventos, es decir cómo es y cómo se manifiesta determinado fenómeno. Los estudios aplicativos buscan la generación de conocimiento con aplicación directa a los diferentes problemas, se basa fundamentalmente en los hallazgos tecnológicos de la investigación básica, ocupándose del proceso de enlace entre la teoría y el producto, en este perfil de proyecto se aplicará una tecnología que es un sistema de seguridad en la red internet.

CAPITULO III

MARCO TEORICO

3.1 Introducción a las Redes

Las infraestructuras de red pueden variar dependiendo del tamaño del área, del número de usuarios conectados y del número y los diferentes tipos de servicios disponibles. Además del dispositivo final, hay otros componentes que hacen posible que se establezca el enlace entre los dispositivos de origen y destino. Dos de los componentes críticos en una red de cualquier tamaño son el router y el switch.

Todos los tipos de mensajes se tienen que convertir a bits, señales digitales codificadas en binario, antes de enviarse a sus destinos. Esto es así sin importar el formato del mensaje original. Generalmente, las redes utilizan diferentes tipos de medios para proporcionar conectividad. Ethernet es la tecnología de red más común en la actualidad. Las redes cableadas son ideales para transmitir gran cantidad de datos a altas velocidades. Las redes inalámbricas permiten el uso de dispositivos conectados a la red en cualquier lugar de una oficina o casa, incluso en el exterior. (Ariganello, 2020)

3.2 Arquitectura de Comunicaciones

Entre los requerimientos necesarios para un diseño de una red de datos están:

- Proporcionar conectividad general de manera robusta, equitativa y económica para una gran cantidad de computadores.
- Ser lo suficientemente flexible para evolucionar y ajustarse a los cambios tecnológicos y a los requerimientos de las nuevas aplicaciones que aparecen constantemente.

Para afrontar esta complejidad, los diseñadores de redes han creado unos modelos generales usualmente llamados arquitecturas de comunicaciones que ayudan en el diseño y la implementación de las redes.

Cuando un sistema se vuelve complejo, el diseñador del sistema introduce otro nivel de abstracción.

- La idea de una abstracción es definir un modelo unificador que capture los aspectos importantes del sistema y oculte los detalles de cómo fue implementado.

El reto es identificar las abstracciones que simultáneamente sean útiles en un amplio número de situaciones y, a la vez, puedan ser implementadas eficientemente.
En sistemas en red, la abstracción lleva al concepto del modelo de capas.

- Se comienza con servicios ofrecidos por la capa física y luego se adiciona una secuencia de capas, cada una de ellas ofreciendo un nivel de servicios más abstracto.

Un modelo de capas ofrece dos características interesantes:

- Descompone el problema de construir una red en partes más manejables (no es necesario construir un sistema monolítico que hace todo)
- Proporciona un diseño más modular (si se quiere colocar un nuevo servicio, sólo se debe modificar la funcionalidad de una capa)

(Ariganello, 2020)

3.2.1 Modelo OSI (Open System Interconnection)

El modelo de referencia OSI puede verse de dos formas:

a) **Como Estándar**:

Las redes experimentales se diseñaron para ser heterogéneas (no importaba la marca del computador). Las redes de los fabricantes de equipos tenían su propio conjunto de convenciones para interconectar sus equipos y lo llamaban su “arquitectura de red”.
La necesidad de interconectar equipos de diferentes fabricantes se hizo evidente, en 1977, la ISO (International Organization for Standarization) reconoció la necesidad de

crear estándares para las redes informáticas y creó el subcomité SC16 (Open Systems Interconnection).

La primera reunión de este subcomité se llevó a cabo en marzo de 1978. El modelo de referencia OSI fue desarrollado después de cerca de 18 meses de discusión.

El modelo OSI fue adoptado en 1979 por el comité técnico TC97 (procesamiento de datos), del cual dependía el subcomité SC16, OSI fue adoptado en 1984 como la norma ISO/IEC 7498. (Ariganello, 2020)

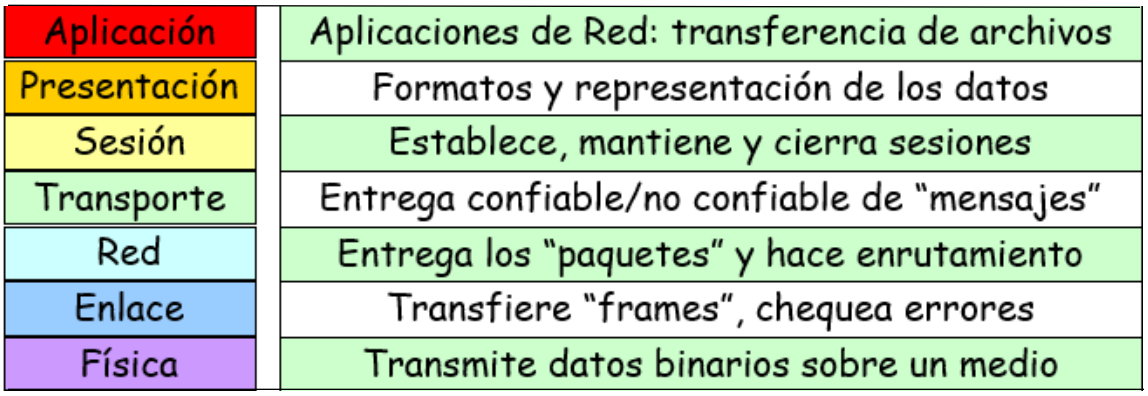
b) Como Modelo de Referencia

A continuación, se citan algunas características de OSI como modelo de referencia:

- OSI es un modelo de referencia que muestra cómo debe transmitirse un mensaje entre nodos en una red de datos.
- El modelo OSI tiene 7 niveles de funciones
- No todos los productos comerciales se adhieren al modelo OSI
- Sirve para enseñar redes y en discusiones técnicas (resolución de problemas).

En su conjunto, el modelo OSI se compone de siete capas bien definidas que son: Aplicación, Presentación, Sesión, Transporte, Red, Enlace de Datos y Física. En la siguiente figura se puede observar las 7 capas que componen la arquitectura del modelo OSI. (Ariganello, 2020)

Figura N°2
Arquitectura del Modelo OSI



Fuente: Diapositivas Curso Cisco

El modelo OSI (Open System Interconnection, no confundir con ISO) divide a la red en diferentes capas con el propósito de que cada desarrollador trabaje específicamente en su campo sin tener necesidad de depender de otras áreas. Un programador crea una aplicación determinada sin importarle cuáles serán los medios por los que se trasladarán los datos, inversamente un técnico de comunicaciones proveerá comunicación sin importarle qué datos transporta. (Ariganello, 2020)

Cada una de estas capas presta servicio a la capa inmediatamente superior, siendo la capa de aplicación la única que no lo hace ya que al ser la última capa su servicio está directamente relacionado con el usuario. Así mismo, cada una de estas siete capas del host origen se comunica directamente con su similar en el host de destino. Las cuatro capas inferiores también son denominadas capas de Medios (en algunos casos capas de Flujo de Datos), mientras que las tres capas superiores se llaman de Host o de Aplicación. (Ariganello, 2020)

Las principales características del modelo de referencia OSI pueden resumirse en los siguientes puntos:

- Proporciona una forma de entender cómo operan los dispositivos en una red.

- Es la referencia para crear e implementar estándares de red, dispositivos y esquemas de internet-working.
- Separa la compleja operación de una red en elementos más simples.
- Permite a los a los administradores de red centrarse en el diseño y desarrollo de funciones modulares ocupándose cada uno de su parte específica.
- Proporciona la posibilidad de definir interfaces estándar para compatibilidad "plug-and-play" e integración multifabricante.

(Ariganello, 2020)

Descripción de las 7 capas del modelo OSI.

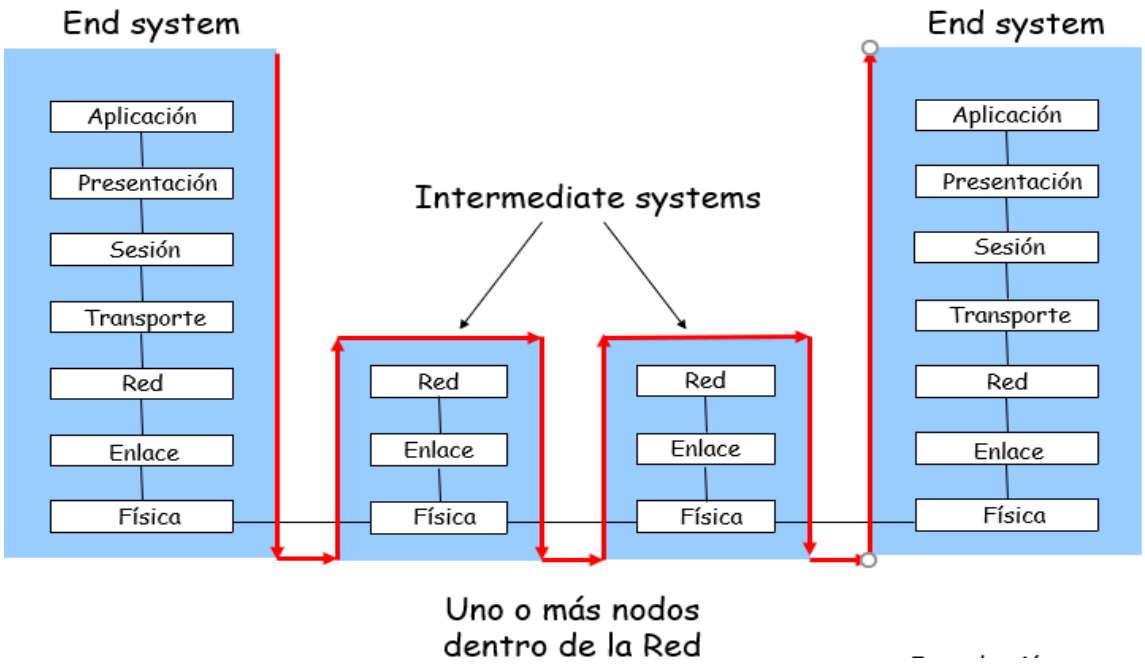
- **Capa de aplicación.** Es la única capa que no presta servicio a otra puesto que es la capa de nivel superior del modelo OSI directamente relacionada con el usuario. La aplicación a través del software dialoga con los protocolos respectivos para acceder al medio. Por ejemplo, se accede a un procesador de textos por el servicio de transferencia de archivos de esta capa. Algunos protocolos relacionados con esta capa son: HTTP, correo electrónico, telnet.
- **Capa de Presentación**. Los datos formateados se proveen de diversas funciones de conversión y codificación que se aplican a los datos provenientes de la capa de aplicación. Estas funciones aseguran que estos datos enviados desde la capa de aplicación de un sistema origen podrán ser leídos por la capa de aplicación de otro sistema destino. Un ejemplo de funciones de codificación sería el cifrado de datos una vez que éstos salen de una aplicación. Por ejemplo, los formatos de imágenes JPEG y GIF que se muestran en páginas web. Este formato asegura que todos los navegadores web puedan mostrar las imágenes, con independencia del sistema operativo utilizado. Algunos protocolos relacionados con esta capa son: JPEG, MIDI, MPEG, QUICKTIME. (Ariganello, 2020)
- **Capa de Sesión**. Es la responsable de establecer, administrar y concluir las sesiones de comunicaciones entre entidades de la capa de presentación. La comunicación en esta capa consiste en peticiones de servicios y respuestas entre aplicaciones ubicadas en diferentes dispositivos. Un ejemplo de este tipo de

coordinación podría ser el que tiene lugar entre un servidor y un cliente de base de datos.

- **Capa de Transporte.** Es la encargada de la comunicación confiable entre host, control de flujo y de la corrección de errores entre otras cosas. Los datos son divididos en segmentos identificados con un encabezado con un número de puerto que identifica la aplicación de origen. En esta capa funcionan protocolos como UDP y TCP, siendo este último uno de los más utilizados debido a su estabilidad y confiabilidad.
- **Capa de Red**. En esta capa se lleva a cabo el direccionamiento lógico que tiene carácter jerárquico, se selecciona la mejor ruta hacia el destino mediante el uso de tablas de enrutamiento a través del uso de protocolos de enrutamiento o por direccionamiento estático. Protocolos de capa de red pueden ser: IP, IPX, RIP, IGRP, Apple Talk.
- **Capa de enlace de datos**. Proporciona las comunicaciones entre puestos de trabajo en una primera capa lógica, transforma los voltios en tramas y las tramas en voltios. El direccionamiento físico y la determinación de si deben subir un mensaje a la pila de protocolo ocurren en esta capa. Está dividida en dos subcapas, la LLC (Logical Link Control) y la subcapa MAC (Media Access Control). Algunos protocolos de capa 2: Ethernet, 802.2, 802.3, HDLC, Frame-Relay.
- **Capa Física**. Se encarga de los medios, conectores, especificaciones eléctricas, lumínicas, radiofrecuencia y de la codificación. Los bits son transformados en pulsos eléctricos, en luz o en radiofrecuencia para ser enviados según sea el medio en que se propaguen. (Ariganello, 2020)

En la siguiente figura se observará la función del modelo OSI:

Figura N°3
Diagrama del Funcionamiento del modelo OSI



Fuente: Diapositivas Cursos Cisco

3.2.2 Modelo TCP/IP

La definición de TCP/IP es la identificación del grupo de protocolos de red que hacen posible la transferencia de datos en redes, entre equipos informáticos e internet. Las siglas TCP/IP hacen referencia a este grupo de protocolos:

- **TCP** es el Protocolo de Control de Transmisión que permite establecer una conexión y el intercambio de datos entre dos anfitriones. Este protocolo proporciona un transporte fiable de datos.
- **IP** o protocolo de internet, utiliza direcciones series de cuatro octetos con formato de punto decimal (como por ejemplo 75.4.160.25). Este protocolo lleva los datos a otras máquinas de la red.
- **TCP/IP** son los protocolos fundamentales de Internet (Aunque se utilizan para Intranets y Extranets)

El modelo TCP/IP permite un intercambio de datos fiable dentro de una red, definiendo los pasos a seguir desde que se envían los datos (en paquetes) hasta que son recibidos. Para lograrlo utiliza un sistema de capas con jerarquías (se construye una capa a continuación de la anterior) que se comunican únicamente con su capa superior (a la que envía resultados) y su capa inferior (a la que solicita servicios). (Ariganello, 2020)

3.2.2.1 Capas del Modelo TCP/IP

Dentro del modelo TCP/IP existen cuatro niveles o capas que hay que tener en cuenta.

Nivel de enlace o acceso a la red: Es la primera capa del modelo y ofrece la posibilidad de acceso físico a la red (que bien puede ser en anillo, ethernet, etc.), especificando el modo en que los datos deben enrutarse independientemente del tipo de red utilizado.

Nivel de red o Internet: Proporciona el paquete de datos o datagramas y administra las direcciones IP. (Los datagramas son paquetes de datos que constituyen el mínimo de información en una red). Esta capa es considerada la más importante y engloba protocolos como IP, ARP, ICMP, IGMP y RARP.

Nivel de Transporte: Permiten conocer el estado de la transmisión, así como los datos de enrutamiento y utilizan los puertos para asociar un tipo de aplicación con un tipo de dato.

Nivel de Aplicación: Es la parte superior del protocolo TCP/IP y suministra las aplicaciones de red tipo Telnet, FTP o SMTP, que se comunican con las capas anteriores (con protocolos TCP o UDP). Las capas del modelo TCP/IP coinciden con algunas capas del modelo teórico OSI, aunque tienen tareas mucha más diversas.
La importancia del protocolo TCP/IP es muy elevada ya que permite que los datos enviados lleguen a su destino sin errores y bajo la misma forma en la que fueron enviados.
(Ariganello, 2020)

3.2.2.2 Ventajas del Modelo TCP/IP

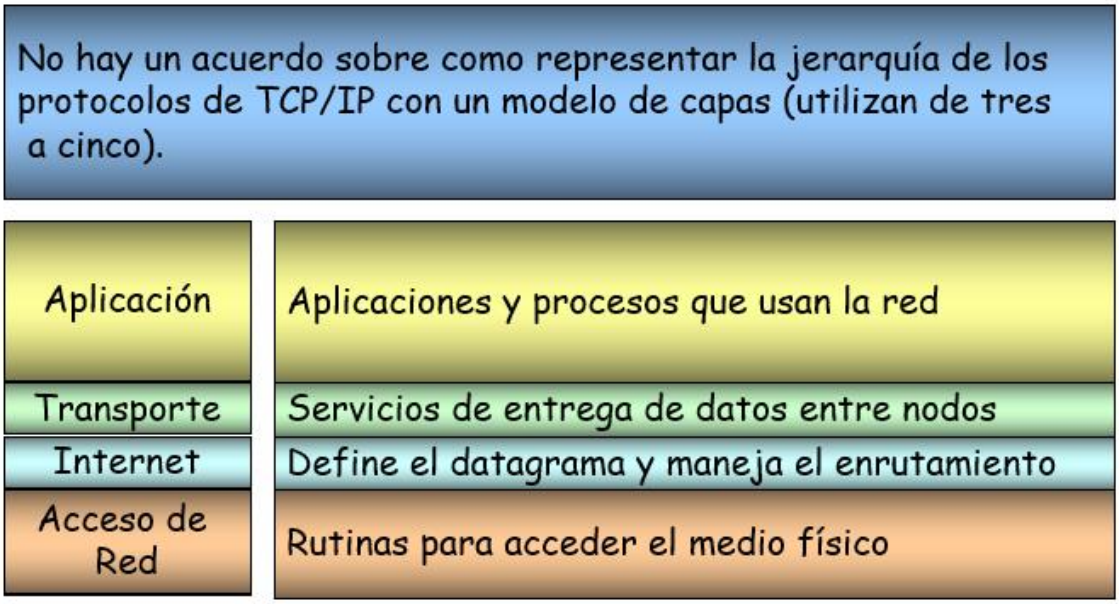
- TCP/IP ofrece ventajas significativas respecto a otros protocolos de red. Una de esas ventajas es que es capaz de trabajar sobre una extensa gama de hardware y soporta muchos sistemas operativos (es multiplataforma). Internet está repleto de pequeñas redes con sus propios protocolos por lo que el uso de TCP/IP se ha estandarizado y es posible utilizarlo como protocolo de comunicación entre redes privadas intranet y extranet, facilitando una red más homogénea.
- TCP/IP es adecuado tanto para grandes y medianas redes como para redes empresariales o domésticas.
- TCP/IP está diseñado para enrutar y además presenta gran compatibilidad con las herramientas estándar para analizar y monitorizar el funcionamiento de una red.
- Es el protocolo estándar que se utiliza a nivel mundial para conectarse a internet y a los servidores web.

3.2.2.3 Desventajas del Modelo TCP/IP

- No distingue bien entre interfaces, protocolos y servicios lo cual afecta al desarrollo de nuevas tecnologías basadas en TCP/IP-
- En redes con bajo volumen de tráfico puede llegar a ser más lento (en redes con mayor volumen de tráfico, que necesiten gran cantidad de enrutamiento, puede ser mucho más rápido).
- Cuando se utiliza en servidores de ficheros o servidores de impresión no ofrecen un gran rendimiento.

(OpenWebinars, 2020)

Figura N°4
Arquitectura de TCP/IP



Fuente: Diapositivas Curso CCNA
https://openwebinars.net/blog/que-es-tcpip/

Mientras los datos de la aplicación bajan al stack del protocolo y se transmiten por los medios de la red, varios protocolos le agregan información en cada nivel. Esto comúnmente se conoce como proceso de encapsulación.

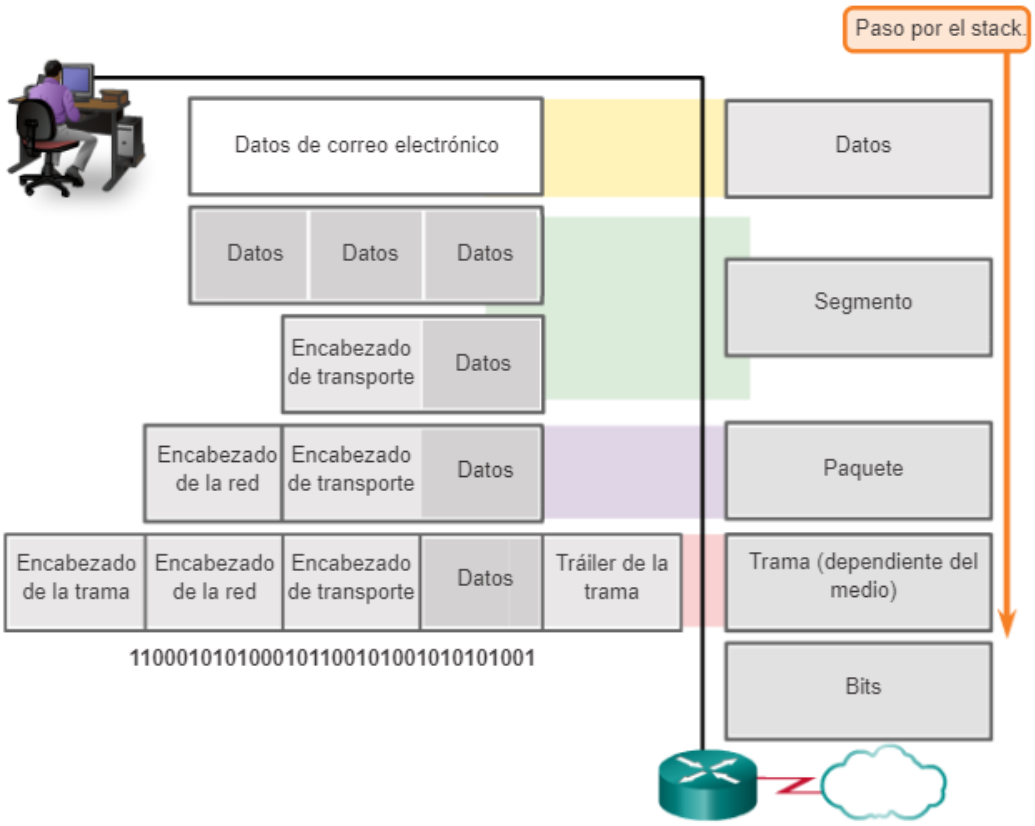
La forma que adopta una porción de datos en cualquier capa se denomina “unidad de datos del protocolo (PDU)”. Durante la encapsulación, cada capa encapsula las PDU que recibe de la capa inferior de acuerdo con el protocolo que se utiliza. En cada etapa del proceso, una PDU tiene un nombre distinto para reflejar sus nuevas funciones. Aunque no existe una convención universal de nomenclatura para las PDU, estas se denominan de acuerdo con los protocolos de la suite TCP/IP, como se muestra en la figura 5:

- **Datos:** Término general para la PDU que se utiliza en la capa de aplicación.
- **Segmento:** PDU de la capa de transporte.
- **Paquete:** PDU de la capa de red
- **Trama:** PDU de la capa de enlace de datos

- **Bits:** PDU de la capa física que se utiliza cuando se transmiten datos físicamente por el medio

(Scribd, 2020)

Figura N°5
Encapsulación de Datos



Fuente: PDF Curso CCNA
http://itroque.edu.mx/cisco/cisco1/course/module3/3.3.1.2/3.3.1.2.html

3.3 Router

3.3.1 Definición

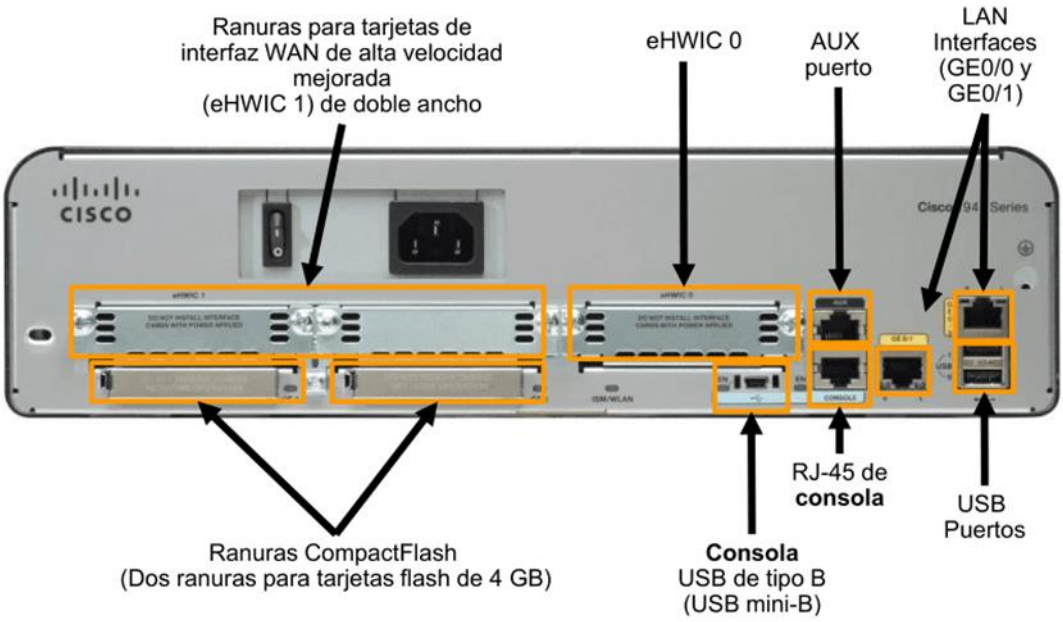
Un rúter, enrutador, (del inglés router) o encaminador, es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red.

En las siguientes figuras podremos ver al Router Real y al Router de aprendizaje que habitualmente se lo usa en simuladores de red.

Figura N°6
Router Real - Parte Frontal

Fuente: PDF Curso CCNA
https://www.cisco.com/c/es_mx/support/routers/1803-integrated-services-router-isr/model.html

Figura N°7
Router Real - Parte Trasera



Fuente: PDF Curso CCNA
https://www.cisco.com/c/es_mx/support/routers/1803-integrated-services-router-isr/model.html

Figura N°8
Router en Simulación para el aprendizaje

Fuente: PDF Curso CCNA
https://www.cisco.com/c/es_mx/support/routers/1803-integrated-services-router-isr/model.html

3.3.2 Funcionamiento

Los routers guían y dirigen los datos de red mediante paquetes que contienen varios tipos de datos, como archivos, comunicaciones y transmisiones simples como interacciones web.

Los paquetes de datos tienen varias capas o secciones; una de ellas transporta la información de identificación, como emisor, tipo de datos, tamaño y, aún más importante, la dirección IP (protocolo de Internet) de destino. El *router* lee esta capa, prioriza los datos y elige la mejor ruta para cada transmisión

3.3.3 Arquitectura

En un enrutador se puede identificar cuatro componentes:

Puertos de Entrada. -Realiza las funciones de la capa física consistentes en la terminación de un enlace físico de entrada a un encaminador; realiza las funciones de la capa de enlace de datos necesarias para interoperar con las funciones de la capa de enlace de datos en el lado remoto del enlace de entrada; realiza también una función de búsqueda y reenvío de modo que un paquete reenviado dentro del entramado de conmutación del encaminador emerge en el puerto de salida apropiado.

Entramado de Conmutación. - Conecta los puertos de entrada del enrutador a sus puertos de salida.

Puertos de Salida. - Almacena los paquetes que le han sido reenviados a través del entramado de conmutación y los transmite al enlace de salida. Realiza entonces la función inversa de la capa física y de la capa de enlace que el puerto de entrada.

Procesador de Encaminamiento. - Ejecuta los protocolos de encaminamiento, mantiene la información de encaminamiento y las tablas de reenvío y realiza funciones de gestión de red dentro del enrutador.

(Textos Cientificos, 2006)

3.3.4 Enrutamiento

3.3.4.1 Definición

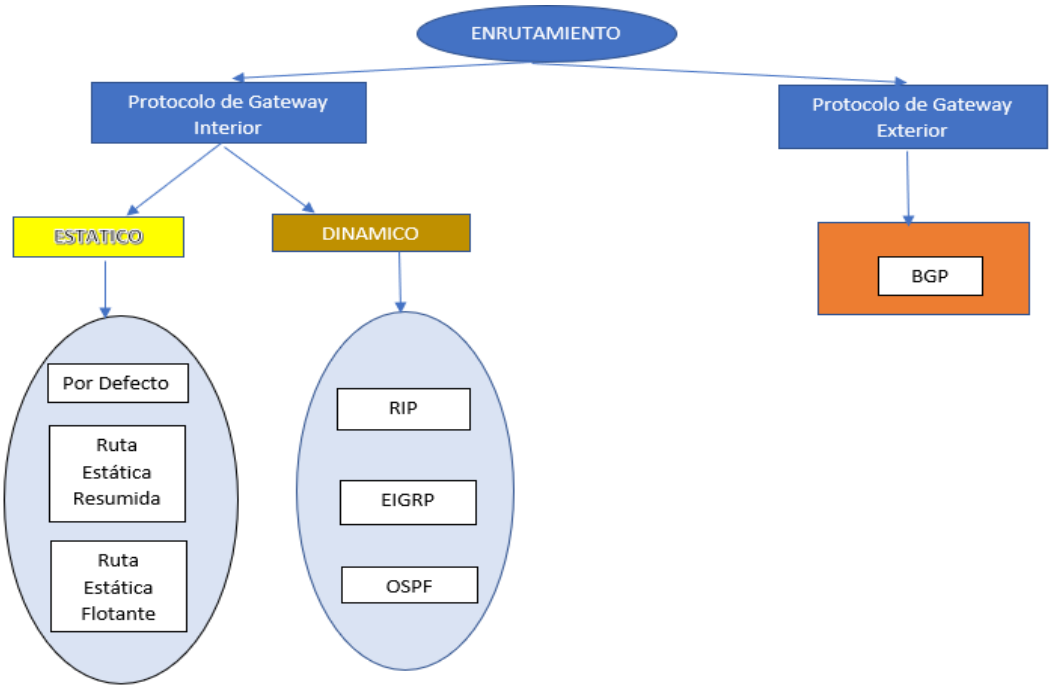
El enrutamiento o ruteo es la función de buscar un camino entre todos los posibles en una red de paquetes cuyas topologías poseen una gran conectividad

3.3.4.2 Tipos de Enrutamiento

El Protocolo de Información de Encaminamiento, *Routing Information* Protocol, es un protocolo de puerta de enlace interna o interior utilizado por los routers o encaminadores para intercambiar información acerca de redes del Internet Protocol a las que se encuentran conectados.

(Ariganello, 2020)

Figura N°9
Tipos de Enrutamiento



Fuente: Elaboración Propia

Un sistema autónomo (AS) es un conjunto de *routers* bajo una administración común, como una empresa o una organización. Los AS también se conocen como "dominios de routing". Los ejemplos típicos de AS son la red interna de una empresa y la red de un ISP (Proveedor de Servicio de Internet).

Debido a que Internet se basa en el concepto de AS, se requieren dos tipos de protocolos de r*outing*:

- **Protocolo de gateway interior (IGP):** Se utiliza para el routing dentro de un AS. También se lo denomina "routing interno de AS". Las empresas, las organizaciones e incluso los proveedores de servicios utilizan un IGP en sus redes internas. Los IGP incluyen RIP, EIGRP, OSPF.
- **Protocolo de gateway exterior (EGP):** Se utiliza para el routing entre AS. Los proveedores de servicios y las empresas grandes pueden interconectarse

mediante un EGP. El protocolo de gateway fronterizo (BGP) es el único EGP viable actualmente y es el protocolo de routing oficial utilizado por Internet.

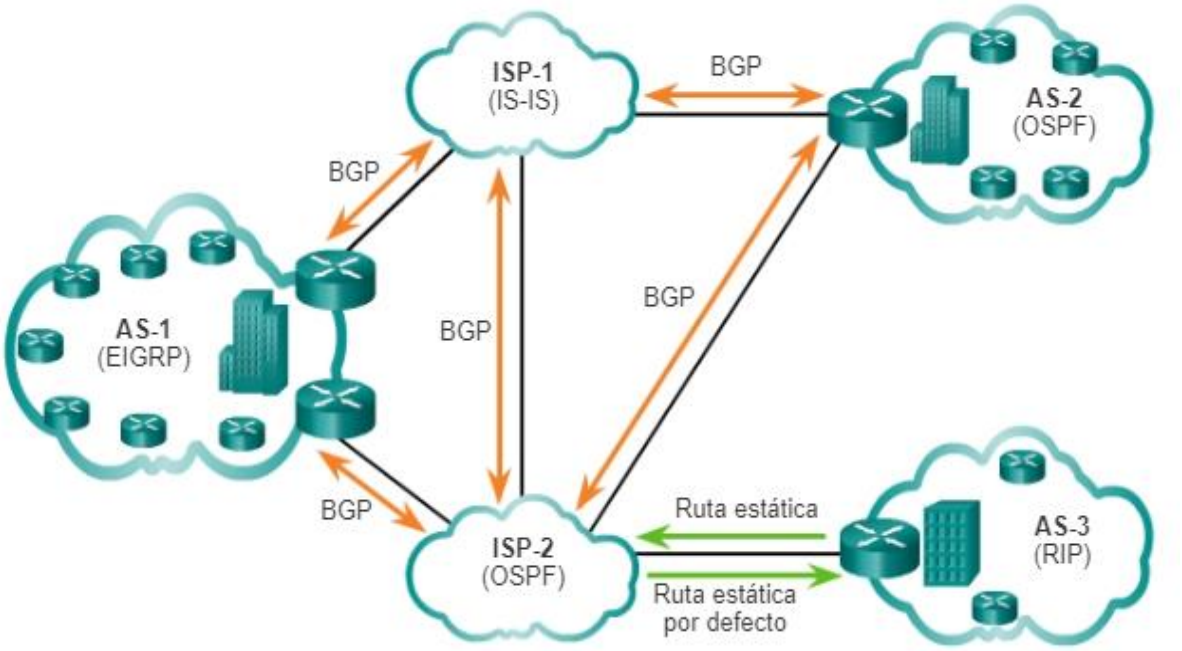
Dado que BGP es el único EGP disponible, no se suele utilizar el término EGP. En cambio, la mayoría de los administradores de red simplemente hacen referencia a BGP.

En el ejemplo de la figura 9, se proporcionan situaciones simples en las que se destaca la implementación de IGP, de BGP y del routing estático:

- **ISP-1:** es un AS que utiliza IS-IS como IGP. Se interconecta con otros sistemas autónomos y proveedores de servicios que utilizan BGP para controlar explícitamente el modo en que se enruta el tráfico.
- **ISP-2:** es un AS que utiliza OSPF como IGP. Se interconecta con otros sistemas autónomos y proveedores de servicios que utilizan BGP para controlar explícitamente el modo en que se enruta el tráfico.
- **AS-1:** se trata de una organización grande que utiliza EIGRP como IGP. Dado que es un entorno de host múltiples (es decir, se conecta a dos proveedores de servicios distintos), utiliza BGP para controlar explícitamente la forma en que el tráfico ingresa al AS y sale de él.
- **AS-2:** se trata de una organización mediana y utiliza OSPF como IGP. También es un entorno de host múltiples, por lo que utiliza BGP para controlar explícitamente la forma en que el tráfico ingresa al AS y sale de él.
- **AS-3:** se trata de una organización pequeña con routers más antiguos dentro del AS y utiliza RIP como IGP. Dado que tiene conexión simple (es decir, conecta a solo un proveedor de servicios), no se requiere BGP. En cambio, se implementa routing estático entre el AS y el proveedor de servicios.

(Institut SA Palomera, 2021)

Figura N°10
Comparación entre Protocolos de Routing IGP y EGP



Fuente: Diapositivas Curso CCNA Cisco
www.itesa.edu.mx/netacad/switching/course/module7/7.1.4.2/7.1.4.2.html

a) Enrutamiento Estático

El enrutamiento estático es la alternativa a los protocolos de enrutamiento, donde se especifican las redes de destino, por donde enviar la información y la distancia administrativa. Una ruta estática no cambia hasta que el administrador la vuelve a configurar en forma manual. (Institut SA Palomera, 2021)

En la siguiente tabla se muestran algunas ventajas y desventajas que presenta el enrutamiento estático.

TABLA N°1
Ventajas y Desventajas del Enrutamiento Estático

Ventajas	Desventajas
Las rutas estáticas no se anuncian a través de la red, lo cual aumenta la seguridad.	La configuración es propensa a errores, especialmente en redes extensas.
Las rutas estáticas consumen menos ancho de banda que los protocolos de *routing* dinámico. No se utiliza ningún ciclo de CPU para calcular y comunicar las rutas.	Se requiere la intervención del administrador para mantener la información cambiante de la ruta.
La ruta que usa una ruta estática para enviar datos es conocida.	No se adapta bien a las redes en crecimiento; el mantenimiento se torna cada vez más complicado.

Fuente: Elaboración Propia

Existen 3 tipos de protocolos de enrutamiento estático los cuales son:

a-1) Por Defecto

Una ruta por defecto o predeterminada, es una ruta que coincide con todos los paquetes y es utilizada por el router si un paquete no coincide con ninguna otra ruta más específica en la tabla de routing. Además, puede ser aprendida de forma dinámica o configurada de manera estática. Una ruta estática predeterminada es simplemente una ruta estática con 0.0.0.0/0 como dirección IPv4 de destino. Al configurar una ruta estática predeterminada, se crea un *gateway* de último recurso.

Las rutas estáticas predeterminadas se utilizan en los siguientes casos:

- Cuando ninguna otra ruta de la tabla de *routing* coincide con la dirección IP destino del paquete. En otras palabras, cuando no existe una coincidencia más específica. Se utilizan comúnmente cuando se conecta un router periférico de una compañía a la red ISP.
- Cuando un router tiene otro router único al que está conectado. En esta situación, se conoce al router como router de rutas internas.

(CCNA desde Cero, 2021)

a-2) Ruta Estática Resumida

Para reducir el número de entradas en la tabla de routing, se pueden resumir varias rutas estáticas en una única ruta estática si se presentan las siguientes condiciones:

- Las redes de destino son contiguas y se pueden resumir en una única dirección de red.
- Todas las rutas estáticas utilizan la misma interfaz de salida o la dirección IP del siguiente salto.

(CCNA desde Cero, 2021)

a-3) Ruta Estática Flotante

Las rutas estáticas flotantes son rutas estáticas que se utilizan para proporcionar una ruta de respaldo a una ruta estática o dinámica principal, en el caso de una falla del enlace. La ruta estática flotante se utiliza únicamente cuando la ruta principal no está disponible. Para lograrlo, la ruta estática flotante se configura con una distancia administrativa mayor que la ruta principal. La distancia administrativa representa la confiabilidad de una ruta. Si existen varias rutas al destino, el router elegirá la que tenga una menor distancia administrativa. (CCNA desde Cero, 2021)

b) Enrutamiento Dinámico

Los protocolos de enrutamiento dinámico ayudan al administrador de red a administrar el proceso riguroso y lento de configuración y mantenimiento de rutas estáticas. Los protocolos de enrutamiento dinámico se implementan en cualquier tipo de red que consta de más de unos pocos routers. Los protocolos de enrutamiento dinámico son escalables y determinan automáticamente las mejores rutas si se produce un cambio en la topología.

Los protocolos de enrutamiento dinámico se utilizan comúnmente en los siguientes escenarios:

- En redes que consisten en más de unos pocos routers

- Cuando un cambio en la topología de red requiere que la red determine automáticamente otra ruta
- Escalabilidad a medida que la red crece, el protocolo de enrutamiento dinámico aprende automáticamente sobre cualquier red nueva.

(CCNA desde Cero, 2021)

En la tabla de la ilustración, se destacan las ventajas y las desventajas del *routing* dinámico:

TABLA N°2

Ventajas y Desventajas del Enrutamiento Dinámico

Ventajas	Desventajas
Es adecuado para topologías donde se requieren varios routers.	La implementación puede ser más compleja.
Por lo general es independiente del tamaño de la red.	Menos seguro, se requieren opciones de configuración adicionales para proporcionarle protección.
Si es posible, adapta automáticamente la topología para volver a enrutar el tráfico en la red.	La ruta depende de la topología actual
	Requiere CPU, RAM y ancho de banda de enlaces adicionales.

Fuente: Elaboración Propia

A continuación, veremos los protocolos de enrutamiento dinámico más importantes:

b-1) Routing Information Protocol (RIP)

Es un protocolo de enrutamiento interior vector distancia, basado en los RFC 1388, 1723 y 2453. Su principal limitación está impuesta por la cantidad máxima de saltos que soporta que es 15.

"Vector distancia" significa que las rutas se publican como vectores de distancia y dirección. La distancia se define en términos de una métrica como el conteo de saltos y la dirección es simplemente el router del siguiente salto o la interfaz de salida. Los protocolos vector distancia generalmente usan el algoritmo Bellman-Ford para la determinación del mejor camino.

Algunos protocolos vector distancia envían en forma periódica tablas de enrutamiento completas a todos los vecinos conectados. En las redes extensas, estas actualizaciones de enrutamiento pueden llegar a ser enormes y provocar un tráfico importante en los enlaces.

(Redes 2, 2016)

Algunas de sus características son:

- La distancia administrativa para RIPv1 y RIPv2 es 120.
- RIPv2 envía actualizaciones de enrutamiento a través de la dirección de multicast 224.0.0.9.
- En los routers Cisco, la versión 2 no se activa por defecto. Es necesario utilizar el comando versión 2 en el modo de configuración de RIP.
- RIPv2 sumariza actualizaciones de enrutamiento automáticamente.
- Su métrica es la cuenta de saltos.

b-2) Enhanced Interior Gateway Routing Protocol (EIGRP)

El protocolo avanzado de enrutamiento interior vector distancia desarrollado por Cisco. El EIGRP (Enhanced Interior Gateway Routing Protocol o protocolo de enrutamiento de gateway interior mejorado) es un protocolo propietario de Cisco de vector distancia, al igual que otros protocolos más simples, como RIP, pero con características avanzadas, propias de los protocolos de estado de enlace.

Al igual que otros protocolos de enrutamiento, EIGRP envía actualizaciones de enrutamiento por los interfaces del router en el que está configurado. Para ello, por medio de mensajes multicast, intentará establecer relaciones de adyacencia, es decir, enviará paquetes de saludo por sus interfaces que, cuando son respondidos, generarán con ese router vecino una relación de adyacencia y ambos comenzarán a intercambiar información de enrutamiento.

(TechClub Tajamar, 2019)

Algunas de sus características son:

- La distancia administrativa de EIGRP es 90

- Algoritmo de actualización difusa
- Establecimiento de adyacencias de vecinos
- Protocolo de transporte confiable
- Actualizaciones parciales y limitadas
- Balanceo de carga de mismo costo o con distinto costo.

b-3) Open Shortest Path First (OSPF)

Es un protocolo de enrutamiento interior de link-state, es un protocolo de direccionamiento de tipo enlace-estado, desarrollado para las redes IP y basado en el algoritmo de primera vía más corta (SPF). OSPF es un protocolo de pasarela interior (IGP).

En una red OSPF, los direccionadores o sistemas de la misma área mantienen una base de datos de enlace-estado idéntica que describe la topología del área. Cada direccionador o sistema del área genera su propia base de datos de enlace-estado a partir de los anuncios de enlace-estado (LSA) que recibe de los demás direccionadores o sistemas de la misma área y de los LSA que él mismo genera. El LSA es un paquete que contiene información sobre los vecinos y los costes de cada vía. Basándose en la base de datos de enlace-estado, cada direccionador o sistema calcula un árbol de extensión de vía más corta, siendo él mismo la raíz, utilizando el algoritmo SPF.

(IBM, 2015)

Las ventajas principales de OSPF son las siguientes:

- En comparación con los protocolos de direccionamiento de distancia-vector como el protocolo de información de direccionamiento (RIP), OSPF es más adecuado para servir entre redes heterogéneas de gran tamaño. OSPF puede recalcular las rutas en muy poco tiempo cuando cambia la topología de la red.
- Con OSPF, puede dividir un sistema autónomo (AS) en áreas y mantenerlas separadas para disminuir el tráfico de direccionamiento de OSPF y el tamaño de la base de datos de enlace-estado de cada área.

- OSPF proporciona un direccionamiento multivía de coste equivalente. Se pueden añadir rutas duplicadas a la pila TCP utilizando saltos siguientes distintos.

Los direccionadores o sistemas de una red OSPF, después de haberse asegurado de que sus interfaces son funcionales, envían en primer lugar paquetes Hello, utilizando el protocolo Hello por sus interfaces OSPF, para descubrir vecinos. Vecinos son los direccionadores o sistemas que tienen interfaces con la red común. Después, los direccionadores o sistemas vecinos intercambian sus bases de datos de enlace-estado para establecer adyacencias. (IBM, 2013)

OSPF es un protocolo de enrutamiento de estado de enlace que utiliza el concepto de áreas. Un administrador de red puede dividir el dominio de enrutamiento en áreas distintas que ayudan a controlar el tráfico de actualización de enrutamiento. Un enlace es una interfaz en un router. Un enlace es también un segmento de red que conecta dos routers, o una red auxiliar, como una LAN Ethernet que está conectada a un único router. La información sobre el estado de un enlace se conoce como estado de enlace. Toda la información del estado del enlace incluye el prefijo de red, la longitud del prefijo y el costo.

Este módulo cubre implementaciones y configuraciones básicas de OSPF de área única.

b-3.1) Componentes de OSPF

Todos los protocolos de enrutamiento comparten componentes similares. Todos usan mensajes de protocolo de enrutamiento para intercambiar información de la ruta. Los mensajes contribuyen a armar estructuras de datos, que luego se procesan con un algoritmo de enrutamiento.

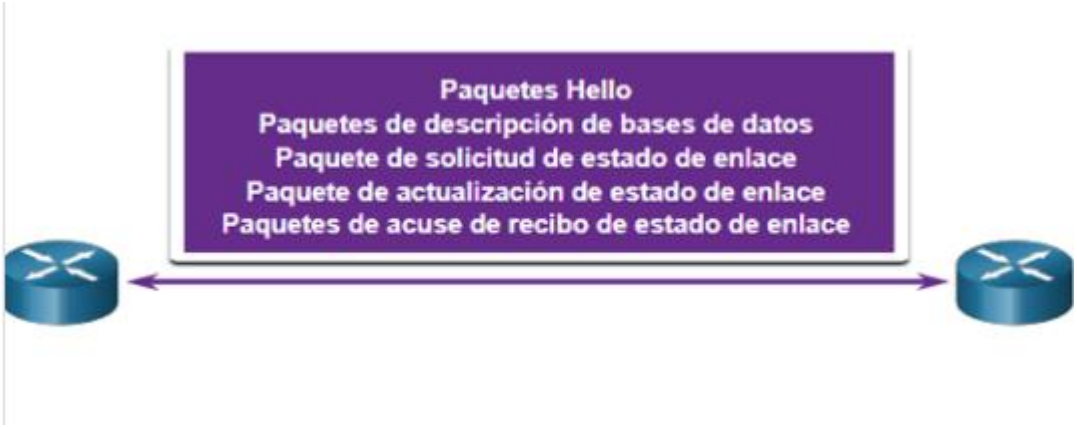
Los routers que ejecutan OSPF intercambian mensajes para transmitir información de enrutamiento por medio de cinco tipos de paquetes. Estos paquetes, que pueden verse en la figura, son los siguientes:

- Paquete Hello
- Paquete de descripción de la base de datos
- Paquete de solicitud de estado de enlace
- Paquete de actualización de estado de enlace

- Paquete de acuse de recibo de estado de enlace

Estos paquetes se usan para descubrir routers vecinos y también para intercambiar información de enrutamiento, a fin de mantener información precisa acerca de la red. (CCNA desde Cero, 2021)

Figura N°11
Mensajes de Protocolos de Enrutamiento



Fuente: Diapositivas Curso CCNA CISCO
https://ccnadesdecero.es/caracteristicas-funciones-ospf/

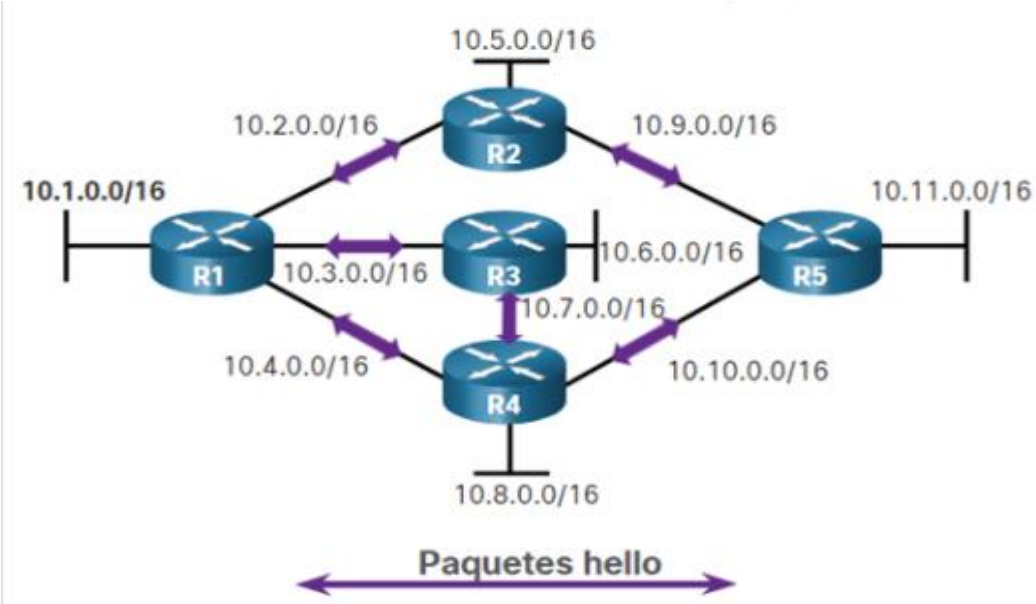
b-3.2) Funcionamiento de Estado de Enlace

A fin de mantener la información de enrutamiento, los routers OSPF realizan el siguiente proceso genérico de routing de estado de enlace para alcanzar un estado de convergencia: La figura 8 muestra una topología de cinco routers. Cada enlace entre routers está etiquetado con un valor de costo. En OSPF, el costo se utiliza para determinar la mejor ruta al destino. Los siguientes son los pasos de enrutamiento de estado de enlace que completa un router:

1. Establecer adyacencias de vecinos
2. Intercambiar anuncios de estado de enlace
3. Crear la base de datos de estado de enlace
4. Ejecutar el algoritmo SPF
5. Elegir la mejor ruta

Los routers con OSPF habilitado, deben reconocerse entre sí en la red antes de que puedan compartir información. Los routers con OSPF habilitado envían paquetes *hello* por todas las interfaces con OSPF habilitado, para determinar si hay vecinos presentes en esos enlaces. Si se detecta un vecino, el router con OSPF habilitado intenta establecer una adyacencia de vecino con ese vecino.
(CCNA desde Cero, 2021)

Figura N°12
Los Routers establecen adyacencia entre vecinos



Fuente: PDF Curso CCNA - CISCO
https://ccnadesdecero.es/caracteristicas-funciones-ospf/

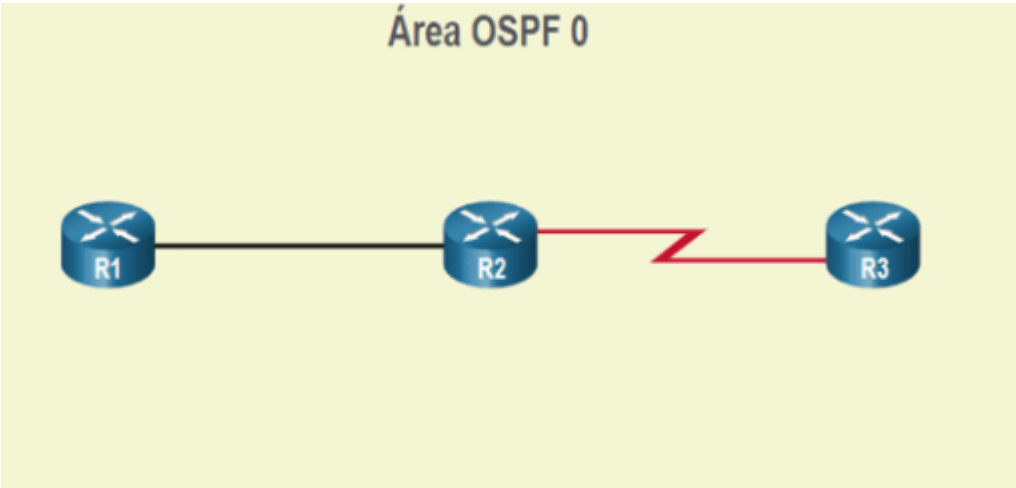
b-3.3) OSPF de Área Única y OSPF Multiarea

Para que OSPF sea más eficaz y escalable, este protocolo admite el enrutamiento jerárquico mediante áreas. Un área OSPF es un grupo de routers que comparten la misma información de estado de enlace en sus LSDB. OSPF se puede implementar de una de estas dos maneras:

- OSPF de área única: todos los routers están en un área. La mejor práctica es usar el área 0.

- OSPF Multiarea: OSPF se implementa mediante varias áreas, de manera jerárquica. Todas las áreas deben conectarse al área troncal (área 0). Los routers que interconectan las áreas se denominan “routers fronterizos de área” (ABR, Área Border Routers)

Figura N°13
OSPF de Área Única



Fuente: PDF Curso CCNA
https://ccnadesdecero.es/caracteristicas-funciones-ospf/

Con OSPF Multiarea, OSPF puede dividir un dominio de enrutamiento grande en áreas más pequeñas a fin de admitir el enrutamiento jerárquico. El enrutamiento todavía ocurre entre las áreas (enrutamiento entre áreas), mientras que muchas de las operaciones de enrutamiento que son intensivas para el procesador, como el recálculo de la base de datos, se mantienen dentro de un área.

Por ejemplo, cada vez que un router recibe información nueva acerca de un cambio de topología dentro del área (como el agregado, la eliminación o la modificación de un enlace), el router debe volver a ejecutar el algoritmo SPF, crear un nuevo árbol SPF y

actualizar la tabla de routing. El algoritmo SPF representa una gran exigencia para el CPU y el tiempo que le toma realizar los cálculos depende del tamaño del área.

Si hubiera demasiados routers en un área, la LSDB sería muy grande y se incrementaría la carga en la CPU. Por lo tanto, la disposición de los routers en distintas áreas divide de manera eficaz una base de datos potencialmente grande en bases de datos más pequeñas y más fáciles de administrar.

Las opciones de diseño de topología jerárquica con OSPF Multiarea pueden ofrecer estas ventajas:

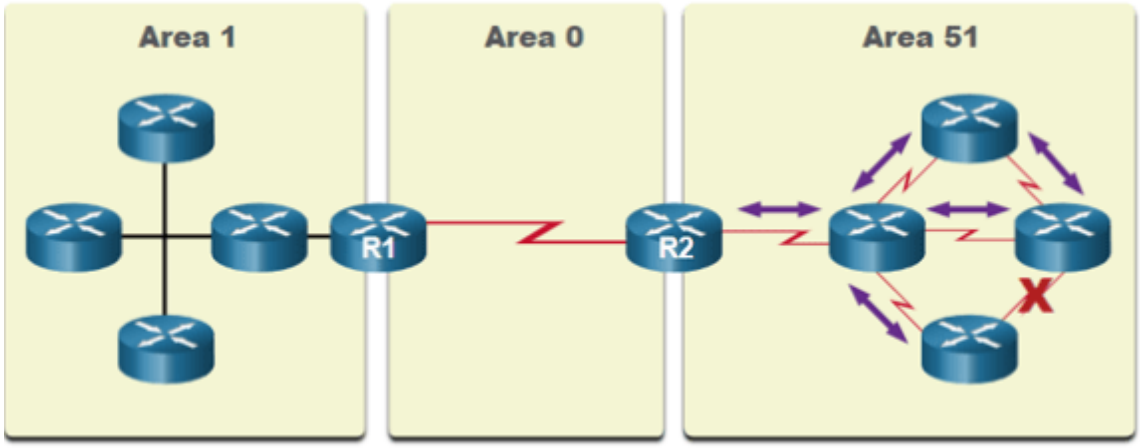
- **Tablas de enrutamiento más pequeñas**: Las tablas son más pequeñas porque hay menos entradas en las tablas de enrutamiento. Esto se debe a que las direcciones de red pueden ser resumidas (sumarizadas) entre áreas. La sumarización de ruta no está habilitada de manera predeterminada.
- **Sobrecarga de actualizaciones de estado de enlace reducida**: El diseño de OSPF Multiarea con áreas más pequeñas minimiza los requisitos de procesamiento y memoria.
- **Menor frecuencia de cálculos de SPF**: Multiarea OSPF localiza el impacto de un cambio de topología dentro de un área. Por ejemplo, minimiza el impacto de las actualizaciones de enrutamiento, debido a que la saturación con LSA se detiene en el límite del área.

Por ejemplo, en la figura 14, R2 es un ABR para el área 51. Un cambio de topología en el área 51 provocaría que todos los routers de área 51 re-ejecutar el algoritmo SPF, crear un nuevo árbol SPF y actualizar sus tablas de enrutamiento IP.

El ABR - R2, enviaría un LSA a los routers del área 0, que eventualmente se inundaría a todos los routers del dominio de enrutamiento OSPF. Este tipo de LSA no hace que los routers en otras áreas re-ejecuten el algoritmo SPF. Sólo tienen que actualizar su LSDB y tabla de enrutamiento.

(CCNA desde Cero, 2021)

Figura N°14
OSPF Multiarea



Fuente: PDF Curso CCNA CISCO
https://ccnadesdecero.es/caracteristicas-funciones-ospf/

- La falla del enlace afecta solo el área local (área 51).
- El ABR (R2) aísla la inundación de un LSA específico al área 51.
- Los routers en las áreas 0 y 1 no necesitan ejecutar el algoritmo SPF.

b-3.4) OSPFv3

OSPFv3 es el equivalente a OSPFv2 para intercambiar prefijos IPv6. En IPv6, la dirección de red se denomina “prefijo” y la máscara de subred se denomina “longitud de prefijo “.

De manera similar a su homólogo para IPv4, OSPFv3 intercambia información de enrutamiento para completar la tabla de enrutamiento de IPv6 con prefijos remotos.

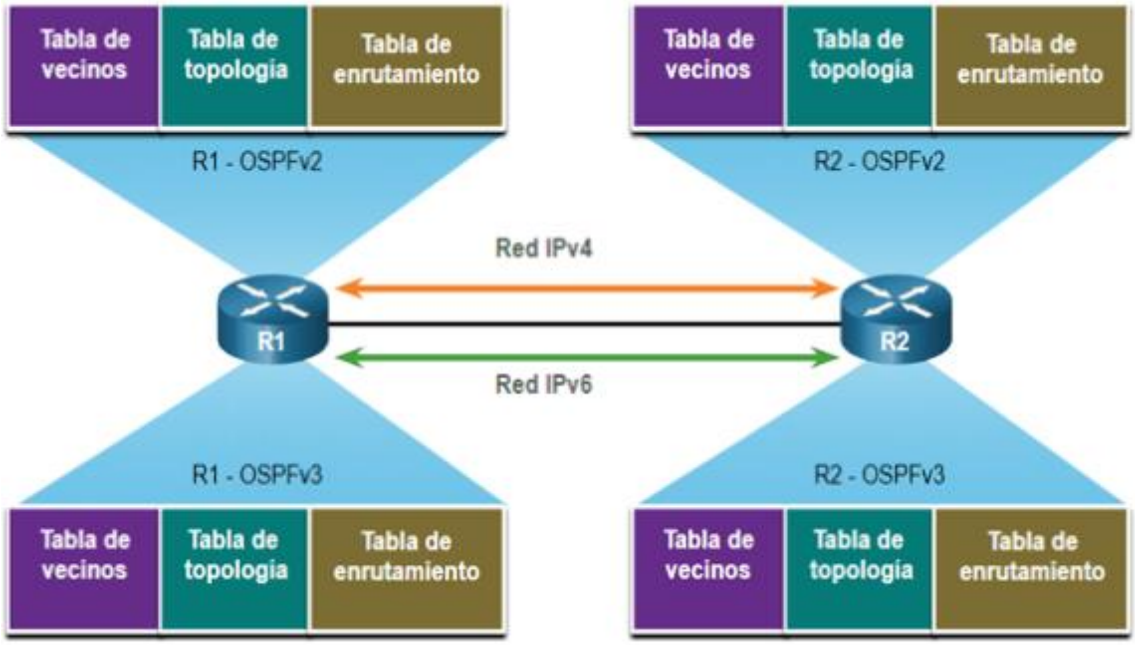
OSPFv2 se ejecuta sobre la capa de red IPv4, comunicándose con otros pares de IPv4 de OSPF y publicando solo rutas IPv4, OSPFv3 tiene la misma funcionalidad que OSPFv2, pero utiliza IPv6 como transporte de la capa de red, por lo que se comunica con pares de

OSPFv3 y anuncia rutas IPv6. OSPFv3 también utiliza el algoritmo SPF como motor de cómputo para determinar las mejores rutas a lo largo del dominio de enrutamiento. OSPFv3 tiene procesos separados de su contra-parte IPv4, los procesos y las operaciones son básicamente los mismos que en el protocolo de enrutamiento IPv4, pero se ejecutan de forma independiente. (CCNA desde Cero, 2021)

OSPFv2 y OSPFv3 tienen tablas de adyacencia, tablas de topología OSPF y tablas de enrutamiento IP independientes, como se muestra en la ilustración. Los comandos de configuración y verificación de OSPFv3 son similares a los que se utilizan en OSPFv2.

(Ariganello, 2020)

Figura N°15
Estructura de Datos OSPFv2 y OSPFv3



Fuente: PDF Curso CCNA CISCO
https://ccnadesdecero.es/caracteristicas-funciones-ospf/

3.4 Switch

3.4.1 Definición

En una red diseñada correctamente, los switches LAN son responsables de controlar el flujo de datos en la capa de acceso y de dirigirlo a los recursos conectados en red. Los switches de Cisco son de configuración automática y no necesitan ninguna configuración adicional para comenzar a funcionar.

(Cisco, 2015)

3.4.2 Funcionamiento

Los switches son piezas de construcción clave para cualquier red. Conectan varios dispositivos, como computadoras, access points inalámbricos, impresoras y servidores; en la misma red dentro de un edificio o campus. Un *switch* permite a los dispositivos conectados compartir información y comunicarse entre sí.

(Cisco, 2008)

3.4.2.1 Switches no administrados

Un switch de red no administrado está diseñado para que pueda simplemente conectarlo y funcione, sin necesidad de configuración. Los switches no administrados se usan generalmente para conectividad básica. En general, se verán en redes domésticas o donde sea que se necesiten unos cuantos puertos más, como en su escritorio, en un laboratorio o en una sala de conferencias.

(Cisco, 2008)

3.4.2.2 Switches administrados

Los switches administrados le ofrecen mayor seguridad y más funciones y flexibilidad, dado que puede configurarlos para que se adapten a su red. Con este mayor control, puede proteger mejor su red y mejorar la calidad del servicio para los que acceden a la red.

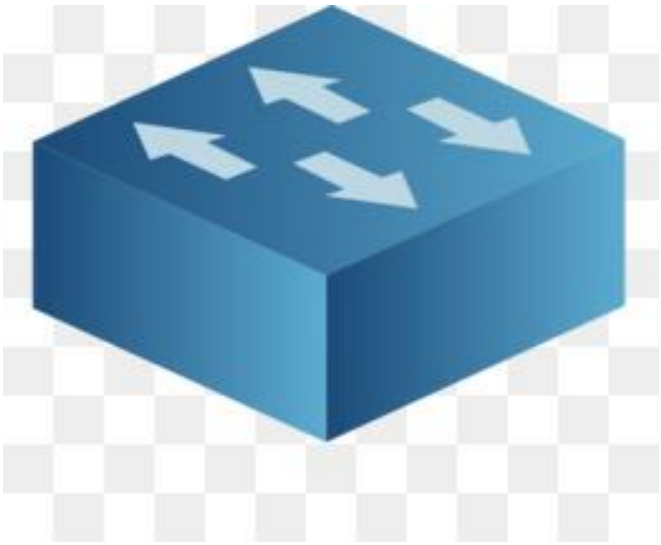
(Cisco, 2015)

En las siguientes figuras se observará un switch real y el switch que se usa en simulación para el aprendizaje.

Figura N°16
Switch Cisco

Fuente: PDF Curso CCNA CISCO
www.google.com/search?q=imagenes+de+switch+cisco&rlz=1C1ALOY

Figura N°17
Switch que se usa en el Simulador para el aprendizaje



Fuente: PDF Curso CCNA CISCO
https://www.freepng.es/png-nvmli9/

3.5 Tipos de Red

El término red hace referencia a un conjunto de sistemas informáticos independientes conectados entre sí, de tal forma que posibilitan un intercambio de datos, para lo que es necesario tanto la conexión física como la conexión lógica de los sistemas. Esta última se establece por medio de unos protocolos de red especiales, como es el caso de TCP (Transmission Control Protocol). Dos ordenadores conectados entre sí ya pueden considerarse una red.

Las redes se configuran con el objetivo de transmitir datos de un sistema a otro o de disponer recursos en común, como servidores, bases de datos o impresoras. En función del tamaño y del alcance de la red de ordenadores, se puede establecer una diferenciación entre diversas dimensiones de red. Entre los tipos de redes más importantes se encuentran: (Ariganello, 2020)

- Personal Área Networks (PAN) o Red de área personal
- Local Área Networks (LAN) o Red de área local
- Metropolitan Área Networks (MAN) o Red de área metropolitana
- Wide Área Networks (WAN) o Red de área amplia
- Global Área Networks (GAN) o Red de área global

3.5.1 Personal Área Networks

Es un estándar de red para la comunicación entre distintos dispositivos cercanos al punto de acceso. Estas redes son de unos pocos metros y para uso personal. Se establece que las redes de área personal son una configuración básica llamada así mismo personal la cual está integrada por los dispositivos que están situados en el entorno personal y local del usuario, ya sea en la casa, trabajo, carro, parque, centro comercial, etc. Esta configuración le permite al usuario establecer una comunicación con estos dispositivos a la hora que sea de manera rápida y eficaz. (Ariganello, 2020)

Figura N°18
Red de Área Personal

Fuente: IONOS, Redes Inalámbricas
https://infotic.fandom.com/es/wiki/Red_de_%C3%A1rea_Personal_(PAN)

3.5.2 Local Área Networks

Red de comunicación entre ordenadores situados en el mismo edificio o en edificios cercanos, de forma que permite a sus usuarios el intercambio de datos y la compartición de recursos.

Una red de área local (LAN) es un grupo de computadoras y dispositivos periféricos que comparten una línea de comunicaciones común o un enlace inalámbrico a un servidor dentro de un área geográfica específica. Una red de área local puede servir a tan solo dos o tres usuarios en una oficina en casa o miles de usuarios en la oficina central de una corporación. Los propietarios de viviendas y los administradores de tecnología de la información (TI) configuran una LAN para que los nodos de la red puedan comunicarse y compartir recursos como impresoras o almacenamiento en red.

La red LAN requiere cables Ethernet y conmutadores de Capa 2 junto con dispositivos que se puedan conectar y comunicarse mediante Ethernet. Las LAN más grandes a

menudo incluyen conmutadores o enrutadores de capa 3 para agilizar los flujos de tráfico.

Una LAN permite a los usuarios conectarse a servidores internos, sitios web y otras LAN que pertenecen a la misma red de área amplia (WAN). Ethernet y Wi-Fi son las dos formas principales de habilitar las conexiones LAN. Ethernet es una especificación del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) que permite que las computadoras se comuniquen entre sí. Wi-Fi utiliza ondas de radio en el espectro de 2,4 gigahercios (GHz) y 5 GHz para conectar computadoras a la LAN.

Las tecnologías LAN heredadas, que incluyen token ring, la interfaz de datos distribuidos por fibra (FDDI) y la red informática de recursos adjuntos (ARCNET) han perdido popularidad a medida que aumentaron las velocidades de Ethernet y Wi-Fi y disminuyeron los costos de conectividad. (Ariganello, 2020)

Hay dos tipos de LAN principales las cuales son:

3.5.2.1 LAN Cableada

Una LAN cableada utiliza conmutadores y cableado Ethernet para conectar puntos finales, servidores y dispositivos de internet de las cosas (IoT) a la red corporativa. Para las pequeñas empresas con solo un puñado de dispositivos, una LAN cableada puede consistir en un solo conmutador LAN no administrado con suficientes puertos Ethernet para interconectar todos los dispositivos. Pero las LAN más grandes que conectan miles de dispositivos requieren hardware, software y pasos de configuración adicionales para garantizar que la red funcione de manera óptima. (Redes Informaticas, 2019)

3.5.2.2 LAN Inalámbricas

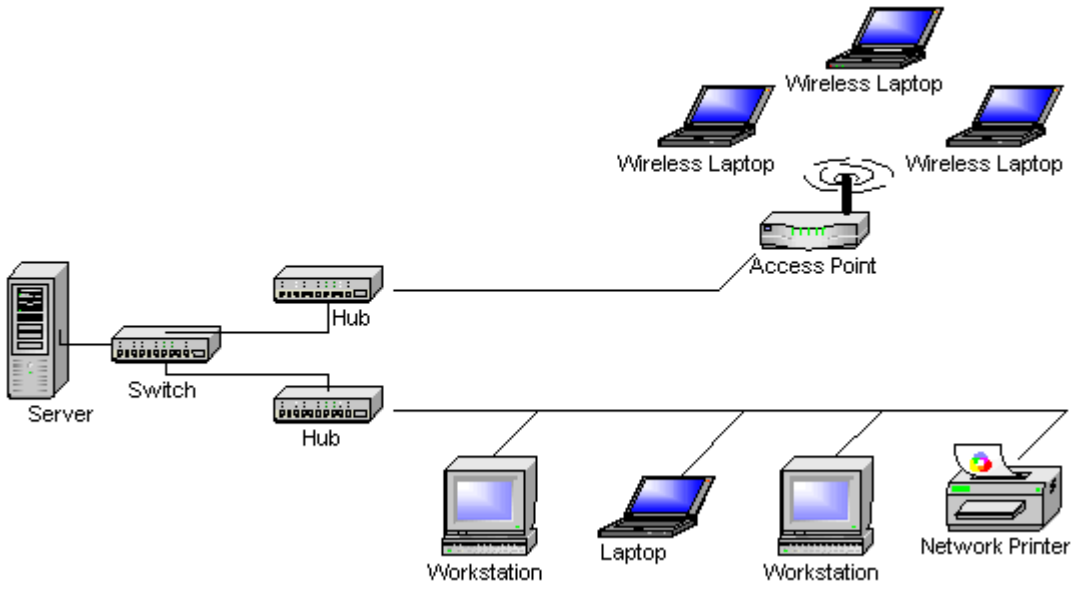
Las LAN inalámbricas utilizan la especificación IEEE 802.11 para transportar datos entre los dispositivos finales y la red utilizando un espectro inalámbrico. En muchas situaciones, una LAN inalámbrica es preferible a una conexión LAN cableada debido a su flexibilidad y ahorro de costos, ya que no es necesario instalar cableado en todo el edificio. Las empresas que evalúan las WLAN como un medio principal de conectividad

a menudo tienen usuarios que dependen exclusivamente de teléfonos inteligentes, tabletas y otros dispositivos móviles.

(Redes Informaticas, 2019)

Figura N°19

Red LAN con medios Físicos e Inalámbricos



Fuente: IONOS, Redes LAN
https://virtual.itca.edu.sv/Mediadores/irmfi2/ITRMFI_14.htm

3.5.2.3 Topologías de la Red LAN

La topología de una red es la configuración o relación de los dispositivos de red y las interconexiones entre ellos. Las topologías LAN y WAN se pueden ver de dos maneras:

a) Topología Física

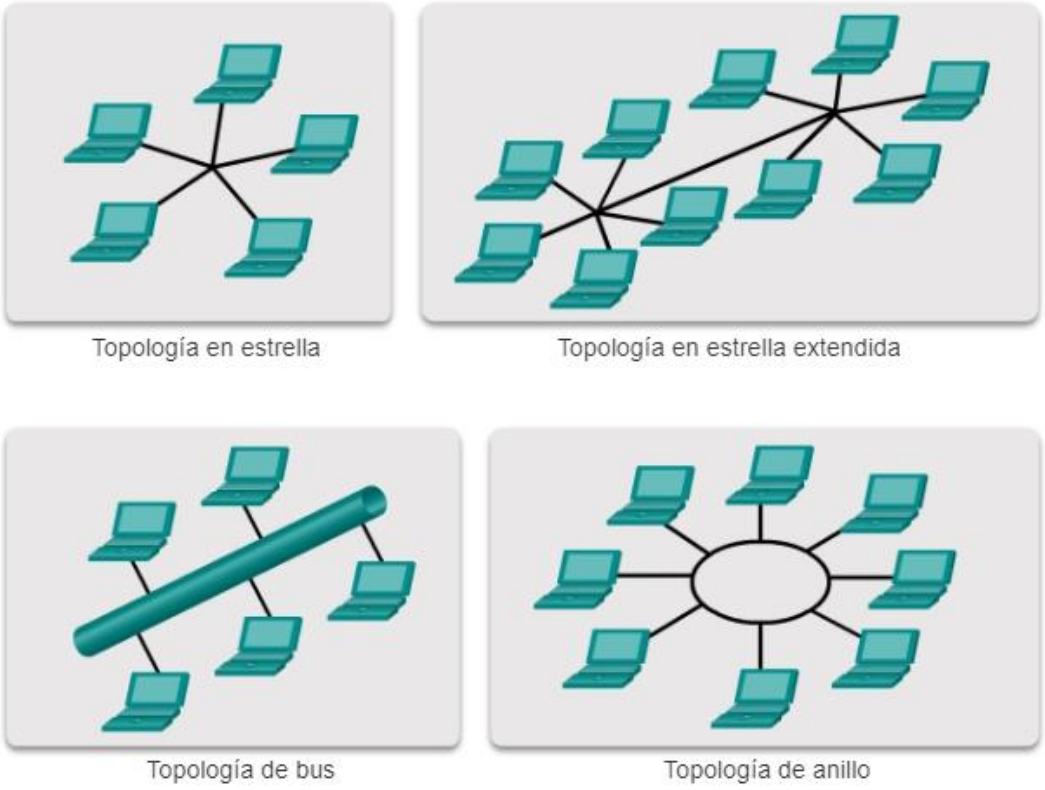
La topología física define cómo se interconectan físicamente los sistemas finales. En las redes LAN de medios compartidos, los dispositivos finales se pueden interconectar mediante las siguientes topologías físicas:

- **Estrella:** Los dispositivos finales se conectan a un dispositivo intermediario central. Las primeras topologías en estrella interconectaban dispositivos finales mediante hubs. Sin embargo, en la actualidad estas topologías utilizan switches. La topología en estrella es la topología física de LAN más común, principalmente porque es fácil de instalar, muy escalable (es fácil agregar y quitar dispositivos finales) y de fácil resolución de problemas.
- **Estrella extendida o híbrida:** En una topología en estrella extendida, dispositivos intermediarios centrales interconectan otras topologías en estrella. En una topología híbrida, las redes en estrella se pueden interconectar mediante una topología de bus.
- **Bus:** Todos los sistemas finales se encadenan entre sí y terminan de algún modo en cada extremo. No se requieren dispositivos de infraestructura, como switches, para interconectar los dispositivos finales. Las topologías de bus se utilizaban en las antiguas redes Ethernet, porque eran económicas y fáciles de configurar.
- **Anillo:** Los sistemas finales se conectan a su respectivo vecino y forman un anillo. A diferencia de la topología de bus, la de anillo no necesita tener una terminación. Las topologías de anillo se utilizaban en las antiguas redes de interfaz de datos distribuida por fibra (FDDI). Específicamente, las redes FDDI emplean un segundo anillo para la tolerancia a fallas o para mejorar el rendimiento.

(Itroque, 2015)

En la ilustración, se muestra cómo se interconectan los dispositivos finales en las redes LAN.

Figura N°20
Topologías Físicas

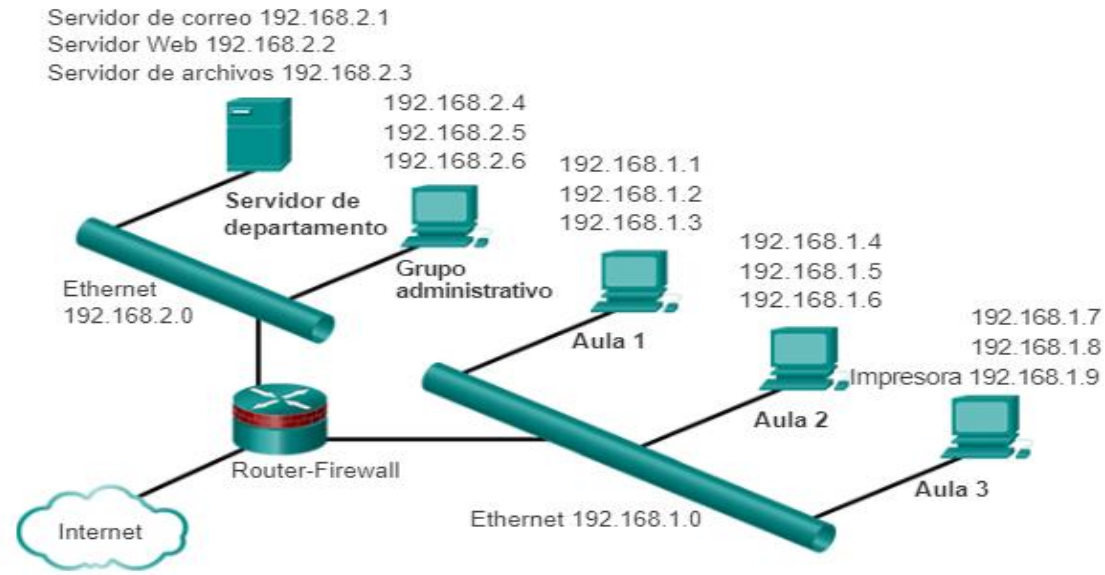


Fuente: Curso Cisco Oficial
http://itroque.edu.mx/cisco/cisco1/course/module4/4.4.1.2/4.4.1.2.html

b) Topología Lógica

Se refiere a la forma en que una red transfiere tramas de un nodo al siguiente. Esta disposición consta de conexiones virtuales entre los nodos de una red. Los protocolos de capa de enlace de datos definen estas rutas de señales lógicas. La topología lógica de los enlaces punto a punto es relativamente simple, mientras que los medios compartidos ofrecen métodos de control de acceso al medio deterministas y no deterministas.
(Itroque, 2015)

Figura N°21
Topología Lógica



Fuente: Curso Cisco Oficial
http://itroque.edu.mx/cisco/cisco1/course/module4/4.4.1.2/4.4.1.2.html

3.5.3 Metropolitan Área Networks

El término MAN proviene de "Metropolitan Área Network" o en español, red de área metropolitana. Este tipo de red es el paso intermedio entre una red LAN y una red WAN, ya que la extensión de este tipo de redes comprende el territorio de una gran ciudad. Las redes MAN son redes de alta velocidad capaces de dar cobertura a una geografía relativamente extensa, aunque nunca superando las dimensiones de una ciudad.

Las topologías que se emplean en este tipo de redes son generalmente malladas con algunos elementos configurados en forma de redes troncales, que normalmente derivan en subredes más pequeñas. En ella se emplean fundamentalmente conexiones mediante cables de par trenzado y cada vez más mediante fibra óptica.

Una red MAN puede llegar a tener velocidades de hasta 10 Gb/s (Gigabit por segundo) con el uso de fibra óptica.

(SCRIBD, 2018)

Figura N°22
Red MAN

Fuente: EL Mundo de las Redes
https://www.profesionalreview.com/2018/12/09/redes-lan-man-wan/#Red_MA

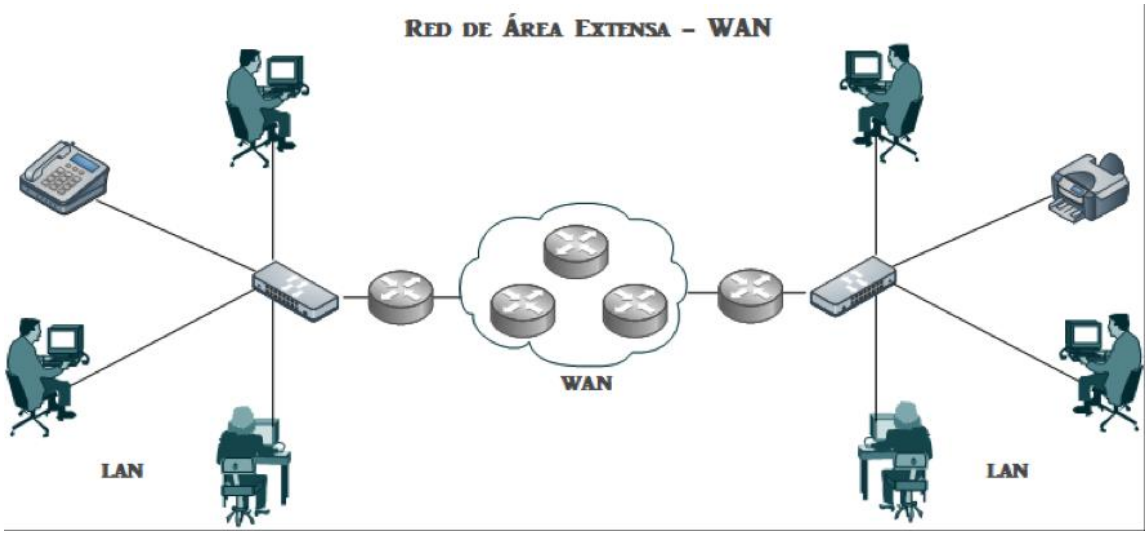
3.5.4 Wide Área Networks

3.5.4.1 Definición

Una red de área amplia, o WAN son redes a gran escala que abarcan países e incluso continentes. No conectan ordenadores individuales, sino otras redes como LAN o MAN. Las WAN pueden ser públicas o estar gestionadas por empresas para conectar varias ubicaciones a grandes distancias. Las WAN públicas son operadas por proveedores de servicios de Internet para permitir a sus clientes el acceso a este. Las redes privadas de área amplia son utilizadas principalmente por empresas, por ejemplo, para permitir servicios en la nube y para conectar las redes de las diferentes sedes de la empresa. (IONOS, 2020)

En la siguiente figura se observará una red de área amplia:

Figura N°23
Red de Área Amplia



Fuente: EL Mundo de las Redes
https://www.profesionalreview.com/2018/12/09/redes-lan-man-wan/#Red_WA

3.5.4.2 Funcionamiento

Como una red WAN no conecta ordenadores individuales, sino redes enteras, la tecnología utilizada difiere de los otros tipos de red. Emplea otros protocolos de transmisión y conceptos de dirección.

Las redes WAN utilizan técnicas y protocolos de transmisión de las capas uno a tres del modelo de referencia OSI. De este modo, una WAN funciona en la capa física, la capa de enlace de datos y la capa de red.

Las redes de área amplia utilizan un esquema de direccionamiento uniforme porque el envío sin dirección de datos sería ineficiente con el número de redes conectadas. Los sistemas intermedios o nodos de red, como conmutadores, puentes y enrutadores garantizan que los paquetes de datos enviados se reenvían a la dirección correcta. Mediante el hardware, los paquetes de datos se envían de una subred a la otra y se entregan al participante de red correcto, ya sea un PC, un teléfono inteligente, un

televisor o un refrigerador. La tecnología básica de esto es la pila de protocolos TCP/IP. Los distintos protocolos de esta familia de protocolos garantizan, por ejemplo, que los datos se procesen correctamente y que los paquetes lleguen a su destino, aunque haya dificultades en la transmisión (IONOS, 2020).

Para la transmisión de datos se emplean también las siguientes tecnologías.

- X.25 (tecnología más antigua, desde los años 70)
- Modo de transferencia asíncrono (ATM) (tecnología antigua)
- Multiprotocol Label Switching (IP/MPLS)
- Jerarquía digital presiócrona (PDH)
- Jerarquía digital síncrona (SDH)
- Ethernet

Los medios de transmisión físicos utilizados son los cables de cobre y fibra óptica, así como los enlaces inalámbricos. Los cables de fibra óptica son especialmente adecuados para conexiones a larga distancia sobre tierra y agua. Los avances más recientes son las vías de transmisión de datos de banda ancha por satélite, que se pueden establecer con relativa rapidez. En la práctica, se suele utilizar una combinación de varios medios de transmisión distintos. Con los llamados convertidores de medios, se pueden interconectar distintos tipos de cables. En los grandes nodos de Internet hay puntos de intercambio especiales interconectados, donde a menudo hay más de cien redes interconectadas para permitir un intercambio de datos eficiente. Los repetidores se encargan de que los paquetes de datos no pierdan información, incluso a grandes distancias (Irene, 2020).

3.5.4.3 Topologías WAN

3.5.4.3.1 Punto a Punto

Esta es la topología WAN más simple y más común. Consiste en un enlace permanente entre dos puntos finales, así como se ilustra a continuación:

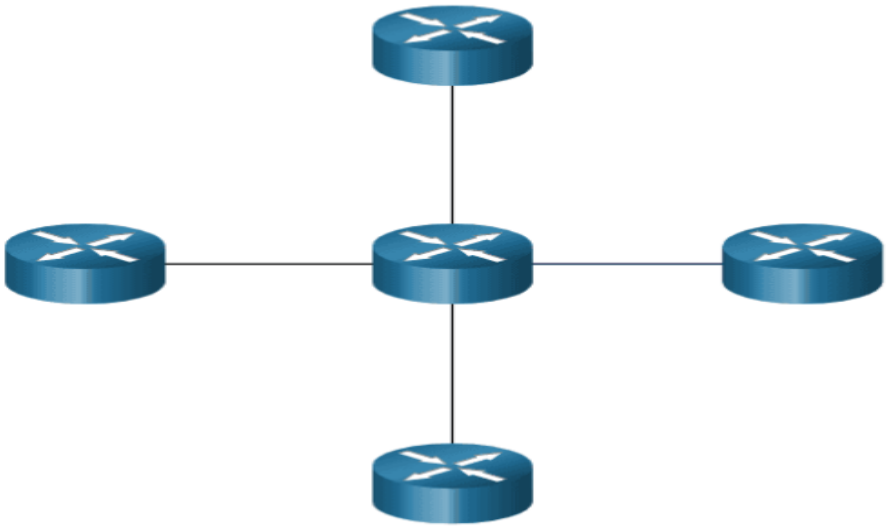
Figura N°24
Topología WAN Punto a Punto

Fuente: Curso CCNA desde Cero
https://ccnadesdecero.es/topologias-red-lan-y-wan/

3.5.4.3.2 Hub and Spoke

Esta es una versión WAN de la topología en estrella en la que un sitio central interconecta sitios de sucursal mediante el uso de enlaces punto a punto. Los sitios de sucursal no pueden intercambiar datos con otros sitios de sucursal sin pasar por el sitio central, así como se muestra en la figura:

Figura N°25
Topología WAN Hub and Spoke

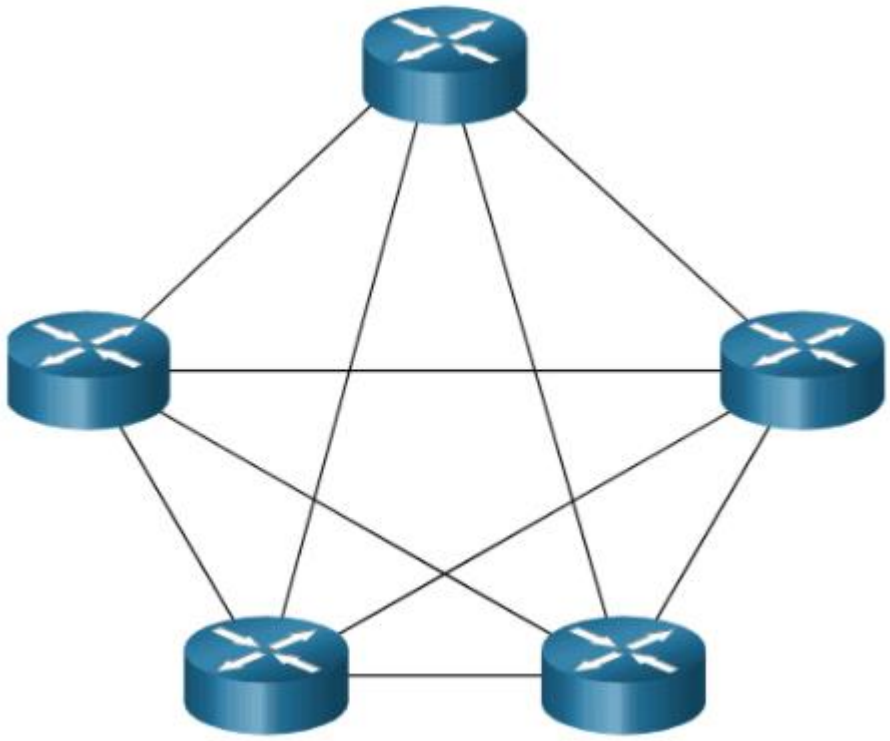


Fuente: Curso CCNA desde Cero
https://ccnadesdecero.es/topologias-red-lan-y-wan/

3.5.4.3.3 Malla

Esta topología proporciona alta disponibilidad, pero requiere que cada sistema final esté interconectado con cualquier otro sistema. Por lo tanto, los costos administrativos y físicos pueden ser significativos. Cada enlace es esencialmente un enlace punto a punto al otro nodo.

Figura N°26
Topología WAN - Malla



Fuente: Curso CCNA desde Cero
https://ccnadesdecero.es/topologias-red-lan-y-wan/

3.6 Internet

3.6.1 Definición

Se podría denominar a Internet como una red insegura global de redes de ordenadores, internet es una colección mundial de redes interconectadas (abreviado: internet Works o internet) que colaboran para intercambiar la libre información entre todos sus usuarios sobre la base de estándares comunes. A través de cables telefónicos, cables de fibra óptica, transmisiones inalámbricas y enlaces satelitales, los usuarios de internet pueden intercambiar información de diversas formas. Internet es un conglomerado de redes que no es propiedad de ninguna persona ni de ningún grupo (Slideshare, 2016).

En la siguiente tabla se podrá observar algunas ventajas y desventajas de internet:

TABLA N°3
Ventajas y Desventajas de la Red Internet

Ventajas	Desventajas
Velocidad en la comunicación	Uso de datos personales con fines desconocidos
Acceso a múltiples contenidos	Delincuencia Digital
Difusión de contenidos propios	Acoso en línea
Masificación del conocimiento	Spam

Fuente: Elaboración Propia

3.6.2 Tecnologías de Acceso a Internet

Son aquellas plataformas que permiten dar conectividad a los usuarios con los ISP (Internet Service Provider).

- Por tecnología estas pueden ser: alámbricas (Eléctricas u ópticas) o inalámbricas.
- Por tipos de usuarios: Conmutados o dedicados.

3.6.2.1 Tecnologías Conmutadas

Son las primeras en aparecer en el mercado, fácil de administrar tanto para los usuarios finales como para los prestadores de servicio, sus costos están basados en el tiempo de conexión. Estas tecnologías son:

- La Red Pública Telefónica Conmutada (RPTC)
- La Red Digital de Servicios Integrados (RDSI).

Estas tecnologías se apoyaron directamente en protocolo PPP (Point to Point Protocol) (Slideshare, 2016)

a) Red Publica Telefónica Conmutada

La red pública conmutada es la tecnología de acceso a Internet que permitió la masificación del servicio, ya que sus bajos costos tanto para el usuario como para ISP, hacían del servicio una posibilidad para cualquier sector o mercado. Su funcionamiento se basa en un esquema orientado a la conexión y en un ambiente de acceso compartido.

A continuación, mencionamos algunas ventajas y desventaja que presenta las tecnologías conmutadas:

TABLA N°4

Ventajas y Desventajas de la RPTC

Ventajas	Desventajas
Bajos Costos	Baja Velocidad
Estandarización de Equipos	"Anulación" del servicio telefónico
Amplia Cobertura	Variación en el consumo por tiempo de conexión
Facilidad de Manejo	

Fuente: Elaboración Propia

b) Red Digital de Servicios Integrados

Nace inicialmente en Europa, aparece como una alternativa interesante para la transmisión de voz, datos y video, a un costo relativamente bajo. Dado a que RDSI es una tecnología totalmente digital, supera el desempeño dado por los módems análogos tradicionales, lo que hizo que se volviera una solución interesante para los usuarios empresariales y residenciales.

b-1) Integración de Servicios

La RDSI se caracteriza básicamente por soportar servicios de comunicación de voz, datos e imágenes a través de la misma red. Debido a esto, un conjunto determinado de interfaces compartidas de usuario-red se estandarizan y se posibilitan varias funciones estándar en la red.

b-2) Funciones de Conexión

La red soporta tanto servicios de conexión conmutada como de conexión semi-permanente (Slideshare, 2012) .

b-3) Servicio Básico

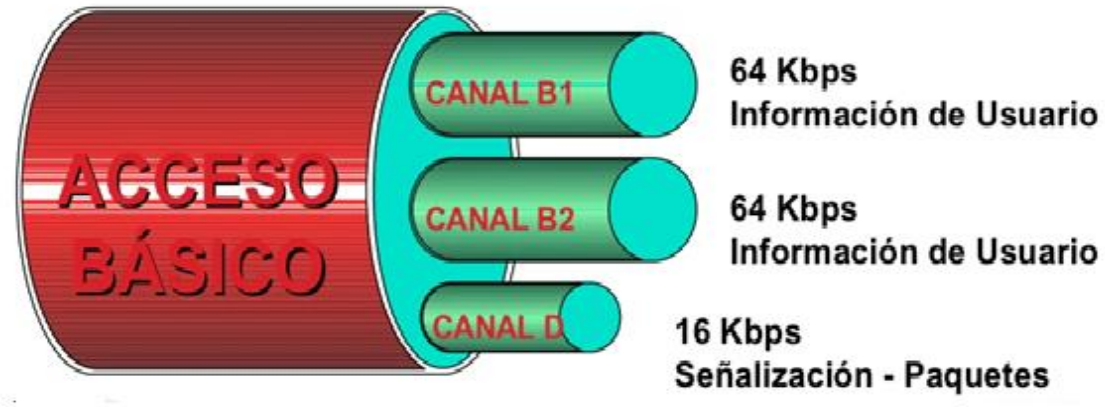
El servicio de 64 kbps por conmutación de circuitos es definido como el servicio básico. Otros servicios diferentes pueden ser soportados de forma simultánea, como la "sumarización" de canales para obtener mayor ancho de banda.

La tecnología RDSI maneja dos tipos de canales:

- Canales B (Bearer, portador): 64 Kb/s, sirven para llevar la voz o datos del usuario, puede haber un número variable según el tipo de interfaz
- Canal D (Data): Se usa para señalización fuera de banda (establecer o terminar la llamada, información de control, etc.). Hay uno por interfaz.

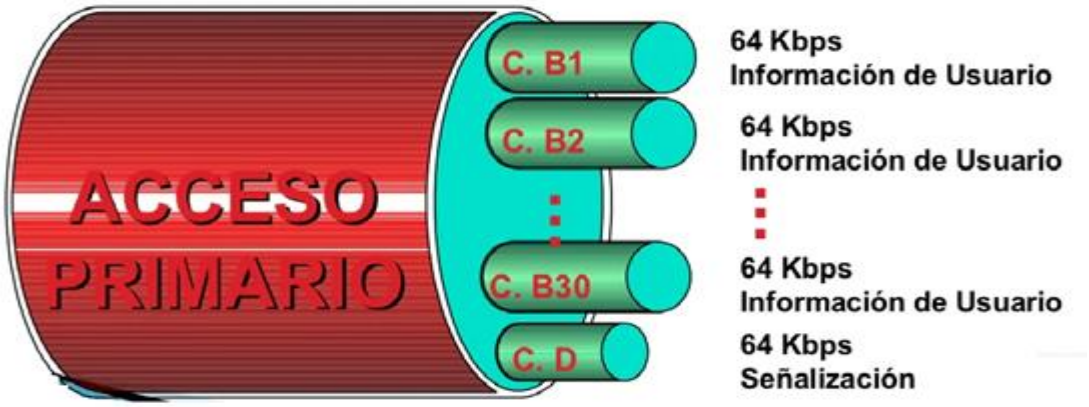
La tecnología RDSI maneja dos tipos de interfaces: Básico y Primario, a continuación, se ilustrará en las siguientes figuras:

Figura N°27
Interfaz de Acceso Básico
Canales Físicos: 2x64 kbps + 16kbps (2B+D)



Fuente: Tecnologias de Acceso a la Red
https://es.slideshare.net/equipoderedes/tecnologas-de-acceso

Figura N°28
Interfaz de Acceso Primario
Canales Físicos:30 x 64 kbps + 64 kbps



Fuente: Tecnologias de Acceso a la Red
https://es.slideshare.net/equipoderedes/tecnologas-de-acceso

Esta tecnología presenta las siguientes características:

TABLA N°5
Ventajas y Desventajas de la tecnología RDSI

Ventajas	Desventajas
Costo por consumo	Costos Variables por tiempo de Conexión
Estandarización de equipos	
La posibilidad de activar canales B bajo demanda de petición de la capa de enlace, por ejemplo, con el protocolo PPP.	
RDSI es muy adecuado para datos cuando la conexión es de pocas horas al día. También para configuraciones de emergencia(backup)	

Fuente: Elaboración Propia

3.6.2.2 Tecnologías Dedicadas

Son aquellas tecnologías que permiten tener conectividad permanente con el prestador de servicios, por lo general su facturación es de manera plana. Inicialmente nacen como tecnologías orientadas al sector empresarial, pero dado a la popularidad de Internet, el tele trabajo, el uso ilimitado del servicio, los grandes anchos de banda que requieren las nuevas aplicaciones y los bajos costos de la tecnología, hoy en día estas plataformas están al alcance del sector residencial. Algunas de estas tecnologías son: (Slideshare, 2012)

3.6.2.2.1 Asymmetric Digital Subscriber Line (ADSL)

ADSL son las siglas de una tecnología descrita literalmente en castellano como Línea de abonado digital asimétrica, este sistema posibilita la transferencia o emisión de todo tipo de información digital gozando de una velocidad banda ancha a través de las líneas telefónicas, prestando de esta manera una multiplicidad de servicios como por ejemplo uno de ellos es el servicio de Internet, es decir que gracias al ADSL los usuarios tienen la posibilidad de acceder a Internet sin tener que interceptar o interrumpir las llamadas telefónicas entrantes a una línea.

En otras palabras, se trata de una línea o tecnología digital de gran velocidad sostenida por un cable trenzado de cobre que guía la línea telefónica convencional; a esto se le califica como un tipo de conexión a Internet que proporciona la transferencia de datos de forma digitalizada a través de una línea telefónica.
(ConceptoDefinicion, 2021)

3.6.2.2.2 Cable

El cable-módem, es un tipo especial de módem, diseñado para modular y demodular la señal de datos sobre una infraestructura de televisión por cable (CATV). Internet por cable es un tipo de acceso de banda ancha a Internet.

3.6.2.2.3 Power Line Communications (PLC)

PLC son las siglas de Power Line Communications. Se trata de una serie de tecnologías que permiten usar los cables de la instalación eléctrica de nuestra casa para llevar Internet de un lado a otro. Lo que estos PLC hacen es enviar los datos de nuestra conexión a Internet usando el mismo cable por el que circula la red eléctrica. A esa señal que lleva los datos se la conoce como "señal portadora".

Para ello, se usan señales de diferente frecuencia y voltaje. La corriente eléctrica tiene una frecuencia de 50 Hz y 220 voltios, mientras que la señal de datos usa un voltaje muchísimo más bajo y una frecuencia mucho más alta (entre 2 y 30 MHz). Así se consigue distinguir una señal de otra (Xataka, 2021).

3.6.2.2.4 Local Multipoint Distribution Service (LMDS)

El Sistema de Distribución Local Multipunto o LMDS es una tecnología de conexión vía radio inalámbrica que permite, gracias a su ancho de banda, el despliegue de servicios fijos de voz, acceso a Internet, comunicaciones de datos en redes privadas, y video bajo demanda.

Las razones de la importancia de la tecnología LMDS son:

- La rápida instalación en comparación con tecnologías de cable.
- La posibilidad de integrar diversos tipos de tráfico como voz digital, video y datos.

- La alta velocidad de acceso a internet, tanto en el sector residencial como en la empresarial.
- La posibilidad de instalar una red de acceso de bajo coste, flexible, modular y fiable.

3.6.2.2.5 Satelital

Es un método, de conexión a Internet, utilizando como medio de enlace un satélite. Es un sistema recomendable de acceso, en aquellos lugares, donde no llega el cable o la telefonía, como zonas rurales o alejadas. Es algo costoso y de ancho de banda limitado.

3.6.2.2.6 Wireless Local Área Network (WLAN)

WLAN es una sigla de la lengua inglesa que alude a Wireless Local Área Network, una expresión que puede traducirse como Red de Área Local Inalámbrica. Como la denominación lo señala, una WLAN es una red de tipo local cuyos equipos no necesitan estar vinculados a través de cables para conectarse.

La WLAN es un tipo específico de LAN, una red informática formada por unidades ubicadas en un espacio geográfico de dimensiones reducidas. Mientras que las computadoras (ordenadores) que forman parte de una LAN se conectan entre sí o a un router con cables, en una WLAN la conexión se realiza utilizando ondas de radiofrecuencia (TechClub Tajamar, 2018).

En la siguiente imagen podremos observar las diferentes tecnologías de acceso a internet**:**

Figura N°29
Tecnologías de Acceso a Internet

Fuente: Tecnologias de Acceso a la Red
https://techclub.tajamar.es/tecnologias-de-acceso-a-internet/

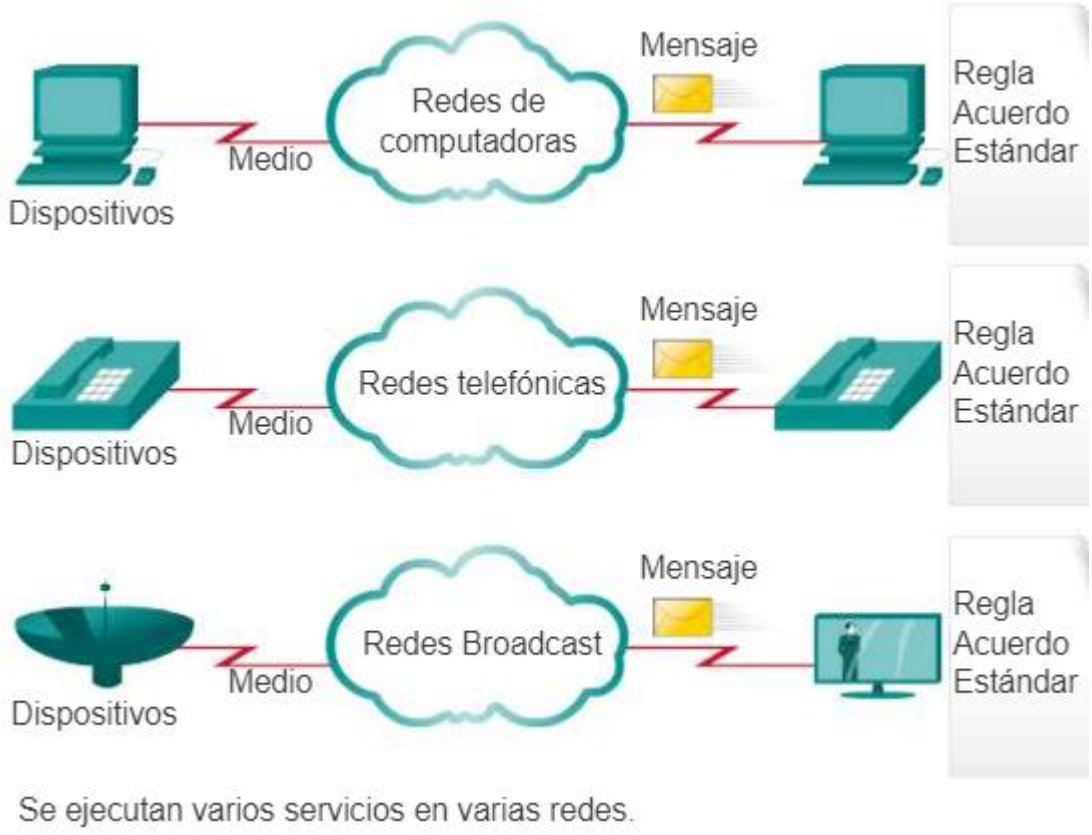
3.7 Redes Convergentes

Las redes modernas están en constante evolución para satisfacer las demandas de los usuarios. Las primeras redes de datos estaban limitadas a intercambiar información con base en caracteres entre sistemas informáticos conectados. Las redes tradicionales de teléfono, radio y televisión se mantenían separadas de las redes de datos. En el pasado, cada uno de estos servicios necesitaba una red dedicada, con distintos canales de comunicación y diferentes tecnologías para transportar una señal de comunicación específica. Cada servicio tenía su propio conjunto de reglas y estándares para asegurar la comunicación satisfactoria.

Podemos poner como ejemplo una escuela construida hace cuarenta años. En ese entonces, las aulas contaban con conexiones por cable para la red de datos, la red

telefónica y la red de video para los televisores. Estas redes separadas eran dispares, es decir, no podían comunicarse entre sí, como se muestra en la siguiente figura:
(CCNA 2020, 2017)

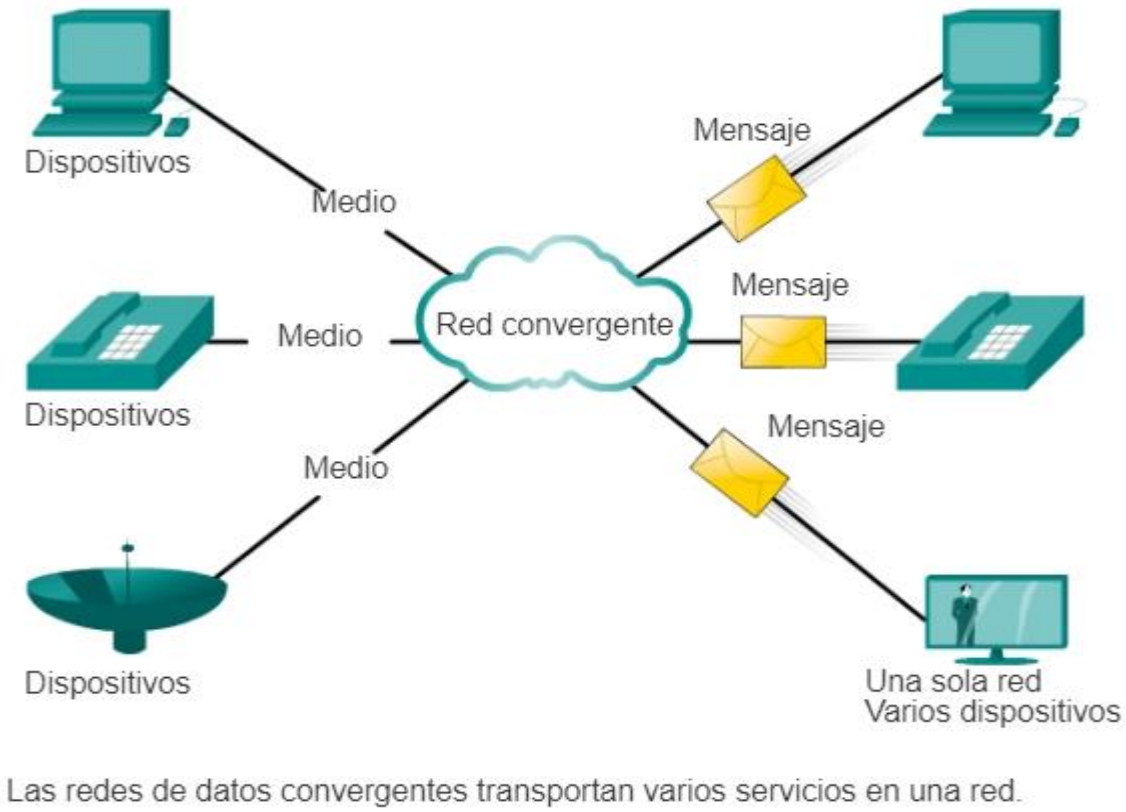
Figura N°30
Redes Dedicadas



Fuente: Curso Netcad Cisco
www.itesa.edu.mx/netacad/introduccion/course/module1/1.3.1.1/1.3.1.1.html

Los avances en la tecnología nos permiten consolidar estos tipos de redes diferentes en una plataforma conocida como “red convergente”. A diferencia de las redes dedicadas, las redes convergentes pueden transmitir voz, streams de video, texto y gráficos entre diferentes tipos de dispositivos utilizando el mismo canal de comunicación y la misma estructura de red, como se muestra en la siguiente figura:

Figura N°31
Red Convergente



Fuente: Curso Netcad Cisco
www.itesa.edu.mx/netacad/introduccion/course/module1/1.3.1.1/1.3.1.1.html

Las formas de comunicación anteriormente individuales y diferentes se unieron en una plataforma común. Esta plataforma proporciona acceso a una amplia variedad de métodos de comunicación alternativos y nuevos que permiten a las personas interactuar directamente con otras en forma casi instantánea.

En las redes convergentes, sigue habiendo muchos puntos de contacto y muchos dispositivos especializados, como computadoras personales, teléfonos, televisores y tablet pc, pero hay una infraestructura de red común. Esta infraestructura de red utiliza el mismo conjunto de reglas, acuerdos y estándares de implementación.

3.8 Direccionamiento IP

3.8.1 Números Binarios

Los dispositivos emiten y reciben pulsos eléctricos o luminosos. Estos pulsos poseen dos estados, SÍ y NO. Este sistema de dos signos se le llama binario, matemáticamente hablando un sistema binario está compuesto por dos estados de unos y ceros siendo, por tanto, una potencia en base 2. En informática se llama bits a la unidad que tiene también dos estados, un byte es un grupo de ocho bits.

Un octeto o un byte se expresa de la siguiente manera:

00000000

Cada uno de estos bits que componen el octeto posee dos estados 1 y 0, obteniendo por tanto 256 estados con todas las combinaciones posibles como podemos observar a continuación en la siguiente tabla:

TABLA N°6

Sistema Binario

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0	Estados
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	1	1
0	0	0	0	0	0	1	0	2
0	0	0	0	0	0	1	1	3
0	0	0	0	0	1	0	0	4
0	0	0	0	0	1	0	1	5
0	0	0	0	0	1	1	0	6
……								
1	1	1	1	1	1	1	0	254
1	1	1	1	1	1	1	1	255

Fuente: Elaboración Propia

Para que estos bits sean más entendibles conviene trasladarlos al modo decimal al que se está más acostumbrado cotidianamente, por tanto, si son potencias de 2, su valor será como se observa en la siguiente tabla:
(Ariganello, 2020)

TABLA N°7
Potencias de Dos

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

Fuente: Elaboración Propia

Los bits que resulten iguales a 1 tendrán el valor correspondiente a esa potencia, mientras que los que permanezcan en 0 tendrán un valor igual a cero, finalmente se suma el conjunto de los decimales resultantes y se obtiene el equivalente en decimal
(Ariganello, 2020)

3.8.1.1 Conversión de Binario a Decimal

Basta con numerar los dígitos de derecha a izquierda comenzando desde cero, a cada número se le asigna la correspondiente potencia base 2 y al final se suman las potencias.
Por ejemplo, el numero binario:

10101100 = 128+0+32+0+8+4+0+0 = El valor decimal será **172**

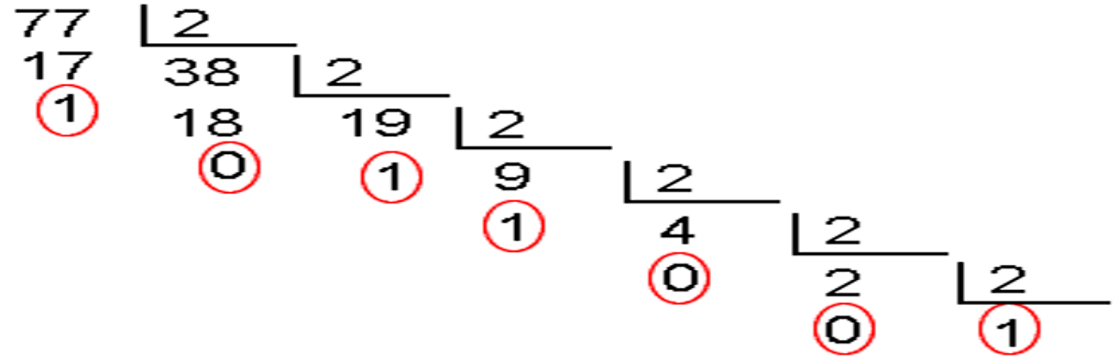
00001111 = 0+0+0+0+8+4+2+1 = El valor decimal será **15**

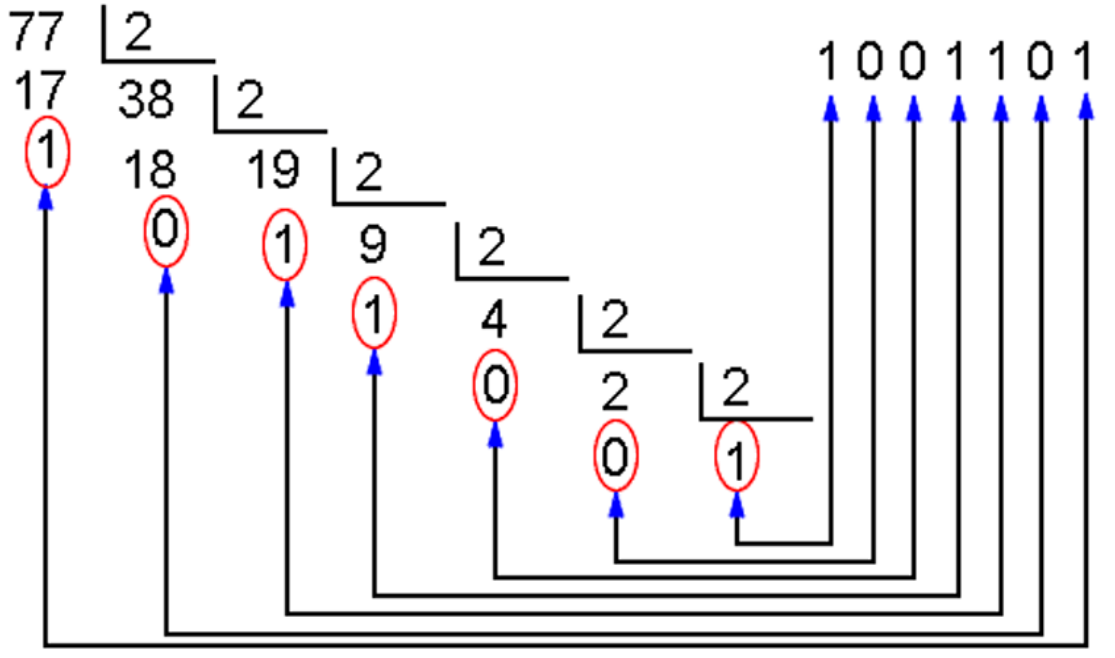
3.8.1.2 Conversión de Decimal a Binario

En el sistema decimal podemos escribir números como 451, 672, 30, etc. Es decir, es un sistema de números (con base de diez) teniendo así diez valores posibles (0, 1, 2, 3, 4, 5, 6, 7, 8, 9) por cada valor posicional. Mientras que en el caso del sistema binario podemos escribir números como 01100111, 1110, 011, 1, etc. Es decir, es un sistema de números (con base de dos) y tiene dos posibles valores (0 y 1) por cada valor posicional.

Por ejemplo, convertiremos el número 77 decimal en binario como se observa en la siguiente figura:

Figura N°32
Conversión de Decimal a Binario





Fuente: https://cual-es-mi-ip.online/herramientas/conversores-numericos/

3.8.1.3 Números Hexadecimales

Los números hexadecimales se basan en potencias de 16, utilizando símbolos alfanuméricos, la siguiente tabla le ayudará a convertir números hexadecimales en binarios o en decimales:

TABLA N°8

Conversión de números hexadecimales a binarios y decimales

Numero Decimal	Numero Hexadecimal	Numero Binario
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Fuente: Elaboración Propia

a) Conversión de Números Hexadecimales

Siguiendo el ejemplo de la figura 32, el número 77 es igual al número binario: 01001101
Divida este octeto en dos grupos de cuatro: 0100 1101

Busque el valor correspondiente en la tabla de estos dos grupos de bits. Al número binario 0100 le corresponde el número hexadecimal 4 y al número binario 1101 le corresponde el número hexadecimal D. Por lo tanto, 77 es igual a 01001101 en binario y al 4D en hexadecimal. Para que no existan confusiones los números hexadecimales se identifican con un 0x delante, en este caso 0x4D.

El proceso inverso será, por ejemplo, el número hexadecimal 0xAE donde:

A es igual a 1010

E es igual a 1110

Por lo tanto, 0xAE es igual el número binario 10101110 si se convierte este número a decimal: 2 7+0+2 5+0+2 3+2 2+2 1+0 = 174.

3.8.2 Direccionamiento IPv4

Para que dos dispositivos se comuniquen entre sí, es necesario poder identificarlos claramente. Una dirección IPv4 es una secuencia de unos y ceros de 32 bits. Para hacer más comprensible el direccionamiento, una dirección IP aparece escrita en forma de cuatro números decimales separados por puntos. La notación decimal punteada es un método más sencillo de comprender que el método binario de unos y ceros.

Esta notación decimal punteada también evita que se produzca una gran cantidad de errores por transposición, que sí se produciría si solo se utilizaran números binarios. El uso de decimales separados por puntos permite una mejor comprensión de los patrones numéricos (Ariganello, 2020).

Una dirección IPv4 consta de dos partes definidas por la llamada máscara de red. La máscara puede describirse a través de una notación decimal punteada o con el prefijo /X, donde X es igual a la cantidad de bits en 1 que contiene dicha máscara. Una parte identifica la red donde se conecta el sistema y la segunda identifica el sistema en particular de esa red. Este tipo de dirección recibe el nombre de dirección jerárquica porque contiene diferentes niveles. Una dirección IPv4 combina estos dos identificadores en un solo número. Este número debe ser exclusivo, porque las direcciones repetidas harían imposible el enrutamiento. La primera parte identifica la dirección de la red del sistema. La segunda parte, la del host, identifica qué máquina en particular de la red (Ariganello, 2020).

A continuación, en la siguiente imagen, se podrá observar un ejemplo:

Figura N°33
Ejemplo de una dirección IPv4

Dirección IP 172.16.1.3

Máscara 255.255.0.0

172	16	1	3
10101100	**00010000**	**00000001**	**00000011**
255	255	0	0
11111111	**11111111**	**00000000**	**00000000**
Porción de red		Porción de host	

Fuente: Redes Cisco, Ernesto Ariganello

3.8.2.1 Tipos de Direccionamiento IPv4

Dentro del rango de direcciones de cada red IPv4, existen tres tipos de direcciones:

- Dirección de red: La dirección en la que se hace referencia a la red o subred.
- Dirección de broadcast: Una dirección especial que se utiliza para enviar datos a todos los hosts de la red.
- Direcciones host: Las direcciones asignadas a los dispositivos finales de la red.

3.8.2.2 Tipos de Comunicación IPv4

En una red IPv4, los hosts pueden comunicarse de tres maneras diferentes:

1) Unicast

Es el método por el cual se envía un paquete de un host individual a otro host individual. La comunicación unicast se usa para una comunicación normal de host a host, tanto en una red de cliente/servidor como en una red punto a punto. Los paquetes unicast utilizan la dirección host del dispositivo de destino como la dirección de destino y pueden enrutarse a través de una internetwork. El envío unicast está habilitado por defecto, es el

más común de los tres tipos de direccionamiento, mientras que los paquetes broadcast y multicast usan direcciones especiales como dirección de destino. Al utilizar estas direcciones especiales, los broadcasts están generalmente restringidos a la red local.

2) Broadcast

El método por el cual se envía un paquete de un host a todos los hosts de la red. Existe un direccionamiento particular cuando los bits de la dirección de host están todos en la llamada dirección de broadcast, o de difusión. Este direccionamiento identifica al host origen, mientras que como destino tiene a todos los dispositivos que integran el mismo dominio. Las NIC están programadas para escuchar todo el tráfico y de esa manera reconocer el que está destinado a la propia dirección local MAC o la dirección MAC de broadcast y, así enviar las tramas a las capas superiores. Una cantidad excesiva de estas difusiones provocará una tormenta de broadcast que hará ineficiente el uso de la red, consumiendo gran cantidad de ancho de banda y haciendo que los hosts utilicen demasiados recursos al estar “obligados” a leer esos paquetes, ya que están dirigidos a todos los hosts que integran ese dominio de broadcast. Existen protocolos de enrutamiento que utilizan broadcasts para distribuir la información de enrutamiento. En lugar de requerir varios paquetes unicast simplemente se envía un paquete que alcanza a todos los dispositivos.

3) Multicast

Es el mecanismo, por el cual se envía un paquete de un host a un grupo seleccionado de hosts. Un dispositivo IP se une a un grupo reconociendo una dirección IP de otro grupo y reprogramando su tarjeta de red (NIC) para copiar todo el tráfico destinado a la dirección MAC del grupo. Debido a que el tráfico multicast está dirigido a diferentes MAC algunos hosts prestarán atención mientras que otros lo ignorarán. El tráfico multicast generalmente es unidireccional, hay un origen que envía el tráfico a todos los destinos, mientras que éstos devuelven el tráfico de manera unicast. El tráfico multicast solamente es procesado por los hosts que están programados para recibirlo.

Estos tres tipos de comunicación se usan con diferentes objetivos en las redes de datos. En los tres casos, se coloca la dirección IPv4 del host de origen en el encabezado del paquete como la dirección de origen.

3.8.2.3 Clases de Direcciones IPv4

La RFC1700 agrupa rangos de direcciones unicast en tamaños específicos llamados direcciones de clase. Las direcciones IPv4 se dividen en clases para definir las redes de tamaño pequeño, mediano y grande. Las direcciones Clase A se asignan a las redes de mayor tamaño. Las direcciones Clase B se utilizan para las redes de tamaño medio y las de Clase C para redes pequeñas. Dentro de cada rango existen direcciones llamadas privadas para uso interno que no veremos en Internet. Las direcciones de clase D son de uso multicast y las de clase E son experimentales, en la siguiente tabla se podrá ver el rango de las direcciones IP.

TABLA N°9
Rango de Direcciones IP

Clase A	Clase B	Clase C	Clase D	Clase E
Rango de direcciones IP 1.0.0.0 a 127.0.0.0	Rango de direcciones IP 128.0.0.0 a 191.255.0.0	Rango de direcciones IP 192.0.0.0 a 223.255.255.0	Rango de direcciones IP 224.0.0.0 a 239.255.255.255	Rango de direcciones IP 240.0.0.0 a 254.255.255.255
Máscara de red 255.0.0.0 /8	Máscara de red 255.255.0.0 /16	Máscara de red 255.255.255.0 /24	Máscara de red Uso Multicast o multidifusión	Máscara de red Experimental
Dirección Privada 10.0.0.0 a 10.255.255.255	Dirección Privada 172.16.0.0 a 172.31.255.255	Dirección Privada 192.168.0.0 a 192.168.255.255	Dirección Privada Uso Multicast o multidifusión	Dirección Privada Experimental

Fuente: Elaboración Propia

3.8.2.4 Direcciones Reservadas IPv4

Hay determinadas direcciones, que no pueden asignarse a los hosts por varios motivos. También hay direcciones especiales que pueden asignarse a los hosts, pero con restricciones en la interacción de dichos hosts dentro de la red, la cuales son:
(Ariganello, 2020)

1) Direcciones de Red y de Broadcast

No es posible asignar la primera ni la última dirección a los hosts dentro de cada red. Estas son respectivamente, la dirección de red y la dirección de broadcast del rango de host (Ariganello, 2020).

2) Ruta Predeterminada

La ruta predeterminada IPv4 se representa como 0.0.0.0. La ruta predeterminada se usa como ruta por defecto cuando no se dispone de una ruta más específica, el uso de esta dirección también reserva todas las direcciones en el bloque de direcciones 0.0.0.0 al 0.255.255.255 (0.0.0.0 /8).

3) Loopback

Es una de las direcciones reservadas IPv4. La dirección de loopback 127.0.0.1 es una dirección especial que los hosts utilizan para dirigir el tráfico hacia ellos mismos. La dirección de loopback crea un método de acceso directo para las aplicaciones y servicios TCP/IP que se ejecutan en el mismo dispositivo para comunicarse entre sí. Al utilizar la dirección de loopback en lugar de la dirección host IPv4 asignada, dos servicios en el mismo host pueden desviar las capas inferiores de la pila TCP/IP. También es posible hacer ping a la dirección de loopback para probar la configuración de TCP/IP en el host local (Ariganello, 2020).

4) Direcciones link-local

Las direcciones IPv4 del bloque de direcciones desde 169.254.0.0 hasta 169.254.255.255 (169.254.0.0 /16) se encuentran designadas como direcciones link-local. El sistema operativo puede asignar automáticamente estas direcciones al host local en entornos donde no se dispone de una configuración IP. Se puede usar en una red de

punto a punto o para un host que no pudo obtener automáticamente una dirección de un servidor de protocolo de configuración dinámica de host (DHCP**).**

(Ariganello, 2020)

6) Encabezado de paquetes IPv4

El encabezado de paquetes IPv4 consta de campos que contienen información importante sobre el paquete. IPv4 se utiliza desde 1983, cuando se implementó en la Advanced Research Projects Agency Network (ARPANET, Red de la Agencia de Proyectos de Investigación Avanzada), que fue la precursora de Internet. Internet se basa en gran medida en IPv4, que continúa siendo el protocolo de capa de red que más se utiliza.

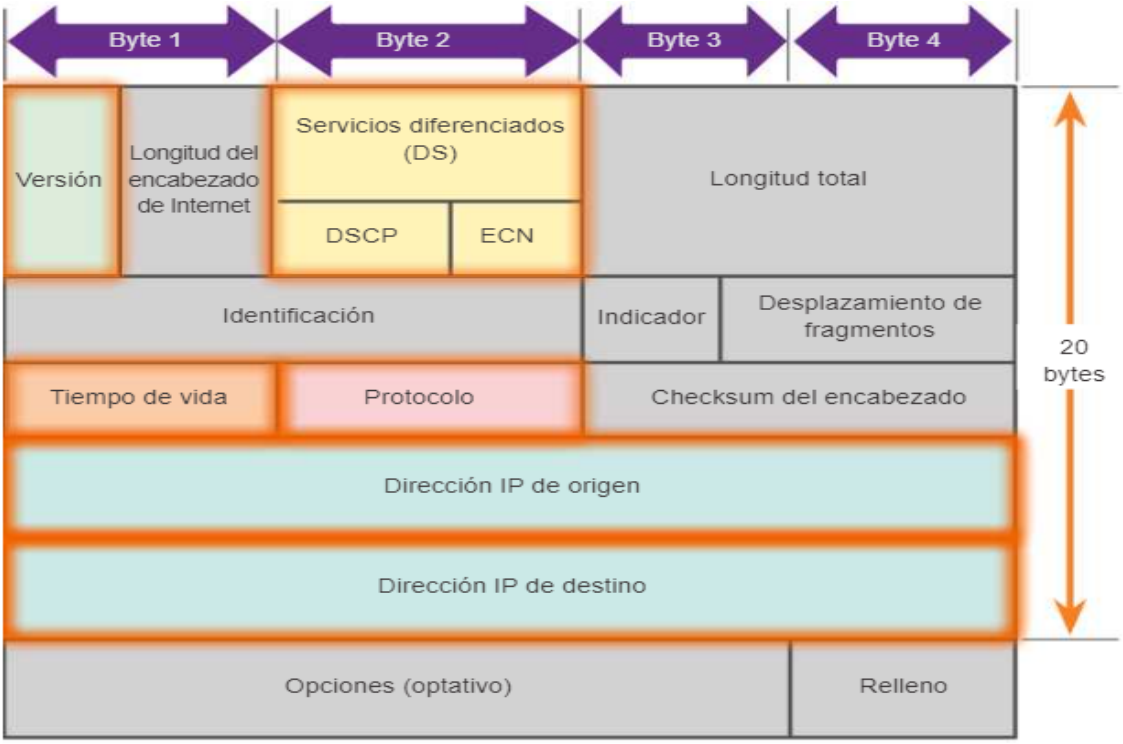
Los paquetes IPV4 tienen dos partes:

- Encabezado IP: Identifica las características del paquete.
- Contenido: Contiene la información del segmento de capa 4 y los datos propiamente dichos.

Como se muestra en la ilustración, los encabezados de paquetes IPV4 constan de campos que contienen información importante sobre el paquete. Estos campos contienen números binarios que se examinan en el proceso de capa 3. Los valores binarios de cada campo identifican las distintas configuraciones del paquete IP.

(Curso Oficial Cisco, 2015)

Figura N°34
Encabezado IPv4



Fuente: Curso Netcad Cisco
http://itroque.edu.mx/cisco/cisco1/course/module6/6.1.3.1/6.1.3.1.html

Los campos importantes del encabezado de IPv4 incluyen los siguientes:

a) Versión. - Contiene un valor binario de 4 bits que identifica la versión del paquete IP, para los paquetes IPv4, este campo siempre se establece en 0100.
b) Servicios diferenciados (DS). - Anteriormente denominado “Tipo de servicio” (ToS), se trata de un campo de 8 bits que se utiliza para determinar la prioridad de cada paquete. Los primeros 6 bits identifican el valor del punto de código de servicios diferenciados (DSCP), utilizado por un mecanismo de calidad de servicio (QoS).
Los últimos 2 bits identifican el valor de Notificación explícita de congestión (ECN), que se puede utilizar para evitar que los paquetes se descarten durante momentos de congestión de la red.

c)Tiempo de vida (TTL). -Contiene un valor binario de 8 bits que se utiliza para limitar la vida útil de un paquete. Se especifica en segundos, pero comúnmente se denomina "conteo de saltos". El emisor del paquete establece el valor inicial de tiempo de vida (TTL), el que disminuye un punto por cada salto, es decir, cada vez que el paquete es procesado por un router. Si el campo TTL disminuye a cero, el router descarta el paquete y envía un mensaje del protocolo de mensajes de control de Internet (ICMP) de Tiempo superado a la dirección IP de origen. El comando traceroute utiliza este campo para identificar los routers utilizados entre el origen y el destino.

d) Protocolo. -Este valor binario de 8 bits indica el tipo de contenido de datos que transporta el paquete, lo que permite que la capa de red pase los datos al protocolo de capa superior correspondiente. Los valores comunes incluyen ICMP (1), TCP (6) y UDP (17).

e) Dirección IP de origen. - Contiene un valor binario de 32 bits que representa la dirección IP de origen del paquete.

f) Dirección IP de destino: Contiene un valor binario de 32 bits que representa la dirección IP de destino del paquete.

Los dos campos que más comúnmente se toman como referencia son las direcciones IP de origen y de destino. Estos campos identifican de dónde proviene el paquete y adónde va. Por lo general, estas direcciones no se modifican durante la transferencia desde el origen hasta el destino.

(Ariganello, 2020)

3.8.3 Direccionamiento IPv6

IPv6 ha estado en desarrollo desde mediados de los 90 y durante varios años. Se había anunciado al principio como el protocolo que podría expandir el direccionamiento IP, llevar IP mobile a la madurez y finalmente ser capaz de incorporar seguridad a nivel de capa 3. Esas afirmaciones son correctas, pero hay que tener en cuenta que a nivel de capa 3 esas capacidades de IPv6 han sido aportadas a IPv4 en los pasados años. Actualmente las direcciones IPv4 son escasas y la mayor razón en Internet para

evolucionar a IPv6 es la necesidad de un mayor direccionamiento, esta necesidad de direccionamiento IP podría ser atenuada intentando utilizar CIDR, VLSM, NAT y asignaciones temporales a través de DHCP, pero teniendo sistemas intermedios manipulando los paquetes complican el diseño y la resolución de problemas. El concepto del diseño de Internet con innumerables sistemas intermedios no hace que NAT trabaje adecuadamente, sin embargo, es un mal necesario. La longitud de una dirección IPv6 es lo primero que sale a relucir, son 128 bits lo que hace 2 128 direcciones IPv6 disponibles, varias de estas direcciones dan funciones especiales y están reservadas, pero aun así quedarían disponibles aproximadamente 5x10 28 direcciones IP por cada habitante del planeta. Lo que permitiría que el direccionamiento pueda crecer sin preocupaciones en contraposición al direccionamiento IPv4 cuya cantidad está limitada a 2 ^ 32. En IPv6 se utiliza una cabecera más simplificada que IPv4, haciendo que el procesamiento sea más eficiente, permitiendo un mecanismo más flexible y a su vez extensible a otras características. Una de esas características es la movilidad, mobile IP es un estándar de la IETF que permite a los usuarios con dispositivos wireless estar conectados de manera transparente y moverse a cualquier sitio sin restricciones.

La seguridad es otro tema importante añadido, IPsec está presente en cada uno de los dispositivos IPv6.

(Ariganello, 2020)

3.8.3.1 Formato del direccionamiento IPv6

La primera diferencia respecto a IPv4 es que las direcciones IPv6 son de 128 bits y están representadas en un formato hexadecimal en lugar de la notación decimal tradicional y separada cada parte por dos puntos en lugar de uno. Teniendo de esta forma 8 partes de 16 bits cada una. Como cada dígito hexadecimal se asocia con 4 bits, cada campo de 16 bits será de 4 dígitos hexadecimales.

Un ejemplo de dirección IPv6 puede ser el siguiente:

2001:0000:0001:0002:0000:0000:0000:ABCD

Este formato se puede reducir hasta de optimizar la lectura para su comprensión. Hay dos formas para conseguir simplificar tanta cantidad de números:

- Todos los 0 a la izquierda de cada uno de los campos pueden ser omitidos.

  2001:0:1: 2:0:0:0: ABCD

- Se pueden omitir los campos consecutivos de 0 con "::" independientemente de la cantidad de campos que se abrevie. Este mecanismo solo puede hacerse una vez debido a que luego no se podrían reestructurar la cantidad de campos exactamente como eran.

  2001:0:1:2::ABCD

(Ariganello, 2020)

3.8.3.2 Prefijos

Los primeros 48 bits de una dirección IPv6 componen la dirección de red, dicho de otra forma, los primeros 3 grupos de la dirección (cada grupo es de 16 bits o 4 caracteres hexadecimales). Por lo general, los ISP de cada región asigna una dirección de red, la cual subdividirán entre todos sus clientes. Los siguientes 16 bits, o el cuarto grupo de caracteres hexadecimales conforman la dirección de subred, esto hace que IPv6 sea mucho más eficiente a nivel de comunicaciones, puesto que la dirección contiene la información de origen y destino sin necesidad de hacer cálculos para averiguarlo o tener que modificar la información transmitida. La dirección única del dispositivo representa los últimos 64 bits de la dirección, o los últimos 4 grupos. Este es el identificador único del dispositivo, algunos dispositivos utilizan la propia dirección física (MAC).

Es posible combinar el prefijo de red y el identificador de la interfaz en una sola notación, la representación de prefijos de red en IPv6 es similar a la notación utilizada en CIDR para los prefijos IPv4, es decir, dirección-IPv6/, longitud del prefijo en bits.

Se permite el uso de formatos abreviados con "::", a continuación, se mostrarán un ejemplo:

2001:0DB8:7654:3210:0000:0000:0000:0000/64

2001:DB8:7654:3210:0:0:0:0/64

2001:DB8:7654:3210::/64

Por lo tanto, esta dirección IPv6 indica que el prefijo de red está constituido por los primeros 64 bits. No existen tienen reglas para la asignación de identificadores de subred (SID) dentro de un sitio. Se pueden utilizar varios métodos como, por ejemplo:

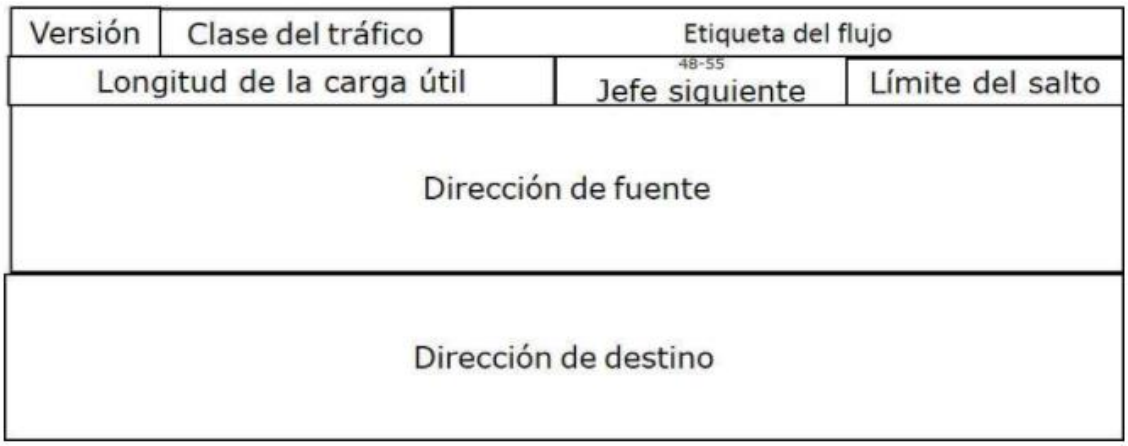
- Enumerar de forma incremental las subredes: 0001, 0002, ... Esta técnica es fácil de implementar en las redes experimentales, pero puede dar lugar a un esquema de direccionamiento plano, difícil de recordar.
- Utilizar el número de VLAN. Permite no tener que memorizar múltiples niveles de numeración.
- Separar los tipos de redes y utilizar las cifras a la izquierda para designarlos. Esta técnica facilita las reglas de filtrado, utilizando al mismo tiempo reglas adecuadas para la gestión de estas subredes en el segmento del lado derecho.

(Ariganello, 2020)

3.8.3.3 Cabecera IPv6

La cabecera IPv6 es optimizada como se muestra en la figura, para procesadores de 32 a 64 bits y las extensiones de cabecera permiten la expansión sin tener que forzar a que los campos que no se usan se estén transmitiendo constantemente. Las principales diferencias entre las cabeceras de las dos versiones es la longitud de los campos de origen y destino. También hay otros campos que son aparentes como checksum, fragmentación y la etiqueta de flujo.

Figura N°35
Encabezado IPv6



Fuente: Modelo OSI
https://www.tutorialspoint.com/es/ipv6/ipv6_headers.htm

Los campos en una cabecera IPv6 son los siguientes:

Versión. - Es un campo de 4 bits que identifica la versión, en este caso a 6.

Clase de Trafico (8 bits). - Similar al campo 2 de IPv4, se utiliza para calidad de servicio.

Etiqueta del Flujo. - Campo de 20 bits que permite que el tráfico sea etiquetado para que se pueda manejar de manera más rápida flujo por flujo.

Longitud de Carga útil. - Campo de 16 bits con la longitud del campo de datos.

Next Header. - Similar al campo de protocolo en la cabecera IPv4. Es un campo de 8 bits que indica cómo los campos después de la cabecera básica de IPv6 deberían ser interpretados. Podría indicar, por ejemplo, que el siguiente campo es TCP o UDP ambos relativos a la capa de transporte o podría indicar que existe una extensión de la cabecera.

Hop Limit. - Similar al campo TTL en IPv4, es de 8 bits y se incrementa por cada router intermediario para prevenir bucles, de tal manera que cuando la cuenta llegue a 0 será descartado. Cuando esto ocurre se envía un mensaje de notificación al origen.

Source Address y Destination Address. - Estos campos de 128 bits son las direcciones IPv6 de origen y de destino de los dispositivos que se están comunicando.

Extension Headers. -Permite agregar más campos opcionales:

- Hop by Hop options: Utilizados para routers intermediarios.
- Destination options. - Opciones para el nodo final.
- Routing. -Utilizado para especificar a los routers intermedios qué ruta tienen que incluir. El efecto final es forzar el enrutamiento por un camino predefinido.

Fragment. - Utilizado para dividir los paquetes que son demasiado largos para la MTU. Esta cabecera reemplaza los campos de fragmentación de la cabecera IPv4.

Authentication y Encapsulating Security Payload (ESP). -Se utiliza por IPsec para proporcionar autenticación, integridad y confidencialidad de los paquetes. AH y ESP son idénticos en IPv4 y en IPv6 (Ariganello, 2020).

3.8.3.4 Tipos de direccionamiento IPv6

IPv6 reconoce tres tipos de direcciones: unicast, multicast y anycast. El tipo de dirección define el destino de la comunicación, es decir, a cuántos receptores debe ser entregado el paquete.

1) Unicast

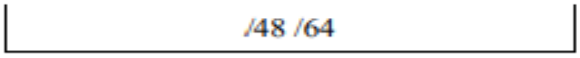
Identifica de manera única una interfaz. Un paquete enviado a ese tipo de dirección será entregado a la interfaz correspondiente. Entre las direcciones unicast, se pueden distinguir aquéllas que tienen una cobertura global, es decir, designan sin ambigüedad un destinatario sobre Internet, y las que tienen cobertura local. Estas últimas no pueden ser enrutadas sobre Internet. Es decir, un paquete que tenga una dirección destino con cobertura local, será ignorado y eliminado por un router de Internet.
(Ariganello, 2020)

2) Global-Unicast

La escalabilidad de la red es sumamente importante, es directamente proporcional a la capacidad de sumarización que tiene la red. Tal como ocurre con IPv4 los bits más a la izquierda indican el prefijo de enrutamiento y pueden ser sumarizados. Teóricamente existen 2^64 prefijos IPv6. Si cada prefijo fuera almacenado en la memoria del router

utilizando 256 bits (32 bytes), entonces la tabla de enrutamiento consumiría 5.9x10^20 bytes, lo cual es demasiado. Esto se reduce a la importancia que tiene la sumarización al momento de construir la tabla de enrutamiento. La siguiente figura muestra un esquema de una dirección Global IPv6, definida por la RFC 3587**:**

Figura N°36
Esquema de Dirección Global Ipv6



Fuente: Redes Cisco, Ernesto Ariganello

Los primeros 48 bits de la dirección Global IPv6 son utilizados para enrutamiento en Internet en el ISP, los siguientes 16 bits forman el sub-net ID permitiendo así a una empresa subdividir su red. Los restantes 64 bits son la interfaz ID en formato EUI-64.

IANA está asignando direcciones que comienzan con el valor binario 001 o en hexadecimal 2000::/3. Este direccionamiento está designado para direcciones globales IPv6 unicast, este es una octava parte del espacio total del direccionamiento IPv6. IANA utiliza el rango 2001::/16 para registros, que normalmente tienen un rango /23 y asigna un rango /32 a los ISP.

Por ejemplo, un ISP podría disponer a una organización de la siguiente dirección 2001:0:1AB::/48. En una subred 5 el prefijo sería 2001:0:1AB:5::/64, con un dispositivo final que tiene una dirección MAC 00-0f-66-81-19-a3, el formato EUI-64 de la interfaz ID será 020F:66FF:FE81:19A3.

Y finalmente, la dirección IPv6 completa será:

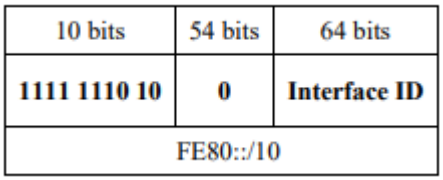
2001:0:1AB:5:20F:66FF:FE81:19A3

(Ariganello, 2020)

3) Link Local

Las direcciones unicast de IPv6 locales (Link local) permiten a dispositivos que estén en la misma red local ser capaces de comunicarse sin necesidad de asignación de un direccionamiento global. Las direcciones locales son utilizadas para el enrutamiento y por los procesos de descubrimiento entre protocolos. Son auto- configuradas utilizando el prefijo FE80::/10 más el formato EUI-64 ID, según muestra la siguiente figura: (Ariganello, 2020)

Figura N°37
Formato EUI- 64 ID



10 bits	54 bits	64 bits
1111 1110 10	**0**	**Interface ID**
FE80::/10		

Fuente: Redes Cisco, Ernesto Ariganello

Por ejemplo, una MAC 00-0f-66-81-19-a3 tendrá una dirección IPv6 Local FE80::020F:66FF:FE81:19A3.

4) Unique Local

El RFC 4193 define un nuevo formato de dirección unicast, las direcciones locales únicas (ULA, Unique Local Address). Estas direcciones son para uso local. No están pensadas para ser enrutadas en Internet, sino dentro de un área acotada, como un sitio o un número limitado de sitios. Con un prefijo de 48 bits, pueden ser manipuladas como las direcciones globales, con un identificador de Subred (SID) de 16 bits y un identificador de interfaz (IID) de 64 bits. Las direcciones locales únicas se crean utilizando un identificador global (Global ID) generado de forma pseudoaleatoria. Estas direcciones tienen el formato siguiente:

- Prefix (7 bits): FC00::/7 prefijo para identificar las direcciones IPv6 locales (ULA).
- L (1 bit): Puesto a 1, el prefijo es asignado localmente. El valor 0 está reservado para usos futuros.
- Global ID (40 bits): Identificador global utilizado para la creación de un prefijo "único" (Globally Unique Prefix).
- Subnet ID (16 bits): Identificador de subred al interior del sitio.
- Interface ID (64 bits): El identificador de interfaz

5) Multicast

Una dirección multicast designa a un grupo de interfaces que pertenecen, en general, a nodos distintos que pueden ubicarse en cualquier parte de Internet. Cuando un paquete tiene una dirección destino multicast, éste se envía por la red a todas las interfaces miembros de ese grupo. Cabe resaltar que desaparecen las direcciones de broadcast (difusión) que existían en IPv4; éstas son remplazadas por direcciones tipo multicast. La dirección de difusión puede ser imitada por una dirección multicast constituyendo un grupo que incluya todos los nodos. La ausencia de direcciones de difusión evita los problemas de saturación en las redes locales conmutadas. Por este motivo una red IPv6 tiene un mejor desempeño sobre este tipo de redes.

El formato de una dirección IPv6 de multicast se ilustra en la siguiente figura:

Figura N°38

Formato de una Dirección IPv6 Multicast

8 bits	4 bits	4 bits	112 bits
1111 1111	**Flag**	**Scope**	**Group ID**
FF00::/8			

Fuente: Redes Cisco, Ernesto Ariganello

Como se muestra en la figura la dirección IPv6 multicast comienza con el prefijo FF00::/8 los siguientes 4 bits son identificadores que se describen a continuación:

1. El primer identificador o bandera es indefinido y siempre tiene el valor de cero.
2. Conocido como el bit “R” tiene el valor en binario de 1, cuando el RP esté contenido en el paquete multicast.
3. Conocido como el bit “P” lleva el valor binario 1 en el caso de que la dirección multicast esté basada en un prefijo unicast.
4. Es el llamado bit “T”, si la dirección está asignada permanentemente lleva el valor 0, si por el contrario el valor es 1 la dirección es temporal.

Los 4 bits después de las banderas indican el ámbito de la dirección limitando cuán lejos esta dirección multicast es capaz de llegar. En IPv4 se utiliza el TTL para poder efectuar esta tarea, pero no es un mecanismo exacto debido a que la distancia permitida por el TTL puede ser demasiado larga en una dirección y demasiado corta en otra. El ámbito en IPv6 es lo suficientemente flexible como para limitar multicast en un sitio o una empresa determinada.

El ID del grupo multicast son los 112 bits de menor ámbito de la dirección. Todos los dispositivos deberían reconocer y responder a estas direcciones multicast de todos los nodos:

- FF01::1 correspondiente a la interfaz local.
- FF02::1 correspondiente al enlace local.

Las direcciones de multicast solicited-nodes son utilizadas en los mensajes de solicitud de vecinos y son enviadas en un enlace local por un dispositivo que quiere determinar la dirección de la capa de enlace de otro dispositivo en el mismo enlace local. Este mecanismo se asemeja a ARP en IPv4. Una dirección de multicast solicited-nodes comienza con el prefijo FF02::1:FF00:/104 y en los últimos 24 bits insertando las direcciones unicast o anycast del dispositivo. Los routers deben poder responder a las direcciones multicast all-router:

- FF01::2 es la dirección de interfaz local.
- FF02::2 es la dirección de enlace local.
- FF05::2 es la dirección del sitio local.

Los routers también se unen a otros grupos para soportar protocolos de enrutamiento como, por ejemplo, OSPF versión 3 (OSPFv3) utiliza FF02::5 y FF02::6, y RIPng (Routing Information Protocol new generation) utiliza FF02::9.
(Ariganello, 2020)

6) Anycast

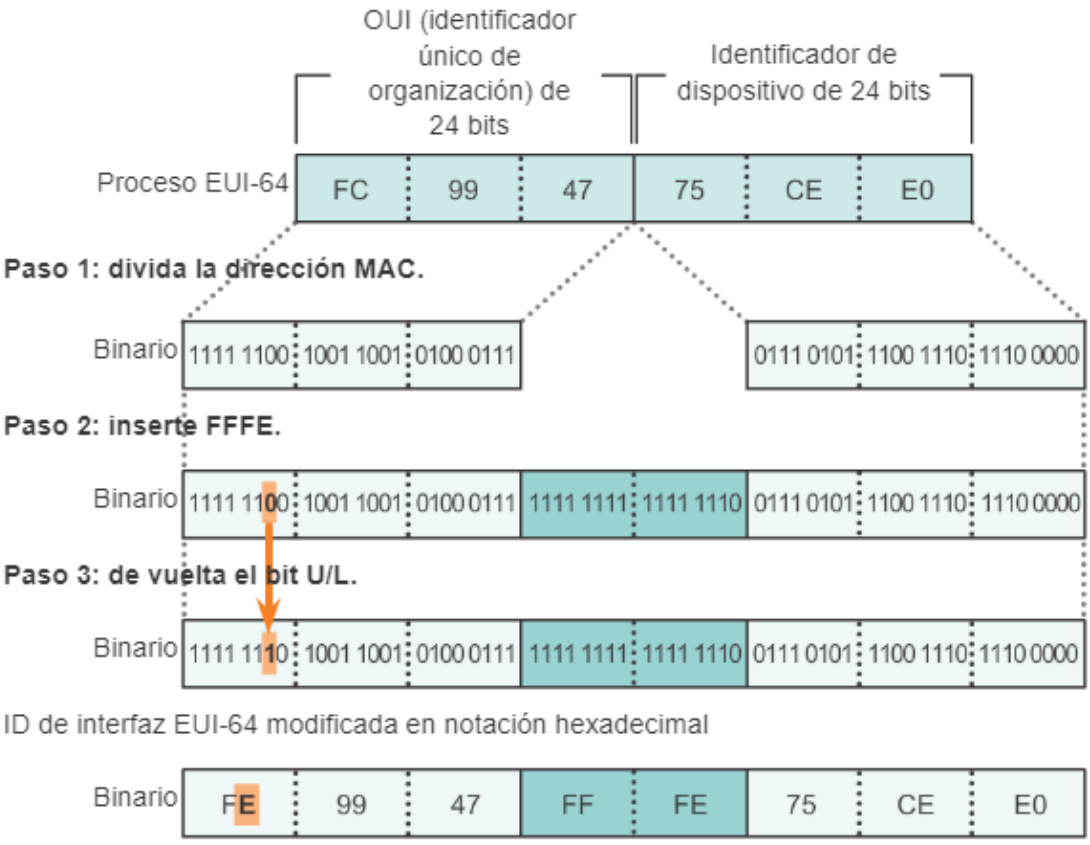
El último tipo de dirección, anycast, se deriva de la oficialización de propuestas hechas para IPv4 (RFC 1546). Como en el caso multicast, una dirección de tipo anycast designa un grupo de interfaces. La principal diferencia consiste en que cuando un paquete tiene una dirección destino anycast, éste es enviado a alguno de los miembros del grupo, no a todos. El receptor del paquete podría ser, por ejemplo, el más cercano de acuerdo a la métrica de usada por los protocolos de enrutamiento. Este tipo de dirección es principalmente experimental.

7) EUI – 64

Los ID de una dirección IPv6 son utilizados para identificar de manera única una interfaz, este segmento de la dirección es llamado porción de host. Estos ID deben ser únicos en los enlaces, tienen una longitud de 64 bits y pueden ser creados dinámicamente basándose en la dirección de la capa de enlace. El tipo de capa de enlace determinará cómo son dinámicamente creadas las interfaces de IPv6 y cómo funcionará la resolución del direccionamiento. Para Ethernet la interfaz ID está basada en la dirección MAC de la interfaz en un formato llamado EUI-64 (Extended Universal Identifier 64-bit). Este formato deriva de la dirección MAC de 48 bits con el agregado de los números hexadecimales FFFE entre el OUI y el código de vendedor. El séptimo bit del primer byte del ID de la interfaz resultante corresponde al bit universal local (U/L) asume el valor binario 1. Este bit indica si la interfaz ID es localmente única en ese enlace o universalmente única. El octavo bit en el primer byte de la interfaz ID

corresponde al individual/group (I/G) que se utiliza para gestionar grupos multicast, en este caso no varía. (Ariganello, 2020)

Figura N°39
Proceso EUI - 64



Fuente: Curso Netcad Cisco
http://itroque.edu.mx/cisco/cisco1/course/module8/8.2.4.5/8.2.4.5.html

3.8.3.5 Asignación de direcciones IPv6

Las direcciones IPv6 pueden ser asignadas de manera manual o de forma dinámica usando DHCPv6 o autoconfiguración stateless.

3.8.3.5.1 Manual

El administrador es el encargado de asignarlas y configurarlas manualmente, supone más trabajo y demanda llevar un registro de las direcciones que han sido asignadas y a qué host.

3.8.3.5.2 SLAAC (Stateless Address Autoconfiguration)

Cada router anuncia información de red incluyendo el prefijo asignado a cada una de sus interfaces. Con la información contenida en este anuncio los sistemas finales crean una dirección única al concatenar el prefijo con el ID en formato EUI-64 de la interfaz. El nombre stateless viene de que ningún dispositivo lleva un registro de las IP que se van asignando. Los sistemas finales piden información de red al router usando un mensaje específico denominado Router Solicitation y los routers responden con un mensaje Router Advertisement. Existe un proceso denominado DAD (Duplicate Address Detection), que se encarga de verificar que las IPs no estén en uso, no sean duplicadas.

3.8.3.5.3 DHCPv6

Se puede definir este método como autoconfiguración stateful y el funcionamiento es similar a DHCP tradicional, asignando direccionamiento a los hosts de un rango preconfigurado. Tiene una ventaja añadida y es que rompe la relación entre MAC e IP (capa 2 y 3) creada si se utiliza la autoconfiguración stateless, aumentando la seguridad.

3.8.3.6 Transición de IPv4 a IPv6

Muchos de los actuales dispositivos de red requieren para su funcionalidad la utilización e implementación de IPv6. Sin embargo y por diferentes razones muchas empresas no pueden cambiar fácilmente de IPv4 a IPv6. Este proceso de migración puede llevar un largo período de cambios y transformaciones por lo que durante esta fase pueden coexistir ambas versiones de IP**.** (Ariganello, 2020)

1) Dual Stack

Con este mecanismo es posible ejecutar IPv4 e IPv6 a la vez sin comunicación entre ambas versiones. Los hosts y los routers llevan configuraciones de las dos versiones de IP y utilizan independientemente unas u otras según los recursos que quieran alcanzar. Si un recurso en concreto proporciona ambas versiones sería conveniente utilizar IPv6 para alcanzarlo. Este mecanismo de dualidad permite a los servidores, clientes y aplicaciones moverse gradualmente hacia el nuevo protocolo provocando un mínimo impacto durante el proceso de transición a IPv6. La mayor desventaja de esta tecnología, es que requiere que todo el equipamiento soporte ambos protocolos, lo cual no es la situación real. (Ariganello, 2020)

2) Tuneles

El mecanismo que proporciona dual stack funciona correctamente siempre y cuando la infraestructura pueda soportar los dos protocolos, pero hay casos en los que los dispositivos sólo soportan IPv4, como por ejemplo en equipos de core. Hasta que estos equipos sean actualizados se debe utilizar otro tipo de técnica que pueda ejecutar IPv6 a través de IPv4. Utilizando túneles los routers que están ejecutando a la vez IPv4 e IPv6 encapsularán el tráfico IPv6 dentro de paquetes IPv4. El origen de los paquetes IPv4 es el propio router local y el destino será el router en el extremo del túnel. Cuando el router destino recibe el paquete IPv4 lo desencapsula y hace un reenvío del tráfico IPv6 que estaba encapsulado. (Ariganello, 2020)

En la actualidad, Internet es básicamente una red IPv4 con algunas islas IPv6; por lo tanto, lo más frecuente es que el tráfico IPv6 viaje encapsulado en paquetes IPv4. Los siguientes son algunos de los tipos de túneles más comunes:

2-1) Configuración Manual

El túnel se crea manualmente, IPv6 es el protocolo pasajero siendo IPv4 el encargado de encapsular y transportar a IPv6.

2-2) 6-to-4

Permite tráfico IPv6 sobre una red IPv4 sin la necesidad de configurar túneles de forma explícita, aunque se mantiene la función de encapsulamiento de IPv6 en IPv4. Los

túneles 6-to-4 utilizan direcciones IPv6 que enlazan las direcciones 2002::/16 con la dirección IPv4 de 32 bits del router borde creando un prefijo de 48 bits.

2-3) Teredo

Encapsulan paquetes IPv6 en segmentos IPv4 UDP y trabajan de manera similar a los otros mecanismos anteriores con el agregado de poder atravesar redes que están utilizando NAT y firewall. La RFC 4380 describe el funcionamiento de este mecanismo.

2-4) Isatap (Intra-Site Automático Tunnel Addressing Protocol)

Trata la red como una NBMA de IPv4 y permite a la red privada IPv4 implementar incrementalmente IPv6 sin actualizar la red. La RFC 4214 describe el funcionamiento de ISATAP. (Ariganello, 2020)

3) Traducción

El problema del mecanismo de túneles, ya sea manual o automático, es que termina siendo una solución del tipo dual stack. Los clientes IPv6 tienen que seguir soportando IPv4 para conectar con otros dispositivos IPv4. La traducción de direcciones es un tipo de solución diferente que permite a dispositivos IPv6 comunicarse con dispositivos IPv4 sin necesidad de dependencia dual stack. Algunas de las técnicas de traducción más empleadas son:

- SIIT (Stateless IP/ICMP Translation): Realiza traducción de encabezados IPv6 a IPv4 y viceversa.
- NAT64: Mecanismo que permite a los hosts IPv6 comunicar con hosts IPv4. Puede implementarse en modo stateless según la RFC6145 o stateful según la RFC6146.
- Stateless NAT64: Mecanismo de traslación de direcciones IPv6 a IPv4, pero garantizando correspondencia 1 a 1, en lugar de usar correspondencia 1 a muchos como en el NAT stateful.

Los dominios de enrutamiento IPv4 e IPv6 también pueden estar conectados a través de un Proxy usando ALG (Application-Level Gateways). Un Proxy intercepta tráfico y lo

convierte al protocolo correspondiente. Un ALG independiente será necesario para soportar cada protocolo, de esta manera este método solo soluciona algunos problemas específicos de la traducción de direcciones.

(Ariganello, 2020)

CAPITULO IV

INGENIERIA DEL PROYECTO

4.1 Ingeniería del Proyecto

El presente proyecto se enfoca específicamente en la aplicación de un sistema de seguridad en la red internet que es denominada insegura, así la Institución Financiera Prendamas podrá realizar la transmisión de datos de forma segura en la red internet entre sus diferentes sucursales en la ciudad de La Paz.

4.1.1 Distribución de Sitios

Al empezar el presente proyecto se definió que el sistema de seguridad denominado Tunnel Gre de Cisco se aplicara en la Institución Financiera Prendamas, se sabe que esta institución es a nivel nacional, pero para fines del proyecto tomaremos las oficinas ubicadas en la ciudad de La Paz.

Así que este sistema de seguridad se aplicara en las siguientes sucursales:

Figura N°40

Sucursal Plaza del Estudiante

Dirección

Plaza del Estudiante N º 221

Fuente: Elaboración Propia

Figura N°41
Sucursal La Ceja

Dirección

Av. Jorge Carrasco N º 509, entre calles 4 y 5. Zona 12 de octubre

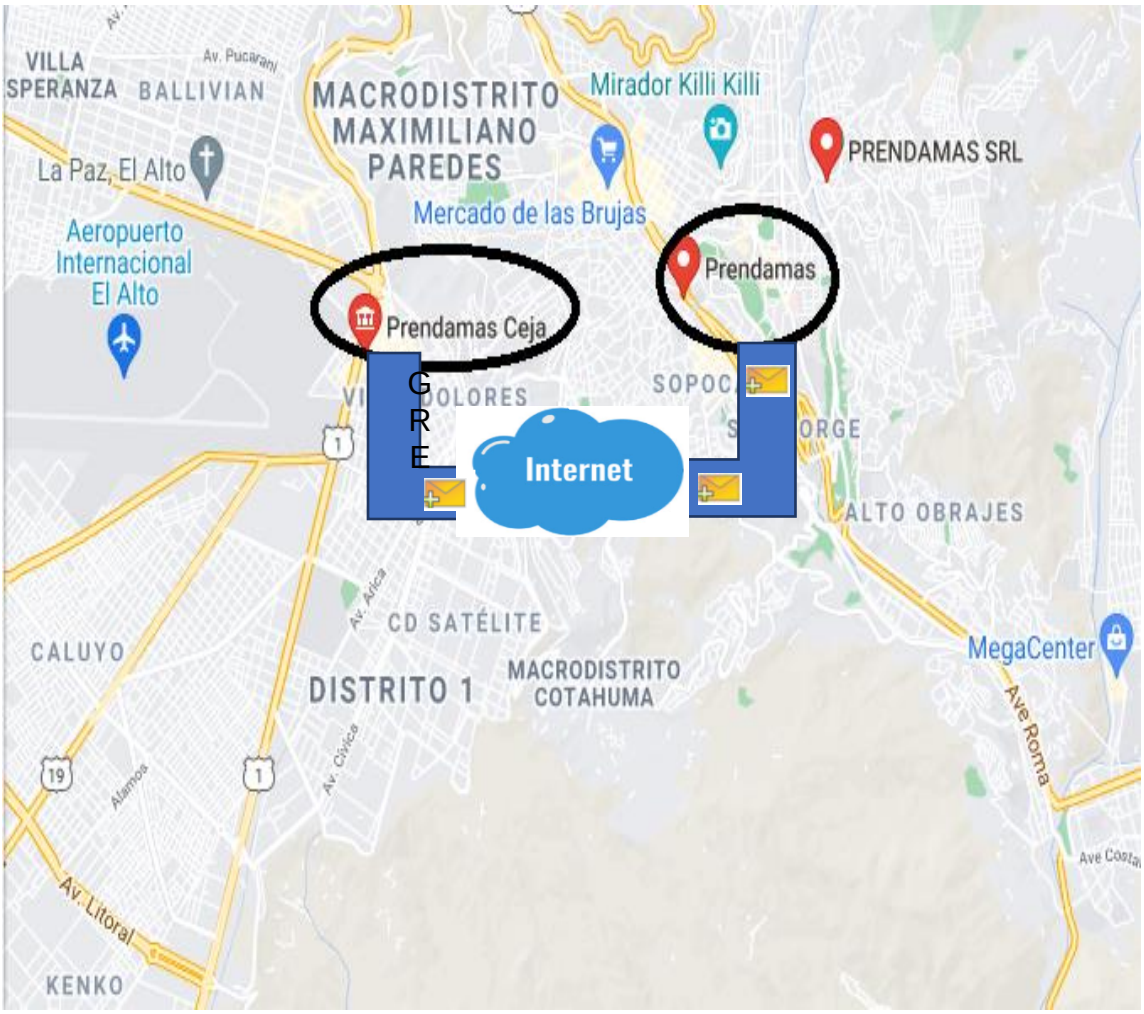
Fuente: Elaboración Propia

4.1.2 Ubicación Geográfica de las Sucursales

En la siguiente imagen se puede observar el lugar geográfico de las sucursales de la Institución Financiera Prendamas donde se realizará la aplicación del Tunnel Gre de Cisco realizando la programación adecuada en los routers de cada sucursal en IPv6.

También en la imagen se puede observar una pequeña idea de cómo funcionara el Tunnel Gre para brindar seguridad en la red internet cuando realice la transmisión de datos.

Figura N°42
Ubicación de Sucursales



Fuente: Elaboración Propia

4.2 Descripción del Tunnel Gre

4.2.1 Características

GRE es un protocolo de tunneling de sitio a sitio básico que puede encapsular una amplia variedad de tipos de paquete de protocolo dentro de túneles IP, lo que permite que una organización entregue otros protocolos mediante una WAN basada en IP.

Como se muestra en la figura 43, una interfaz de túnel admite un encabezado para cada uno de los siguientes protocolos:

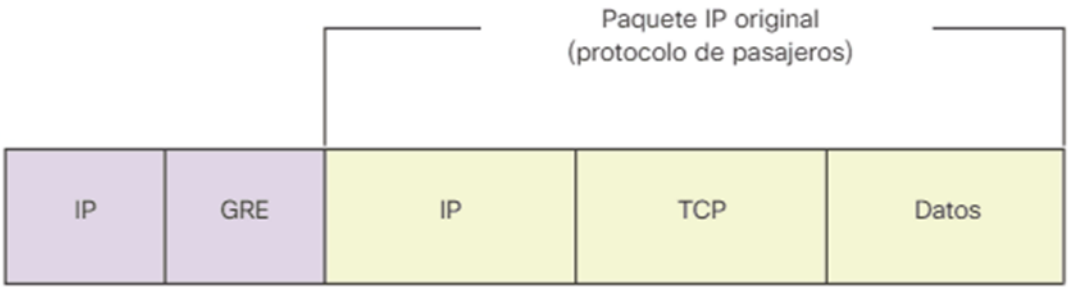
• Un protocolo encapsulado, como IPv4, IPv6, AppleTalk, Decnet o IPx.

•Un protocolo de encapsulación (o portadora), como GRE

•Un protocolo de entrega de transporte, como IP que es el protocolo que transporta al protocolo encapsulado

Figura N°43

Encapsulación de enrutamiento genérico (Gre)



Fuente: https://ccnadesdecero.es/tuneles-gre-caracteristicas-cisco

4.2.2 Funcionamiento

En la actualidad GRE se considera una red privada que crea con tunneling a través de una red pública. Mediante la encapsulación, un túnel GRE crea un enlace virtual punto a punto a los routers Cisco en puntos remotos a través de una internetwork IP. Además, GRE admite el tunneling de multidifusión IP.

GRE está diseñada para administrar el transporte del tráfico multiprotocolo y de multidifusión IP entre dos o más sitios, que probablemente solo tengan conectividad IP. Puede encapsular varios tipos de paquete de protocolo dentro de un túnel IP, a continuación, podremos observar una figura sobre el Tunnel Gre.

Figura N°44
Tunnel Gre

Fuente: https://ccnadesdecero.es/tuneles-gre-caracteristicas-cisco

4.2.3 Ventajas

Las ventajas de GRE son que se puede utilizar para canalizar el tráfico que no es IP a través de una red IP, lo que permite la expansión de la red mediante la conexión de subredes multiprotocolo en un entorno de backbone de protocolo único. Además, GRE admite el tunneling de multidifusión IP.

4.3 Descripción Técnica de la Red LAN de cada Sucursal

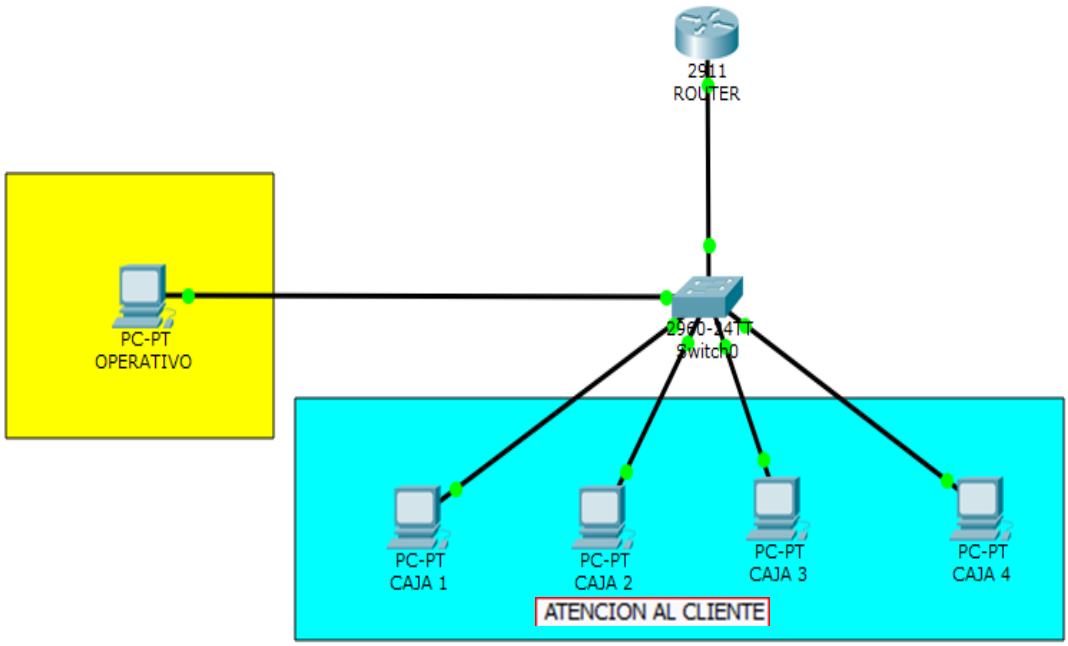
Cada sucursal es diferente en su red LAN dependiendo con la cantidad de equipos con los que cuenten, pero en la mayoría de todos, el cuarto de telecomunicaciones de cada sucursal es el mismo ya que cuentan en el Rack con un Router 2911 y un Switch de 24 interfaces ambos de marcas cisco. Este switch es suficiente para cada sucursal debido a que su red LAN no es muy extensa.

Los equipos tienen una dirección IPv4 y el Router está programado también en IPv4.

4.3.1 Infraestructura de la Red LAN - Sucursal Plaza del Estudiante

Esta sucursal cuenta con 4 cajas de atención al cliente y un operativo que esta de encargado del funcionamiento de los servicios que ofrece Prendamas. El switch catalyst 2060 tiene 24 interfaces de los cuales 6 interfaces están ocupadas eso nos quiere decir que esta red es escalable tiende a crecer.

Figura N°45
Red LAN - Sucursal Plaza del Estudiante

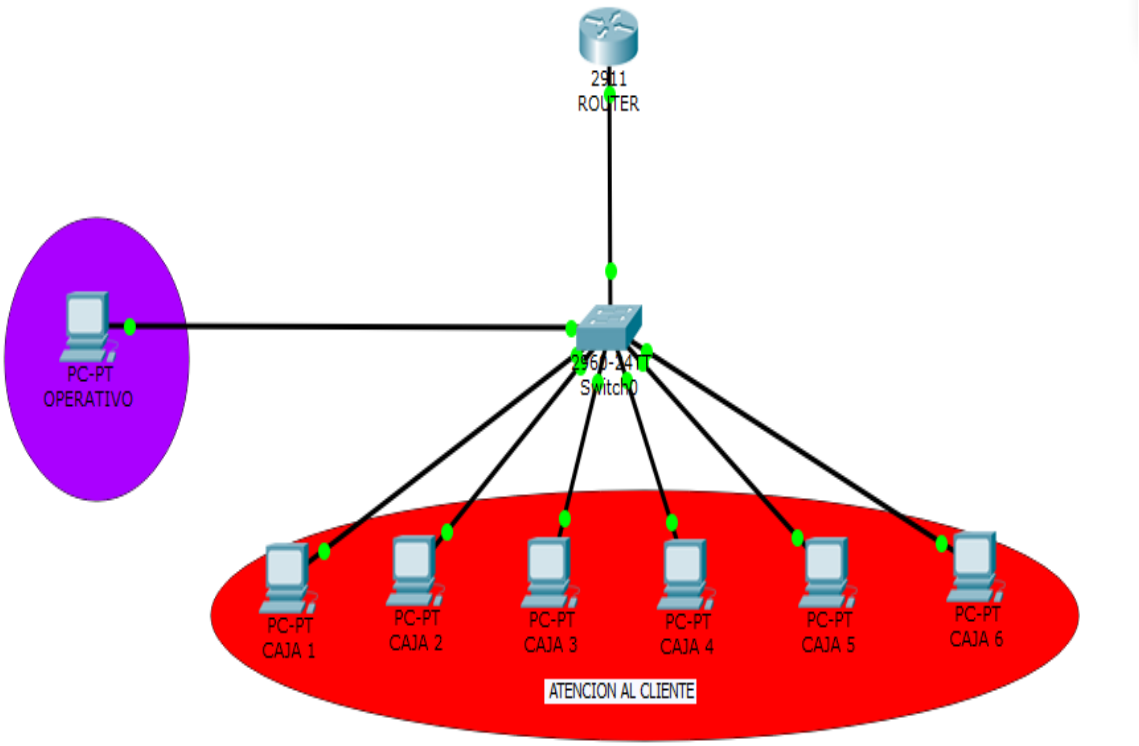


Fuente: Elaboración Propia

4.3.2 Infraestructura de la Red LAN - Sucursal La Ceja

Esta sucursal cuenta con 6 cajas de atención al cliente y un operativo que esta de encargado del funcionamiento de los servicios que ofrece Prendamas. El switch catalyst 2060 tiene 24 interfaces de los cuales 8 interfaces están ocupadas eso nos quiere decir que esta red es escalable tiende a crecer.

Figura N°46
Red LAN - Sucursal La Ceja



Fuente: Elaboración Propia

4.4 Aplicación del Tunnel Gre

4.4.1 Direccionamiento IP

4.4.1.1 Migración de IPv4 a IPv6

En IPv6 ya no se utiliza el termino host si no que ahora se le conoce con el termino de Interfaz ID. Procedemos a realizar el cálculo de las interfaces Id de cada equipo en las respectivas sucursales.

Sucursal Plaza del Estudiante:

En esta sucursal se tiene 5 equipos por lo tanto tendremos que realizar el cálculo para este número de interfaces, cada equipo tiene su dirección MAC el cual indica en IPv6

según la IEEE definió al identificador único extendido (EUI) modificado. Este proceso utiliza la dirección MAC de Ethernet de 48 bits de un cliente e introduce otros 16 bits en medio de la dirección MAC de 48 bits para crear un Id de interfaz de 64 bits.

Para esta Red LAN se usará la siguiente dirección de red IPv6 FC00:db8:abcd:5005::/64 y con la ayuda de la dirección MAC de cada equipo que es única podremos formar las interfaces id de cada equipo.

PC – Operativo:

Dirección MAC: 0090-2B20-A9ED

Entonces aplicamos el proceso EUI-64:

00:90:2B:20:A9:ED ⇒ 00:90:2B:FF:FE:20:A9:ED

0000 0000
0000 0010 ⇒ 02

0290:2BFF:FE20:A9ED

Ahora la interfaz id será la siguiente tomado en cuenta la dirección de red:

FC00:db8:abcd:5005:0290:2BFF:FE20:A9ED/64

Caja 1:

Dirección MAC: 0060-4751-C595

Entonces aplicamos el proceso EUI-64:

00:60:47:51:C5:95 ⇒ 00:60:47:FF:FE:51:C5:95

0000 0000

0000 0010 ⇒ 02

0260:47FF:FE51:C595

Ahora la interfaz id será la siguiente tomado en cuenta la dirección de red:

FC00:db8:abcd:5005: 0260:47FF:FE51:C595/64

Caja 2:

Dirección MAC: 00E0-A37B-17E5

Entonces aplicamos el proceso EUI-64:

00:E0:A3:7B:17:E5 ⇒ 00:E0:A3:FF:FE:7B:17:E5

0000 0000

0000 0010 ⇒ 02

02E0:A3FF:FE7B:17E5

Ahora la interfaz id será la siguiente tomado en cuenta la dirección de red:

FC00:db8:abcd:5005: 02E0:A3FF:FE7B:17E5/64

Caja 3:

Dirección MAC: 00E0-B01D-9D2D

Entonces aplicamos el proceso EUI-64:

00:E0:B0:1D:9D:2D ⇒ 00:E0:B0:FF:FE:1D:9D:2D

0000 0000

0000 0010 ⇒ 02

02E0:B0FF:FE1D:9D2D

Ahora la interfaz id será la siguiente tomado en cuenta la dirección de red:

FC00:db8:abcd:5005: 02E0:B0FF:FE1D:9D2D/64

Caja 4:

Dirección MAC: 0001-97A9-8ED7

Entonces aplicamos el proceso EUI-64:

00:01:97:A9:8E:D7 ⇒ 00:01:97:FF:FE:A9:8E:D7

0000 0000

0000 0010 ⇒ 02

0201:97FF:FEA9:8ED7

Ahora la interfaz id será la siguiente tomado en cuenta la dirección de red:

FC00:db8:abcd:5005:0201:97FF:FEA9:8ED7/64

Sucursal La Ceja:

En esta sucursal se tiene 7 equipos por lo tanto tendremos que realizar el cálculo para este número de interfaces.

Para esta Red LAN se usará la siguiente dirección de red IPv6 FD00:db8:abc5:7560::/64 y con la ayuda de la dirección MAC de cada equipo que es única podremos formar las interfaces id de cada equipo.

Pc – Operativo:

Dirección MAC: 0006-2AD0-1EBA

Entonces aplicamos el proceso EUI-64:

00:06:2A:D0:1E:BA ⇒ 00:06:2A:FF:FE:D0:1E:BA

0000 0000

0000 0010 ⇒ 02

0206:2AFF:FED0:1EBA

Ahora la interfaz id será la siguiente tomado en cuenta la dirección de red:

FD00:db8:abc5:7560: 0206:2AFF:FED0:1EBA/64

Caja 1:

Dirección MAC: 00E0-B090-7A57

Entonces aplicamos el proceso EUI-64:

00:E0:B0:90:7A:57 ⇒ 00:E0:B0:FF:FE:90:7A:57

0000 0000

0000 0010 ⇒ 02

02E0:B0FF:FE90:7A57

Ahora la interfaz id será la siguiente tomado en cuenta la dirección de red:

FD00:db8:abc5:7560:02E0:B0FF:FE90:7A57/64

Caja 2:

Dirección MAC: 0090-2B09-EBB7

Entonces aplicamos el proceso EUI-64:

00:90:2B:09:EB:B7 ⇒ 00:90:2B:FF:FE:09:EB:B7

0000 0000

0000 0010 ⇒ 02

0290:2BFF:FE09:EBB7

Ahora la interfaz id será la siguiente tomado en cuenta la dirección de red:

FD00:db8:abc5:7560: 0290:2BFF:FE09:EBB7/64

Caja 3:

Dirección MAC: 0001-4341-6BA4

Entonces aplicamos el proceso EUI-64:

00:01:43:41:6B:A4 ⇒ 00:01:43:FF:FE:41:6B:A4

0000 0000

0000 0010 ⇒ 02

0201:43FF:FE41:6BA4

Ahora la interfaz id será la siguiente tomado en cuenta la dirección de red:

FD00:db8:abc5:7560:0201:43FF:FE41:6BA4/64

Caja 4:

Dirección MAC: 0002-1739-D39E

Entonces aplicamos el proceso EUI-64:

00:02:17:39:D3:9E ⇒ 00:02:17:FF:FE:39:D3:9E

0000 0000

0000 0010 ⇒ 02

0202:17FF:FE39:D39E

Ahora la interfaz id será la siguiente tomado en cuenta la dirección de red:

FD00:db8:abc5:7560: 0202:17FF:FE39:D39E/64

Caja 5:

Dirección MAC: 0030-F29E-4E35

Entonces aplicamos el proceso EUI-64:

00:30:F2:9E:4E:35 ⇒ 00:30:F2:FF:FE:9E:4E:35

0000 0000

0000 0010 ⇒ 02

0230:F2FF:FE9E:4E35

Ahora la interfaz id será la siguiente tomado en cuenta la dirección de red:

FD00:db8:abc5:7560: 0230:F2FF:FE9E:4E35/64

Caja 6:

Dirección MAC: 00E0-F7EB-5132

Entonces aplicamos el proceso EUI-64:

00:E0:F7:EB:51:32 ⇒ 00:E0:F7:FF:FE:EB:51:32

0000 0000

0000 0010 ⇒ 02

02E0:F7FF:FEEB:5132

Ahora la interfaz id será la siguiente tomado en cuenta la dirección de red:

FD00:db8:abc5:7560: 02E0:F7FF:FEEB:5132/64

4.4.2 Protocolo de Enrutamiento

4.4.2.1 Enrutamiento OSPF en IPv4

Sucursal Plaza del Estudiante:

```
Router(Config)# router ospf 1
Router(Config-router)#router-id 1.1.1.1
Router(Config-router)#network 192.168.1.0  0.0.0.3 área 0
Router(Config-router)#exit
```

Router(config)# ipv6 unicast-routing
Router(config)#ipv6 router rip prendamas
Router(config)#exit
Router(config)#interface gigabitEthernet0/0
Router(config-if)#ipv6 rip prendamas enable
Router(config-if)#exit

Sucursal La Ceja

Router(Config)# router ospf 1
Router(Config-router)#router-id 2.2.2.2
Router (Config-router) #network 192.168.1.4 0.0.0.3 área 0
Router(Config-router)#exit
Router(config)# ipv6 unicast-routing
Router(config)#ipv6 router rip prendamas
Router(config)#exit
Router(config)#interface gigabitEthernet0/0
Router(config-if)#ipv6 rip prendamas enable
Router(config-if)#exit

4.4.2.2 Programación del Tunnel Gree

Sucursal Plaza del Estudiante

Router(config)# interface tunnel 0
Router(config-if)#ipv6 address FC55:db8:4860:4871::1/64
Router(config-if)#ipv6 rip prendamas enable
Router(config-if)#tunnel source serial 0/3/0
Router(config-if)#tunnel destination 192.168.1.5
Router(config-if)#tunnel mode ipv6ip
Router(config-if)#exit

Sucursal La Ceja

Router(config)# interface tunnel 0
Router(config-if)#ipv6 address FC55:db8:4860:4871::2/64
Router(config-if)#ipv6 rip prendamas enable
Router(config-if)#tunnel source serial 0/3/0
Router(config-if)#tunnel destination 192.168.1.1
Router(config-if)#tunnel mode ipv6ip
Router(config-if)#exit

En las siguientes imágenes podemos observar que después de la programación en los Routers de cada sucursal, en estos mismos ya se encuentra programado el tunnel gre.

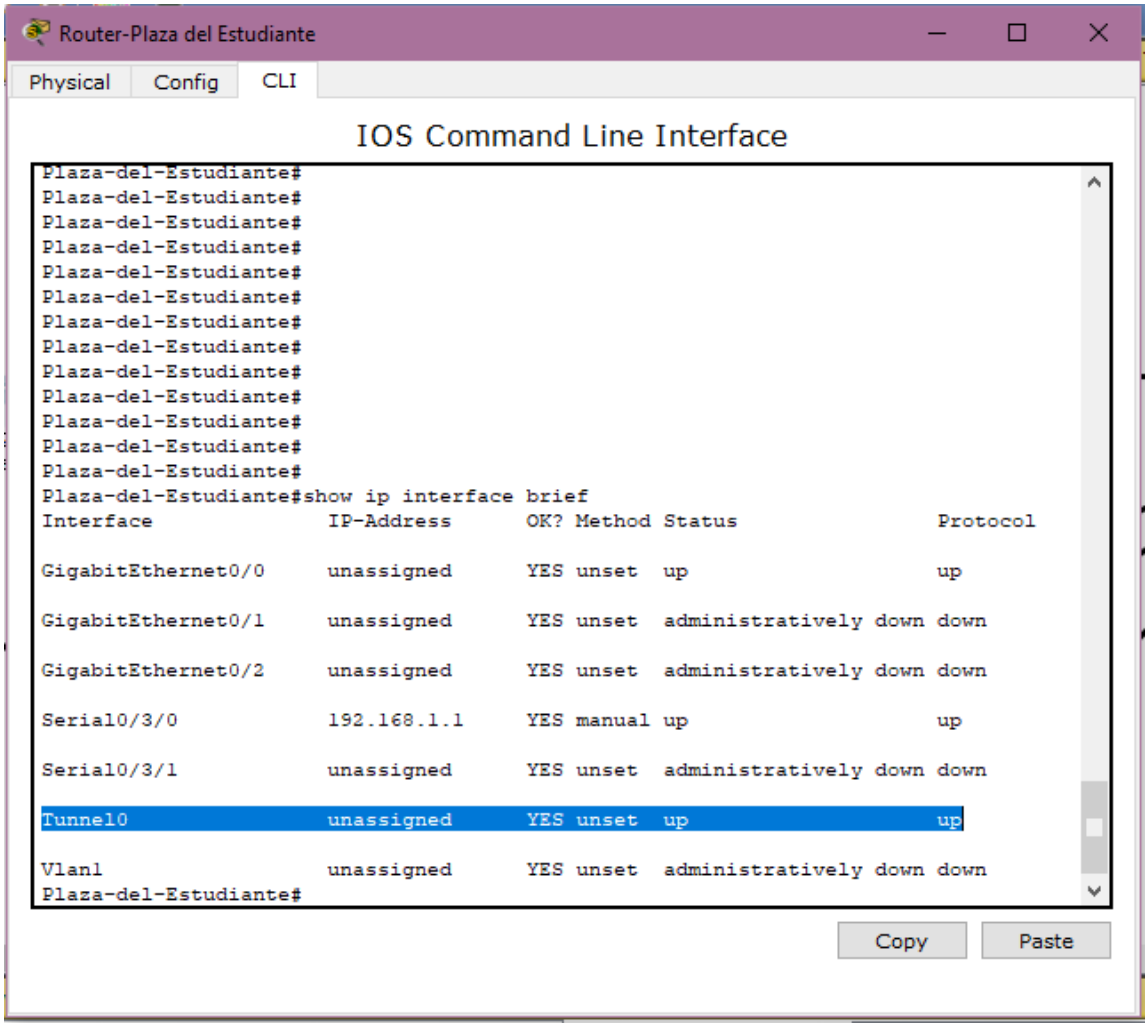
Entonces para la verificación realizamos el siguiente comando en cada router el cual es:

Show ip interface brief

Este comando nos indicada el estado de cada interface del router por lo tanto podemos observar que el tunnel gre ya está levantado.

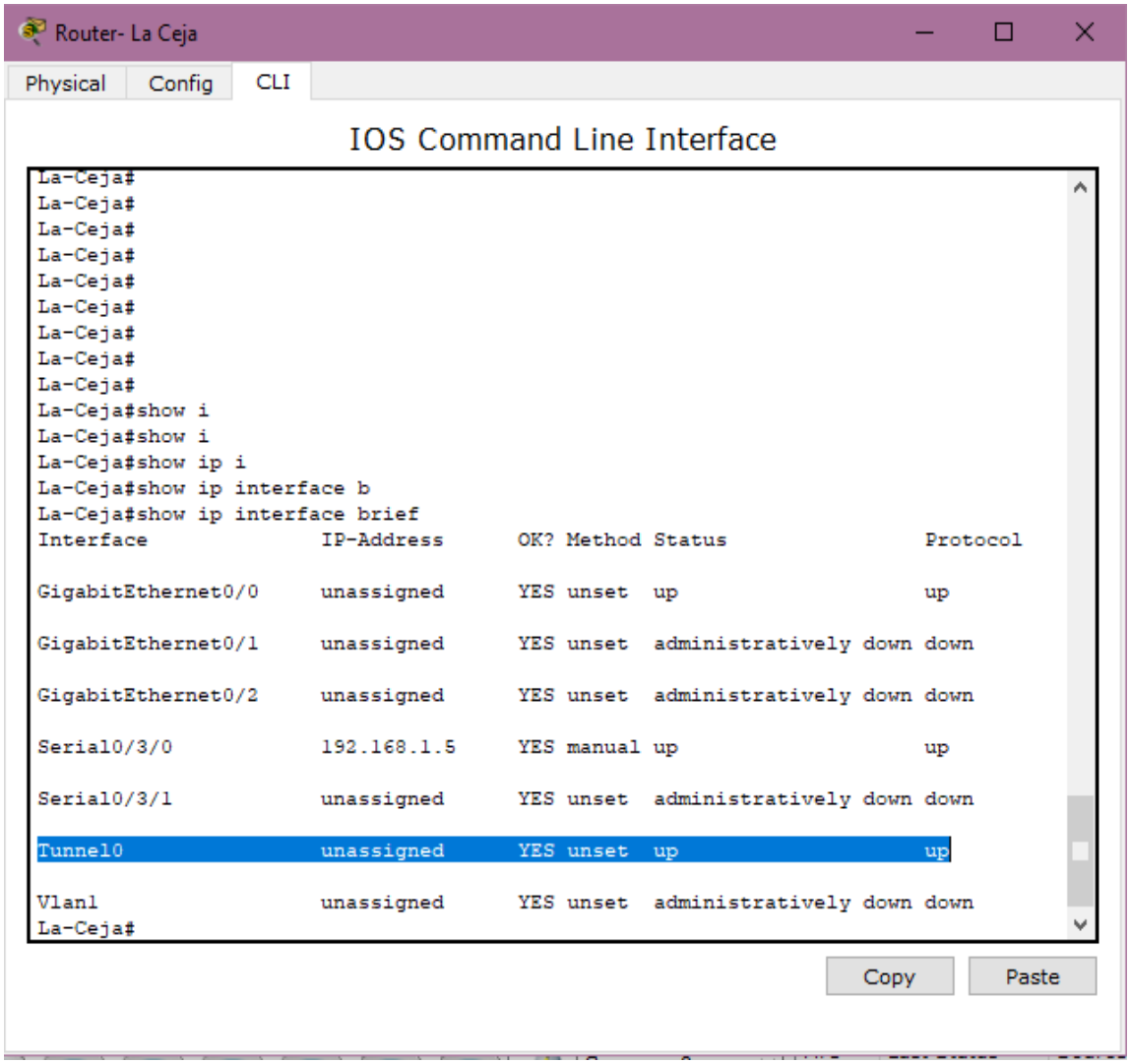
Figura N°47

Tunnel Gre en estado UP - Plaza del Estudiante



Fuente: Elaboración Propia

Figura N°48
Tunnel Gre en estado UP - La Ceja



Fuente: Elaboración Propia

En las siguientes imágenes podemos observar la programación que se realizó en cada el tunnel gre de cada router en las respectivas sucursales.

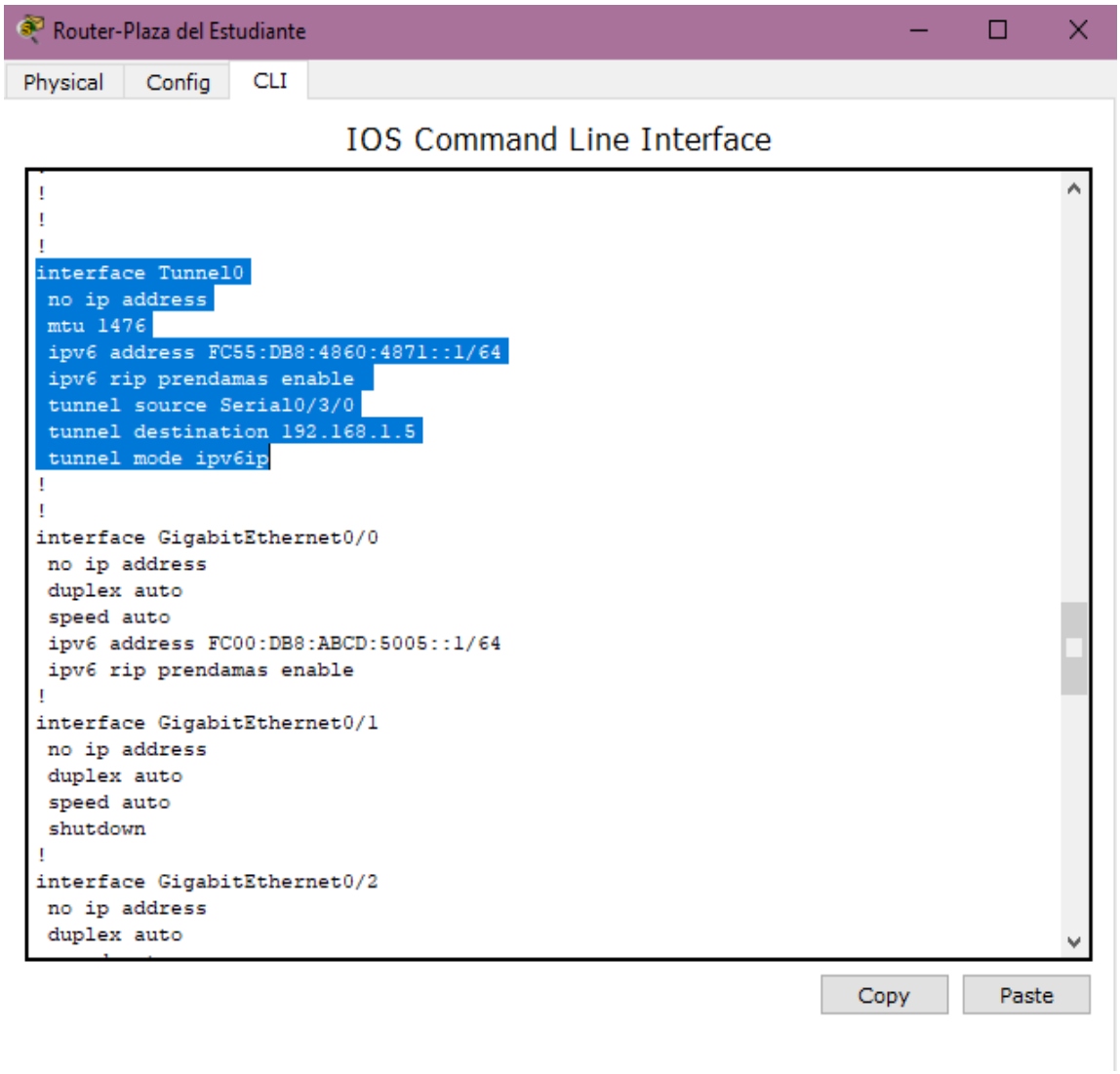
Entonces para la verificación que el tunnel gree este programado en Ipv6 realizamos el siguiente comando:

Show running-config

Con este comando podremos ver toda la configuración que se realizó en los routers de cada sucursal, pero para fines del proyecto vemos en específico la configuración de la interface tunnel, así como se muestra en las siguientes imágenes:

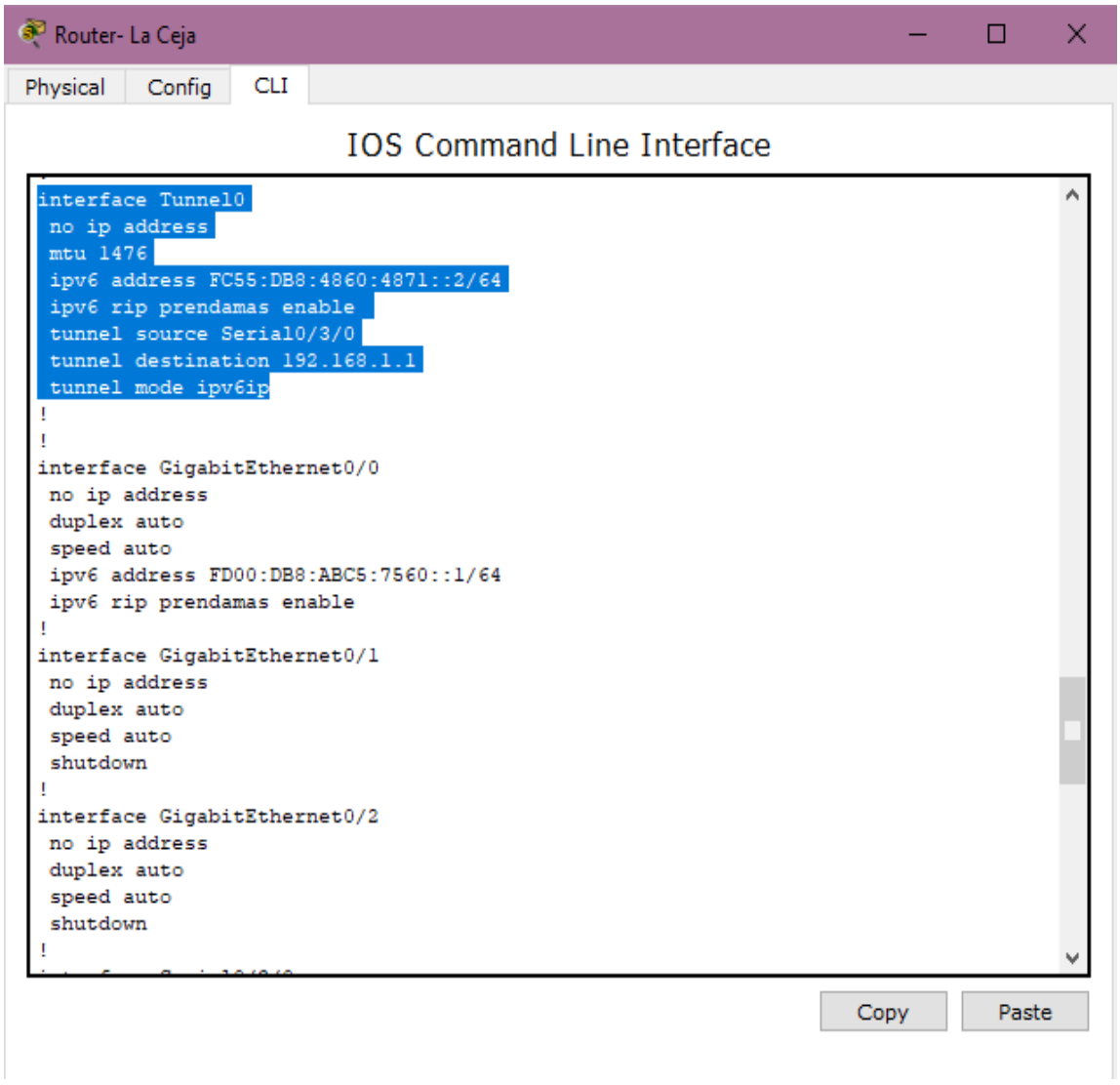
Figura N°49

Configuración del Tunnel Gre - Plaza del Estudiante



Fuente: Elaboración Propia

Figura N°50
Configuración del Tunnel Gre - La Ceja



Fuente: Elaboración Propia

CAPITULO V

ANALISIS DE COSTOS

5.1 Costos

El costo del proyecto se clasifica en:

- Costos Fijos
- Costos Variables

Los costos fijos son aquellos que siempre se deberá pagar, independientemente del nivel del desarrollo en la Institución Financiera, como los equipos de implementación que se necesita para realizar la programación, pero en este caso dicha institución ya cuenta con los equipos para realizar la programación lo que debería comprar es una dirección de red en Ipv6 para que el proyecto se desarrolle de manera muy factible.

Los costos variables son aquellos que se deberá pagar para la respectiva programación del sistema de seguridad en la red de internet, en otras palabras, se deberá pagar la mano de obra que estas pueden variar de acuerdo al Administrador de Red, tomando en cuenta el lapso de tiempo. Mientras el tiempo sea el adecuado se garantiza la viabilidad del proyecto.

5.1.1 Costos Fijos

El Registro de Direcciones de Internet de América Latina y Caribe es una organización no gubernamental internacional, establecida en Uruguay en el año 2002. Su función es asignar y administrar los recursos de numeración de Internet (IPv4, IPv6), números autónomos y resolución inversa para la región**.**

En la Asamblea de Miembros de LACNIC de mayo de 2017 (Foz de Iguazú, Brasil), se aprobaron nuevas tarifas, mismas que entrarán en vigor a partir del día 1° de enero de 2018. Para referencia, se muestran las tarifas vigentes hasta el día 31 de diciembre de 2017 y las tarifas que entrarán en vigor a partir del 1° de enero de 2018.

El tipo de moneda que se maneja al realizar los costos del proyecto es el dólar, así como se muestra en las siguientes tablas.

TABLA N°10
Costos Fijos

Prefijos de Direcciones IPv6	Cantidad	Costo Unitario ($)	Costo ($)
Mayor o igual a /35 hasta /48 inclusive	1	2,500	2,500
Renovación de Asignación Anual de dirección IPv6	1	600	600
		TOTAL	**3100 ($)**

Fuente: Elaboración Propia

5.1.2 Costos Variables

TABLA N°11
Costos Variables

Item	Detalle	Cantidad	Costo Unitario ($)	Costo ($)
1	Programación en los Routers	2	400	800
2	Configuración en los hosts finales	12	40	480
3	Cable Ethernet categoría 5	12	2	24
4	Conector RJ45	24	8	192
5	Mano de Obra	1	1000	1000
			TOTAL	**2496 ($)**

Fuente: Elaboración Propia

5.1.3 Costo Total

TABLA N°12
Costo Total

N°	Tipo de Costo	Costo en Dólares ($)
1	Costos Variables	2496
2	Costos Fijos	3100

COSTO TOTAL	**5596 ($)**

Fuente: Elaboración Propia

CAPITULO VI

CONCLUSIONES, RECOMENDACIONES Y BIBLIOGRAFIA

6.1 Conclusiones

En el estudio que se realizó a la Institución Financiera Prendamas, se pudo sacar varias conclusiones entre ellos podemos mencionar el servicio que ofrece a la sociedad el cual es sobre préstamos prendarios, nos ayudó en mucho ya que se pudo identificar el tipo y nivel de información que manejan.

Al contar ya con la información que recabamos sobre los datos que se maneja en dicha Institución se pudo llegar a la conclusión que su nivel de información es de Nivel Medio.

Se realizo la migración de Ipv4 a Ipv6 en los hosts finales para colaborar con el sistema de seguridad, también se realizó la programación del Tunnel Gre en los Routers en base a IPv6.

Este sistema de seguridad permitirá que la Institución Financiera Prendamas maneje su información en la red de internet, pero de forma segura y garantizada a que no sufrirá ningún tipo de perdida de datos en la red.

6.2 Recomendaciones

Para poder aplicar este sistema de seguridad en otra organización se recomienda primeramente realizar un estudio minucioso al tipo de datos y al nivel de información que se maneja.

Este sistema de seguridad solo es sugerido para Instituciones que maneje un nivel medio de información pero que si necesiten que sus datos sean protegidos en la red.

También verificar que las características de los equipos como ser computadoras y routers sean capaces de trabajar con IPv6 para no generar problemas de seguridad.

Para que el sistema de seguridad trabaje de forma eficaz realizar un cronograma de mantenimiento preventivo a los equipos.

6.3 Bibliografía

6.3.1 Referencias Bibliográficos de libros

Ernesto Ariganello, 2020, Redes Cisco CCNA 200-301

Akin Ramirez, 2008, Principios Basicos de Enrutamiento y switching CCNA1 V5

Javier Velasco, 2000, Introduccion a la Seguridad en Redes

Artuto Martin Romero, 2005, Seguridad Informatica y Alta Disponibilidad

William Stalling, 2008, Comunicación y Redes de Computación, 6ta edición.

Andrew S. Tanenbaum, 1981, Redes de Computadoras

Ruben Bustamante Sanchez, 2007, Seguridad en Redes

6.3.2 Referencias bibliográficas de Internet

https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwici-

https://ccnadesdecero.es/caracteristicas-funciones-ospf/

https://ccnadesdecero.es/routing-o-enrutamiento-estatico

https://conceptodefinicion.de/adsl/

http://itroque.edu.mx/cisco/cisco1/course/module6/6.1.3.1/6.1.3.1.html

https://www.ibm.com/docs/es/i/7.2?topic=routing-open-shortest-path-firs

https://www.ibm.com/docs/es/i/7.2?topic=routing-open-shortest-pat

www.itesa.edu.mx/netacad/switching/course/module7/7.1.4.2/7.1.4.2.html

https://www.ionos.es/digitalguide/servidores/know-how/wan/

https://es.slideshare.net/equipoderedes/tecnologas-de-acceso

6.4 Anexos

MANUAL DE FUNCIONAMIENTO DEL SISTEMA DE SEGURIDAD (TUNNEL GRE)

Funcionamiento.

La programación del sistema de seguridad se realizó en los Routers de cada sucursal de Prendamas, los cuales están conectados entre sí generando una red privada, y cada router tiene su propia red LAN el cual está conectado a un Switch de 24 puertos de los cuales están conectados los usuarios finales.

Los usuarios finales se enviarán datos entre distintas sucursales, pero la información viajara por internet de forma segura.

Recomendaciones.

Se establece las siguientes recomendaciones.

- Realizar mantenimientos periódicos para el buen funcionamiento y el uso completo de la vida útil de los equipos del Rack.
- No sobrecargar al Switch más de su capacidad.
- No conectar artefactos o equipos electrónicos como ser (aspiradora, ventiladores, calderas eléctricas, etc.) en el Rack ya que ahí se encuentran los equipos de telecomunicaciones.
- Tener el Router, Switch y host finales en constante supervisión para evitar cualquier problema con el mismo.