INSTITUTO TECNOLÓGICO
DE TUXTLA GUTIÉRREZ

Departamento académico de ingeniería de eléctrica y electrónica

INGENIERIA ELECTRÓNICA

Implementación y puesta en servicio de la Red Operativa de Datos de la EPS CFE Transmisión.

ESQUINCA GARCIA VICENTE ALEJANDRO

TUXTLA GUTIÉRREZ, CHIAPAS A 10 DE ENERO DE 2019

Índice

Capítulo 1. Generalidades

1.1 Introducción

El presente documento tiene como finalidad dar a conocer el proyecto de la Red Eléctrica Inteligente (REI) desarrollado en la Empresa Productiva del Estado CFE Transmisión en el ámbito de la Gerencia Regional de Transmisión Sureste que comprende los estados de Tabasco, Oaxaca y Chiapas.

La Plataforma Tecnológica Europea define a la REI como una red eléctrica que puede integrar de forma inteligente todas las acciones de los usuarios conectados a ella - generadores, consumidores y aquellos que hacen ambas cosas, a fin de cumplir de manera eficiente con suministro de electricidad en forma sustentable, económica y segura (ESTA International, LLC, 2014).

La Red Operativa servirá para integrar una red de comunicaciones para la transmisión de información de carácter operativo, orientada a la implementación de una Red Eléctrica Inteligente en el ámbito de la Dirección de Transmisión, lo cual permitirá que las actividades propias del personal encargado de la operación, control, mantenimiento, atención a contingencias, coordinación y administración técnico, financiera garanticen la confiabilidad de la red eléctrica nacional y la productividad en el ámbito de la Dirección de Transmisión, Gerencias Regionales, Zonas, Sectores y Subestaciones que la conforman.

1.2 Información general de la institución o empresa donde se desarrolló el proyecto

El 14 de agosto de 1937, el gobierno federal crea la Comisión Federal de Electricidad (CFE), que tendría por objeto organizar y dirigir un sistema nacional de generación, transmisión y

distribución de energía eléctrica, basado en principios técnicos y económicos, sin propósitos de lucro y con la finalidad de obtener con un costo mínimo, el mayor rendimiento posible en beneficio de los intereses generales.

En 1938 CFE tenía apenas una capacidad de 64 kW, misma que, en ocho años, aumentó hasta alcanzar 45,594 kW. Hacia 1960 la CFE aportaba ya el 54% de los 2,308 MW de capacidad instalada, la empresa Mexican Light el 25%, la American and Foreign el 12%, y el resto de las compañías 9%.

A inicios del año 2000, se tenía ya una capacidad instalada de generación de 35,385 MW, cobertura del servicio eléctrico del 94.70% a nivel nacional, una red de transmisión y distribución de 614,653 km, lo que equivale a más de 15 vueltas completas a la Tierra y más de 18.6 millones de usuarios, incorporando casi un millón cada año (CFE, s.f.).

A finales del año 2013 con la aprobación la reforma energética se crea la ley de la industria eléctrica la cual separa a las principales áreas de CFE generación, transmisión y distribución en empresas productivas subsidiarias, por lo que se crea la EPS CFE Transmisión.

Misión

Prestar el Servicio Público de transmisión de Energía Eléctrica, mediante la operación, mantenimiento, expansión y modernización de la Red Nacional de Transmisión garantizando un acceso abierto y no indebidamente discriminatorio y cumpliendo con condiciones reguladas de disponibilidad, continuidad y eficiencia para crear valor económico y rentabilidad para el Estado Mexicano.

Visión

Ser una empresa de Servicio Público de Transmisión con un desempeño equiparable a las mejores empresas del mundo, con presencia internacional y fortaleza financiera, mediante el máximo aprovechamiento de su infraestructura y contribución de su capital humano.

1.3 Área del proyecto: Departamento de Monitoreo y Operaciones

Como se observa en la figura 1.1 en la parte de comunicaciones de CFE Transmisión que es la que está a cargo del proyecto de la REI, pero la red de datos está a cargo del departamento de monitoreo y operaciones.

Todas las áreas de la subgerencia de comunicaciones se ven involucradas en la red de datos, cada área es de suma importancia debido a que aporta una parte que ayuda al adecuado funcionamiento de la red, sin embargo, el proyecto presentado a continuación en este documento será desarrollado en el área de Monitoreo y Operaciones, que es el área encargada específicamente de la red de datos.

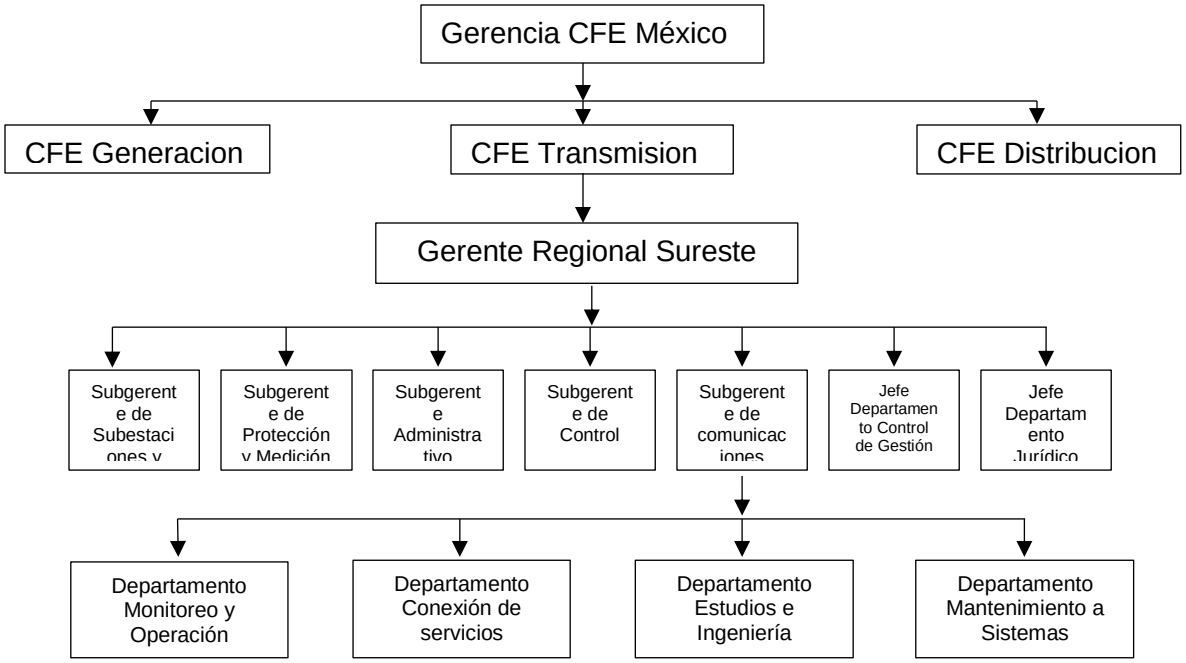


Fig. 1.1 Organigrama de la empresa

1.4 Antecedentes

Derivado de los cambios recientes en los servicios de energía en México, se ha planteado la necesidad de contar con una arquitectura tecnológica que permita la evolución del negocio de Comisión Federal de Electricidad (CFE), para lograr la integración de nuevos servicios, lo cual debe ser de manera segura y operando bajo las mejores prácticas de la industria, buscando la reducción de pérdida de energía, la integración y automatización de procesos y la generación de opciones más sencillas para la facturación de servicios, que ayuden a llevar a cabo la evolución de los procesos y servicios en el área de Transmisión, utilizando los recursos de red ya disponibles y generando mejoras en las diversas partes del proceso productivo, aumentando los niveles de eficiencia y respuesta de las aplicaciones críticas.

Como parte de la reforma energética, se encuentra en proceso la interconexión de terceros hacia la red eléctrica nacional, por ello surge la necesidad de contar con una red de datos inteligente que facilite la integración de los canales dedicados que provengan de las instalaciones de los terceros, cuyo objeto es que la medición obtenida en el punto de interconexión quede a disposición de los Centros de Control de Comisión Federal de Electricidad y del Mercado de Energía; lo anterior de acuerdo a lo establecido en el apartado 2.4 Equipo de Medición, de las Reglas Generales de Interconexión al Sistema Eléctrico Nacional del Diario Oficial de la Federación publicado el Martes 22 de Mayo de 2012 (Boyzo Boyzo, y otros, 2016).

1.5 Planteamiento del problema

Con la nueva reforma energética donde los particulares pueden vender energía a la propia CFE se necesita medios más eficientes para distribuir esta energía desde un punto a otro, por lo que CFE necesita de un Red eléctrica inteligente. Este es uno de muchos factores, además de la adaptación para sumar a la red eléctrica la generación de energías limpias y

el avance en la necesidad de carga para los futuros carros eléctricos e híbridos, por los que se necesita un avance significativo en la Red Eléctrica nacional.

La Red Eléctrica en nuestro país conforme el paso de los años se ha ido expandiendo considerablemente por el resto del país, pero la red solamente ha crecido en tamaño y con más empresas generadoras de electricidad se necesitan nuevas tecnologías para tener una mejor eficiencia en la generación, transmisión y distribución de electricidad para que ésta se encuentre siempre en completa sintonía.

1.6 Nombre del proyecto

Implementación y puesta en servicio de la Red Operativa de Datos de la EPS CFE Transmisión.

1.7 Objetivos generales y específicos

implementar una plataforma multiservicios para la Red Eléctrica Inteligente, garantizando en todo momento la integridad, confidencialidad y disponibilidad de los datos, con el propósito de alcanzar lo siguiente: (Boyzo Boyzo, y otros, 2016):

- Integración de las nuevas tecnologías de las Redes Eléctricas Inteligentes:

    a) Modernización de los sistemas de automatización de las instalaciones eléctricas de mediana y alta tensión.

    b) Sistema de Transferencia de Datos al Mercado Eléctrico Mayorista.

    c) Aplicaciones Avanzadas de Sincrofasores.

d) Sistema de Control de Adquisición de Datos (SCADA) de nueva generación.

e) Sistemas de control de flujo y voltaje de nueva generación.

f) Despliegue de tecnologías inteligentes para la medición y comunicación en las REI.

- Comunicaciones Unificadas Empresariales

  a) Telefonía

  b) Videoconferencia

  c) Correo de Voz

  d) Correo Electrónico

  e) Servicios en la Nube

  f) Colaboración

  g) Sistemas Institucionales

- Reducción de las pérdidas de energía mediante:

  a) Aplicación de tecnología y procesos

  b) Reducción de fallas técnicas y no técnicas

- Gestión de activos de CFE.

  a) Georreferenciación (GIS)

b) Análisis de Falla

c) Monitoreo

1.8 Justificaciones del proyecto

Se pretende que con nuevos criterios de planeación y con la incorporación de las tecnologías de las REI se contribuya a (SENER, 2016):

- Mejorar la operación del Sistema Eléctrico Nacional, incrementando su eficiencia, flexibilidad resiliencia, Calidad, Confiabilidad, Continuidad, seguridad y sustentabilidad;
- Promover la generación de electricidad proveniente de fuentes de energía limpia, a gran escala.
- Permitir la optimización dinámica de la operación del SEN;
- Apoyar en la gestión del Mercado Eléctrico Mayorista;
- Incorporar la Generación Distribuida, incluyendo la de fuentes de energía renovable;
- La interacción del usuario con el sistema;
- Incidir para mejorar la calidad del servicio que se presta al usuario;
- Facilitar la provisión de servicios adicionales y la integración de los vehículos eléctricos y fuentes de almacenamiento.

Que el costo/beneficio de la implementación de las REI, sea evaluado en razón del beneficio a corto o largo plazo, que resulte a favor de los involucrados en los procesos y de acuerdo con los motivadores por los cuales se incorporaron, esto de acuerdo con la política y regulación que la autoridad emita.

1.9 Alcances y limitaciones del proyecto

El proyecto de la REI tiene como finalidad cubrir el total de la red eléctrica existente en la República Mexicana desde casas hasta todos los dispositivos, actuadores, sensores y empresas generadoras de energía. Como bien se sabe la red eléctrica del país es extensa por lo que esto es un proyecto de años.

Por ello nos limitaremos a trabajar exclusivamente en lo que es la Red de Datos encontrada en el hotel Telecom Tuxtla Gutiérrez en la Gerencia Regional de Transmisión Sureste.

1.10. Metodología para el desarrollo del proyecto

El proyecto se desarrollará mediante simulaciones en un programa de la compañía Cisco llamado Cisco Packet Tracer para la verificación de lo que ha sido realizado se encuentre correcto. Finalizada la simulación se implementará en la red de datos que hay entre la Gerencia, Tuxtla y Malpaso.

Capítulo 2. Fundamento teórico

2.1 ¿Qué es una red?

Una red es una interconexión de diferentes dispositivos mediante cable o de forma inalámbrica como computadoras, teléfonos, impresoras, etc. Que permiten compartir recursos e información entre sí, en la figura 2.1 podemos ver a grandes rasgos como se compone una red típica.

Según la ubicación, se puede distinguir varios tipos de redes según su extensión:

- LAN (Local Area Network): si la red se encuentra dentro de un mismo edificio
- CAN (Campus Area Network): si la red se encuentra distribuida en varios edificios dentro de un mismo lugar, por ejemplo, en dos edificios de una universidad.
- MAN (Metropolitan Area Network): si la red se encuentra distribuida en varios edificios, pero dentro de una misma ciudad.
- WAN (Wide Area Network): si la red se encuentra distribuida en diferentes localidades, en un país o fuera de este.

(Raya Cabrera & Raya González, 2006)

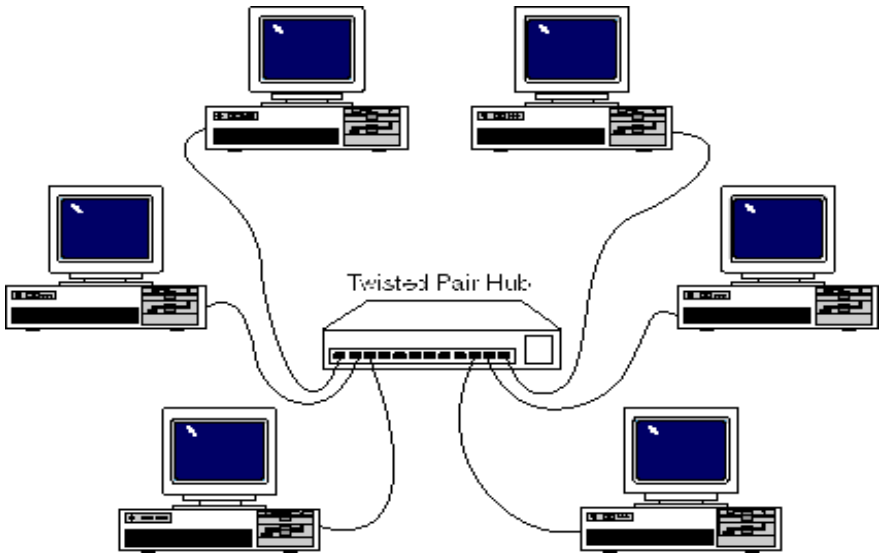


Fig. 2.1 Vista típica de una red (Redes y Seguridad, 2009)

2.1.1 Componentes de una red

Existen componentes básicos para establecer una red, en la figura 2.2 podemos visualizar como se encuentran los componentes distribuidos en una red:

- Computadora: Sirven como dispositivos finales de una red, la cual permite usar esta como medio para enviar o recibir información.

- Interconexiones: Es el componente que proporciona el medio por el cual viajará la información de un dispositivo a otro dentro de la red. Incluye tarjetas de red, medio de comunicación de red como cables o medios inalámbricos y conectores.

- Switches: Son dispositivos que proporcionan conexión a la red de dispositivos finales y realizan el envío inteligente de los datos dentro de una LAN.

- Routers: Son dispositivos que interconectan redes y se encargan de elegir la mejor ruta para el envío de datos.

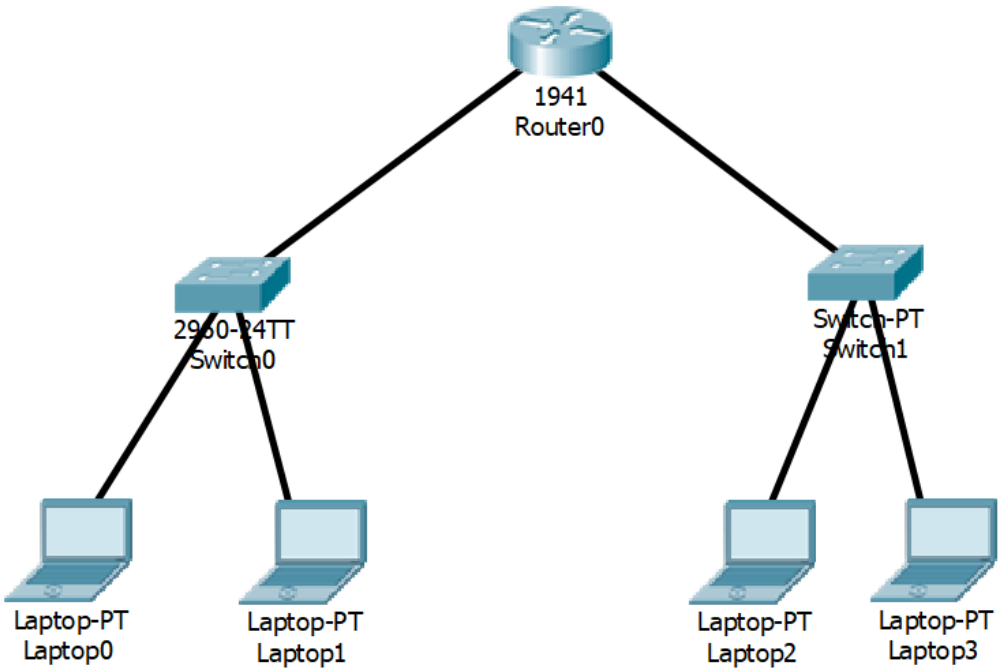


Fig. 2.2 Componentes básicos de una red

2.1.2 Interpretación de un diagrama de topología

Un diagrama de topología utiliza símbolos y/o imágenes para representarnos las diferentes conexiones y dispositivos que forman una red, un ejemplo de un diagrama de topología lógica se observa en la figura 2.3. Con el diagrama podemos comprender fácilmente como

se conectan los diferentes dispositivos en una red grande. El uso de estos diagramas es fundamental para poder visualizar la organización y el funcionamiento de una red.

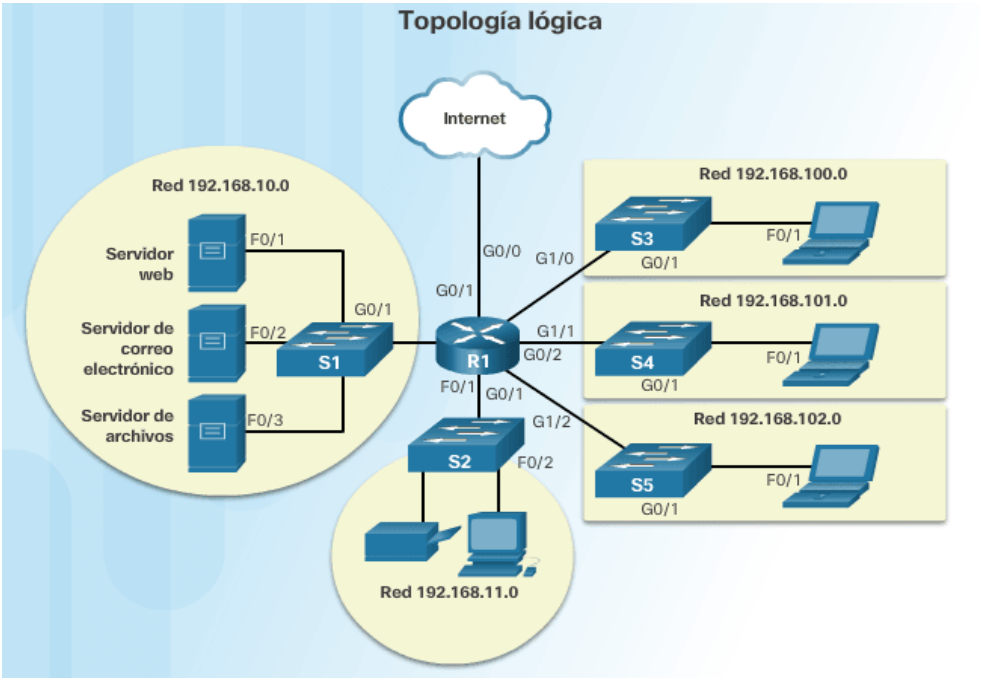


Fig. 2.3 Diagrama de topología (Cisco,

1En la figura 2.4 podemos observar la simbología empleada para realizar un diagrama de topología.

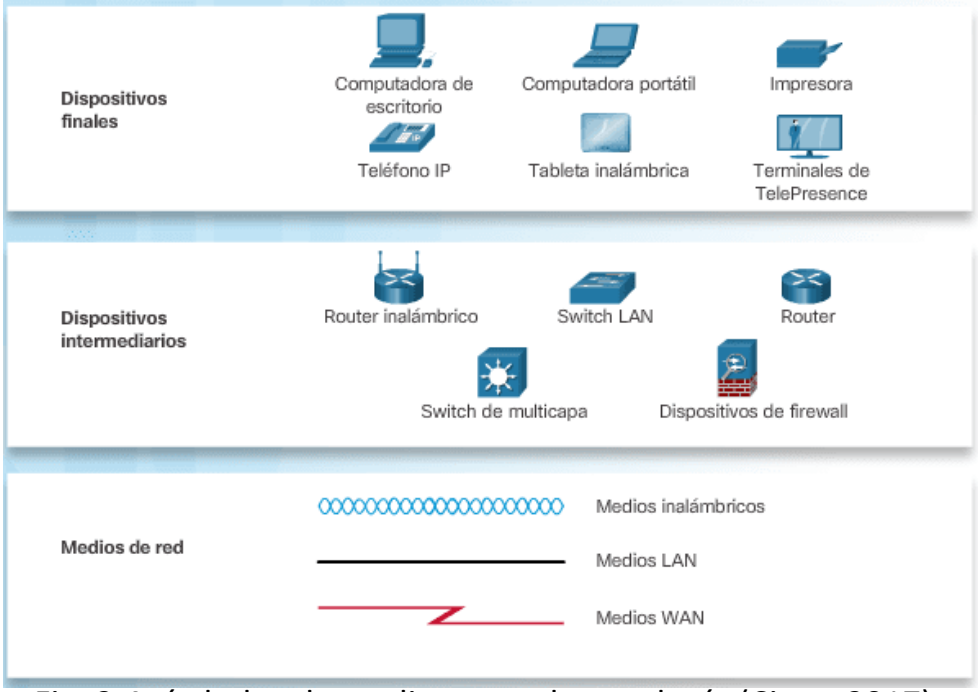


Fig. 2.4 símbolos de un diagrama de topología (Cisco, 2017)

2.2 Características de una red

Puedes describir una red de acuerdo con su rendimiento y estructura, según cisco, como observamos en la imagen 2.5:

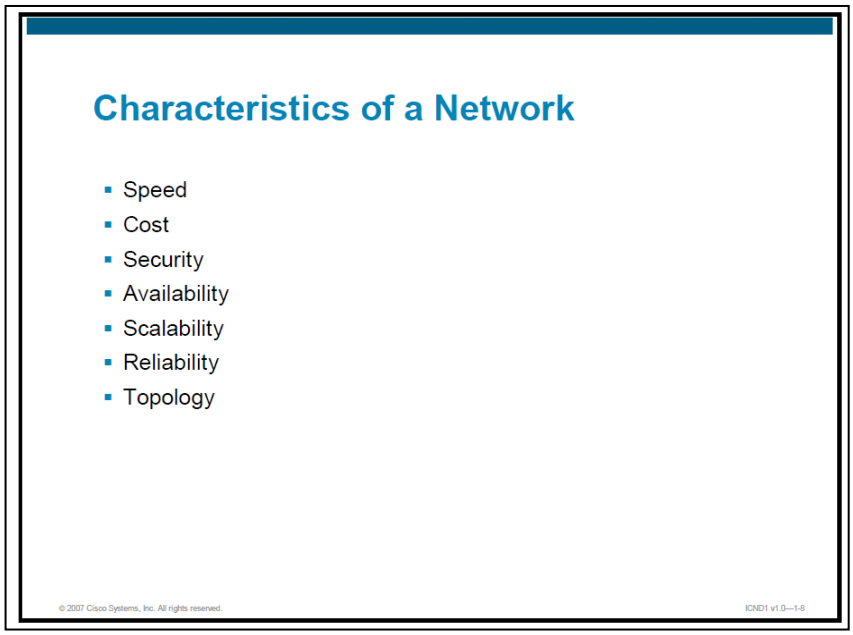


Fig. 2.5 características de una red por su rendimiento y estructura (Cisco Systems, 2007)

- **Velocidad:** Velocidad de los datos que son transmitidos a través de la red.

- **Costo:** Indica el coste general de los componentes, la instalación y el mantenimiento de la red.

- **Seguridad:** Indica cómo proteger la red, incluyendo los datos que se transmiten por esta. El tema de la seguridad es importante y está en constante evolución.

- **Disponibilidad:** Medida de probabilidad de disposición de la red para su uso cuando se necesite. La disponibilidad se calcula dividiendo el tiempo realmente disponible por el tiempo total en un año y luego multiplicando por 100 para obtener un porcentaje.

- **Escalabilidad:** Esta indica cómo la red puede dar cabida a más usuarios y requerimientos de transmisión de datos.

- **Confiabilidad:** Indica la fiabilidad de los componentes (routers, conmutadores, PC, etc.) que conforman la red.

- **Topología:** En las redes, hay dos tipos de topologías: topología física, en la que se encuentran la disposición del cable, dispositivos de red y sistemas finales (ordenadores y servidores) y la topología lógica, que es el camino que toman las señales de datos a través de la topología física.

2.3 Topología de la red

La topología de red hace referencia a la forma en cómo se encuentran distribuidos los diferentes dispositivos y conexiones de una red.

La topología de red tiene como objetivo buscar la forma de conectar los diferentes dispositivos de una manera más económica y eficaz, al mismo tiempo facilitar la fiabilidad del sistema, evitar los tiempos de espera y permitir un mejor control de la red.

2.3.1 Topología de Bus

Es una de las topologías de red más sencillas y económicas debido a que usa un solo canal para conectar todas las estaciones y cada estación se encarga de recoger la información que le corresponde, un ejemplo de esta topología lo podemos observar en la figura 2.6. Uno de los problemas de esta topología es que al aumentar el número de estaciones el flujo aumenta dentro del canal lo cual puede provocar mayor colisión.

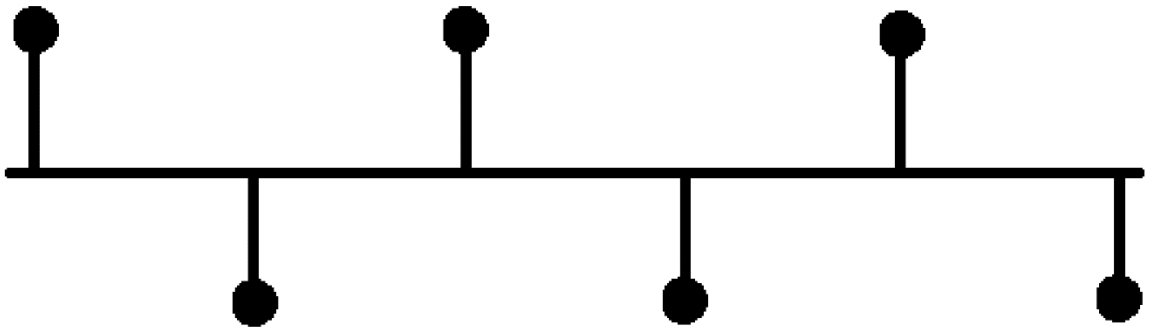


Fig. 2.6 Topología de bus

2.3.2 Topología de estrella y estrella extendida

La topología de estrella es aquella en la que cada una de las estaciones están conectadas a un mismo nodo como se observa en la figura 2.7. Esta topología es algo costosa debido a que tiene la necesidad de utilizar mucho cable, al igual que si el nodo falla toda la red se viene abajo, ya que toda la información pasa por dicho nodo.

La topología de estrella extendida usa el mismo principio que la topología de estrella, toda la red se concentra en un solo nodo, pero divide las estaciones en subredes para disminuir la probabilidad de que la red falle y volverla más robusta, pero vuelve la red más compleja. Como se observa en la figura 2.7 el lado derecho es muy similar a la del izquierdo, siendo en este caso una división en subredes la diferencia.

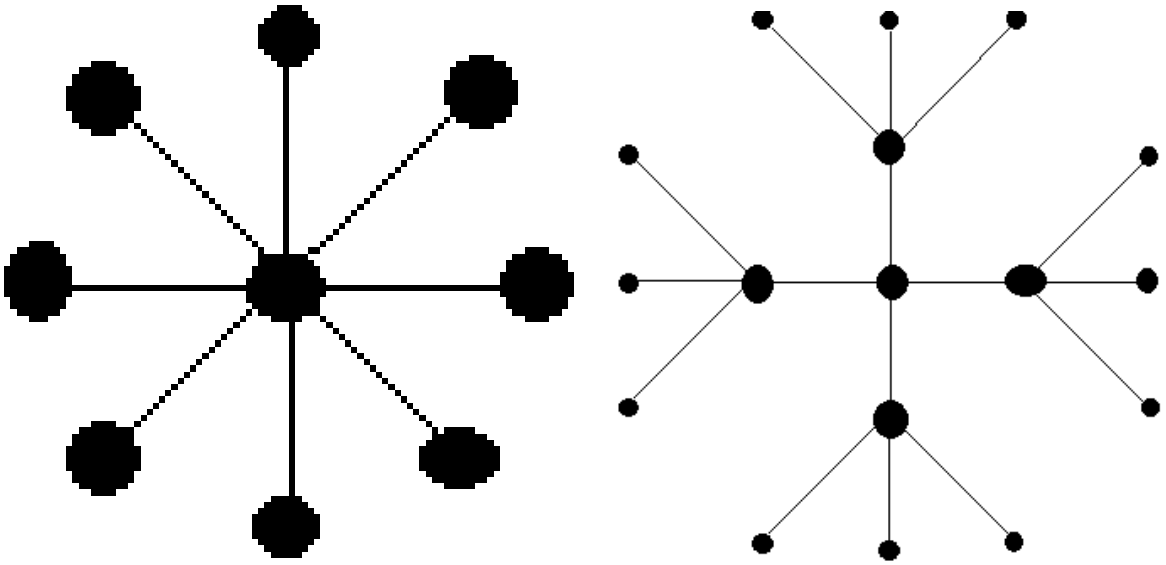


Fig. 2.7 Topología de estrella y estrella extendida

2.3.3 Topología anillo y anillo doble

La topología de anillo todas las estaciones están conectadas entre sí por medio de un canal formando un anillo, de ahí su nombre, por lo que cada estación cuenta con dos conexiones a otras dos estaciones como podemos observar en la figura 2.8 de lado izquierdo.

En esta topología de red la información suele viajar en un solo sentido por lo que la información debe pasar por todas las estaciones necesarias hasta llegar a la estación correspondiente. Al igual que si se presenta un fallo en un canal, la red quedará bloqueada.

En la topología de anillo doble usa doble canal por conexión entre estaciones por lo cual genere un anillo doble, en cada anillo formado la información viaja en sentido opuesto. Como podemos observar en la figura 2.8 de lado derecho se nos representa como se usan dos anillos para enviar y recibir datos, pero en cada anillo observamos como la información viaja en sentido opuesto. Gracias a la implementación del doble anillo hace que la topología sea más resistente que la topología de anillo simple.

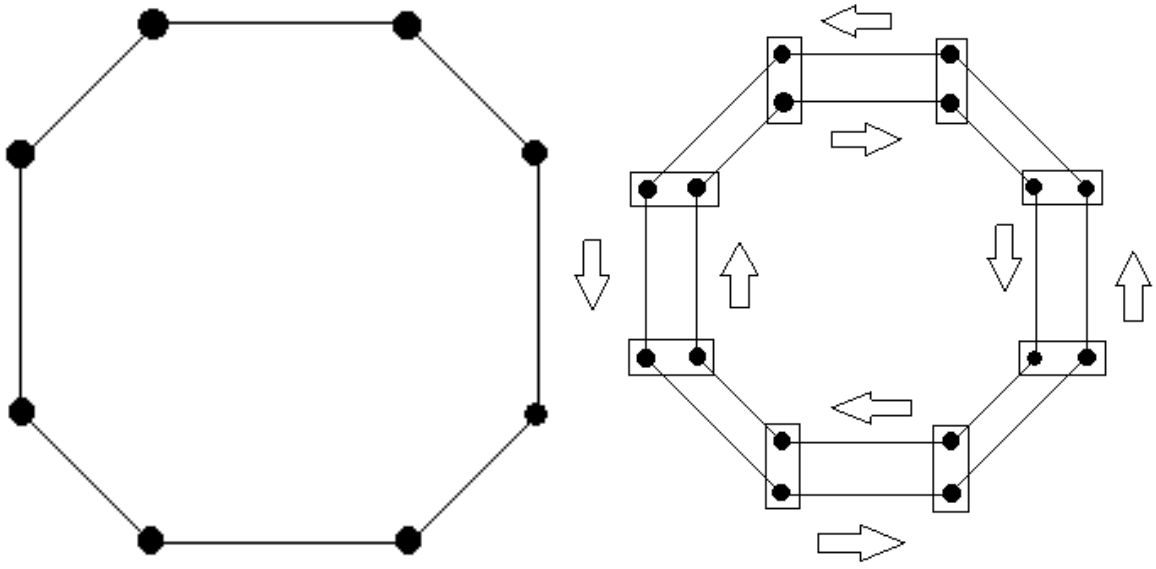


Fig. 2.8 Topología de anillo y anillo doble.

2.3.4 Topología malla completa y malla parcial

En la topología de malla completa cada estación se conecta con cada estación que compone la red como se observa en la figura 2.9, lo que hace que estas topologías resulten caras. Esta topología proporciona gran redundancia ya que si un canal falla tiene otros canales por el cual la información puede llegar desde un punto hasta el otro.

La topología de malla parcial interconecta los nodos principales de la red como se aprecia en la figura 2.9 podemos ver que dicha topología se encuentran menos conexiones. Es más económica que la topología de malla completa, pero proporciona menos redundancia, sin embargo, tiene un gran equilibrio entre tolerancia de fallos y costo.

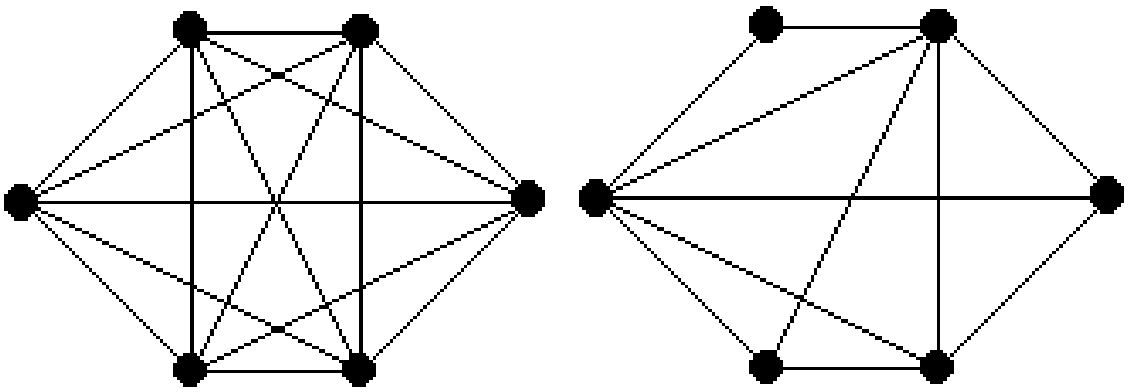


Fig. 2.9 Topología de malla completa y malla parcial.

2.4 Protocolo de internet

Es un protocolo de comunicación de datos digitales que funciona en la capa de red del modelo OSI.

Su función principal es el uso de enrutamiento del origen al destino de comunicación para transmitir datos mediante un protocolo no orientado a conexión que transfiere paquetes conmutados a través de distintas redes físicas según la norma OSI de enlace de datos.

2.4.1 Dirección IP

La dirección IP es una dirección lógica compuesta de 32 bits en su versión 4, que sirve para el enrutamiento eficaz de paquete de datos sobre la red, suele emplearse a nivel de red en el modelo TCP/IP.

Esta dirección debe de ser única por host (computadoras, impresoras, dispositivos finales) en la red, es decir, no se puede repetir la IP en la red.

En total los 32 bits se componen de dos partes la primera que la dirección IP de red (network ID) que es la que describe la ubicación de la red del dispositivo y la segunda parte que es la dirección específica del dispositivo conectado a la red (host ID).

2.4.1.1 Formato de dirección IP

La dirección IP en su versión 4 se conforma de 32 bits está formado por cuatro campos de 8 bits también conocidos como octetos, cada octeto se encuentra separado por un punto.

La dirección IP tiene un formato en forma binaria:

01111111.00000000.00000000.00000001

Cada uno de los octetos puede tener un valor desde 00000000 en binario (cero en decimal) o 11111111 (255 en decimal).

Por lo que bien la dirección IP anteriormente mostrada se puede representar de igual forma de manera decimal, por ejemplo:

Dirección IP de 32 bits	Ejemplo			
	01111111.00000000.00000000.00000001			
La dirección se divide en 4 octetos (8-bits)	01111111	00000000	00000000	00000001
Cada octeto (o byte) puede ser convertido a decimal	127	0	0	1
La dirección puede ser escrita en notación decimal dividido por puntos	127.	0.	0.	1

Tabla 2.1 Dirección IP binaria a decimal.

2.4.1.2 Clases de direccionamiento IP

Para adaptarse a redes de distintos tamaños y para ayudar a clasificarlas, las direcciones IP se dividen en grupos llamados clases. Esto se conoce como direccionamiento classfull.

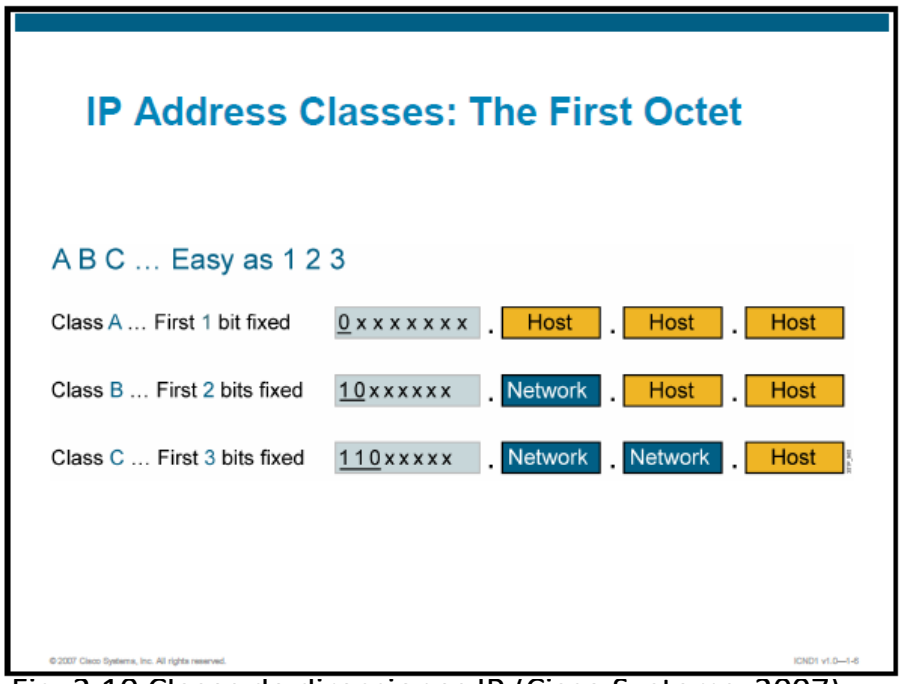
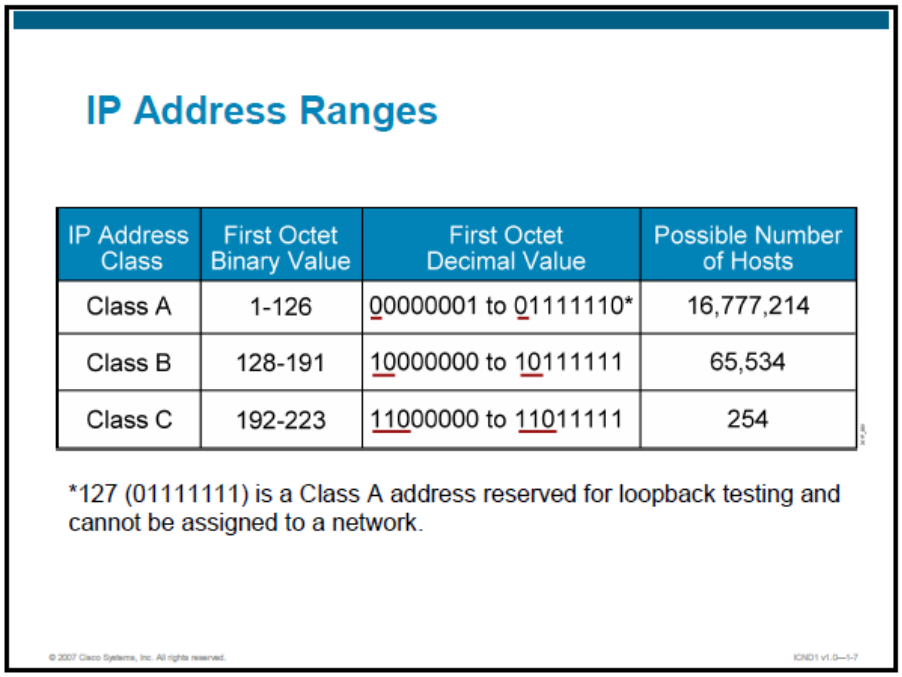


Fig. 2.10 Clases de direcciones IP (Cisco Systems, 2007).

Cada IP se divide en dos partes, la primera que es el “Network ID” y la segunda que es el “Host ID”. Al igual que hay bits al inicio de cada dirección IP, que es el bit que determina a

qué clase de dirección pertenece la IP, en la figura 2.10 podemos apreciar cómo se componen las diferentes clases de IP.

En total existen cinco clases de redes: la clase A, la clase B, la clase C, la clase D, la clase E. sin embargo la clase D es reservada para todas las direcciones para multidestino y la clase E se utiliza con fines experimentales únicamente y no están disponible al público. En la figura 2.11 la tabla nos muestra con cuantos Hosts puede contar nuestra red dependiendo de la clase de dirección IP.



IP Address Ranges

IP Address Class	First Octet Binary Value	First Octet Decimal Value	Possible Number of Hosts
Class A	1-126	00000001 to 01111110*	16,777,214
Class B	128-191	10000000 to 10111111	65,534
Class C	192-223	11000000 to 11011111	254

*127 (01111111) is a Class A address reserved for loopback testing and cannot be assigned to a network.

Fig. 2.11 Numero de Hosts por clase de IP (Cisco Systems, 2007).

2.4.1.3 Clase A

Bien sabemos que las direcciones IP se conforman de 4 octetos por lo que en la clase A se toma el primer octeto para representar las redes y los octetos restantes, nos sirven para representar los Host que contendrá la red. En el caso de esta clase de redes el primer bit, del primer octeto siempre será “0”, como bien se ocupa el primer bit los 7 restantes nos

sirven para representar las redes por lo que podemos tener 128 (01111111) redes de la clase A, aunque en realidad tiene 126 redes, ya que las redes que empiezan en cero (00000000) y por 127 (01111111) están reservadas.

Cada una de las redes puede tener 16,777,216 Host, aunque en realidad tienen 16,777,214 Host ya que se reservan aquellas direcciones de Host que todos los valores sean ceros o unos.

Las direcciones de la clase A se encuentran comprendidas en el rango de 0.0.0.0. y 127.255.255.255. y la máscara de subred será de 255.0.0.0.

2.4.1.4 Clase B

En esta clase se usan los primero 2 octetos de la dirección IP para representar las direcciones de red, aunque los primeros dos bits siempre serán 10 por lo que solo se usaran 14 bit de los dos primeros octetos. Y los otros 2 octetos restantes se usan para representar las direcciones de Host, por lo que esta clase permite tener un máximo de redes de 16,384 y cada red puede tener un máximo de 65,536 Host, aunque como bien sabemos en realidad serian 65,534 porque se reservan todas aquellas direcciones de Host que sus valores sean ceros o bien sean unos.

Las direcciones están comprendidas entre 128.0.0.0 y 191.255.255.255 con una máscara de subred de 255.255.0.0.

2.4.1.5 Clase C

En la clase C se utilizan los 3 primeros octetos para las direcciones de red de los cuales se usan 21 bits ya que estas clases siempre inician en el primer octeto con el valor 110 (11000000) y el ultimo octeto sirve para direcciones de red, lo que nos permite tener un máximo de 2,097,152 redes y cada una de las redes puede tener un 256 Host o como bien sabemos 254 ya que las direcciones en ceros y unos están reservadas. Las direcciones están comprendidas entre 192.0.0.0 y 223.255.255.255 y la mascará de subred en esta clase será de 255.255.255.0.

2.5 Modelo de referencia OSI

A principios de la década de 1980 se produjo un enorme crecimiento en la cantidad y el tamaño de las redes. A medida que las empresas tomaron conciencia de las ventajas de usar tecnología de networking, las redes se agregaban o expandían a casi la misma velocidad a la que se introducían las nuevas tecnologías de red (CISCO, 2011).

Para mediados de la década de 1980, estas empresas comenzaron a sufrir las consecuencias de la rápida expansión. De la misma forma en que las personas que no hablan un mismo idioma tienen dificultades para comunicarse, las redes que utilizaban diferentes especificaciones e implementaciones tenían dificultades para intercambiar información. El mismo problema surgía con las empresas que desarrollaban tecnologías de networking privadas o propietarias. "Propietario" significa que una sola empresa o un pequeño grupo de empresas controla todo uso de la tecnología. Las tecnologías de networking que respetaban reglas propietarias en forma estricta no podían comunicarse con tecnologías que usaban reglas propietarias diferentes (CISCO, 2011).

Para enfrentar el problema de incompatibilidad de redes, la Organización Internacional de Normalización (ISO) investigó modelos de networking como la red de Digital Equipment Corporation (DECnet), la Arquitectura de Sistemas de Red (SNA) y TCP/IP a fin de encontrar un conjunto de reglas aplicables de forma general a todas las redes. En base a esta investigación, la ISO desarrolló un modelo de red que ayuda a los fabricantes a crear redes que sean compatibles con otras redes (CISCO, 2011).

El modelo de referencia de Interconexión de Sistemas Abiertos (OSI) lanzado en 1984 fue el modelo de red descriptivo creado por ISO. Proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red producidos por las empresas a nivel mundial (CISCO, 2011). En la figura 2.12 se aprecian las capas con las que cuenta dicho modelo al igual observamos como la información se encapsula y desencapsula al enviarse de un Hosts.

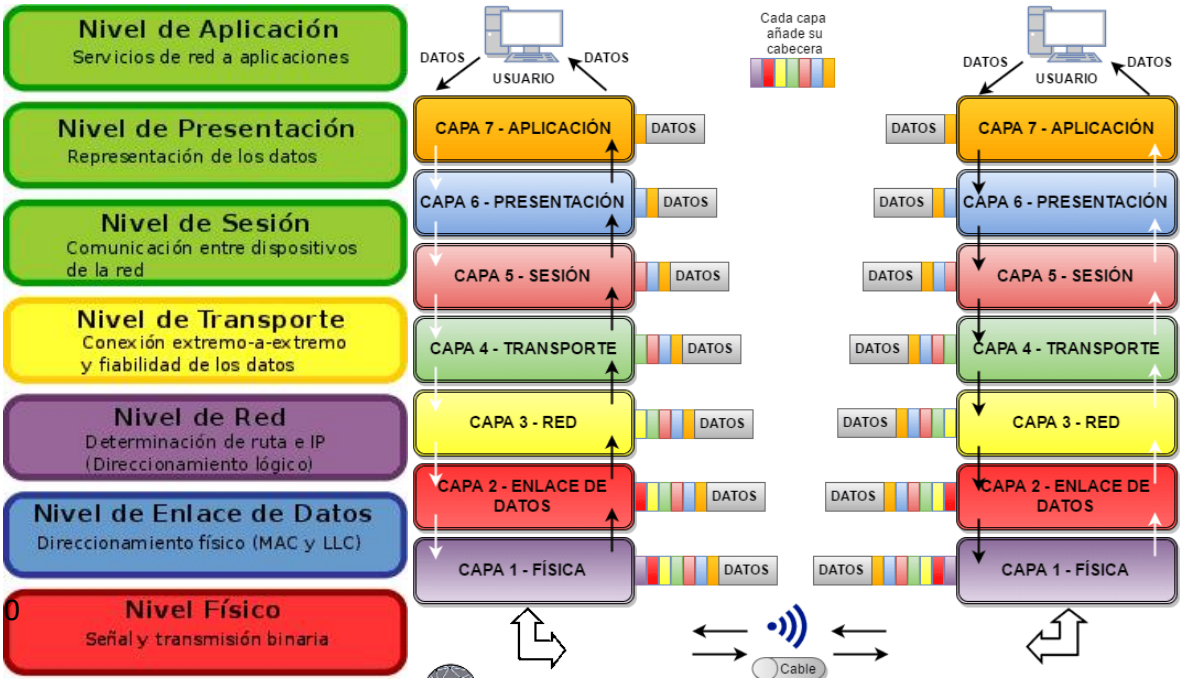


Fig. 2.12 representación de la transferencia de datos del modelo OSI (Vázquez, 10) (Rico, s.f.).

El modelo de referencia OSI es uno de los modelos más reconocido para las comunicaciones por red. Aunque existen diferentes modelos los fabricantes desarrollan más sus productos con base a este modelo de referencia.

2.6 Las capas del modelo OSI

El modelo de referencia OSI sirve para comprender como viaja la información a través de la red. Explica de qué manera los paquetes de datos viajan a través de varias capas de un equipo a otro en una red, sin importar si el emisor y el receptor cuentan con diferentes tipos de medios de red.

El modelo de referencia OSI cuenta con 7 (los cuatro primeros tendrán funciones de comunicación y los tres restantes de proceso). Cada una de las capas dispondrá de los protocolos específico para su control.

2.6.1 Capa física

Comprende las características eléctricas y mecánicas de la red para establecer la conexión física (tarjetas, dimensiones físicas de los conectores, los cables, voltajes, velocidad de transmisión de los datos).

2.6.2 Capa de enlace de datos

Se encargan de establecer y mantener el flujo de datos. Controlar la producción errores y la corrección (se incluye el formato de trama. Los códigos de dirección, el orden de los datos transmitidos, la detección y la recuperación de errores).

- Provee transferencia de datos confiables a través del medio
- Conectividad y selección de ruta entre sistemas.

2.6.3 Capa de red

Se encarga del direccionamiento de los datos dentro de la red (administración y gestión de los datos, la emisión de mensajes y regula el tráfico en la red).

2.6.4 Capa de transporte

Se encarga de asegurar la transferencia de datos a pesar de los fallos presentados en los niveles anteriores (detección de bloqueos, caídas del sistema, asegura la igualdad entre la velocidad de transmisión y recepción y la búsqueda de rutas alternas).

- Se ocupa de aspectos de transporte entre Host.
- Confiabilidad del transporte de datos.
- Establecer, mantener, terminar circuitos virtuales.
- Detección de fallas y control de flujo de información de recuperación.

2.6.5 Capa de sesión

Administra las funciones que permiten que dos usuarios se comuniquen por la red (tareas de seguridad, contraseñas de usuarios y la administración de sistema).

- Establece, administra y termina sesiones entre aplicaciones

2.6.6 Capa de presentación

Traduce la información del formato máquina a un formato comprensible para el usuario (control de impresoras, emulación de terminal y los sistemas de codificación).

- Garantizar que los datos sean legibles para el sistema receptor
- Formato de los datos
- Estructura de datos
- Negocia la sintaxis de transferencia de datos para la capa de aplicación

2.6.7 Capa de aplicación

Es la encarga del intercambio de información entre los usuarios y el sistema operativo (transferencia de archivos y los programas de aplicación).

- Suministra servicios de red a los procesos de aplicaciones (como, por ejemplo, correo electrónico, transferencia de archivos y emulación de terminales).

En la figura 2.13 se muestran los protocolos que más se usan en cada capa del modelo OSI.

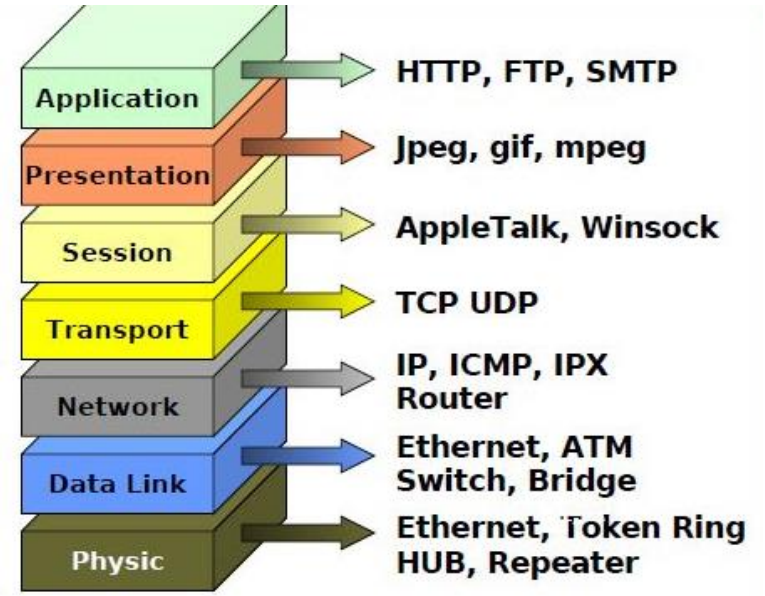


Fig. 2.13 Protocolo usado en cada capa (IDE, 25).

2.7 TCP/IP

El nombre del protocolo proviene de los dos protocolos más importantes de la familia de protocolos internet, el *Transmission Control Protocolo* (TCP) y el *Internet Protocolo* (IP).

La ventaja principal del TCP/IP estriba en que está diseñado para comunicar dispositivos de diferentes tipos, incluyendo PCs, minis y mainframes que ejecutan sistemas operativos distintos, sin importar el tamaño de la red.

La gran desventaja del TCP/IP estriba en la dificultad de su configuración, por ello no es recomendado en redes pequeñas.

TCP/IP fue desarrollado por el departamento de defensa de los EE. UU. (DoD) ejecutándose en *ARPANET* (una red de área extensa del Departamento de Defensa).

TCP/IP transfiere datos mediante el ensamblaje de datos en paquetes. Cada paquete empieza con una cabecera que contienen información de control seguida de los datos.

IP es un protocolo a nivel de red en OSI, permite a las aplicaciones ejecutarse de forma transparente sobre las redes interconectadas.

TCP es un protocolo del nivel de transporte en OSI, que se encarga de que los datos sean entregados tal cual como se mandaron y que los paquetes se reensamblen en el orden que fueron enviados.

El modelo TCP/IP tiene cuatro capas como se observa en la figura 2.14 las capas son:

- Capa de aplicación
- Capa de transporte
- Capa de Internet
- Capa de acceso a la red

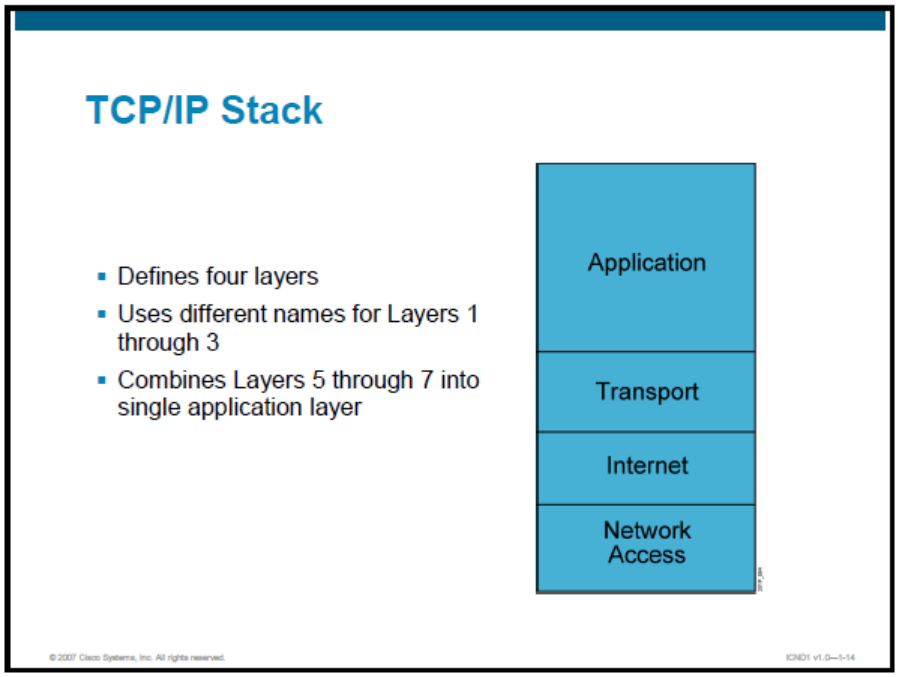


Fig. 2.14 Capas del modelo TCP/IP (Cisco Systems, 2007).

Aunque algunas de las capas del modelo TCP/IP tienen el mismo nombre que las capas del modelo OSI, las capas de ambos modelos no se corresponden de manera exacta.

2.7.1 Capa de aplicación

En el modelo de TCP/IP la capa de aplicación integra los detalles de las capas de sesión y de presentación del modelo OSI. En este modelo la capa de aplicación maneja aspectos de representación, codificación y control de dialogo.

Protocolos más comunes:

- Protocolo de Transferencia de Archivos (FTP)
- Protocolo de Transferencia de Hipertexto (HTTP)
- Protocolo simple de transferencia de correo (SMTP)
- Sistema de denominación de dominios (DNS)
- Protocolo Trivial de Transferencia de Archivos (TFTP)

2.7.2 Capa de transporte

La capa de transporte se encarga de los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Uno de sus protocolos, el protocolo para el control de la transmisión (TCP), ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo (CISCO, 2011).

Protocolos más comunes:

- Protocolo para el Control del Transporte (TCP)
- Protocolo de Datagrama de Usuario (UDP)

2.7.3 Capa de internet

la capa Internet es dividir los segmentos TCP en paquetes y enviarlos desde cualquier red. Los paquetes llegan a la red de destino independientemente de la ruta que utilizaron para llegar allí. El protocolo específico que rige esta capa se denomina Protocolo Internet (IP). En

esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes (CISCO, 2011).

El protocolo más común:

- Protocolo Internet (IP)

2.7.4 Capa de acceso de transporte

A esta capa se le conoce también como la capa de host a red. La capa de acceso de transporte tiene relación con todos los componentes físico como lógicos, necesarios para lograr una conexión física. También se encuentran en esta capa los detalles de tecnología networking, y todos los detalles de las capas física y de enlace de datos del modelo OSI.

2.8 OSI vs TCP/IP

Las similitudes incluyen:

- Ambos se dividen en capas.
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.
- Ambos modelos deben ser conocidos por los profesionales de networking.
- Ambos suponen que se conmutan paquetes. Esto significa que los paquetes individuales pueden usar rutas diferentes para llegar al mismo destino. Esto se contrasta con las redes conmutadas por circuito, en las que todos los paquetes toman la misma ruta.

Las diferencias incluyen:

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.
- TCP/IP combina la capa de enlace de datos y la capa física del modelo OSI en la capa de acceso de red.
- TCP/IP parece ser más simple porque tiene menos capas.
- Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló la Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, por lo general las redes no se desarrollan a partir del protocolo OSI, aunque el modelo OSI se usa como guía.

En la figura 2.15 se aprecia gráficamente las diferencias entre el modelo TCP/IP y el modelo OSI.

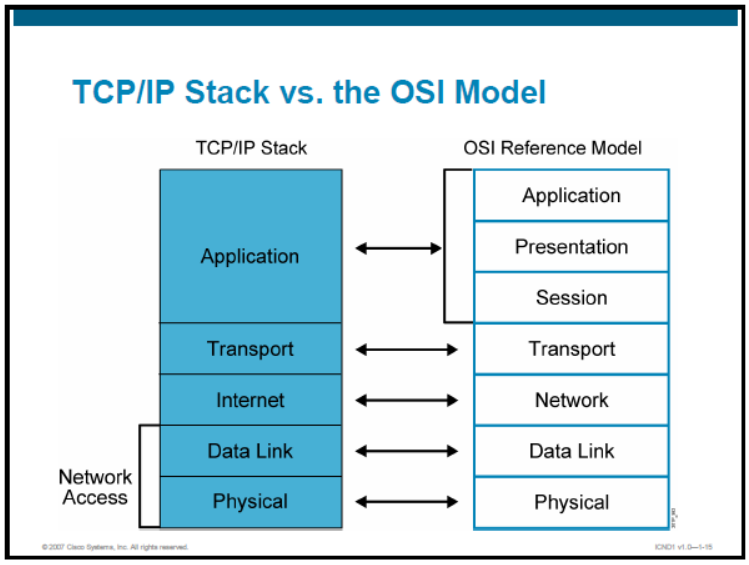


Fig. 2.15 TCP/IP vs. Modelo OSI (Cisco Systems, 2007).

2.9 Mascara de subred

La mascará de subred nos sirve para poder dividir una dirección de red en diferentes subredes dependiendo del número específicos de Host que deseamos se elegirá la subred con el Host más grande para hacer la división a través de este número.

Por lo que la máscara de subred igual ayuda a saber cuál es la dirección de red, con cuantas subredes cuenta la red y los Host con los que cuenta cada subred.

2.10 Subnetting

El subnetting no es más que la subdivisión de una red en varias subredes. El subneteo permite a los administradores de red puedan dividir una red en varias subredes. Esto se traduce en que el router que establece la conexión entre la red e Internet se especifica como dirección única, aunque puede que haya varios hosts ocultos. Así, el número de hosts que están a disposición del administrador aumenta considerablemente.

En el subnetting se toman bits del host ID “prestados” para crear una subred. Con solo un bit se tiene la posibilidad de generar dos subredes, puesto que solo se tiene en cuenta el 0 o el 1. Para un número mayor de subredes se tienen que liberar más bits, de modo que hay menos espacio para direcciones de hosts.

2.11 Direcciones de red

Una dirección IP que tiene en 0s todos los bits de host está reservada para la dirección de red.

Por ejemplo, la red de Clase A, 10.0.0.0 contiene al host 10.1.2.3.

Una red de Clase B puede ser la 172.16.0.0 y una dirección de Clase C puede ser la 192.16.1.0. Un ruteador utiliza la dirección de red cuando busca en su tabla de ruteo IP a una dirección destino. Un ejemplo de una dirección IP para un dispositivo en la red 172.16.0.0 sería la 172.16.16.1. En este ejemplo, 172.16 es la porción de dirección de red y 16.1 es la porción de dirección de usuarios (hosts).

2.12 Directed Broadcast Address

Para enviar datos a todos los dispositivos en una red, se utiliza la dirección de Broadcast. La dirección de Broadcast IP termina con los bits de la parte de hosts en 1s. Por ejemplo, para la red 172.16.0.0 en la cual los últimos 16 bits forman la parte del campo de hosts, el broadcast que se enviaría a todos los destinatarios de esta red sería con la dirección 172.16.255.255. El directed broadcast es capaz de ser ruteado. Para algunas versiones de CISCO IOS operating system, el rutero de este directed broadcasts no es una condición establecida por default.

2.13 Local Broadcast Address

Si un dispositivo con una dirección IP quiere comunicarse con todos los dispositivos en la red local, este pone como dirección destino todos los bits en 1s (255.255.255.255) y transmite el paquete. Por ejemplo, los hosts que no conocen su número de red y preguntan a algún servidor pueden utilizar esta dirección. El local broadcast nunca es ruteado.

2.14 Network ID

La porción de red de una dirección IP siempre se refiere al identificador de la red, la cual es importante para saber cuáles usuarios se podrán comunicar directamente entre ellos ya que los hosts que estén dentro de la misma red tendrán comunicación sin necesidad de utilizar un enrutador (router).

Un network ID permite al router poner un paquete en el segmento apropiado. El host ID ayuda al router para entregar el paquete a un usuario (host) específico en la red. Como resultado, la dirección IP es mapeada a la dirección MAC correcta, necesario para el proceso de capa 2 en el router para direccionar la trama.

2.15 Host ID

Cada clase de red permite cierto número de hosts. En una red de Clase A, el primer octeto es asignado a la red, dejando los últimos tres octetos para ser asignados a los hosts. La primera dirección en cada red (todos los bits de hosts en 0s) está reservada para la dirección de red y la dirección final de cada red (todos los bits en 1s) está reservada para la dirección de broadcast. El número máximo de hosts de una red Clase A es 224-2 (se resta tanto la dirección de red como la de broadcast) o 16,777,214.

En una red de Clase B, los primeros dos octetos son asignados a la red, dejando los últimos dos para ser asignados a los hosts. El número máximo de hosts en una red Clase B son 216-2 o 65,534.

2.16 Direcciones públicas y privadas

Las redes que se conectan con otras a través de internet son consideradas redes públicas y las que no, se consideran redes privadas.

2.16.1 Direcciones publicas

Es la que tiene asignada cualquier equipo o dispositivo conectado de forma directa a Internet.

Las IP públicas son siempre únicas. No se pueden repetir. Dos equipos con IP de ese tipo pueden conectarse directamente entre sí.

LA ICANN que es una organización que opera a nivel multinacional/internacional y es la responsable de asignar las direcciones del protocolo IP, de los identificadores de protocolo, de las funciones de gestión del sistema de dominio y de la administración del sistema de servidores raíz.

ICANN se dedica a preservar la estabilidad de Internet por medio de procesos basados en el consenso.

En la figura 2.16 se muestra los rangos de las direcciones IP publicas dependiendo la clase de dirección.

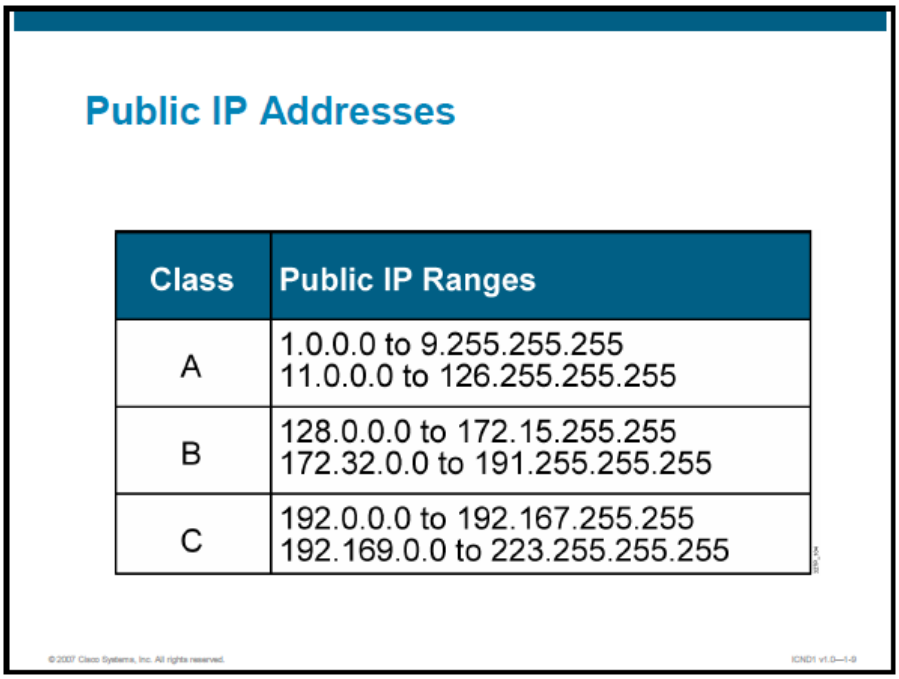


Fig. 2.16 direcciones públicas (Cisco Systems, 2007).

2.16.2 Direcciones privadas

Se utiliza para identificar equipos o dispositivos dentro de una red doméstica o privada. En general, en redes que no sean la propia Internet y utilicen su mismo protocolo.

Las IP privadas están en cierto modo aisladas de las públicas. Se reservan para ellas determinados rangos de direcciones.

Son estos para IPv4:

CLASE a 10.0.0.0 a 10.255.255.255

CLASE B 172.16.0.0 a 172.31.255.255

CLASE C 192.168.0.0 a 192.168.255.255

2.17 Tecnología Ethernet

La tecnología ethernet es un estándar que se usa en las redes LAN para computadores con acceso al medio por detección de la onda portadora y con detección de colisiones (CSMA/CD). Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI, por lo que esta tecnología opera tanto en la capa física como en la de enlace de datos.

2.17.1 Características de la tecnología Ethernet

El sistema Ethernet tiene cuatro elementos básicos:

El medio físico: compuesto por los cables, radiotransmisores y otros elementos de hardware, como conectores, utilizados para transportar la señal entre los computadores conectados a la red.

Los componentes de señalización: dispositivos electrónicos estandarizados (transceivers) que envían y reciben señales sobre un canal Ethernet.

El conjunto de reglas para acceder el medio: protocolo utilizado por la interfaz (tarjeta de red) que controla el acceso al medio y que les permite a los computadores acceder (utilizar) de forma compartida el canal Ethernet. Existen dos modos: half y full dúplex.

La trama Ethernet: conjunto de bits organizados de forma estándar, la forma en la que se organiza la trama se puede observar en la figura 2.17. La trama es utilizada para llevar los datos dentro del sistema Ethernet. También recibe el nombre de marco o frame.

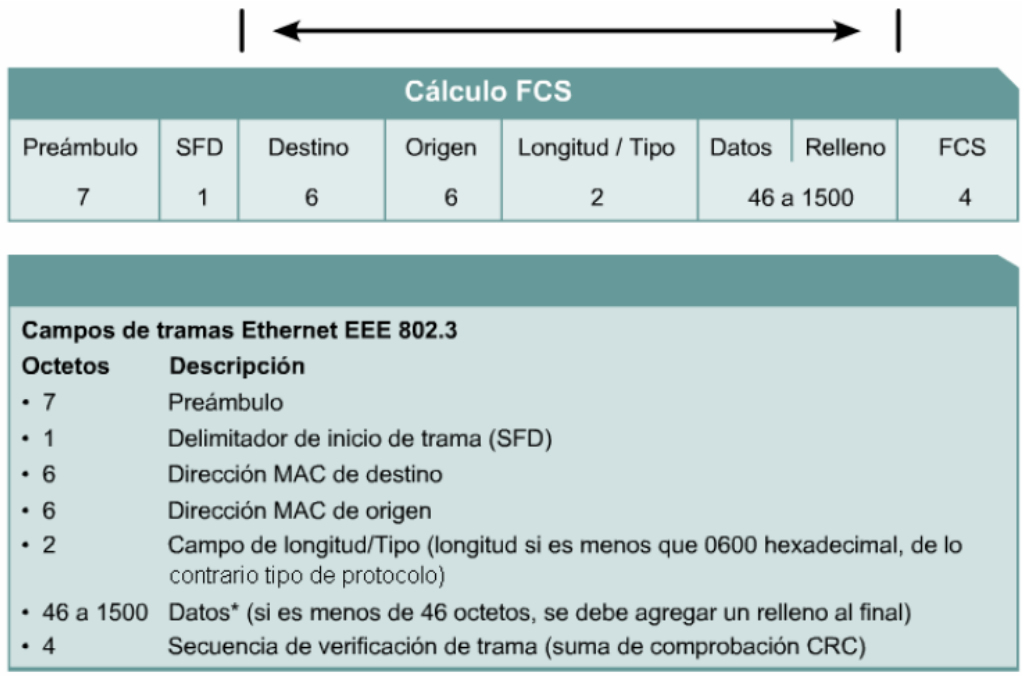


Fig. 2.17 Estructura de la trama (CISCO, 2011).

2.17.2 Direcciones MAC

Las direcciones MAC (Media Access Control) están formadas por 48 bits que se representan por dígitos hexadecimales que se agrupan en 6 parejas las cuales se separan entre sí, ya sea por dos puntos o mediante guiones.

Un ejemplo de una dirección MAC es la siguiente: 01:F1:B1:C4:B2:A6.

Las tarjetas de red tipo Ethernet alojan este número en un espacio de memoria. La dirección MAC es también llamada dirección física porque identifica físicamente a un elemento del hardware. Cada tarjeta MAC viene de fábrica con un número MAC distinto. La mitad de los bits de la dirección MAC son usados para identificar al fabricante de la tarjeta y los otros 24

bits son usados para diferenciar a cada tarjeta producida por ese fabricante (Internetmania).

2.17.3 Direcciones Unicast, Multicast y Broadcast

Una dirección Unicast: es aquella que identifica una sola estación de la red. Las direcciones Unicast en Ethernet se reconocen porque el primer byte de la dirección MAC es un número par (al transmitir se envía primero un cero). Por ejemplo: f2:3e:c1:8a:b1:01 es una dirección unicast porque “f2” (242) es un número par (Selvas, 1).

Una dirección de Multicast permite que un solo frame Ethernet sea recibido por varias estaciones a la vez. En Ethernet las direcciones multicast se representan con un número impar en su primer octeto (al transmitir al medio se envía primero un uno). Por ejemplo: 01:00:81:00:01:00 es multicast pues “01” es un número impar (Selvas, 1).

Una dirección de Broadcast permite que un solo frame sea recibido por todas las estaciones que vean el frame. La dirección de broadcast tiene todos los 48 bits en uno (ff:ff:ff:ff:ff:ff). Una dirección Broadcast es un caso especial de dirección Multicast (Selvas, 1).

En la figura 2.18 se aprecia gráficamente como es una dirección unicast a un solo destino, una dirección multicast a muchos destinos y una dirección broadcast que es a todos los destinos dentro de la red.

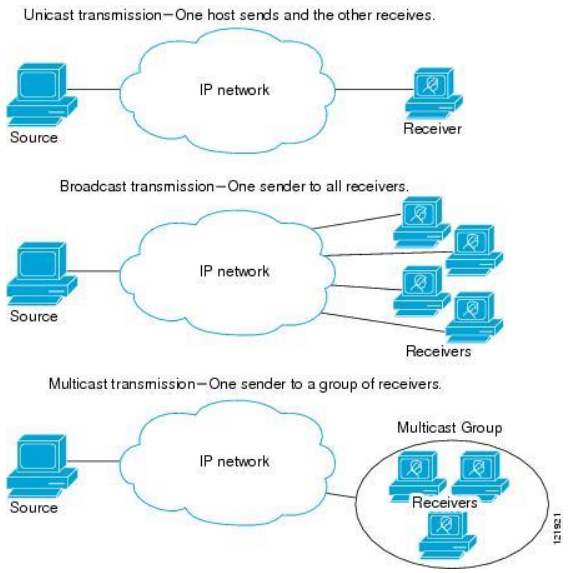


Fig. 2.18 Dirección unicast, multicast y broadcast (CISCO).

2.17.4 Algoritmo CSMA/CD

El algoritmo CSMA/CD (por sus siglas en inglés: Carrier Sense Multiple Access with Collision Detection) o, en español, acceso múltiple con detección de portadora y detección de colisiones, es un algoritmo que se encarga del control del acceso al medio. Este algoritmo se usa principalmente en redes ethernet. En este algoritmo las estaciones escuchan el medio antes de transmitir, es decir, se necesita escuchar si el canal esta libre para poder llevar a cabo la transmisión. Además, se mejora el rendimiento de CSMA finalizando el envió cuando se detecta una colisión.

Carrier sense: monitorea el bus para determinar si hay una transmisión.

Múltiple Access: más de un nodo puede intentar transmitir datos al mismo tiempo.

Collision Detection: un nodo de la red puede determinar si su propia transmisión se ha corrompido.

En la figura 2.19 se observa cómo trabaja el algoritmo CSMA/CD primero se lleva acabo el Carrier Sense, seguido del Multiple Access y por último Collision Detection.

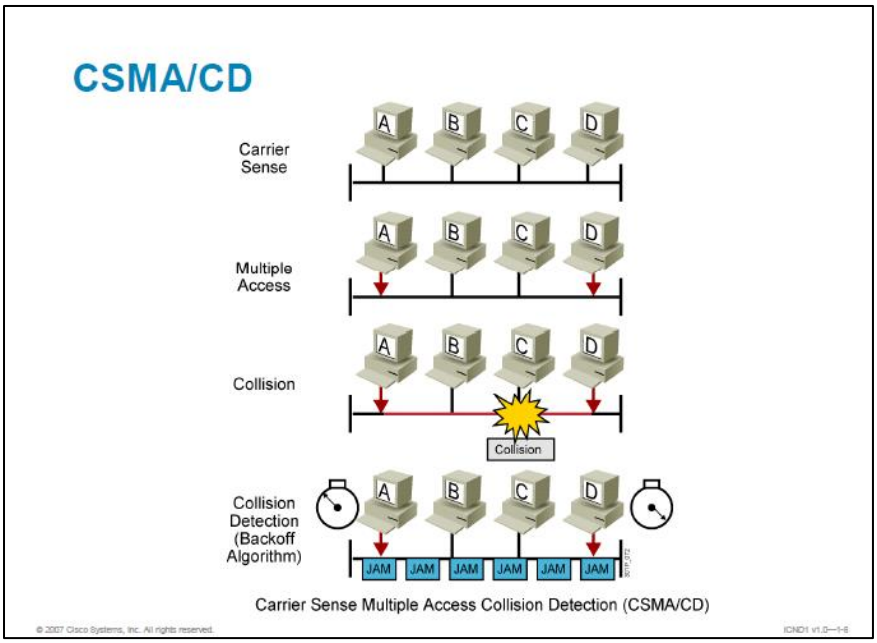


Fig. 2.19 Funcionamiento del algoritmo CSMA/CD (Cisco Systems, 2007).

2.17.5 Redes ethernet

En la tabla 2.2 se encuentra los diferentes tipos de tecnología Ethernet al igual que sus características de cada una de ellas.

Tecnología	Velocidad de transmisión	Tipo de cable	Distancia máxima	Topología
10Base2	10 Mbit/s	Coaxial	185 m	Bus (Conector T)
10BaseT	10 Mbit/s	Par Trenzado	100 m	Estrella (Hub o Switch)
10BaseF	10 Mbit/s	Fibra óptica	2000 m	Estrella (Hub o Switch)
100BaseT4	100 Mbit/s	Par Trenzado (categoría 3UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (switch)
100BaseTX	100 Mbit/s	Par Trenzado (categoría 5UTP)	100 m	Estrella. Half Duplex (hub) y Full Duplex (switch)
100BaseFX	100 Mbit/s	Fibra óptica	2000 m	No permite el uso de hubs
1000BaseT	1000 Mbit/s	(categoría 5e o 6UTP)	100 m	Estrella. Full Duplex (switch)
1000BaseSX	1000 Mbit/s	Fibra óptica (multimodo)	550 m	Estrella. Full Duplex (switch)
1000BaseLX	1000 Mbit/s	Fibra óptica (monomodo)	5000 m	Estrella. Full Duplex (switch)

Tabla 2.2 Tipo de cable según el protocolo Ethernet.

2.18 ¿Qué es una VLAN?

VLAN es el acrónimo de virtual LAN (Red de Área Local), las VLANs son redes lógicas que se encuentran dentro de una misma red física. En una red física pueden coexistir muchas redes VLAN. La ventaja de usar las VLANs es que ayudan a reducir el dominio de difusión y a la administración de la red, separando las redes lógicas y que no deberían intercambiar datos de la red física.

Una VLAN tiene dos o más estaciones que se comportan como si estuviesen conectados al mismo conmutador, aunque se encuentren físicamente conectados a diferentes segmentos de una red de una LAN.

En la figura 2.20 nos muestra como son las VLANs podemos apreciar que, aunque correspondan a diferentes redes estas se puedan agrupar como si pertenecieran a una misma red y compartir recursos.

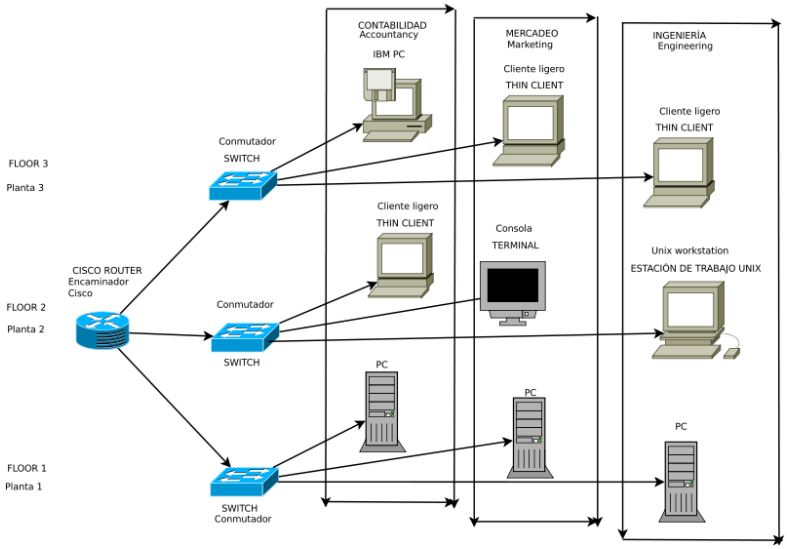


Fig. 2.20 Ejemplo de una VLAN (wikipedia, 2012).

2.18.1 Directrices para aplicar direccionamiento IP.

- Asignar una subred IP por VLAN
- Declarar espacios de direcciones IP en bloques contiguos (sumarización).

2.19 Enrutamiento

El enrutamiento es el proceso usado por el router para enviar paquetes a la red de destino. Un router toma decisiones en función de la dirección de IP de destino de los paquetes de datos. Todos los dispositivos intermedios usan la dirección de IP de destino para guiar el paquete hacia la dirección correcta, de modo que llegue finalmente a su destino. A fin de tomar decisiones correctas, los routers deben aprender la ruta hacia las redes remotas. Cuando los routers usan enrutamiento dinámico, esta información se obtiene de otros routers. Cuando se usa enrutamiento estático, el administrador de la reconfigura manualmente la información acerca de las redes remotas (CISCO, 2011).

2.20 Enrutamiento estático.

Las rutas estáticas son aquellas en la que un administrador de la red configure manualmente las rutas que deberá seguir el enrutador para poder llegar de una estación a otra. Por lo que cualquier cambio en la red tiene que ser configurado manualmente, dado que este trabajo lo tiene que realizar una persona y dependiendo del tamaño de la red puede que el enrutamiento estático no sea el más adecuado ya que llevaría mucho tiempo realizarlo en una red grande, por este motivo es más factible usarlo en redes pequeñas. Debido a los requisitos de administración adicionales, el enrutamiento estático no tiene la escalabilidad o capacidad de adaptarse al crecimiento del enrutamiento dinámico. Aun en redes de gran tamaño, a menudo se configuran rutas estáticas, cuyo objetivo es satisfacer requerimientos específicos, junto con un protocolo de enrutamiento dinámico.

2.21 Enrutamiento dinámico

Un protocolo de enrutamiento es el esquema de comunicación entre routers. Un protocolo de enrutamiento permite que un router comparta información con otros routers, acerca de las redes que conoce, así como de su proximidad a otros routers. La información que un router obtiene de otro, mediante el protocolo de enrutamiento, es usada para crear y mantener las tablas de enrutamiento (CISCO, 2011).

Ejemplos de protocolos de enrutamiento:

- Protocolo de información de enrutamiento (RIP)
- Protocolo de enrutamiento de gateway interior (IGRP)
- Protocolo de enrutamiento de gateway interior mejorado (EIGRP)
- Protocolo "Primero la ruta más corta" (OSPF)

2.21.1 Protocolos de enrutamiento

Un router puede utilizar un protocolo de enrutamiento de paquetes IP para llevar a cabo el enrutamiento. Esto lo realiza mediante la implementación de un algoritmo de enrutamiento específico y emplea la capa de interconexión de redes del conjunto de protocolos TCP/IP. Algunos ejemplos de protocolos de enrutamiento de paquetes IP son:

- **RIP**: Un protocolo de enrutamiento interior por vector-distancia.
- **IGRP**: El protocolo de enrutamiento interior por vector-distancia de Cisco.
- **OSPF**: Un protocolo de enrutamiento interior de estado del enlace
- **EIGRP**: El protocolo mejorado de enrutamiento interior por vector-distancia de Cisco.
- **BGP**: Un protocolo de enrutamiento exterior por vector-distancia

El Protocolo de información de enrutamiento (RIP) fue descrito originalmente en el RFC 1058. Sus características principales son las siguientes:

- Es un protocolo de enrutamiento por vector-distancia.
- Utiliza el número de saltos como métrica para la selección de rutas.
- Si el número de saltos es superior a 15, el paquete es desechado.
- Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 30 segundos.

El Protocolo de enrutamiento interior de gateway (IGRP) es un protocolo patentado desarrollado por Cisco. Entre las características de diseño claves del IGRP se destacan las siguientes:

- Es un protocolo de enrutamiento por vector-distancia.
- Se considera el ancho de banda, la carga, el retardo y la confiabilidad para crear una métrica compuesta.
- Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 90 segundos.

El protocolo público conocido como "Primero la ruta más corta" (OSPF) es un protocolo de enrutamiento de estado del enlace no patentado. Las características clave del OSPF son las siguientes:

- Es un protocolo de enrutamiento de estado del enlace.
- Es un protocolo de enrutamiento público (open standard), y se describe en el RFC 2328.
- Usa el algoritmo SPF para calcular el costo más bajo hasta un destino.

- Las actualizaciones de enrutamiento producen un gran volumen de tráfico al ocurrir cambios en la topología.

El EIGRP es un protocolo mejorado de enrutamiento por vector-distancia, patentado por Cisco. Las características claves del EIGRP son las siguientes:

- Es un protocolo mejorado de enrutamiento por vector-distancia.
- Utiliza balanceo de carga asimétrico.
- Utiliza una combinación de los algoritmos de vector-distancia y de estado del enlace.
- Utiliza el Algoritmo de actualización difusa (DUAL) para el cálculo de la ruta más corta.
- Las actualizaciones son mensajes de multicast a la dirección 224.0.0.10 generadas por cambios en la topología.

El Protocolo de gateway de frontera (BGP) es un protocolo de enrutamiento exterior. Las características claves del BGP son las siguientes:

- Es un protocolo de enrutamiento exterior por vector-distancia.
- Se usa entre ISPs o entre los ISPs y sus clientes.
- Se usa para enrutar el tráfico de Internet entre sistemas autónomos.

2.22 Protocolo OSPF

Open Shortest Path First (OSPF) 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).

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 uno de estos 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.

Los tres componentes principales del protocolo de routing OSPF incluyen lo siguiente:

- **Estructuras de datos**

  OSPF crea y mantiene tres bases de datos:

  - **Base de datos de adyacencia:** crea la tabla de vecinos.
  - **Base de datos de estado de enlace (LSDB):** crea la tabla de topología.
  - **Base de datos de reenvío:** crea la tabla de routing.

Estas tablas contienen una lista de routers vecinos para intercambiar información de routing, y se guardan y mantienen en la RAM.

- **Mensajes de protocolo de routing**

OSPF intercambia mensajes para transmitir información de routing mediante cinco tipos de paquetes. Estos paquetes, los cuales se muestran en la figura 2, son los siguientes:

- Paquete de saludo
- 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 routing a fin de mantener información precisa acerca de la red.

- **Algoritmo**

La CPU procesa las tablas de vecinos y de topología mediante el algoritmo SPF de Dijkstra. El algoritmo SPF se basa en el costo acumulado para llegar a un destino.

El algoritmo SPF crea un árbol SPF posicionando cada router en la raíz del árbol y calculando la ruta más corta hacia cada nodo. Luego, es utilizado para calcular las mejores rutas. OSPF coloca las mejores rutas en la base de datos de reenvío, que son usadas para crear la tabla de routing.

2.23 Protocolo EIGRP

El IGRP utiliza la tecnología de ruteo del vector de distancia. El concepto es que cada router no necesita conocer todas las relaciones del router/del link para toda la red. Cada router anuncia destinos con una distancia correspondiente. Cada router que escucha la información ajusta la distancia y la propaga a los routers vecinos.

Se representa a la información de distancia en IGRP como un compuesto de ancho de banda disponible, demora, uso de carga y confiabilidad de link. Esto permite afinar las características del link para alcanzar trayectos óptimos.

El EIGRP es una versión mejorada de IGRP. La tecnología de vector de igual distancia que se usa en IGRP también se emplea en EIGRP. Además, la información de la distancia subyacente no presenta cambios. Las propiedades de convergencia y la eficacia de operación de este protocolo han mejorado significativamente. Esto permite una arquitectura mejorada y, a la vez, retiene la inversión existente en IGRP.

El algoritmo difusor de actualización (DUAL) es el algoritmo usado para obtener la loop-libertad en cada instante en un cómputo de la ruta. Esto les permite a todos los routers involucrados en una topología cambiar para sincronizarse al mismo tiempo. Los routers que no se ven afectados por los cambios de topología no se incluyen en el recálculo. El tiempo de convergencia con DUAL compite con el de cualquier otro protocolo de ruteo existente.

EIGRP ha sido extendido para que sea independiente del protocolo de la capa de red, y así permita que DUAL soporte otros conjuntos de protocolos.

EIGRP tiene cuatro componentes básicos:

- Recuperación/Detección de vecino
- Protocolo de transporte confiable
- Máquina de estados finitos DUAL
- Módulos dependientes del protocolo

La detección o recuperación de vecinos es el proceso que utilizan los routers para aprender dinámicamente de otros routers conectados directamente a sus redes. Los routers también deben detectar cuando sus vecinos se vuelven inalcanzables o dejan de funcionar. Este proceso se logra con carga general baja al enviar pequeños paquetes de saludo. Mientras se reciben paquetes de saludo, un router puede determinar que un vecino está activo y en funcionamiento. Una vez que esto se determina, los routers de la vecindad pueden intercambiar información del ruteo.

El transporte confiable es responsable de garantizado, las entregas ordenadas de paquete EIGRP a todos los vecinos. Soporta la transmisión de multicast o los paquetes de unidifusión entremezclados. Algunos paquetes EIGRP deben transmitirse de manera confiable, mientras que para otros esto no es necesario. Para mayor eficacia, la confiabilidad sólo se brinda cuando es necesaria. Por ejemplo, en una red de acceso múltiple que tiene capacidades de multidifusión, tal como Ethernet, no es necesario enviar saludos confiables a todos los vecinos en forma individual. Entonces, EIGRP envía un saludo de multidifusión único con una indicación en el paquete que informa a los receptores que dicho paquete no necesita ser reconocido. Otros tipos de paquetes, como las actualizaciones, requieren reconocimiento y eso se indica en el paquete.

La máquina de estados finitos DUAL contiene el proceso de decisión de todos los cálculos de rutas. Rastrea todas las rutas anunciadas por todos los vecinos. La información de distancia, conocida como métrica, se usa mediante DUAL para seleccionar trayectos eficientes sin loops. DUAL selecciona las rutas que se insertarán en una tabla de ruteo, según los sucesores factibles. Un sucesor es un router vecino utilizado para el reenvío de paquetes que tenga el trayecto de menor costo a un destino que no es parte de un loop de ruteo. Cuando no existen sucesores factibles, pero si hay vecinos que anuncian el destino, se debe realizar un recálculo. Éste es el proceso donde se determina un nuevo sucesor. La

cantidad de tiempo necesario para volver a calcular la ruta afecta el tiempo de convergencia. Cuando ocurre un cambio de topología, DUAL prueba sucesores factibles. Si hay sucesores factibles, utilizará ningunos que encuentre para evitar cualquier recálculo innecesario.

Los módulos dependientes de protocolo son responsables de la capa de red, los requisitos del protocolo específico. Por ejemplo, el módulo IP-EIGRP es responsable del envío y de la recepción de paquetes EIGRP que son encapsulados en IP. El IP-EIGRP es responsable de analizar los paquetes EIGRP y la información DUALES de la nueva información recibida. IP-EIGRP solicita a DUAL efectuar decisiones de ruteo, cuyos resultados se almacenan en la tabla de IP Routing. IP-EIGRP es responsable de redistribuir las rutas aprendidas en otros protocolos de IP Routing.

2.24 OSPF vs EIGRP

A continuación, en la tabla 2.3 se pueden analizar las diferencias y similitudes entre el protocolo OSPF y el protocolo EIGRP.

Protocolo	EIGRP	OSPF
Tipo	Vector Distancia	Estado de Enlace
Algoritmo	Diffusing Update Algorithm (DUAL)	Shortest Path First (SPF o Dijkstra)
Distancia Administrativa	5 (Summary), 90 (Internal), 170 (External)	110
Protocolo IP	88	89

Soporte IPv6	Sí	Sí (OSPFv3)
Dirección IP Multicast	224.0.0.10	224.0.0.5 (DR/BDR a DRothers, 224.0.0.6 (DRothers a DR/BDR)
Métrica	Compuesta (Delay, Bandwidth, Load, Reliability, MTU)	Costo (Bandwidth)
Autenticación	MD5	Texto plano, MD5
Convergencia	Instantánea	Lenta
Escalabilidad en redes de gran tamaño	Baja	Alta
Interoperabilidad de fabricantes	No	Sí
Complejidad de troubleshooting	Baja	Alta

Tabla 2.3 Características entre EIGRP y OSPF (Colomès, 15).

Como sabemos los dos protocolos son los más utilizados en el mercado dado que son los que mejor hacen el trabajo, el hecho de que protocolo usar para una red depende de muchos factores del tamaño de la red, de la marca de los dispositivos de la red, ya que el protocolo de EIGRP funciona exclusivamente para dispositivos Cisco.

Finalmente, la decisión de adoptar EIGRP u OSPF en una infraestructura va a depender de múltiples factores, pero yo lo definiría así: (Colomès, 15)

- Si tengo presupuesto disponible y no tengo problemas en comprar equipamiento más caro: EIGRP
- Si en mi red existen dispositivos de múltiples fabricantes: OSPF
- Si lo importante es una red que converja rápido a los cambios: EIGRP
- Si lo importante es controlar una infraestructura muy grande, aun cuando requiera mayor planificación y diseño: OSPF

Capítulo 3. Desarrollo e implementación del proyecto

3.1 Introducción

El proyecto a realizar se refiere a la implementación y puesta en servicio de la red operativa de datos, la cual formara parte de la Red Eléctrica Inteligente (REI). En la Fig. 3.1, se muestra la topología que se desea llegar de la Red Operativa de Datos de CFE Transmisión trabajando en conjunto con la REI.

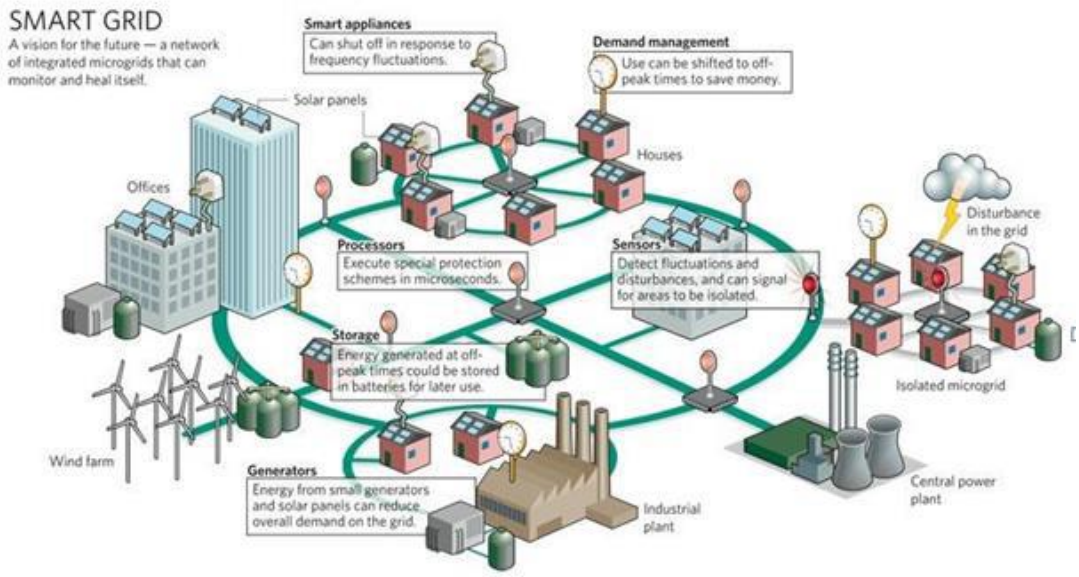


Fig. 3.1 la visualización de CFE de la REI (ESTA International, LLC,

CFE transmisión se compone de 9 gerencias, pero nos centraremos a hablar de la gerencia en la cual se desarrolló el proyecto antes mencionando que es CFE Transmisión Sureste, la gerencia cuenta con 5 zonas, la zona Villahermosa, zona Tuxtla, zona Tapachula, zona Istmo y zona Malpaso.

En la figura 3.2 se puede apreciar la topología de la Red de Datos a grandes rasgos de CFE Transmisión Sureste.

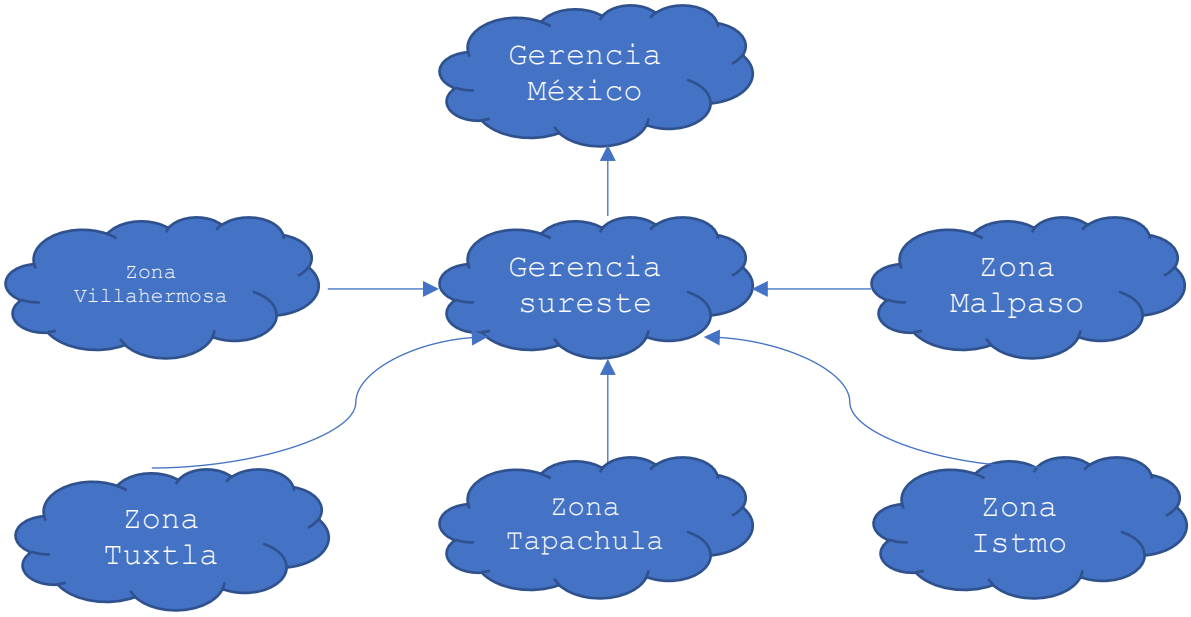


Fig. 3.2 Topología de la Red de Datos de CFE Transmisión Sureste

Como se observa en la figura 3.2 la Red de Datos de CFE Transmisión es bastante grande hablando de que existen 9 gerencias y cada uno cuenta con determinadas zonas, es por ello que lo realizado a continuación se llevó acabo en la gerencia y dos zonas más de CFE Transmisión Sureste. En la gerencia, donde es encontrado el Hotel Telecom fue donde se llevó la programación y en las dos zonas fue por vía remota.

A continuación, se mostrará lo que se realizó para llevar a cabo el proyecto, se empieza con lo que es el Subneteo, proceso fundamental para el desarrollo de una red. El Subneteo en esta ocasión es demostrativo para poder comprender de donde provienen las direcciones IP, debido a que CFE Transmisión ya tiene designada su red y lleva años trabajando en ella, cuenta con una base de datos proveniente de la Gerencia de México con la red subneteada con todas las IP disponible.

Después del Subneteo se empezó con la programación de switch capa 2 para poder crear VLANs. Posteriormente se realizó la programación en router o switch capa 3 para poder enrutar paquetes de datos entre diferentes redes y VLANs. Por último, se llevó acabo el enrutamiento dinámico que es indispensable dado que la Red de Datos trabaja con el enrutamiento OSPF.

3.2 Problemas de Subneteo

Problema 1. subnetear la IP de red 192.168.0.0/24 en 4 subredes

paso1 convertimos la máscara de subred dada a binario para un mejor análisis.

Mascara de subred en binario: 11111111.11111111.11111111.00000000

paso2 analizamos cuantas subredes deseamos

Numero de subredes deseadas: 4

paso3 calculamos cuantos son los bits que prestaremos con la fórmula 2^N (donde N es el número de bits prestados de la parte Host) de la parte de Hosts de la red para poder obtener nuestras subredes. El valor de 2^N debe de ser mayor o igual que el número de nuestras subredes deseadas.

Números de bits prestados: $2^N=2^2=4$ subredes

paso4 Calculamos la nueva mascara para nuestras nuevas subredes, donde los bits prestados se convierten en uno.

Calcular nueva máscara de subred: 11111111.11111111.11111111.(11)000000/26

paso5 este paso nos sirve para saber cuántos Hosts tendremos disponibles por subred

Numero de Hosts por subred. $2^m-2=2^6-2=62$ Hosts.

En la tabla 3.1 se muestra el desarrollo del Subneteo para poder ver nuestras redes, los Hosts utilizables y la dirección de broadcast.

Primer octeto	Segundo octeto	Tercer octeto	Cuarto octeto		Redes
11000000	10101000	00000000	00	000000	1 Red
11000000	10101000	00000000	00	000001	1 Host
11000000	10101000	00000000	00	111110	Ult. Host
11000000	10101000	00000000	00	111111	Broadcast

11000000	10101000	00000000	01	000000	2 Red
11000000	10101000	00000000	01	000001	1 Host
11000000	10101000	00000000	01	111110	Ult. Host
11000000	10101000	00000000	01	111111	Broadcast
11000000	10101000	00000000	10	000000	3 Red
11000000	10101000	00000000	10	000001	1 Host
11000000	10101000	00000000	10	111110	Ult. Host
11000000	10101000	00000000	10	111111	Broadcast
11000000	10101000	00000000	11	000000	4 Red
11000000	10101000	00000000	11	000001	1 Host
11000000	10101000	00000000	11	111110	Ult. Host
11000000	10101000	00000000	11	111111	Broadcast

Tabla 3.1 Desarrollo del Subneteo para la identificación de nuestras redes.

En la tabla 3.2 se muestra el resulta final más simplificado del Subneteo anteriormente realizado en el cual vemos los números de subredes con los que contamos, las direcciones de subred, los Hosts utilizables por subred y la dirección de broadcast.

N°	Subred	Primera utilizable	Ultima utilizable	Broadcast
1	192.168.0.0	192.168.0.1	192.168.0.62	192.168.0.63
2	192.168.0.64	192.168.0.65	192.168.126	192.168.0.127
3	192.168.0.128	192.168.0.129	192.168.0.190	192.168.0.191
4	192.168.0.192	192.168.0.193	192.168.0.254	192.168.0.255

Tabla 3.2 resultados de nuestro Subneteo por subred en decimal y las IP disponible.

Problema 2. Subnetear la red 10.127.0.0/16 en 8 subredes y la cuarta subred resultante subnetear en 4 subredes.

paso1 Convertimos la máscara de subred dada a binario para un mejor análisis.

Mascara de subred en binario: 11111111.11111111.00000000.00000000

paso2 Analizamos cuantas subredes deseamos

Numero de subredes deseadas: 8

paso3 Calculamos cuantos son los bits que prestaremos con la fórmula 2^N (donde N es el número de bits prestados de la parte Host) de la parte de Hosts de la red para poder obtener nuestras subredes. El valor de 2^N debe de ser mayor o igual que el número de nuestras subredes deseadas.

Números de bits prestados: $2^N = 2^3 = 8$ subredes

paso4 Calculamos la nueva mascara para nuestras nuevas subredes, donde los bits prestados se convierten en uno.

Calcular nueva mascara de subred: 11111111.11111111.11100000.00000000/19

paso5 Este paso nos sirve para saber cuántos Hosts tendremos disponibles por subred, donde m es el numero ceros en la parte de la máscara de subred.

Numero de Hosts por subred. $2^m-2=2^{13}-2=8{,}190$ Hosts.

En la tabla 3.3 se muestra el desarrollo del Subneteo para poder ver nuestras redes, los Hosts utilizables y la dirección de broadcast.

Primer octeto	Segundo octeto	Tercer octeto		Cuarto octeto	Redes
00001010	01111111	000	00000	00000000	1 Red
00001010	01111111	000	00000	00000001	1 Host
00001010	01111111	000	11111	11111110	Ult. Host
00001010	01111111	000	11111	11111111	Broadcast
00001010	01111111	001	00000	00000000	2 Red
00001010	01111111	001	00000	00000001	1 Host
00001010	01111111	001	11111	11111110	Ult. Host
00001010	01111111	001	11111	11111111	Broadcast
00001010	01111111	010	00000	00000000	3 Red
00001010	01111111	010	00000	00000001	1 Host
00001010	01111111	010	11111	11111110	Ult. Host
00001010	01111111	010	11111	11111111	Broadcast
00001010	01111111	011	00000	00000000	4 Red
00001010	01111111	011	00000	00000001	1 Host
00001010	01111111	011	11111	11111110	Ult. Host
00001010	01111111	011	11111	11111111	Broadcast
00001010	01111111	100	00000	00000000	5 Red

00001010	01111111	100	00000	00000001	1 Hosts
00001010	01111111	100	11111	11111110	Ult.Host
00001010	01111111	100	11111	11111111	Broadcast
00001010	01111111	101	00000	00000000	6 Red
00001010	01111111	101	00000	00000001	1 Host
00001010	01111111	101	11111	11111110	Ult. Host
00001010	01111111	101	11111	11111111	Broadcast
00001010	01111111	110	00000	00000000	7 Red
00001010	01111111	110	00000	00000001	1 Host
00001010	01111111	110	11111	11111110	Ult. Host
00001010	01111111	110	11111	11111111	Broadcast
00001010	01111111	111	00000	00000000	8 Red
00001010	01111111	111	00000	00000001	1 Host
00001010	01111111	111	11111	11111110	Ult. Host
00001010	01111111	111	11111	11111111	Broadcast

Tabla 3.3 Desarrollo del Subneteo para la identificación de nuestras redes.

En la tabla 3.4 se muestra el resultado final simplificado del Subneteo anteriormente realizado en el cual vemos los números de subredes con los que contamos, las direcciones de subred, los Hosts utilizables por subred y la dirección de broadcast.

N°	Subred	Primera utilizable	Ultima utilizable	Broadcast
1	10.127.0.0	10.127.0.1	10.127.31.254	10.127.31.255
2	10.127.32.0	10.127.32.1	10.127.63.254	10.127.63.255
3	10.127.64.0	10.127.64.1	10.127.95.254	10.127.95.255
4	10.127.96.0	10.127.96.1	10.127.127.254	10.127.127.255
5	10.127.128.0	10.127.128.1	10.127.159.254	10.127.159.255

6	10.127.160.0	10.127.160.1	10.127.191.254	10.127.191.255
7	10.127.192.0	10.127.192.1	10.127.223.254	10.127.223.255
8	10.127.224.0	10.127.224.1	10.127.224.254	10.127.224.255

Tabla 3.4 resultados de nuestro Subneteo por subred en decimal y las IP disponible.

De lo anterior que hemos obtenido nos pide subnetear la cuarta red 10.127.96.0 en 4 subredes.

paso1 Convertimos la máscara de subred dada a binario para un mejor análisis.

Mascara de subred en binario: 11111111.11111111.11100000.00000000

paso2 Analizamos cuantas subredes deseamos

Numero de subredes deseadas: 4

paso3 Calculamos cuantos son los bits que prestaremos con la fórmula 2^N (donde N es el número de bits prestados de la parte Host) de la parte de Hosts de la red para poder obtener nuestras subredes. El valor de 2^N debe de ser mayor o igual que el número de nuestras subredes deseadas.

Números de bits prestados: $2^N = 2^2 = 4$ subredes

paso4 Calculamos la nueva mascara para nuestras nuevas subredes, donde los bits prestados se convierten en uno.

Calcular nueva mascara de subred: 11111111.11111111.11111000.00000000/21

paso5 Este paso nos sirve para saber cuántos Hosts tendremos disponibles por subred, donde m es el numero ceros en la parte de la máscara de subred.

Numero de Hosts por subred. $2^m-2=2^{11}-2=2{,}046$ Hosts.

En la tabla 3.5 se muestra el desarrollo del Subneteo para poder ver nuestras redes, los Hosts utilizables y la dirección de broadcast.

Primer octeto	Segundo octeto	Tercer octeto			Cuarto octeto	Redes
00001010	01111111	011	00	000	00000000	1 Red
00001010	01111111	011	00	000	00000001	1 Host
00001010	01111111	011	00	111	11111110	Ult. Host
00001010	01111111	011	00	111	11111111	Broadcast
00001010	01111111	011	01	000	00000000	2 Red
00001010	01111111	011	01	000	00000001	1 Host
00001010	01111111	011	01	111	11111110	Ult. Host
00001010	01111111	011	01	111	11111111	Broadcast
00001010	01111111	011	10	000	00000000	3 Red
00001010	01111111	011	10	000	00000001	1 Host
00001010	01111111	011	10	111	11111110	Ult. Host
00001010	01111111	011	10	111	11111111	Broadcast
00001010	01111111	011	11	000	00000000	4 Red
00001010	01111111	011	11	000	00000001	1 Host

00001010	01111111	011	11	111	11111110	Ult. Host
00001010	01111111	011	11	111	11111111	Broadcast

Tabla 3.5 Desarrollo del Subneteo para la identificación de nuestras redes.

En la tabla 3.6 se muestra el resultado final más simplificado del Subneteo anteriormente realizado en el cual vemos los números de subredes con los que contamos, las direcciones de subred, los Hosts utilizables por subred y la dirección de broadcast.

N°	Subred	Primera utilizable	Ultima utilizable	Broadcast
1	10.127.0.0	10.127.96.1	10.127.103.254	10.127.103.255
2	10.127.104.0	10.127.104.1	10.127.111.254	10.127.111.255
3	10.127.112.0	10.127.112.1	10.127.119.254	10.127.119.255
4	10.127.120.0	10.127.120.1	10.127.127.254	10.127.127.255

Tabla 3.6 resultados de nuestro Subneteo por subred en decimal y las IP disponible.

3.3 Conexiones

Las conexiones a realizar fueron dentro del Hotel Telecom Tuxtla ubicado en la Gerencia de Transmisión Sureste. Las conexiones se hicieron de los enlaces troncales que terminan en los distribuidores de fibra óptica hacia los routers o switch capa 3 posteriormente se realizaron conexión a los switch capa 2 correspondientes, los cables empleados fueron de fibra óptica multimodo.

3.4 Comandos básicos para capa 2

- Enable: Entrar al switch.

- Configure terminal: A modo configuración en el switch

- Vlan “N”: Crear redes de área local virtual, donde N es el numero de la vlan, por ejemplo: vlan 10

- Name “nombre”: Asignar nombre a la vlan, por ejemplo: name administración

- Description: Poner una descripción a una vlan

- Show vlan: Para poder ver las vlan que tiene creadas el switch

- Interface fastethernet “n”: Acceder a una interface fastethernet del switch donde n es el numero de la interface a la que se desea acceder.

- Interface gigabiethernet “n”: Acceder a una interface gigabiethernet del switch donde n es el numero de la interface a la que se desea acceder.

- Switchport mode access: Indicar que la interface a la que hemos accedido se una interface de acceso.

- Switchport access vlan “n”: Indica que dicha interface que es de acceso pertenece a la VLAN “n” donde n es el numero de la VLAN

- Switchport mode trunk: Configurar el puerto como troncal.

- Speed “n”: Indicar la velocidad de la interface. Si es fastethernet puede ser de 10 Mbps o de 100 Mbps, donde n puede ser 10 o puede ser 100, en el caso de una interface gigabitethernet n puede tener valores de 10, 100 o 1000.

- Dúplex full: Configuramos que el puerto sea bidireccional.

- Dúplex half: Configuramos que el puerto sea unidireccional.

3.5 Creación de VLAN en capa 2

Crearemos una red en un simulador propiedad de cisco llamado Cisco Packet Tracer en la cual crearemos cuatro VLAN que llevaran por nombre: SCADA, monitoreo, voz y video, intranet.

Elegimos las direcciones IP por cada VLAN creada:

- SCADA: 10.127.97.0/26
- Monitoreo: 10.127.97.64/26
- Voz y video: 10.127.97.128/26
- Intranet: 10.127.97.192/26

Arrastramos nuestros componentes de la barra de herramientas inferior al área de trabajo nuestros dispositivos, los dos switch y las ocho computadoras como se muestra en la figura 3.3, las cuales simularan nuestros Hosts de cada una de las VLANs.

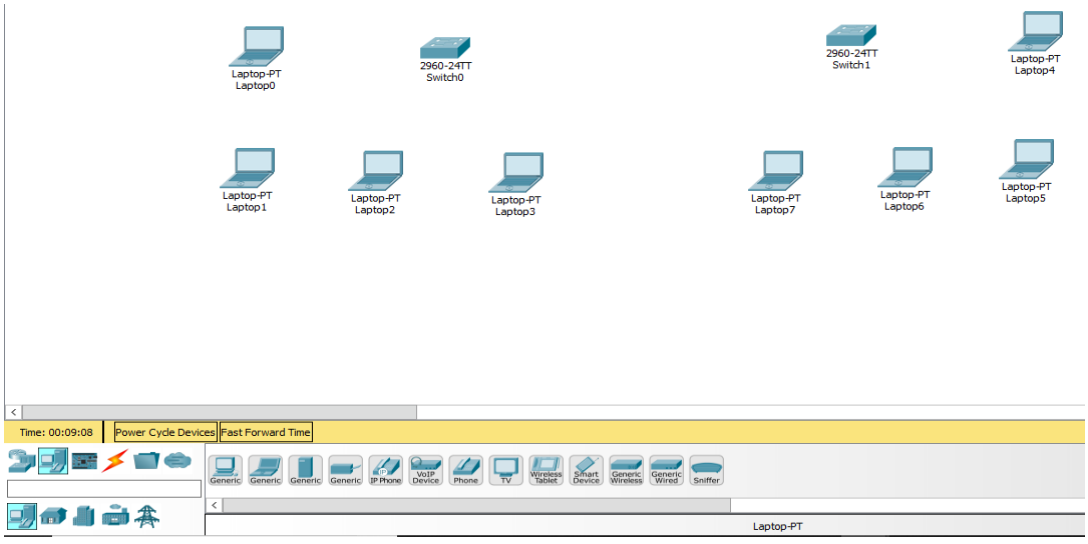


Fig. 3.3 insertar dispositivos al workspace.

Hacemos toda la conexión de nuestra red con cable ethernet directo entre computadora y switch, y cable cruzado entre los switches.

Seleccionamos el cable ethernet directo y conectamos en un extremo a la interface fastethernet0 de la computadora como se muestra en la figura 3.4.

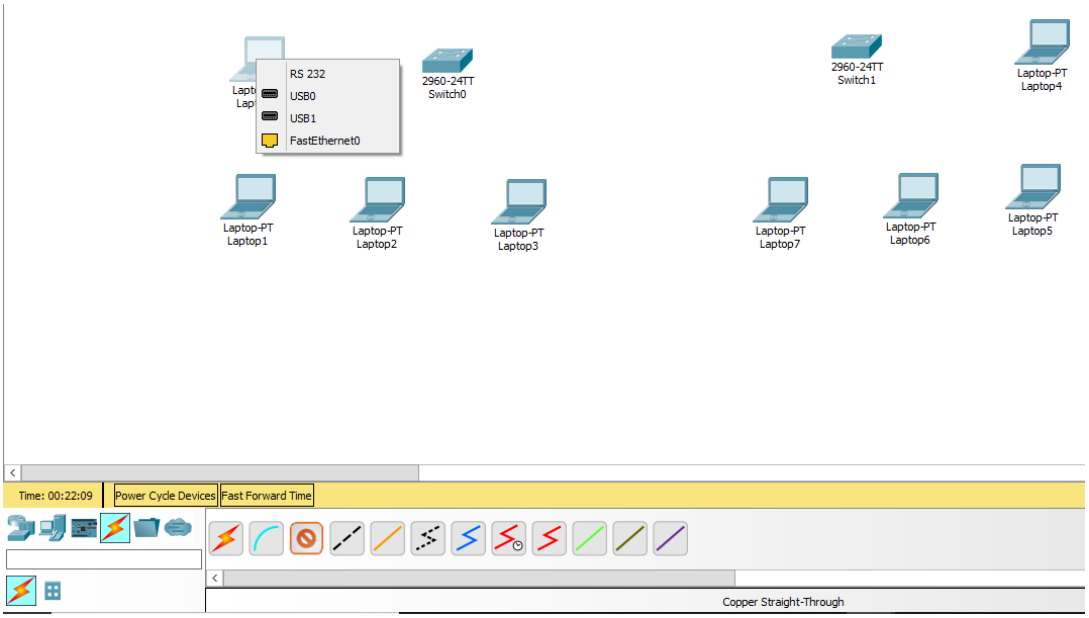


Fig. 3.4 conexión a la computadora.

Conectamos por la otra parte del cable ethernet directo al switch, al área en la cual se llevó a cabo el proyecto se tiene por entendido dejar las primeras cinco interfaces libres para conexiones troncales, es por ello que la conexión se hace a partir de la quinta interface como se muestra en la figura 3.5.

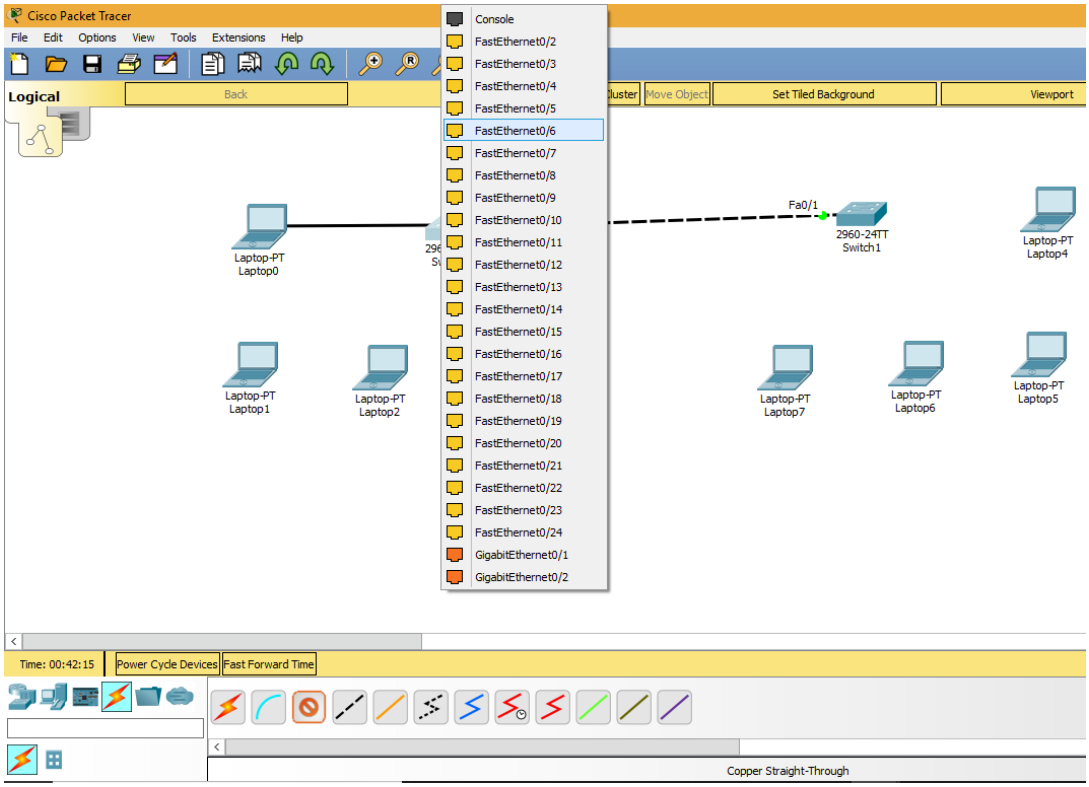


Fig. 3.5 conexión al switch.

Como apreciamos en la figura 3.6 la conexión se hace en la primera interface de cada switch porque estos son enlaces troncales.

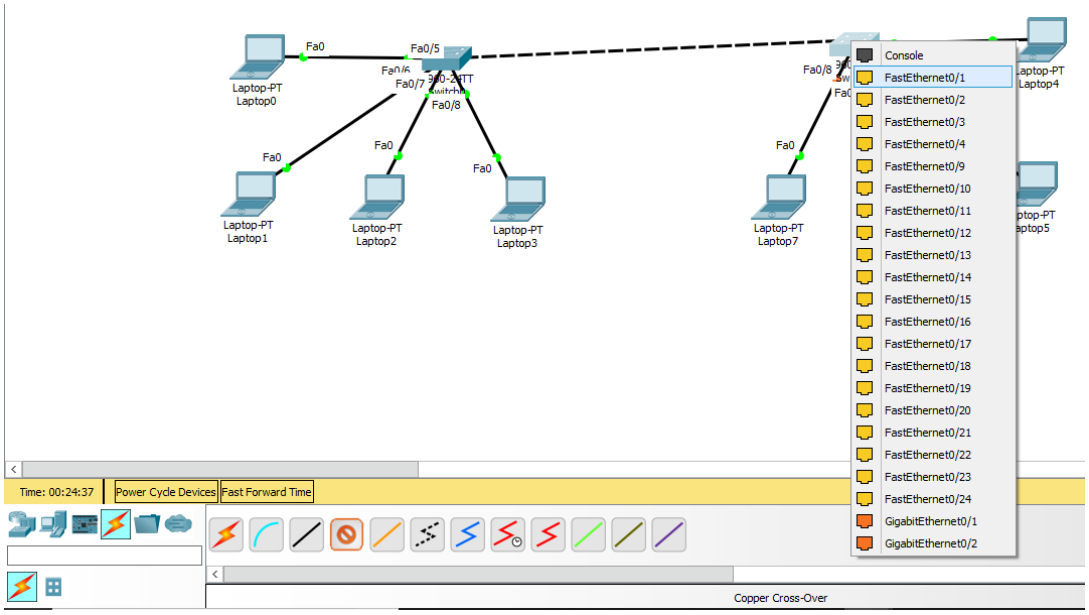


Fig. 3.6enlace troncal.

Procedemos a configurar nuestras PC asignándoles una dirección IP, su máscara de subred y su Gateway, en el área de CFE Transmisión que se realizó el proyecto, se utiliza como Gateway la última IP utilizable de la subred como se muestra en la figura 3.7.

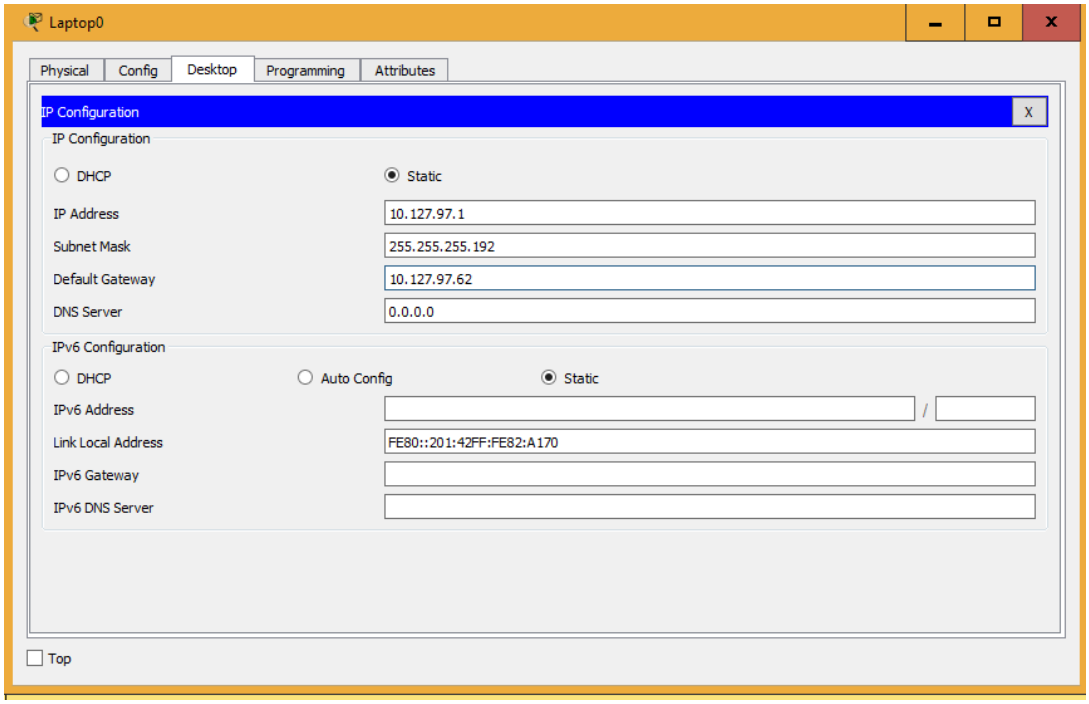


Fig. 3.7 configuración IP, mascara de subred y Gateway de Hosts.

Entraremos a los switch capa 2 para configurar cada uno de sus puertos por Hosts, y sus puertos troncales además de la creación de las VLANs.

- Programación switch 2A

```
switch_2A>enable
switch_2A#config ter
switch_2A(config)#vlan 10
switch_2A(config-vlan)#name SCADA
switch_2A(config-vlan)#vlan 20
switch_2A(config-vlan)#name monitoreo
switch_2A(config-vlan)#vlan 30
switch_2A(config-vlan)#name vozyvideo
switch_2A(config-vlan)#vlan 40
switch_2A(config-vlan)#name intranet
switch_2A(config-vlan)#inter fa 0/6
```

```
switch_2A(config-if)#switchport mode access
switch_2A(config-if)#switchport access vlan 10
switch_2A(config-if)#inter fa 0/7
switch_2A(config-if)#switchport mode access
switch_2A(config-if)#switchport access vlan 20
switch_2A(config-if)#inter fa 0/8
switch_2A(config-if)#switchport mode access
switch_2A(config-if)#switchport access vlan 30
switch_2A(config-if)#inter fa 0/9
switch_2A(config-if)#switchport mode access
switch_2A(config-if)#switchport access vlan 40
switch_2A(config-if)#inter fa 0/1
switch_2A(config-if)#switchport mode trunk
switch_2A(config-if)#speed 100
switch_2A(config-if)#duplex full
```

- programación switch 2B

```
Switch>enable
Switch#config ter
Switch(config)#vlan 10
Switch(config-vlan)#name SCADA
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name monitoreo
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name vozyvideo
Switch(config-vlan)#vlan 40
Switch(config-vlan)#name intranet
Switch(config-vlan)#int fa 0/6
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int fa 0/7
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#int fa 0/8
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#int fa 0/9
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 40
```

```
Switch(config-if)#int fa 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#speed 100
Switch(config-if)#duplex full
```

Como se observa en la programación para configurar los switch capa 2 primero accedemos al switch 2A, luego a configuración y procedemos a crear las VLAN asignándoles un nombre, en esta ocasión no se les puso alguna descripción, siguiendo esto se accedió a las interfaces conectadas a los hosts y se les configuro como interfaces de acceso y se les asigno a una VLAN, por último se configuro la interface troncal en modo troncal y se le asignó una velocidad de 100Mbps y una conexión full dúplex, como se observa en las programaciones es exactamente la misma configuración para ambos switch.

Finalmente, para saber si nuestras VLANs están trabajando correctamente le mandamos un ping entrando a una computadora a los comandos y mandamos ping + IP del dispositivo al que queremos llegar. Como se observa en la figura 3.8 si tenemos respuesta del host al que le hemos mandado ping y este se encuentra dentro de la VLAN quiere decir que nuestra configuración es correcta, si el host no responde el ping que le hemos enviado quiere decir que algo está mal o bien sino responde es porque pertenece a otra VLAN.

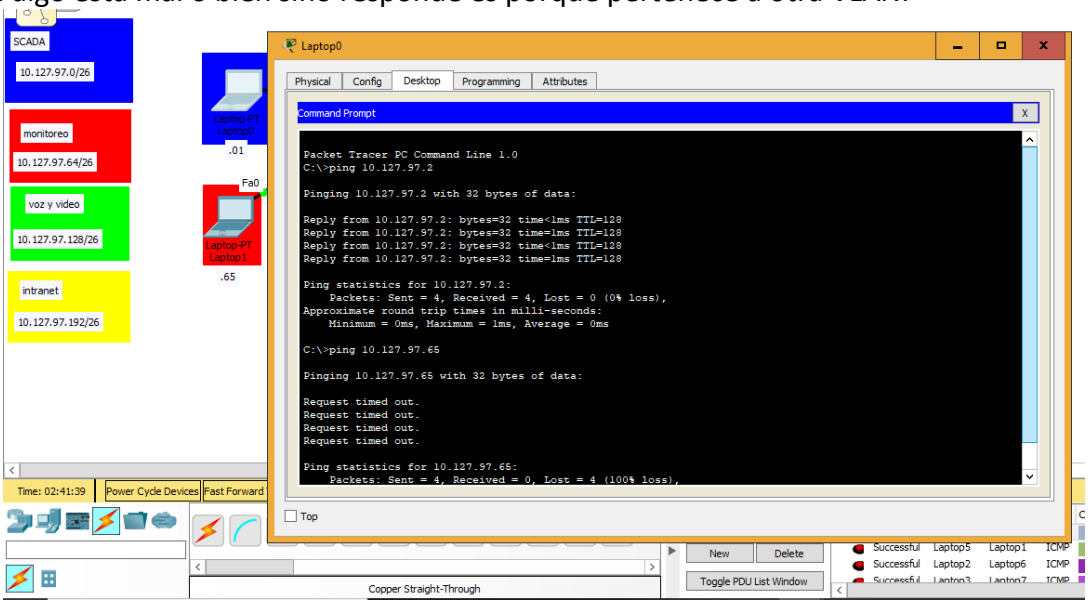


Fig. 3.8 enviar ping.

3.6 Programación en capa 3 con router

Como sabemos hasta ahorita los switch capa 2 nos permiten crear VLANs y comunicar dispositivos. Pero al crear estas VLANs los dispositivos solo pueden comunicarse son los que se encuentran dentro de su misma VLANs, ¿Qué pasaría si estos dispositivos tienen la necesidad de comunicarse entre diferentes VLANs? Entonces ahí entraría en función lo routers o switch capa 3, para que las diferentes VLANs puedan intercambiar datos entre sí.

Nos basaremos en el laboratorio que anteriormente fue creado donde ya teníamos nuestros hosts configurados, nuestros switch capa 2 configurados y nuestras VLANs creadas para no repetir este procedimiento.

Procedemos a elegir nuestro router la barra de herramientas de la parte inferior, lo arrastramos hasta nuestra área de trabajo y conectamos mediante un cable ethernet directo de la interface gigabit Ethernet 0/1 del switch a la interface gigabit Ethernet 0/0 del router como se muestra en la figura 3.9.

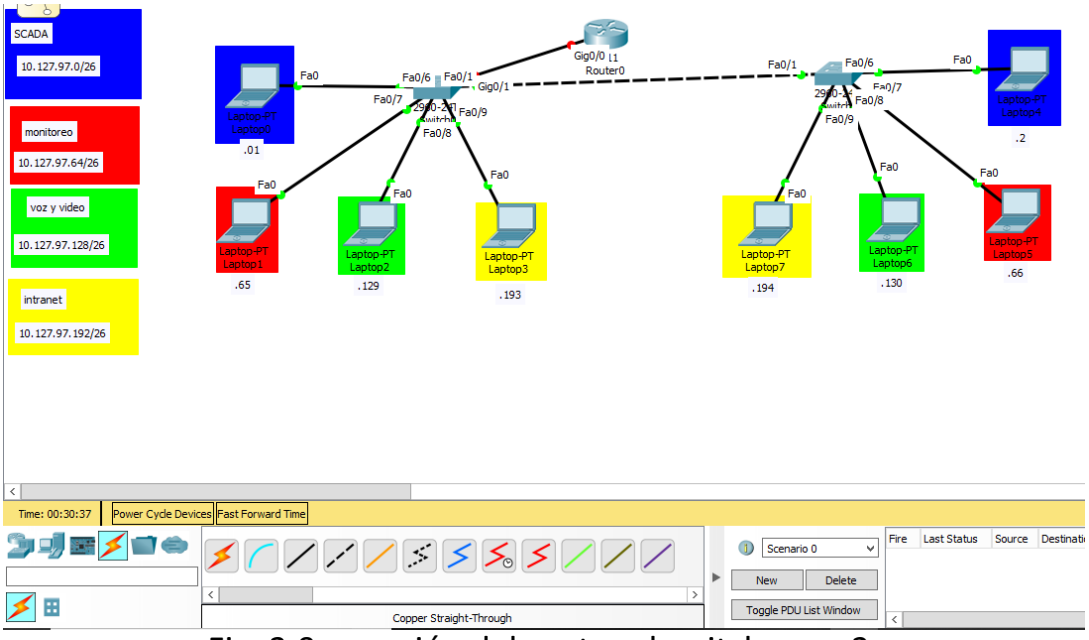


Fig. 3.9 conexión del router al switch capa 2.

Procedemos a configurar la interface gigabit Ethernet en modo troncal del switch capa 2.

- Programación switch 2A

```
switch_2A>enable
switch_2A#config ter
Enter configuration commands, one per line. End with CNTL/Z.
switch_2A(config)#int gig 0/1
switch_2A(config-if)#switchport mode trunk
switch_2A(config-if)#speed 1000
switch_2A(config-if)#duplex full
```

Como se observa en la programación en el switch capa 2 solo se hace una configuración a la interface gigabit ethernet 0/1 en modo troncal, se configura la velocidad en este caso he elegido mil ya que es una interface gigabit.

- Programación Router A

```
Router>enable
Router#config ter
Router(config)#int gig 0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 10.127.97.62 255.255.255.192
Router(config-subif)#int gig 0/0.20
Router(config-subif)#encapsulation dot1q 20
Router(config-subif)#ip address 10.127.97.126 255.255.255.192
Router(config-subif)#int gig 0/0.30
Router(config-subif)#encapsulation dot1q 30
Router(config-subif)#ip address 10.127.97.190 255.255.255.192
Router(config-subif)#int gig 0/0.40
Router(config-subif)#encapsulation dot1q 40
Router(config-subif)#ip address 10.127.97.254 255.255.255.192
Router(config-subif)#int gig 0/0
Router(config-if)#speed 1000
Router(config-if)#duplex full
Router(config-if)#no shutdown
```

Para programar las VLANs en los routers se denominan subinterfaces. Para crear las subinterfaces necesitas poner un punto y el número de VLAN a lado de la interface como se observa en la programación, posteriormente se menciona el tipo de encapsulamiento que usara el router en este caso es un encapsulamiento dot1q seguido del número de la VLAN, por último, para la creación de la subinterfaz se pone la dirección IP del Gateway y la máscara de subred.

Por último, se accede a la interfaz troncal que en este caso es la interfaz gigabit ethernet 0/0 donde se configura la velocidad en 1000 Mbps, una comunicación bidireccional y por último le damos un no shutdown para levantar el puerto.

Para comprobar que nuestro router y programación está trabajando correctamente debemos de mandar un ping a los dispositivos de las otras VLANs si tenemos respuesta de estos dispositivos es que nuestro router está trabajando bien como se muestra en la figura 3.10.

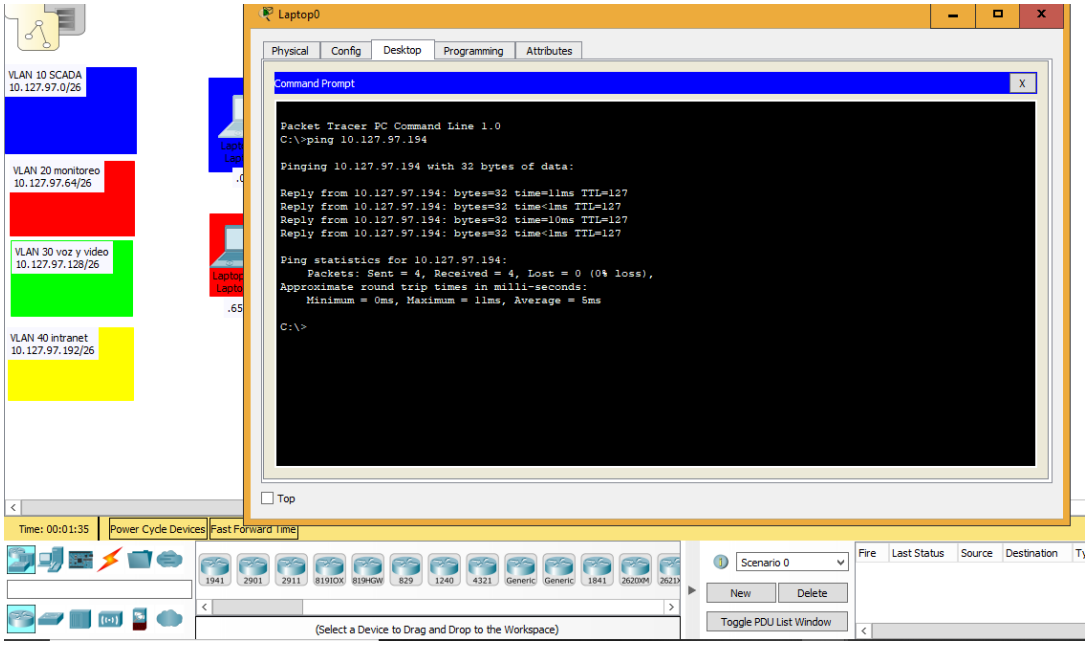


Fig. 3.10 ping entre VLANs.

3.7 Programación en capa 3 con switch capa 3

En este caso igual procederemos a programar en capa 3 pero ahora será en un switch para poder conectar VLANs entre sí, seguiremos trabajando con el mismo laboratorio, pero ahora procederemos a quitar el router y colocar el switch capa 3 usando la interfaz fastethernet del switch como lo indica la figura 3.11.

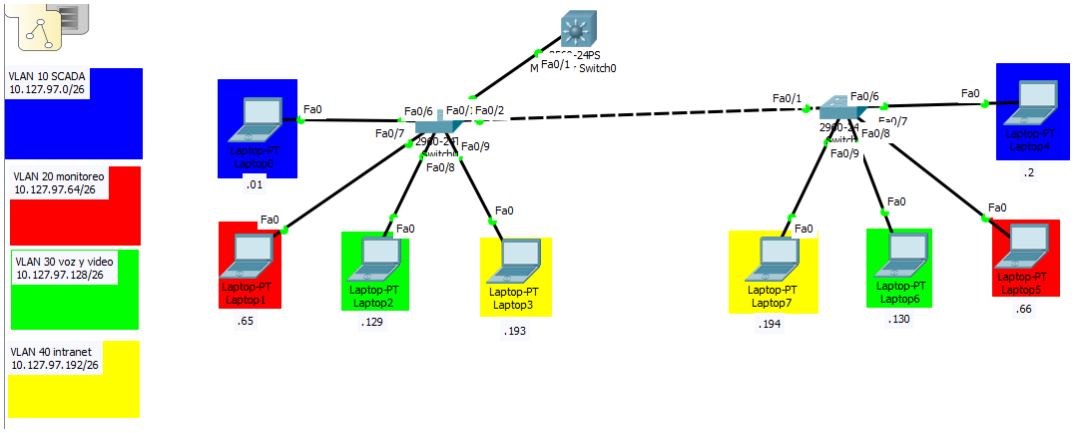


Fig. 3.11 conexión del switch capa 3.

Procedemos a configurar la interfaz fast ethernet del switch capa 2 en modo troncal con una velocidad de 100 Mbps en full dúplex.

Si comparamos la figura 3.12 con la figura 3.11 observamos que en la 3.12 el enlace ha pasado de color verde a color rojo lo que nos indica que este enlace se ha caído debido a que ambos puertos no corren a la misma velocidad, ni comparte información bidireccional, por lo que procederemos a configurar el puerto fastethernet del switch capa 3.

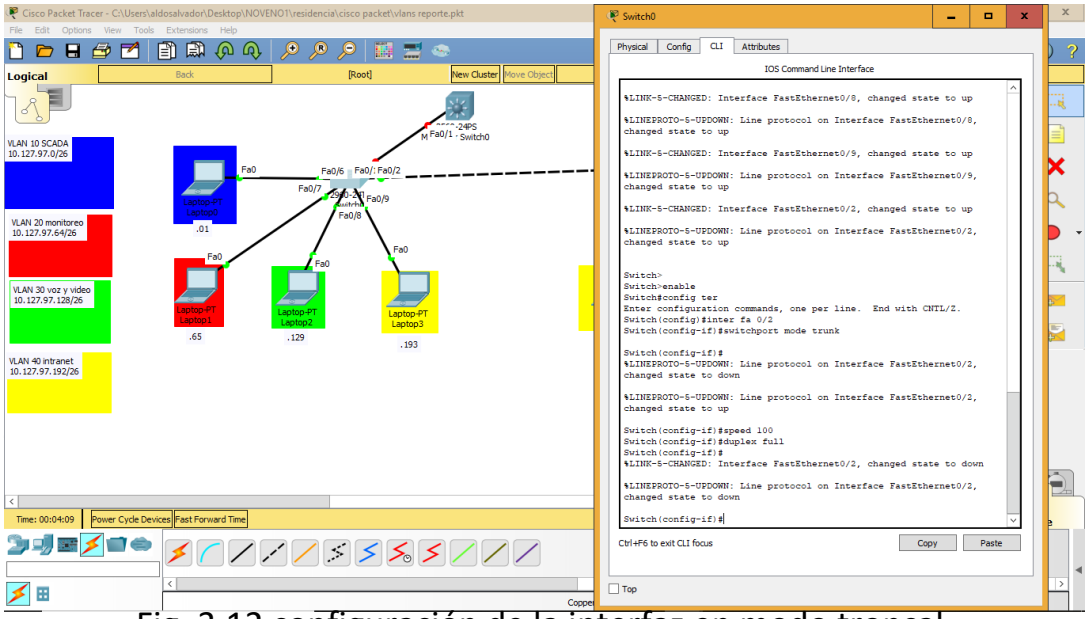


Fig. 3.12 configuración de la interfaz en modo troncal.

Switch>enable
Switch#config ter
Switch(config)#ip routing
Switch(config)#vlan 10
Switch(config-vlan)#name SCADA
Switch(config-vlan)#vlan 20
Switch(config-vlan)#name monitoreo
Switch(config-vlan)#vlan 30
Switch(config-vlan)#name vozyvideo
Switch(config-vlan)#vlan 40
Switch(config-vlan)#name intranet
Switch(config-vlan)#int vlan 10
Switch(config-if)#ip address 10.127.97.62 255.255.255.192
Switch(config-if)#no shutdown
Switch(config-if)#int vlan 20
Switch(config-if)#ip address 10.127.97.126 255.255.255.192
Switch(config-if)#no shutdown
Switch(config-if)#int vlan 30
Switch(config-if)#ip address 10.127.97.190 255.255.255.192
Switch(config-if)#no shutdown
Switch(config-if)#int vlan 40
Switch(config-if)#ip address 10.127.97.254 255.255.255.192
Switch(config-if)#no shutdown
Switch(config-if)#int fa 0/1
Switch(config-if)#switchport trunk encapsulation dot1q
Switch(config-if)#speed 100

Switch(config-if)#duplex full

Lo primero que se realiza en el switch es escribir el comando ip routing para que reconozca nuestro switch como funcionamiento de un router, dado que estos switch pueden realizar funciones de capa 2 o capa 3. Después de haber configurado esto procedemos a crear las VLANs y asignarles nombre, luego accedemos a cada una de las VLANs y le colocamos la dirección de Gateway que le hemos colocado a los dispositivos pertenecientes a su respectiva VLAN. Por consiguiente, entramos a la interfaz y la declaramos como un puerto troncal con un encapsulamiento dot1q, luego elegimos la velocidad de 100 Mbps y una comunicación bidireccional. Ahora podemos observar en la figura 3.13 que el enlace se encuentra en color verde lo que nos indica que el enlace esta levantado.

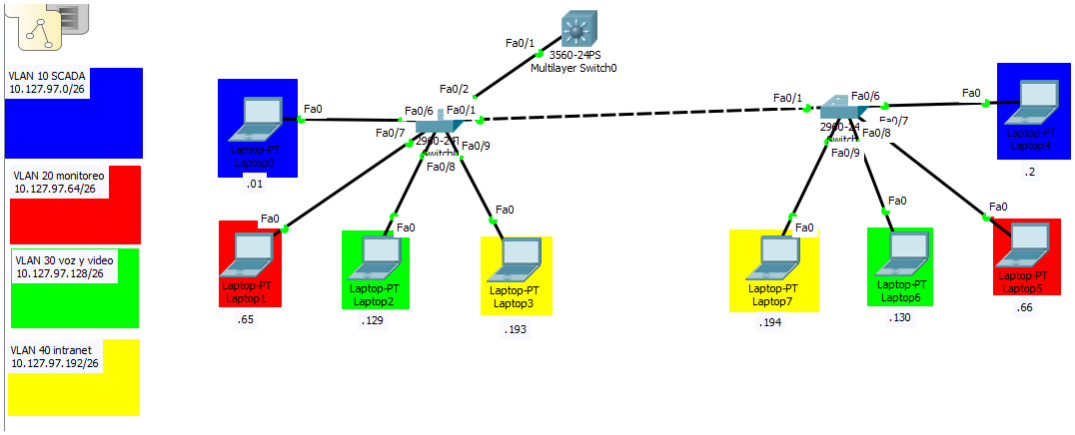


Fig. 3.13 enlace levantado.

Si queremos comprobar que nuestra programación es correcta podemos mandar ping a diferentes dispositivos perteneciente a diferente VLAN del dispositivo de origen como se mencionó anteriormente.

3.8 Enrutamiento por rutas estáticas

Con lo anterior antes aprendido se realizó un laboratorio más complejo que a grandes rasgos simulan tres zonas de lo que es CFE Transmisión sureste la gerencia, Tuxtla y malpaso como se muestra en la figura 3.14.

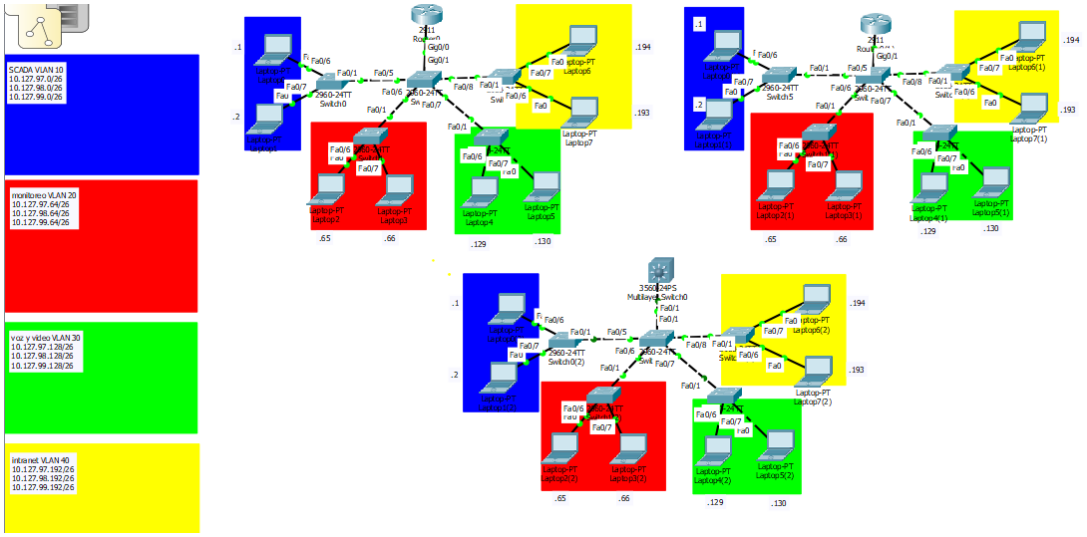


Fig. 3.14 representación de tres zonas de CFE Transmisión.

Bien para entender el funcionamiento del enrutamiento sea realizado el laboratorio de la figura 3.14 el cual ya mencionamos, se procederá a conectar estas tres zonas haciendo un enlace WAN entre ellas como muestra la figura 3.15.

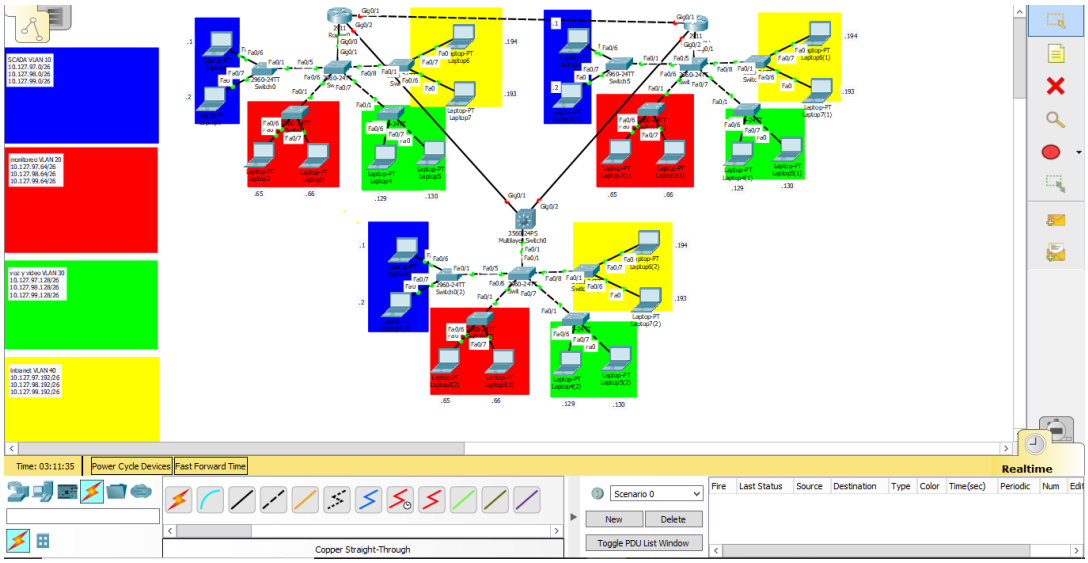


Fig. 3.15 enlaces WAN.

Podemos observar en la figura 3.15 que hemos establecido los enlaces WAN, pero estos se encuentran caídos ya que los puntos se encuentran en color rojo, al igual que si intentamos comunicarnos de una zona a otra o de un Host a otro que se encuentre en otra zona, esto lo verificamos haciendo pin entre ellos.

Así que procederemos a establecer a programas las interfaces de estos router para establecer la conexión y posteriormente programaremos el enrutamiento estático para que pueda haber comunicación entre host de distintas zonas.

El enrutamiento estático como ya se mencionó anteriormente en el tema de "enrutamiento estático" el operador de la red le indica a cada ruteador por donde este debe de mandar los datos para que llegue de un punto A a un punto B. para ello también emplearemos una dirección IP por cada interfaz que forme un enlace WAN.

- Programación en Router A

```
ROUTER_A>enable
ROUTER_A#config ter
ROUTER_A(config)#int gig 0/1
ROUTER_A(config-if)#ip address 10.127.64.1 255.255.255.252
ROUTER_A(config-if)#speed 1000
ROUTER_A(config-if)#duplex full
ROUTER_A(config-if)#int gig 0/2
ROUTER_A(config-if)#ip address 10.127.64.5 255.255.255.252
ROUTER_A(config-if)#speed 1000
ROUTER_A(config-if)#duplex half
ROUTER_A(config-if)#no shutdown
ROUTER_A(config-if)#int gig 0/1
ROUTER_A(config-if)#no shutdown
ROUTER_A(config-if)#exit
ROUTER_A(config)#ip route 10.127.98.0 255.255.255.252 10.127.64.6
```

```
ROUTER_A(config)#ip route 10.127.98.64 255.255.255.252 10.127.64.6
ROUTER_A(config)#ip route 10.127.98.128 255.255.255.252 10.127.64.6
ROUTER_A(config)#ip route 10.127.98.192 255.255.255.252 10.127.64.6
ROUTER_A(config)#ip route 10.127.99.0 255.255.255.252 10.127.64.2
ROUTER_A(config)#ip route 10.127.99.64 255.255.255.252 10.127.64.2
ROUTER_A(config)#ip route 10.127.99.128 255.255.255.252 10.127.64.2
ROUTER_A(config)#ip route 10.127.99.192 255.255.255.252 10.127.64.2
ROUTER_A(config)#exit
ROUTER_A# wr
Building configuration...
[OK]
```

- Programación en Router B

```
ROUTER_B>enable
ROUTER_B#config ter
ROUTER_B(config)#int gig 0/1
ROUTER_B(config-if)#ip addres 10.127.64.2 255.255.255.252
ROUTER_B(config-if)#speed 1000
ROUTER_B(config-if)#duplex full
ROUTER_B(config-if)#int gig 0/2
ROUTER_B(config-if)#ip addres 10.127.64.9 255.255.255.252
ROUTER_B(config-if)#speed 1000
ROUTER_B(config-if)#duplex half
ROUTER_B(config-if)#no shutdown
ROUTER_B(config-if)#int gig 0/1
ROUTER_B(config-if)#no shutdown
ROUTER_B(config-if)#exit
ROUTER_B(config)#ip route 10.127.97.0 255.255.255.192 10.127.64.1
ROUTER_B(config)#ip route 10.127.97.64 255.255.255.192 10.127.64.1
ROUTER_B(config)#ip route 10.127.97.128 255.255.255.192 10.127.64.1
ROUTER_B(config)#ip route 10.127.97.192 255.255.255.192 10.127.64.1
ROUTER_B(config)#ip route 10.127.98.0 255.255.255.192 10.127.64.10
ROUTER_B(config)#ip route 10.127.98.64 255.255.255.192 10.127.64.10
ROUTER_B(config)#ip route 10.127.98.128 255.255.255.192 10.127.64.10
ROUTER_B(config)#ip route 10.127.98.192 255.255.255.192 10.127.64.10
ROUTER_B(config)#exit
ROUTER_B# wr
Building configuration...
[OK]
```

- Programación en Switch A

```
SWITCH_A>enable
SWITCH_A#config ter
SWITCH_A(config)#int gig 0/1
SWITCH_A(config-if)#no switchport
SWITCH_A(config-if)#ip address 10.127.64.6 255.255.255.252
SWITCH_A(config-if)#speed 1000
SWITCH_A(config-if)#no shutdown
SWITCH_A(config-if)#exit
SWITCH_A(config)#int gig 0/2
SWITCH_A(config-if)#no switchport
SWITCH_A(config-if)#ip address 10.127.64.10 255.255.255.252
SWITCH_A(config-if)#speed 1000
SWITCH_A(config-if)#no shutdown
SWITCH_A(config-if)#exit
SWITCH_A(config)#ip route 10.127.97.0 255.255.255.192 10.127.64.5
SWITCH_A(config)#ip route 10.127.97.64 255.255.255.192 10.127.64.5
SWITCH_A(config)#ip route 10.127.97.128 255.255.255.192 10.127.64.5
SWITCH_A(config)#ip route 10.127.97.192 255.255.255.192 10.127.64.5
SWITCH_A(config)#ip route 10.127.99.0 255.255.255.192 10.127.64.9
SWITCH_A(config)#ip route 10.127.99.64 255.255.255.192 10.127.64.9
SWITCH_A(config)#ip route 10.127.99.128 255.255.255.192 10.127.64.9
SWITCH_A(config)#ip route 10.127.99.192 255.255.255.192 10.127.64.9
SWITCH_A(config)#exit
SWITCH_A#wr
Building configuration...
[OK]
```

Como se puede analizar en los códigos la forma de enrutar estáticamente es entrar a la interfaz de cada enlace asignarle una dirección IP, una velocidad y designar si es dúplex full o half en el caso de los enlaces con el Switch he puesto dúplex half ya que este Switch sus interfaces solo soportan dúplex half o bien se podría poner un dúplex auto para que los router negocien el dúplex. Por consiguiente, se designa cual será la ruta a tomar para mandar datos, esto se hace mediante el comando “ip route” seguido de la dirección a la red que se quiere llegar con su máscara de subred y la dirección IP con la que se llegara a esta

subred. Así es como se programa subred por subred hasta haber cubierto todas las subredes de la red y esto se repite en cada ruteador que se encuentra la red.

Se puede visualizar que el enrutamiento estático está trabajando bien mandando un ping entre diferentes hosts de diferentes zonas como se visualiza en la barra de herramientas inferior en la figura 3.16, de igual manera puedes ver la tabla de enrutamiento de cada router con el comando “show ip route”.

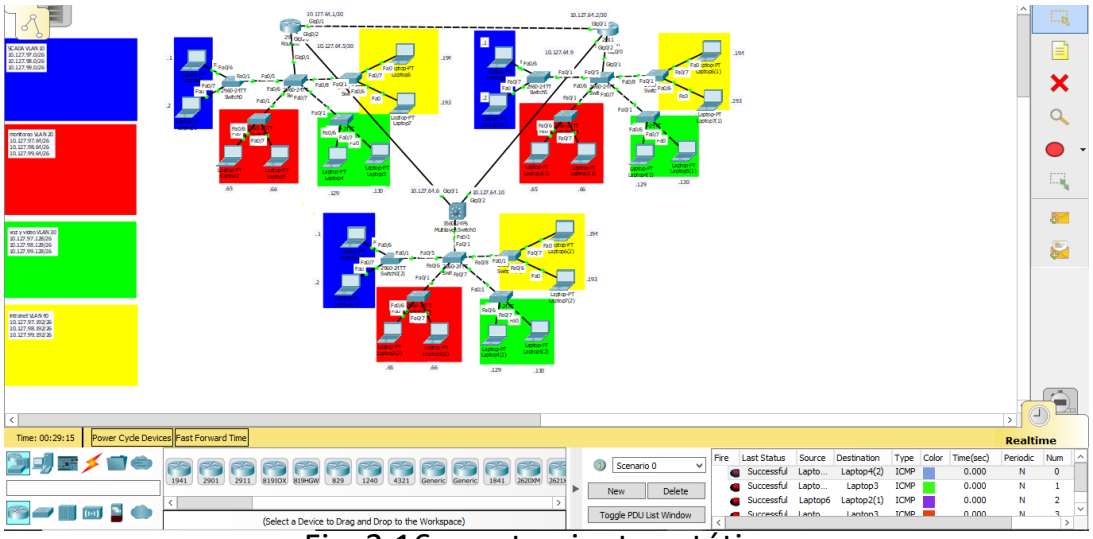


Fig. 3.16 enrutamiento estático.

El defecto de este tipo es que si un enlace se cae como el router solo conoce esa forma de llegar a la subred no buscara nuevos caminos para llegar a ella a pesar de que lo existan.

3.9 Enrutamiento dinámico por el protocolo OSPF

Para el enrutamiento mediante OSPF regresaremos al mismo escenario como estábamos en figura 3.14 empezando lo que es el enrutamiento desde cero. Este es el protocolo que

más nos interesa porque es el protocolo en el cual se basa la red de datos la cual es de lo que se desarrolló este proyecto.

- Programación en Router A

```
ROUTER_A>enable
ROUTER_A#config ter
ROUTER_A(config)#int gig 0/1
ROUTER_A(config-if)#ip address 10.127.64.1 255.255.255.252
ROUTER_A(config-if)#speed 1000
ROUTER_A(config-if)#duplex full
ROUTER_A(config-if)#no shutdown
ROUTER_A(config-if)#int gig 0/2
ROUTER_A(config-if)#ip address 10.127.64.5 255.255.255.252
ROUTER_A(config-if)#speed 1000
ROUTER_A(config-if)#duplex half
ROUTER_A(config-if)#no shutdown
ROUTER_A(config-if)#exit
ROUTER_A(config)#router ospf 65001
ROUTER_A(config-router)#router-id 1.1.1.1
ROUTER_A(config-router)#network 10.127.0.0 0.0.255.255 area 8
ROUTER_A(config-router)#exit
ROUTER_A(config)#exit
ROUTER_A#wr
Building configuration...
[OK]
```

- Programación Router B

```
ROUTER_B>enable
ROUTER_B#config ter
ROUTER_B(config)#inter gig 0/1
ROUTER_B(config-if)#ip address 10.127.64.2 255.255.255.252
ROUTER_B(config-if)#speed 1000
ROUTER_B(config-if)#duplex full
ROUTER_B(config-if)#no shutdown
```

```
ROUTER_B(config-if)#inter gig 0/2
ROUTER_B(config-if)#ip address 10.127.64.9 255.255.255.252
ROUTER_B(config-if)#speed 1000
ROUTER_B(config-if)#duplex half
ROUTER_B(config-if)#no shutdown
ROUTER_B(config-if)#exit
ROUTER_B(config)#router ospf 65001
ROUTER_B(config-router)#router-id 2.2.2.2
ROUTER_B(config-router)#network 10.127.0.0 0.0.255.255 area 8
ROUTER_B(config-router)#exit
ROUTER_B(config)#exit
ROUTER_B#wr
Building configuration...
[OK]
```

- Programación Switch A

```
SWITCH_A>enable
SWITCH_A#config ter
SWITCH_A(config)#int gig 0/1
SWITCH_A(config-if)#no switchport
SWITCH_A(config-if)#ip address 10.127.64.6 255.255.255.252
SWITCH_A(config-if)#speed 1000
SWITCH_A(config-if)#no shutdown
SWITCH_A(config-if)#int gig 0/2
SWITCH_A(config-if)#no switchport
SWITCH_A(config-if)#ip address 10.127.64.10 255.255.255.252
SWITCH_A(config-if)#speed 1000
SWITCH_A(config-if)#no shutdown
SWITCH_A(config-if)#exit
SWITCH_A(config)#route ospf 65001
SWITCH_A(config-router)#router-id 3.3.3.3
SWITCH_A(config-router)#network 10.127.0.0 0.0.255.255 area 8
SWITCH_A(config-router)#exit
SWITCH_A(config)#exit
SWITCH_A# wr
Building configuration...
[OK]
```

Para programar enrutamiento dinámico OSPF lo primero que debemos de hacer al igual que el enrutamiento estático es asignarle una subred a cada enlace WAN y una dirección IP a cada interfaz de los routers, después de haber hecho esto y de darle sus especificaciones como la velocidad y el direccionamiento, proseguimos a crear el enrutamiento OSPF primero con el número determinado, se le asigna un id y por otro declaramos la red que queremos enrutar con el protocolo como en este caso es la red 10.127.0.0 seguido de su wildcard

El wildcard no es más que todo lo contrario de la máscara de subred, para saber cuál es el wildcard convierte una máscara de subred en binario y convierte todos los bits que estén en “1” a “0” y los que estén en “0” a “1” y el resultado en decimal será el wildcard. Con ello ya tendremos funcionando nuestro enrutamiento dinámico con OSPF.

Para saber si nuestra programación es correcta podemos mandar ping entre diferentes Host de diferentes zonas como lo indica la figura 3.17, o bien podemos acceder al router, colocar en modo privilegiado el comando “show ip route” el cual nos mostrara a que redes puede llegar el router y por medio de que enrutamiento.

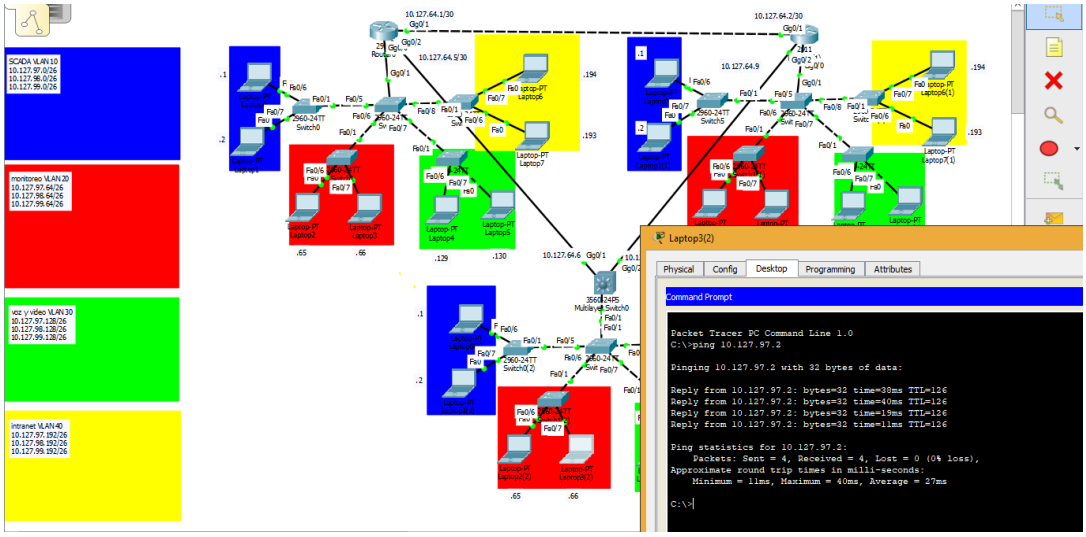


Fig. 3.17 enrutamiento mediante OSPF.

3.10 Enrutamiento dinámico por el protocolo EIGRP

Continuamos con el mismo ejemplo de la figura 3.14 volvemos a donde teníamos tres zonas con 4 VLANs y procederemos a hacer el enrutamiento dinámico, pero ahora utilizando el protocolo EIGRP de cisco.

Para el protocolo EIGRP la programación es similar a la del protocolo OSPF como se observa a continuación.

- Programación Router A

```
ROUTER_A>enable
ROUTER_A#config ter
ROUTER_A(config)#int gig 0/1
ROUTER_A(config-if)#ip address 10.127.64.1 255.255.255.252
ROUTER_A(config-if)#speed 100
ROUTER_A(config-if)#duplex full
ROUTER_A(config-if)#no shutdown
ROUTER_A(config-if)#int gig 0/2
ROUTER_A(config-if)#ip address 10.127.64.5 255.255.255.252
ROUTER_A(config-if)#speed 100
ROUTER_A(config-if)#duplex half
ROUTER_A(config-if)#no shutdown
ROUTER_A(config-if)#exit
ROUTER_A(config)#router eigrp 65001
ROUTER_A(config-router)#network 10.127.0.0
```

- Programación Router B

```
ROUTER_A>enable
ROUTER_A#config ter
ROUTER_A(config)#int gig 0/1
ROUTER_A(config-if)#ip address 10.127.64.1 255.255.255.252
ROUTER_A(config-if)#speed 100
```

```
ROUTER_A(config-if)#duplex full
ROUTER_A(config-if)#no shutdown
ROUTER_A(config-if)#int gig 0/2
ROUTER_A(config-if)#ip address 10.127.64.5 255.255.255.252
ROUTER_A(config-if)#speed 100
ROUTER_A(config-if)#duplex half
ROUTER_A(config-if)#no shutdown
ROUTER_A(config-if)#exit
ROUTER_A(config)#router eigrp 65001
ROUTER_A(config-router)#network 10.127.0.0
```

- Programación en Switch A

```
SWITCH_A>enable
SWITCH_A#config ter
SWITCH_A(config)#int gig 0/1
SWITCH_A(config-if)#no switchport
SWITCH_A(config-if)#ip address 10.127.64.6 255.255.255.252
SWITCH_A(config-if)#speed 100
SWITCH_A(config-if)#int gig 0/2
SWITCH_A(config-if)#no switchport
SWITCH_A(config-if)#ip address 10.127.64.10 255.255.255.252
SWITCH_A(config-if)#speed 100
SWITCH_A(config-if)#exit
SWITCH_A(config)#router eigrp 65001
SWITCH_A(config-router)#network 10.127.0.0
```

Observamos en la programación de los router y el switch se asemeja mucho a la programación en OSPF, no obstante, en el caso de EIGRP no es utilizado el wildcard, el área y el comando router-id, ya que no maneja estos datos y no hace la división de la red por áreas.

Para saber que nuestra red está trabajando correctamente podemos hacerle ping a cada uno de los diferentes hosts que hay en la red, o de igual manera ver la tabla de enrutamiento de los routers con el comando “show ip route” como se muestra a continuación en la figura 3.18.

```
ROUTER_A#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 21 subnets, 3 masks
C       10.127.64.0/30 is directly connected, GigabitEthernet0/1
L       10.127.64.1/32 is directly connected, GigabitEthernet0/1
C       10.127.64.4/30 is directly connected, GigabitEthernet0/2
L       10.127.64.5/32 is directly connected, GigabitEthernet0/2
D       10.127.64.8/30 [90/7680] via 10.127.64.2, 01:06:48, GigabitEthernet0/1
                       [90/7680] via 10.127.64.6, 01:01:01, GigabitEthernet0/2
C       10.127.97.0/26 is directly connected, GigabitEthernet0/0.10
L       10.127.97.62/32 is directly connected, GigabitEthernet0/0.10
C       10.127.97.64/26 is directly connected, GigabitEthernet0/0.20
L       10.127.97.126/32 is directly connected, GigabitEthernet0/0.20
C       10.127.97.128/26 is directly connected, GigabitEthernet0/0.30
L       10.127.97.190/32 is directly connected, GigabitEthernet0/0.30
C       10.127.97.192/26 is directly connected, GigabitEthernet0/0.40
L       10.127.97.254/32 is directly connected, GigabitEthernet0/0.40
D       10.127.98.0/26 [90/25628160] via 10.127.64.6, 01:01:01, GigabitEthernet0/2
D       10.127.98.64/26 [90/25628160] via 10.127.64.6, 01:01:01, GigabitEthernet0/2
D       10.127.98.128/26 [90/25628160] via 10.127.64.6, 01:01:01, GigabitEthernet0/2
D       10.127.98.192/26 [90/25628160] via 10.127.64.6, 01:01:01, GigabitEthernet0/2
D       10.127.99.0/26 [90/30720] via 10.127.64.2, 01:07:16, GigabitEthernet0/1
D       10.127.99.64/26 [90/30720] via 10.127.64.2, 01:07:16, GigabitEthernet0/1
D       10.127.99.128/26 [90/30720] via 10.127.64.2, 01:07:16, GigabitEthernet0/1
D       10.127.99.192/26 [90/30720] via 10.127.64.2, 01:07:16, GigabitEthernet0/1
```

Fig. 3.18 tabla de enrutamiento.

En la figura 3.18 se puede apreciar la tabla de enrutamiento del Router A así como observamos a que dispositivos está conectado, a través de que interfaz lo está y que tipo de protocolo usa para comunicarse con ellos. Los que inician con una “L” nos indica que están directamente conectados al router y los que inician con “D” nos indica que se conecta con ellos a través del protocolo EIGRP.

Conclusiones

Para concluir empezaremos hablando del proyecto de la Red Eléctrica Inteligente (REI). La REI es un proyecto que se ve obligado a realizar por las empresas generadoras de electricidad para modernización de la industria eléctrica dado a los avances de tecnología que contamos hoy en día.

La REI es un proyecto enorme que pretende unificar todo el servicio de luz eléctrica, desde los medidores, los paneles solares, la carga en los vehículos eléctricos actuales y de futuro hasta la generación de energía, es decir, pretende abarcar desde su generación hasta el usuario final.

El propósito de la REI es demasiado extenso por ello es un proyecto grande, hablamos de unos 10 a 30 años, tiempo que depende mucho de la empresa y el país en el que se realice. En países de primer mundo algunos ya se encuentran implementándola desde aproximadamente unos 10 años, sin embargo, ninguno hasta hoy en día cuenta con el proyecto ya terminado.

Como bien sabemos que la REI es un proyecto grande de este se derivan cientos de proyectos, uno de ellos es la Implementación y Puesta en Servicio de la Red Operativa de Datos.

Para que la REI funcione adecuadamente se necesita un medio para la transmisión de datos generada es ahí donde hablamos de la red de datos. El proyecto se realizó en la Gerencia

Regional de Transmisión Sureste ubicada en Tuxtla Gutiérrez, Chiapas. Por lo que el trabajo se realizó en las zonas pertenecientes a la gerencia.
La Red Operativa de Datos de la Gerencia Regional de Transmisión Sureste abarca cinco zonas de las cuales se realizó la implementación y puesta en servicio de la gerencia con la zona Tuxtla y la zona Malpaso.

Para realizar el proyecto primero se tuvieron que realizar modificaciones en el Hotel Telecom ubicado en la gerencia, para realizar conexiones a través de fibra óptica, posteriormente se llevó a cabo la programación de los equipos switches y routers para la puesta en servicio de la Red Operativa de Datos.

Se ejecutó en los switches y routers la programación de los enlaces entre los diferentes routers de las zonas para levantar los enlaces, posteriormente se accedió a cada equipo para configurarle las interfaces con la información dada por las diferentes zonas y la tabla de direcciones otorgada por la propia CFE Transmisión. Configurando las interfaces procedimos a programar los switches para la creación de VLANs dentro de las zonas, una vez programado los switches continuamos con los router a programar para el direccionamiento de datos entres las VLANs y las Zonas.

Para que las zonas se comuniquen CFE emplea el protocolo de enrutamiento OSPF, por lo que se procedió a programar en cada uno de los routers el protocolo OSPF, para finalizar con el proyecto se observó que se tuviera alcance de los dispositivos mediante ping.

Es todo lo que se realizó a la Red Operativa de Datos, aunque aún falta mucho trabajo para que funcione en todo el país y por toda la Red Eléctrica de CFE, se logró implementar y poner en servicio en estas zonas concluyendo el proyecto establecido.

Observaciones y sugerencias

La Red Eléctrica Inteligente (REI) en México a cargo de la Comisión Federal de Electricidad, viene a revolucionar la Industria Eléctrica Mexicana. La REI es uno de los mejores proyectos que se a llevado acabo en años, ya que como su nombre lo dice pretende que toda la Red Eléctrica de México sea inteligente. La Red se logrará que sea inteligente mediante la implementación de sensores y actuadores, con los cuales podrá tomar decisiones correctas sin necesidad de una persona tanto para el usuario como para la infraestructura y las empresas.

La REI es un proyecto muy complejo por lo que ahorita no hay que agregar nada, por lo que todavía está en desarrollo, además de que CFE emplea equipos de la más reciente tecnología y con la mayor capacidad de velocidad y procesamiento. Por ello ahorita es un proyecto muy completo, probablemente con la introducción de nuevas tecnologías y el crecimiento de la Red Eléctrica, necesite de una capacidad de procesamiento y velocidad mayor.

La REI en CFE es de mucho aprendizaje, dado que es un proyecto que abarca toda la Red Eléctrica, por lo que el aprendizaje obtenido es sobre diversas áreas.

Referencias

Boyzo Boyzo, R. E., Rojas Vassallo, O. G., Rosales Tovar, J. V., Ortega Rojas, M. A., Sánchez Díaz, F., & Pineda Selvas, M. A. (2016). *POLITICAS Y LINEAMIENTOS PARA LA RED ELÉCTRICA INTELIGENTE.*

CFE. (s.f.). *CFE*. Obtenido de https://www.cfe.mx/acercacfe/Quienes%20somos/Pages/historia.aspx

CISCO. (09 de 2011). *CONSULTEC-BETO SAMANIEGO.* Recuperado el 12 de 11 de 2018, de CONSULTEC-BETO SAMANIEGO: https://betosamaniego.files.wordpress.com/2011/09/ccna-1-y-2.pdf

Cisco. (16 de 11 de 2017). *CCNA desde cero*. (A. Walton, Editor) Recuperado el 06 de 11 de 2018, de CCNA desde cero: https://ccnadesdecero.es/representacion-red-diagrama-de-topologia/

CISCO. (s.f.). *IP Multicast Routing Configuration Guide, Cisco IOS Release 15.2(2)E (Catalyst 3750-X and 3560-X Switches)*. Recuperado el 01 de 08 de 2017, de http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750x_3560x/software/release/15-2_2_e/multicast/configuration_guide/b_mc_1522e_3750x_3560x_cg/b_mc_3750x_3560x_chapter_01.html

Cisco Systems. (2007).

Colomès, P. (27 de 11 de 15). *REDES CISCO.NET*. Recuperado el 21 de 11 de 2018, de REDES CISCO.NET: http://www.redescisco.net/sitio/2015/11/27/eigrp-vs-ospf/comment-page-1/

Comisión Federal de Electricidad. (2016). *Informe Anual 2016.* Recuperado el 26 de 10 de 2018, de https://www.cfe.mx/inversionistas/Documents/informe_anual/Informe%20Anual%202016%20CFE.pdf

Comisión Federal de Electricidad. (s.f.). *Comisión Federal de Electricidad*. Recuperado el 08 de 10 de 2018, de Comisión Federal de Electricidad: https://www.cfe.mx/acercacfe/Quienes%20somos/Pages/conceptocfe.aspx

ESTA International, LLC. (2014). *Marco Regulatorio de la Red Eléctrica Inteligente (REI) en México.* Herndon: ESTA International, LLC. Recuperado el 26 de 10 de 2018

Hayden, M. (1999). *Aprendiendo Redes en 24 Horas* (primera ed.). (C. R. Pedraza, Trad.) México, México: PRENTICE HALL HISPANOAMERICANA S.A. Recuperado el 11 de 11 de 2018

IDE. (2010 de 05 de 25). *IDE*. Recuperado el 12 de 11 de 2018, de IDE: http://ide-construccionderedes.blogspot.com/2010/05/modelo-osi.html

Internetmania. (s.f.). *¿Qué es una dirección MAC?* Obtenido de http://www.internetmania.net/int0/int55.htm

Raya Cabrera , J. L., & Raya González, L. (2006). *Redes Locales* (cuarta ed.). (ALFAOMEGA, Ed.) Madrid, España: Ra-Ma. Recuperado el 06 de 11 de 2018

Redes y Seguridad. (09 de Enero de 2009). *Redes y Seguridaad*. Recuperado el 06 de 11 de 2018, de Redes y Seguridaad: http://www.redesyseguridad.es/¿que-es-una-red/

Rico, E. (s.f.). *ERMESH*. Obtenido de ERMECH: http://www.ermesh.com/modelo-osi-parte-1-aspectos-generales/

Selvas, M. A. (2018 de FEBRERO de 1). INTRODUCCIÓN A LA REDES DE DATOS. TUXTLA GUTIÉRREZ, CHIAPAS, MÉXICO. Recuperado el 2018 de 11 de 14

SENER. (1 de 05 de 2016). *gob.mx*. Recuperado el 22 de 11 de 2018, de gob.mx: https://www.gob.mx/cms/uploads/attachment/file/90007/Programa_de_Redes_El_ctricas_Inteligentes_09_05_16.pdf

Vázquez, M. (18 de 03 de 10). *BONAVAL*. Recuperado el 12 de 11 de 18, de BONAVAL: https://www.bonaval.com/kb/sistemas/redes/modelo-osi

wikipedia. (21 de 01 de 2012). *WIKIPEDIA*. Recuperado el 14 de 11 de 2018, de WIKIPEDIA: https://es.wikipedia.org/wiki/VLAN#/media/File:VLAN.svg