UNIVERSIDAD POLITÉCNICA DE PUEBLA
Ingeniería en Informática

Proyecto de Estancia Práctica en Desarrollador en Sistemas de Software y Administrador de Redes

Diseño e identificación de una red LAN y WAN de la zona Puebla y San Martin Texmelucan, CPI y terminales de los servicios de red de PEMEX

Área temática del CONACYT: VII
Ingenierías y tecnologías

Presenta:
Jan Carlos Robles Ortega

Asesor técnico
Ing. Oscar Mario Macías García
Asesor académico
MC Rebeca Rodríguez Huesca

Juan C. Bonilla, Puebla, México. 19 de Diciembre de 2018

Resumen

Las redes hoy en día son muy importantes para las empresas, pues gracias a su gran desempeño les permite ahorrar tiempo y dinero, dado a que hoy todo tiende a realizarse a través de la internet. El mismo mercado exige a las empresas demostrar su mayor potencial para poder posicionarse en una de las mejores empresas. Además permite a los empleados comunicación inmediata a los diferentes departamentos que se encuentren, no importando su localización geográfica.

El presente proyecto consiste en el Diseño e Identificación de una red LAN (Red de área local) y WAN (Red de área amplia) de la zona Puebla y San Martín Texmelucan Puebla, el cuál estudiará la problemática actual de la empresa Petróleos Mexicanos (PEMEX), analizando los requerimientos de la misma para la elaboración del proyecto. Es por ello, que el proyecto antes mencionado planteará una solución viable a los requerimientos de la empresa PEMEX. Se pretende tener comunicación en las terminales de los servicios de red de PEMEX, debido a esto será necesario realizar una topología física y lógica para después partir al cableado físico de acuerdo a las normativas ANSI/TIA/EIA-568, que nos facilitarán el correcto funcionamiento y rendimiento de la instalación, así como la reducción de riesgos y gastos económicos. Así mismo, se pone en práctica los conocimientos adquiridos en la carrera de Ingeniería en Informática en la Universidad Politécnica de Puebla.

La finalidad de este proyecto es crear una red LAN en el edificio de Telecomunicaciones Tecnologías de la Información, así como proporcionar internet a los trabajadores de PEMEX y al mismo tiempo permitir comunicación en las terminales de los servicios de red de la empresa.

Índice

1. Introducción

En esta sección se pretende dar a conocer las necesidades de la empresa, lo cual es primordial para el inicio del proyecto. A partir de ello se planteará una solución viable de acuerdo a las problemáticas detectadas en la empresa.
Esta solución permitirá a la empresa PEMEX tener su propia Red LAN en el departamento de Telecomunicaciones y Tecnologías de la Información para así poder proporcionar internet a sus empleados y al mismo tiempo tener comunicación en las diferentes terminales de los servicios de red de la misma.

1.1 Descripción del problema o necesidad

En la empresa PEMEX presentan diversos problemas en el departamento de Telecomunicaciones y Tecnologías de la Información que son reflejados en las quejas y sugerencias de los trabajadores de la misma.

Como problema principal se encuentran fallas e inestabilidades en las terminales de los servicios de la red y esto provoca que los trabajadores no tengan acceso a internet y no exista comunicación en los departamentos permanecientes en la empresa. Otro problema reflejado es la configuración inadecuada de los dispositivos intermediarios (Router y Switch) y dispositivos finales (Computadoras) debido a que los paquetes de información no llegan a su destino, por consecuencia se llevará a cabo la configuración de protocolos de enrutamiento y encapsulamiento.
Además se detectó inestabilidad en la implementación del cableado estructurado, el cual se encuentra dañado debido a la ausencia del mantenimiento preventivo que se debe de dar respectivamente. Debido a que la empresa adoptó una nueva tecnología llamada “Huawei” se deben hacer modificaciones y actualizaciones en cada subred.

Actualmente las empresas en el área de Telecomunicaciones y Tecnologías de la Información con mayor demanda están obligadas a tener una Red LAN en cada departamento para así tener mejor comunicación en las terminales pertenecientes de la empresa. Es por ello que deben contar un una red confiable y segura.

1.2 Justificación

De acuerdo a las problemáticas antes planteadas se realizará un diseño de red LAN y WAN en la empresa PEMEX en el departamento de Telecomunicaciones y Tecnologías de la Información, esto incluye realizar topología física y lógica,

subneteo, configuración de protocolos en enrutamiento y encapsulamiento en el router, creación de VLAN y puertas troncales en el switch y asignación de direcciones ip a los equipos de cómputos.
Hoy en día las empresas necesitan de una red LAN propia para poder tener comunicación en los demás departamentos internos de la misma. Además si quieren tener comunicación en otras terminales CPI no importando su localización geográfica ni arquitectura necesitan una configuración adecuada, es por ello la gran importancia de este proyecto. Se considera que esta solución es viable debido a que se cuenta con los recursos humanos, materiales y económicos necesarios para llevarlo a cabo.
El departamento de Telecomunicaciones y Tecnologías de la Información cuenta con un almacén, la cual contiene tiene todas las herramientas necesarias para llevar a cabo el proyecto como cable UTP, cable Serial, conectores RJ45, ponchadoras, switch, router por mencionar algunos.

Con la solución propuesta se espera un crecimiento productivo, dado que la empresa podrá establecer comunicación inmediata en la zona Puebla y San Martin Texmelucan Puebla, CPI y terminales de los servicios de red de PEMEX.

1.3 Objetivo General y Específicos

Diseñar una Red LAN y WAN en el departamento de Telecomunicaciones y Tecnologías de la información para permitir la comunicación inmediata y segura en las terminales de servicio de red de la empresa.

Objetivos Específicos

- Diseñar la red basados en los requerimientos de cableado estructurados y sus normas.
- Diseñar una topología física y lógica.
- Configurar los dispositivos intermediarios y finales.
- Asignar direcciones Ipv4 a los equipos de cómputo.
- Proporcionar internet con un ancho de banda estable.
- Establecer la seguridad en la red de la empresa.

2. Metodología y herramientas

En este capítulo se dará a conocer la fundamentación teórica para el desarrollo del proyecto. Además se presentarán las herramientas con su respectiva descripción, ventajas y desventajas con el fin de dar a conocer la importancia de cada una de ellas.

Para que una red LAN sea efectiva y satisfaga las necesidades de los usuarios y trabajadores de la empresa PEMEX en el departamento de Telecomunicaciones y Tecnologías de la Información, se debe de diseñar e implementar de acuerdo con una serie planificada de pasos sistemáticos y ordenados.

Por consiguiente se dará a conocer la metodología a utilizar:

Metodología Top-Down

Es una metodología para diseñar redes que comienza en las capas superiores del modelo de referencia de OSI antes de mover a las capas inferiores. Esto se concentra en aplicaciones, sesiones, y transporte de datos antes de la selección de router, switch, y medios que funcionan en las capas inferiores.

A continuación se presentarán la descripción de las etapas que conforman la metodología:

- **Analizar requerimientos**
  En esta etapa se realizará un estudio general de los requerimientos necesarios de la empresa para poder llevar a cabo el proyecto. Es un punto importante debido a que da origen al inicio del proyecto. Conociendo cada uno de las problemáticas se podrá dar solución.

- **Desarrollar diseño Físico**
  Esta etapa implica en seleccionar las tecnologías y dispositivos específicos que darán satisfacción a los requerimientos técnicos identificados. Es por ello que se llevará a cabo el cableado estructurado de acuerdo a las normativas ANSI/TIA/EIA-568-B con el fin de garantizar el buen funcionamiento de la red y proveer acceso a los servicios telefónicos y redes de computadoras.

- **Desarrollar diseño lógico**
  En esta etapa se llevará a cabo la creación de subredes para el departamento de Telecomunicaciones y Tecnologías de la información, para simplificar la administración y permitir el crecimiento de la red. El diseño lógico también incluye la seguridad y administración de la red.

- **Implementar y configurar la red**
  En esta etapa se realizará la configuración de los dispositivos intermediarios (Switch, Router) así como la asignación de direccionamiento IP, mascara de subred y default gateway de acuerdo a las subredes creadas en la etapa anterior en los dispositivos finales (Computadoras

- **Probar y Verificar la red**
  En esta etapa se realizarán diferentes pruebas de la red para verificar él envió de los paquetes, la conectividad inmediata y la asignación de direccionamiento IP. Para establecer y asegurar la conectividad de las terminales de la empresa PEMEX.

2.1 Cableado estructurado

Un cableado estructurado es definido como la configuración de todos los cables y accesorios, instalados en un local determinado, y que constituyen una infraestructura de telecomunicaciones completas. La infraestructura, sin depender de dispositivos o aplicaciones, se destina a una amplia variedad de usos, como también, proveer acceso a los servicios telefónicos o de redes de computadoras [1].

2.1.1 Estandarización de Instalaciones de Cableado

La estandarización de las instalaciones de cableado es necesaria para garantizar el buen funcionamiento de sistemas cada vez más complejos. Las industrias del cableado en EE.UU. Aceptan la American National Standars Institute/Telecommunications Industry Association/Electronic Industries Alliance (ANSI/TIA/EIA), como las organizaciones responsables por proveer y mantener las normas y procedimientos que rigen la profesión [2].

La ANSI conjuntamente con la TIA/EIA ha publicado una serie de normas para el diseño, instalación y manutención de instalaciones de cableado de todos los tipos. La aplicación correcta de las normas, garantiza instalaciones de cableado bien ejecutadas.

Los siguientes puntos son los beneficios de las normas:

- Coherencia entre el proyecto y la instalación del cableado
- Conformidad con los requisitos físicos y de transmisión.

- Una base para examinar propuestas de expansiones y de otras alteraciones.
- Uniformidad en la documentación.

2.1.2 Cableado Horizontal

La ANSI/TIA/EIA-568-B.1 define como [3]:

El cableado horizontal es la parte de un sistema de cableado de telecomunicaciones que se extiende desde el conector de salida de telecomunicaciones en el área de trabajo, hasta la conexión cruzada horizontal en el cuarto de telecomunicaciones y Tecnologías de la Información.

El cableado horizontal comprende los cables horizontales, conectores o salidas en el área de trabajo.

En la sección de un cableado horizontal, debe considerarse lo siguiente:

- La longitud máxima permitida del cable horizontal es 90m (295 pies).
- Se requiere un mínimo de dos conectores o salidas de telecomunicaciones, para cada área de trabajo, en cumplimiento de la ANSI/TIA/EIA-568-B.1.
- El cableado horizontal debe acomodar una variedad de aplicaciones (voz, datos, video) reduciendo los cambios a medida que las necesidades del usuario aumenten.

La ANSI/TIA/EIA-568-B.1 requiere el uso de dos medios para servicios de telecomunicaciones en un área de trabajo:

- Cable de 4 pares trenzado sin blindaje (UTP) de 100 Ω cable de par trenzado apantallado (ScTP).
- Cable de fibra óptica multimodo, de dos o más fibras, cada una de 50/125 mm o 62,5/128mm.

2.1.3 Áreas de trabajo (WAs)

Un área de trabajo típica es de aproximadamente $10m^2$(100 $pies^2$). Incluyendo los componentes que se extienden desde el conector o salida de telecomunicaciones, hasta el equipo de la estación.

Estos componentes, que están fuera del ámbito de la ANSI/TIA/EIA-568-B.1, pueden ser, por ejemplo, teléfonos, terminales de datos, equipos de video y computadoras. También se incluye en el área de trabajo los cables que van desde los equipos de la estación hasta el conector o salida de telecomunicaciones [4].

En la planificación de un cableado de WA, se tiende presente lo siguiente:

- Los cables de conexión se diseñan para facilitar los cambios de rutas.
- La longitud máxima del cable horizontal se especifica.
- Los cables de conexión más utilizados son aquellos con conectores idénticos en ambas extremidades. Deben ser ensamblados y probados en fábrica.
- El requisito para los cables de conexión de cobre es que sean de cable trenzado.
- Cuando se necesite usar adaptadores para aplicaciones específicas (adaptador modular) en el WA, la ANSI/TIA/EIA-568-B.1 especifica que se instalen externamente al conector o salida de telecomunicaciones.

Cabe destacar que el uso de adaptadores en el WA puede perjudicar la eficiencia de transmisión de un sistema de cableado. Por consiguiente, es importante considerar la compatibilidad de los mismos con los equipos y cableado del local, antes de instalarlos en la red.

2.1.4 Salas de Equipos (ER)

Una sala de equipos (ER) es un cuarto especialmente acondicionado para alojar y mantener un ambiente operacional adecuado para grandes equipos de telecomunicaciones. Las ER, en general, se destinan a servir un edificio completo (o campus), mientras que un cuarto de telecomunicaciones (TR) sirve un piso, o una parte de él [5].

Las ER (a veces llamadas de TR principales):

- Proveen las terminaciones y las conexiones cruzadas del cableado troncal y de los cables horizontales.
- Proporcionan espacio de trabajo entre el personal de servicios.
- Son proyectados de acuerdo a los requisitos específicos asociados al costo, tamaño, crecimiento y complejidad de los equipos involucrados.
- Alojan partes de los equipos comunes de control, tales como: voz, datos, video, alarma de incendios, gestión de energía, detección de entradas.

Aunque una ER normalmente sirve a un edificio entero, a veces es necesario utilizar más de una ER para proporcionar:

- Instalaciones separadas para diferentes tipos de equipos y servicios.
- Instalaciones de reserva y evitación de desastres.
- Servicios separados para cada inquilino de un edificio de multiusuario.

Consideraciones que se tomaron en cuenta en el proyecto de una ER:

- Debe ser versátil y diseñada para alojar las aplicaciones actuales y futuras.

- Debe prever el crecimiento y poder soportar las substituciones y actualizaciones de los equipos durante la vida útil y poder soportar con un mínimo de interrupciones y al más bajo costo.
- Debe satisfacer los requisitos de: iluminación, aire acondicionado, carga de **piso, electricidad y de espacios mínimos.**

2.1.5 Normas

TIA (Telecommunications Industry Association), fundada en 1985 después de la ruptura del monopolio de AT&T. Desarrolla normas de cableado industrial voluntario para muchos productos de las telecomunicaciones y tiene más de 70 normas preestablecidas [6].

ANSI (American National Standards Institute): Es una organización sin ánimo de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unidos. ANSI es miembro de la Organización Internacional para la Estandarización (ISO) y de la Comisión Electrotécnica Internacional (International Electrotechnical Commission, IEC).

EIA (Electronic Industries Alliance): Es una organización formada por la asociación de las compañías electrónicas y de alta tecnología de los Estados Unidos cuya misión es promover el desarrollo de mercado y la competitividad de la industria de alta tecnología de los Estados Unidos con esfuerzos locales e internacionales de la política.

ISO (International Standards Organization): Es una organización no gubernamental creada en 1947 a nivel mundial de cuerpos de normas nacionales, con más de 140 países.

IEEE (Instituto de Ingenieros Eléctricos y de Electrónica): Principalmente responsable por las especificaciones de redes de área local como 802.3 Ethernet,802.5 TokenRing, ATM y las normas de GigabitEthernet.

2.1.6 Estándares del cableado UTP

Los estándares de cableado estructurado definen varios tipos de conexiones que se pueden utilizar a la hora de ensamblar el cable de par trenzado con el conector RJ-45, tanto en conectores macho como hembra. De todas ellas, las que más se utilizan son la ANSI/EIA/TIA-568A y ANSI/EIA/TIA- 568B.

El instalador debe decidir qué norma resulta más recomendable seguir, sobre todo si ya existe cableado anterior que se quiere reutilizar.

Cabe mencionar que no es aconsejable utilizar las dos normas a la vez al realizar el cableado de un edificio, ya que puede dar lugar a problemas de instalación y mantenimiento.

En el departamento de Telecomunicaciones y Tecnologías de la información se utilizará Cable de Categoría 5e (UTP) debido a que admite velocidades de 1000 Mbps

Norma EIA/TIA 568A (T568A) y 568B (T568B)

La norma garantiza que los sistemas que se ejecuten de acuerdo a ella soportarán todas las aplicaciones de telecomunicaciones presentes y futuras por un lapso de al menos diez años. Posteriormente, la ISO (International Organization for Standards) y el IEC (International Electrotechnical Commission) la adoptan bajo el nombre de ISO/IEC DIS 11801 (1994). Haciéndola extensiva a Europa (que ya había adoptado una versión modificada, la CENELEC TC115) y el resto del mundo [7].

El cableado estructurado para redes de computadores tiene dos tipos de normas, la EIA/TIA-568A (T568A) y la EIA/TIA-568B (T568B).

Se diferencian por el orden de los colores de los pares a seguir en el armado de los conectores RJ45. Si bien el uso de cualquiera de las dos normas es indiferente, generalmente se utiliza la T568B para el cableado recto.

EIA/TIA-568B

Ambos extremos del cable montados de la misma manera. El switch se encarga de cruzar la señal para que la Transmisión llegue a la recepción correspondiente.

EIA/TIA-568A

Uno de los extremos se monta según la norma EIA/TIA 568 B y el otro extremo según la norma EIA/TIA 568 A. Este tipo de cables se utiliza para unir dos equipos directamente a través de sus correspondientes tarjetas de red.

Pruebas de los cables UTP

Tester

El tester de redes LAN cubre el ámbito de la instalación y control de redes. Este tester de redes LAN puede ser utilizado in situ y de un modo rápido, por ello es ideal para profesionales de servicio técnico y para administradores de red.

Este tester de redes LAN facilita la determinación Visión general de los productos de direcciones IP, la identificación de la polaridad, la medición a doble carga, la detección de un cable concreto.

2.2 Topología Física

La topología LAN está relacionada a la topología de los medios físicos que la constituyen. Básicamente, la topología LAN es determinada por el cómo los

canales de transmisión son utilizados para conectar los dispositivos de la red. Generalmente, se refiere al armado físico de la LAN, a su configuración lógica y a la estrategia de cableado siendo usada. Es reconocido que la topología es la base de una LAN.

Existen tres topologías básicas, estrella, bus y datos. A partir de estas tres, se han desarrollado varias topologías hibridas, tales como: anillo, árbol, alambrado, en forma de estrella, estrella agrupada y estrella jerárquica. La topología física que se requiere para un sistema de cableado estructurado (SCS) es la topología estrella. Debido a que ofrece una gran flexibilidad debido a que se puede ser configurada para funcionar con cada una de las topologías lógicas (estrella, bus, anillo e hibridas) [8]. La empresa PEMEX tiene una combinación de topologías, debido al gran número de dispositivos conectados en la red, las cuales son de se presentarán a continuación.

2.2.1 Topología Estrella

Es una topología de estrella, el concentrador o conmutador es colocado en el centro físico, como también en el centro lógico de la red. Los otros dispositivos de la red son conectados a esta unidad central como las puntas de una estrella. Cada dispositivo tiene su propia línea, directa y dedicada, hacia el concentrador o conmutador. Cualquier dispositivo de la red que envi9e un mensaje a otro dispositivo de la misma, lo hace a través de éste centralizador.

La estación que envía el mensaje lo manda al concentrador. Enseguida, éste lo envía a la estación de destino especificado, lo que se conoce como conmutación [9].

Figura 1. Topología de estrella

La figura 1 representa la distribución de los dispositivos en una topología de estrella, cabe mencionar que debe existir un servidor central que permita la distribución y almacenamiento de la información de las computadoras de la red.

Ventajas:

- El cableado es de fácil instalación y manutención

- En el caso de que un dispositivo sea desactivado o aislado del concentrador central, sólo él es afectado.
- Las fallas son fáciles de localizar y aislar.
- Proporciona un lugar central para administrar la red.

Desventajas:

Podría ser vulnerable a las interrupciones ya que la red es esencialmente controlada por un dispositivo en un local central.

2.2.2 Topología Bus

La topología bus tiene una configuración lineal. Coloca todos los dispositivos de la red en una longitud de cable, similarmente a los paraderos de una ruta de buses en una ciudad. Todos los dispositivos periféricos, los concentradores, servidores, y estaciones usan la misma longitud continua del cableado.

En esta distribución, el extremo del cable no es conectado a los dispositivos de la red.

Ordinariamente los problemas aparezcan cuando la señal transmitida es enviada a lo largo del cable y alcanzan cualquiera de los extremos. Por esta razón, cada extremo del cable es conectado a un terminador.

Cuando un mensaje se transmite sobre esta topología, la señal transmitida sale del dispositivo transmisor y viaja a lo largo del cable en ambas direcciones. El dispositivo para lo cual el mensaje esta designado, reconocerá la transmisión y lo leerá.

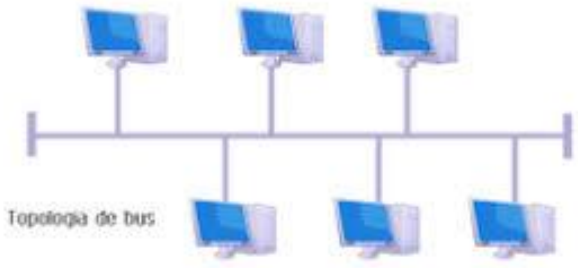


Figura 2. Topología de bus

La figura 2 representa la distribución de los dispositivos en una topología de bus, la información es enviada por el mismo bus de datos.

Ventajas:

- Adaptabilidad a varios ambientes, puede ser configurada para ajustarse a la mayoría de las situaciones
- Expansibilidad, debido a que puede agregarse dispositivos en varios puntos a lo largo del cable

Desventajas:

Carece de un control central, por lo tanto resulta difícil localizar una falla.

En el caso de que una de las extremidades del cable sea damnificada o pierda su terminador, toda la red fallará.

2.3 Topología Lógica

La topología lógica describe la manera en que los datos son convertidos a un formato de trama específico y la manera en que los pulsos eléctricos son transmitidos a través del medio de comunicación, por lo que esta topología está directamente relacionada con la Capa Física y la Capa de Enlace del Modelo *OSI*.

2.3.1 Modelo OSI

El Modelo *OSI* divide en 7 capas el proceso de transmisión de la información entre equipo informáticos, donde cada capa se encarga de ejecutar una determinada parte del proceso global [10].

Capa 1: Física – Este es el nivel de lo que llamamos llánamente hardware. Define las características físicas de la red, como las conexiones, niveles de voltaje, cableado, etc. Como habrás supuesto, podemos incluir en esta capa la fibra óptica, el par trenzado, cable cruzados, etc.

- *Función:* recibir los datos e iniciar el proceso (o lo contrario, introducir datos y completar el proceso).
- *Dispositivos:* cables, conectores, concentradores, transceiver (traducción entre las señales ópticas y eléctricas - que se desplaza en cables diferentes).
- *PDU:* bits.

Capa 2: Datos – También llamada capa de enlaces de datos. En esta capa, el protocolo físico adecuado es asignado a los datos. Se asigna el tipo de red y la secuencia de paquetes utilizada

- *Función:* Enlace de datos de un host a otro, por lo que es a través de los protocolos definidos para cada medio específico por el cual se envían los datos.
- *Protocolos:* PPP, Ethernet, FDDI, ATM, Token Ring.
- *Dispositivos:* Interruptores, Tarjeta de red, interfaces.

- *PDU:* Trama

Capa 3: Red – Esta capa determina la forma en que serán mandados los datos al dispositivo receptor. Aquí se manejan los protocolos de enrutamiento y el manejo de direcciones IP.

- *Función:* direccionamiento, enrutamiento y definir las mejores rutas posibles.
- *Protocolos:* ICMP, IP, IPX, ARP, IPSEC.
- *Dispositivos:* Routers.
- *PDU:* Paquetes.

Capa 4: Transporte – Esta capa mantiene el control de flujo de datos, y provee de verificación de errores y recuperación de datos entre dispositivos. Control de flujo significa que la capa de transporte vigila si los datos vienen de más de una aplicación e integra cada uno de los datos de aplicación en un solo flujo dentro de la red física. Como ejemplos más claros tenemos TCP y UDP.

- *Función:* hacer frente a todas las cuestiones de transporte, entrega y recepción de datos de la red, con calidad de servicio.
- *Protocolos:* TCP, UDP, SPX.
- *Dispositivos:* Routers.
- *PDU:* Segmento.

Capa 5: Sesión – Esta capa establece, mantiene y termina las comunicaciones que se forman entre dispositivos. Un punto importante aquí es la necesidad de sincronización entre los anfitriones, de lo contrario la comunicación se verá comprometida, incluso dejar de trabajar. Esta capa añade marcas de los datos transmitidos. Por lo tanto, si la comunicación falla, puede ser reiniciado por última vez el marcado recibió válida.

Función: iniciar, gestionar y terminar sesiones de la capa de presentación, por ejemplo, sesiones TCP.

Capa 6: Presentación - Esta capa tiene la misión de coger los datos que han sido entregados por la capa de aplicación, y convertirlos en un formato estándar que otras capas puedan entender. En esta capa tenemos como ejemplo los formatos MP3, MPG, GIF, etc.

- *Función:* encriptación, compresión, formato y la presentación de formatos de datos (por ejemplo, JPEG, GIF, MPEG) para las aplicaciones.
- *Protocolos:* SSL, TLS.
- Dispositivos: Gateways (protocolos de traducción entre diferentes redes).

Capa 7: Aplicación - Esta es la capa que interactúa con el sistema operativo o aplicación cuando el usuario decide transferir archivos, leer mensajes, o realizar otras actividades de red. Por ello, en esta capa se incluyen tecnologías tales como http, DNS, SMTP, SSH, Telnet, etc. En esta capa tenemos las interfaces de usuario, que son creados por los propios datos (correo electrónico, transferencia de archivos, etc.) Aquí es donde los datos son enviados y recibidos por los usuarios. Estas peticiones se realizan por las aplicaciones de acuerdo a los protocolos utilizados.

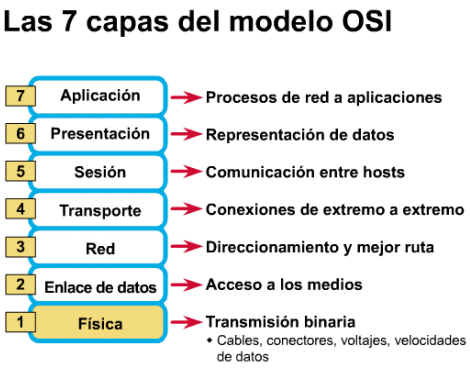


Figura 3. Modelo OSI

La figura 3 muestra las 7 capas del modelo *OSI* con una pequeña descripción de cada una de ellas.

2.3.2 Protocolo

Un protocolo es un método establecido de intercambiar datos en Internet. Un protocolo es un método por el cual dos ordenadores acuerdan comunicarse, una especificación que describe cómo los ordenadores hablan el uno al otro en una red. El protocolo determina lo siguiente [11]:

- El tipo de comprobación de errores que se utilizará.
- Cómo indicará el dispositivo que envía que ha acabado el enviar un mensaje.
- Cómo indicará el dispositivo que recibe que ha recibido un mensaje.

Protocolos de enrutamiento

Un protocolo de enrutamiento indica al enrutador (router) cuál es la ruta adecuada que deben de seguir para enviar los datos, para eso se utiliza el vector distancia, que permite contabilizar un salto cada vez que un dato atraviesa un router. Es decir, un protocolo de enrutamiento se configura en un enrutador para que el mismo aprenda las mejores rutas disponibles y luego envié los paquetes

hasta su destino final. Básicamente, el protocolo de enrutamiento establece las reglas sobre cómo un enrutador aprende redes remotas y luego anuncia estas redes a enrutadores vecinos dentro de la misma red.

Vector Distancia: Su métrica se basa en lo que se le llama en redes “Numero de Saltos”, es decir la cantidad de routers por los que tiene que pasar el paquete para llegar a la red destino, la ruta que tenga el menor número de saltos es la más óptima y la que se publicará.

Estado de Enlace: Su métrica se basa el retardo, ancho de banda, carga y confiabilidad, de los distintos enlaces posibles para llegar a un destino en base a esos conceptos el protocolo prefiere una ruta por sobre otra. Estos protocolos utilizan un tipo de publicaciones llamadas Publicaciones de estado de enlace (LSA), que intercambian entre los routers, mediante estas publicaciones cada router crea una base datos de la topología de la red completa.

Existen dos tipos de protocolos de enrutamiento:

1. **Enrutamiento dinámico:**

El enrutamiento dinámico se logra mediante el uso de un o más protocolos de enrutamiento, como ser RIP, IGRP, EIGRP u OSPF. Un enrutador configurado con un protocolo de enrutamiento dinámico puede:

- Recibir y procesa las actualizaciones enviadas por enrutadores vecinos, que ejecutan el mismo protocolo de enrutamiento.
- Aprender sobre redes remotas por medio de las actualizaciones recibidas de enrutadores vecinos.
- Si existiesen múltiples rutas a una misma red remota, aplicar un algoritmo para determinar la mejor ruta, la más rápida.
- Anunciar, a enrutadores vecinos, sobre sus rutas a redes remotas.
- Actualizar sus rutas cuando, por algún motivo, ocurre algún cambio en la topología.

2. **Enrutamiento estático**

Con el enrutamiento estático, el enrutador es literalmente ordenado, por el administrador de la red, por donde llegar a las redes remotas.

En otras palabras, el administrador configura manualmente las rutas estáticas en el enrutador. Es como decirle al enrutador, literalmente; "Para enviar paquetes a la red X, envíalos por la interfaz X o, a la dirección IP del próximo salto X". Es ideal para redes pequeñas.

Protocolos de enrutamiento

- **RIP**: Es un protocolo de encaminamiento interno. Es muy usado en sistemas de conexión a internet, en el que muchos usuarios se conectan a una red y pueden acceder por lugares distintos.
  Cuando uno de los usuarios se conecta el servidor de terminales (equipo en el que finaliza la llamada) avisa con un mensaje RIP al router más cercano advirtiendo de la dirección IP que ahora le pertenece.
- **IGRP:** Protocolo de enrutamiento de Gateway Interior por vector distancia, del cual es propietario *CISCO*.

- **EIGRP:** Protocolo de enrutamiento de *Gateway* Interior por vector distancia, es una versión mejorada de *IGRP*.

TCP/IP

TCP/IP se ha convertido en el estándar de-facto para la conexión en red corporativa. Las redes *TCP/IP* son ampliamente escalables, para lo que TCP/IP puede utilizarse tanto para redes pequeñas como grandes.

Direccionamiento IP

Para que dos o más computadoras se comuniquen, es necesario que los equipos puedan dialogar en un "lenguaje común", o sea que puedan comunicar entre sí. Se requiere un conjunto de reglas o convenciones (lo que se denomina protocolo), para lograr el intercambio de información en forma ordenada y eficaz. Para posibilitar la comunicación entre diferentes tipos de computadoras y redes de desarrollo, denominado protocolo de *TCP/IP* (Protocolo de transmisión y protocolo de internet) que posibilitó asegurar que la información llegue a un destino específico

Existen 5 clases de redes identificadas como:

Clase A: Utilizada para grandes organizaciones

Clase B: Utilizada para organizaciones medias

Clase C: Utilizada para organizaciones pequeñas

Clase D: Utilizadas para grupos de multidifusión

Clase E: Utilizada para redes científicas o experimentales.

Dirección de red: Utilizada para identificar la red entre sí.

Dirección de broadcast: Utilizada para realizar el broadcast de paquetes hacia todos los dispositivos de la red.

Mascara de Red

Prefijo de red extendida. Número que acompaña a una dirección IP, indicando los bits totales ocupados para la parte de la red.

Figura 4. Clases de redes

La figura 4 muestra la 5 clases de redes que existen y cada una de ellas tienen diferente identificador de red, y se usa dependiendo los requerimientos de la empresa. Debido a que la empresa PEMEX es una organización grande, se utilizó la clase A.

DHCP

Es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

2.3.3 Creación de Subredes

Una subred es una agrupación física o lógica de dispositivos de red que conforman una sección de un sistema autónomo o como tal pueden ser un sistema autónomo [13].

Pasos para la creación e una subred

1. Selección de la cantidad de bits que se usaran para la subred, dependerá de la cantidad de host necesarios por cada subred que se creara.
2. Calcular la máscara con la cantidad de bits utilizados para la parte de red y subred para ser configurada en los dispositivos
3. Calculo de redes utilizables
4. Calculo de host utilizables
5. Determinar los límites de las subredes creada

Subneteo

Consiste en dividir las clases de direcciones de red completas en partes de menor tamaño.

Es dividir una red IP en una serie de subredes, de tal forma que cada una de ellas va a funcionar luego, a nivel de envió y recepción de paquetes, como una red individual, aunque todas pertenezcan a la misma red principal y por lo tanto, al mismo dominio.

El Subneteo permite una mejor administración, control de tráfico y seguridad al segmentar la red por función.

2.4 Configuración de dispositivos intermediarios y finales

Los dispositivos intermediarios interconectan dispositivos finales. Estos dispositivos proporcionan conectividad y operan detrás de escena para asegurar que los datos fluyan a través de la red. Los dispositivos intermediarios conectan los hosts individuales a la red y pueden conectar varias redes individuales para formar una internetwork.

La administración de datos mientras fluyen a través de la red también es una función de los dispositivos intermediarios. Estos dispositivos utilizan la dirección host de destino, conjuntamente con información sobre las interconexiones de la red, para determinar la ruta que deben tomar los mensajes a través de la red. Los procesos que se ejecutan en los dispositivos de red intermediarios realizan las siguientes funciones [14]:

- Regenerar y retransmitir señales de datos,
- Mantener información sobre qué rutas existen a través de la red y de la internetwork,
- Notificar a otros dispositivos los errores y las fallas de comunicación,
- Direccionar datos por rutas alternativas cuando existen fallas en un enlace,
- Clasificar y direccionar mensajes según las prioridades de QoS (calidad de servicio), y
- Permitir o denegar el flujo de datos en base a configuraciones de seguridad.

Es por ello la importancia de la configuración de dispositivos intermediarios y finales para asegurarnos que la comunicación inmediata entre ellos.

Por consiguiente se presentarán los dispositivos que son factor para la realización del proyecto.

2.4.1 Configuración de Switch

Un switch o conmutador es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local

(LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet (o técnicamente IEEE 802.3) [15].

La función básica de un switch es la de unir o conectar dispositivos en red. Es importante tener claro que un switch no proporciona por si solo conectividad con otras redes, y obviamente, tampoco proporciona conectividad con Internet. Para ello es necesario un router.

El switch es posiblemente uno de los dispositivos con un nivel de escalabilidad más alto. Existen switch de cuatro puertos con funciones básicas para cubrir pequeñas necesidades de interconexión. Pero también podemos encontrar switch con cientos de puertos y con unas prestaciones y características muy avanzadas.

Puertos

Los puertos son los elementos del switch que permiten la conexión de otros dispositivos al mismo. Como por ejemplo un PC, portátil, un router, otro switch, una impresora y en general cualquier dispositivo que incluya una interfaz de red Ethernet.

El número de puertos es una de las características básicas de los switch. Aquí existe un abanico bastante amplio, desde los pequeños switch de 4 puertos hasta switch que admiten cientos de puertos.

Velocidad

Dado que Ethernet permite varias velocidades y medios de transmisión, otra de las características destacables sobre los puertos de los switch es precisamente la velocidad a la que pueden trabajar sobre un determinado medio de transmisión. Podemos encontrar puertos definidos como 10/100, es decir, que pueden funcionar bajo los estándares 10BASE-T (con una velocidad de 10 Mbps) y 100BASE-TX (velocidad: 100 Mbps). Otra posibilidad es encontrar puertos 10/100/1000, es decir, añaden el estándar 1000BASE-T (velocidad 1000 Mbps). También se pueden encontrar puertos que utilicen fibra óptica utilizando conectores hembra de algún formato para fibra óptica. Existen puertos 100BASE-FX y 1000BASE-X.

Configuración

- Configuración de nombres
- Configuración de contraseñas
- Cifrado de contraseñas
- Mensaje de aviso
- Creación de VLAN y enlaces troncales
- Creación de VTP
- Líneas vty 0 15

- Configuraciones de acceso.

2.4.2 Configuración de Router

Un router es un dispositivo de red que permite el enrutamiento de paquetes entre redes independientes. Este enrutamiento se realiza de acuerdo a un conjunto de reglas que forman la tabla de enrutamiento. Es un dispositivo que opera en la capa 3 del modelo OSI.

Funciona en el ámbito de capa 3 y por ello requiere un análisis del protocolo Internet IP. Permiten mejorar la eficiencia de la red ya que toleran distintos caminos dentro de la red. El Router puede segmentar datagramas muy largos en caso de congestión, en cambio no pueden ensamblar datagramas.

Los router se pueden interconectar a alta velocidad mediante interfaces de 100 Mb/s (mediante pares o fibra óptica) y 1000 Mb/s (mediante Gigabit Ethernet) para formar redes de alta velocidad.

Configuración

- Configuración de nombres
- Configuración de contraseñas
- Cifrado de contraseñas
- Mensaje de aviso
- Protocolos de Enrutamiento
- Configuración de sub-interfaces
- Líneas vty 0 4

2.4.3 Configuración de Computadoras

La información de dirección IP se puede introducir en la PC en forma manual o mediante el Protocolo de configuración dinámica de host (DHCP). El protocolo DHCP permite configurar la información de IP de los dispositivos finales de manera automática [16].

DHCP es una tecnología que se utiliza en casi todas las redes comerciales. Para comprender mejor por qué DHCP es tan popular, tenga en cuenta todo el trabajo adicional que habría que realizar sin este protocolo. DHCP permite la configuración automática de direcciones IPv4 para cada dispositivo final de una red con DHCP habilitado. Debido a la cantidad de tiempo que se llevaría si se configura los equipos manualmente, considerando que por cada vez que se conecte un nuevo dispositivo, se tendría que introducir su respectiva dirección IP, la máscara de subred, el Gateway predeterminado, es por ello que no se optó para reducir el tiempo de asignación de direccionamiento. En los equipos de cómputo que estarán conectados en la red, se les asignara una dirección IP mediante el protocolo DHCP el cual estará configurado en el dispositivo intermediario (Router).

2.4.4 Herramientas

2.5 Verificación de Conectividad

Es de mayor importancia hacer la verificación de conectividad para asegurar el envió y recibiendo de paquetes en la red. Por lo tanto tenemos la necesidad de verificar una instalación realizada o atender un aviso de avería, una anomalía detectada o cualquier tipo de incidencia en una red que ya ha sido instalada y, supuestamente, verificada.

Esto determina los procedimientos sistemáticos que deben emplearse en uno u otro caso. Por un lado, la verificación de una instalación comprende su certificación dentro de la normativa internacional, mediante un dispositivo certificador que comprueba que los parámetros de la red se ajustan a los valores asignados de velocidad y calidad de transmisión del tipo de cable instalado.

Los procedimientos generales de resolución de incidencias en redes de área local se clasifican en tres fases, recopilación, ubicación y corrección [17].

Los métodos de resolución de problemas están basados en el modelo de pila de protocolos del modelo OSI, de modo que, la capa que se tome de inicio, determina el método a emplear.

De esta forma hay tres métodos:

- **Ascenso de capas:** Se empieza con la capa 1 del modelo OSI, y se comprueba cada dispositivo. Luego la 2, etc… Es práctico si se sospecha de anomalía física, pero es un trabajo faraónico si la red es grande.
- **Descenso de capas:** Se empieza con la capa 7, las aplicaciones, aunque, en realidad, se comienza comprobando los hábitos de trabajo del usuario. Luego se desciende para estudiar el software en la capa 6, y luego 5. Generalmente, el fallo está en la gestión del usuario o en la configuración de la aplicación usada. El caso de los plug-in o complementos del navegador de Internet, es lo más habitual.
- **Selección de capa**. El administrador de red determina la capa que puede estar causando la anomalía y, a partir de ahí, si no localiza el fallo, sigue por las capas contiguas.

Generalmente, si el problema es limitado, conviene el método de descenso de capas, pero si es más complejo o extraño, es más conveniente el ascenso de capas. El método de selección es más conveniente después de haber aplicado otros métodos que nos orientan sobre la ubicación (capa) de la anomalía.

Para ello existen diferentes formas de verificar la conectividad de dispositivos:

2.5.1 El Comando Ping

El comando ping es una manera eficaz de probar la conectividad. La prueba se denomina prueba de stack de protocolos, porque el comando ping se mueve desde la Capa 3 del Modelo OSI hasta la Capa 2 y luego hacia a la Capa 1. El ping utiliza el protocolo ICMP (Protocolo de mensajes de control de Internet) para comprobar la conectividad.

Indicadores de Ping IOS

- Un ping de IOS cederá a una de varias indicaciones para cada eco ICMP enviado. Los indicadores más comunes son:
- !: indica la recepción de una respuesta de eco ICMP.
- .: indica un límite de tiempo cuando se espera una respuesta.
- U: se recibió un mensaje ICMP inalcanzable.
- El "!" (signo de exclamación) indica que el ping se completó correctamente y verifica la conectividad de la Capa 3.
- El "." (punto) puede indicar problemas en la comunicación.
- Puede señalar que ocurrió un problema de conectividad en algún sector de la ruta. También puede indicar que un router a lo largo de la ruta no tenía una ruta hacia el destino y no envió un mensaje ICMP de destino inalcanzable. También puede señalar que el ping fue bloqueado por la seguridad del dispositivo.
- La "U" indica que un router del camino no tenía una ruta hacia la dirección de destino y respondió con un mensaje ICMP inalcanzable.

2.5.2 Prueba de Loopback

A modo de primer paso en la secuencia de prueba, se utiliza el comando ping para verificar la configuración IP interna en el host local. Recuerde que esta prueba se cumple con el comando ping en una dirección reservada denominada loopback (127.0.0.1). Esto verifica la correcta operación del stack de protocolos desde la capa de red a la capa Física, y viceversa, sin colocar realmente una señal en el medio. Los comandos ping se ingresan en una línea de comandos.

2.5.3 Prueba de Red Local

La siguiente prueba de la secuencia corresponde a los hosts en la LAN local.

Al hacer ping a los hosts remotos satisfactoriamente se verifica que tanto el host local (en este caso, el router) como el host remoto estén configurados correctamente. Esta prueba se realiza al hacer ping a cada host en forma individual en la LAN.

Si un host responde con el mensaje "Destination Unreachable" (destino inalcanzable), observe qué dirección no fue satisfactoria y continúe haciendo ping a los otros hosts de la LAN.

2.5.4 Traceroute

El objetivo principal de esta herramienta, es conocer el camino que recorre un paquete a través de nuestra red.

Este comando de red permite saber por dónde pasa el paquete (máquinas, switch, router) y comprobar que nuestra red funciona correctamente. Si detecta cualquier problema, nos va a permitir tener una idea aproximada acerca de donde se encuentra el fallo.

2.6 Herramientas

Para realizar el cableado estructurado se utilizaron diferentes tipos de herramientas, las cuales fueron fundamentales y necesarias para llevar a cabo el proyecto. Cabe destacar que el material fue proporcionado por el departamento de Tecnologías de la información y Comunicación. Sin más preámbulo se presentarán más adelante

2.6.1 Cable UTP

Este tipo de categoría está definida en el estándar EIA/TIA 568B con el cual se puede implementar para la ejecución CDDI y permite transmitir datos a velocidades de hasta 100 Mbps a frecuencias de hasta 100 MHZ [7].

Se utilizó el cable UTP categoría 5e por su velocidad de transmisión de datos, facilidad de rendimiento y su bajo costo a comparación de fibra óptica.

Ventajas:

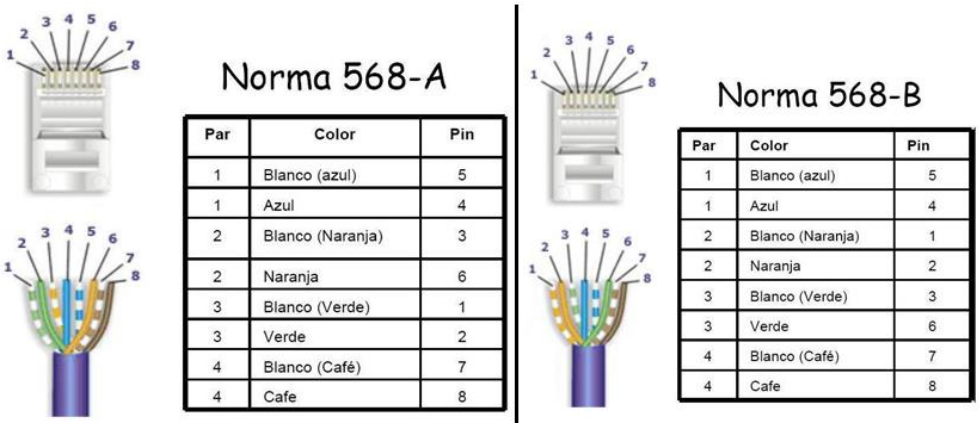
- Bajo costo en su contratación.
- Alto número de estaciones de trabajo por segmento.
- Facilidad para el rendimiento y la solución de problemas.
- Puede estar previamente cableado en un lugar o en cualquier parte.

Desventajas:

- Altas tasas de error a altas velocidades.
- Ancho de banda limitado.
- Baja inmunidad al ruido.
- Alto costo de los equipos.
- Distancia limitada (100 metros por segmento).

2.6.2 Conectores RJ45

Los hilos deben de estar sin trenzar solo en el trecho necesario para unir el conector.



Norma 568-A

Par	Color	Pin
1	Blanco (azul)	5
1	Azul	4
2	Blanco (Naranja)	3
2	Naranja	6
3	Blanco (Verde)	1
3	Verde	2
4	Blanco (Café)	7
4	Cafe	8

Norma 568-B

Par	Color	Pin
1	Blanco (azul)	5
1	Azul	4
2	Blanco (Naranja)	1
2	Naranja	2
3	Blanco (Verde)	3
3	Verde	6
4	Blanco (Café)	7
4	Cafe	8

Figura 5. Normativas 568-A y 568-B

La figura 5 muestra las normativas 568-A y 568-B, las cuales se utilizan para realizar el cable *UTP*. Cada una de las normativas tiene diferente orden de colocación de los hilos.

Tipos de cables UTP

- Cable directo de Ethernet
  Estándar: Ambos extremos son T568A o T5**68**B
  Aplicación: Conexión de un host de red a un dispositivo de red como un switch o hub.
- Cruzado Ethernet
  Estándar: Un extremo T568A, otro extremo T568B
  Aplicación: Conecta dos hosts de red
  Conecta dos dispositivos de red intermediarios (un switch a un switch, o un router a un router).
- De consola
  Estándar: Propietario de Cisco
  Aplicación: Conecta el puerto serial de una estación de trabajo al puerto de consola de un router utilizando un adaptador.

Ventajas:

- Velocidad de 10 / 100 Mbps
- Usa estándar de red: 100BASE-TX (IEEE 802.3u)
- Son económicos.

Desventajas:

No son reutilizables una vez que son ponchados.

2.6.3 Ponchadoras

Es una herramienta versátil y útil, por las múltiples funciones que ofrece. Esta permite ponchar conectores 8P8C/RJ45; además de cortar y pelar cables para red de tipo LAN.

Se utilizaron porque son las más recomendables para ponchar cables sin afectar su estado físico.

Características

- Tiene navajas para pelar cable
- Máximo control y precisión gracias a su alta calidad
- Modulo para plug Sellador (ponchador)

Ventajas:

- Poncha conectores modulares de 6 y 8 posiciones (RJ11, RJ12 y RJ45).
- Herramienta necesaria para la instalación de redes.
- Fácil de usar en Jack RJ45

Desventajas:

Se debe que aplicar fuerza para ponchar el cable.

2.6.4 Tester

El tester de redes LAN cubre el ámbito de la instalación y control de redes. Este tester de redes LAN puede ser utilizado en modo rápido, por ello es ideal para profesionales de servicio técnico y para administradores de red. Este tester de redes LAN facilita la determinación Visión general de los productos de direcciones IP, la identificación de la polaridad, la medición a doble carga, la detección de un cable concreto [18].

Este tester consta de dos partes, la primera está equipada con 16F84A, es la encargada de generar una serie de señales que se introducirán por uno de los extremos del cable, una segunda con una serie de LEDS, se conectan en el otro extremo para recibir los pulsos generados por la primera e indicarnos el estero del cable.

Las fallas que destacadas en este instrumento incluyen conectores conectados a pines incorrectos, conductores cortados o cortocircuitos en el interior del cable.

Se utilizó este dispositivo por su facilidad de uso, además permite conocer el estado real de los cables UTP, para así asegurar el funcionamiento correcto que debe desempeñar. Cabe destacar que es uso profesional de servicio técnico a comparación de otros dispositivos.

Ventajas:

- Permite probar cables UTP 8P8C (8 hilos), 6P6C(6 hilos), cables telefonicos (4 hilos) diagnosticando y probando cada hilo.
- Fácil de utilizar
- Identifica conectores mal ponchados y dañados.

Desventajas:

- Son de alto costo.

2.6.5 Putty

Es un cliente Ssh, Telnet, rlogin, y TCP raw con licencia libre. Disponible para Microsoft Windows, Unix, y se está desarrollando la versión para Mac OS clásico y Mac OS X. Otros desarrolladores han contribuido con versiones no oficiales para otras plataformas, tales como Symbian para teléfonos móviles. Es software beta escrito y mantenido principalmente por Simon Tatham, Open Source y licenciado bajo la Licencia MIT [19].

Se utilizó este programa debido a que la empresa PEMEX lo utiliza para conectar servidores remotamente y poder configurar mediante consola.

Características

- El almacenamiento de hosts y preferencias para uso posterior.
- Control sobre la clave de cifrado SSH y la versión de protocolo.
- Control sobre el redireccionamiento de puertos con SSH, incluyendo manejo empotrado de reenvío X11.
- Completos emuladores de terminal xterm, VT102, y ECMA-48.
- Soporte IPv6.
- Soporte 3DES, AES, RC4, Blowfish, DES.
- Soporte de autenticación de Criptografía asimétrica.
- Soporte para conexiones de puerto serie local.

Ventajas

- Funcionalidad como la reconexión automática al volver del modo suspendido, reconexión cuando hay fallos o el guardado de datos en ficheros para hacerlo portable en discos USB.
- Es de código abierto y se puede descargar gratuitamente.
- Respuestas de puertos
- Soporte Ipv6
- Soporte SCP y SFTP

Desventajas:

- Actualización de controladores de puertos Polific COM

2.6.6 Visio

Microsoft Visio Express es uno de los nuevos productos o programas que ofrece Microsoft Office, el cual tiene como función principal la creación de Diagramas tanto empresariales como técnicos, los cuales permitirán transmitir, visualizar y comunicar de una manera más clara, concisa y eficaz todo tipo de información organizacional que esté representada en diagramas. Es un software de dibujo vectorial para Microsoft Windows [20].

Nos permiten realizar diagramas de oficinas, diagramas de bases de datos, diagramas de flujo de programas, UML, y más, que permiten iniciar al usuario en los lenguajes de programación.

Cabe destacar que se utilizó este programa porque es uso profesional a comparación de otros programas no oficiales.

Ventajas

- Amplia galería de imágenes. Visio contiene una extensa galería de imágenes y símbolos para que puedas crear y completar tus diagramas y mapas. Estos iconos ayudan a mejorar la apariencia de tus documentos y proporcionan una información extra, muy útil para comprender mejor el diseño. Desde formas geométricas, dibujos de mobiliario o iconos muy esquemáticos, pero fácilmente reconocibles, son algunos de los motivos que encontrarás en su galería.
- Fácil de personalizar. Una de las grandes ventajas que ofrece siempre el grupo Microsoft, es que posee diferentes plantillas que puedes personalizar con los colores corporativos y el logo de la empresa. Además, estas plantillas, que tienen como fin simplificar el trabajo, puedes modificarlas y adaptarlas a tus necesidades, con tan solo un clic. Cambiar el estilo, insertar nuevas imágenes, modificar el tipo de letra, son algunas de las opciones que te permite esta herramienta para cambiar la apariencia de tu documento.
- Facilita el trabajo en equipo. La nueva versión de Visio, ofrece mejoras que facilitan el trabajo en equipo. Ahora puedes adjuntar comentarios a los documentos, para hacer seguimientos, ofrecer propuestas de mejora, realizar recordatorios o avisos o para debatir sobre algún aspecto. Además, también puedes gestionar estos comentarios, comentarlos, eliminarlos o vincularlos con otros datos para enriquecer el trabajo en grupo.

- Tres versiones para elegir. Puedes elegir entre tres versiones diferentes, Visio Estándar, Visio Profesional o Visio Pro para office 365, según tus necesidades. La primera es una versión más básica y económica pero que cuenta con los recursos y funcionalidades imprescindibles para diseñar cronogramas, mapas de flujo de trabajo y otras herramientas.
- Compatible con otras herramientas. También puedes incorporar tu hoja de Visio, con el diagrama de flujo, por ejemplo, en tus informes elaborados con Word. Y es que Visio 2013 es compatible con todas las aplicaciones de office, como Word, Excel o Microsoft Project.

Desventajas

- No se puede medir ni la productividad de las maquinas ni de las persona. Esto supone una gran desventaja para el programa, ya que es un item importante para el control de proyectos.
- Muy caro comparado con las alternativas que presenta la competencia.
- La aplicación para trabajar en Internet se compra aparte
- No se trata de un programa multiplataforma (los que funcionan tanto en LINUX como WINDOWS), de manera que tiene restringido su uso a ciertos usuarios.
- No cuenta tampoco con las herramientas básicas para la planeación de la mayoría de proyectos.
- El 80% de los usuarios de MS Project acaba usando tan sólo el 20% de sus numerosas opciones, de manera que acaba siendo su aplicación poco eficiente.

2.6.7 CMD

Es un programa (cmd.exe) de Microsoft Windows equivalente al programa command.com, intérprete de comandos de MS-DOS (MicroSoft Disk Operating System). Para su ejecución es necesario la inserción de comandos [21].

Son comandos muy útiles que nos van a permitir acceder a información básica de nuestro equipo para poder por ejemplo, comunicarnos vía remota o con otros equipos de la red.

Se utilizó porque es bastante flexible, viene instalado de manera predeterminada en los dispositivos finales (computadoras) a comparación de otros programas.

Ventajas:

- Permite conocer la configuración básica de la red (IP, la máscara de red, puerta de enlace).
- Permite verificar la conectividad de dispositivos que se encuentran en la red.

- Permite visualizar el camino que siguen los paquetes de red desde un equipo a otro y así determinar si existe algún problema en algún momento entre ambos.

Desventajas:

- Solo se puede ejecutar una tarea al mismo tiempo.
- Es monousuario, por lo tanto solo un usuario a la vez lo puede utilizar.

3. Resultados

En este capítulo se dará a conocer los pasos necesarios para implementar el proyecto, añadiendo imágenes y descripciones de cada una de las etapas de la metodología antes planteada.

3.1 Analizar Requerimientos

Se identificó el fallo de envío de paquetes a los destinos finales en cada subred en el departamento de Telecomunicaciones y Tecnologías de información. Esto es contraproducente debido a que no existe comunicación en los dispositivos y esto provoca inestabilidades en la empresa PEMEX.

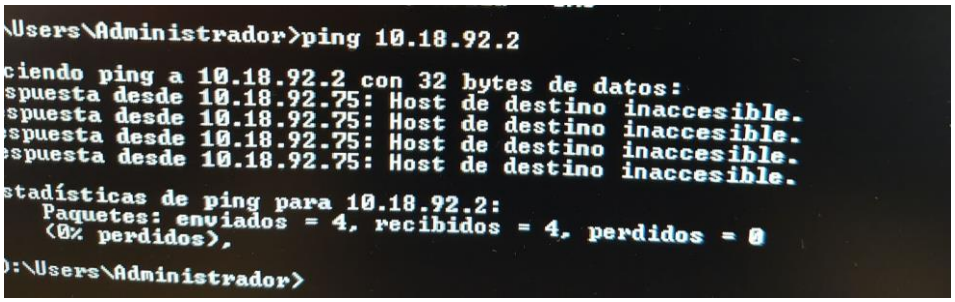


Figura 6. Destino inaccesible

La figura 6 muestra el fallo de envío de paquetes, por lo tanto existe inestabilidad en la red, lo cual provoca que los dispositivos intermediarios (computadoras) no puedan comunicarse.

Se encontró un cableado estructurado mal diseñado y empleado que no cumple con las normativa ANSI/TIA/EIA-568-B. Se debe solucionar esta problemática inmediatamente debido que puede provocar daño en los cables y causar fallas en la comunicación de los dispositivos. Otro punto importante es la ausencia de la calidad y estabilidad en el cableado, lo cual puede afectar la integridad de la empresa.

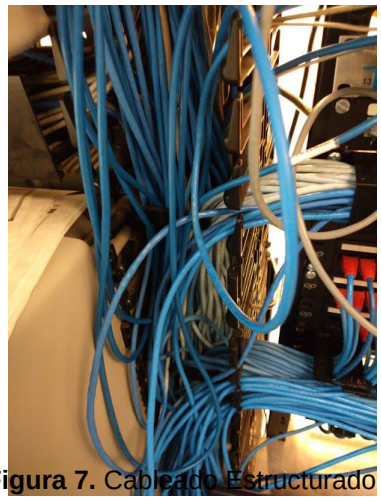


Figura 7. Cableado Estructurado

La figura 7 muestra la mala implementación del cableado. Cabe destacar que es necesario cumplir con la normativa *ANSI/TIA/EIA-568-B* para realizar a cabo un cableado estructurado.

Figura 8. Desorganización de cables

La figura 8 muestra la conexión desorganizada de los cables *UTP* a los Switch, además no utilizaron cinchos para sostenerlos, lo cual es un problema para distinguir el puerto que corresponde cada cable *UTP* conectado al switch.

En la empresa PEMEX tenían un convenio con *CISCO* en los dispositivos intermediarios (Switch y Router) pero tuvieron la necesidad de implementar *VoIP* y contrataron *Huawei*. Por lo tanto tuvieron la necesidad de migrar toda la información en los nuevos dispositivos que proporcionaba la empresa *Huawei*.

Figura 9. Telefonía VoIP Huawei

La figura 9 muestra un teléfono *VoIP Huawei*. Se hizo un nuevo convenio con la empresa antes mencionada y la misma proporcionó telefonía *VoIP*. La empresa solicitó esto debido a que van a implementar estos dispositivos en cada departamento de la empresa PEMEX para que puedan comunicarse a través de la red.

Figura 10. Rack Huawei

De igual manera la empresa *Huawei* proporcionó *racks* como muestra la figura 10, para alojar switch y router. Con el objetivo de asegurar los dispositivos, incluyendo un candado, evitando el alcance de cualquier persona no autorizada. Otro factor importante es el aprovechamiento del espacio debido que se encontrarán todos los dispositivos intermediarios (switch y router) en un solo lugar.

3.2 Desarrollar diseño Físico

En el departamento de Telecomunicaciones y Tecnologías de la Información se realizó cableado estructurado cumpliendo con las normativa ANSI/TIA/EIA-568-B.

A continuación se mostrarán los pasos que fueron realizados:

Figura 11. Cable UPT categoría 5e

Como fue mencionado anteriormente, se utilizó cable *UTP* categoría 5e como se muestra en la figura 11, para realizar el cableado estructurado. Cabe mencionar que fue proporcionado por el almacén de herramientas interno del departamento.

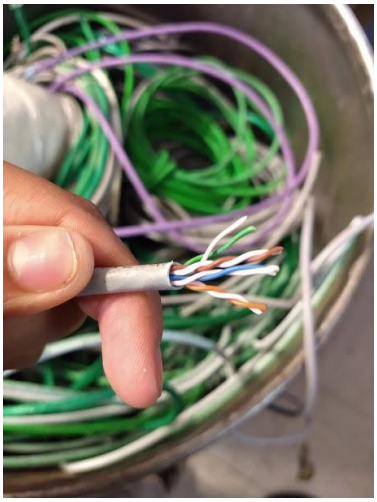


Figura 12. Pelar el cable UTP

Se peló el cable *UTP*, sin afectar los hilos del cable como se muestra en la figura 12, para después juntar los cables en su respectivo lugar de acuerdo a la normativa 568-B.

Figura 13. Conector RJ45

Se utilizó conectores RJ45 como se muestra en la figura 13, con su respectivo protector, estos conectores son utilizados para sostener los hilos trenzados en su respectivo lugar.

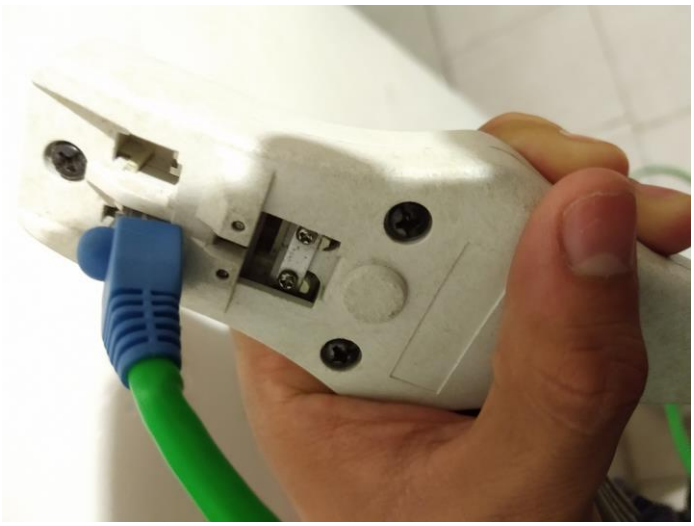


Figura 14. Ponchado de cable UTP

La figura 14 muestra el ponchado de los cables *UTP*, se ingresó el conector RJ45 y se presionó fuerte para que el ponchado fuera correcto.

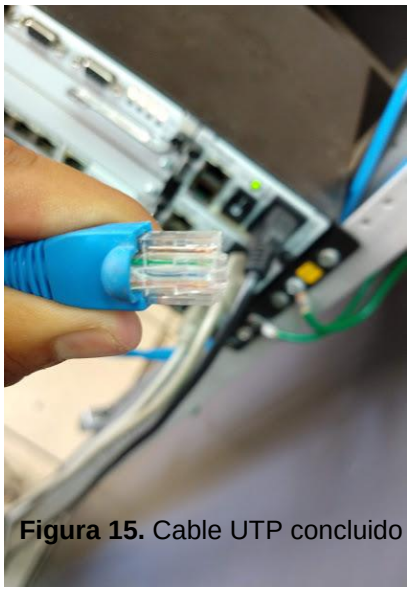


Figura 15. Cable UTP concluido

La figura 15 representa el cable *UTP* categoría 5e finalizado.

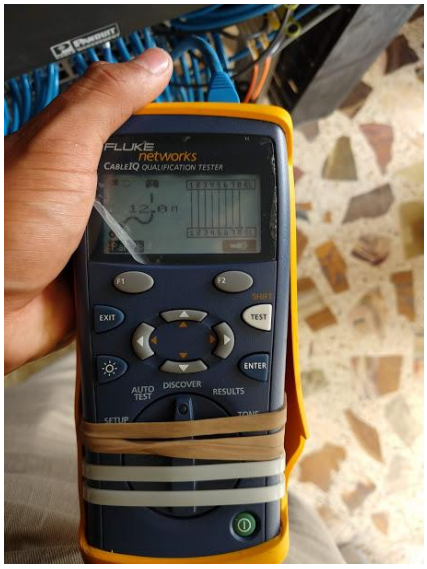


Figura 16. Probar Cable UTP con Tester

El siguiente paso fue probar el cabe *UTP* con un *tester,* como se muestra en la figura 16. Cabe destacar que fue importante verificar las líneas que muestra la imagen, las cuales deben tocar ambos puntos para estar seguros de su correcto funcionamiento y hacer uso del cable.

Figura 17. Conexión de cables UTP

Se probaron todos los cables que fueron realizados con el *tester* para poder hacer uso de ellos y conectarlos directamente con el switch y router. En la figura 17 se puede apreciar un *rack* que almacena 4 switch y 2 router, los cuales fueron conectados por el cable *UTP*.

Figura 18. Fijar Cables UTP

Se juntaron todos los cables *UTP* con cinchos como se puede apreciar en la figura 18. Es importante hacerlo para fijar los cables y no permitirles estar sueltos y puedan sufrir daños a futuro por cualquier circunstancia.

Figura 19. Uso de Pulsera antiestática

La figura 19 representa el uso de una pulsera antiestática para dar inicio a la conexión de dispositivos físicos, el cual consiste la primera capa del modelo *OSI* (capa física). Esta pulsera consiste en una cinta con un velcro para fijarla en la muñeca conectada a un cable de toma de tierra que permite descargar cualquier acumulación de electricidad estática en el cuerpo de un operario de equipos sensibles.

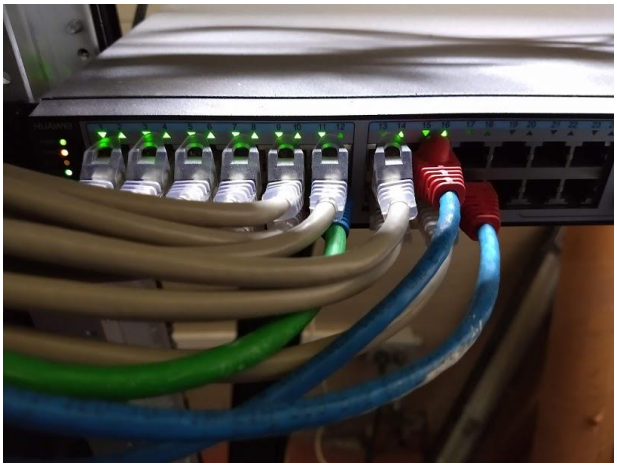


Figura 20. Conectar Cables UTP al Switch

Teniendo todo el cableado, el paso siguiente fue conectar el cable *UTP* al Switch en los puertos disponibles, como se muestra en la figura 20. Para después configurar el puerto de acuerdo al dispositivo final conectado (computadora, impresora, telefonía *VoIP*).

Figura 21. Cable SFTP

Debido a que se ocuparon todos los puertos del Switch y se requirió conectar más computadoras en la misma subred, fue necesario añadir un nuevo switch, es por ello que se utilizó en cable *SFTP* como se muestra en la figura 21.

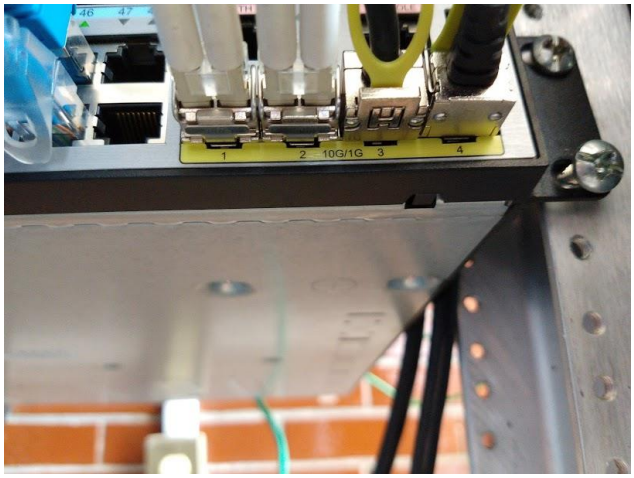


Figura 22. Conexión de cable SFTP a switch

La figura 22 muestra la conexión del cable *SFTP* al puerto del switch para poder ampliar el número de puertos. Su uso es fundamental cuando el número de puertos se agota en un switch y se desea ampliar la red, sólo tenemos que conectar este cable en el switch nuevo para poder seguir conectando dispositivos en el mismo. Cabe destacar que la numeración sigue incrementando, no inicia en uno, esto es de vital importancia ya que nos facilita en la configuración de los nuevos puertos evitando modificar los puertos iniciales ya conectados y funcionando.

Figura 23. Conexión de Switch a Router

La figura 23 muestra la conexión de switch a router en el departamento de Telecomunicaciones y Tecnologías de la información. Cabe mencionar que también se hicieron conexiones en los departamentos internos de PEMEX.

Figura 24. Conexión de Switch a Patch

La figura 24 muestra la conexión de Switch a *Patch Panel*, con el objetivo de interconectar la red, ya que permite el tráfico de datos.

Figura 25. Conexión de Router a Router

La figura 25 muestra la interconexión de 2 routers con los cables seriales, para permitir el acceso a *WAN* (red de área amplia), considerando el *DCE* como proveedor de servicios el cuál se configurará en la siguiente etapa y el cable *DTE* para recibir el servicio del *DCE.*

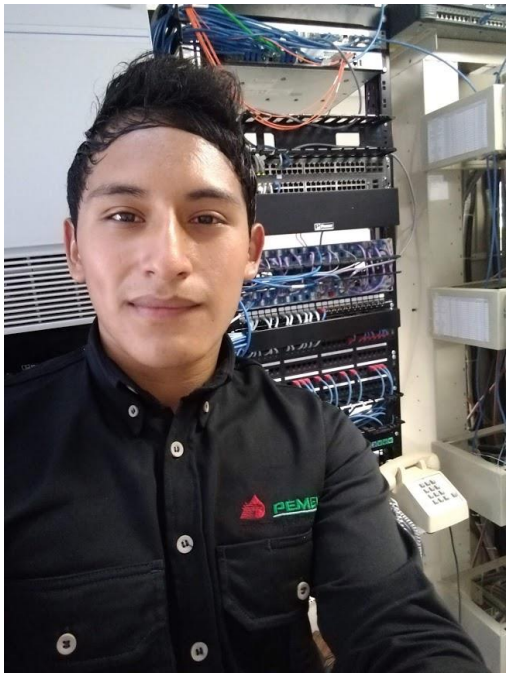


Figura 26. Racks

En la figura 26 se visualiza los *racks* del departamento de Instrumentos de PEMEX, el cual contiene 2 paneles de parcheo, 2 switch y un router.

Figura 27. Conexión de Cables UTP a Teléfono VoIP

La figura 27 muestra la conexión de los teléfonos *VoIP* a la red. Cabe mencionar que el cable *UTP* que está conectado en la computadora, se conectó al teléfono *VoIP*, ya que este dispositivo nos facilita hacerlo.

Figura 28. Conexión de Cables UTP a Impresora

La figura 28 muestra la conexión de cable *UTP* a impresoras pertenecientes en el departamento para que puedan realizar impresiones.

Figura 29. Conexión de Cables UTP a rosetas

Se reutilizaron las rosetas donde van incluidos los conectores RJ45 hembra como se muestra en la figura 29, por lo tanto se conectaron los cables en las rosetas correspondientes.

Se identificaron los nodos que estaban conectados, colocando el número de puerto que estaba conectado: computadora, impresora, según sea el caso, en la roseta con el objetivo de tener un control y un registro. Para así, cuando se presente una problemática en cualquier dispositivo, podamos identificar inmediatamente a qué puerto está conectado y poder dar solución a ello.

Es por ello que se realizó un registro en Excel que contendrá el número del puerto de Switch, panel de parcheo, ubicación y dispositivo que esté conectado, ya sea teléfono, computadora o impresora.

Considerando que si no se realiza esto, cuando se presente cualquier situación tendríamos que estar desconectando cada puerto para verificar que computadora está conectada y esto es contraproducente debido a que dejaríamos sin acceso internet a los demás trabajadores de la empresa.

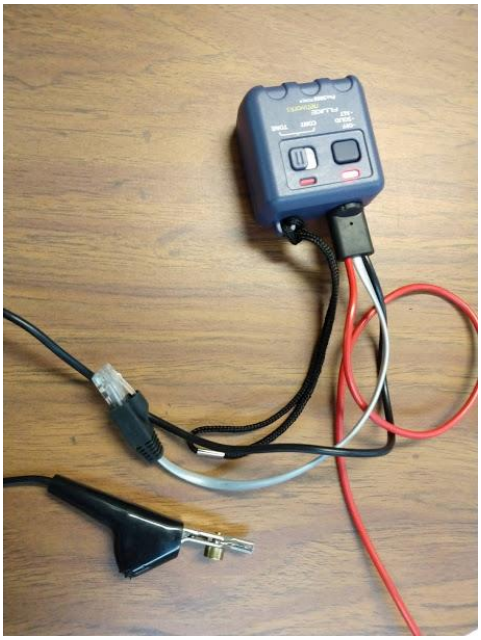


Figura 30. Herramienta Fluke Networks

Se utilizó una herramienta llamada *fluke networks* como se muestra en la figura 30, para identificar el origen de conexión de los cables *UTP.* Una excelente herramienta que nos facilita detectar la ubicación de cada cable.

Figura 31. Ubicación de Cable UTP

La figura 31 representa la conexión del cable *UTP* perteneciente de la herramienta *fluke networks*, y la roseta a localizar para después identificar la ubicación del cable *UTP* que está conectado en la misma.

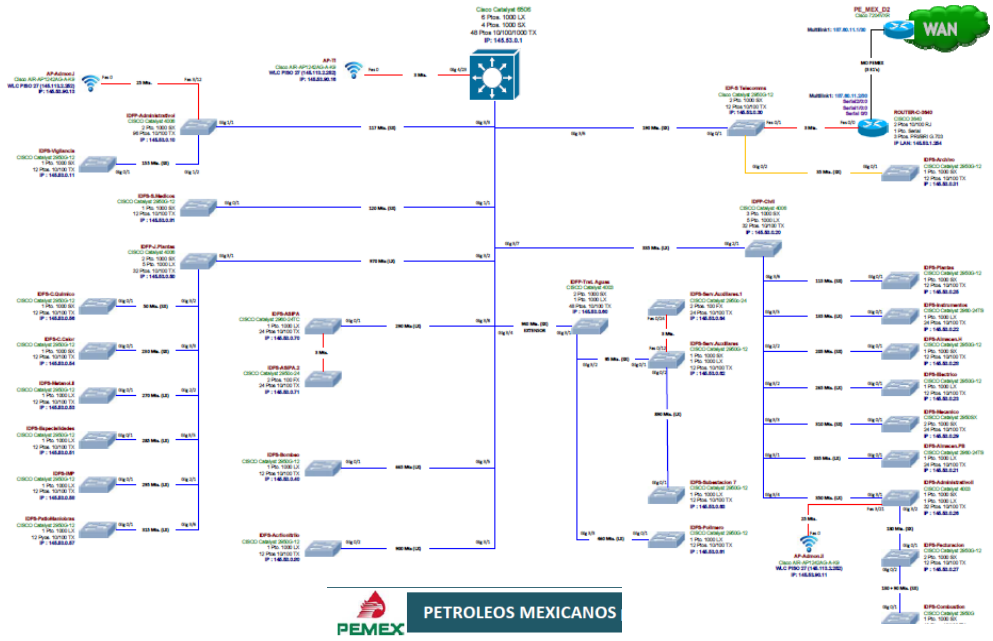
Figura 32. Localización de Cable UTP

La figura 32 representa la localización de los cables *UTP*. Con este dispositivo se identificó el cable que está conectado en la roseta, efectuando un ruido fuerte al localizar el cable correspondiente. Con ello podremos asegurarnos de la ubicación correcta.

Puerto Switch	PANEL	EXT/PC	UBICACIÓN
1	D12	35429	RECEPTORIA
2		35298	RECEPTORIA
3	D07	PC	RECEPTORIA
4	D08	35419	RECEPTORIA
5		35275	RECEPTORIA
6	D05	35459	ALMACENISTA "A"
7	D01	35806	AYUDANTE "B" ALMACENISTA
8	D02	35808	ALMACENISTA "B"
9	D18	35472	JEFE SECC. DESPACHO
10	D21	35753	DESPACHO
11	D19	35444	DESPACHO
12	D20	35389	DESPACHO
13	D22	35499	DESPACHO
14	D17	PC	INVENTARIOS
15			
16	D24	PC	INVENTARIOS
17	D16	35274	" "
18	D15	35383	OFICINA INVENTARIOS
19	D13	35270	OFICINA INVENTARIOS
20	D09	35431	JEFATURA ALMACEN
21	D23	PC	INVENTARIOS
22			
23			
24			
10(CISCO)	D11	IMPRESORA	PLANTA BAJA
14(CISCO)	D14	IMPRESORA	PLANTA ALTA

Figura 33. Tabla de Registros

Teniendo las ubicaciones de cada cable conectado en su respectiva roseta en cada departamento, se realizó un registro en Excel como se muestra en la figura 33, considerando: puerto de switch, panel de parcheo, extensión de telefonía o computadora que esté conectado y la ubicación del mismo.



.

Figura 34. Topología Física

Se realizó la topología física en la aplicación *Visio*, la figura 34 muestra la distribución de los dispositivos intermediarios que estarán en los departamentos de la empresa PEMEX.

Figura 35. Cable estructurado finalizado

La figura 35 muestra el terminado del cableado estructurado en el departamento de Telecomunicaciones y Tecnologías de la información, asegurando el funcionamiento de cada uno de los cables.

3.3 Desarrollar diseño Lógico

Para asignar el direccionamiento IP a los quipos que pertenecerán en los departamentos de la empresa PEMEX, fue necesario crear subredes para asignar los rangos de las mismas. Considerando que PEMEX es una macroempresa con diferentes departamentos se eligió la clase A por el número de *host* que permite esta clase.
Es por ello que es necesario realizar Subneteo, a continuación se darán a conocer los pasos efectuados:

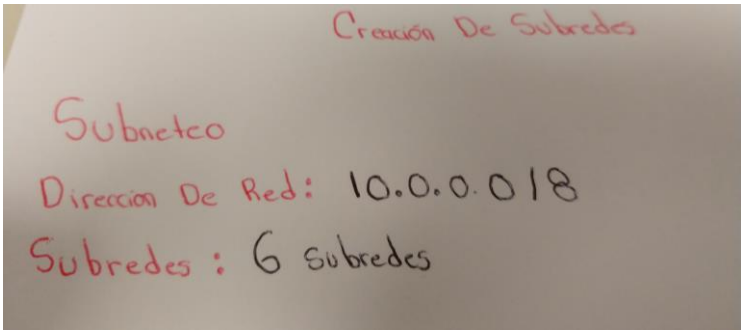


Figura 36. Datos iniciales

Para realizar el Subneteo, fue necesario que la empresa nos proporcionará el número de subredes a crear y la dirección de red, la cual es *10.0.0.0* con máscara de subred: *255.255.255.0,* como muestra la figura 36.

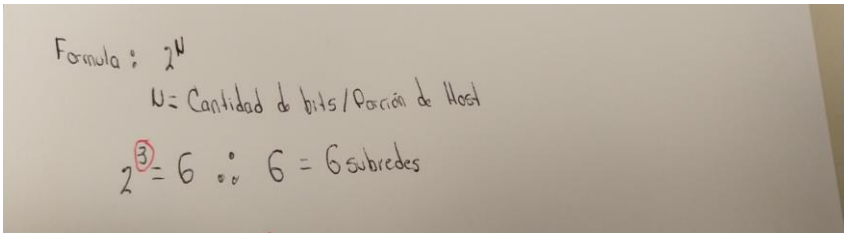


Figura 37. Uso de fórmula

La figura 37 muestra la sustitución de la fórmula 2^n, donde:
N=Cantidad de bits/ Porción de *Host*
El producto de la fórmula debe ser igual o mayor al número de redes a crear. Por lo tanto *6=6.*

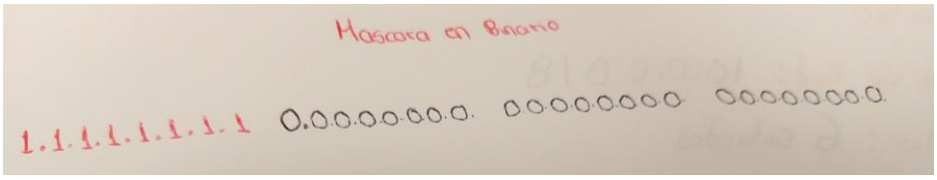


Figura 38. Máscara de red inicial en binario

La máscara de red es *255.255.255.0* como muestra la figura 38, pero fue necesario convertirla a binario para poder visualizar la porción de red y la porción de *host*. Cabe destacar que el número **1** pertenece a la porción de red y el número **0** pertenece a la porción de host.

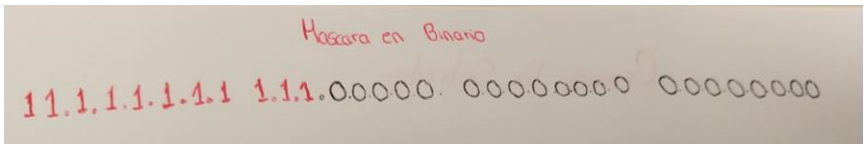


Figura 39. Máscara de red nueva en binario

Tomando la máscara en binario como muestra la figura 39, en la parte de red se agregó los *3 bits* que tomamos a la porción de *host* reemplazando por **1** y así obtenemos *255.224.0.0.*

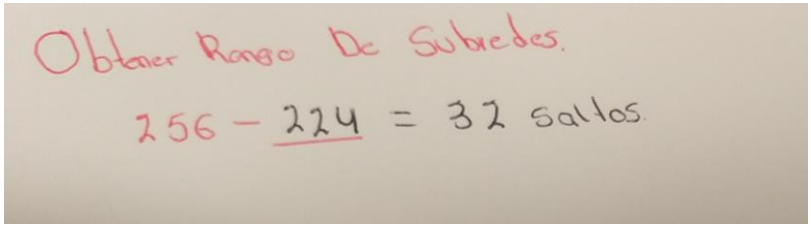


Figura 40. Obtener rango de subredes

Para obtener el número de rango (tambien conocido como salto), en cada subred se restó 256 al número de máscara de red adaptada, como muestra la figura 40.

Número de Subred	Desde	Hasta
1	10.0.0.0	10.31.255.255
2	10.32.0.0	10.63.255.255
3	10.64.0.0	10.95.255.255
4	10.96.0.0	10.127.255.255
5	10.128.0.0	10.159.255.255
6	10.160.0.0	10.191.255.255
7	10.192.0.0	10.223.255.255
8	10.224.0.0	10.255.255.255

Figura 41. Rango de subredes

La figura 41 muestra una tabla que contiene el número de subredes creadas con sus respectivos rangos de direcciones IP, las cuales serán asignadas en la siguiente etapa de la metodología de este proyecto. Cabe mencionar que la empresa requirió de 2 subredes más, por lo tanto se

agregaron en la tabla de direccionamiento, respetando el número de saltos de cada subred.

Cabe destacar que las direcciones que se utilizaron en los departamentos de PEMEX son privadas teniendo en cuenta lo siguiente:

Direcciones privadas

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

3.4 Implementar y configurar la red

En esta etapa se configuraron los dispositivos intermediarios (switch y router) y finales (computadoras) con el fin de permitir la comunicación entre ellos. Para poder configurar los Router y Switch de cada departamento de la empresa PEMEX, fue necesario realizar diferentes pasos, a continuación se darán a conocer:

Figura 42. Cable DB9 macho a RJ45

Se utilizó un adaptador de USB a serial (DB9) hembra como muestra la figura 42, para hacer la conexión con el cable serial DB9 a RJ45.

Figura 43. Adaptador cable USB a serial DB9

Se utilizó el cable Serial DB9 macho a RJ45 como muestra la figura 43, para conectarse al puerto de consola del switch y router.

Una vez realizado las conexiones físicas, fue necesario instalar el controlador del adaptador USB a serial. El disco de instalación fue proporcionado por la empresa PEMEX.

Figura 44. Instalación de controlador

La figura 44 muestra el disco que se utilizó para la instalación de actualización del adaptador en la computadora donde se realizarán las configuraciones del Switch y Router.

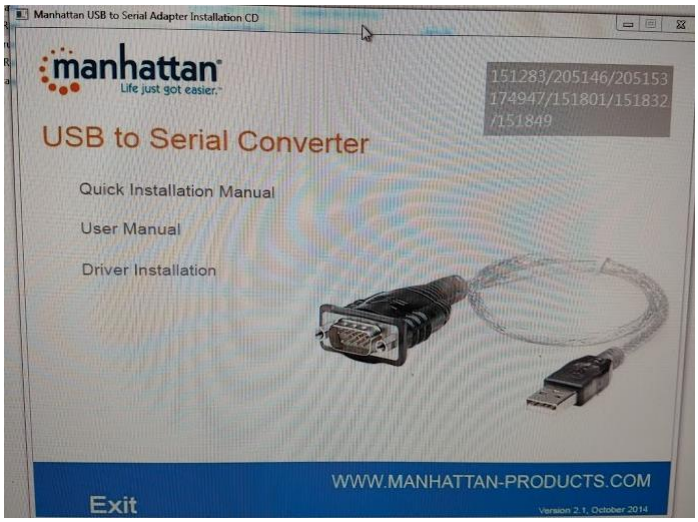


Figura 45 Proceso de instalación

La figura 45 muestra el proceso de instalación del controlador, se seleccionó la opción *driver installation.* Por consecuencia, se instaló el controlador del cable serial manhattan para poder hacer uso de él.

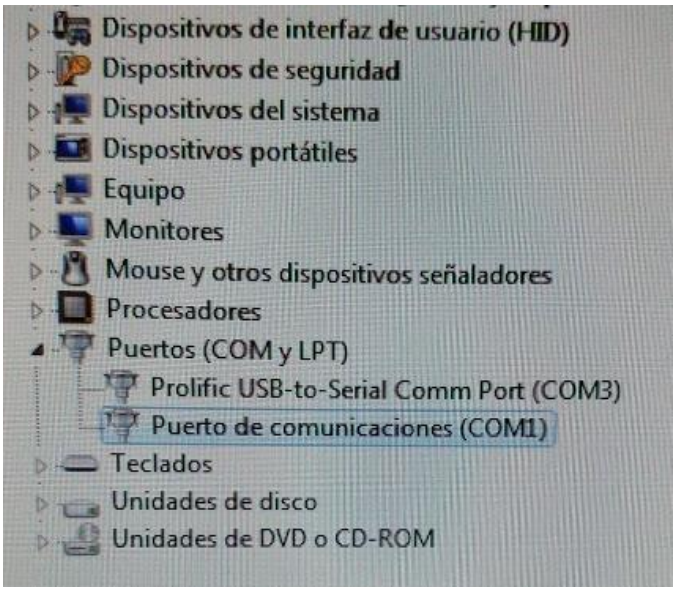


Figura 46. Verificación de Controlador

Se verificó la instalación del controlador en “administrador de dispositivos”, como muestra la figura 46. En la parte de Puertos (*COM y LPT*) se puede ver el puerto de comunicaciones listo para usarse.

Teniendo listo el controlador del adaptador, el siguiente paso fue la conexión del cable DB9 a RJ45 al Switch y Router, según sea el caso.

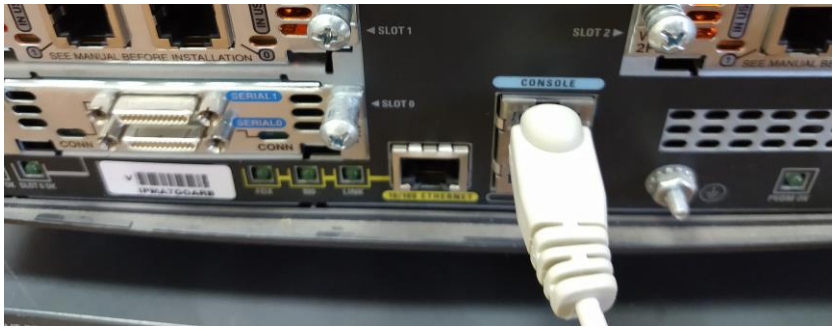


Figura 47. Conexión serial a puerto de Consola.

La figura 47 muestra la conexión del cable DB9 a RJ45 en el puerto de consola del router y Switch para poder tener acceso.

Para tener acceso virtualmente al Switch y Router se utilizó la aplicación Putty, el cual nos permite conectarnos de diferentes maneras.
A continuación se darán a conocer los pasos que fueron realizados:

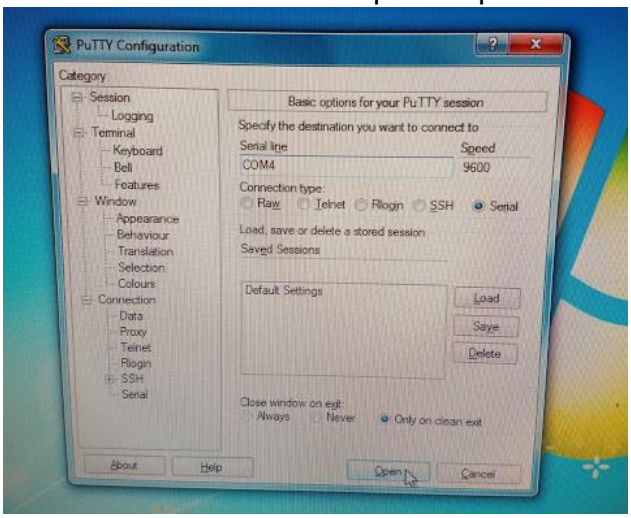


Figura 48. Conexión serial con Putty

La figura 48 muestra la conexión mediante el cable serial, por lo tanto se seleccionó la opción “serial” y se dio clic en *open.*

Teniendo acceso a los dispositivos, se realizaron las configuraciones básicas, asignando nombre, contraseñas, encriptación en cada uno de los mismos.

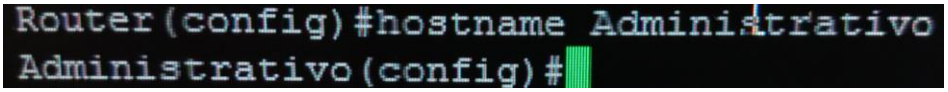


Figura 49. Asignación de nombre

En cada Switch y router se asignó un nombre diferente para poder identificarlos. Se realizó el comando *hostname* para poder asignar el nombre como muestra la figura 49.

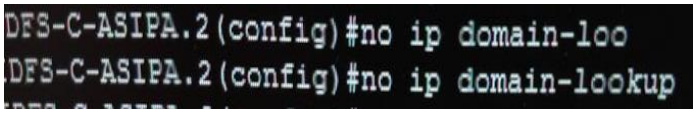


Figura 50. Desactivación de errores de comandos

La figura 50 muestra el uso del comando *no ip domain-lookup* para la desactivación de traducción de nombres a dirección del dispositivo en el Router y Switch. Esto es de gran ayuda debido a que cualquier error de digitación en el dispositivo, simplemente enviará el mensaje indicando que el comando es desconocido o que no ha podido localizar el nombre de host, ahorrando tiempo de espera.

En cada subred se requiere seguridad y autenticación, debido a que deben de existir permisos de restricción en los dispositivos intermediarios (switch y router). Es por ello que para cada dispositivo se crearon diferentes contraseñas. A continuación se darán a conocer los pasos efectuados cabe destacar que no se mostrara la contraseña creada debido a la autenticación de la empresa PEMEX.

Figura 51. Configuración de contraseña

La figura 51 muestra el uso del comando *enable secret* para asignarle una contraseña al intentar entrar al modo privilegiado de los Switch y Router.

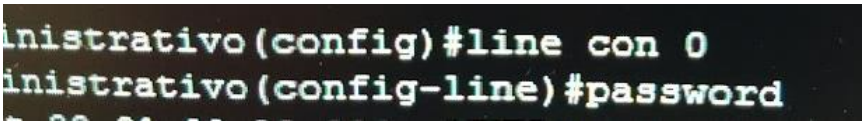


Figura 52. Asignación de contraseña en línea específica

La figura 52 muestra el uso del comando *line console 0,* ya que identifica la línea específica para la configuración y se asignó una contraseña.

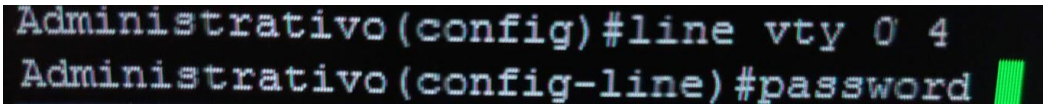


Figura 53. Configuración de línea VTY en Router

En la figura 53 muestra el uso del comando *line vty 0 4* para la configuración de línea VTY en el router. Se configuró la contraseña del *VTY* 0 4. Esta contraseña es para que cuando se deseé entrar al router remotamente, pida una contraseña. Sí la línea del *VTY* no tiene una contraseña configurada no es posible tener acceso al router remotamente (*telnet* o *ssh*).

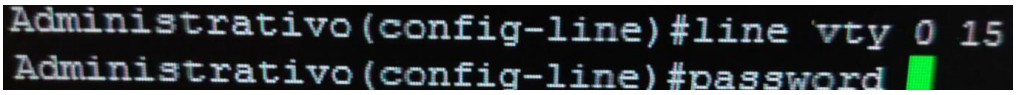


Figura 54. Configuración de línea VTY en Switch

Se configuró la contraseña vty 0 15 en el switch para poder acceder remotamente, se utilizó el comando *line vty 0 15* como muestra la figura 54.

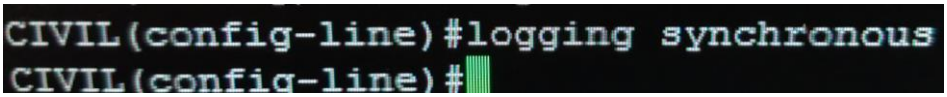


Figura 55. Desactivación de comandos en

Se utilizó el comando *logging synchronous* como muestra la figura 55, para evitar que los mensajes inesperados que aparecen en pantalla, se desplacen los comandos que se están escribiendo en el momento.

Figura 56. Encriptación de contraseñas.

Fue necesario encriptar las contraseñas realizadas en el Switch y router, para evitar que se muestre las contraseñas al intentar visualizarlas, para ello se utilizó el comando *service password-encryption* como muestra la figura 56.

Figura 57. Verificación de contraseña encriptada.

Al efectuar el comando *show running-config* se puede visualizar las configuraciones realizadas, como las contraseñas creadas. La figura 57 muestra la contraseña encriptada, la cual no puede visualizarse. Esto es de vital importancia, ya que proporciona seguridad a los dispositivos.

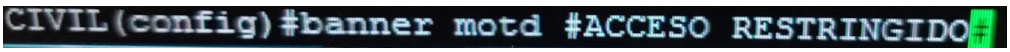


Figura 58. Creación de mensaje.

Es importante usar el comando *banner motd* como muestra la figura 58, para poder escribir un anuncio, el cual se mostrará cada vez que se ingrese a un Switch y router.

Figura 59. Mensaje de inicio en Switch y Router

Cada vez que se intente entrar a configurar al Switch y Router, se mostrará el mensaje que aparece en la figura 59. Cabe mencionar que no se podrá acceder a modo privilegiado sin ingresar la contraseña correcta, con ello los dispositivos intermediarios estarán protegidos de personas intrusas que quieran alterar las confguraciones creadas en cada uno de ellos.

Despues de la configuración básica de los dispositivos intermediarios (Switch y Router), fue necesario crear *VLAN* (Red de Área Local Virtual) en cada Switch, debido a que son una tecnología a nivel de capa 2 del modelo *OSI,* la cual ayuda a optimizar, proteger y segmentar el tráfico de la red.

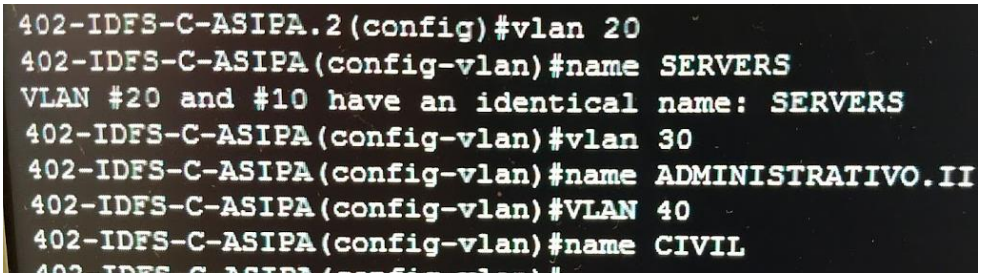
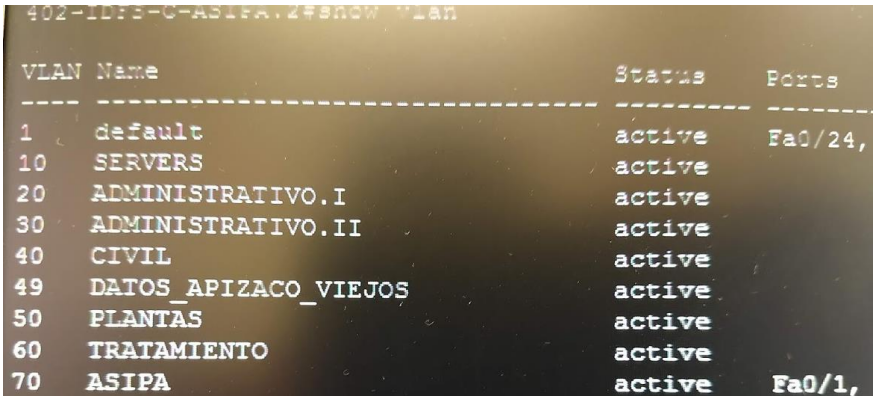


Figura 60. Creación de VLAN en el Switch

Se crearon diferentes *VLAN* con su respectivo nombre para poder identificarlas, para así poder administrarlas y hacer uso de ellas. Con el comando *VLAN* como muestra la figura 60, fue posible crearla, seguido del ID, después con el comando *name* podemos asignarle un nombre a cada *VLAN* creada.



```
402-IDFs-C-ASIPA.24#show vlan

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------
1    default                             active    Fa0/24,
10   SERVERS                             active
20   ADMINISTRATIVO.I                    active
30   ADMINISTRATIVO.II                   active
40   CIVIL                               active
49   DATOS_APIZACO_VIEJOS                active
50   PLANTAS                             active
60   TRATAMIENTO                         active
70   ASIPA                               active    Fa0/1,
```

Figura 61. VLAN creadas

La figura 61 muestra todas las *VLAN* creadas con su ID y nombre correspondiente, así como el puerto asignado utilizando el comando *show vlan*.

Sin embargo, fue necesario crear más *VLAN* en los Switch debido a los requerimientos de la empresa PEMEX. Cada *VLAN* se creó con diferente identificador y diferente nombre.
A continuación se mostrará todas las *VLAN* creadas en los Switch.

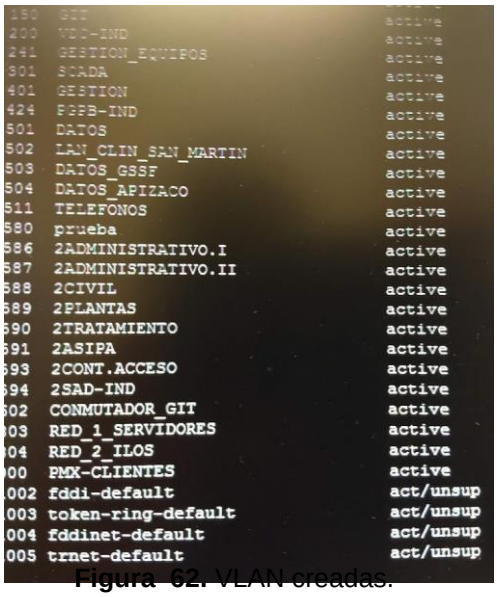


Figura 62. VLAN creadas.

Como se puede ver en la figura 62, se crearon diferentes *VLAN* con diferente identificador y nombre, cabe destacar que en el Switch de la otra subred tambien fue necesario crear las mismas *VLAN*, para permitir los enlaces troncales y la comunicación de cada una de ellas.

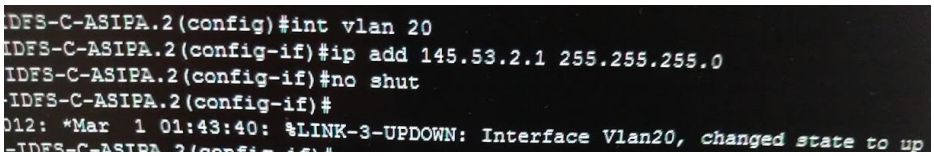


Figura 63. Asignación de direccionamiento IP en VLAN

La figura 63 muestra la asignación de direccionamiento IP en VLAN correspondiente. En cada *Vlan* se asignó una direccion *IP* con su submascara para administrarla remotamente. Para asignarle una dirección *IP* a la *VLAN* correspondiente se usó el comando *ip add* seguido de la *IP* y submascara de red, y despues levantarla administrativamente con el comando *no shutdown.*

Además se asignaron las *VLAN* correspondientes en los puertos de los switch, para permitir la comunicación y envío de información. Algunos puertos fueron configurados en modo troncales para permitir el tráfico de diferentes *VLAN* a través de ellos, y otros en modo de acceso para asignar las *VLAN* en las interfaces correspondientes del Switch. Además la configuración de VLAN nativa, debido a que las tramas no se modifican cuando se envían por medio del enlace troncal.

A continuación se mostrará los pasos que fueron realizados:

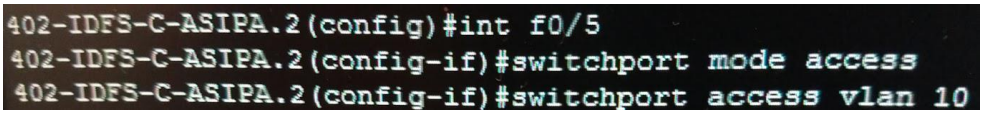


Figura 64. Asignación de VLAN en puertos de Switch

La figura 64 muestra la asignación de VLAN en los puertos de switch. Se asignó la *VLAN* 10 en la interfaz f0/5 del switch en modo de acceso, para ello se accedió a la interfaz antes mencionada y se utilizó el comando *switchport mode acccess* y *switchport access vlan 10.*

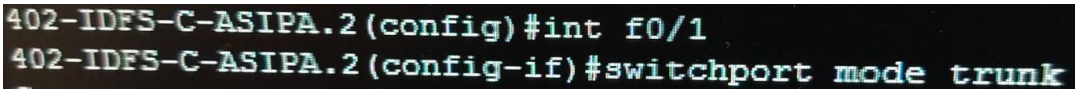


Figura 65. Configuración modo troncal.

En la figura 65 muestra la configuración de la interfaz f0/1 en modo troncal para permitir el envío de varias *VLAN* creadas en las subredes. Para ello se asignó a la interfaz antes mencionada y se utilizó el comando *switchport mode trunk.*

.

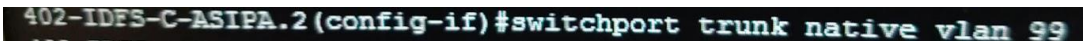


Figura 66. Configuración de VLAN nativa.

La figura 66 muestra la configuracion de VLAN nativa. Cabe mencionar que la *VLAN* nativa predeterminada es la *VLAN* 1. Al configurar un puerto de enlace troncal 802.1Q, se asignó el valor del ID de la *VLAN* nativa al ID de la *VLAN* de puerto predeterminado (*PVID*). Sin embargo se configuró la *VLAN* como *VLAN* nativa, por lo tanto el tráfico sin etiquetar que ingresa o sale del puerto 802.1Q se envía a la *VLAN* 99. Se utilizó el comando *switchport trunk native vlan 99.*

Los routers tienen una cantidad limitada de interfaces físicas para conectarse a diferentes VLAN. A medida que aumenta la cantidad de VLAN en una red, el hecho de tener una interfaz física del router por VLAN agota rápidamente la capacidad de interfaces físicas de un router.

Una alternativa en redes más grandes es utilizar subinterfaces y enlaces troncales de VLAN. Los enlaces troncales de VLAN permiten que una única interfaz física del router enrute el tráfico de varias VLAN.

Esta técnica se denomina *router-on-a-stick* y utiliza subinterfaces virtuales en el router para superar las limitaciones de interfaces físicas del hardware. Cabe mencionar que se creó una subinterfaz diferente por cada *VLAN* creada en el Switch.

A continuación se mostrará la configuracion de subinterfaces en el router:

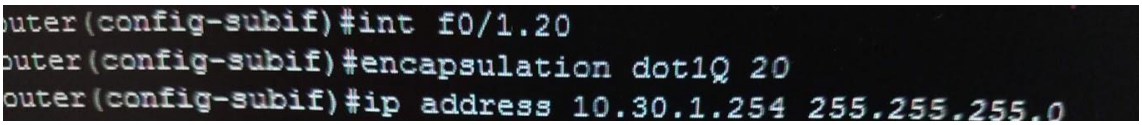


Figura 67. Creación de subinterfaces en el router

La figurab 67 muestra la creación de subinterfaces en el router. Las subinterfaces son interfaces virtuales basadas en software asignadas a interfaces físicas. Cada subinterfaz se configura de forma independiente con su propia dirección *IP* y máscara de subred. Esto permite que una única interfaz física forme parte de varias redes lógicas de manera simultánea. Para ello se accedio a la interfaz añadiendo un punto, el cual llevará el ID de la *VLAN* correspondiente, ademas se utilizó el comando *encapsulation dot1q* [Id de *vlan]* y se le asignó una dirección *IP* y submáscara de red.

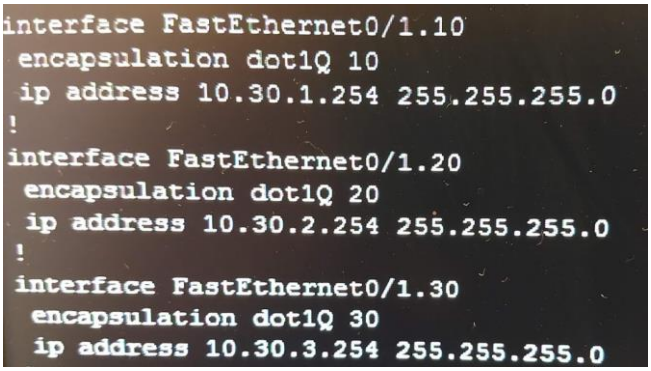


Figura 68. Subinterfaces creadas en el router

La figura 68 muestra algunas de las subinterfaces creadas en el router, se utilizó el comando *show running-config para* visualizar la configuración realizada.
A medida que aumenta el número de switches en una red en la empresa PEMEX, la administración general requerida para administrar las *VLAN* y los enlaces troncales en una red se convierte en un desafío.
Es por ello que se configuró el protocolo de troncal *VLAN (VTP),* el cual permite la administración de las *VLAN* en un switch configurado como servidor *VTP*.
El servidor VTP distribuye y sincroniza la información de la *VLAN* en los enlaces troncales a los switches habilitados por el *VTP* en toda la red conmutada. Esto minimiza los problemas causados por las configuraciones incorrectas y las inconsistencias de configuración. *VTP* opera en 3 modos distintos: Servidor, Cliente y transparente

A continuación se mostrará la configuracion del protocolo *VTP* en sus 3 modos distintos:

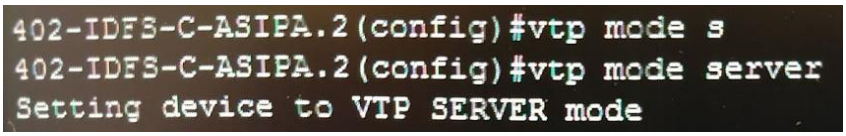


Figura 69. Configuración VTP modo Servidor

La figura 69 muestra la configuración *vtp* en modo servidor. Se utilizó el comando *vtp mode server,* debido a que se pueden crear, eliminar o modificar *VLANs.* Su cometido es anunciar su configuración al resto de switches del mismo dominio *VTP* y sincronizar dicha configuración con la de otros servidores, basándose en los mensajes recibidos a través de sus enlaces trunk.

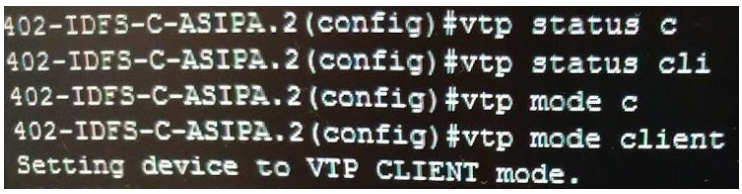


Figura 70. Configuración VTP modo cliente

La figura 70 muestra la configuración *vtp* en modo cliente. Se utilizó el comando *vtp mode client,* debido a que no se pueden crear, eliminar o modificar *VLANs*, tan sólo sincronizar esta información basándose en los mensajes *VTP* recibidos de servidores en el propio dominio. Un cliente *VTP* sólo guarda la información de la *VLAN* para el dominio completo

mientras el switch está activado. Un reinicio del switch borra la información de la *VLAN*.

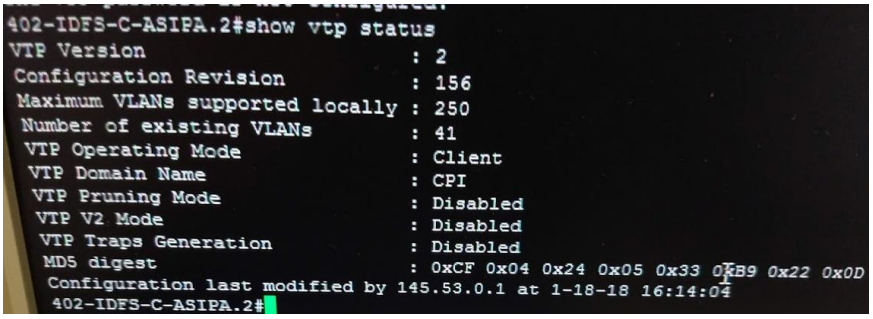


Figura 71. Configuración VTP modo transparente

De manera predeterminada se encuentra en modo transparente, por lo tanto se ingresó el comando *show vtp status* como muestra la figura 71, para monitorear el estado de operación que se esta manejando. Se dejó en modo transparente porque de este modo tampoco se pueden crear, eliminar o modificar *VLANs* que afecten a los demás switches. La información *VLAN* en los switches que trabajen en este modo sólo se puede modificar localmente.
En el router se configuró el protocolo de *DHCP* para proveer direcciones *IP* de manera dinámica a los dispositivos finales.

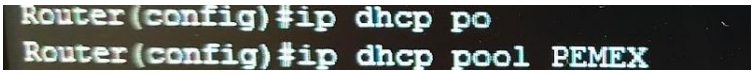


Figura 72. Creación de Pool

La figura 72 muestra la creación de *Pool* de direcciones IP, debido a que las agrupaciones de direcciones se configuran mediante la seccion *Pool* y se asignó el nombre de PEMEX. Se utilizó el comando *ip dhcp pool* para la creación de la misma.

Figura 73. Creación de dominio.

Se creó el nombre de dominio de la empresa, el cual es *pemex.pmx.com.* Se utilizó el comando *domain-name* como muestra la figura 73, para asignar el nombre del dominio.

Figura 74. Asignación de rango de direcciones IP

La figura 74 muestra la asignación del rango de las direcciones IP a asignar. Como la máscara es 255.255.255.0, el rango de direcciones IP a asignar serán desde la 10.0.0.1 hasta la 10.0.0.254.

Figura 75. Asignación de tiempo

La figura 75 muestra la asignación del tiempo máximo que puede asignarse una dirección IP a un nodo de la red. En este caso, el tiempo especificado es 1 días. Después de las 24 horas, el nodo hará un *Refresh* y se le asignará una nueva dirección IP.

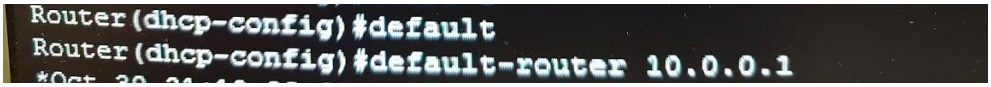


Figura 76. Asignación de dirección IP de puerta de enlace

La figura 76 muestra la asignación de dirección de la puerta de enlace en la red *LAN*, la cual es *10.0.0.1*. Se utilizó el comando *default-router* para la creación de la misma.

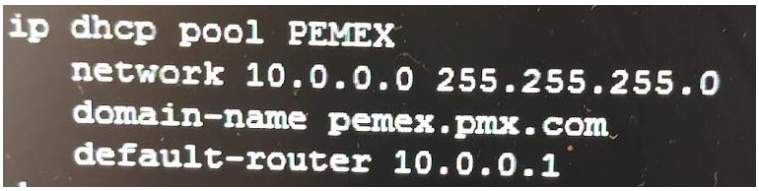


Figura 77. Configuración finalizada

La figura 77 muestra la configuración *DHCP* realizada con el comando *show running-config*.

En los dispositivos finales (computadoras) se configuró el protocolo IPv4 para asignarle una dirección IP dinámica. Es por llo que en el router se habilitó y se configuró el protocolo *DHCP* para poder asignar a cada computadora una direccion IP y máscara de subred.

A continuación se mostrará la asignacion de direccionamiento IP:

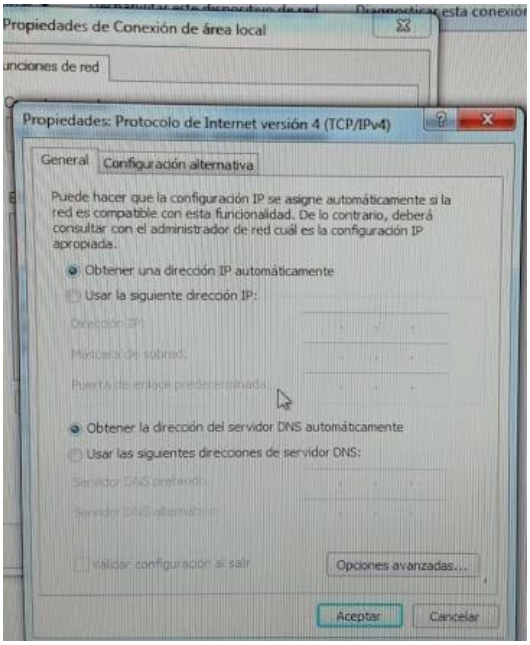


Figura 78. Asignación de direccionamiento IP dinámico

En propiedades del protocolo IPV4, se configuró para asignar una dirección IP, para ello se selecionó en la opción “Obtener una dirección IP automaticamente” como muestra la figura 78, debido a que el router asignará de manera automática direcciones IP a las computadoras pertenecientes en la red.

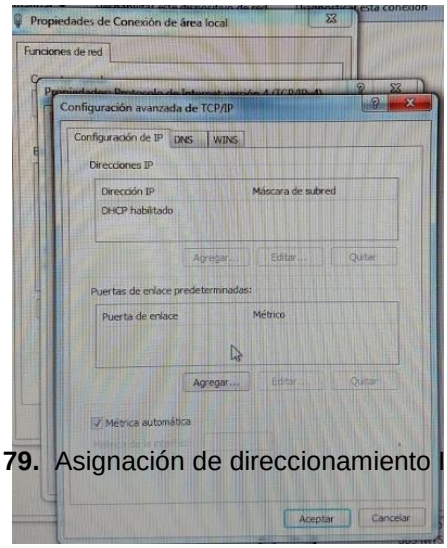


Figura 79. Asignación de direccionamiento IP dinámico

La figura 79 muestra las propiedades avanzadas del protocolo de internet version 4(TCP/IPV4), se verificó que el protocolo *DHCP* estuviera habilidato.

Figura 80. Verificación de asignación por DHCP

Se utilizó el comando *ipconfig /all* en las computadoras de todas las subredes como muestra la figura 80, para verificar la asignación de direccionamiento IP por el protocolo *DHCP*. Cada computadora tiene asignada una dirección IP y máscara de subred.

3.5 Probar y verificación de la red

Para la verificación de la red, fue necesario enviar paquetes mediante el símbolo de sistema a un dispositivo perteneciente a la red, para así confirmar la comunicación inmediata de cada subred y supervisar que el destino final reciba los paquetes e información sin ningún tipo de problema.

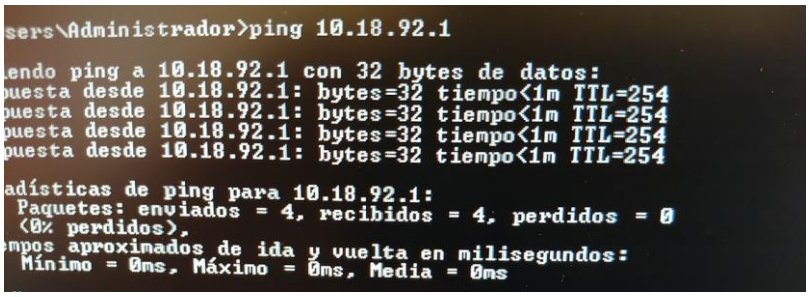


Figura 81. Envío de paquetes

Se enviaron paquetes con el comando *ping,* al destino final con *IP* 10.18.92.1 como se puede apreciar en la figura 81, el envío de paquetes fue exitoso, por lo tanto se puede confirmar que existe comunicación.

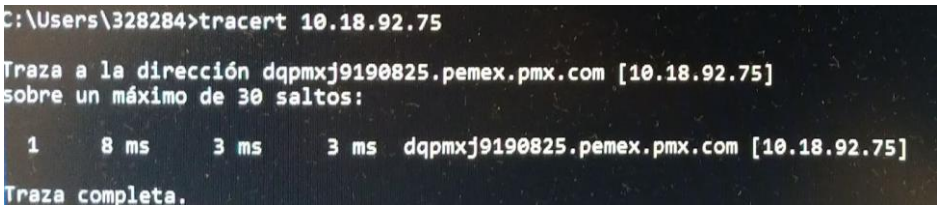


Figura 82. Envío de tracert

Se utilizó el comando *tracert* para determinar el camino que siguen los paquetes de red desde un equipo a otro y así determinar si existe algún problema en algún momento en la red. Sí la conexión es directa entonces habrá un salto como muestra la figura 82.

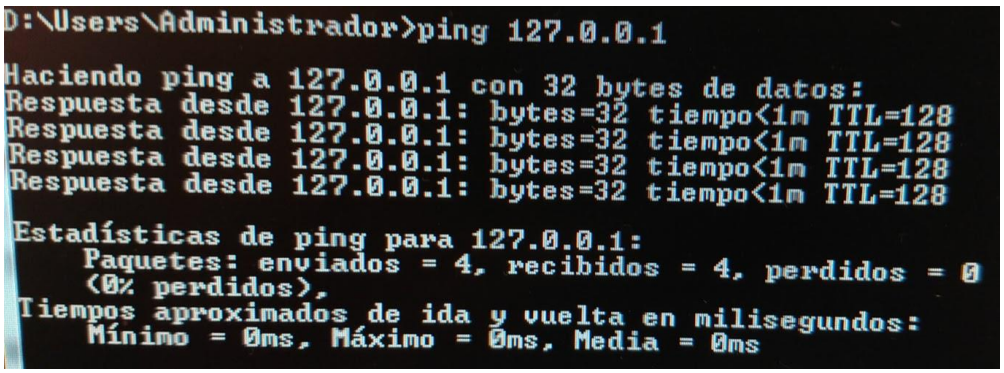


Figura 83. Envío de paquetes a Loopback

La figura 83 muestra el envío de paquetes a *Loopback.* Se utilizó el comando *ping* para verificar la configuración IP interna en el host local. Esta prueba se cumple con el comando ping en una dirección reservada denominada *loopback* (127.0.0.1). Esto verifica la correcta operación de protocolos desde la capa de red a la capa Física.

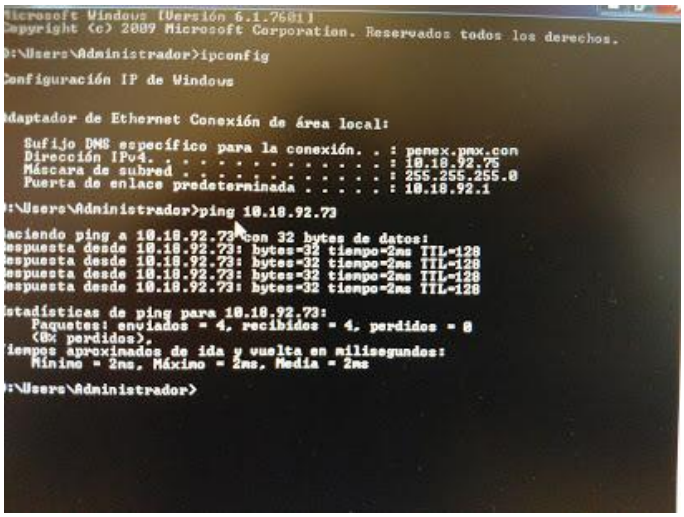


Figura 84. Confirmación de comunicación

Las computadoras pertenecen a la misma red, máscara de subred y al *DNS* el cual es *pemex.pmx.com,* como se muestra en la figura 84. Con ello podemos concluir el proyecto, debido a que la red está funcionando correctamente en tiempo real.

Figura 85. Proyecto finalizado

En la figura 85 se puede ver el jefe del departamento de Telecomunicaciones y Tecnologías de la Información. Los resultados fueron satisfactorios, después de realizar todos los pasos antes mencionados, la empresa PEMEX cuenta con diferentes subredes en los departamentos internos de la misma. Los empleados tienen comunicación inmediata con otros CPI, por lo tanto pueden enviar y recibir información sin ningún problema.

4. Conclusiones y recomendaciones

A lo largo de la implementación del proyecto se adquirieron conocimientos, habilidades y experiencias. Durante cada etapa de la metodología fue necesario realizar investigaciones para sustentar la información. Sin embargo el apoyo de los ingenieros fue de gran ayuda, por lo tanto pude aprender nuevos conceptos, herramientas, óptimas y mejores estrategias que me permitieron distinguir los problemas con mayor facilidad para poder dar solución inmediatamente a cada uno de ellos.

Sinceramente fue una experiencia única y agradable, debido a que pude conocer internamente la empresa PEMEX, así como sus políticas, forma de trabajo y departamentos. La elaboración del proyecto me permitió relacionarme con trabajadores de la empresa, ingenieros con grandes habilidades, aptitudes y experiencias, los cuales me ayudaron y guiaron en el desarrollo del proyecto.

Se llevaron a cabo los conocimientos adquiridos en la Universidad Politécnica de Puebla, cabe mencionar que fue de gran ayuda el curso de CISCO CCNA Introducción a las redes y principios básicos de routing y switching, que fue impartido en la institución antes mencionada. Además me pude dar cuenta, que realmente estoy preparado para el campo laboral, ya que pude resolver las problemáticas que se presentaron en tiempo real en la empresa PEMEX.

Los trabajadores quedaron satisfechos con mi trabajo, ya que existe comunicación inmediata entre ellos y con otros CPI, por lo tanto pueden enviar y recibir información sin ningún problema. Es por ello que me felicitaron por mi gran desempeño y eso fue muy grato para mí. Por lo tanto me llevo una gran satisfacción por mi trabajo y esfuerzo, así como nuevos conocimientos y habilidades, los cuales me servirán a lo largo de mi vida personal y profesional.

Recomendaciones

En lo personal recomiendo que sigan las etapas y pasos efectuados en este proyecto para el diseño e implementación de una Red LAN y WAN, ya que se presenta información sustentada por libros y páginas web oficiales. No obstante intervinieron 2 asesores: el Ing. Oscar Mario Macías García, jefe del departamento de Telecomunicaciones y Tecnologías de la información como asesor técnico y MC Rebeca Rodríguez Huesca, maestra de la Universidad Politécnica de Puebla como asesor académico.

A continuación se mencionarán algunas recomendaciones sí se desea llevar a cabo el proyecto:

- Realizar un diagnóstico general del proyecto a realizar para determinar si es viable o no.
- Analizar las problemáticas que se presentan dentro de la empresa para poder adaptarlo al proyecto o dar una posible solución.
- Realizar un plan de trabajo para asignar fechas y tareas al equipo de trabajo.
- Investigar las normativas ANSI/TIA/EIA-568-B.1 para realizar el cableado estructurado.
- Aprovechar al máximo las instalaciones y herramientas de la empresa a desarrollar el proyecto.
- Tener un registro de las ubicaciones de las computadoras conectadas en los puertos del Switch, para identificar la(s) computadora(s) afectada(s) y poder dar solución inmediatamente.
- Realizar subneteo para dejar direcciones IP disponibles, permitiendo escalabilidad a la empresa.
- Encriptar las contraseñas de los dispositivos intermediarios (Switch y router).
- Configurar el protocolo VTP para la administración de VLAN.
- Realizar mantenimiento preventivo al cableado estructurado.
- Revisar los pasos efectuados en las etapas de la metodología de este proyecto.

5. Referencias bibliográficas

[1] America National Standards Institute/Electronic Industries Alliance. ANSI/EIA-310-D Cabinets, Racks, Panels, and Associated Equipment. Arlington, VA: Telecommunications Industry Association/Electronic Industries Alliance, 1992.

[2] America National Standards Institute/Insulated Cable Engineers Association. ANSI/ICEA S-80-576. Communications –wire and Cable for Premises Wiring. Yarmouth, MA: Imsulated Cable Engineers Association, 1994.

[3] ANSI/ICEA S-83-596.Fiber Optic Premises Distribution Cable. Yarmouth, MA: Insulated Cable Engineers Association, 1994.

[4] American National Standards Institute/National Fire Protection Association, Inc ANSI/NFPA-70. National Electrical Code. Quincy, MA: National Fire Protection Association, Inc, 1999.

[5] ANSI/NFPA-71. Installation Maintenance, and Use of Signaling Systems for Central Station Service. Quincy, MA: National Fire Protection Association, Inc, 1989.

[6] ANSI/NFPA-72. National Fire Alarm Code. Quincy, MA: National Fire Protection Association, Inc, 1999.

[7] https://tabasco.gob.mx/sites/default/files/Manual-para-aplicar-la-norma-TIA-EIA-para-Cableado-Estructurado.pdf Página de dirección general de Tecnologías de la Información y Comunicaciones, en ella puede consultar información acerca de cableado estructurado. Fecha de consulta: 02/octubre/2018

[8] “Redes de Computadores y Arquitectura de Comunicaciones. Supuestos Prácticos”. Nicolás Barcia y otros. Ed. Pearson Prentice-Hall. 2005.

[9]https://www.unac.edu.pe/images/inventario/documentos/manuales/topologia-e-infraestructura_guia_v02.pdf Página de topología e Infraestructura básica de redes, en ella puede consultar información de Topologías de red. Fecha de Consulta: 30/Septiembre/2018

[10] Cisco, 2008a] “Academia de Networking de Cisco Systems: Guía del primer año CCNA 1 y 2”. 3º Edición. Cisco Press, Madrid, 2008.

[11] "Internet, TCP/IP y Desarrollo de Sistemas Distribuidos". Fco. Javier Yágüez y otros. Servicio de Publicaciones de la F.I. 2004.

[12] "Transmisión de datos y redes de comunicaciones". 4ª edición. Behrouz A. Forouzan. Ed. McGraw-Hill. 2007.

[13]https://issuu.com/elizabeth2910/docs/introduccion_de_como_subnetear_una_red_de_computad Página de Redes comunicación de datos en ella puede consultar información acerca de creación de subredes. Fecha de consulta: 01/Octubre/2018.

[14]http://itroque.edu.mx/cisco/cisco1/course/module1/1.2.1.3/1.2.1.3.html Página de Cisco CCNA1 en ella puede consultar información acerca de los dispositivos intermediarios. Fecha de consulta: 03/Octubre/2018

[15]https://www.mhe.es/cf/ciclos_informatica/844819974X/archivos/unidad9_recurso1.pdf Página de Configuración de Switch y Router, en ella puede consultar información acerca de productos Cisco para redes IP. Fecha de Consulta: 03/Octubre/2018

[16] Data Networks, IP and the Internet Martin P. Clark, Ed. Wiley 2002

[17]https://www.adrformacion.com/knowledge/administracion-de-sistemas/verificacion_y_prueba_de_conectividad_de_una_red_local.html Página de administración de sistemas, en ella puede consultar información acerca de la verificación de conectividad. Fecha de consulta: 04/Octubre/2018.

[18]https://www.pce-instruments.com/espanol/instrumento-medida/medidor/tester-de-redes-lan-kat_71710_1.htm

[19] https://www.ecured.cu/PuTTY Página oficial de Ecured, en ella puede consultar información acerca del programa que permite conectar servidores remotos. Fecha de consulta: 05/Octubre/2018

[20]https://www.obs-edu.com/int/blog-project-management/herramientas/ventajas-que-te-ofrece-microsoft-visio-2013-mega Página oficial de Business School, en ella puede consultar información acerca de Visio. Fecha de consulta: 07/Octubre/2018

[21]https://quintodeprogramacion.wordpress.com/2014/10/20/ventajas-y-desventajas-de-los-sistemas-operativos-ms-do/ Página de Quinta programación, en ella puede consultar información acerca de Cmd. Fecha de consulta: 09/Octubre/2018

Universidad Politécnica de Puebla
Ingeniería en Informática

Jan Carlos Robles Ortega
Oscar Mario Macías García
Rebeca Rodríguez Huesca