UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio de Ciencias e Ingenierías

DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN PARA LA EMPRESA PALINDA.

Propuesta tecnológica

LI PING ZHENG HUANG

Redes y Sistemas Operativos

Trabajo de titulación presentado como requisito para la obtención del título de Licenciado en Redes y Sistemas Operativos.

Quito, 12 de mayo de 2017

UNIVERSIDAD SAN FRANCISCO DE QUITO USFQ

Colegio De Ciencias e Ingenierías

HOJA DE CALIFICACIÓN
DE TRABAJO DE TITULACIÓN

DISEÑO E IMPLEMENTACIÓN DE UNA RED LAN PARA LA EMPRESA PALINDA

LI PING ZHENG HUANG

Calificación: _____

Nombre del profesor, Título académico: Ney Acosta., Ing.
Jose Medina., Mg.

Firma del profesor: _____

Firma del profesor: _____

Quito, 12 de mayo de 2017

DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído todas las Políticas y Manuales de la Universidad San Francisco de Quito USFQ, incluyendo la Política de Propiedad Intelectual USFQ, y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo quedan sujetos a lo dispuesto en esas Políticas.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Firma del estudiante: _____

Nombres y apellidos: LI PING ZHENG HUANG

Código: 00064027

Cédula de Identidad: 171066008-3

Lugar y fecha: Quito, 12 de mayo de 2017

AGRADECIMIENTOS

Agradezco a mi familia por su apoyo, siempre incentivándome para terminar mi carrera universitaria.

Agradezco a mi esposo Sergio por toda su paciencia durante el tiempo que me demoro en culminar mi carrera y el tiempo que me tomo para desarrollar este proyecto de titulación.

Agradezco a mis hijos Matías y Xiao que están siempre conmigo.

Agradezco a mi amigo Robert por ser una guía para poder desarrollar este caso de estudio para la obtención del título de Licenciado de Redes y Sistemas Operativos.

A todos los maestros de la universidad que, con sus conocimientos me permitieron desarrollar habilidades y actitudes que requieren para ser un profesional.

RESUMEN

La administración de las redes LAN y WAN en la actualidad ha permitido a las empresas e instituciones optimizar el uso de los recursos mediante una red centralizada permitiendo disponer la información de forma segura y rápida.

El presente proyecto busca integrar servicios de comunicación, permitiendo la transmisión de datos desde un punto central hacia los diferentes departamentos de PALINDA. El hecho de realizar un análisis de los requerimientos de la infraestructura nos permite determinar una solución con los recursos técnicos disponibles y financieramente con costos bajos.

PALINDA actualmente no cuenta con ninguna infraestructura tecnológica de comunicación por lo que poder administrar la red en un solo sistema, permitirá agilizar los trámites y procesos para que los usuarios obtengan la información actualizada, sistematizada y en tiempo real agilitando las funciones.

Palabras clave: LAN, WAN, Infraestructura, Comunicación, Red.

ABSTRACT

The management of the LAN and WAN networks has allowed companies and institutions to optimize the use of resources through a centralized network, allowing the availability of information in a secure and fast way.

The present project seeks to integrate communication services, allowing the transmission of data from a central point to the different departments of PALINDA. The fact of performing an analysis of the requirements of the infrastructure allows us to determine a solution with the available technical resources and financially with low costs.

PALINDA currently does not have any infrastructure communication technology, so to be able to manage the network in a single system, allows to streamline the procedures and processes so that users get updated information, systematized and in real time streamlining functions.

Key words: LAN, WAN, Infrastructure, Communication, Network.

CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

1 INTRODUCCIÓN

Actualmente existe una gran cantidad de compañías que utilizan las redes de computadoras para poder comunicarse entre sí por medio de conexiones ya sean físicas o inalámbricas. Dependiendo de las necesidades de las empresas, se implementa arquitectura que permiten la transmisión de datos en un área geográficamente pequeña, es decir conectan estaciones de trabajos, terminales y otros dispositivos en un solo edificio, o puede necesitar la implementación de comunicaciones entre áreas geográficamente separadas.

Hace seis años fundé PALINDA, un negocio la cual abrí enfocándome en la alimentación a base de soya para las personas veganas y vegetarianas. PALINDA fue creada con la finalidad de elaborar alimentos a base de soya como el Tofu, Nata de Soya, Tofu ahumado, Láminas de soya. En ese tiempo bastaba un sistema manual en donde solo se requería un punto de red con la comunicación hacia el Internet. Con el tiempo, las ventas aumentaron, se diversificaron los clientes, se manejaba una recepción, despacho e inventario en línea y en el mismo se podía verificar los pedidos de cada cliente. Debido a la concientización de las personas por una alimentación sana, nuestros pedidos aumentaron significativamente a nivel nacional y eso me obligó como fundadora de PALINDA y administradora de red, a planificar e implementar un sistema de comunicación en donde toda la información y los recursos estén disponibles y centralizados.

Debido a que es una fuerte inversión, se requiere equipamiento informático, aplicaciones, cableado estructurado, infraestructura que se comuniquen entre sí para poder realizar las operaciones diarias.

Se debe considerar los beneficios de la implementación de sistemas de comunicación para enlazar los datos por lo que se requiere un estudio de las diferentes opciones para analizar sus ventajas y desventajas.

2 TERMINOLOGIA DE NETWORKING

2.1 REDES DE DATOS:

Son redes de comunicación en las que se han diseñado para transmitir datos. Las redes de datos es un método eficaz de compartir la información a los usuarios aumentando la productividad mientras se ahorra dinero y evitar la duplicación del equipo y de los recursos.

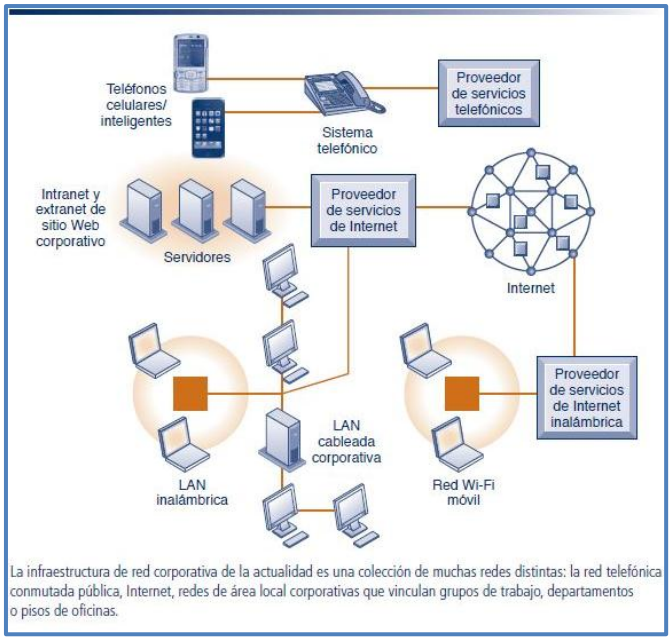

Figura No. 1 Redes de Datos

Fuente: http://4.bp.blogspot.com/-FsGh-zMfgdE/Vi_W1a6lhNI/AAAAAAAAAWw/OWZlGBEa3Xw/s640/7.2.JPG

2.2 ESTACIONES DE TRABAJO:

Es una computadora cliente que se utiliza para ejecutar aplicaciones y que está conectada a un servidor del cual se obtiene datos compartidos con otras computadoras.

2.3 SERVIDORES

En un entorno de sistema operativo de red, los usuarios acceden y comparten recursos de uno o varios servidores, por lo que deben estar equipados para soportar el acceso recurrente de los usuarios y múltiples tareas, es recomendable adquirir el equipo con unidades de disco de alta capacidad y velocidad.

Los sistemas operativos de red están diseñados para proporcionar procesos de red a los clientes, estos servicios más frecuentes incluyen World Wide Web, compartición de ficheros, intercambio de correo, administración remota, impresión, servicios de directorios. Los servicios basados en este conjunto de protocolo son vulnerables a análisis no autorizados y ataques maliciosos como DoS (Denial of Services) por lo que se recomienda proteger los recursos mediante autenticación y encriptaciones.

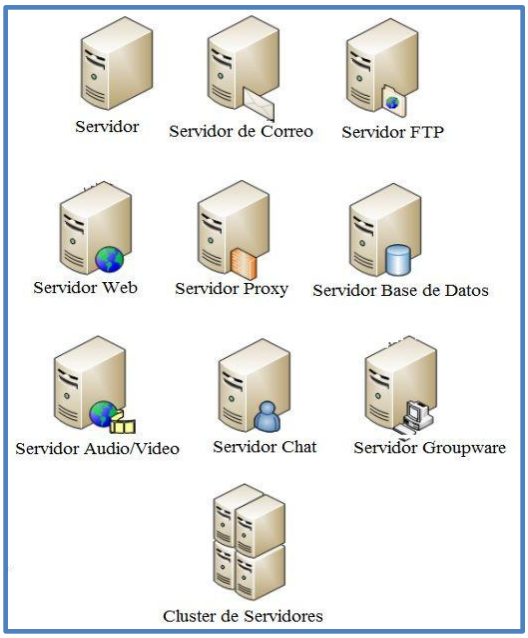

Figura No. 2 Tipos de Servidores

Fuente: http://www.areatecnologia.com/informatica/imagenes/tipos-de-servidores.jpg

2.4 ANCHO DE BANDA:

El ancho de banda es la cantidad de información que puede atravesar una conexión de red desde un punto a otro en un periodo de tiempo dado. Se utiliza como sinónimo de velocidad de transferencia de datos. Se expresa bits por secundo (bps). Actualmente se puede llegar a tener velocidades de millones (Mbps) de bits por secundo hasta miles de millones de bits por segundo (Gbps). A pesar del tipo de medio que se utilicen para construir la red, hay limitaciones para llevar la información.

2.5 LATENCIA:

Es el retardo entre el momento de que un dispositivo solicita acceso a la red hasta que haya obtenido el permiso para transmitir.

2.6 COLISION

Ocurre cuando dos o más estaciones de trabajo intentan enviar datos sobre el cable de la red al mismo tiempo, todos los datos se corrompen, por lo que las redes de computadoras tienen mecanismo de ordenamiento para prevenirlas.

2.7 MODELO OSI (Open System Interconnection)

Es un sistema de reglas que aplica a todas las redes en la cual proporcionó a los fabricantes una serie de estándares asegurando compatibilidad e interoperabilidad de los equipos de diferentes marcas. El modelo OSI representa una serie de pasos donde se comunican mediante envíos y recibos de datos a través de la red.

Este modelo nos permite entender de cómo la información viaja a través de la red, es decir nos explica como los paquetes viajan a través de diferentes capas de una red a otra. En este modelo hay siete capas, cada una con diferente función permitiendo romper la comunicación de la red en pequeñas partes para ser más manejables, estandariza los

componentes de la red, además de permitir que varios tipos de software y hardware se comuniquen. Esto también evita que los cambios de una capa afecten otras capas.

2.7.1 CAPA FISICA:

Se encarga de transmitir y recibir los bits sin procesar al medio físico hacia la siguiente capa, en esta capa está el cableado, los conectores, las interfaces físicas, mecánicas, voltaje. En una falla de red, esta es la primera capa en la que se debe verificar.

2.7.2 CAPA DE ENLACE DE DATOS

Se encarga del acceso al medio y control del enlace. Los datos llegan de la capa física en forma de bits y los transforma en tramas para el direccionamiento físico, notificación de errores y control de flujo.

2.7.3 CAPA DE RED

En esta capa determina la mejor ruta para la trasmisión, en esta capa se produce un dialogo con la red para establecer las prioridades y el direccionamiento, es decir que enruta los paquetes

2.7.4 CAPA DE TRANSPORTE

Es una conexión de extremo a extremo permitiendo que los datos enviados y recibidos lleguen en orden sin errores. Es decir que establece, mantiene y controla el flujo para la detección y recuperación de fallas.

2.7.5 CAPA DE SESION

En esta capa proporciona la comunicación ente aplicaciones para el uso eficiente de las comunicaciones, agrupan datos de diferentes aplicaciones para ya sea enviarlos juntos, detener la comunicación, o restablecer el envío. En esta capa establece, administra y

finaliza las sesiones de comunicación que consta de solicitudes y respuestas de servicio que se presentan entre aplicaciones.

2.7.6 CAPA DE PRESENTACION

Aquí representa los datos, es decir que asegura que los datos sean entendidos por el destino. Negocia la sintaxis de la transferencia de datos entre aplicaciones.

2.7.7 CAPA DE APLICACIÓN

En esta capa están las aplicaciones de red que permiten utilizar los recursos, aplicaciones ya sea procesos como email, web browser, ftp.

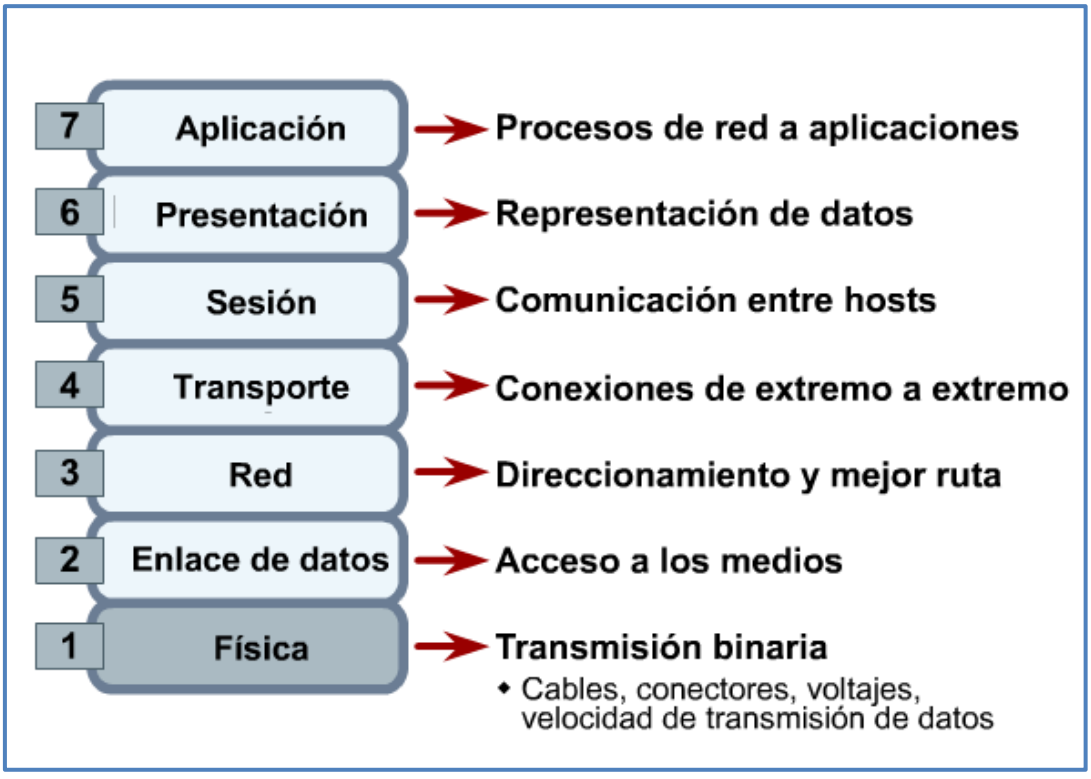

Figura No. 3 Modelo OSI

Fuente: http://zoombie-linux.blogspot.com/2011/03/modelo-osi.html

2.8 DISPOSITIVO DE RED

Son todos los dispositivos que conectan entre si a los dispositivos de usuario final permitiendo la intercomunicación. Estos dispositivos son los encargados de transportar los datos hacia los dispositivos de usuario final. Estos dispositivos proporcionan el tendido de las conexiones, la conversión de los formatos de datos, la administración de la transferencia de datos.

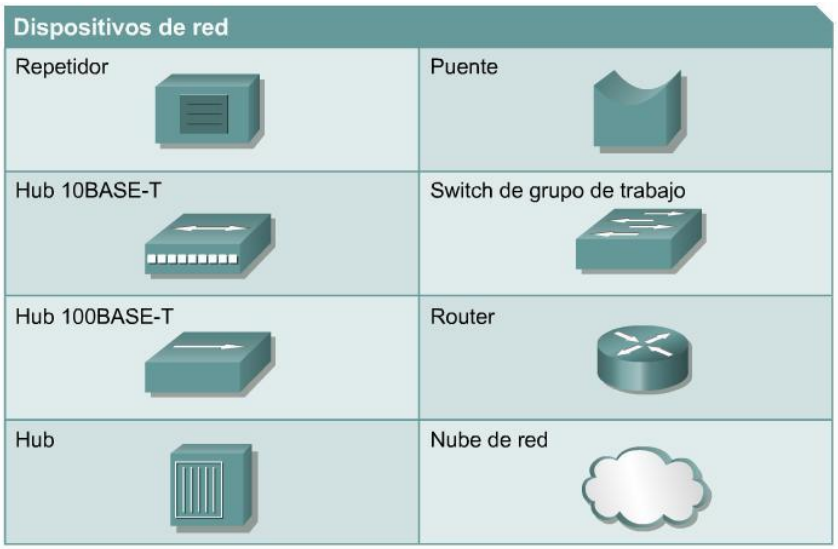

Figura No. 4 Dispositivos de Red

Fuente: https://glendasnotepad.files.wordpress.com/2008/07/red.jpg

2.8.1 **REPETIDOR**

Dispositivo que regenera y re sincroniza los datos enviados por la red para alcanzar distancias más largas. Cuando un repetidor recibe datos de un segmento de red, descodifica y codifica la información binaria (bits) y retransmite la señal al destino, permitiendo extender la red más lejos y aumentando la capacidad de incrementar el número de dispositivos conectado a la red. Una de las desventajas es que intercambian los dominios de colisión. Un repetidor no realiza enrutamiento inteligente como los switches y routers. Se recomienda usar a regla de cuatro repetidores para Ethernet de 10-Mbps

como estándar al ampliar segmentos de LAN, esto significa que no se debe implementar más de cuatro repetidores en una LAN, permitiendo limitar la latencia, ya que demasiada latencia en la LAN, se aumenta el número de colisiones tardías haciendo que la red sea menos eficiente.

2.8.2 **HUB**

Dispositivo de capa 1 conocido también como concentrador o repetidor multipuerto. Permite que más usuarios tengan acceso a la red, se encarga de regenerar la señal permitiendo la extensión de la red a una mayor distancia. Los hubs no toman ninguna decisión de las señales que reciben.

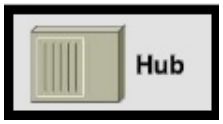

Figura No. 5 Representación de un Hub

2.8.3 SWITCH

Dispositivo de red de capa 2 que funciona en la capa de enlace de datos y sirve como un punto de concentración para conectar estaciones de trabajo, impresoras, router, hubs, servidores. Los switch toman decisiones inteligentes de si dejar o no pasar las señales de datos en una red. Un switch proporciona un circuito virtual dedicado y punto a punto entre dos dispositivos de red que están conectados evitando colisiones ya que operan de modo dúplex, es decir que puede recibir y enviar datos en el mismo tiempo dado.

Figura No. 6 Representación de un Switch

El switch aprende la dirección de cada dispositivo identificando la dirección MAC de origen de la trama y etiqueta el puerto por donde la trama entro en el switch, añade esta información a la base de datos llamada tabla de conmutación. Estas direcciones se aprenden dinámicamente y las almacenan en la CAM (memoria de contenido direcionable).

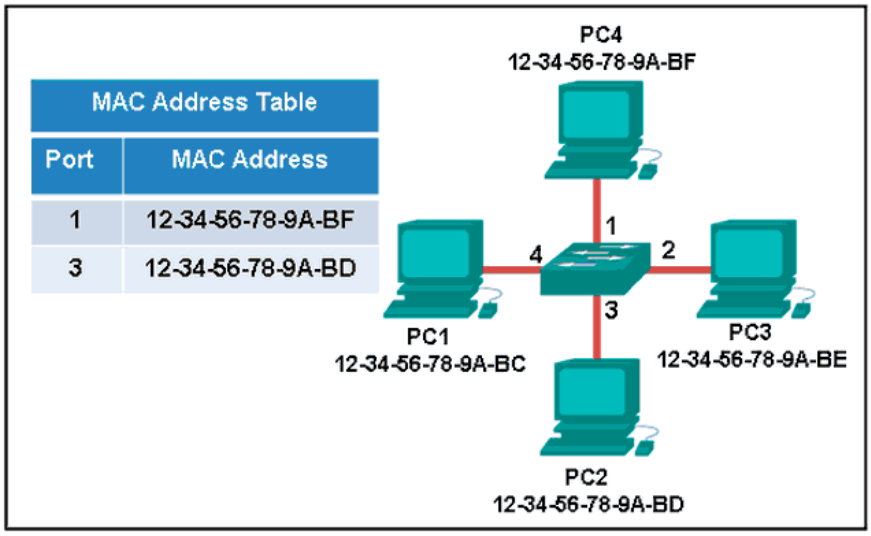

Figura No. 7 Tablas de puenteado

Fuente: https://lh6.googleusercontent.com/-3MZrwVnJSe8/Uvq24wv6yPI/AAAAAAAAAIE/DdftzMSYgxg/w645-h402-no/p20-exa5-ccna1.png

El proceso de un switch al momento de tomar la decisión, ocurre de esta manera:

- ✓ Si el dispositivo destino está en el mismo segmento de la trama, el switch bloquea la trama hacia los otros segmentos, a este proceso se lo conoce como ***filtrado***.
- ✓ Si el dispositivo destino está en segmento distinto, el switch transmite la trama hacia el segmento apropiado.

- ✓ Si la dirección del destino es desconocida, el switch transmite la trama a todos los segmentos excepto por el cual la trama fue recibida, este proceso se lo conoce como ***flooding o inundación.***

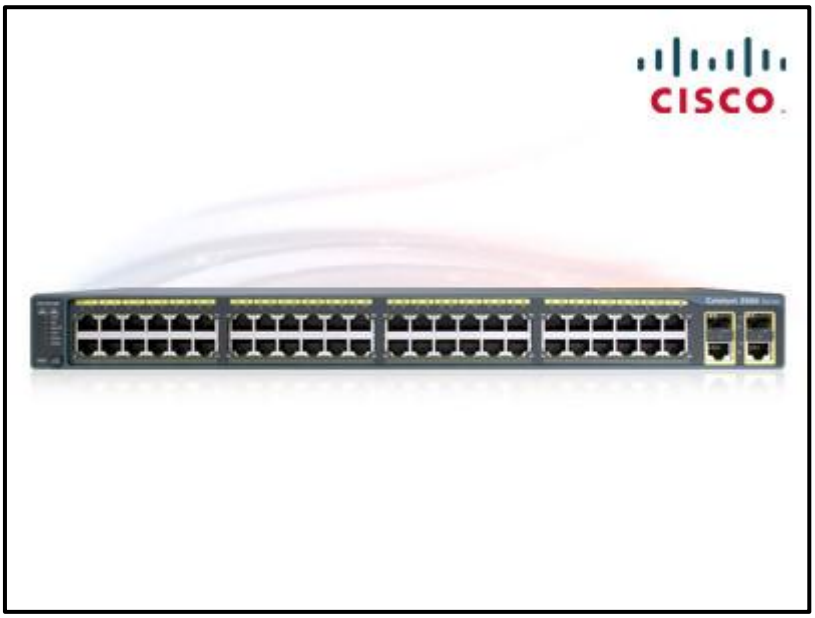

Figura No. 8 Switch Catalyst 2960

Fuente: http://www.tecnoredsolutions.com/wp-content/uploads/2014/09/CATALYS2960-24TT.jpg

2.8.4 ROUTER

Dispositivo de capa 3 que utiliza una o más métricas para determinar la ruta optima por la que se debe enviar el tráfico de la red. Los routers envían paquetes de una red a otra red basándose en la información de la capa de red.

Figura No. 9 Simbología de un router

Generalmente los router retransmiten un paquete de enlaces de datos a otro, estas utilizan dos funciones básicas: la determinación de la ruta y la conmutación. La conmutación permite a un router aceptar un paquete en una interfaz y reenviarlo a una segunda interfaz para reenviar un paquete.

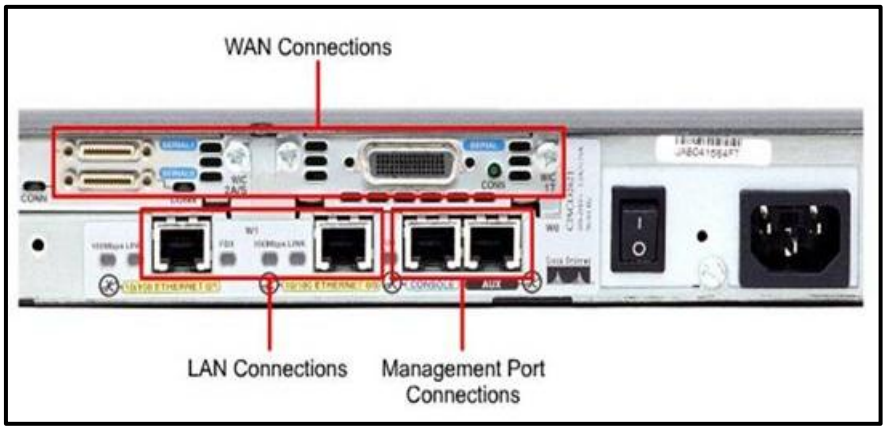

Figura No. 10 Interfaces de un router

Fuente: https://d1hx5100zal7gj.cloudfront.net/images/stories/cisco-ccna/ch-2-1.1-ios/cisco-ccna-ios-03.jpg

2.9 DIRECCION IPv4

Una dirección de 32 bits que se asigna a un host, está escrita como cuatro octetos y separados por puntos. Cada dirección consta de un numero de red, opcionalmente un numero de subred y un numero de host y se los utiliza para dirigirse a un host individual de la red.

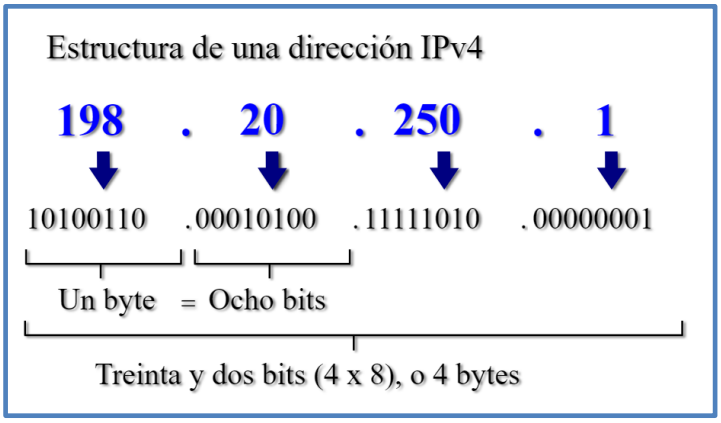

Figura No. 11 Dirección IP v4

Fuente Elaboración propia

2.10 MASCARA DE SUBRED

Una máscara de subred se utiliza para extraer la información de redes y subredes de la dirección IP.

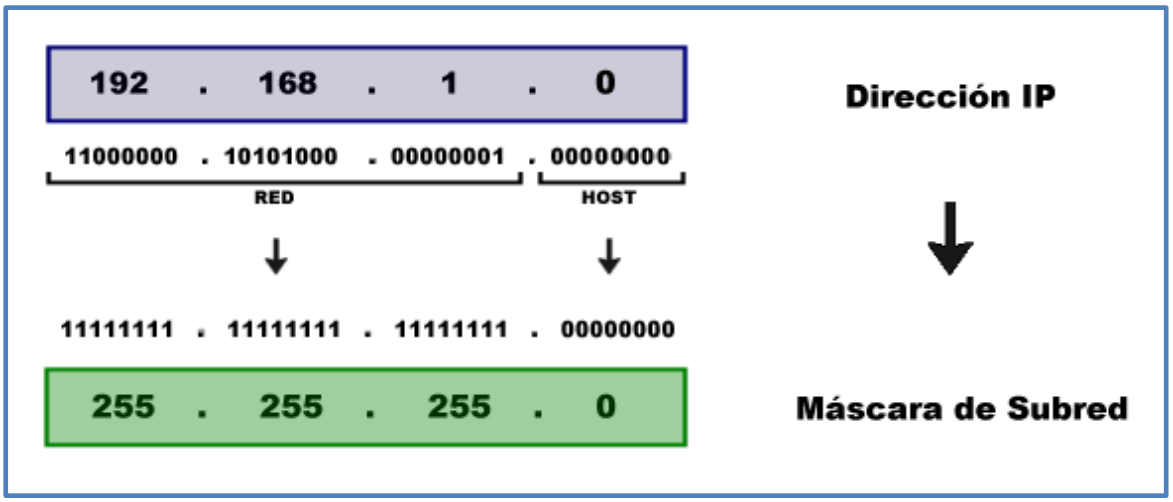

Figura No. 12 Mascara de Subred

Fuente: Elaboración propia

Otra forma de representar las máscaras de subred más sencilla es por el número de bits que se utiliza para red en la dirección IP. Por ejemplo, en el caso de clase C sabemos que son 24 bits así pues también se puede representar como /24.

Tipo de Red	Rango de Red	Nº Bits para Red	Máscara de Subred
Clase A	0.0.0.0 - 127.255.255.255	8	255.0.0.0
Clase B	128.0.0.0 - 191.255.255.255	16	255.255.0.0
Clase C	192.0.0.0 - 223.255.255.255	24	255.255.255.0

Figura No. 13 Representación de Mascara de Subred

Fuente: Elaboración propia

2.11 VLSM (MASCARA DE SUBRED DE LONGITUD VARIABLE)

Nos permite utilizar más de una máscara de subred dentro del mismo espacio de direcciones. Esta opción nos permite como administrador de red dividir en subredes una subred y maximizar la eficacia de direccionamiento.

2.12 DHCP (PROTOCOLO DE CONFIGURACION DINAMICA DEL HOST)

Es un protocolo que proporciona un mecanismo para asignar direcciones IP dinámicamente para que estas direcciones IP puedan volver a utilizarse automáticamente cuando los host ya no los necesite. DHCP trabaja en modo cliente/servidor, ya que valida los host en una red IP para obtener sus configuraciones desde un servidor, reduciendo así el trabajo de un administrador de red.

2.13 TOPOLOGIA DE RED

Es la estructura de la red, que se define en dos partes, la física y la lógica.

2.13.1 TOPOLOGIA FISICA

Muestra la disposición de los cables o medios, las más comunes en la implementación de una red es:

- ✓ TOPOLOGIA DE BUS: Arquitectura Lineal donde solo se usa un cable backbone que debe terminarse en ambos extremos y donde todos los hosts se conectan al backbone.
- ✓ TOPOLOGIA DE ANILLO: Arquitectura en donde un host conecta con el host siguiente creando un anillo físico de cable.
- ✓ TOPOLOGIA DE ESTRELLA: Topología LAN en la que los puntos finales de una red están conectados a un switch / hubs central mediante enlaces punto a punto.
- ✓ TOPOLOGIA EN ESTRELLA EXTENDIDA: Conexión de varias estrellas individuales, ampliando el alcance y la cobertura de la red.
- ✓ TOPOLOGIA JERARQUICA: Diseño parecido a una estrella extendida, con la diferencia que el control del acceso al medio está controlado con una computadora que controla el tráfico de la topología.
- ✓ TOPOLOGIA EN MALLA: Cada host tiene sus propias conexiones al resto, se lo implementa para proporcionar tanta protección como sea posible contra a interrupción del servicio.

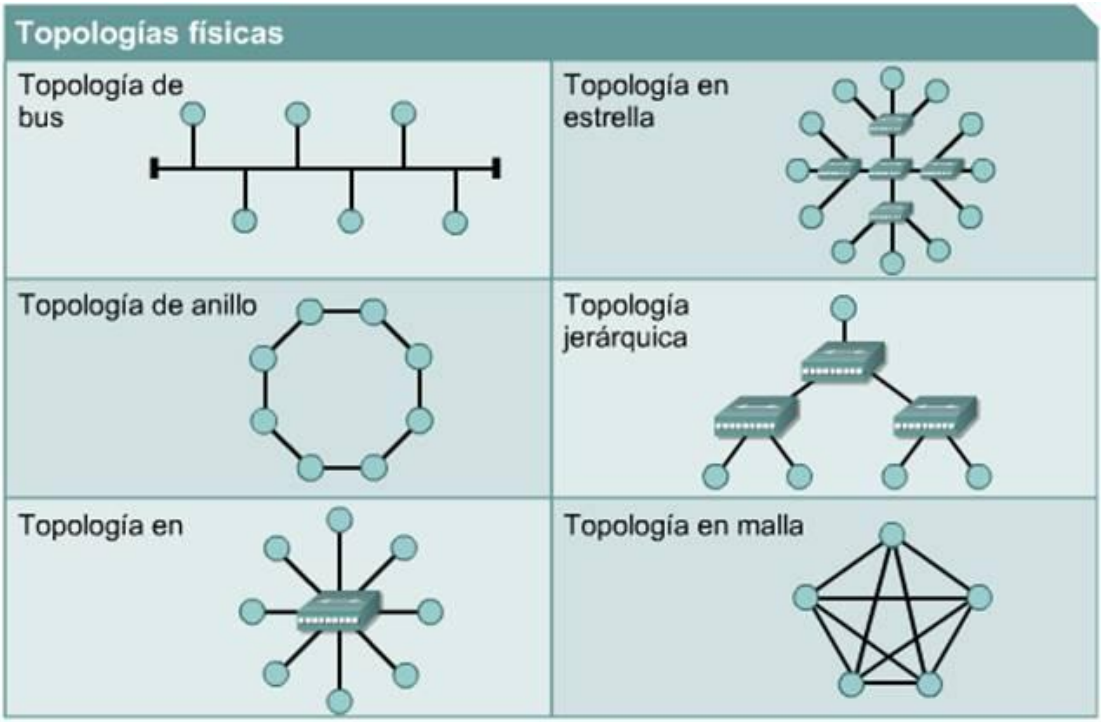

Figura No. 14 Topología Física

Fuente: http://alumnosistema.galeon.com/IS-1Y2/TEMA_II/TEMA_2_1_4_archivos/image002.jpg

2.13.2 TOPOLOGIA LOGICA:

Se define como los medios son alcanzados por los hosts para enviar datos, es decir la forma en que los hosts se comunica a través del medio. Las topologías lógicas más comunes son ***broadcast*** es decir que cada host envía sus datos al resto de los hosts en el medio de la red y el primero que viene, es el primero que se procesa un ejemplo de esta topología es Ethernet y ***transmisión de tokens*** que controla el acceso a la red pasando un token electrónico secuencialmente a cada host. El Token Ring y FDDI (Fiber Distributed Data Interface) son dos ejemplos de las redes que utilizan la transmisión de token

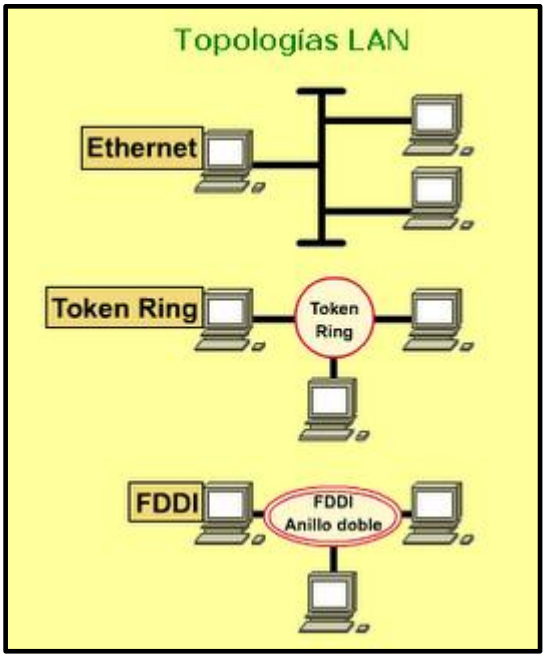

Figura No. 15 Topología Lógica

Fuente: http://4.bp.blogspot.com/-NH3Vgx3Bryk/TZK5d7nsbcI/AAAAAAAAAjE/XBHYcE0_v84/s1600/TOPOLOGIA+LAN+HT.png

2.14 PROTOCOLO DE RED

Son un conjunto de reglas que permiten la comunicación de la red desde un host hasta otro host pasando a través de las redes. Estos protocolos determinan el formato, la secuencia, sincronización y el control de errores en la transmisión y recepción de datos.

2.15 LAN (LOCAL AREA NETWORK)

Es una red de datos que cubre un área geográficamente pequeña y limitada, que conectan las estaciones de trabajo, terminales, dispositivos ya sea en un edificio, oficina o campus. Una LAN consiste en computadoras, dispositivos periféricos, dispositivos de Red, Tarjetas de Interface de Red (NICs). Proveen conectividad todas las 24 horas y utilizan las normas de la capa física y la capa de enlace de datos del modelo OSI. Ehternet, FDDI y Token Ring son algunas de las tecnologías LAN más comunes aunque el estándar más utilizado es el Ethernet.

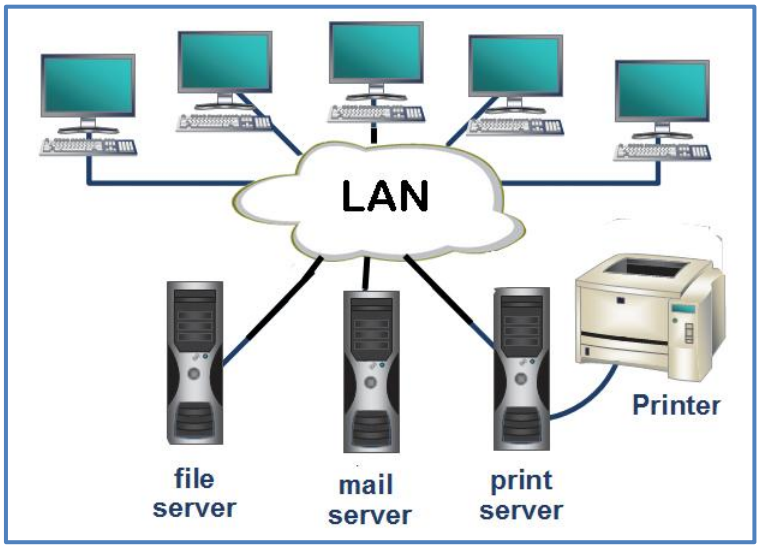

Figura No. 16 LOCAL AREA NETWORK

Fuente: https://userscontent2.emaze.com/images/0b4644f2-654a-47a2-a22e-ccff9ef1cc1d/6e6c655870e319102b16b0d8dc3b1085.jpg

2.16 VLAN (VIRTUAL LOCAL AREA NETWORK)

Un grupo de dispositivos que están configurados de un modo que puedan comunicarse como si estuvieran conectados por el mismo cable. Las VLAN segmentan lógicamente las redes conmutadas basándose en las funciones. Se utilizan las VLAN para escalar, mayor seguridad y administrar el flujo de tráfico.

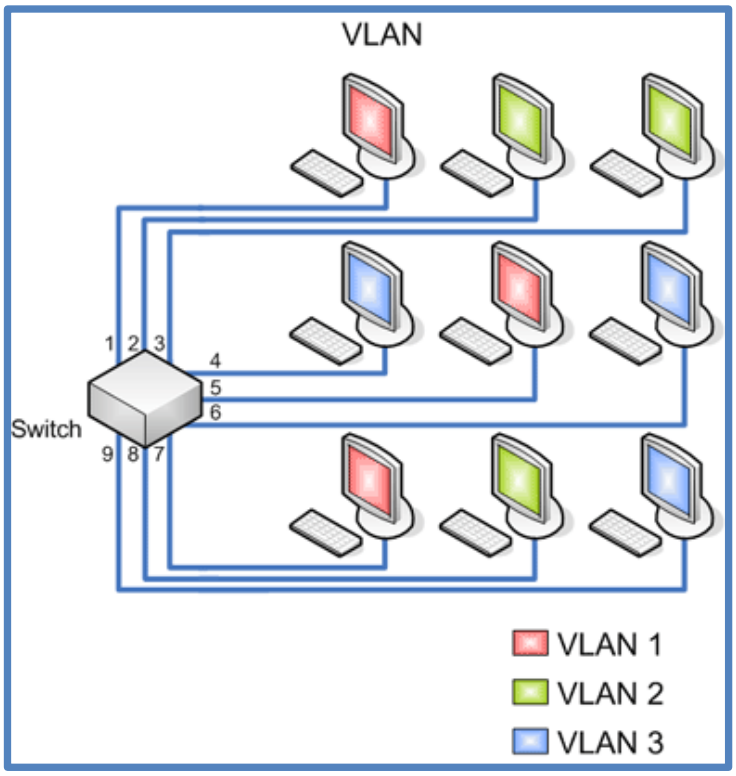

Figura No. 17 VLAN

Fuente: http://redesconfiguracion.blogspot.com/2015/07/que-es-una-vlan-y-su-funcion.html

2.16.1 BENEFICIOS DE LAS VLAN

Cada año las empresas crecen y se reorganizan continuamente, las VLAN facilitan el diseño de una red para dar soporte a los objetivos de una organización. Los principales beneficios en la implementación de las VLAN son los siguientes:

- ✓ Los usuarios que manejan datos sensibles están separados del resto de la red, disminuyendo las posibilidades de comprometer los datos, garantizando mayor seguridad.
- ✓ Reducir el uso ancho de banda haciendo más efectiva la red debido a que reduce el tráfico de datos innecesarios.
- ✓ Reduce los dominios de difusión.
- ✓ Administración centralizada y efectiva para el administrador de red.

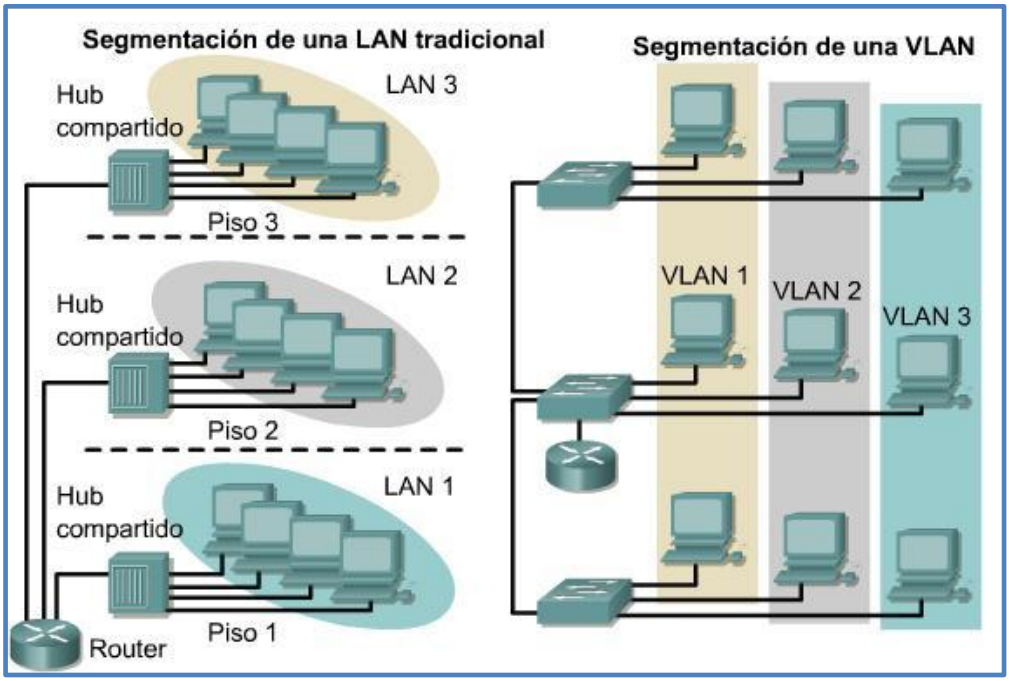

Figura No. 18 Las VLAN y los límites físicos

Fuente: http://cursos.clavijero.edu.mx/cursos/069_cIII/modulo4/imagenes/tema4.1/subtema4.1.1/4.1.1a.JPG

2.17 VTP (PROTOCOLO DE TRUNKING VLAN)

VTP es un protocolo pantentado por CISCO, que reduce la administración en una red conmutada, es un protocolo de mensajería que utiliza las tramas troncales de la capa 2 para agregar, eliminar y renombrado de VLAN en un solo dominio, permite cambios centralizados que se comunican a todos los switches de la red.

Se creó VTP para solucionar problemas de funcionamiento en un entorno de red conmutada de VLAN ya que mantiene la coherencia de la configuración VLAN a lo largo de un dominio de administración común, es decir que al configurar una VLAN nueva en un servidor VTP, la VLAN se distribuye a través de todos los switches en el dominio, reduciendo así la necesidad de configurar la misma VLAN en todos los sitios.

VTP proporciona las siguientes ventajas además de la coherencia en la configuración VLAN de toda la red:

- ✓ Esquema de asignación que permite que una VLAN sea troncal
- ✓ Seguimiento de las VLAN
- ✓ Monitoreo preciso de VLAN
- ✓ Configuración plug and play al momento de añadir nuevas VLAN
- ✓ Informe dinámico de las VLAN que se añade a la red.

2.18 NAT (NETWORK ADDRESS TRANSLATION)

Es un mecanismo para reducir la necesidad de IP address, permite que las empresas cuyas direcciones no son globalmente exclusivas se conecten a Internet transformando esas direcciones en espacio de direccionamiento enrutable globalmente.

2.19 WAN (WIDE AREA NETWORK)

Las WANs interconectan LANs, es decir que abarcan áreas geográficamente grandes, permitiendo a las empresas comunicarse entre sí a pesar de las distancias. Tiene la capacidad de comunicarse en tiempo real con diferentes usuarios, permitiendo el acceso a recursos de otras ciudades.

La principal variación entre WAN y LAN es la escalabilidad. Se espera que la WAN se estire porque el requisito de cubrir varias ciudades, incluso países y continentes, es una necesidad. Un grupo de conmutadores y enrutadores están interrelacionados con una red de área amplia. Los conmutadores se pueden conectar en diversas localidades como red completa y redes parciales también. Una red de área amplia puede ser confidencialmente poseído o contratado de un proveedor de servicios, pero no se puede ignorar el hecho de que cubre varios servidores.

Los equipos de conmutación de paquetes y conmutación de circuitos se emplean en la WAN. En una unidad de conmutación de paquetes, las redes tienen asociaciones en la red de la portadora, y numerosos clientes dividen el conjunto de conexiones de la portadora. El portador puede entonces generar circuitos eficaces entre los sitios de los clientes, mediante los cuales los paquetes de datos se distribuyen de uno a otro, a través de la red.. La conmutación de circuitos permite que las conexiones de datos determinen cuando sea necesario y luego se concluye cuando la transmisión es generalizada. Estos actos como la línea telefónica normal de trabajo para la correspondencia de voz. La red digital de servicios integrados (ISDN) es una buena ilustración de la conmutación de circuitos. Cuando un enrutador tiene información para un sitio remoto, el circuito conmutado es proporcional a la cantidad de circuito de la disposición remota de toda la red. Se han reunido amplias redes WAN, junto con redes de paquetes comunales, grandes redes corporativas, redes armadas, redes de depositarios, redes de corretaje de acciones y redes de reservas de aerolíneas.

Las características de los servicios de comunicación directa a una importancia y prominencia en la competencia de las técnicas de comunicación en los planes ideados de WAN. Es importante dominar la cantidad de tráfico. Muchas WAN también ponen en práctica complicadas medidas administrativas para informar sobre qué consumidor utiliza los recursos de la red. Esto se utiliza para producir información de facturación para fijar el precio del uso y el gasto de los consumidores individuales. La tasa de conducción se extendió de forma recurrente de 1200 bps a 6 Mbps; A pesar de que algunas conexiones como ATM y líneas arrendadas pueden ser utilizadas a velocidades avanzadas en comparación con 156 Mbps. Los contactos de comunicación estándar que participan en WAN son líneas telefónicas, enlaces de microondas y red de satélite. Los protocolos que comprenden paquetes sobre SONET / SDH, MPLS, ATM y

Frame relay son comúnmente empleados por proveedores de provisión para entregar las conexiones que se utilizan en WAN.

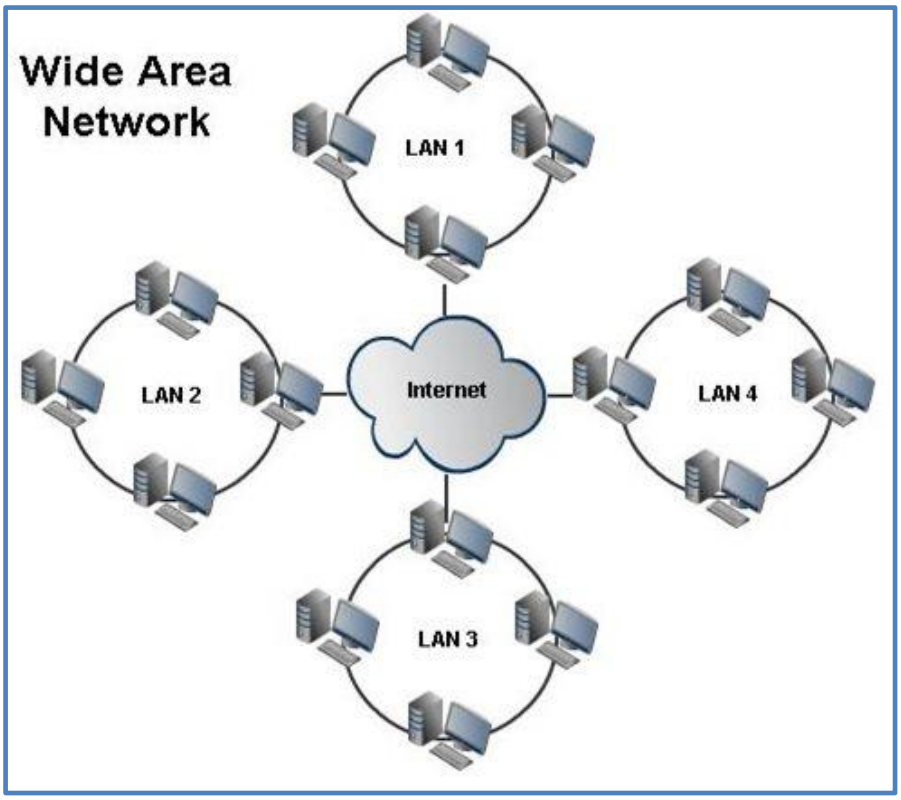

Figura No. 19 Wide Area Network

Fuente: http://www.mbaskool.com/2015_images/stories/may-images/kum-wan.jpg

2.20 DISEÑO JERARQUICO DE UNA RED

En la estructura jerárquica la red está organizada en capas que realizan tareas específicas, las ventajas de la implementación de este modelo es que los divide en capas con funciones similares y definidas para que el administrador de la red pueda añadir, reemplazar y eliminar elementos de la red. Este tipo de flexibilidad y adaptabilidad hace que la red sea escalable, un método idóneo para el diseño de una red.

2.20.1 VENTAJAS DEL USO DEL DISEÑO JERARQUICO

Este modelo de red divide el complejo problema del diseño de la misma en otros problemas más pequeños y manejables ya que cada nivel identifica un conjunto diferente de problemas en el hardware y software. Los dispositivos del primer nivel están diseñados para aceptar tráfico de una red y pasarlo hacia las capas superiores. Este diseño esta agrupado en tres capas: capa central, capa de distribución y capa de acceso.

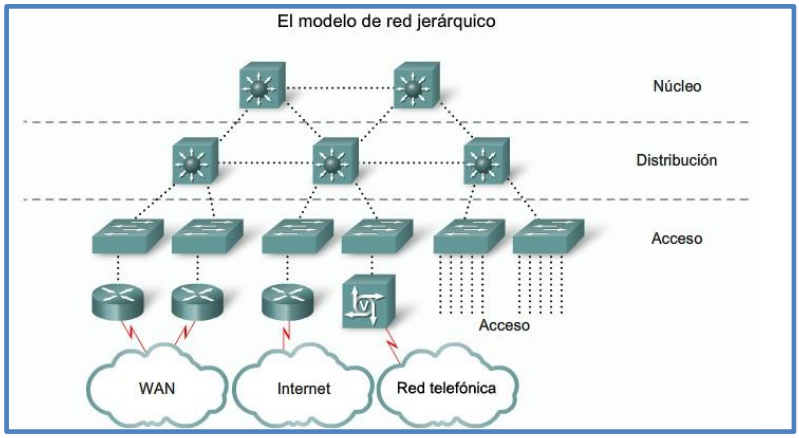

Figura No. 20 Modelo de Diseño Jerárquico

Fuente: http://3.bp.blogspot.com/-SdRo2H08ZRs/UTd8z-TNt4I/AAAAAAAAAfk/gUzF2KoltHw/s1600/toporedjerarquica.jpg

Debido a que los dispositivos de cada nivel tienen funciones similares y bien definidas, este modelo permite a los administradores de red añadir, reemplazar o eliminar elementos de la red de forma sencilla.

2.20.2 CAPA CENTRAL (CORE o NUCLEO)

Ofrece una estructura de transporte fiable y optimizado para reenviar el tráfico a altas velocidades, debe ser capaz de conmutar paquetes tan rápido como sea posible. Esta capa ofrece una ruta rápida entre sitios remotos, la cual no debería efectuar ninguna manipulación de paquetes como las listas de control de acceso.

2.20.3 CAPA DE DISTRIBUCION

Ofrece una definición de límites usando listas de acceso y otros filtros para limitar lo que entra en el núcleo, es decir en esta capa define las normas de red para manipular cierto tipo de tráfico que incluye las actualizaciones y resúmenes de enrutamiento, el tráfico VLAN y la incorporación de direcciones con el objetivo de preservar los recursos de tráfico innecesarios.

2.20.4 CAPA DE ACCESO

Es el punto a través del cual los usuarios pueden ingresar en la red. Es el punto de entrada a la red de las máquinas de los usuarios y servidores. Esta capa también puede usar listas de control de acceso o filtros para optimizar las necesidades de un grupo de usuarios, esta capa se encarga de:

- ✓ Ancho de banda compartido
- ✓ Ancho de banda conmutado
- ✓ Filtrado de la capa MAC
- ✓ Microsegmentación

3 IMPLEMENTACION DE LA RED LAN EN PALINDA

3.1 SITUACION ACTUAL DE PALINDA

En 2011 surgió PALINDA con una plataforma tecnológica básica en la cual funcionaba con los servicios de Internet tradicional como acceso al correo electrónico para poder chequear los pedidos, navegación por Internet, etc., funciones básicas que se requería en ese tiempo. Actualmente necesitamos una red con un conjunto de hardware y software en la cual se puedan comunicar las computadoras para compartir recursos como programas, impresión, discos, etc. Además, de enlazar a un sistema en donde se puedan almacenar todos los documentos electrónicos emitidos por los clientes de Palinda, ya que actualmente se manejan las retenciones de la fuente, facturas, comprobantes de pago, notas de crédito de manera electrónica. Para esto necesitamos empezar con un diagnóstico de nuestro espacio y los requerimientos, en este análisis abarca la parte lógica y física permitiendo identificar las necesidades y las ventajas de la infraestructura que vamos a implementar.

3.2 OBJETIVO

Nuestra meta es que Palinda pueda contar con todos los equipos de red y de usuario final con la arquitectura de *Cliente-Servidor* , permitiendo la distribución de información de manera eficiente y en tiempo real, para ello debemos:

- ✓ Identificar y establecer las necesidades de cada departamento
- ✓ Determinar la cantidad de estaciones de trabajo
- ✓ Realizar el estudio de costos para la implementación de los equipos

- ✓ Diseñar la LAN
- ✓ Instalación y configuración de la red

3.2.1 RAZONES BASICAS PARA ESTABLECER LA RED

- ✓ **Compartir de Base de Datos:** debido a que se manejan con diferentes clientes, productos, costos, se ha implementado un sistema de gestión de bases de datos para permitir a los usuarios dentro de la empresa acceder a los archivos en diferentes puntos.

- ✓ **Compartir recursos de red:** Para optimizar equipos, la red proporciona un enlace de comunicación. Entre los recursos de red que se requiere compartir son las impresoras Zebra ZT-230, dispositivos de almacenamiento y los recursos de comunicación.

- ✓ **Compartir Programas y archivos:** Estos programas y archivos que requiere la empresa, se guardan en un Servidor de Archivos, al cual los usuarios dentro de la red pueden acceder. La compra de licencias de software dentro de un servidor representa un ahorro significativo para la empresa, en vez de adquirir el software para cada equipo.

- ✓ **Separar las diferentes áreas:** La red proporciona la creación de varios grupos, dependiendo de la función y estructura de la empresa, permitiéndole operar y acceder a la información de acuerdo al campo dado.

- ✓ **Correo electrónico:** Para facilitar la comunicación entre cada usuario se ha implementado un servidor Microsoft Exchange en la cual se incluyó calendarios,

agenda de citas, reuniones, programación de tareas, recordatorios entre otros servicios.

3.3 DISEÑO LAN PARA PALINDA

El presente diseño de la red, se basa en un estudio para mejorar el rendimiento de los equipos y la capacidad del medio, debemos diseñar una red que tenga tendencia escalable permitiendo la interconexión con todos los departamentos de la organización, por lo que resulta fundamental conocer el tipo de tráfico que se requiere para cada departamento.

Una red precisa no solo de conectar computadoras, sino es un proceso que mantiene características que la haga manejable, fiable y escalable, por lo que el primer paso del diseño de una LAN es establecer y documentar los objetivos del mismo. Nuestra red para PALINDA debe considerar como objetivos las siguientes características:

3.3.1 Funcionalidad:

La red Palinda debe ser capaz de conectar todos los puntos de red de los diferentes departamentos para poder comunicarse de usuario a usuario e usuario a aplicación con una velocidad con una latencia mínima y fiabilidad razonable, es decir que los datos lleguen al destino.

3.3.2 Escalabilidad

Nuestra red debe ser capaz de crecer, por lo que es importante diseñar para poder realizar futuros cambios a nuestra red inicial. En estos seis años, Palinda está creciendo exponencialmente las ventas y con clientes de diferentes sectores, por lo que vamos a diseñar una red con un alto potencial de crecimiento.

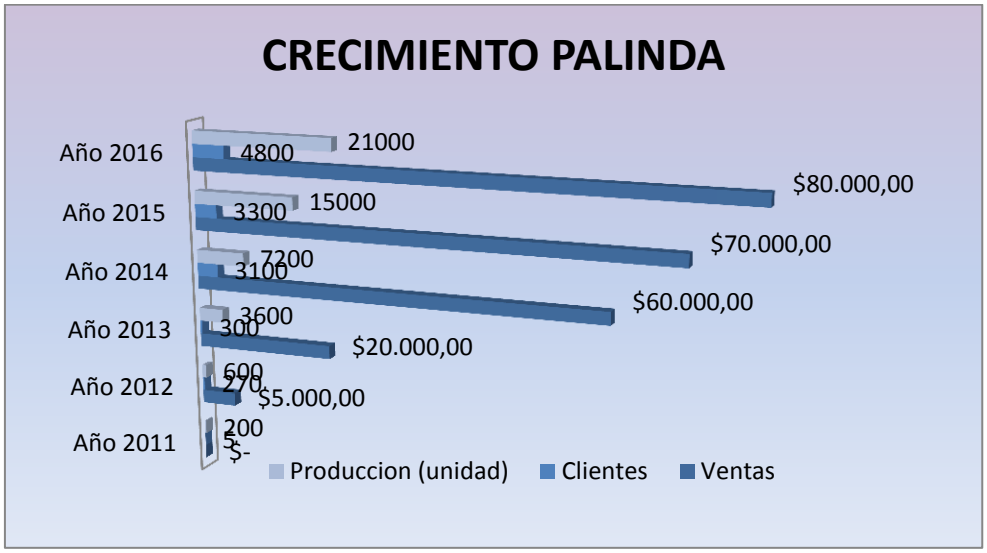

Tabla 1 Crecimiento de Palinda

3.3.3 Adaptabilidad

Nuestra red va a estar diseñada para adaptar tecnología futura, tenemos planeado crecer a nivel nacional, por lo que diseñaremos la red para llegue a un área geográficamente extensa cuando llegue el momento de implementar un enlace WAN.

3.3.4 Manejabilidad

Vamos a diseñar la red para que sea fácil monitorizar y gestionar. Es por eso que debemos definir las funciones de los usuarios y de los servidores.

3.4 ANALISIS DE REQUISITOS Y EXPECTATIVAS DE LA RED PALINDA

Con el rápido crecimiento y la evolución de las tecnologías de alta velocidad en comunicaciones, nos hemos visto en la necesidad de implementar la red para maximizar el ancho de banda, rendimiento, las funciones de los usuarios, la ubicación de los

servidores, la segmentación de los dominios de colisión, por lo que debemos diseñar la estructura topología en capa 1, 2 y 3.

3.4.1 ESTRUCTURA ORGANIZACIONAL

Palinda requiere el diseño y la administración de la red, que de acuerdo a cada función se dividirá en diferentes departamentos, las cuales cada usuario tendrá asignado un punto de red con acceso ya sea a Pc o laptops para poder realizar su trabajo.

Como fundadora de Palinda y administradora de la red, he visto la necesidad de crear un departamento de Contabilidad, Sistemas, Ventas y Gerencia. Actualmente Palinda cuenta con la Planta Procesadora, Bodega y Recepción.

- ✓ FUNCIONES DEL GERENTE:
    a) Nombrar y remover los empleados
    b) Toma de decisiones

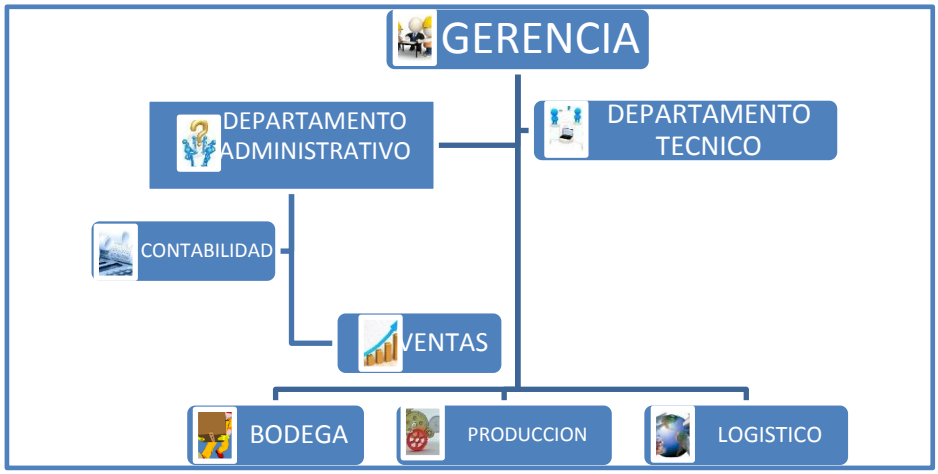

Figura No. 21 Organigrama de la Empresa

Fuente: Elaboración Propia

La infraestructura local permitirá el acceso a los recursos de acuerdo a su nivel de autorización. Como administradora de red otorgaré privilegios a los grupos y de manera individual a los usuarios que lo requieran. Además, con las autorizaciones a acceso de los recursos de red, optimizaré el uso de los recursos en conjunto con un adecuado balanceo de carga y dimensionamiento de enlaces.

Para del Departamento de Contabilidad, que se encarga de administrar los activos y pasivos, recaudando las ventas y pagando todos los impuestos de ley, además de realizar el registro y control de las transacciones de todos los movimientos de recursos presupuestarios. Por las funciones que realiza este departamento, debo configurar acceso al servidor de Aplicaciones y el Servidor de Archivos e Impresión.

En Gerencia, que se encarga de dirigir y gestionar los asuntos del funcionamiento de Palinda, debe coordinar los recursos internos, representar a la compañía y controlar las metas y objetivos, para esto debe acceder a toda la información almacenada en el servidor de archivos y acceso al servidor de aplicaciones donde podrá revisar el sistema de inventarios, facturación, pedidos, etc.

En Bodega pondremos un punto de red conectado a una computadora con acceso al servidor de Aplicaciones para poder chequear el inventario de los productos que ingresan y de los productos que salen, para tener un mejor control en el momento de adquirir la materia prima para la elaboración.

Para el Departamentos de Ventas controlaremos el tráfico hacia el servidor de archivos e impresiones, este departamento será el encargado de ingresar y mantener la base de datos de nuestros clientes.

3.5 DISEÑAR LA TOPOLOGIA O ESTRUCTURA DE LA LAN

El sistema eléctrico de PALINDA está ubicado en la planta baja con acceso restringido en la cual dispone de una alimentación eléctrica hacia la red pública con conexiones de sistema trifásico con un medidor de energía eléctrica. Cada puesto de trabajo debe contar con un conector RJ-45. Para este diseño, no solamente debemos considerar la carga eléctrica de los equipos que vamos a implementar como Swiches, estaciones de trabajo, impresoras, servidores, sino que se debe construir un sistema de alimentación independiente para cualquier otra carga eléctrica con el fin de evitar variaciones en el voltaje afectando las interferencias por el ruido eléctrico producido por otros equipos. Es necesario que la Red Eléctrica para el equipo de Telecomunicaciones y Estaciones de Trabajo, este instalado con capacidad de crecimiento para poder atender a las futuras demandas.

El cableado de datos que vamos a instalar es el cable UTP de categoría 5 (CAT 5). El cable UTP es un tipo de cable de par trenzado que no se encuentran blindado, es fácil de instalar y es menos costoso, el cable de cada par trenzado esta alrededor del otro para impedir interferencias electromagnéticas, la longitud máxima es de 100m sin utilizar ningún tipo de regeneración de señal. Se incluye el transporte de voz y datos.

El punto de demarcación es el lugar donde se conecta los cables del distribuidor externo junto con los equipos internos de la empresa. En este caso hay tres proveedores externos: uno de Telconet, para el servicio de Internet, otro de le Empresa Eléctrica y otra de Andinatel para la Telefonía fija. Telconet ofrece la tecnología de fibra óptica multimodo en la última milla para proveer servicio de Internet.

En el siguiente esquema describe los planos de Palinda:

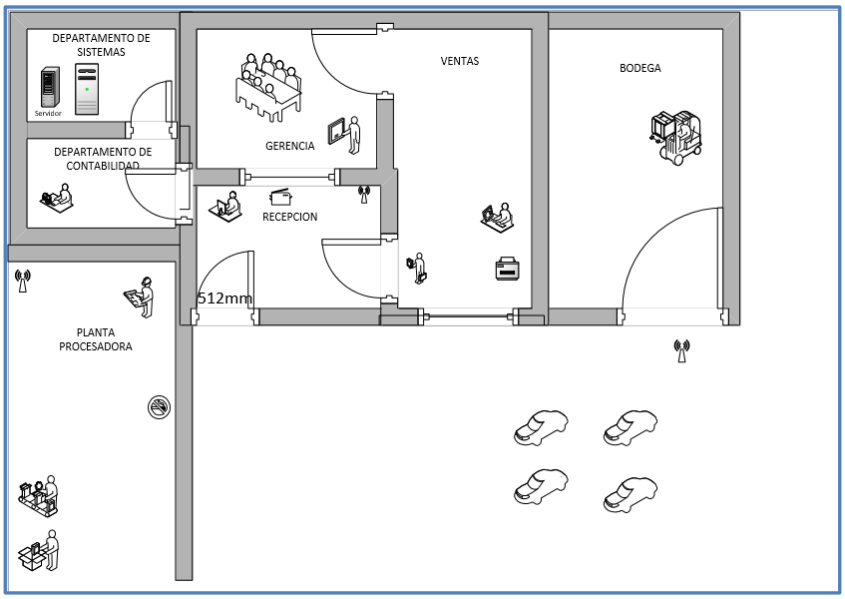

Figura No. 22

Fuente Elaboración propia en Microsoft Visio

En el siguiente esquema describe la Topología de la Red Palinda:

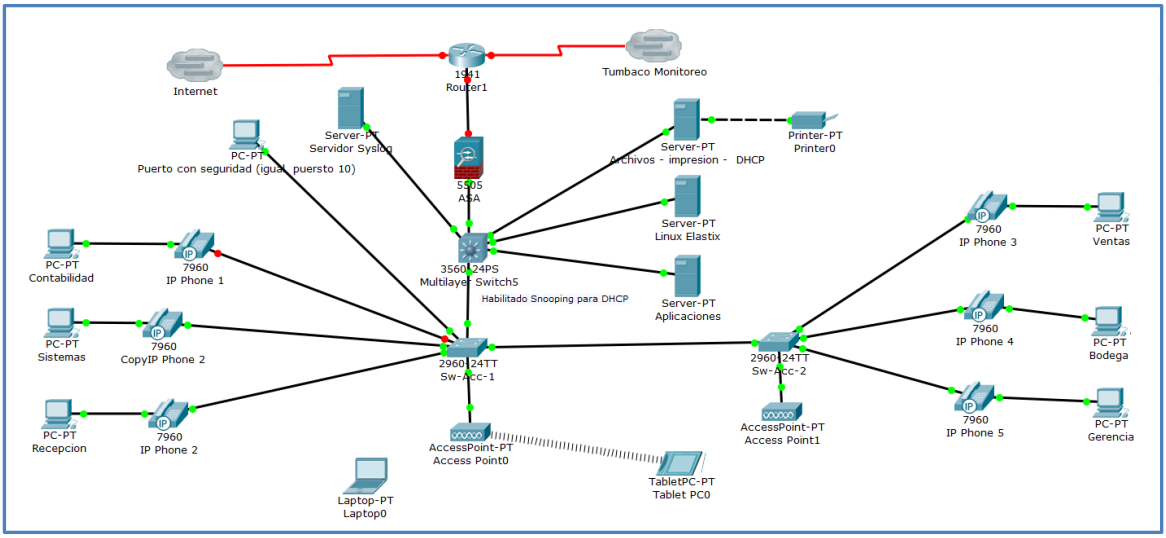

Figura No. 23 Red PALINDA

Fuente Elaboración Propia desde el Packet Tracer

3.6 NOMBRAR LAS SWITCHES DE ACCESO Y DE DISTRIBUCION

Nombrar los switch de acceso 1

```
Switch>en
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Sw-Acc-1
Sw-Acc-1(config)#end
Sw-Acc-1#
%SYS-5-CONFIG_I: Configured from console by console
copy run st
Destination filename [startup-config]?
Building configuration...
[OK]
Sw-Acc-1#
```

Nombrar al switch de acceso 2

```
Switch>en
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Sw-Acc-2
Sw-Acc-2(config)#end
Sw-Acc-2#
%SYS-5-CONFIG_I: Configured from console by console
copy run st
Destination filename [startup-config]?
Building configuration...
[OK]
Sw-Acc-2#
Sw-Acc-2#
```

Nombrar el switch de distribución

```
Switch>en
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname Sw-Dis-1
Sw-Dis-1(config)#end
Sw-Dis-1#
%SYS-5-CONFIG_I: Configured from console by console
copy run st
Destination filename [startup-config]?
Building configuration...
[OK]
Sw-Dis-1#

Sw-Dis-1#
```

3.7 CREAR VLAN

Vamos a crear VLAN para agrupar las diferentes estaciones de trabajo de acuerdo a la función y de los servidores además de mejorar la eficiencia de la red en un menor consumo de ancho de banda de la LAN

NUMERO DE VLAN	NOMBRE
110	SISTEMAS
120	GERENCIA
130	CONTABILIDAD
140	VENTAS
150	BODEGA
160	RECEPCION
170	SERVIDORES
180	Voip
190	WIFI
100	VLAN NATIVA

Tabla 2 Asignación de Nombres a las VLAN

3.7.1 CONFIGURACION DE LAS VLAN

Las VLAN se configuran en el Switch de la Capa de Distribución y se propagan a través de VTP a los Switches de la Capa de Acceso.

En los Switches de la Capa de Acceso se asocia cada puerto con la VLAN especifica.

Para configurar se introduce los siguientes comandos:

```
Sw-Dis-1>en
Password:
Password:
Sw-Dis-1#confi term
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Dis-1(config)#vlan 110
Sw-Dis-1(config-vlan)#name Sistemas
Sw-Dis-1(config-vlan)#exit
Sw-Dis-1(config)#

Sw-Dis-1(config)#vlan 120
```

```
Sw-Dis-1(config-vlan)#name Gerencia
Sw-Dis-1(config-vlan)#exit
Sw-Dis-1(config)#

Sw-Dis-1(config)#vlan 130
Sw-Dis-1(config-vlan)#name Contabilidad
Sw-Dis-1(config-vlan)#exit
Sw-Dis-1(config)#
```

Para asociar las VLAN en cada uno de los puertos se implementa la siguiente configuración en cada uno de los Switches de la Capa de Acceso:

En el switch de Acceso 1:

```
Sw-Acc-1#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Acc-1(config-if)#interface FastEthernet0/10
Sw-Acc-1(config-if)#description Usuario Contabilidad
Sw-Acc-1(config-if)#switchport access vlan 130
!
Sw-Acc-1#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Acc-1(config-if)#interface FastEthernet0/11
description Usuario Sistemas
switchport access vlan 110
!
Sw-Acc-1#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Acc-1(config-if)#interface FastEthernet0/12
Sw-Acc-1(config-if)#description Usuario Recepcion
Sw-Acc-1(config-if)#switchport access vlan 160
!
Sw-Acc-1#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Acc-1(config-if)#interface FastEthernet0/13
Sw-Acc-1(config-if)#description Usuario Red Inalambrica
Sw-Acc-1(config-if)#switchport access vlan 190
```

En el switch de acceso 2 también se debe configurar

```
Sw-Acc-2#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Acc-2(config-if)#interface FastEthernet0/10
Sw-Acc-2(config-if)#description Usuario Ventas
Sw-Acc-2(config-if)#switchport access vlan 140
!
Sw-Acc-2#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Sw-Acc-2(config-if)#interface FastEthernet0/11
description Usuario Bodegas
switchport access vlan 150
!
Sw-Acc-2#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Acc-2(config-if)#interface FastEthernet0/12
Sw-Acc-2(config-if)#description Usuario Gerencia
Sw-Acc-2(config-if)#switchport access vlan 120
!
Sw-Acc-2#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Acc-2(config-if)#interface FastEthernet0/13
Sw-Acc-2(config-if)#description Usuario Red Inalambrica
Sw-Acc-2(config-if)#switchport access vlan 190
```

Verificación de las VLAN creadas en el Switch de Acceso 1

```
Sw-Acc-1#show vlan

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/2, Fa0/3, Fa0/4, Fa0/5
Fa0/6, Fa0/7, Fa0/8, Fa0/9
Fa0/14, Fa0/15, Fa0/16, Fa0/17
Fa0/18, Fa0/19, Fa0/21, Fa0/22
Fa0/23, Gig0/1, Gig0/2
100 Native active
110 Sistemas active
120 Gerencia active
130 Contabilidad active Fa0/10
140 Ventas active
150 Bodega active
160 Recepcion active
170 Servidores active
180 VoIP active
190 Wifi active Fa0/13, Fa0/20
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active
1005 trnet-default active

--More—
```

Verificación de las VLAN creadas en el Switch de Acceso 2

```
Sw-Acc-2#
%SYS-5-CONFIG_I: Configured from console by console
show vlan

VLAN Name Status Ports
---- -------------------------------- --------- -------------------------------
1 default active Fa0/1, Fa0/2, Fa0/3, Fa0/4
Fa0/5, Fa0/6, Fa0/7, Fa0/8
Fa0/9, Fa0/10, Fa0/11, Fa0/12
```

Fa0/13, Fa0/14, Fa0/15, Fa0/16
Fa0/17, Fa0/18, Fa0/19, Fa0/20
Fa0/21, Fa0/22, Fa0/23, Gig0/1
Gig0/2
100 Native active
110 Sistemas active
120 Gerencia active
130 Contabilidad active
140 Ventas active
150 Bodega active
160 Recepcion active
170 Servidores active
180 VoIP active
190 Wifi active
1002 fddi-default active
1003 token-ring-default active

--More—

Verificación de las VLAN creadas en el Switch de Distribución 1

Sw-Dis-1>en
Password:
Sw-Dis-1#show vlan

VLAN Name Status Ports
---- ---------- --------- ----------
1 default active Fa0/2, Fa0/3, Fa0/4, Fa0/5
Fa0/6, Fa0/7, Fa0/8, Fa0/9
Fa0/10, Fa0/11, Fa0/12, Fa0/13
Fa0/14, Fa0/15, Fa0/16, Fa0/17
Fa0/18, Fa0/19, Fa0/20, Fa0/21
Fa0/23, Fa0/24, Gig0/1, Gig0/2
100 Native active
110 Sistemas active
120 Gerencia active
130 Contabilidad active Fa0/22
140 Ventas active
150 Bodega active
160 Recepcion active
170 Servidores active
180 VoIP active
190 Wifi active
1002 fddi-default active
1003 token-ring-default active
1004 fddinet-default active

--More—

Definimos la VLAN nativa como VLAN 100 y la configuramos en los puertos que conectan los switches de Acceso y Distribución. Adicional se debe configurar el puerto como un puerto troncal.

```
Sw-Dis-1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Dis-1(config)#interface fastEthernet 0/1
Sw-Dis-1(config-if)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to "trunk"
mode.
Sw-Dis-1(config-if)#switchport trunk native vlan 100
Sw-Dis-1(config-if)#
Sw-Dis-1#
%SYS-5-CONFIG_I: Configured from console by console
```

El mensaje de error que se muestra es porque el tipo de switch que se ha escogido acepta configuraciones automáticas.

```
Sw-Acc-1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Acc-1(config)#interface fastEthernet 0/2
Sw-Acc-1(config-if)#switchport mode trunk
Sw-Acc-1(config-if)#switchport trunk native vlan 100
Sw-Acc-1(config-if)#
Sw-Acc-1#
%SYS-5-CONFIG_I: Configured from console by console
```

```
Sw-Acc-2#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Acc-2(config)#interface fastEthernet 0/2
Sw-Acc-2(config-if)#switchport mode trunk
Sw-Acc-2(config-if)#switchport trunk native vlan 100
Sw-Acc-2(config-if)#
Sw-Acc-2#
%SYS-5-CONFIG_I: Configured from console by console
```

3.8 CONFIGURACION VTP (VLAN TRUNKING PROTOCOL)

Para la correcta propagación de las VLAN implementaremos el protocolo VTP en el switch de distribución el cual será el servidor VTP y los switches de acceso será cliente VTP.

```
Sw-Dis-1 (config)#vtp domain Palinda
Changing VTP domain name from NULL to Palinda
Sw-Dis-1 (config)#vtp password cisco
Setting device VLAN database password to cisco
Sw-Dis-1 (config)#
Sw-Dis-1 (config)#vtp version 2
Sw-Dis-1(config)#vtp mode server
```

```
Sw-Dis-1#show vtp status
VTP Version : 2
```

```
Configuration Revision : 31
Maximum VLANs supported locally : 1005
Number of existing VLANs : 15
VTP Operating Mode : Server
VTP Domain Name : Palinda
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x76 0x82 0x1B 0xFA 0x89 0xAC 0xC1 0xF0
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 192.168.100.1 on interface Vl1 (lowest numbered VLAN interface found)
```

En los switch de acceso debemos configurar y verificar que está en modo cliente

```
Sw-Acc-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Acc-1(config)#vtp mode client
Device mode already VTP CLIENT.
Sw-Acc-1(config)#
Sw-Acc-1#
%SYS-5-CONFIG_I: Configured from console by console
 Sw-Acc-1>en
Sw-Acc-1#show vtp status
VTP Version : 2
Configuration Revision : 31
Maximum VLANs supported locally : 255
Number of existing VLANs : 15
VTP Operating Mode : Client
VTP Domain Name : Palinda
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x76 0x82 0x1B 0xFA 0x89 0xAC 0xC1 0xF0
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Sw-Acc-1#
```

```
Sw-Acc-2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Acc-2(config)#vtp mode client
Device mode already VTP CLIENT.
Sw-Acc-2(config)#
Sw-Acc-2#
%SYS-5-CONFIG_I: Configured from console by console
 Sw-Acc-2>en
Sw-Acc-2#show vtp status
VTP Version : 2
Configuration Revision : 31
Maximum VLANs supported locally : 255
Number of existing VLANs : 15
VTP Operating Mode : Client
VTP Domain Name : Palinda
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x76 0x82 0x1B 0xFA 0x89 0xAC 0xC1 0xF0
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

3.8.1 VERIFICACION DE LA CONFIGURACION DE LOS PUERTOS TRONCALES

Sw-Acc-1#show interfaces fastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
Sw-Acc-1#show interfaces fastEthernet 0/15 switchport
Name: Fa0/15
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none
Sw-Acc-1#show interfaces fastEthernet 0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk

Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 110 (Sistemas)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: 180
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
Protected: false
Appliance trust: none

3.9 DIRECCIONAMIENTO IP

En este entorno de red, las estaciones finales se comunican con los servidores, los hosts u otras estaciones finales, ya que cada nodo debe poseer una dirección lógica de 32 bits única conocida como dirección IP. La red lo vamos a segmentar en una serie de pequeñas redes llamadas subredes.

El direccionamiento lógico de Capa 3 en nuestra LAN, debe planificarse y documentarse aunque se asignen las direcciones IP de manera automática con un servidor DHCP, para evitar las duplicaciones de direcciones IP y para cuando crezca la red.

Vamos a utilizar la red privada 192.168.1.0

1	2	3	4	5	6	7	8	bits prestados
128	64	32	16	8	4	2	1	variación
128	192	224	240	248	252	254	255	mascara de red

Para cubrir las necesidades de direccionamiento IP, necesitamos 7 subredes, 1 por cada departamento de la Palinda, la fórmula para obtener 7 subredes es:

$2^n \geq 7$, en donde n es la cantidad de bits que se tomaron prestados. Así que tomaremos 3 bits prestados.

$2^3 = 8$, con esta fórmula obtendremos 8 subredes.

Con los 5 bits restantes, con la siguiente formula obtendremos la cantidad de host por subred

$2^n - 2 =$ número de host disponible /subred

$2^5 - 2 =$ 30 host / subred

Con estos datos, nuestra red es 192.168.1.0 255.255.255.224

En la siguiente tabla se plantea un esquema de direccionamiento de nuestra red.

Dirección de red	Dirección de broadcast	Rango de direcciones IP utilizables	Departamento	
192.168.1.0	162.168.1.31	192.168.1.1 - 192.168.1.30	Gerencia	
192.168.1.32	192.168.1.63	192.168.1.33 - 192.168.1.62	Contabilidad	
192.168.1.64	192.168.1.95	192.168.1.63 - 192.168.1.94	Sistemas	
192.168.1.96	192.168.1.127	192.168.1.97 - 192.168.1.126	Ventas	
192.168.1.128	192.168.1.159	192.168.1.161 - .192.168.1.158	Recepción	
192.168.1.160	192.168.1.191	192.168.1.161 - 192.168.1.190	Bodega	
192.168.1.192	192.168.1.223	192.168.1.193 - 192.168.1.222	WIFI	
192.168.1.224	192.168.1.256	192.168.1.225 - 192.168.1.255	Logística	No asignado, reservado

Tabla 3 Rango de Direcciones IP

3.9.1 VLSM A LA RED GERENCIA

Para el rango de direcciones asignado al Departamento de Gerencia, vamos a subnetear para tener suficientes direcciones IP para nuestros servidores, impresoras y dispositivos de red, además si llegara a crecer exponencialmente Palinda, se crearía nuevos puestos para los diferentes Gerencias, con el subeneteo ya no sería un problema en el momento de requerir direcciones IP.

Vamos a requerir 6 host por cada subred 192.168.1.0 255.255.255.224. Para esto pediremos prestados 3 bits:

1	2	3	4	5	6	7	8	bits prestados
128	64	32	16	8	4	2	1	variación
128	192	224	240	248	252	254	255	mascara de red

$2^3 - 2 =$ 6 host / subred

Nuestra red Gerencia quedaría con máscara /29: 192.168.1.0 255.255.255.248

En la siguiente tabla se detalla el direccionamiento IP de la subred Gerencia con máscara /29

Direccion de subred	Direccion de broadcast	Rango de direcciones IP utilizables	
192.168.1.0	162.168.1.7	192.168.1.1 - 192.168.1.6	Gerencia
192.168.1.8	192.168.1.15	192.168.1.8 - 192.168.1.14	Servidores
192.168.1.16	192.168.1.23	192.168.1.17 - 192.168.1.22	Switches y Router
192.168.1.24	192.168.1.31	192.168.1.25 - 192.168.1.30	Access Point - Impresoras

Tabla 4 *Subneteo de la Red Gerencia*

3.9.2 CONFIGURAR DHCP

Para nuestra red, vamos a excluir las direcciones que van a ser estáticas, por ejemplo para nuestros servidores, switches, impresora, routers, Access point.

```
Sw-Dis-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sw- Dis -1(config)#ip dhcp excluded-address 192.168.1.8 255.255.255.248
Sw- Dis -1(config)#ip dhcp excluded-address 192.168.1.16 255.255.255.248
Sw- Dis -1(config)#ip dhcp excluded-address 192.168.1.24 255.255.255.248
Sw- Dis -1(config)#
Sw- Dis -1#
%SYS-5-CONFIG_I: Configured from console by console

Sw- Dis -1(config)#ip dhcp pool Recepcion
Sw- Dis -1(dhcp-config)#network 192.168.1.128 255.255.255.224
Sw- Dis -1(dhcp-config)#default-router 192.168.1.129
Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4
Sw- Dis -1(config)#ip dhcp pool Sistemas
Sw- Dis -1(dhcp-config)#network 192.168.1.64 255.255.255.224
Sw- Dis -1(dhcp-config)#default-router 192.168.1.65
Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4
Sw- Dis -1(config)#ip dhcp pool Contabilidad
Sw- Dis -1(dhcp-config)#network 192.168.1.32 255.255.255.224
Sw- Dis -1(dhcp-config)#default-router 192.168.1.33
Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4
Sw- Dis -1(config)#ip dhcp pool Gerencia
Sw- Dis -1(dhcp-config)#network 192.168.1.0 255.255.255.248
Sw- Dis -1(dhcp-config)#default-router 192.168.1.1
Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4
Sw- Dis -1(config)#ip dhcp pool Ventas
Sw- Dis -1(dhcp-config)#network 192.168.1.96 255.255.255.224
Sw- Dis -1(dhcp-config)#default-router 192.168.1.97
Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4
Sw- Dis -1(config)#ip dhcp pool Bodega
Sw- Dis -1(dhcp-config)#network 192.168.1.160 255.255.255.224
Sw- Dis -1(dhcp-config)#default-router 192.168.1.161
Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4
Sw- Dis -1(config)#ip dhcp pool Produccion
Sw- Dis -1(dhcp-config)#network 192.168.1.192 255.255.255.224
Sw- Dis -1(dhcp-config)#default-router 192.168.1.193
Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4
Sw- Dis -1(config)#ip dhcp pool Logistica
Sw- Dis -1(dhcp-config)#network 192.168.1.224 255.255.255.224
Sw- Dis -1(dhcp-config)#default-router 192.168.1.225
Sw- Dis -1(dhcp-config)#dns-server 8.8.4.4
!
```

3.10 POLITICAS DE SEGURIDAD

3.10.1 ACCESS-LIST

Como es vital el acceso al Internet debemos asegurar nuestra red ante amenazas, podemos crear una lista de acceso que restringe el acceso a los dispositivos en rangos de tiempo fuera de oficina.

Para esto vamos a crear una lista de acceso por tiempo, la cual se va a activar a una hora especifica denegando el acceso a un sitio especifico, para nuestro caso en el Facebook, se desactivará luego de la jornada laboral, es decir desde las 17h00 de lunes a viernes.

Lo primero que se debe hacer es definir un rango de tiempo, pero para esto se debe definir la fecha y hora del equipo con el comando Clock Set, como se lo realizo en el caso del syslog.

Sw-Dis-1(config)#Time-range DIASLABORABLES

Sw-Dis-1(config-time-range)#periodic Monday Tuesday Wednesday Thursday Fridays 08:00 to 17:00

Previamente debemos descubrir la dirección IP de Facebook con el comando NSLOOKUP www.facebook.com en una ventana de comandos.

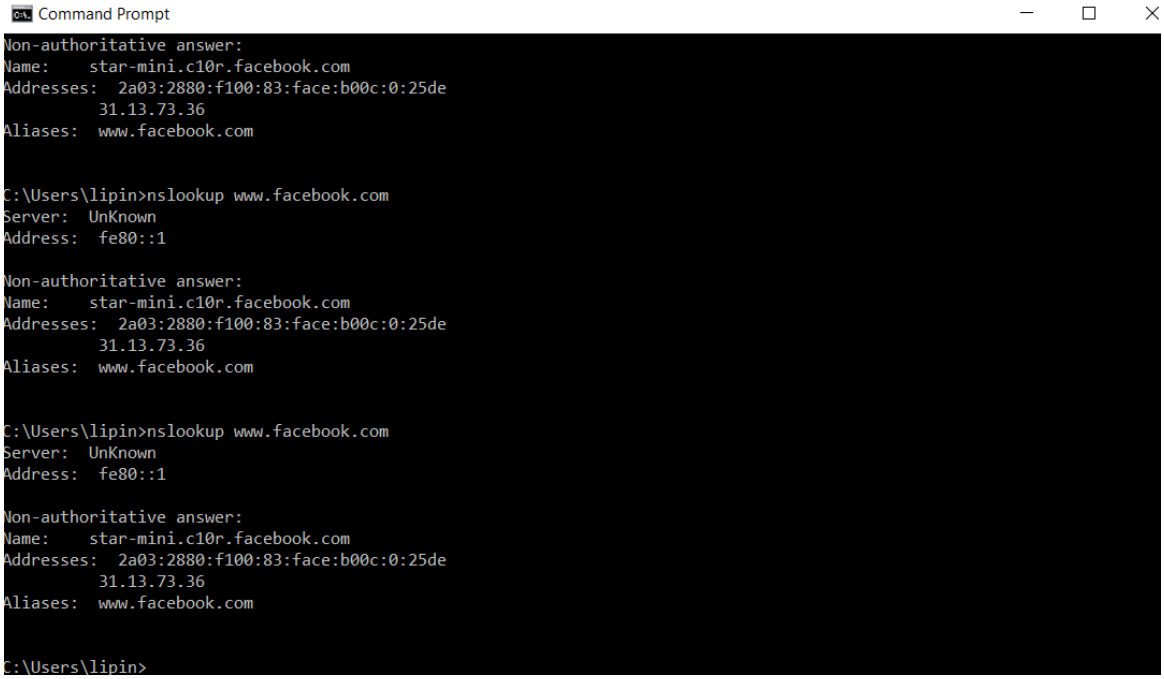

Figura No. 24 Busqueda de Direccion IP de Facebook

FUENTE PROPIA

Creamos la lista de acceso:

Sw-Dis-1(config)#access-list 150 deny TCP 192.168.1.0 0.0.255.255 31.13.73.36 time-range DIASLABORABLES

El siguiente paso es aplicarla la lista de control de acceso a la interfaz de salida con el siguiente comando:

Sw-Dis-1(config)#interface f0/2

Sw-Dis-1(config-if)#ip access-group 150 out

3.10.2 SEGURIDAD DE LOS PUERTOS DE LOS SWITCHES DE ACCESO

Los puertos de Switch de Acceso se deben asegurar, ya que son accesibles a través del cableado estructurado de las tomas, cualquier intruso puede conectar un PC o laptop. Los puertos del switch es un punto de entrada potencial a usuarios sin autorización.

CONFIGURACION DEL SWITCHPORT SECURITY EN LA INTERFACE FASTEHTERNET 0/5

```
Sw-Acc-1#conf ter
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Acc-1(config)#inter fastEthernet 0/5
Sw-Acc-1(config-if)#switchport mode access
Sw-Acc-1(config-if)#switchport port-security maximum 1
Sw-Acc-1(config-if)#switchport port-security violation shutdown
Sw-Acc-1(config-if)#switchport port-security mac-address sticky
Sw-Acc-1(config-if)#
Sw-Acc-1#
%SYS-5-CONFIG_I: Configured from console by console
```

VERIFICACION DE LOS PUERTOS ASEGURADOS

```
Sw-Acc-1#show port-security interface fastEthernet 0/5
Port Security              : Enabled
Port Status                : Secure-down
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0000.0000.0000:0
Security Violation Count   : 0

Sw-Acc-1#show port-security interface fastEthernet 0/10
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 3
```

```
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 1
Last Source Address:Vlan   : 0030.A338.4D92:1
Security Violation Count   : 0

Sw-Acc-1#sh port-security interface fastEthernet 0/6
Port Security : Enabled
Port Status : Secure-down
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0


Sw-Acc-1#show port-security address
  Secure Mac Address Table
------------------------------------------------------------------------------
Vlan Mac Address Type   Ports  Remaining Age
      (mins)
---- ----------- ----   -----  -------------
1 0007.EC18.3B8B SecureSticky  FastEthernet0/10  -
1 0030.A338.4D92 DynamicConfigured FastEthernet0/10  -
------------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 1024
Sw-Acc-1#
```

3.10.2.1 SYSLOG

Este protocolo informa la actividad, eventos y condiciones de error de los equipos y sus procesos enviando mensajes, que contiene la información del evento, a un dispositivo o búfer a la consola del equipo.

Se recomienda usar el comando service time-stamps para añadir una marca horaria a cada evento que genere el equipo, de esta manera tendremos la seguridad de la hora y fecha en la que se suscitó el evento. Para poder lograr esto es necesario configurar la hora en el equipo, sea a través del comando CLOCK SET o configurando un servidor NTP.

```
User Access Verification

Password:

Sw-Dis-1>ena
Password:
Password:
Password:
% Bad secrets

Sw-Dis-1>en
Password:
Password:
Password:
Sw-Dis-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Dis-1#clock set 12:48:12 5 may 2017
Sw-Dis-1#conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Dis-1(config)#service timestamps log datetime msec
Sw-Dis-1(config)#logging on
Sw-Dis-1(config)#logging trap debugging
Sw-Dis-1(config)#logging 192.168.100.100
Sw-Dis-1(config)#logging host 192.168.100.100

Sw-Dis-1(config)#


Sw-Dis-1#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
        0 flushes, 0 overruns, xml disabled, filtering disabled)
No Active Message Discriminator.

No Inactive Message Discriminator.

   Console logging: level debugging, 66 messages logged, xml disabled,
        filtering disabled
   Monitor logging: level debugging, 66 messages logged, xml disabled,
        filtering disabled
   Buffer logging:  disabled, xml disabled,
        filtering disabled
   Logging Exception size (4096 bytes)
   Count and timestamp logging messages: disabled
   Persistent logging: disabled
No active filter modules.
ESM: 0 messages dropped
   Trap logging: level debugging, 66 message lines logged
      Logging to 192.168.200.100  (udp port 514,  audit disabled,
           authentication disabled, encryption disabled, link up),
           8 message lines logged,
           0 message lines rate-limited,
           0 message lines dropped-by-MD,
           xml disabled, sequence number disabled
           filtering disabled
      Logging to 192.168.100.100  (udp port 514,  audit disabled,
           authentication disabled, encryption disabled, link up),
           6 message lines logged,
           0 message lines rate-limited,
           0 message lines dropped-by-MD,
           xml disabled, sequence number disabled
```

filtering disabled

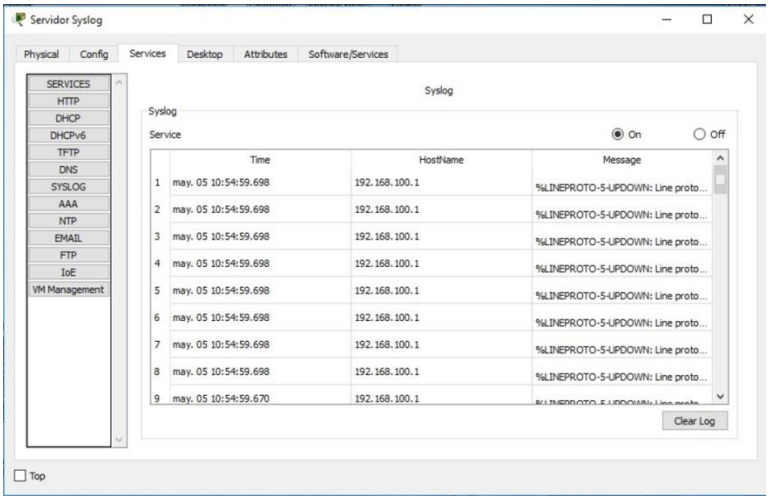

Figura No. 25 Captura del Servidor Syslog

Fuente Servidor Syslog del packet tracer

3.11 NAT (NETWORK ADDRESS TRANSLATION)

Para acceder al Internet, el proveedor de servicios Telconet nos asignaron un rango de Direcciones IP Publicas:147.60.50.160 hasta147.60.50.163 con la máscara 255.255.255.252.

Este rango se va ingresar con el siguiente comando:

Ip nat pool NAT-PALINDA 147.60.50.160 147.60.50.169 netmask 255.255.255.252 en modo de configuración global.

El siguiente paso es definir el tráfico que va a someterse a la traducción, en nuestro caso son todas las direcciones de las subredes 192.168.1.0 /27 y se lo hara con una acces list estándar:

Access-list 1 permit 192.168.0.0 0.0.0.255.255

Y después el siguiente paso es asociar la lista de control del acceso con el pool creado con el siguiente comando y sobrecargarlo

ip nat inside source list pool NAT-PALINDA overload

Una vez creado el pool y clasificado el trafico, debemos definer las interface de entrada de trafico y salida de trafico, en nuestro caso la interfaz de entrada es a Fastethernet 0/1 del Switch Capa 3 3560.

```
Sw-Dis-1>en
Password:
Password:
Sw-Dis-1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Dis-1(config)#interface fastEthernet 0/1
Sw-Dis-1(config-if)#ip nat inside
Sw-Dis-1(config-if)#
Sw-Dis-1#
```

Como estamos configurando en un switch de capa 3 se debe convertir el puerto en un puerto ruteo para que soporte el comando NAT con el siguiente comando.

```
Sw-Dis-1(config-if)#no switchport
Sw-Dis-1(config-if)#
```

El siguiente paso es definir el puerto externo que conecta al internet, este es el puerto fastethernet 0/2 del switch capa 3 3560, previamente se lo debe convertir en un puerto de ruteo con el comando

```
Sw-Dis-1(config-if)#no switchport
Sw-Dis-1>en
Password:
Password:
Sw-Dis-1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
Sw-Dis-1(config)#interface fastEthernet 0/2
Sw-Dis-1(config-if)#ip nat outside
```

Sw-Dis-1(config-if)#
Sw-Dis-1#

Verificación de la NAT con el comando sh ip nat statistics

Sw-Dis-1#sh ip nat statistics
Total translations: 0 (0 static, 0 dynamic, 0 extended)
Outside Interfaces: FastEthernet0/2
Inside Interfaces: FastEthernet0/1
Hits: 0 Misses: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool NAT-PALINDA refCount 0
pool NAT-PALINDA: netmask 255.255.255.252
start 147.60.50.160 end 147.60.50.163

type generic, total addresses 4 , allocated 0 (0%), misses 0

3.11.1 COTIZACION DE LOS EQUIPOS

TOTALTEK tecnología y servicio

UIO: De los Guarumos 449 y Av. 6 de Diciembre, Edf.: TotalTek — PBX: (593) 2 244-0501
GYE: Av. Isidro Ayora y Jose Luis Tamayo cc Polaris Of.: 14 — PBX: (593) 4 602-5288
CUE: Av. 24 de Mayo, Edf.: Portales del Rio — PBX: (593) 7 404-9714

Identificación Cotización	
No. Cotización:	TPG0096-1
Fecha:	42850
Validez:	15 dias

Cliente	Contacto	Teléfonos:	Dirección:
PALINDA	Li Ping Zheng	Tel.: Cel.: 984012378	CUMBAYA QUITO

Asesor Comercial	Información General de la Cotización	Facturación y Forma de Pago
Tania Gallegos Tel.: 2440501 ext: 244 Cel.: 098 385 9105 Mail: tgallegos@totaltek.com.ec	ARQUITECTURA DE SEGURIDAD Y COMUNICACIONES Garantía:	Anticipo: 0.5 Facturación: Pago: Saldo a la entrega de los equipos

Línea	Numero de Parte	Descripción	Cantidad	Precio Unitario	Precio Total		
		CABLEADO ESTRUCTURADO					
1		**MATERIALES**	1				
2	UTP6R-MSB	Cable UTP CAT 6 gris CMR	305	$0.69	$210.45		
3	69586-U24	Patch Panel sólido CAT 6	1	$134.22	$134.22		
4	42080-1WS	Face Plate 1 posición	11	$2.48	$27.28		
5	61110-RL6	Jack CAT 6 azúl	11	$5.33	$58.63		
6	62460-07L	Patch Cord CAT6 de 7ft. azúl	11	$6.19	$68.09		
7	62460-03L	Patch Cord CAT 6 de 3ft. azúl	11	$4.07	$44.77		
8	DXN5011S	Caja Dexson 40mm.	11	$1.62	$17.82		
				SUBTOTAL ITEM	**$561.26**		
		CABLEADO ESTRUCTURADO					
9		**MEDIOS DE CONDUCCIÓN**	1				
10	DXN10161	Canaleta 40x25 C/D blanca	20	$6.06	$121.20		
11	DXN11082	Ángulo interno 40x25	8	$1.16	$9.28		
12	DXN11081	Ángulo externo 40x25	8	$1.16	$9.28		
13	DXN11083	Ángulo Plano 40x25	8	$1.16	$9.28		
14	DXN11084	Derivación en T 40x25	8	$1.16	$9.28		
15	DXN11086	Unión 40x25	10	$1.16	$11.60		
16	DXN11085	Tapa final 40x25	4	$1.16	$4.64		
17	DXN10271	Canaleta 32x12	4	$2.83	$11.32		
18	DXN11143	Aángulo Plano 32x12	2	$0.53	$1.06		
19		Taco Fisher Nro. 8	100	$0.05	$5.00		
20		Tornillo Nro.8	100	$0.05	$5.00		
				SUBTOTAL ITEM	**$196.94**		
		CABLEADO ESTRUCTURADO					
21		**SERVICIOS DE INSTALACIÓN**	1				

Línea	Numero de Parte	Descripción	Cantidad	Precio Unitario	Precio Total		
22	SRV-INST-PD	Instalación de Punto de Datos	11	$37.32	$410.52		
23	SRV-CER-PD	Certificación de Punto de Datos	11	$6.22	$68.42		
24	SRV-MEM-TEC	Memoria Técnica Cableado Estructurado	1	$248.79	$248.79		
				SUBTOTAL ITEM	**$727.73**		
		CUARTO DE COMUNICACIONES					
25		**MATERIALES**	1				
26	I-1006-N	Rack cerrado modelo Júpiter con puerta de malla metálica 2000x600x1000	1	$800.87	$800.87		
27	I-1101	Bandeka estándar 19''	2	$12.27	$24.54		
28	I-1134	Multitoma Vertical 12 tomas dobles	1	$56.96	$56.96		
29	I-1142	Organizador con canaleta 40x60	1	$10.62	$10.62		
30	I-1159	Organizador vertical 80x80	1	$38.44	$38.44		
31	SURTA1500RMXL2U	APC Smart-UPS RT 1500VA Rack Tower 120V	1	$985.18	$985.18		
				SUBTOTAL ITEM	**$1,916.61**		
		CUARTO DE COMUNICACIONES					
32		**SERVICIOS DE INSTALACIÓN**	1				
33	SRV-INST-R42	Instalación y Peinado de Rack de Comunicaciones	1	$186.59	$186.59		
34	SRV-INST-GAB	Gabinete de By-Pass para UPS, incluye: * Acometida 10m * Gabinete con sistema de bloqueo * NEMAS de conexión	1	$373.18	$373.18		
				SUBTOTAL ITEM	**$559.77**		
		EQUIPAMIENTO ACTIVO					
35		**EQUIPOS**	1				
36	SG500-28-K9-NA	Cisco SG500-28 24 10/100/1000 ports-4 Gigabit Ethernet (2 combo* Gigabit Ethernet + 2 1GE/5GE SFP)	1	$1,112.33	$1,112.33		
37	WAP371-A-K9	Dual Radio 802.11ac Access Point with PoE (FCC)	1	$441.62	$441.62		
38	SB-PWR-INJ2-NA	Cisco Gigabit Power over Ethernet Injector-30W	1	$104.04	$104.04		
				SUBTOTAL ITEM	**$1,657.99**		
		EQUIPAMIENTO ACTIVO					
39		**GARANTÍAS**	1				
40	CON-SNT-SG5021NA	Cisco SG500-28 28-port Gigabit Stackable Managed Switch	1	$76.94	$76.94		
41	CON-SNT-WAP71AK9	Dual Radio 802.11ac Access Point with PoE (FCC)	1	$24.44	$24.44		
				SUBTOTAL ITEM	**$101.38**		
		EQUIPAMIENTO ACTIVO					
42		**SERVICIOS DE INSTALACIÓN Y CONFIGURACIÓN**	1				
43	SRV-INST-CONF-EA	Instalación y configuración	1	$435.37	$435.37		
				SUBTOTAL ITEM	**$435.37**		
		SISTEMA DE VIDEOVIGILANCIA					

Línea	Numero de Parte	Descripción	Cantidad	Precio Unitario	Precio Total		
44		**EQUIPAMIENTO**	1				
45	NVR201-08LP	8-ch, 1 SATA interface, Smart 1U, 8 PoE, Plastic Case +1X2TB Seagate	1	$304.76	$304.76		
46	IPC324ER3-DVPF36	Mini Dome 4MP, H.265, lens 3.6mm	2	$140.57	$281.14		
				SUBTOTAL ITEM	**$585.90**		
SISTEMA DE VIDEOVIGILANCIA							
47		**SERVICIOS DE INSTALACIÓN Y CONFIGURACIÓN**	1				
48	SRV-INST-CONF-SV	Instalación y configuración	1	$186.59	$186.59		
				SUBTOTAL ITEM	**$186.59**		
FIREWALL							
49		**EQUIPOS**	1				
50	FG-30E-BDL-950-12	Hardware plus 1 Year 24x7 FortiCare and FortiGuard UTM Bundle for FortiGate-30E	1	$1,020.24	$1,020.24		
51	RM-FR-T9	Rack Mount Kit for FortiGate 30E / 50E series	1	$328.94	$328.94		
				SUBTOTAL ITEM	**$1,349.18**		
FIREWALL							
52		**SERVICIOS DE INSTALACIÓN Y CONFIGURACIÓN**	1				
53	SRV-INST-FW	Instalación y Configuración	1	$373.18	$373.18		
				SUBTOTAL ITEM	**$373.18**		
				SUBTOTAL:	**$8,651.90**		
				I.V.A. 14%:	**$1,211.27**		
				TOTAL:	**$9,863.17**		

Figura No. 26 Cotización de equipos

Fuente: Proforma de la empresa TOTALTEK

4 CONCLUSIONES

En este proyecto me base de acuerdo a las necesidades que requería Palinda dejando en claro las expectativas en cuanto a su uso y limitaciones. Con el desarrollo de este proyecto nos enfocamos en que Ethernet es la tecnología de red de área local más extendida en la actualidad, ya que combina la fácil administración e implementación, costos relativamente bajos y velocidad ya que permite un mayor aprovechamiento de ancho de banda disponible en la red.

Se enfocó en diseñar una red jerárquica permitiendo agrupar equipos con funciones específicas, separándolo en tres niveles para facilitar el diseño, la implementación y mantenimiento de la red, haciendo la red más confiable y escalable.

Se creó las VLAN para controlar el tráfico, además facilita la administración de la red porque separa segmentos lógicos LAN.

Implementamos políticas de seguridad con las listas de control de acceso y aseguramos los puertos de los Switches de Acceso para cualquier intruso que intente acceder a la red.

5 RECOMENDACIONES

- ✓ Proceder con la implementación de la red propuesto y solicitar transferencia de conocimiento.

- ✓ Se debe realizar un Plan de Contingencias con todos los procedimientos que se debe tomar en cuenta cuando falla un punto de red.

- ✓ Se debería adquirir servidores de respaldo de información, ya que Palinda tiene información crítica.

6 BIBLIOGRAFIA

CISCO. (2004). *Guia del segundo año CCNA 3 y 4.* Madrid: PEARSON EDUCATION, S.A.

CISCO. (16 de Octubre de 2012). *Internetworking Technology Handbook.* Obtenido de http://docwiki.cisco.com/w/index.php?title=Internetworking_Technology_Handbook&oldid=49158

CISCO. (12 de Febrero de 2014). *Cisco IOS IP Configuration Guide, Release 12.2.* Obtenido de http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfipadr.html

CISCO. (1 de Febrero de 2016). *Cisco Connected Grid Ethernet Switch Module Interface Card Software Configuration Guide.* Obtenido de http://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/switch_module_swcg/cgr-esm-configuration/config_vlans.html#33099

CISCO. (26 de Septiembre de 2016). *Cisco Nexus 5000 Series NX-OS Software Configuration Guide.* Obtenido de http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli/CLIConfigurationGuide/VLANs.html

WIKIPEDIA. (29 de Agosto de 2014). *RED DE AREA LOCAL*. Obtenido de https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local