INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

"UNIDAD CULHUACAN"

SEMINARIO: INTERCONECTIVIDAD Y SEGMENTACION DE REDES DE ALTA VELOCIDAD

TEMA: DISEÑO DE LAS PRACTICAS DE REDES EN LA ESIME UNIDAD CULHUACAN "ROUTING Y SWITCHING"

INTEGRANTES:

RICARDO APARICIO GARCÍA

LILIANA MACEDO MARTÍNEZ

ADOLFO RAFAEL PALMA VEGA

OSCAR ALBERTO SUÁREZ PUENTE

INDICE

Capitulo 1: INTRODUCCIÓN A LAS REDES

I. INTRODUCCIÓN

OBJETIVO

Presentar las experiencias en la implementación de las prácticas académicas de redes LAN para el laboratorio de redes de ESIME Culhuacán

Analizar aspectos estándares de codificación que ayuden a realizar una implementación adecuada para un esquema de red en particular.

ALCANCE

Realizar los procedimientos de codificación, documentación e implementación para las practicas de RIP, OSPF, STP, VLAN, VTP, ACL, NAT, y PAT.

PROBLEMA

Inexistencia de documentación que sirva de apoyo a los estudiantes sobre las prácticas en el laboratorio de redes de la ESIME Culhuacán. Así como de consulta para diversas utilidades de tipo académicas. Tampoco cuentan con las prácticas implementadas para observar físicamente dicha comunicación.

JUSTIFICACIÓN

Apoyar al desarrollo de prácticas y su documentación para ampliar en entendimiento de de las redes LAN, así como guiar de forma práctica y teórica en la implementación de las mismas.

II. MARCO TEORICO

Capitulo 1: INTRODUCCIÓN A LAS REDES

1.1 ¿QUÉ ES UNA RED?

La industria de ordenadores ha mostrado un progreso espectacular en muy corto tiempo. El viejo modelo de tener un solo ordenador para satisfacer todas las necesidades de cálculo de una organización se está reemplazando con rapidez por otro que considera un número grande de ordenadores separados, pero interconectados, que efectúan el mismo trabajo. Estos sistemas, se conocen con el nombre de redes de ordenadores. Estas nos dan a entender una colección interconectada de ordenadores autónomos. Se dice que los ordenadores están interconectados, si son capaces de intercambiar información. La conexión no necesita hacerse a través de un hilo de cobre, el uso de láser, microondas y satélites de comunicaciones. Al indicar que los ordenadores son autónomos, excluimos los sistemas en los que un ordenador pueda forzosamente arrancar, parar o controlar a otro, éstos no se consideran autónomos.

1.2 TIPOS DE REDES

Principales tipos de redes para soportar los sistemas distribuidos son:

1.2.1 ***Redes De Área Local (Lan):*** las redes de área local (local area networks) llevan mensajes a velocidades relativamente grande entre computadores conectados a un único medio de comunicaciones : un cable de par trenzado. Un cable coaxial o una fibra óptica. Un segmento es una sección de cable que da servicio y que puede tener varios computadores conectados, el ancho de banda del mismo se reparte entre dichas computadores. Las redes de área local mayores están compuestas por varios segmentos interconectados por conmutadores (switches) o concentradores (hubs). El ancho de banda total del sistema es grande y la latencia pequeña, salvo cuando el tráfico es muy alto.

En los años 70s se han desarrollado varias tecnologías de redes de área local, destacándose Ethernet como tecnología dominante para las redes de área amplia; estando esta carente de garantías necesarias sobre latencia y ancho de banda necesario para la aplicación multimedia. Como consecuencia de esta surge ATM para cubrir estas falencias impidiendo su costo su implementación en redes de área local. Entonces en su lugar se implementan las redes Ethernet de alta velocidad que resuelven estas limitaciones no superando la eficiencia de ATM.

1.2.2 ***Redes De Área Extensa (Wan):*** estas pueden llevar mensajes entre nodos que están a menudo en diferentes organizaciones y quizás separadas por grandes distancias, pero a una velocidad menor que las redes LAN. El medio de comunicación está compuesto por un conjunto de círculos de enlazadas mediante computadores dedicados, llamados rotures o encaminadores. Esto gestiona la red de comunicaciones y encaminan mensajes o

paquetes hacia su destino. En la mayoría de las redes se produce un retardo en cada punto de la ruta a causa de las operaciones de encaminamiento, por lo que la latencia total de la transmisión de un mensaje depende de la ruta seguida y de la carga de tráfico en los distintos segmentos que atraviese. La velocidad de las señales electrónicas en la mayoría de los medios es cercana a la velocidad de la luz, y esto impone un límite inferior a la latencia de las transmisiones para las transmisiones de larga distancia.

1.2.3 ***Redes De Área Metropolitana (Man):*** las redes de área metropolitana (metropolitan area networks) se basan en el gran ancho de banda de las cableadas de cobre y fibra óptica recientemente instalados para la transmisión de videos, voz, y otro tipo de datos. Varias han sido las tecnologías utilizadas para implementar el encaminamiento en las redes LAN, desde Ethernet hasta ATM. IEEE ha publicado la especificación 802.6 [IEEE 1994], diseñado expresamente para satisfacer las necesidades de las redes WAN. Las conexiones de línea de suscripción digital, DLS (digital subscribe line) y los MODEM de cable son un ejemplo de esto. DSL utiliza generalmente conmutadores digitales sobre par trenzado a velocidades entre 0.25 y 6.0 Mbps; la utilización de este par trenzado para las conexiones limita la distancia al conmutador a 1.5 kilómetros. Una conexión de MODEM por cable utiliza una señalización análoga sobre el cable coaxial de televisión para conseguir velocidades de 1.5 Mbps con un alcance superior que DSL.

1.2.4 ***Redes Inalámbricas (Wireless):*** la conexión de los dispositivos portátiles y de mano necesitan redes de comunicaciones inalámbricas (wireless networks). Algunos de ellos son la IEEE802.11 (wave lan) son verdaderas redes LAN inalámbricas (wireless local área networks; WLAN) diseñados para ser utilizados en vez de los LAN. También se encuentran las redes de area personal inalámbricas, incluida la red europea mediante el Sistema Global para Comunicaciones Móviles, GSM (global system for mobile communication). En los Estados Unidos, la mayoría de los teléfonos móviles están actualmente basados en la análoga red de radio celular AMPS, sobre la cual se encuentra la red digital de comunicaciones de Paquetes de Datos Digitales Celular, CDPD (Celular Digital Packet Data).

Dado el restringido ancho de banda disponible y las otras limitaciones de los conjuntos de protocolos llamados Protocolos de Aplicación Inalámbrica WAP (Wireless Aplication Protocol)

1.2.5 ***Interredes:*** una Interred es un sistema de comunicación compuesto por varias redes que se han enlazado juntas para proporcionar unas posibilidades de comunicación ocultando las tecnologías y los protocolos y métodos de interconexión de las redes individuales que la componen.

Estas son necesarias para el desarrollo de sistemas distribuidos abiertos extensibles. En ellas se puede integrar una gran variedad de tecnología de redes de área local y amplia, para proporcionar la capacidad de trabajo en red necesaria para cada grupo de usuario. Así, las interredes aportan gran parte de los beneficios de los sistemas abiertos a las comunicaciones de los sistemas distribuidos.

Las interredes se construyen a partir de varias redes. Estas están interconectadas por computadoras dedicadas llamadas routers y computadores de propósito general llamadas

gateways, y por un subsistema integrado de comunicaciones producidos por una capa de software que soporta el direccionamiento y la transmisión de datos a los computadores a través de la interred. Los resultados pueden contemplarse como una red virtual construida a partir de solapar una capa de interred sobre un medio de comunicación que consiste en varias redes, routers y gateways subyacentes.

1.3 TOPOLOGÍAS DE LAS REDES

La topología o forma lógica de una red se define como la forma de tender el cable a estaciones de trabajo individuales; por muros, suelos y techos del edificio. Existe un número de factores a considerar para determinar cual topología es la más apropiada para una situación dada.
La topología en una red es la configuración adoptada por las estaciones de trabajo para conectarse entre sí.

Topologías más Comunes:
1.3.1 *Bus:* Esta topología permite que todas las estaciones reciban la información que se transmite, una estación transmite y todas las restantes escuchan. Consiste en un cable con un terminador en cada extremo del que se cuelgan todos los elementos de una red. Todos los nodos de la red están unidos a este cable: el cual recibe el nombre de "Backbone Cable". Tanto Ethernet como Local Talk pueden utilizar esta topología.
El bus es pasivo, no se produce regeneración de las señales en cada nodo. Los nodos en una red de "bus" transmiten la información y esperan que ésta no vaya a chocar con otra información transmitida por otro de los nodos. Si esto ocurre, cada nodo espera una pequeña cantidad de tiempo al azar, después intenta retransmitir la información.
1.3.2 *Anillo:* Las estaciones están unidas unas con otras formando un círculo por medio de un cable común. El último nodo de la cadena se conecta al primero cerrando el anillo. Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo. Con esta metodología, cada nodo examina la información que es enviada a través del anillo. Si la información no está dirigida al nodo que la examina, la pasa al siguiente en el anillo. La desventaja del anillo es que si se rompe una conexión, se cae la red completa.
1.3.3 *Estrella:* Los datos en estas redes fluyen del emisor hasta el concentrador, este realiza todas las funciones de la red, además actúa como amplificador de los datos.
La red se une en un único punto, normalmente con un panel de control centralizado, como un concentrador de cableado. Los bloques de información son dirigidos a través del panel de control central hacia sus destinos. Este esquema tiene una ventaja al tener un panel de control que monitorea el tráfico y evita las colisiones y una conexión interrumpida no afecta al resto de la red.

1.3.4 *Híbridas:* El bus lineal, la estrella y el anillo se combinan algunas veces para formar combinaciones de redes híbridas.

1.3.4.1 Anillo en Estrella: Esta topología se utiliza con el fin de facilitar la administración de la red. Físicamente, la red es una estrella centralizada en un concentrador, mientras que a nivel lógico, la red es un anillo.

1.3.4.2 Bus en Estrella: El fin es igual a la topología anterior. En este caso la red es un "bus" que se cablea físicamente como una estrella por medio de concentradores.

1.3.4.3 Estrella Jerárquica: Esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada par formar una red jerárquica.

1.3.4.4 Árbol: Esta estructura se utiliza en aplicaciones de televisión por cable, sobre la cual podrían basarse las futuras estructuras de redes que alcancen los hogares. También se ha utilizado en aplicaciones de redes locales analógicas de banda ancha.

1.3.4.5 Trama: Esta estructura de red es típica de las WAN, pero también se puede utilizar en algunas aplicaciones de redes locales (LAN). Las estaciones de trabajo están conectadas cada una con todas las demás.

1.3.5 Topologías Para Interredes:

1.3.5.1 Red de Enlace Central: Se encuentra generalmente en los entornos de oficina o campos, en los que las redes de los pisos de un edificio se interconectan sobre cables centrales. Los Bridges y los Routers gestionan el tráfico entre segmentos de red conectados.

1.3.5.2 Red de Malla: Esta involucra o se efectúa a través de redes WAN, una red malla contiene múltiples caminos, si un camino falla o está congestionado el tráfico, un paquete puede utilizar un camino diferente hacia el destino. Los routers se utilizan para interconectar las redes separadas.

1.3.5.3 Red de Estrella Jerárquica: Esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada para formar una red jerárquica.

1.4 MECANISMOS PARA LA RESOLUCIÓN DE CONFLICTOS EN TRANSMISIÓN DE DATOS

***1.4.1 CSMA/CD*:** Son redes con escucha de colisiones. Todas las estaciones son consideradas igual, es por ello que compiten por el uso del canal, cada vez que una de ellas desea transmitir debe escuchar el canal, si alguien está transmitiendo espera a que termine, caso contrario transmite y se queda escuchando posibles colisiones, en este último espera un intervalo de tiempo y reintenta de nuevo.

1.4.2 Token Bus: Se usa un token (una trama de datos) que pasa de estación en estación en forma cíclica, es decir forma un anillo lógico. Cuando una estación tiene el token, tiene el derecho exclusivo del bus para transmitir o recibir datos por un tiempo determinado y luego pasa el token a otra estación, previamente designada. Las otras estaciones no

pueden transmitir sin el token, sólo pueden escuchar y esperar su turno. Esto soluciona el problema de colisiones que tiene el mecanismo anterior.

1.4.3 Token Ring: La estación se conecta al anillo por una unidad de interfaz (RIU), cada RIU es responsable de controlar el paso de los datos por ella, así como de regenerar la transmisión y pasarla a la estación siguiente. Si la dirección de la cabecera de una determinada transmisión indica que los datos son para una estación en concreto, la unidad de interfaz los copia y pasa la información a la estación de trabajo conectada a la misma.
Se usa en redes de área local con o sin prioridad, el token pasa de estación en estación en forma cíclica, inicialmente en estado desocupado. Cada estación cundo tiene el token (en este momento la estación controla el anillo), si quiere transmitir cambia su estado a ocupado, agregando los datos atrás y lo pone en la red, caso contrario pasa el token a la estación siguiente. Cuando el token pasa de nuevo por la estación que transmitió, saca los datos, lo pone en desocupado y lo regresa a la red.

1.5 MODELO OSI

Durante los años 60 y 70 se crearon muchas tecnologías de redes, cada una basada en un diseño específico de hardware. Estos sistemas eran construidos de una sola pieza, una arquitectura monolítica. Esto significa que los diseñadores debían ocuparse de todos los elementos involucrados en el proceso, estos elementos forman una cadena de transmisión que tiene diversas partes: Los dispositivos físicos de conexión, los protocolos software y hardware usados en la comunicación.
Los programas de aplicación realizan la comunicación y la interfaz hombre-máquina que permite al humano utilizar la red. Este modelo, que considera la cadena como un todo monolítico, es poco práctico, pues el más pequeño cambio puede implicar alterar todos sus elementos.

1.5.1 Diseño Original De Internet

El diseño original de Internet del Departamento de Defensa Americano disponía un esquema de cuatro capas, aunque data de los 70 es similar al que se continúa utilizando:
1.5.1.1 Capa Física o de Acceso de Red: Es la responsable del envío de la información sobre el sistema hardware utilizado en cada caso, se utiliza un protocolo distinto según el tipo de red física.
1.5.1.2 Capa de Red o Capa Internet: Es la encargada de enviar los datos a través de las distintas redes físicas que pueden conectar una máquina origen con la de destino de la información. Los protocolos de transmisión, como el IP están íntimamente asociados a esta capa.
1.5.1.3 Capa de Transporte: Controla el establecimiento y fin de la conexión, control de flujo de datos, retransmisión de datos perdidos y otros detalles de la transmisión entre

dos sistemas. Los protocolos más importantes a este nivel son TCP y UDP (mutuamente excluyentes).

1.5.1.4 Capa de Aplicación: Conformada por los protocolos que sirven directamente a los programas de usuario, navegador, e-mail, FTP, TELNET, etc.

Respondiendo a la teoría general imperante el mundo de la computación, de diseñar el hardware por módulos y el software por capas, en 1978 la organización ISO (International Standards Organization), propuso un modelo de comunicaciones para redes al que titularon "The reference model of Open Systems Interconnection", generalmente conocido como MODELO OSI.

Su filosofía se basa en descomponer la funcionalidad de la cadena de transmisión en diversos módulos, cuya interfaz con los adyacentes esté estandarizada. Esta filosofía de diseño presenta una doble ventaja: El cambio de un módulo no afecta necesariamente a la totalidad de la cadena, además, puede existir una cierta inter-operatividad entre diversos productos y fabricantes hardware/software, dado que los límites y las interfaces están perfectamente definidas.

1.5.2 ***Capas Del Modelo OSI***

La descripción de las diversas capas que componen este modelo es la siguiente:

1.5.2.1 Capa física: Es la encargada de transmitir los bits de información por la línea o medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes, de la velocidad de transmisión, si esta es unidireccional o bidireccional (simplex, duplex o flull-duplex).

También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas.

Como resumen de los cometidos de esta capa, podemos decir que se encarga de transformar un paquete de información binaria en una sucesión de impulsos adecuados al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable), electromagnéticos (transmisión Wireless) o luminosos (transmisión óptica). Cuando actúa en modo recepción el trabajo es inverso, se encarga de transformar estos impulsos en paquetes de datos binarios que serán entregados a la capa de enlace.

1.5.2.2 Capa de enlace: Puede decirse que esta capa traslada los mensajes hacia y desde la capa física a la capa de red. Especifica cómo se organizan los datos cuando se transmiten en un medio particular. Esta capa define como son los cuadros, las direcciones y las sumas de control de los paquetes Ethernet.

Además del direccionamiento local, se ocupa de la detección y control de errores ocurridos en la capa física, del control del acceso a dicha capa y de la integridad de los datos y fiabilidad de la transmisión. Para esto agrupa la información a transmitir en bloques, e incluye a cada uno una suma de control que permitirá al receptor comprobar su integridad. Los datagramas recibidos son comprobados por el receptor. Si algún

datagrama se ha corrompido se envía un mensaje de control al remitente solicitando su reenvío.

La capa de enlace puede considerarse dividida en dos subcapas:

1.5.2.2.1 Control lógico de enlace LLC: define la forma en que los datos son transferidos sobre el medio físico, proporcionando servicio a las capas superiores.

1.5.2.2.2 Control de acceso al medio MAC: Esta subcapa actúa como controladora del hardware subyacente (el adaptador de red). De hecho el controlador de la tarjeta de red es denominado a veces "MAC driver", y la dirección física contenida en el hardware de la tarjeta es conocida como dirección. Su principal consiste en arbitrar la utilización del medio físico para facilitar que varios equipos puedan competir simultáneamente por la utilización de un mismo medio de transporte. El mecanismo CSMA/CD ("Carrier Sense Multiple Access with Collision Detection") utilizado en Ethernet es un típico ejemplo de esta subcapa.

1.5.2.3 Capa de Red: Esta capa se ocupa de la transmisión de los datagramas (paquetes) y de encaminar cada uno en la dirección adecuada tarea esta que puede ser complicada en redes grandes como Internet, pero no se ocupa para nada de los errores o pérdidas de paquetes. Define la estructura de direcciones y rutas de Internet. A este nivel se utilizan dos tipos de paquetes: paquetes de datos y paquetes de actualización de ruta. Como consecuencia esta capa puede considerarse subdividida en dos:

1.5.2.3.1 Transporte: Encargada de encapsular los datos a transmitir (de usuario). Utiliza los paquetes de datos. En esta categoría se encuentra el protocolo IP.

1.5.2.3.2 Conmutación: Esta parte es la encargada de intercambiar información de conectividad específica de la red. Los routers son dispositivos que trabajan en este nivel y se benefician de estos paquetes de actualización de ruta. En esta categoría se encuentra el protocolo ICMP responsable de generar mensajes cuando ocurren errores en la transmisión y de un modo especial de eco que puede comprobarse mediante ping.

Los protocolos más frecuentemente utilizados en esta capa son dos: X.25 e IP.

1.5.2.4 Capa de Transporte: Esta capa se ocupa de garantizar la fiabilidad del servicio, describe la calidad y naturaleza del envío de datos. Esta capa define cuando y como debe utilizarse la retransmisión para asegurar su llegada. Para ello divide el mensaje recibido de la capa de sesión en trozos (datagramas), los numera correlativamente y los entrega a la capa de red para su envío.

Durante la recepción, si la capa de Red utiliza el protocolo IP, la capa de Transporte es responsable de reordenar los paquetes recibidos fuera de secuencia. También puede funcionar en sentido inverso multiplexando una conexión de transporte entre diversas conexiones de datos. Este permite que los datos provenientes de diversas aplicaciones compartan el mismo flujo hacia la capa de red.

1.5.2.5 Capa de Sesión: Es una extensión de la capa de transporte que ofrece control de diálogo y sincronización, aunque en realidad son pocas las aplicaciones que hacen uso de ella.

1.5.2.6 Capa de Presentación: Esta capa se ocupa de garantizar la fiabilidad del servicio, describe la calidad y naturaleza del envío de datos. Esta capa define cuando y como debe

utilizarse la retransmisión para asegurar su llegada. Para ello divide el mensaje recibido de la capa de sesión en trozos (datagramas), los numera correlativamente y los entrega a la capa de red para su envío.
Durante la recepción, si la capa de Red utiliza el protocolo IP, la capa de Transporte es responsable de reordenar los paquetes recibidos fuera de secuencia. También puede funcionar en sentido inverso multiplexando una conexión de transporte entre diversas conexiones de datos. Este permite que los datos provenientes de diversas aplicaciones compartan el mismo flujo hacia la capa de red.
Esta capa se ocupa de los aspectos semánticos de la comunicación, estableciendo los arreglos necesarios para que puedan comunicar máquinas que utilicen diversa representación interna para los datos. Describe como pueden transferirse números de coma flotante entre equipos que utilizan distintos formatos matemáticos.
1.5.2.7 Capa de Aplicación: Esta capa describe como hacen su trabajo los programas de aplicación (navegadores, clientes de correo, terminales remotos, transferencia de ficheros etc.). Esta capa implementa la operación con ficheros del sistema. Por un lado interactúan con la capa de presentación y por otro representan la interfaz con el usuario, entregándole la información y recibiendo los comandos que dirigen la comunicación.
Algunos de los protocolos utilizados por los programas de esta capa son HTTP, SMTP, POP, IMAP etc.

Aplicación	El nivel de aplicación es el destino final de los datos donde se proporcionan los servicios al usuario.
Presentación	Se convierten e interpretan los datos que se utilizarán en el nivel de aplicación.
Sesión	Encargado de ciertos aspectos de la comunicación como el control de los tiempos.
Transporte	Transporta la información de una manera fiable para que llegue correctamente a su destino.
Red	Nivel encargado de encaminar los datos hacia su destino eligiendo la ruta más efectiva.
Enlace	Enlace de datos. Controla el flujo de los mismos, la sincronización y los errores que puedan producirse.
Físico	Se encarga de los aspectos físicos de la conexión, tales como el medio de transmisión o el hardware.

Tabla 1.1 Modelo OSI

1.6 DEFINICIÓN TCP/IP

Se han desarrollado diferentes familias de protocolos para comunicación por red de datos para los sistemas UNIX. El más ampliamente utilizado es el Internet Protocol Suite, comúnmente conocido como TCP / IP.
Es un protocolo DARPA que proporciona transmisión fiable de paquetes de datos sobre redes. El nombre TCP/IP proviene de dos protocolos importantes de la familia, el

Transmission Contorl Protocol (TCP) y el Internet Protocol (IP). Todos juntos llegan a ser más de 100 protocolos diferentes definidos en este conjunto.
El TCP/IP es la base del Internet que sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local y área extensa. TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en el ARPANET una red de área extensa del departamento de defensa.

1.6.1 ***Comandos TCP/IP***

TCP/IP incluye dos grupos de comandos utilizados para suministrar servicios de red:

- Los comandos remotos BERKELEY
- Los comandos DARPA

Los comandos remotos BERKELEY, que fueron desarrollados en la Universidad Berkeley (California), incluyen órdenes para comunicaciones entre sistemas operativos UNIX, como copia remota de archivos, conexión remota, ejecución de shell remoto, etc.
Permiten utilizar recursos con otros hosts, pudiendo tratar distintas redes como si fueran una sola.
En la versión 4 para UNIX Sistema V, se pueden distinguir los siguientes comandos más comunes:

- RCP Realiza una copia de archivos al mismo o a otro servidor
- RLOGINGL-RLOGINVT Se utiliza para hacer una conexión al mismo o a otro servidor
- REXEC-RSH Permite ejecutar comandos del sistema operativo en el mismo o en otro servidor.

Los comandos DARPA incluyen facilidades para emulación de terminales, transferencia de archivos, correo y obtención de información sobre usuarios. Pueden ser utilizadas para comunicación con computadores que ejecutan distintos sistemas operativos.
En la versión 2.05 para DOS, dependiendo de las funciones que realizan, se pueden distinguir los siguientes grupos de comandos:

1.6.1.1 Kernel PC/TCP y herramientas asociadas

Se utilizan para cargar el núcleo TCP/IP en la memoria del computador.

- BOOTP Asigna la dirección IP de la estación de trabajo
- INET Descarga el núcleo PC/TCP de la memoria y/o realiza estadísticas de red
- KERNEL Carga el núcleo TCP/IP en la memoria y lo deja residente

1.6.1.2 Configuración de la red

Permiten configurar TCP/IP con determinados parámetros.

- IFCONFIG Configura el hardware para TCP/IP
- IPCONFIG Configura el software TCP/IP y la direcci6n IP

1.6.1.3 Transferencia de archivos

Se utilizan para transferir archivos entre distintos computadores.

- DDAT'ES Muestra las fechas y horas guardadas en un archivo creado con el comando TAR
- FTP Transfiere archivos entre una estación de trabajo y un servidor
- FRPSRV Convierte una estación de trabajo en un servidor FTP
- PASSWD Se utiliza para poner contraseñas en las estaciones de trabajo a los usuarios para poder utilizar el comando FTPSRV
- RMT Permite realizar copia de archivos en una unidad de cinta
- TAR Realiza una copia de archivos creando un único archivo de BACKUP
- TFTP Transfiere archivos entre una estación de trabajo un servidor o a otra estación de trabajo sin necesidad de validar al usuario
- Impresión Permiten el control de la impresión en las impresoras conectadas al servidor.
- DOPREDIR Imprime un trabajo de impresión que aún no ha sido impreso
- IPRINT Envía un texto o un archivo a un servidor de impresoras de imagen
- LPQ Indica el estado de la cola de impresión indicada
- LPR Envía un texto o un archivo a una impresora local o de red.
- LPRM Elimina trabajos pendientes de la cola de impresión
- ONPREDIR Realiza tareas de configuración para el comando PREDIR
- PREDIR Carga o descarga el programa que permite la impresión remota y lo deja residente.
- PRINIT Se usa con los comandos PREDIR y ONPREDIR
- PRSTART Indica a la estación de trabajo remota que imprima un archivo usando la configuración por defecto

1.6.1.4 Conexión a servidores

Permiten la conexión de los computadores a servidores de nuestra red.

- SUPDUP Permite conectarse a otro servidor de la red
- TELNET - TN Es el método normal de conectarse a un servidor de la red
- Información sobre los usuarios Muestran información sobre los usuarios conectados a la red.
- FINGER Muestra información sobre un usuario conectado a otra estación de trabajo
- NICNAME Muestra información sobre un usuario o sobre un servidor solicitada al centro de informaci6n de redes
- WHOIS Muestra información sobre un usuario registrado que esté conectado a otra estación de trabajo
- Envío y recepción de correo Estos comandos permiten el envío y/o recepción de correo entre los usuarios de la red.
- MAIL Permite enviar y recibir correo en la red
- PCMAIL Permite leer correo. Se ha de usar con el comando VMAIL
- POP2 - POP3 Se utiliza para leer correo. Se han de usar con VMAIL Y SMTP

- SMTP Se utiliza para enviar correo en la red
- SMTPSRV Permite leer el correo recibido
- VMAIL Es un comando que muestra una pantalla preparada para leer el correo recibido. Se utiliza en conjunción con los comandos PCMAIL, POP2 0 POP3

1.6.1.5 Chequeo de la red

Permiten chequear la red cuando aparecen problemas de comunicaciones.

- HOST Indica el nombre y la dirección IP de una estación de trabajo determinada
- PING Envía una Llamada a una estación de trabajo e informa si se puede establecer conexión o no con ella
- SETCLOCK Muestra la fecha y la hora que tiene la red

1.6.2 ***Como funciona TCP/IP***

Una red TCP/IP transfiere datos mediante el ensamblaje de bloques de datos en paquetes, cada paquete comienza con una cabecera que contiene información de control; tal como la dirección del destino, seguido de los datos. Cuando se envía un archivo por la red TCP/IP, su contenido se envía utilizando una serie de paquetes diferentes. El Internet protocol (IP), un protocolo de la capa de red, permite a las aplicaciones ejecutarse transparentemente sobre redes interconectadas. Cuando se utiliza IP, no es necesario conocer que hardware se utiliza, por tanto ésta corre en una red de área local.

El Transmisión Control Protocol (TCP); un protocolo de la capa de transporte, asegura que los datos sean entregados, que lo que se recibe, sea lo que se pretendía enviar y que los paquetes que sean recibidos en el orden en que fueron enviados. TCP terminará una conexión si ocurre un error que haga la transmisión fiable imposible.

1.6.3 ***Administración TCP/IP***

TCP/IP es una de las redes más comunes utilizadas para conectar computadoras con sistema UNIX. Las utilidades de red TCP/IP forman parte de la versión 4, muchas facilidades de red como un sistema UUCP, el sistema de correo, RFS y NFS, pueden utilizar una red TCP/CP para comunicarse con otras máquinas.

Para que la red TCP/IP esté activa y funcionando será necesario:

1. Obtener una dirección Internet.
2. Instalar las utilidades Internet en el sistema
3. Configurar la red para TCP/IP
4. Configurar los guiones de arranque TCP/IP
5. Identificar otras máquinas ante el sistema
6. Configurar la base de datos del o y ente de STREAMS
7. Comenzar a ejecutar TCP/IP.

1.7 ¿QUÉ ES INTERNET?

Internet es una red de computadoras que utiliza convenciones comunes a la hora de nombrar y direccionar sistemas. Es una colecciona de redes independientes interconectadas; no hay nadie que sea dueño o active Internet al completo.
Las computadoras que componen Internet trabajan en UNIX, el sistema operativo Macintosh, Windows 95 y muchos otros. Utilizando TCP/IP y los protocolos veremos dos servicios de red.

1.7.1 ***Servicios de red:***

- ✓ Servicios de Internet a nivel de aplicación
- ✓ Servicios de Internet a nivel de red

1.7.2 ***Características de los servicios TCP/IP***

Muchas redes proporcionan servicios básicos similares a los servicios TCP/IP, pero existen unas características principales que los distingue de los otros servicios:

1.7.2.1 Independencia de la tecnología de red. Ya que el TCP/IP está basado en una tecnología convencional de conmutación de paquetes, es independiente de cualquier marca de hardware en particular. La Internet global incluye una variedad de tecnologías de red que van de redes diseñadas para operar dentro de un solo edificio a las diseñadas para abarcar grandes distancias. Los protocolos TCP/IP definen la unidad de transmisión de datos, llamada datagrama, y especifican cómo transmitir los datagramas en una red en particular.

1.7.2.2 Interconexión universal. Una red de redes TCP/IP permite que se comunique cualquier par de computadoras conectadas a ella. Cada computadora tiene asignada una dirección reconocida de manera universal dentro de la red de redes. Cada datagrama lleva en su interior las direcciones de destino para tomar decisiones de ruteo.

1.7.2.3 Acuses de recibo punto-a-punto. Los protocolos TCP/IP de una red de redes proporcionan acuses de recibo entre la fuente y el último destino en vez de proporcionarlos entre máquinas sucesivas a lo largo del camino, aún cuando las dos máquinas no estén conectadas a la misma red física.

1.7.2.4 Estándares de protocolo de aplicación. Además de los servicios básicos de nivel de transporte (como las conexiones de flujo confiable), los protocolos TCP/IP incluyen estándares para muchas aplicaciones comunes, incluyendo correo electrónico, transferencia de archivos y acceso remoto. Por lo tanto, cuando se diseñan programas de aplicación que utilizan el TCP/IP, los programadores a menudo se encuentran con que el software ya existente proporciona los servicios de comunicación que necesitan.

Capitulo 2: Switcheo ethernet

2.1 ¿QUÉ ES UN SWITCH ETHERNET?

Un cambio es algo que se utiliza para activar o desactivar los dispositivos electrónicos diversos. Sin embargo, en las redes de computadoras, un conmutador se utiliza para conectar varios ordenadores entre sí. Dado que se trata de un dispositivo externo se convierte en parte de los equipos periféricos utilizados en la operación de un sistema informático. Esta conexión se realiza dentro de una red de área local (LAN) y sólo es idéntico a un concentrador Ethernet en términos de apariencia, salvo con más inteligencia. Estos interruptores no sólo reciben los paquetes de datos, sino que también tienen la capacidad de inspeccionar ellos antes de pasarlos a la siguiente computadora. Es decir, que pueden averiguar la fuente, el contenido de los datos, y determinar el destino también. Debido a esta singularidad, que envía los datos a los sistema conectado solamente, utilizando para ello menos ancho de banda de alto rendimiento en las tasas.

2.2 VLAN (RED DE ÁREA LOCAL VIRTUAL)

Una VLAN es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLAN's pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un switch capa 3).
Una 'VLAN' consiste en una red de ordenadores que se comportan como si estuviesen conectados al mismo conmutador, aunque pueden estar en realidad conectados físicamente a diferentes segmentos de una red de área local. Los administradores de red configuran las VLANs mediante software en lugar de hardware, lo que las hace extremadamente flexibles. La comunicación entre los diferentes equipos en una LAN está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento de equipos según determinados criterios (direcciones MAC, números de puertos, protocolo, etc.).

2.2.1 ***Protocolos y diseño***

El protocolo de etiquetado IEEE 802.1Q domina el mundo de las VLANs. Antes de su introducción existían varios protocolos propietarios, como el ISL (Inter-Switch Link) de Cisco, una variante del IEEE 802.1Q, y el VLT (Virtual LAN Trunk) de 3Com.
Los primeros diseñadores de redes enfrentaron el problema del tamaño de los dominios de colisión (Hubs) esto se logró controlar a través de la introducción de los conmutadores pero a su vez se introdujo el problema del aumento del tamaño de los dominios de difusión y una de las formas más eficientes para manejarlo fue la introducción de las

VLANs. Las VLANs también pueden servir para restringir el acceso a recursos de red con independencia de la topología física de ésta, si bien la robustez de este método es discutible al ser el salto de VLAN (VLAN hopping) un método común de evitar tales medidas de seguridad.
Las VLANs funcionan en el nivel 2 (enlace de datos) del modelo OSI. Sin embargo, los administradores suelen configurar las VLANs como correspondencia directa de una red o subred IP, lo que les da apariencia de funcionar en el nivel 3 (red).
En el contexto de las VLANs, el término trunk (troncal) designa una conexión de red que transporta múltiples VLANs identificadas por etiquetas (tags) insertadas en sus paquetes. Dichos trunks deben operar entre tagged ports (puertos etiquetados) de dispositivos con soporte de VLANs, por lo que a menudo son enlaces conmutador a conmutador o conmutador a enrutador más que enlaces a nodos. (Para mayor confusión, el término trunk también se usa para lo que Cisco denomina “canales”; véase agregado de enlaces). Un enrutador (conmutador de nivel 3) funciona como columna vertebral para el tráfico de red transmitido entre diferentes VLANs.
En los dispositivos Cisco, VTP (VLAN Trunking Protocol) permite definir dominios de VLAN, lo que facilita las tareas administrativas. VTP (Cisco) también permite podar, lo que significa dirigir tráfico VLAN específico sólo a los conmutadores que tienen puertos en la VLAN destino.

2.2.2 ***Segmentación***

Con los switches se crean pequeños dominios, llamados segmentos, conectando un pequeño hub de grupo de trabajo a un puerto de switch o bien se aplica micro segmentación la cual se realiza conectando cada estación de trabajo y cada servidor directamente a puertos de switch teniendo una conexión dedicada dentro de la red, con lo que se consigue aumentar considerablemente el ancho de banda a disposición de cada usuario.
Una de las ventajas que se pueden notar en las VLAN es la reducción en el trafico de la red ya que solo se transmiten los paquetes a los dispositivos que estén incluidos dentro del dominio de cada VLAN, una mejor utilización del ancho de banda y confidencialidad respecto a personas ajenas a la VLAN, alta performance, reducción de latencia, facilidad para armar grupos de trabajo.

2.2.3 ***Tipos de VLAN***

Se han definido diversos tipos de VLAN, según criterios de conmutación y el nivel en el que se lleve a cabo:

- **2.2.3.1 VLAN de nivel 1** (también denominada VLAN basada en puerto) define una red virtual según los puertos de conexión del conmutador;

- **2.2.3.2 VLAN de nivel 2** (también denominada VLAN basada en la dirección MAC) define una red virtual según las direcciones MAC de las estaciones. Este tipo de VLAN

es más flexible que la VLAN basada en puerto, ya que la red es independiente de la ubicación de la estación;

- **2.2.3.3 VLAN de nivel 3**: existen diferentes tipos de VLAN de nivel 3:

  - **2.2.3.3.1 VLAN basada en la dirección de red** conecta subredes según la dirección IP de origen de los datagramas. Este tipo de solución brinda gran flexibilidad, en la medida en que la configuración de los conmutadores cambia automáticamente cuando se mueve una estación. En contrapartida, puede haber una ligera disminución del rendimiento, ya que la información contenida en los paquetes debe analizarse detenidamente.
  - **2.2.3.3.2 VLAN basada en protocolo** permite crear una red virtual por tipo de protocolo (por ejemplo, TCP/IP, IPX, AppleTalk, etc.). Por lo tanto, se pueden agrupar todos los equipos que utilizan el mismo protocolo en la misma red.

2.2.4 *Cisco VLAN Terminología*

Usted necesita algunos detalles para definir una VLAN en la mayoría de los equipos Cisco. Lamentablemente, debido a que Cisco adquiere a veces las tecnologías que utilizan para llenar su conmutación, enrutamiento y seguridad de las líneas de productos, las convenciones de nombres no siempre son coherentes.

- **2.2.4.1 VLAN ID** - La VLAN ID es un valor exclusivo que se asigna a cada VLAN en un único dispositivo. Con el enrutamiento de Cisco o la conmutación de dispositivos que ejecute IOS, su rango es de 1-4096. Al definir una VLAN que suelen utilizar la sintaxis "VLAN x" donde x es el número al que desea asignar a la VLAN ID. VLAN 1 está reservado como una VLAN administrativa. Si la tecnología VLAN está activada, todos los puertos son miembros de la VLAN 1 por defecto.
- **2.2.4.2 VLAN Nombre** - El nombre de VLAN es un texto que se utiliza para identificar su VLAN, tal vez para ayudar a personal técnico en la comprensión de su función. La cadena utilizada puede ser entre 1 y 32 caracteres de longitud.
- **2.2.4.3 Private VLAN** - Usted también puede definir si la VLAN se va a una empresa privada VLAN en la definición, y lo demás VLAN podría estar asociado con él en la sección de definición. Cuando se configura una VLAN de Cisco como una empresa privada-VLAN, esto significa que los puertos que son miembros de la VLAN no pueden comunicarse directamente entre sí por defecto.
  Normalmente todos los puertos que son miembros de una VLAN pueden comunicarse directamente entre sí del mismo modo que sería capaz de haber sido miembro de un segmento de red estándar. VLANs privadas se crean para mejorar la seguridad en una red donde hosts que coexisten en la red no puede ni debe confiar en los demás. Esta es una práctica común de utilizar la Web en granjas o en otros entornos de alto riesgo, cuando la comunicación entre máquinas de la misma subred no son necesarias.
- **2.2.4.4 VLAN modos** - en Cisco IOS, sólo hay dos modos de una interfaz puede operar en "modo de acceso" y "modo de tronco". Modo de acceso es para fines dispositivos o aparatos que no requieren múltiples VLANs. Tronco se utiliza el modo de transmitir

múltiples VLANs a otros dispositivos de red, o para finales de los dispositivos que tienen necesidad de pertenencia a múltiples VLANs a la vez. Si se está preguntando qué modo utilizar, el modo es probablemente "el modo de acceso".

2.2.5 ***Configuración de VLAN***

Una VLAN no sirve de mucho si no le ha sido asignada una dirección IP, máscara de red la subred, y el puerto de miembros. En condiciones normales a un segmento de red en la configuración de routers, interfaces individuales o grupos de interfaces (llamados canales) se asignan las direcciones IP. Cuando usted usa VLANs, las interfaces son miembros de VLANs y no tienen direcciones IP individuales, y, en general, no tienen listas de acceso que se apliquen a ellos. Estas características son generalmente reservadas para las interfaces VLAN.

Y en la "dirección IP " es la dirección que desea asignar este dispositivo en las VLAN, y la máscara de red es para la subred que le han asignado la VLAN.

2.3 VTP (VLAN TRUNKING PROTOCOL)

Protocolo troncal de VLAN (VTP) es una protocolo de capa 2 de mensajería que gestiona la adición, supresión y cambio de VLAN en una red, en toda la base. VTP reduce la administración de una red conmutada. Cuando se configura una nueva VLAN sobre un VTP servidor, el VLAN se distribuye a través de todos los switches en el dominio. Esto reduce la necesidad de configurar la misma VLAN en todas partes. VTP es una propiedad de Cisco que está disponible en la mayoría de los Cisco Catalyst y productos de la familia.

VTP se asegura de que todos los switches en el dominio VTP son consistentes en todas las VLANs. Hay ocasiones, sin embargo, cuando VTP pueden crear tráfico innecesario. Todos los unicasts desconocidos y las emisiones en una VLAN se inundan en toda la VLAN. Todos los switches en la red reciben todas las emisiones, incluso en situaciones en las que pocos usuarios están conectados en esa VLAN. VTP pruning es una característica utilizada para eliminar este tráfico innecesario.

Por defecto, todos los conmutadores Cisco Catalyst están configurados para ser servidores VTP. Esto es adecuado para pequeñas redes en las que el tamaño de la VLAN de información es pequeño y fácilmente almacenado en todos los interruptores (en NVRAM). En una red grande, se debe hacer un juicio en algún momento para saber cuando la NVRAM necesita realizar el almacenamiento si desperdiciar espacio, porque se duplica en cada switch. En este punto, el administrador de red debe elegir unos pocos switches y mantenerlos como servidores VTP. Todo lo demás que participan en VTP puede convertirse en un cliente. El número de servidores VTP debe ser elegido a fin de proporcionar el grado deseado de redundancia en la red.

2.3.1 ***Modos De Operación***

2.3.1.1 Servidor

VTP en modo de servidor, puede crear, modificar y suprimir VLAN y especificar otros parámetros de configuración (tales como VTP versión y poda) para todo el dominio VTP.

VTP publica a sus servidores la configuración de VLAN a los otros switches en el mismo dominio VTP y sincronizar su configuración de VLAN con otros modificadores sobre la base de anuncios recibiendo más enlaces troncales. VTP servidor es el modo por defecto.

2.3.1.2 Transparente

VTP transparente no participa en el VTP. Un VTP transparente no anuncia su configuración VLAN y no se sincroniza su configuración de VLAN basada en la publicidad recibida. Sin embargo, en la versión 2 de VTP transparente se hace avanzar la publicación que recibe de sus puertos troncales.

2.3.1.3 Cliente

VTP cliente se comporta del mismo modo que los servidores VTP, pero no se puede crear, cambiar o suprimir VLAN sobre un VTP cliente.

2.3.2 ***Anuncios***

Las configuraciones VTP en una red son controladas por un número de revisión. Si el número de revisión de una actualización recibida por un switch en modo cliente o servidor es más alto que la revisión anterior, entonces se aplicará la nueva configuración. De lo contrario se ignoran los cambios recibidos. Cuando se añaden nuevos dispositivos a un dominio VTP, se debe resetear los números de revisión de todo el dominio VTP para evitar conflictos. Se recomienda mucho cuidado al usar VTP cuando haya cambios de topología ya sean lógicos o físicos.

2.3.2.1 Anuncios Resumen

Cuando el conmutador recibe un paquete de publicación resumen, compara el nombre de dominio VTP con su propio nombre de dominio VTP. Si el nombre es diferente, el cambio simplemente hace caso omiso de los paquetes. Si el nombre es el mismo, a continuación, el switch compara la configuración de revisión de su propia revisión. Si la configuración de su propia revisión es igual o superior, el paquete es ignorado. Si es inferior, envía un anuncio de la solicitud.

2.3.2.2 Anuncios subconjunto

Al añadir, eliminar o cambiar una VLAN en un switch, cambiara el servidor donde los cambios se hicieron y un resumen de las cuestiones publicadas, seguido por uno o varios subconjuntos de anuncios. Un subconjunto de anuncios contiene una lista de información VLAN. Si hay varias VLAN, más de un subconjunto de publicidad puede ser necesario con el fin de anunciar a todos ellos.

2.3.2.3 Anuncio de pie

Pueden cambiar las necesidades de un anuncio VTP solicitud en las siguientes situaciones:

- El cambio se ha restablecido.
- El nombre de dominio VTP se ha cambiado.
- El cambio ha recibido un anuncio resumen VTP con una mayor revisión de la configuración de su cuenta.

2.3.3 Seguridad VTP

VTP puede operar sin autenticación, en cuyo caso resulta fácil para un atacante falsificar paquetes VTP para añadir, cambiar o borrar la información sobre las VLAN´s. Existen herramientas disponibles gratuitamente para realizar esas operaciones. Debido a eso se recomienda establecer un password para el dominio VTP y usarlo en conjunto con la función hash MD5 para proveer autenticación a los paquetes VTP. Y tan importante es para los enlaces troncales de la vlan

2.4 (STP) SPANNING TREE PROTOCOL

STP es un protocolo de red de la segunda capa OSI, (nivel de enlace de datos). Está basado en un algoritmo diseñado por Radia Perlman mientras trabajaba para DEC. Hay 2 versiones del STP: la original (DEC STP) y la estandarizada por el IEEE (IEEE_802.1D), que no son compatibles entre sí. En la actualidad, se recomienda utilizar la versión estandarizada por el IEEE.

Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología está libre de lazos. STP es transparente a las estaciones de usuario.

Los bucles infinitos ocurren cuando hay rutas alternativas hacia una misma máquina o segmento de red de destino. Estas rutas alternativas son necesarias para proporcionar redundancia, ofreciendo una mayor fiabilidad. Si existen varios enlaces, en el caso que uno falle, otro enlace puede seguir soportando el tráfico de la red. Los problemas aparecen cuando utilizamos dispositivos de interconexión de nivel de enlace, como un puente de red o un conmutador de paquetes.

Cuando hay lazos en la topología de red, los dispositivos de interconexión de nivel de enlace reenvían indefinidamente las tramas Broadcast y multicast, al no existir ningún campo TTL (Time To Live, *Tiempo de Vida*) en la Capa 2, tal y como ocurre en la Capa 3. Se consume entonces una gran cantidad de ancho de banda, y en muchos casos la red queda inutilizada. Un router, por el contrario, si podría evitar este tipo de reenvíos indefinidos. La solución consiste en permitir la existencia de enlaces físicos redundantes, pero creando una topología lógica libre de lazos. STP permite solamente una trayectoria activa a la vez entre dos dispositivos de la red (esto previene los bucles) pero mantiene los caminos redundantes como reserva, para activarlos en caso de que el camino inicial falle.

Si la configuración de STP cambia, o si un segmento en la red redundante llega a ser inalcanzable, el algoritmo reconfigura los enlaces y restablece la conectividad, activando uno de los enlaces de reserva. Si el protocolo falla, es posible que ambas conexiones estén activas simultáneamente, lo que podrían dar lugar a un bucle de tráfico infinito en la LAN.

Existen varias variantes del *Spaning Tree Protocol*, debido principalmente al tiempo que tarda el algoritmo utilizado en converger. Una de estas variantes es el Rapid Spanning Tree Protocol.

El árbol de expansión (Spanning tree) permanece vigente hasta que ocurre un cambio en la topología, situación que el protocolo es capaz de detectar de forma automática. El máximo tiempo de duración del árbol de expansión es de cinco minutos. Cuando ocurre uno de estos cambios, el puente raíz actual redefine la topología del árbol de expansión o se elige un nuevo puente raíz.

2.4.1 ***Funcionamiento***

Este algoritmo cambia una red física con forma de malla, en la que existen bucles, por una red lógica en árbol en la que no existe ningún bucle. Los puentes se comunican mediante mensajes de configuración llamados Bridge Protocol Data Units (B.P.D.U).
El protocolo establece *identificadores por puente* y elige el que tiene la prioridad más alta (el número más bajo de prioridad numérica), como el *puente raíz*. Este puente raíz establecerá el camino de menor coste para todas las redes; cada puerto tiene un parámetro configurable: el Span path cost. Después, entre todos los puentes que conectan un segmento de red, se elige un *puente designado*, el de menor coste (en el caso que haya mismo coste en dos puentes, se elige el que tenga el menor identificador), para transmitir las tramas hacia la raíz. En este puente designado, el puerto que conecta con el segmento, es el *puerto designado* y el que ofrece un camino de menor coste hacia la raíz, el *puerto raíz*. Todos los demás puertos y caminos son bloqueados, esto es en un estado ya estacionario de funcionamiento.

2.4.1.1 Elección del puente raíz

La primera decisión que toman todos los switches de la red es identificar el puente raíz ya que esto afectará al flujo de tráfico. Cuando un switch se enciende, supone que es el switch raíz y envía las BPDU que contienen la dirección MAC de sí mismo tanto en el ID raíz como emisor. Cada switch reemplaza los ID de raíz más alta por ID de raíz más baja en las BPDU que se envían. Todos los switches reciben las BPDU y determinan que el switch que cuyo valor de ID raíz es el más bajo será el puente raíz. El administrador de red puede establecer la prioridad de switch en un valor más pequeño que el del valor por defecto (32768), lo que hace que el ID sea más pequeño. Esto sólo se debe implementar cuando se tiene un conocimiento profundo del flujo de tráfico en la red.

2.4.2 ***Mantenimiento del Spanning Tree***

Cada intervalo de tiempo marcado en el valor "Hello Time" de las BPDU, suele ser 2 segundos, el puente raíz emite un BPDU proponiéndose como raíz. Los puentes designados cambian sus identificadores y recalculan los costes hasta la raíz. Cuando un puente recibe una BPDU en el que el identificador de la raíz es mayor que el suyo propio, intenta convertirse en raíz y envía BPDU's en los que el identificador de la raíz es su propio identificador.
En cambio, si cuando un puente recibe una BPDU en el que el camino a la raíz es mayor que el coste que él mismo puede ofrecer por uno de sus puertos, intenta convertirse en puente designado. Si el coste es el mismo, se compararían identificadores.

El algoritmo converge cuando todos los puertos de los puentes están en estado de envío o bloqueo.

2.4.3 *Estado de los puertos*

Los estados en los que puede estar un puerto son los siguientes:

- **Bloqueo**: En este estado sólo se pueden recibir BPDU's. Las tramas de datos se descartan y no se actualizan las tablas ARP.
- **Escucha**: A este estado se llega desde Bloqueo. En este estado, los switches determinan si existe alguna otra ruta hacia el puente raíz. En el caso que la nueva ruta tenga un coste mayor, se vuelve al estado de Bloqueo. Las tramas de datos se descartan y no se actualizan las tablas ARP. Se procesan las BPDU.
- **Aprendizaje**: A este estado se llega desde Escucha. Las tramas de datos se descartan pero ya se actualizan las tablas ARP (ya se aprenden las direcciones MAC). Se procesan las BPDU.
- **Envío**: A este estado se llega desde Aprendizaje. Las tramas de datos se envían y se actualizan las tablas ARP. Se procesan las BPDU.
- **Desactivado**: A este estado se llega desde cualquier otro. Se produce cuando un administrador deshabilita el puerto o éste falla. No se procesan las BPDU

2.4.4 *Rapid Spanning Tree Protocol*

Rapid Spanning Tree Protocol (RSTP) es un protocolo de red de la segunda capa OSI, (nivel de enlace de datos), que gestiona enlaces redundantes. Especificado en IEEE 802.1w, es una evolución del Spanning tree Protocol (STP), reemplazándolo en la edición 2004 del 802.1d. RSTP reduce significativamente el tiempo de convergencia de la topología de la red cuando ocurre un cambio en la topología.

2.4.4.1 Roles de los puertos RSTP:

Raíz: Un puerto de envío elegido para la topología Spanning Tree.
Designado: Un puerto de envío elegido para cada segmento de la red.
Alternativo: Un camino alternativo hacia el Puente Raíz. Este camino es distinto al que usan los puertos raíz.
Respaldo: Un camino de respaldo/redundante (de mayor costo) a un segmento donde hay otro puerto ya conectado.
Deshabilitado: Un puerto que no tiene un papel dentro de la operación de Spanning Tree.
Los puertos raíz y designado forman parte de la topología activa. Los puertos alternativo y de respaldo no están incluidos en la topología activa

RSTP monitorea el estado de todas las trayectorias:

- Si una dirección activa se cae, RSTP activa las direcciones redundantes.
- Configura de nuevo la topología de la red adecuadamente.
- RSTP es una versión mejorada del STP.

2.4.4.2 Objetivos del RSTP

- Disminuir el tiempo de convergencia cuando un enlace falla.
- De 30 ó 60 s a milisegundos.
- Soporta redes extendidas.
- 2048 conexiones o 4096 puertos interconectados en comparación con 256 puertos conectados en STP.
- Compatibilidad con STP.

Capitulo 3: Enrutamiento

3.1 ¿CÓMO FUNCIONAN LOS PROTOCOLOS DE ENRUTAMIENTO?

Hay 3 procesos básicos que están involucrados en la construcción, mantenimiento y uso de las tablas de enrutamiento. Cada uno de estos procesos es independiente de los demás:

- Los protocolos de enrutamiento envían información respecto de las rutas o redes.
- Las tablas de enrutamiento reciben las actualizaciones de los protocolos de enrutamiento y generan la información necesaria para el proceso de forwarding.
- El proceso de forwarding selecciona una ruta de la tabla de enrutamiento para hacer el reenvío del datagrama.

Estos procesos se ejecutan tomando como base la métrica que es el parámetro que utilizan los protocolos de enrutamiento para definir cuál es la mejor ruta hacia una red de destino.

Las métricas de los principales protocolos son:

- RIP versión 1 y 2 - número de saltos.
- IGRP - ancho de banda, delay, carga y confiabilidad.
- EIGRP - ancho de banda, delay, carga y confiabilidad.
- OSPF - costo.
- IS-IS - costo.

•**La distancia administrativa**: Cuando en un dispositivo se ejecuta más de un proceso de enrutamiento, se utiliza este parámetro para definir la información obtenida a través de qué protocolo actualizará la tabla de ruteo. Es una medida de la confiabilidad de la fuente de información de ruteo. La distancia administrativa es el parámetro utilizado por la tabla de ruteo en la selección de rutas.

•**La longitud del prefijo**: El proceso de forwarding utilizará la ruta cuya definición esté dada por una máscara de subred con mayor cantidad de bits en 1. Es decir, selecciona la ruta más específica.

•**La longitud de la máscara:** es el parámetro utilizado por el proceso de forwarding en el momento de seleccionar una ruta hacia el destino.

3.2 TIPOS DE PROTOCOLOS DE ENRUTAMIENTO:

• 3.2.1 ***Protocolos classful***

Son los protocolos que no transmiten la máscara de subred en sus actualizaciones.

- La sumarización ocurre en los límites de la red.
- Las rutas que se intercambian entre redes diferentes se sumarizan al límite de la clase.
- Dentro de la red, las rutas a las subredes se intercambian sin la máscara de subred.
- Todas las interfaces de los dispositivos deben utilizar la misma máscara de subred.
- Es el caso de los protocolos RIP v.1 e IGRP.

• 3.2.2 ***Protocolos classless***

Son los protocolos que incluyen la máscara de subred en sus actualizaciones.

- Las interfaces de los dispositivos de una misma red pueden tener diferentes máscaras de subred (VLSM).
- Soportan el enrutamiento entre dominios sin utilizar clases (CIDR).
- Algunas rutas pueden ser sumarizadas dentro de los límites de una clase. Esto se hace manualmente.
- Es el caso de los protocolos RIP v.2, OSPF, EIGRP, IS-IS y BGP.

3.2.3 ***Tipos de Enrutamiento***

Los protocolos de enrutamiento proporcionan mecanismos distintos para elaborar y mantener las tablas de enrutamiento de los diferentes routers de la red, así como determinar la mejor ruta para llegar a cualquier host remoto. En un mismo router pueden ejecutarse protocolos de enrutamiento independientes, construyendo y actualizando tablas de enrutamiento para distintos protocolos encaminados.

- **3.2.3.1 Enrutamiento Estático**. El principal problema que plantea mantener tablas de enrutamiento estáticas, además de tener que introducir manualmente en los routers toda la información que contienen, es que el router no puede adaptarse por sí solo a los cambios que puedan producirse en la topología de la red. Sin embargo, este método de enrutamiento resulta ventajoso en las siguientes situaciones:

    - Un circuito poco fiable que deja de funcionar constantemente. Un protocolo de enrutamiento dinámico podría producir demasiada inestabilidad, mientras que las rutas estáticas no cambian.
    - Se puede acceder a una red a través de una conexión de acceso telefónico. Dicha red no puede proporcionar las actualizaciones constantes que requiere un protocolo de enrutamiento dinámico.
    - Existe una sola conexión con un solo ISP. En lugar de conocer todas las rutas globales, se utiliza una única ruta estática.
    - Un cliente no desea intercambiar información de enrutamiento dinámico.

- **3.2.3.2 Enrutamiento Predeterminado**. Es una ruta estática que se refiere a una conexión de salida o Gateway de "último recurso". El tráfico hacia destinos desconocidos por el router se envía a dicha conexión de salida. Es la forma más fácil de enrutamiento para un dominio conectado a un único punto de salida. Esta ruta se indica como la red de destino 0.0.0.0/0.0.0.0.
- **3.2.3.3 Enrutamiento Dinámico**. Los protocolos de enrutamiento mantienen tablas de enrutamiento dinámicas por medio de mensajes de actualización del enrutamiento, que contienen información acerca de los cambios sufridos en la red, y que indican al software del router que actualice la tabla de enrutamiento en consecuencia. Intentar utilizar el enrutamiento dinámico sobre situaciones que no lo requieren es una pérdida de ancho de banda, esfuerzo, y en consecuencia de dinero.

3.3 TIPOS DE DIRECCIONAMIENTO Y OTROS CONCEPTOS

Para el diseño de arquitectura de cualquier red, es también muy importante conocer y utilizar los siguientes conceptos, con el fin de optimizar y simplificar el direccionamiento y el tamaño de las tablas de enrutamiento. Gracias a la utilización de estas técnicas, los datos reales a principios de 2000 mostraban que el tamaño de la tabla de enrutamiento era aproximadamente de 76000 rutas.

- **3.3.1** ***Direccionamiento Con Clase***. Es también conocido como Direccionamiento IP básico. Siguiendo este modelo de direccionamiento, a una dirección IP únicamente se le puede asignar su máscara predeterminada o máscara natural. Esto supone muy poca flexibilidad, y no es recomendable salvo para redes locales muy pequeñas.
- **3.3.2** ***Subnetting***. La técnica de subnetting, permite dividir una red en varias subredes más pequeñas que contienen un menor número de hosts. Esto nos permite adquirir, por ejemplo, una red de clase B, y crear subredes para aprovechar este espacio de direcciones entre las distintas oficinas de nuestra empresa. Esto se consigue alterando la máscara natural, de forma que al añadir unos en lugar de ceros, hemos ampliado el número de subredes y disminuido el número de hosts para cada subred.
- **3.3.3** ***Máscara de Subred de Longitud Variable (VLSM)***. Utilizar protocolos de enrutamiento y dispositivos que soporten VLSM, nos permite poder utilizar diferentes máscaras en los distintos dispositivos de nuestra red, lo cual no es más que una extensión de la técnica de subnetting. Mediante VLSM, podemos dividir una clase C para albergar dos subredes de 50 máquinas cada una, y otra subred con 100 máquinas. Es importante tener en cuenta que RIP1 e IGRP no suportan VLSM.
- **3.3.4** ***Supernetting o Agregación***. La técnica de supernetting o agregación, permite agrupar varias redes en una única superred. Para esto se altera la máscara de red, al igual que se hacía en subnetting, pero en este se sustituyen algunos unos por ceros. El principal beneficio es para las tablas de enrutamiento, disminuyendo

drásticamente su tamaño. Un dominio al que se le ha asignado un rango de direcciones tiene la autoridad exclusiva de la agregación de sus direcciones, y debería agregar todo lo que sea posible siempre y cuando no introduzca ambigüedades, lo cual es posible en el caso de redes con interconexiones múltiples a distintos proveedores.

- **3.3.5 *Notación CIDR***. La notación CIDR, permite identificar una dirección IP mediante dicha dirección, seguida de una barra y un número que identifica el número de unos en su máscara. Así, se presenta una forma de notación sencilla y flexible, que actualmente es utilizada en la configuración de gran cantidad de dispositivos de red. Un ejemplo sería: 194.224.27.00/24.
- **3.3.6 *Convergencia***. La convergencia se refiere al tiempo que tardan todos los routers de la red en actualizarse en relación con los cambios que se han sufrido en la topología de la red.

Todas las interfaces operativas conectadas al router se sitúan en la tabla de enrutamiento. Por ello, si sólo hay un router en la red, éste tiene información sobre todas las redes o subredes diferentes y no hay necesidad de configurar un enrutamiento estático o dinámico.

3.4 ALGORITMOS DE ENRUTAMIENTO POR VECTOR DE DISTANCIA

El término vector de distancia se deriva del hecho de que el protocolo incluye un vector (lista) de distancias (número de saltos u otras métricas) asociado con cada destino, requiriendo que cada nodo calcule por separado la mejor ruta para cada destino. Los envían mensajes actualizados a intervalos establecidos de tiempo, pasando toda su tabla de enrutamiento al router vecino más próximo (routers a los que está directamente conectado), los cuales repetirán este proceso hasta que todos los routers de la red están actualizados. Si un enlace o una ruta se vuelven inaccesibles justo después de una actualización, la propagación del fallo en la ruta se iniciará en la próxima propagación, ralentizándose la convergencia. Los protocolos de vector de distancia más nuevos, como EIGRP y RIP-2, introducen el concepto de actualizaciones desencadenadas. Éstas propagan los fallos tan pronto ocurran, acelerando la convergencia considerablemente. Los protocolos por vector de distancia tradicionales trabajan sobre la base de actualizaciones periódicas y contadores de espera: si no se recibe una ruta en un cierto periodo de tiempo, la ruta entra en un estado de espera, envejece y desaparece, volviéndose inalcanzable.

3.4.1 *Bucles de Enrutamiento en Algoritmos por Vector de Distancia*

Los bucles de enrutamiento producen entradas de enrutamiento incoherentes, debido generalmente a un cambio en la topología. Si un enlace de un router A se vuelve inaccesible, los routers vecinos no se dan cuenta inmediatamente, por lo que se corre el riego de que el router A crea que puede llegar a la red pérdida a través de sus vecinos que mantienen entradas antiguas. Así, añade una nueva entrada a su tabla de enrutamiento con un coste superior. A su vez, este proceso se repetiría una y otra vez, incrementándose

el coste de las rutas, hasta que de alguna forma se parase dicho proceso. Los métodos utilizados para evitar este caso son los que siguen:

- **3.4.1.1 Horizonte Dividido**. La regla del horizonte dividido es que nunca resulta útil volver a enviar información acerca de una ruta a la dirección de dónde ha venido la actualización original.
- **3.4.1.2 Actualización Inversa**. Cuando una red de un router falla, este envenena su enlace creando una entrada para dicho enlace con coste infinito. Así deja de ser vulnerable a actualizaciones incorrectas proveniente de routers vecinos, donde esté involucrada dicha red. Cuando los routers vecinos ven que la red ha pasado a un coste infinito, envían una actualización inversa indicando que la ruta no está accesible.
- **3.4.1.3 Definición de Máximo**. Con este sistema, el protocolo de enrutamiento permite la repetición del bucle hasta que la métrica exceda el valor máximo permitido. Una vez que la red alcanza ese máximo, se considera inalcanzable.
- **3.4.1.4 Actualización desencadenada**. Normalmente, las nuevas tablas de enrutamiento se envían a los routers vecinos a intervalos regulares. Una actualización desencadenada es una nueva tabla de enrutamiento que se envía de forma inmediata, en respuesta a un cambio. El router que detecta el cambio envía inmediatamente un mensaje de actualización a los routers adyacentes que, a su vez, generan actualizaciones desencadenadas para notificar el cambio a todos sus vecinos. Sin embargo surgen dos problemas:
  - Los paquetes que contienen el mensaje de actualización podrían ser descartados o dañados por algún enlace de la red.
  - Las actualizaciones desencadenadas no suceden de forma instantánea. Es posible que un router que no haya recibido aún la actualización desencadenada genere una actualización regular que cause que la ruta defectuosa sea insertada en un vecino que hubiese recibido ya la actualización.

Combinando las actualizaciones desencadenadas con los temporizadores se obtiene un esquema que permite evitar estos problemas

3.5 ALGORITMOS DE ENRUTAMIENTO DE ESTADO DE ENLACE

Utiliza un modelo de base de datos distribuida y replicada. Los routers intercambian paquetes de estado de enlace que informa a todos los routers de la red sobre el estado de sus distintos interfaces. Esto significa que sólo se envía información acerca de las conexiones directas de un determinado router, y no toda la tabla de enrutamiento como ocurre en el enrutamiento por vector de distancia. Aplicando el algoritmo SPF (primero la ruta más corta), más conocido como algoritmo Dijkstra, cada router calcula un árbol de las ruta más cortas hacia cada destino, situándose a sí mismo en la raíz. Los protocolos de estado de enlace no pueden proporcionar una solución de conectividad global, como la que se requiere en grandes redes como Internet, pero si son utilizados por muchos

proveedores como protocolo de enrutamiento en el interior de un SA. Los protocolos más conocidos son OSPF e IS-IS. Algunos de los beneficios de estos protocolos son:

- No hay límite en el número de saltos de una ruta. Los protocolos del estado de enlace trabajan sobre la base de las métricas de enlace en lugar de hacerlo en función del número de saltos.
- El ancho de banda del enlace y los retrasos puede ser factorizados cuando se calcule la ruta más corta hacia un destino determinado.
- Los cambios de enlace y nodo son inmediatamente introducidos en el dominio mediante actualizaciones del estado de enlace.
- Soporte para VLSM y CIDR, ya que intercambian información de máscara en las actualizaciones.

3.6 OPEN SHORTEST PATH FIRST (OSPF)

Es un protocolo de enrutamiento jerárquico de pasarela interior o IGP (Interior Gateway Protocol), que usa el algoritmo Dijkstra enlace-estado (LSA - *Link State Algorithm*) para calcular la ruta más corta posible. Usa *cost* como su medida de métrica. Además, construye una base de datos enlace-estado (*link-state database*, LSDB) idéntica en todos los enrutadores de la zona.

OSPF es probablemente el tipo de protocolo IGP más utilizado en grandes redes. Puede operar con seguridad usando MD5 para autentificar a sus puntos antes de realizar nuevas rutas y antes de aceptar avisos de enlace-estado. Como sucesor natural de RIP, acepta VLSM o *sin clases* CIDR desde su inicio. A lo largo del tiempo, se han ido creando nuevas versiones, como OSPFv3 que soporta IPv6 o como las extensiones multidifusión para OSPF (MOSPF), aunque no están demasiado extendidas. OSPF puede "etiquetar" rutas y propagar esas etiquetas por otras rutas.

Una red OSPF se puede descomponer en redes más pequeñas. Hay un área especial llamada **área backbone** que forma la parte central de la red y donde hay otras áreas conectadas a ella. Las rutas entre diferentes áreas circulan siempre por el backbone, por lo tanto todas las áreas deben conectar con el backbone. Si no es posible hacer una conexión directa con el backbone, se puede hacer un enlace virtual entre redes.

Los encaminadores en el mismo dominio de multidifusión o en el extremo de un enlace punto-a-punto forman enlaces cuando se descubren los unos a los otros. En un segmento de red Ethernet los encaminadores eligen a un encaminador designado (*Designated Router*, DR) y un encaminador designado secundario (*Backup Designated Router*, BDR) que actúan como hubs para reducir el tráfico entre los diferentes encaminadores. OSPF puede usar tanto multidifusiones como unidifusiones para enviar paquetes de bienvenida y actualizaciones de enlace-estado. Las direcciones de multidifusiones usadas son 224.0.0.5 y 224.0.0.6. Al contrario que RIP o BGP, OSPF no usa ni TCP ni UDP, sino que usa IP directamente, mediante el protocolo IP 89.

3.6.1 *Tráfico de enrutamiento*

OSPF mantiene actualizada la capacidad de enrutamiento entre los nodos de una red mediante la difusión de la topología de la red y la información de estado-enlace de sus distintos nodos. Esta difusión se realiza a través de varios tipos de paquetes:

- **3.6.1.1 Paquetes *Hello*** (tipo 1). Cada *router* envía periódicamente a sus vecinos un paquete que contiene el listado de vecinos reconocidos por el *router*, indicando el tipo de relación que mantiene con cada uno.
- **3.6.1.2 Paquetes de descripción de base de datos estado-enlace (*DataBase Description*, DBD)**.
- **3.6.1.3 Paquetes de estado-enlace o *Link State Advertisements* (LSA)**. Los cambios en el estado de los enlaces de un *router* son notificados a la red mediante el envío de mensajes LSA. Dependiendo del estatus del *router* y el tipo de información transmitido en el LSA, se distinguen varios formatos: *Router-LSA* o LSA de encaminador, *Network-LSA* o LSA de red, *Summary-LSA* o LSA de resumen (de dos tipos, tipo 3, dirigidos a un router fronterizo de red; y tipo 4, dirigidos a una subred interna) y *AS-External-LSA* o LSA de rutas externas a la red. En OSPFv3, los *Summary-LSA* tipo 3 son renombrados como *Inter-Area-Prefix-LSA* y los *Summary-LSA* tipo 4 pasan a denominarse *Intra-Area-Prefix-LSA*. Además, se añade un nuevo formato, el *Link-LSA* o LSA de enlace.

3.6.2 *Áreas*

Una red OSPF está dividida en áreas. Estas áreas son grupos lógicos de Routers cuya información se puede resumir para el resto de la red. Los cambios en un área no afectan al rendimiento de otras áreas, esto permite a OSPF limitar el tráfico a estas áreas. Se pueden definir diferentes tipos de áreas "especiales":

3.6.2.1 Área Backbone

El *backbone*, también denominado área cero, forma el núcleo de una red OSPF. Es la única área que debe estar presente en cualquier red OSPF, y mantiene conexión, física o lógica, con todas las demás áreas en que esté particionada la red. Los routers que conectan un área con el *backbone* se denominan *Area Border Routers* (ABR, routers fronterizos de área), y son responsables de la gestión de las rutas no-internas del área (esto es, de las rutas entre el área y el resto de la red).

3.6.2.2 Área *stub*

Un área *stub* es aquella que no recibe rutas externas. Las rutas externas se definen como rutas que fueron inyectadas en OSPF desde otro protocolo de enrutamiento. Por lo tanto, las rutas de segmento necesitan normalmente apoyarse en las rutas predeterminadas para poder enviar tráfico a rutas fuera del segmento.

3.6.2.3 Área *not-so-stubby*

También conocidas como NSSA se trata de un tipo de área *stub* que puede importar rutas externas de sistemas autónomos y enviarlas al backbone, pero no puede recibir rutas externas de sistemas autónomos desde el backbone u otras áreas.

3.6.3 *Interfaces en OSPF*

Los nodos de una red basada en OSPF se conectan a ella a través de una o varias interfaces con las que se conectan a otros nodos de la red. El tipo de enlace (*link*) define la configuración que asume la interface correspondiente. OSPF soporta las siguientes tipos de enlace, y provee para cada uno de ellos una configuración de interfaz:

- Punto a punto (*point-to-point*, abreviadamente ptp).
- Punto a multipunto (*point-to-multipoint*, abreviadamente ptmp).
- Broadcast.
- Enlace virtual (*virtual link*).
- Enlace de múltiple acceso no-broadcast (*Non-broadcast Multiple Access*, NBMA).

3.6.4 *Relación con los vecinos en OSPF*

Diagrama de estados de vecinos y transiciones entre estados en OSPF.

Cada encaminador OSPF realiza un seguimiento de sus nodos vecinos, estableciendo distintos tipos de relación con ellos. Respecto a un encaminador dado, sus vecinos pueden encontrarse en siete estados diferentes. Los vecinos OSPF progresan a través de estos estados siguiendo el diagrama de la derecha.

3.6.4.1 Estado Desactivado (DOWN)

En el estado desactivado, el proceso OSPF no ha intercambiado información con ningún vecino. OSPF se encuentra a la espera de pasar al siguiente estado (Estado de Inicialización)

3.6.4.2 Estado de Inicialización (INIT)

Los *routers* (enrutadores) OSPF envían paquetes tipo 1, o paquetes Hello, a intervalos regulares con el fin de establecer una relación con los Routers (encaminadores) vecinos. Cuando una interfaz recibe su primer paquete Hello, el *router* (encaminador) entra al estado de Inicialización. Esto significa que este sabe que existe un vecino a la espera de llevar la relación a la siguiente etapa.

Los dos tipos de relaciones son Bidireccional y Adyacencia. Un *router* (encaminador) debe recibir un paquete Hello (Hola) desde un vecino antes de establecer algún tipo de relación.

3.6.4.3 Estado Bidireccional (TWO-WAY)

Empleando paquetes Hello, cada enrutador OSPF intenta establecer el estado de comunicación bidireccional (dos-vías) con cada enrutador vecino en la misma red IP. Entre otras cosas, el paquete Hello incluye una lista de los vecinos OSPF conocidos por el origen. Un enrutador ingresa al estado Bidireccional cuando se ve a sí mismo en un paquete Hello proveniente de un vecino.

El estado Bidireccional es la relación más básica que vecinos OSPF pueden tener, pero la información de encaminamiento no es compartida entre estos. Para aprender los estados de enlace de otros encaminadores y eventualmente construir una tabla de encaminamiento, cada encaminador OSPF debe formar a lo menos una adyacencia. Una adyacencia es una relación avanzada entre encaminadores OSPF que involucra una serie de estados progresivos basados no sólo en los paquetes Hello, si también en el intercambio de otros 4 tipos de paquetes OSPF. Aquellos encaminadores intentando

volverse adyacentes entre ellos intercambian información de encaminamiento incluso antes de que la adyacencia sea completamente establecida. El primer paso hacia la adyacencia es el estado ExStart.

3.6.4.4 Estado EXSTART

Técnicamente, cuando un encaminador y su vecino entran al estado ExStart, su conversación es similar a aquella en el estado de Adyacencia. ExStart se establece empleando descripciones de base de datos tipo 2 (paquetes DBD), también conocidos como DDPs. Los dos encaminadores vecinos emplean paquetes Hello para negociar quien es el "maestro" y quien es el "esclavo" en su relación y emplean DBD para intercambiar bases de datos.

Aquel encaminador con el mayor router ID "gana" y se convierte en el maestro. Cuando los vecinos establecen sus roles como maestro y esclavo entran al estado de Intercambio y comienzan a enviar información de encaminamiento.

3.6.4.5 Estado de Intercambio (EXCHANGE)

En el estado de intercambio, los encaminadores vecinos emplean paquetes DBD tipo 2 para enviarse entre ellos su información de estado de enlace. En otras palabras, los encaminadores se describen sus bases de datos de estado de enlace entre ellos. Los encaminadores comparan lo que han aprendido con lo que ya tenían en su base de datos de estado de enlace. Si alguno de los encaminadores recibe información acerca de un enlace que no se encuentra en su base de datos, este envía una solicitud de actualización completa a su vecino. Información completa de encaminamiento es intercambiada en el estado Cargando.

3.6.4.6 Estado Cargando (LOADING)

Después de que las bases de datos han sido completamente descritas entre vecinos, estos pueden requerir información más completa empleando paquetes tipo 3, requerimientos de estado de enlace (LSR). Cuando un enrutador recibe un LSR este responde empleando un paquete de actualización de estado de enlace tipo 4 (LSU). Estos paquetes tipo 4 contienen las publicaciones de estado de enlace (LSA) que son el corazón de los protocolos de estado de enlace. Los LSU tipo 4 son confirmados empleando paquetes tipo 5 conocidos como confirmaciones de estado de enlace (LSAcks).

3.6.4.7 Estado de Adyacencia completa (FULL)

Cuando el estado de carga ha sido completado, los enrutadores se vuelven completamente adyacentes. Cada enrutador mantiene una lista de vecinos adyacentes, llamada base de datos de adyacencia.

3.7 ROUTING INFORMATION PROTOCOL (RIP)

RIP son las siglas de Routing Information Protocol (Protocolo de encaminamiento de información). Es un protocolo de puerta de enlace interna o IGP (Internal Gateway Protocol) utilizado por los routers (enrutadores), aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

3.7.1 *Versiones RIP*

En la actualidad existen tres versiones diferentes de RIP, las cuales son:

- **3.7.1.1 RIPv1**: No soporta subredes ni CIDR. Tampoco incluye ningún mecanismo de autentificación de los mensajes. No se usa actualmente. Su especificación está recogida en el RFC 1058.
- **3.7.1.2 RIPv2**: Soporta subredes, CIDR y VLSM. Soporta autenticación utilizando uno de los siguientes mecanismos: no autentificación, autentificación mediante contraseña, autentificación mediante contraseña codificada mediante MD5 (desarrollado por Ronald Rivest). Su especificación está recogida en RFC 1723 y en RFC 2453.
- **3.7.1.3 RIPng**: RIP para IPv6. Su especificación está recogida en el RFC 2080.

También existe un RIP para IPX, que casualmente lleva el mismo acrónimo, pero no está directamente relacionado con el RIP para redes IP, ad-hoc.

3.7.2 *Funcionamiento RIP*

RIP utiliza UDP para enviar sus mensajes y el puerto 520.
RIP calcula el camino más corto hacia la red de destino usando el algoritmo del vector de distancias. La distancia o métrica está determinada por el número de saltos de router hasta alcanzar la red de destino.
RIP tiene una distancia administrativa de 120 (la distancia administrativa indica el grado de confiabilidad de un protocolo de enrutamiento, por ejemplo EIGRP tiene una distancia administrativa de 90, lo cual indica que a menor valor mejor es el protocolo utilizado)
RIP no es capaz de detectar rutas circulares, por lo que necesita limitar el tamaño de la red a 15 saltos. Cuando la métrica de un destino alcanza el valor de 16, se considera como infinito y el destino es eliminado de la tabla (inalcanzable).
La métrica de un destino se calcula como la métrica comunicada por un vecino más la distancia en alcanzar a ese vecino. Teniendo en cuenta el límite de 15 saltos mencionado anteriormente. Las métricas se actualizan sólo en el caso de que la métrica anunciada más el coste en alcanzar sea estrictamente menor a la almacenada. Sólo se actualizará a una métrica mayor si proviene del enrutador que anunció esa ruta.
Las rutas tienen un tiempo de vida de 180 segundos. Si pasado este tiempo, no se han recibido mensajes que confirmen que esa ruta está activa, se borra. Estos 180 segundos, corresponden a 6 intercambios de información.

3.7.3 *Mensajes RIP*

Los mensajes RIP pueden ser de dos tipos.
3.7.3.1 Petición: Enviados por algún enrutador recientemente iniciado que solicita información de los enrutadores vecinos.
3.7.3.2 Respuesta: mensajes con la actualización de las tablas de enrutamiento. Existen tres tipos:

Mensajes *ordinarios*: Se envían cada 30 segundos. Para indicar que el enlace y la ruta siguen activos.

Mensajes enviados como *respuesta* a mensajes de petición.
Mensajes enviados cuando *cambia algún coste*. Se envía toda la tabla de routing.

3.7.3.3 Formatos de los mensajes RIP

Los mensajes tienen una cabecera que incluye el tipo de mensaje y la versión del protocolo RIP, y un máximo de 25 entradas RIP de 20 bytes.
Las entradas en RIPv1 contienen la dirección IP de la red de destino y la métrica.
Las entradas en RIPv2 contienen la dirección IP de la red de destino, su máscara, el siguiente enrutador y la métrica. La autentificación utiliza la primera entrada RIP.

3.7.4 ***Actualizaciones de Enrutamiento***

El protocolo RIP envía mensajes de actualización de enrutamiento cuando detecta que la topología de la red ha cambiado. Cuando un router recibe un mensaje de actualización que incluye cambios no registrados, este actualiza su propia tabla para asentar la nueva ruta. El valor de la métrica para el mensaje es aumentado por el router en uno, y el origen es indicado como el próximo salto. Los enrutamientos con RIP utilizan solamente la mejor ruta (la que tenga la métrica más baja) hacia un destino. Luego de que un router actualiza sus tablas, inmediatamente comienza a transmitir la información de actualización de enrutamiento a los routers vecinos. Estas actualizaciones son enviadas independientemente de las actualizaciones programadas que RIP envía.

3.7.5 ***Métrica de Enrutamiento de RIP***

RIP utiliza una métrica simple para determinar las distancias entre un origen y un destino. Esta métrica se mide en "saltos", cada salto esta determinados por cada router que atraviesa la información. Con cada salto desde el origen hacia el destino es aumentado en uno un contador. Cuando un router recibe una actualización de enrutamiento que contiene una nueva ruta o algún cambio con respecto a sus propias tablas, el router modifica sus tablas, y luego agrega un valor a la métrica, esto indica que las tablas han sido actualizadas, la dirección IP del origen será utilizada para el próximo salto.

3.7.6 ***Prevención de loops***

El protocolo Rip previene loops continuos implementando un límite de saltos desde el origen al destino final. El número máximo de saltos permitido por el protocolo RIP es de 15 saltos. Si un router recibe una actualización que contiene una nueva entrada o algún cambio no registrado, y el aumento del valor del campo de salto llega a 16 o lo supera, el destino de la red se considera inalcanzable.

3.7.7 ***Aspectos de estabilidad de RIP***

Para ajustarse rápidamente a los cambios en la red, RIP especifica un número de parámetros de estabilidad que son comunes a muchos protocolos de enrutamiento. RIP, por ejemplo, implementa el llamado Horizonte Dividido y el mecanismo de

Temporizadores de espera para prevenir que se propague información de enrutamiento incorrecta. Además, el protocolo RIP previene los loops de enrutamiento utilizando el método de cuenta al infinito.

3.7.8 *RIP Timers*

RIP utiliza una gran cantidad de relojes para regular su performance. Estos relojes llamados como timers y no traduciremos sus significados para no alejarnos de la denominación más usual. Entre ellos se incluyen los routing-update timer, route timeout y route-flush timer. Los routing-update timer establecen el intervalo entre las actualizaciones de tablas de enrutamiento periódicas. Por lo general, este valor esta seteado en 30 segundos, con un rango muy pequeño de segundos agregados a cada tiempo para prevenir colisiones. Cada entrada en las tablas de enrutamiento tienen un route timeout timer asociado con ellas. Cuando el route timeout timer expira, la ruta es señalada como invalida, pero no es borrada de la tabla hasta que expira el route-flush timer.

Capitulo 4: Seguridad

Sin el desarrollo de nuevas tecnologías de asignación de direcciones IP, el rápido crecimiento de Internet habría agotado la cantidad actual de direcciones IP. Para compensar esta falta de direcciones IP, se buscaron diferentes soluciones. Una solución ampliamente implementada es la Traducción de direcciones de red (NAT) el cual es un mecanismo para conservar direcciones IP registradas en las grandes redes y simplificar las tareas de administración de direccionamiento IP.

Mientas se enruta un paquete a través de un dispositivo de red, por lo general un firewall o router fronterizo, la dirección IP fuente se traduce de una dirección de red interna privada a una dirección IP pública enrutable. Esto permite que se transporte el paquete a través de redes externas públicas como la Internet. La dirección pública de la respuesta se traduce de nuevo a la dirección interna privada para su entrega dentro de la red interna. Una variación de NAT, conocida como Traducción de direcciones de puerto (PAT), permite la traducción de muchas direcciones privadas internas con una sola dirección pública externa.

Los routers, servidores y otros dispositivos fundamentales de la red por lo general requieren de una configuración IP estática, la cual se introduce de forma manual. Sin embargo, los clientes de escritorio no necesitan una dirección específica, sino una que pertenezca a un rango de direcciones. Este rango se encuentra por lo general dentro de una subred IP. A una estación de trabajo dentro de una red específica se le puede asignar cualquier dirección dentro de un rango, mientras que otros valores son estáticos, incluyendo la máscara de subred, el gateway por defecto y el servidor DNS.

El protocolo de configuración dinámica de host (DHCP) se diseñó para asignar las direcciones IP y toda información de configuración de red importante de forma dinámica. Como los clientes de escritorio por lo general conforman la mayoría de los nodos de red, el DHCP es una herramienta muy útil que ahorra tiempo a los administradores de red.

4.1 TIPOS DE DIRECCIONES IP

Según la clasificación de las direcciones de red, se cuenta con los siguientes bloques de direcciones IP privadas:

- Una dirección Clase A
- Dieciséis direcciones de Clase B
- 256 direcciones Clase C

Estas direcciones son sólo para el uso particular de la red interna. Los paquetes que contienen a estas direcciones no se enrutan a la Internet.

Clase	Intervalo de direcciones internas RFC 1918	Prefijo CIDR
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16

Tabla 4.1 Tipos de direcciones IP

Las direcciones IP privadas son direcciones reservadas y cualquiera las puede utilizar. Eso quiere decir que distintas redes, pueden utilizar la misma dirección privada. Un router nunca debe enrutar las direcciones privadas fuera de una red interna. Los ISP por lo general configuran los routers fronterizos para impedir que el tráfico direccionado de forma privada se envíe al exterior. NAT ofrece grandes beneficios a empresas individuales y a la Internet. Antes del desarrollo de NAT, un host con dirección privada no podía acceder a la Internet. Con NAT, las empresas individuales pueden direccionar algunos o todos sus hosts con direcciones privadas y utilizar NAT para brindar acceso a la Internet.
Al hablar de NAT podemos encontrar las siguientes definiciones:

- **4.1.1 *Dirección local interna*:** la dirección IP asignada al host en la red interna la cual por lo general no es asignada por el Centro de Información de la Red de Internet (InterNIC) o el proveedor de servicios.
- **4.1.2 *Dirección global interna*:** una dirección IP legítima asignada por InterNIC o un proveedor de servicios que representa una o más direcciones IP locales internas al mundo exterior.
- **4.1.3 *Dirección local externa*:** la dirección IP de un host externo, como la conocen los hosts en la red interna.
- **4.1.4 *Dirección global externa*:** la dirección IP asignada a un host en la red externa. El dueño del host asigna esta dirección.

4.2 TRADUCCIÓN DE DIRECCIÓN DE RED (NAT)

Network Address Translation: es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.
Su uso más común es permitir utilizar direcciones privadas (definidas en el RFC 1918) y aún así proveer conectividad con el resto de Internet. Existen rangos de direcciones privadas que pueden usarse libremente y en la cantidad que se quiera dentro de una red privada. Si el número de direcciones privadas es muy grande puede usarse solo una parte de direcciones públicas para salir a Internet desde la red privada. De esta manera simultáneamente sólo pueden salir a Internet con una dirección IP tantos equipos como direcciones públicas se hayan contratado. Esto es necesario debido al progresivo agotamiento de las direcciones IPv4. Se espera que con el advenimiento de IPv6 no sea necesario continuar con esta práctica.

4.2.1 ***Funcionamiento***

El protocolo TCP/IP tiene la capacidad de generar varias conexiones simultáneas con un dispositivo remoto. Para realizar esto, dentro de la cabecera de un paquete IP, existen campos en los que se indica la dirección origen y destino con sus respectivos puertos. Esta combinación de números define una única conexión.
Una pasarela NAT cambia la dirección origen en cada paquete de salida y, dependiendo del método, también el puerto origen para que sea único. Estas traducciones de dirección se almacenan en una tabla, para recordar qué dirección y puerto le corresponde a cada dispositivo cliente y así saber donde deben regresar los paquetes de respuesta. Si un paquete que intenta ingresar a la red interna no existe en la tabla de traducciones, entonces es descartado. Debido a este comportamiento, se puede definir en la tabla que en un determinado puerto y dirección se pueda acceder a un determinado dispositivo, como por ejemplo un servidor web, lo que se denomina NAT inverso o DNAT (Destination NAT).
NAT tiene muchas formas de funcionamiento, entre las que destaca:

4.2.1.1 Estático (SNAT)

Es un tipo de NAT en el que una dirección IP privada se traduce a una dirección IP pública, y donde esa dirección pública es siempre la misma. Esto le permite a un host, como un servidor Web, el tener una dirección IP de red privada pero aún así ser visible en Internet.

4.2.1.2 Dinámico

Es un tipo de NAT en la que una dirección IP privada se mapea a una IP pública basándose en una tabla de direcciones de IP registradas (públicas). Normalmente, el router NAT en una red mantendrá una tabla de direcciones IP registradas, y cuando una IP privada requiera acceso a Internet, el router elegirá una dirección IP de la tabla que no esté siendo usada por otra IP privada. Esto permite aumentar la seguridad de una red dado que

enmascara la configuración interna de una red privada, lo que dificulta a los hosts externos de la red el poder ingresar a ésta. Para este método se requiere que todos los hosts de la red privada que deseen conectarse a la red pública posean al menos una IP pública asociada.

4.2.1.3 Sobrecarga

La forma más utilizada de NAT, proviene del NAT dinámico, ya que toma múltiples direcciones IP privadas (normalmente entregadas mediante DHCP) y las traduce a una única dirección IP pública utilizando diferentes puertos. Esto se conoce también como PAT (Port Address Translation - Traducción de Direcciones por Puerto), NAT de única dirección o NAT multiplexado a nivel de puerto.

4.2.1.4 Solapamiento

Cuando las direcciones IP utilizadas en la red privada son direcciones IP públicas en uso en otra red, el ruteador posee una tabla de traducciones en donde se especifica el reemplazo de éstas con una única dirección IP pública. Así se evitan los conflictos de direcciones entre las distintas redes.

4.2.2 *Características Principales*

Las traducciones NAT se pueden usar para una variedad de propósitos y pueden asignarse de manera dinámica o estática. NAT estática está diseñada para permitir que cada dirección local se mapee a su correspondiente dirección global. Esto resulta particularmente útil para los hosts que deban tener una dirección constante que esté accesible desde la Internet. Estos hosts internos pueden ser servidores de empresas o dispositivos de networking.

NAT dinámica está diseñada para mapear una dirección IP privada a una dirección pública. Cualquier dirección IP de un conjunto de direcciones IP públicas se asigna a un host de red. La sobrecarga, o Traducción de direcciones de puerto (PAT), mapea varias direcciones IP privadas a una sola dirección IP pública. Se pueden mapear varias direcciones a una sola dirección porque cada dirección privada se diferencia por el número de puerto.

PAT utiliza números únicos de puerto origen en la dirección IP global interna para distinguir entre las traducciones. El número de puerto se codifica en 16 bits. En teoría, el número total de direcciones internas que se pueden traducir a una dirección externa podría ser hasta 65,536 por dirección IP. En realidad, el número de puertos que se pueden asignar a una sola dirección IP es aproximadamente 4000.

PAT intenta preservar el puerto origen original. Si el puerto origen está en uso, PAT asigna el primer número de puerto disponible comenzando desde el principio del grupo de puertos correspondiente 0-511, 512-1023, o 1024-65535. Cuando no hay más puertos disponibles y hay más de una dirección IP externa configurada, PAT utiliza la próxima dirección IP para tratar de asignar nuevamente el puerto origen original. Este proceso continúa hasta que no haya puertos ni direcciones IP externas disponibles.

4.2.3 *Ventajas de NAT*

- Elimina la reasignación de una nueva dirección IP a cada host cuando se cambia a un nuevo ISP. NAT elimina la necesidad de re-direccionar todos los hosts que requieran acceso externo, ahorrando tiempo y dinero.
- Conserva las direcciones mediante la multiplexión a nivel de puerto de la aplicación. Con PAT, los hosts internos pueden compartir una sola dirección IP pública para toda comunicación externa. En este tipo de configuración, se requieren muy pocas direcciones externas para admitir muchos hosts internos, y de este modo se conservan las direcciones IP
- Protege la seguridad de la red. Debido a que las redes privadas no publican sus direcciones o topología interna, ellas son razonablemente seguras cuando se las utiliza en conjunto con NAT para tener un acceso externo controlado.

4.3 TRADUCCIÓN DE DIRECCIONES DE PUERTO (PAT)

Port Address Translation (PAT) es una característica del estándar NAT que traduce conexiones TCP y UDP hechas por un host y un puerto en una red externa a otra dirección y puerto de la red interna. PAT permite que una sola dirección IP sea utilizada por varias máquinas de la intranet. Con PAT, una IP externa puede responder hasta a 64000 direcciones internas.

Éste método permite a varias máquinas de la intranet compartir una sola dirección en Internet, cualquier paquete IP contiene la dirección y el puerto tanto del origen como del destino. En el destino, el puerto le dice al receptor cómo procesar el paquete, un paquete con puerto 80 indica que contiene una página web, mientras que el puerto 25 es usado para transmitir correo electrónico entre servidores de correo. La traducción de los puertos, llamada PAT para distinguirla de la traducción de direcciones (NAT), se apoya en el hecho de que el puerto de origen carece de importancia para la mayoría de los protocolos. Igual que NAT, PAT se sitúa en la frontera entre la red interna y externa, y realiza cambios en la dirección del origen y del receptor en los paquetes de datos que pasan a través de ella. Los puertos (no las ips), se usan para designar diferentes hosts en el intranet. El servicio PAT es como una oficina de correo que entrega las cartas. El sobre se cambia para que el remitente sea la oficina de correos, mientras que las cartas que llegan de fuera pierden su dirección y reciben la nueva con la calle y el número real.

Cuando un ordenador del intranet manda un paquete hacia fuera, queremos ocultar su dirección real. El servicio PAT remplaza la IP interna con la nueva IP del propio servicio. Luego asigna a la conexión un puerto de la lista de puertos disponibles, inserta el puerto en el campo apropiado del paquete de datos y envía el paquete. El servicio NAT crea una entrada en su tabla de direcciones IP internas, puertos internos y puertos externos. A partir de entonces, todos los paquetes que provengan del mismo hosts serán traducidos con los mismos puertos.

El receptor del paquete utilizará los ip y puerto recibidos para responder, por lo que dicha respuesta llegará a la "oficina de correos". Inicialmente, si el puerto destino no existe en la tabla del NAT, los datos serán descartados. En otro caso, la nueva dirección y el nuevo puerto reemplazarán los datos de destino en el paquete y éste será enviado por la red interna. La traducción de puertos permite a varias máquinas compartir una única dirección IP. El servicio PAT borra las traducciones periódicamente de su tabla cuando aparenten no estar en uso. Como el número de posibles puertos a otorgar es de 16 bit (65535), la probabilidad de que un ordeandor no encuentre una traducción es realmente pequeña.

4.4 LISTAS DE CONTROL DE ACCESO (ACL´S)

Las Listas de Control de Acceso se pueden usan para aplicar una política de seguridad que permite o deniega el acceso de cierta parte de una red a otra área de la misma. Estas partes o segmentos pueden ser desde ciertas computadoras específicas hasta partes de una subred o una subred completa, es decir, permite que se conceda o niegue el acceso desde un único PC hasta otro, de un segmento de red a otro o cualquier combinación que se quiera.

También se puede decir que una ACL es un conjunto de reglas contra las que se compara cada paquete que cruce una interfaz en la que se instaló la lista de acceso. Cada paquete se compara contra las reglas una por una empezando por la primera y continuando con las siguientes. Sólo si el paquete no corresponde a lo que indica una regla se continúa con las siguientes, una vez que el paquete se corresponde con una de las reglas de la ACL, se le aplica la acción asociada a la regla y no se compara el paquete con ninguna otra regla. Las ACLs entonces son reglas, una por línea, que se identifican con un número o una palabra y que identifican flujos de datos o conjuntos de direcciones. Cada regla hace uso de una dirección de referencia y una máscara wildcard que condicionan la acción a ejecutar sobre un paquete en cuestión. La condición consiste en que los paquetes coincidan con la dirección de referencia en los bits que la máscara wildcard tenga en cero, por lo tanto si una wildcard es 0.0.0.0 significa que todos los bits de la dirección origen o destino de un paquete que cruce la interfaz por la que está instalada la ACL se comparará bit a bit con la dirección de referencia, de esa manera yo especifico una dirección completa de host. La dificultad de diseñar e instalar ACLs radica en la dificultad de concebir los patrones de tráfico como un conjunto de paquetes heterogéneos que pasan por una interfaz en una dirección en particular.

4.4.1 *WILDCARDS*

Una máscara wildcard es una cantidad de 32-bits que se divide en cuatro octetos. Una máscara wildcard se compara con una dirección IP. Los números uno y cero en la máscara se usan para identificar cómo tratar los bits de la dirección IP correspondientes. El término máscara wildcard es la denominación aplicada al proceso de comparación de bits de máscara y proviene de una analogía con el "wildcard" (comodín) que equivale a cualquier otro naipe en un juego de póquer. Las máscaras wildcard no guardan relación funcional con las máscaras de subred. Se utilizan con distintos propósitos y siguen distintas reglas.

Las máscaras de subred y las máscaras de wildcard representan dos cosas distintas al compararse con una dirección IP. Las máscaras de subred usan unos y ceros binarios para identificar las porciones de red, de subred y de host de una dirección IP. Las máscaras de wildcard usan unos y ceros binarios para filtrar direcciones IP individuales o en grupos, permitiendo o rechazando el acceso a recursos según el valor de las mismas. La única similitud entre la máscara wildcard y la de subred es que ambas tienen 32 bits de longitud y se componen de unos y ceros.

4.4.2 *ACL´s estándar*

Dentro de las ACL más comunes están las ACL estándar y las ACL extendidas, las extendidas permiten más detalles de filtrado y ambos tipos de listas se pueden numerar o nombrar. Las más simples son las ACLs estándar, que permiten definir tráfico con base en las direcciones IP de origen de los paquetes que correspondan con las reglas de la ACL.
Las ACL estándar entonces especifican un sólo par dirección de referencia/wildcard contra el que se comparan todos los paquetes que entren o salgan de la interfaz en la que se instale la ACL, en otras palabras, una ACL estándar filtra tráfico con base en la dirección IP origen de los paquetes. Estas ACL se crean en modo de configuración global con el comando *access-list* seguido de un número de *1 a 99 o de 1300 a 1999,* estos rangos identifican que el tipo de ACL es estándar, otros rangos identifican ACLs extendidas (100 a 199 y 2000 a 2699).
Cada regla debe tener el mismo número para pertenecer a la misma ACL, si el número cambia, la regla en particular pertenecerá a otra ACL. Luego de *Access-list <número>* sigue la acción a ejecutar (*permit* o *deny*) y finalmente la condición que deben cumplir los paquetes para aplicarles la acción o continuar examinando más reglas. Las ACL estándar usan un sólo par dirección/wildcard para especificar la condición que deben cumplir los paquetes para que se les aplique la acción *permit* o *deny*. La condición examina la dirección IP origen de cada paquete y la compara con el par dirección/wildcard pero sólo en los bits en los que la wildcard tenga ceros.
Una consideración importante es tener en cuenta siempre que las listas de acceso terminan en denegación por defecto, por lo tanto, si una ACL sólo tiene reglas de denegación lo único que logra es denegar TODO el tráfico. Una ACL debe tener siempre por lo menos una regla de permitir.

4.4.3 *ACL´s extendida*

A diferencia de lo que sucede con la ACL estándar, las extendidas permiten especificar hacia dónde se dirige el tráfico. Con ésta característica se puede bloquear o permitir un tráfico de una manera mucho más específica. De esta forma se logra comparar las direcciones destino de los paquetes contra la ACL, no sólo las direcciones origen. En las ACL´s extendidas se especifican dos pares de direcciones de referencia/wildcard, un par para la dirección origen de los paquetes y otro par para la dirección destino de los mismos.

Capitulo 5: PRACTICAS DE REDES EN LA ESIME UNIDAD CULHUACAN

Para especificaciones del laboratorio y equipo ver Anexos.

5.1 PRACTICA RIP 1, RIP 2 y OSPF

5.1.1 *Introducción*

En la siguiente práctica veremos algunas de las configuraciones básicas de los router, así como la habilitación de las formas de ruteo como el ruteo estático que aunque es poco común en forma aislada en la práctica, se utiliza mucho en forma combinada con algunos protocolos de ruteo para establecer las preferencias del administrador de red no contempladas dentro de algún protocolo, un protocolo de vector-distancia que es de los más comunes RIP y un protocolo de enlace-estado el más común OSPF; ya que estos son los más representativos de dichas métricas dentro de los protocolos de enrutamiento y también veremos algunas variantes de los mismos en cuanto a las versiones RIP, puesto que la versión 1 que ya es poco utilizada no nos permite el manejo de enmascaramiento variable entre otras características esta es de las más representativas de la versión 2 o de la complejidad de OSPF ya que como hemos visto anteriormente utiliza la métrica del costo y esta métrica involucra varios factores los cuales pueden ser configurados por el administrador de red, pero es preferente que el mismo protocolo realice los cálculos más exactos para determinar los elementos que determinan dicha métrica del costo .

5.1.2 *Objetivos*

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología
- Realizar las tareas de configuración básicas en un router
- Asignar los protocolos de ruteo RIP versión 1 y 2
- Reconocer las diferencias entre RIP 1 y 2
- Asignar el protocolo de ruteo OSPF
- Asignar el ruteo estático de una red
- Reconocer las diferencias entre el ruteo por vector-distancia y estado-enlace
- Guardar la configuración de las tablas de ruteo
- Modificar las configuraciones de la tabla de ruteo
- Eliminar las rutas establecidas en un router

5.1.3 *Equipo a utilizar*

a. 3 routers 2800
b. 1 switch 2960
c. 1 switch 3550
d. 1 switch 500
e. 5 PCV's

5.1.4 *Desarrollo*

5.1.4.1 Topología

Paso 1: Construcción de la topología:

Conecta tres routers como se muestra en el diagrama, a cada router conéctale un switch y a cada switch las PC's que desees. Y siguiendo la configuración inicial del router mencionada anteriormente asígnales los nombres: D.F.; GUADALAJARA y MONTERREY.

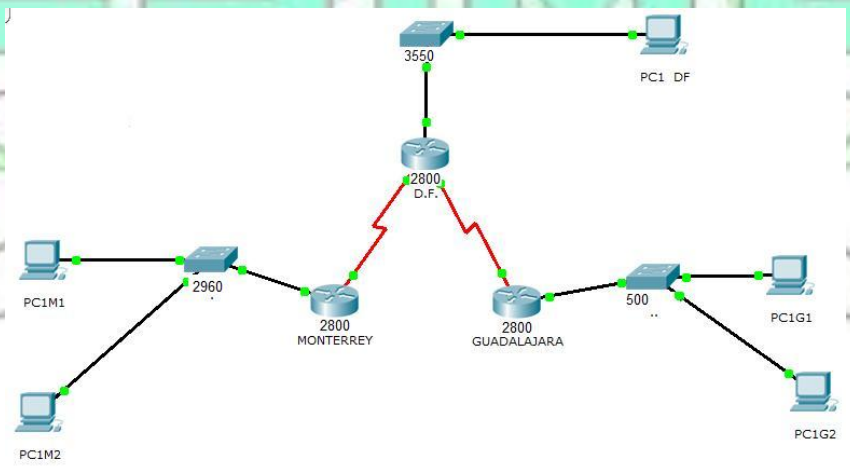

Imagen 5.1 Topología RIP-OSPF

Conectaremos a cada equipo de la siguiente manera: para cada router y su configuración tenemos que utilizar un cable de consola que viene con el mismo router de cisco router (este cable también se utiliza para la configuración del switch), este cable es el de configuración que el lado que va conectado a la pc es el DB9 y el lado que va conectado al puerto de consola del router es Ethernet. El router DF lo vamos a conectar con un cable serial de su puerto serial 0/0 al router GUADALAJARA a su puerto serial 0/1 ya, el router MONTERREY lo vamos a conectar con un cable serial de su puerto serial 0/0 al puerto serial 0/1 del router DF, a cada router lo conectaremos con su respectivo switch con un cable 1 a 1 ethernet, ya sea, con la configuración TIA/EIA 568-A u TIA/EIA 568-B; procure utilizar una sola norma en todo el cableado que utilizaremos, ya que, garantiza el buen

funcionamiento de nuestra practica. El cable uno a uno que se conecta del router DF será del puerto fastethernet 0/0 al puerto 24 del switch, en el router MONTERREY conectaremos de igual forma su switch como en el caso del router Df y lo mismo con el router GUADALAJARA y cada PC la conectaremos con nuestro cable 1 a 1 en cualquier puerto de nuestro switch.

5.1.4.2 Direccionamiento

VLAN	Puerto	Dirección IP	Mascara de Subred
VLAN 10	FA 0/0.10	172.17.10.1	255.255.255.0
VLAN 20	FA 0/0.20	172.17.20.1	255.255.255.0
VLAN 30	FA 0/0.30	172.17.30.1	255.255.255.0
VLAN 40	FA 0/0.40	172.17.40.1	255.255.255.0
VLAN 50	FA 0/0.50	172.17.50.1	255.255.255.0

Tabla 5.2 Direccionamiento de VLAN's-Router

5.1.4.3 Configuraciones Básicas

Paso 2: Configure las interfaces seriales y ethernet de los tres routers. Configure las interfaces de los routers, las interfaces seriales tendrán la red 192.168.1.0, la interfaz Ethernet del D.F. tendrá la red 192.168.2.0, la de Guadalajara 192.168.3.0 y Monterrey 192.168.4.0.

D.F.> **enable**
Ingresa a modo privilegiado
D.F.# **configure terminal**
Ingresa en modo de configuración global
D.F.(config)# **interface serial 0/0**
Ingresa en modo de configuración de la interface
D.F.(config-if)# **ip address 192.168.1.1 255.255.255.0**
Asigna una dirección ip y una máscara de red a la interface serial
D.F.(config-if)# **clock rate 56000**
Configure un reloj de sincronización para la transferencia de datos y su velocidad puesto que es un equipo DCE
D.F.(config-if)# **no shutdown**
Habilita la interfaz
D.F.(config-if)# **exit**

Repite el proceso anterior pero en el router DF solo que este no llebara reloj puesto que es un equipo DTE en la interfaz serial 0/1

D.F.(config)# **interface serial 0/1**
D.F.(config-if)# **ip address 192.168.1.2 255.255.255.0**
D.F.(config-if)# **no shutdown**
D.F.(config-if)# **exit**

D.F.(config)# **interface fastethernet 0/1**
D.F.(config-if)# **ip address 192.168.2.1 255.255.255.0**
Se le asigna una dirección ip y una máscara de red a la interface ethernet
D.F.(config-if)# **no shutdown**
Habilita la interface
D.F.(config)# **exit**

Se repite el proceso en el router Guadalajara para configurar sus interfaces, contemplando que su interface serial es una DCE y lleva un reloj

GUADALAJARA# **enable**
GUADALAJARA# **configure terminal**
GUADALAJARA(config)# **interface serial 0/0**
GUADALAJARA(config-if)# **ip address 192.168.1.3 255.255.255.0**
GUADALAJARA(config-if)# **clock rate 56000**
GUADALAJARA(config-if)# **no shutdown**
GUADALAJARA(config-if)# **exit**
GUADALAJARA(config)# **interface fastethernet 0/1**
GUADALAJARA(config-if)# **ip address 192.168.3.1 255.255.255.0**
GUADALAJARA(config-if)# **no shutdown**
GUADALAJARA(config)# **exit**

Se repite el proceso en el router Monterrey para configurar sus interfaces, contemplando que su interface serial es una DTE por lo que no lleva reloj

MONTERREY# **enable**
MONTERREY# **configure terminal**
MONTERREY(config)# **interface serial 0/1**
MONTERREY(config-if)# **ip address 192.168.1.4 255.255.255.0**
MONTERREY(config-if)# **no shutdown**
MONTERREY(config-if)# **exit**
MONTERREY(config)# **interface fastethernet 0/1**
MONTERREY(config-if)# **ip address 192.168.4.1 255.255.255.0**
MONTERREY(config-if)# **no shutdown**
MONTERREY(config)# **exit**

Paso 3: Verifique el direccionamiento IP y las interfaces. Utilice el comando **show ip interface brief** para verificar que el direccionamiento IP es correcto y que las interfaces están activas. Cuando haya finalizado, asegúrese de guardar la configuración en ejecución para la NVRAM del router.

D.F.# **copy running-config startup-config**
GUADALAJARA# **copy running-config startup-config**
MONTERREY# **copy running-config startup-config**
Guarda la configuración en la memoria para cuando se apague o reinicie este la conserve

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol

FastEthernet0/0        192.168.9.158   YES manual up                    up

FastEthernet0/1        unassigned      YES manual administratively down down

Serial0/0/0            192.168.9.161   YES manual up                    up

Serial0/0/1            192.168.9.193   YES manual up                    up
```

Imagen 5.2 show brief OSPF

Paso 4: Configure las interfaces Ethernet de las PCS de las tres LAN. Configure las interfaces Ethernet de las PCS con las direcciones IP y gateways por defecto.

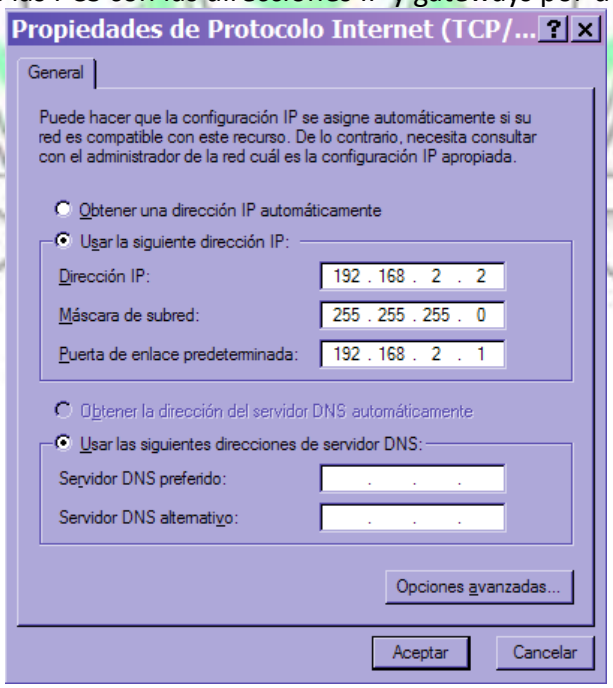

Imagen 5.3 TCP/IP

Se hace en todas las PC con los datos especificados en la siguiente tabla:

Router	PC	IP	Mascara de red	Getway
DF	PC1DF	192.168.2.2	255.255.255.0	192.168.2.1
GUADALAJARA	PC1G1	192.168.3.2	255.255.255.0	192.168.3.1
GUADALAJARA	PC2G1	192.168.3.3	255.255.255.0	192.168.3.1
MONTERREY	PC1M1	192.168.4.2	255.255.255.0	192.168.4.1
MONTERREY	PC2M2	192.168.4.3	255.255.255.0	192.168.4.1

Tabla 5.2 Direccionamiento PC-Router

Paso 5: Pruebe la configuración de la PC ejecutando un ping desde la PC al gateway por defecto.

5.1.4.4 Configuración de ruteo estático y cuestionario.

Paso 6: *Se establecen las ip y las rutas de cada red para alcanzar la siguiente*

DF(config)# ip route 192.168.3.0 255.255.255.0 serial 0/0
DF(config)# ip route 192.168.4.0 255.255.255.0 serial 0/1
GUADALAJARA(config)# ip route 192.168.2.0 255.255.255.0 serial 0/0
MONTERREY(config)# ip route 192.168.2.0 255.255.255.0 serial 0/1

Donde:
Ip route X I
X: Direccion Ip destino + mascara
I: interface por la que llega a esta red

Paso 7: *Configuración de la ruta estática por defecto.* Cuando el destino al que se pretende llegar son múltiples redes o no se conocen se pueden crear rutas estáticas por defecto. También se puede hacer para eliminar las rutas establecidas.

DF(config)# ip route 0.0.0.0 0.0.0.0 serial 0/0
DF(config)# ip route 0.0.0.0 0.0.0.0 serial 0/1
GUADALAJARA(config)# ip route 0.0.0.0 0.0.0.0 serial 0/0
MONTERREY(config)# ip route 0.0.0.0 0.0.0.0 serial 0/1
Los parametros son los mismos que en el ruteo estatico definido anteriormente

Cuestionario
¿Qué dirección Ip se debe especificar en el ruteo estático?
La dirección IP de la red destino
¿Cuándo se aconsejan las rutas estáticas?
Cuando un circuito de datos es poco fiable, cuando existe una sola conexión y cuando se accede a la red a través de una conexión de acceso telefónico

¿Cuándo se aconsejan las rutas estáticas por defecto?
Cuando el destino son multiples redes o no se conocen las redes destino
¿Si se desconoce la interfaz de salida que otro parámetro se puede utilizar?
La IP del primer salto

5.1.4.5 Configurar el protocolo RIP y cuestionario.

Paso 8: *Habilite un enrutamiento dinámico***.** Para habilitar un protocolo de enrutamiento dinámico, ingrese al modo de configuración global y utilice el comando **router**. Para habilitar RIP, ingrese el comando **router rip** en el modo de configuración global. Una vez que se encuentre en el modo de configuración de enrutamiento, ingrese la dirección de red con clase para cada red conectada directamente por medio del comando **network**.

DF(config)#**router rip**
Activa el protocolo de ruteo RIP
DF(config-router)# **network 192.168.1.0**
DF(config-router)# **network 192.168.2.0**
Se le debe de decir cuáles son las redes que se encuentran directamente conectadas al router tanto en sus interfaces seriales como ethernet
DF(config-router)# **end**

Se realize el mismo proceso en el router Guadalajara
GUADALAJARA(config)#**router rip**
GUADALAJARA(config-router)# **network 192.168.1.0**
GUADALAJARA(config-router)# **network 192.168.3.0**
GUADALAJARA(config-router)# **end**

Se realice el mismo proceso el router Monterrey
MONTERREY(config)#**router rip**
MONTERREY(config-router)# **network 192.168.1.0**
MONTERREY(config-router)# **network 192.168.4.0**
MONTERREY(config-router)# **end**

Para cambiar la versión de RIP
MONTERREY(config)#**router rip**
MONTERREY(config)#**version 2**

Paso 9: *Al finalizar la configuración RIP, regrese al modo EXEC privilegiado y guarde la configuración actual para la NVRAM*.

DF#**copy run start**
GUADALAJARA#**copy run start**

MONTERREY#**copy run start**
Guarda la configuración en la memoria para cuando se apague o reinicie este la conserve

Verificar el enrutamiento RIP.

Paso 10: *Utilice el comando show ip route para verificar que cada router cuente con todas las redes en la topología ingresadas en la tabla de enrutamiento*.
Las rutas reveladas a través de RIP se codifican con una **R** en la tabla de enrutamiento. Si las tablas no convergen como se muestra a continuación, resuelva los problemas de configuración. ¿Verificó que las interfaces configuradas estén activas? ¿Configuró RIP correctamente? Regrese a la Tarea 3 y a la Tarea 4 para revisar los pasos necesarios para lograr la convergencia.

DF#**show ip route**
GUADALAJARA#**show ip route**
MONTERREY#**show ip route**
Muestra las tablas de ruteo establecidas por el protocol RIP

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

Gateway of last resort is not set

     192.168.9.0/27 is subnetted, 7 subnets
S       192.168.9.0 [1/0] via 192.168.9.162
S       192.168.9.32 [1/0] via 192.168.9.162
S       192.168.9.64 [1/0] via 192.168.9.194
S       192.168.9.96 [1/0] via 192.168.9.194
C       192.168.9.128 is directly connected, FastEthernet0/0
C       192.168.9.160 is directly connected, Serial0/0/0
C       192.168.9.192 is directly connected, Serial0/0/1
```

Imagen 5.4 Show IP route RIP

Paso 11: *Utilice el comando show ip protocols para visualizar la información acerca de los procesos de enrutamiento*. El comando **show ip protocols** se puede utilizar para visualizar información acerca de los procesos de enrutamiento que se producen en el router. Se puede utilizar este resultado para verificar los parámetros RIP para confirmar que:

- El uso del enrutamiento RIP está configurado.
- Las interfaces correctas envían y reciben las actualizaciones RIP.
- El router notifica las redes correctas.
- Los vecinos RIP están enviando actualizaciones.

DF#**show ip protocols**
GUADALAJARA#**show ip protocols**
MONTERREY#**show ip protocols**
Muestra el o los protocolos activos y sus características

Paso 12: *Utilice el comando debug ip rip para visualizar los mensajes RIP que se envían y reciben.* Las actualizaciones rip se envían cada 30 segundos, por lo que deberá esperar para visualizar la información de depuración.

DF#**debug ip rip**
GUADALAJARA#**debug ip rip**
MONTERREY#**debug ip rip**
Muestra los mensajes que el protocolo RIP envía

Paso 13: *Detenga el resultado de la depuración con el comando undebug all.*
DF#**undebug all**
GUADALAJARA#**undebug all**
MONTERREY#**undebug all**
Detiene el envió de mensajes

Cuestionario

¿Si no se especifica la versión de RIP cual adopta?
La versión 1 pero recibe actualizaciones de ambas versiones
¿Con que comando puedo verificar la configuración de RIP?
Show ip route
¿Con que comando cambio la versión del RIP?
Con "versión 2"
¿Cuál es la principal diferencia de RIP versión 1 y 2?
Que RIP versión 2 maneja el enmascaramiento variable

5.1.4.6 Configurar enrutamiento OSPF y cuestionario.

Paso 14: Borrar el enrutamiento de los routers.

DF# **no router rip**
Desactiva el protocolo de RIP
DF# **no ip route 192.168.1.1 255.255.255.0 serial 0/0**
DF# **no ip route 192.168.1.2 255.255.255.0 serial 0/1**
DF# **no ip route 192.168.2.1 255.255.255.0 fastethernet 0/1**

Elimina las rutas mencionadas la cual inicia con la red, su máscara y la interfaz, estas se pueden observar mediante el comando show ip rout mostrado más adelante
Se repite el proceso en el router Guadalajara
GUADALAJARA# **no router rip**
GUADALAJARA# **no ip route 192.168.1.3 255.255.255.0 serial 0/0**
DGUADALAJARA# **no ip route 192.168.3.1 255.255.255.0 fastethernet 0/1**

Se repite el proceso en el router Monterrey
MONTERREY# **no router rip**
MONTERREY# **no ip route 192.168.1.4 255.255.255.0 serial 0/1**
MONTERREY# **no ip route 192.168.4.1 255.255.255.0 fastethernet 0/1**

Si existieran mas rutas también se deberán borrar se puede revisar con el comando
DF# **show ip route**
GUADALAJARA# **show ip route**
MONTERREY# **show ip route**

Y de la misma manera borrar las rutas restantes.

Paso 15: *Utilizar el comando router ospf en el modo de configuración global para habilitar OSPF en el router DF.*

Ingrese una ID de proceso 1 para el parámetro *process-ID*.

DF(config)#**router ospf 1**
Activa el protocolo de ruteo OSPF
GUADALAJARA(config)#**router ospf 1**
Activa el protocolo de ruteo OSPF
MONTERREY(config)#**router ospf 1**
Activa el protocolo de ruteo OSPF

Paso 16: *Configurar la sentencia de red para la red LAN.*

El comando OSPF network utiliza una combinación de *network-address* y *wildcard-mask* similar a la que puede utilizar EIGRP. A diferencia de EIGRP, es necesaria la máscara wildcard en OSPF.

Utilice una ID de área 0 para el parámetro OSPF *area-id*. 0 se utilizará para la ID de área OSPF en todas las sentencias **network** en esta topología.

DF(config-router)#**network 192.168.1.1 0.0.0.255 area 0**
DF(config-router)#**network 192.168.1.2 0.0.0.255 area 0**
DF(config-router)#**network 192.168.2.1 0.0.0.255 area 0**

Se le indica las redes directamente conectadas
DF(config-router)#**end**

Se repite el proceso en el router Guadalajara
GUADALAJARA(config-router)#**network 192.168.1.3 0.0.0.255 area 0**
GUADALAJARA(config-router)#**network 192.168.3.1 0.0.0.255 area 0**
GUADALAJARA(config-router)# **end**

Se repite el proceso en el router Monterrey
MONTERREY(config-router)#**network 192.168.1.4 0.0.0.255 area 0**
MONTERREY(config-router)#**network 192.168.4.1 0.0.0.255 area 0**
MONTERREY(config-router)# **end**

Paso 17: *Verificar que todos los datos introducidos sean correctos mediante los siguientes comandos:*

DF# **show ip protocols**
Muestra el o los protocolos activos y sus características
DF#**show ip ospf neighbors**
Muestra la información de los vecinos ospf

GUADALAJARA# **show ip protocols**
Muestra el o los protocolos activos y sus características
GUADALAJARA# **show ip ospf neighbors**
Muestra la información de los vecinos ospf

MONTERREY# **show ip protocols**
Muestra el o los protocolos activos y sus características
MONTERREY# **show ip ospf neighbors**
Muestra la información de los vecinos ospf

Cuestionario

¿Cuál es el área 0?
Es el área principal o backbone
¿Qué redes se deben anunciar en el comando network?
Solo las directamente conectadas
¿Cuál es la diferencia entre la identificación de las network en comparación con RIP?
Que OSPF las identifica por su wildcard
¿Pueden existir múltiples procesos OSPD en ejecución?
Si

5.2 PRACTICA VLAN, VTP Y STP

5.2.1 *Introducción*

La práctica que a continuación elaboraremos nos permitirá tener conocimientos de los temas antes mencionados.
Las **VLAN** como sus siglas en ingles nos dicen son redes de área local virtuales, es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un switch capa 3). En tanto el **VTP** Se encarga de manejar las vlans configuradas en la red y mantener la consistencia entre los switches. Para que VTP administre las vlans, debe crearse un servidor VTP. Todos los servidores que necesiten compartir información usarán el mismo dominio, y un switch sólo podrá estar en un dominio a la vez. Es decir, un switch sólo compartira la información con los otros switches del mismo domino VTP.
El **STP** (Spanning Tree Protocol) es un estándar utilizado en la administración de redes, basado en el algoritmo de Árbol Abarcador, para describir como los puentes y conmutadores puedes comunicarse para evitar bucles en la red.
El protocolo STP automatiza la administración de la topología de la red con enlaces redundantes, la función principal del protocolo spanning-tree es permitir rutas conmutadas/puenteadas duplicadas sin considerar los efectos de latencia de los loops en la red.

5.2.2 *Objetivos de aprendizaje*

Al completar esta práctica de laboratorio podrá:

- Cablear una red según el diagrama de topología
- Borrar la configuración inicial y volver a cargar un switch al estado predeterminado
- Realizar las tareas de configuración básicas en un switch
- Configurar las VLAN y el protocolo VLAN Trunking (VTP)
- Asignar puertos de switch a una VLAN
- Agregar, mover y cambiar puertos
- Verificar la configuración de la VLAN
- Habilitar el enlace troncal
- Verificar la configuración de enlace troncal
- Modificar los modos VTP y observar el impacto.
- Crear las VLAN en el servidor VTP y distribuir la información de estas VLAN a los switches en la red.

- Observar y explicar el comportamiento predeterminado del Protocolo Spanning Tree (STP, 802.1D)
- Observar la respuesta a un cambio en la topología del spanning tree.
- Guardar la configuración de la VLAN.

5.2.3 *Equipo a Utilizar*

1. 11 pc´s.
2. Switch Series 2960.
3. Switch 3550.
4. Router Series 2800.
5. Cables de consola.

5.2.4 *Desarrollo*

5.1.4.1 Topología

Cablear una red de manera similar al diagrama de topología.
Puede utilizar cualquier switch actual en su práctica de laboratorio siempre y cuando éste tenga las interfaces.

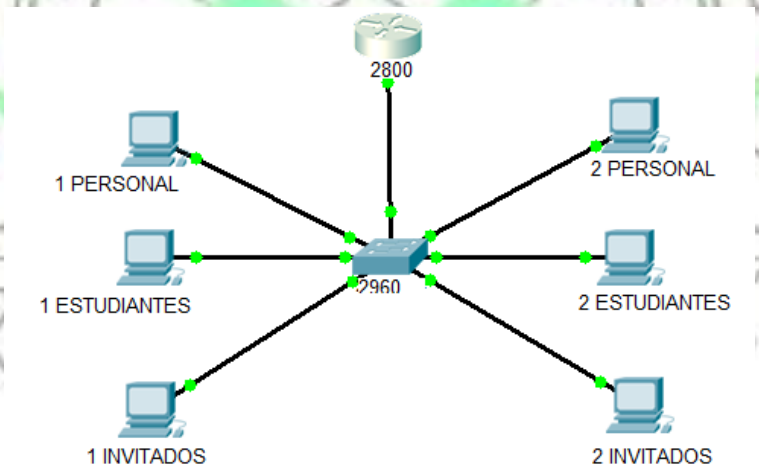

Imagen 5.5 Topología VLAN

En esta práctica el cableado que utilizaremos para conectar lo siguiente: para la configuración del router necesitamos un cable de configuración (consola) que el extremo del conector DB9 va a ir a la pc que utilizaremos para configurar dicho router (este cable también se utiliza para la configuración del switch), y el extremo con conector Ethernet lo conectaremos en el puerto de consola de nuestro router. El cable que conectara el switch al router será un cable Ethernet 1 a 1, como mencionamos anteriormente este tipo de cable debe de tener la misma norma para su buen funcionamiento este lo conectaremos

del puerto Ethernet 0/0 del router al puerto 24 de nuestro switch, y el cableado de las pc serán 1 a 1.

5.2.4.2 Direccionamiento

Tabla de Direccionamiento

A cada pc se le asignaran las siguientes direcciones para poder empezar a trabajar con las vlan.

Nombre de Host	Dirección IP	Mascara de Subred	Gateway
1 Personal	172.17.10.21	255.255.255.0	172.17.10.1
2 Personal	172.17.10.24	255.255.255.0	172.17.10.1
3 Personal	172.17.10.25	255.255.255.0	172.17.10.1
1 Estudiantes	172.17.20.22	255.255.255.0	172.17..20.1
2 Estudiantes	172.17.20.25	255.255.255.0	172.17..20.1
3 Estudiantes	172.17.20.26	255.255.255.0	172.17..20.1
1 Invitados	172.17.30.23	255.255.255.0	172.17..30.1
2 Invitados	172.17.30.26	255.255.255.0	172.17..30.1
3 Invitados	172.17.30.27	255.255.255.0	172.17..30.1
Biblioteca	172.17.40.10	255.255.255.0	172.17..40.1
Dirección General	172.17.50.10	255.255.255.0	172.17..50.1

Tabla 5.3 Direccionamiento PC-VLAN's

Direccionamiento para R1

VLAN	Puerto	Dirección IP	Mascara de Subred
VLAN 10	FA 0/0.10	172.17.10.1	255.255.255.0
VLAN 20	FA 0/0.20	172.17.20.1	255.255.255.0
VLAN 30	FA 0/0.30	172.17.30.1	255.255.255.0
VLAN 40	FA 0/0.40	172.17.40.1	255.255.255.0
VLAN 50	FA 0/0.50	172.17.50.1	255.255.255.0

Tabla 5.4 Direccionamiento VLAN's

5.2.4.3 Configuraciones Básicas

Realizar las configuraciones básicas del switch *(ver anexos para switch 500)*

Paso 1: *Configurar los switches* de acuerdo con la siguiente guía:

Configure el nombre de host del switch.
switch(config)# **hostname A**
Deshabilite la búsqueda DNS.
Configure una contraseña de modo EXEC: **clase**.
A(config)# **enable password calse**
Configure la contraseña **cisco** para las conexiones de consola.
A(config)# **line console 0**
A(config-line)# **password cisco**
Configure la contraseña **cisco** para las conexiones de vty.
A(config)#**line vty 0 4**
A(config)# **password cisco**
A(config)#**login**

5.2.4.4 Configuración de VLAN'S y cuestionario

Configurar y activar las interfaces Ethernet

Paso 2: *Configurar las vlan en el switch A. (ver anexos para switch 500)*

Utilice el comando vlan *vlan-id* en modo de configuración global para añadir una VLAN al switch A. Hay cuatro VLAN configuradas para esta práctica de laboratorio: VLAN 10 (personal); VLAN 20 (estudiantes); VLAN 30 (invitados) y la VLAN 99(administración). Después de crear la VLAN, estará en modo de configuración de vlan, donde puede asignar un nombre para la VLAN mediante el comando name *vlan name*.

A(config)#**vlan 10**
SE LE ASIGNA EL NUMERO A LA VLAN
A(config-vlan)#**name personal**
SE LE ASIGNA EL NOMBRE A DICHA VLAN
A(config-vlan)#**vlan 20**
A(config-vlan)#**name estudiantes**
REPETIMOS LO ANTERIOR CON LAS SIGUIENTES VLAN QUE NOS PIDE LA TABLA
A(config-vlan)#**vlan 30**
A(config-vlan)#**name invitados**

Paso 3: *Verificar que las VLAN estén creadas en A*. Use el comando show vlan brief para verificar que las VLAN se hayan creado.
A#**show vlan brief**

```
VLAN Name                                Status
---- ----------------------------------- ---------
1    default                             active



10   PERSONAL                            active
20   ESTUDIANTES                         active
30   INVITADOS                           active
40   BIBLIOTECA                          active
50   DIRECCIONGENERAL                    active
```

Imagen 5.6 Show VLAN brief

Paso 4: *Asignar puertos de switch a las VLAN en A* . Los puertos se asignan a las VLAN en modo de configuración de interfaces, utilizando el comando switchport access vlan *vlan-id*. Puede asignar cada puerto en forma individual o se puede utilizar el comando interface range para simplificar la tarea, como se muestra en este ejemplo. Los comandos se muestran sólo para A, pero B se debe configurar de manera similar. Guarde la configuración al terminar.

A(config)#**interface fa0/1**
Entrar a la configuración del puerto Ethernet 1
A(config-if-range)#**switchport access vlan 10**
Asignación de la vlan 10 al puero 1
A(config-if-range)#**interface fa0/2**
A(config-if-range)#**switchport access vlan 20**
A(config-if-range)#**interface fa0/3**
A(config-if-range)#**switchport access vlan 30**
A(config-if-range)#**end**
A#**copy running-config startup-config**
Se guardan todos los cambios hechos en el switch A.

Paso 5: *Configurar el enlace troncal.*
Los enlaces troncales son conexiones entre los switches que permiten a los mismos intercambiar información para todas las VLAN. De manera predeterminada, un puerto troncal pertenece a todas las VLAN, a diferencia del puerto de acceso que sólo puede pertenecer a una sola VLAN. Si el switch admite tanto el encapsulamiento de VLAN ISL como el de 802.1Q, los enlaces troncales deben especificar qué método utilizan.

Cuestionario:

Al enviar un ping entre los host personal 1 y personal 3 ¿Qué sucede? Mencione el comportamiento de la red.

_____
_____

Haga un ping entre un host de la vlan estudiantes y un host de la vlan biblioteca.
Hay comunicación_____.
¿Porqué?_____
_____

Configurar las VLAN en el router R1.

Se deben de dar de alta las VLAN creadas en el switch para que pueda existir la comunicación.

PASO 6: *Dar de alta la interfaz del puerto utilizada en cada VLAN con el id de la VLAN correspondiente. Con el siguiente comando:*
R1(config)# **int fast ethernet 0/0.10**
0/0.10 es el id de la VLAN 10

PASO 7: *Configurar la encapsulación.*
R1(config-if)# **encapsulation dot1q (# VLAN)**

PASO 8: *Proporcionar una dirección ip a la interfaz y dar de alta la misma.*
R1(config-if)# **ip add 172.17.10.1 255.255.255.0**
R1(config-if)# **no shut**
Hacer lo mismo para las otras dos VLAN en el router R1.

PASO 9: *Copiar las configuraciones en la NVRAM*.
RI#copy running-config startup-config

Cuestionario.

1. **Hacer un ping entre un host de la vlan estudiantes y un host de la vlan persona, mencionar si existe comunicación y el porqué.**_____
2. **¿Por qué es necesaria la configuración de un router cuando utilizamos vlan en nuestra red?**_____
   _____

5.2.4.5 Configurar VTP y Cuestionario

PASO 10: *Conectar un switch mas en la topología* y conectarlo al switch A para conformar el VTP. En el switch B conectar 5 PC más, para que quede una topología similar a la siguiente:

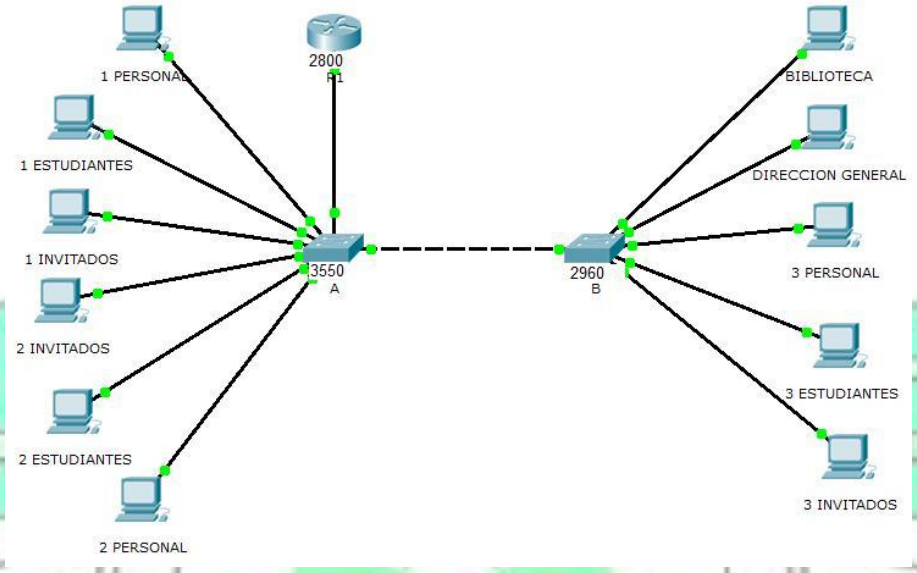

Imagen 5.7 Topología VTP

Paso 11: *Proporcionar direcciones IP* a los HOST que están conectadas al switch B.

El cable que utilizaremos para conectar ambos switches será un cable cruzado que será conectado del puerto 23 el switch A al puerto 24 del switch B.

Paso 12: *Configurar el modo operativo*, el nombre de dominio y la contraseña de VTP en los dos switches. Establezca LAB como nombre de dominio VTP y cisco como contraseña en los dos switches. Configure A en modo servidor y B en modo cliente.

A(config)#vtp mode server
Modo dispositivo ya es SERVIDOR VTP.
A(config)#**vtp domain Lab**
Cambiar el nombre del dominio VTP de NULL a Lab
A(config)#**vtp password cisco**
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco A(config)#end
Salir de el modo configuración del switch A.
B(config)#**vtp mode client**
Configurar el dispositivo en modo CLIENTE VTP
B(config)#**vtp domain Lab**
Cambiar el nombre del dominio VTP de NULL a Lab

B(config)#**vtp password cisco**
Configurar la contraseña de la base de datos VLAN del dispositivo en cisco
B(config)#**end**

Paso 13: *Configurar los enlaces troncales y la VLAN nativa* para los puertos de enlace troncales en los tres switches. Simplifique esta tarea con el comando interface range en el modo de configuración global.
B(config)#interface fa0/24
Entrar a la configuracion del Puerto 24 del switch B.
B(config-if-range)#switchport mode trunk

Paso 14: *Dar de alta las VLAN en el switch* A y asignar los puertos de interfaz que están directamente conectadas al switch B, y darlos de alta en las VLAN correspondiente.

A(config)# vlan # **de vlan**
A(config-vlan)# **name PERSONAL**
Hacer lo mismo para las siguientes VLAN

B(config)# **interface fa 0/1**
B(config-if)# **switchport mode access**
B(config-if)# **switchport access vlan 10**
Realizar las mismas configuraciones para las demas interfaces.

Paso 15: *Dar de alta las VLAN* 10, 20, 30,40 y 50 en el router R1 con los siguientes comandos:

R1(config)# **int fa 0/0.10**
0/0.10 es el id de la VLAN (10)
R1(config)# **encapsulation dot1q (# VLAN)**
R1(config-if)# **ip add 172.17.10.1 255.255.255.0**
R1(config-if)# **no shut**

Paso 16: *Realizar ping entre las PC de diferentes VLAN* para checar que exista comunicación entre todas las VLAN de la red. Los ping deben ser exitosos, en dado caso que no haya comunicación entre las PC checar que estén creadas las VLAN tanto en el router R1 como en los switches A y B y que el direccionamiento sea el correcto.

Paso 17: *Copiar la configuración en la NVRAM.*
RI#**copy running-config startup-config**

Cuestionario.

1. ¿Qué sucede cuando conectamos el nuevo switch?

2. ¿Existe comunicación entre las vlan de cada switch?
3. ¿Por qué?

5.2.4.6 Configuraciones STP y cuestionario

Paso 18: *Borrar toda configuración existente en los switches*. Borre la NVRAM, borre el archivo vlan.dat y reinicie los switches. Después de que la recarga se haya completado, utilice el comando privilegiado EXEC **show vlan** para verificar que sólo existan vlan predeterminadas y que todos los puertos se asignen a VLAN 1.

S1#**show vlan**
Muestra la vlan del switch.

Construir una topología parecida a la siguiente:

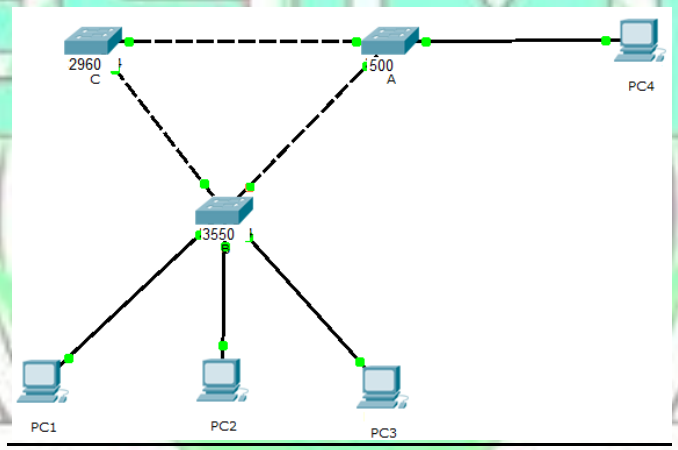

Imagen 5.8 Topología STP

Al conectar esta red tenemos que utilizar 3 cables cross – over que tendrán que ser conectados del switch A al switch C, del switch A al switch B y del switch B al switch C. las PC´S estarán conectadas con sus cables 1 a 1 que sean de la misma norma. El cable de configuración de cada switch será un cable de consola.

Paso 19: *Configurar los parámetros básicos del switch.(ver anexos para switch 500)*
Configure los switches A, B y C según las siguientes pautas:

Configure el nombre de host del switch.
Deshabilite la búsqueda DNS.
Configure una contraseña de modo EXEC: **class**.
Configure la contraseña **cisco** para las conexiones de consola.
Configure la contraseña **cisco** para las conexiones de vty.

Tabla de Direccionamiento

Nombre de Host	Dirección IP	Mascara de Subred	Gateway
A	172.17.10.1	255.255.255.0	----------
B	172.17.10.2	255.255.255.0	----------
C	172.17.10.3	255.255.255.0	----------
PC1	172.17.10.21	255.255.255.0	172.17.10.254
PC2	172.17.10.22	255.255.255.0	172.17.10.254
PC3	172.17.10.23	255.255.255.0	172.17.10.254
PC4	172.17.10.27	255.255.255.0	172.17.10.254

Tabla 5.5 Direccionamiento PC-STP

Preparar la red

Paso 20: *Deshabilitar todos los puertos con el comando shutdown*. Asegúrese de que los estados del puerto de switch estén inactivos con el comando **shutdown**. Simplifique esta tarea con el comando **interface range** .

A(config)#**interface range fa0/1 - 24**
Entramos a la configuración de los puertos del puesrto 1 hasta el puerto 24 del switch A.
A(config-if-range)#**shutdown**
Damos de baja los 24 puertos del switch A.
B(config)#**interface range fa0/1 - 24**
Hacemos lo mismo con el switch B.
B(config-if-range)#**shutdown**
C(config)#**interface range fa0/1 - 24**
C(config-if-range)#**shutdown**

Paso 21: *Volver a habilitar los puertos de usuario en A y B en modo de acceso*. Consulte el diagrama de topología para determinar qué puertos de switch en B están activados para acceso por el dispositivo de usuario final. Estos tres puertos se configurarán para modo de acceso y se habilitarán con el comando **no shutdown**.
A(config)#**interface fa0/3**
A(config-if)#**switchport mode access**
A(config-if)#**no shutdown**
B(config)#**interface range fa 0/3 , fa 0/4, fa 0/5**
B(config-if-range)#**switchport mode access**
B(config-if-range)#**no shutdown**

Paso 22: *Habilitar los puertos de enlace troncal en A, B y C* Usaremos solamente una VLAN en esta práctica de laboratorio; no obstante, se ha habilitado enlace troncal en todos los enlaces entre los switches para permitir que otras VLAN puedan agregarse en el futuro.

A(config-if-range)**#interface range fa0/1, fa0/2**
A(config-if-range)**#switchport mode trunk**
A(config-if-range)**#no shutdown**
B(config-if-range)**#interface range fa0/1, fa0/2**
B(config-if-range)**#switchport mode trunk**
B(config-if-range)**#no shutdown**
C(config-if-range)**#interface range fa0/1, fa0/2**
C(config-if-range)**#switchport mode trunk**
C(config-if-range)**#no shutdown**

Paso 23: *Configurar la dirección de la interfaz de administración en los tres switches*.

A(config)**#interface vlan1**
Accesa a la interface de la vlan 1
A(config-if)**#ip address 172.17.10.1 255.255.255.0**
Asigna la direction ip a la interface de la vlan 1.
A(config-if)**#no shutdown**
Levantamos la interfaz.
B(config)**#interface vlan1**
Hacemos lo mismo con el switch B.
B(config-if)**#ip address 172.17.10.2 255.255.255.0**
B(config-if)**#no shutdown**
B(config)**#interface vlan1**
B(config-if)**#ip address 172.17.10.3 255.255.255.0**
B(config-if)**#no shutdown**

Configurar las PC host
Configure las interfaces Ethernet de PC1, PC2 , PC3 y PC4 con la dirección IP, la máscara de subred y la gateway indicadas en la tabla de direccionamiento al comienzo de la práctica de laboratorio.

Configurar Spanning Tree

Paso 24: Poner *los switches en modo spanning tree debug* utilizando el comando spanning-tree events

A(config)# **spanning-tree vlan 10 20 30 40 50**
B(config)# **spanning-tree vlan 10 20 30 40 50**

C(config)# **spanning-tree vlan 10 20 30 40 50**

Poner el comando debug para ver anuncios de los cambios del STP

A#**debug spanning-tree events**
Spanning Tree event debugging is on
B#**debug spanning-tree events**
Spanning Tree event debugging is on
C#**debug spanning-tree events**
Spanning Tree event debugging is on

Cuestionario.

1. Mandar un ping del host pc2 al host pc4 ¿Que sucede?
2. Al caerse el enlace entre el switch A y el switch C ¿Que sucede con el switch B?
3. Con este enlace hacer un ping de cualquier host del switch B al host pc 4. ¿Qué sucede?
4. ¿Si hay comunicación? ¿Por qué?

5.3 PRACTICA ACL, NAT Y PAT

5.3.1 *Introducción*

En esta actividad, desarrollara su capacidad para configurar las ACL que cumplen con tres políticas de seguridad. Además, de cablear la topología adecuada y sus principales comandos, desde darle un nombre al equipo, su contraseña, así como el manejo de seguridad en el equipo a través de dos mecanismos tecnológicos característico de los equipos cisco como es el NAT y el PAT. Que con la ayuda de filtrado de direcciones a través de las ACL nos permite traducir las direcciones a las que mejor convengan para dicha seguridad.

5.3.2 *Objetivos*

Al completar esta práctica de laboratorio, el usuario podrá:

- Diseñar ACL nombradas estándar y extendidas
- Aplicar ACL nombradas estándar y extendidas
- Implementar y verificar diversas políticas de seguridad de ACL
- Configurar la traducción de direcciones NAT y PAT
- Aplicar NAT y PAT para seguridad de las redes

5.3.3 *Equipo a utilizar*

a. 3 Routers modelo 2800
b. 1 Switch modelo 2960
c. 1 Switch modelo 3550
d. 2 Switches modelo 500
e. 5 PC´S
f. 1 Servidor WEB
g. 1 Servidor de Archivos
h. Sus respectivos cables (seriales, de consola, etc.)

5.3.4 *Desarrollo*

5.3.4.1 Topología

Paso 1: *Armar la topología.* Armar una topología similar a la que se muestra en la figura.

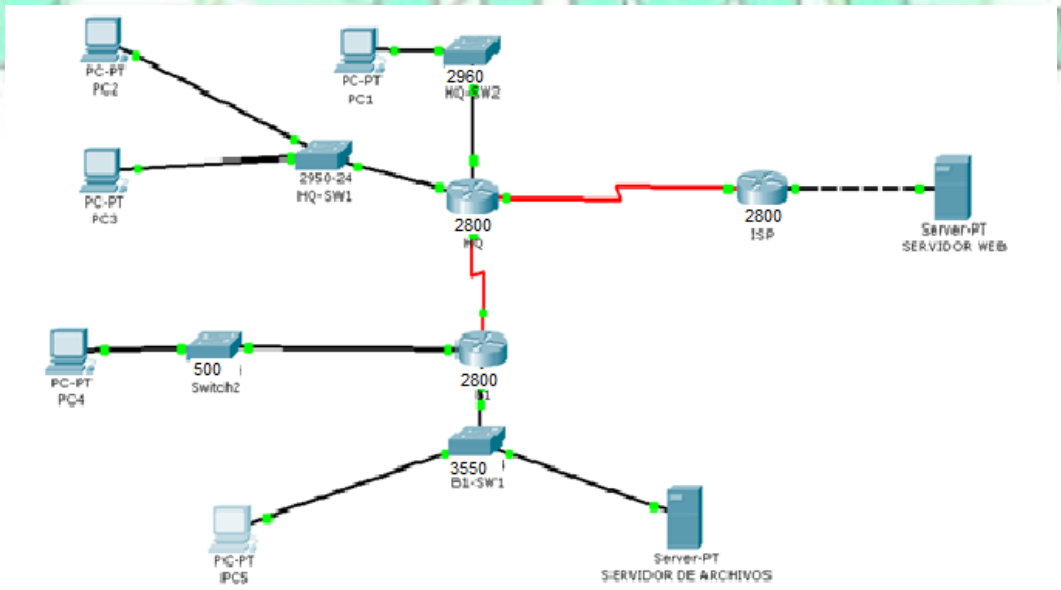

Imagen 5.9 Topología ACL

Para esta topología el cableado que debemos utilizar es el siguiente: utilizaremos cables de consola para la configuración de cada router y cada switch ya que para cisco podemos utilizar estos cables, utilizaremos cableado 1 a 1 para la conexión de cada pc a su respectivo switch y también ese tipo de cable lo conectaremos de cada switch a su router como se muestra en el diagrama, y para hacer la conexión entre routers tenemos que utilizar cables seriales conectados como su configuración nos diga ya sea como DTE o como DCE y también utilizaremos un cable cross – over que tenemos que conectar del servidor web a nuestro router ISP.

5.3.4.2 Direccionamiento

Paso 2: *Proporcionar direcciones ip a cada equipo e interfaces*. Otorgar las direcciones ip a los equipos utilizados en el diagrama de topología, según la tabla siguiente:

DISPOSITIVO	INTERFAZ	DIRECCION IP	MASCARA DE SUBRED
HQ	S0/0/0	10.1.1.1	255.255.255.252
HQ	S0/0/1	10.1.1.5	255.255.255.252
HQ	S0/1/0	209.165.201.2	255.255.255.252
HQ	FA0/0	10.1.50.1	255.255.255.0
HQ	FA0/1	10.1.40.1	255.255.255.0
B1	S0/0/0	10.1.1.2	255.255.255.252
B1	FA0/0	10.1.10.1	255.255.255.0
B1	FA0/1	10.1.20.1	255.255.255.0
ISP	S0/0/0	209.165.201.1	255.255.255.252
ISP	FA0/0	209.165.202.129	255.255.255.252
SERVIDOR WEB	NIC	209.165.202.130	255.255.255.252
SERVIDOR DE ARCHIVOS	NIC	10.1.10.2	255.255.255.0
PC1	NIC	10.1.40.89	255.255.255.0
PC2	NIC	10.1.50.75	255.255.255.0
PC3	NIC	10.1.50.7	255.255.255.0
PC4	NIC	10.1.20.163	255.255.255.0
PC5	NIC	10.1.10.5	255.255.255.0

Tabla 5.6 Direccionamiento PC-ACL

5.3.4.3 Configuraciones Básicas

router>**enable**
router# **config t**
router(config)**#int fa 0/0**
router(config-if)**#ip add 10.1.50.1 255.255.255.0**
Se le asigna una dirección ip y su máscara de red a la interface Ethernet que irá a un switch
router(config-if)**#no shut**
Se habilita la interface
router(config-if)#e**xit**

router(config)**#int ser 0/0/0**
router(config-if)**#ip add 10.1.1.1 255.255.255.252**
Se le asigna una dirección ip y su máscara de red a la interface serial que irá a otro router
router(config-if)**#clock rate 56000**
Se configure un reloj de sincronización y su velocidad porque es un equipo DCE
router(config-if)**#no shut**
Se habilita la interfaz
Realizar la misma operación para cada uno de los routers y cada interfaz tanto serial como ethernet.

Paso 3: *Darle nombres a cada equipo y una contraseña en modo exec*

router>**enable**
router# **config t**
router(config)**#hostname HQ**
Le asigna el nombre HQ al router
HQ(config)**#enable password LABORATORIO**
Le asigna una contraseña para poder ingresar a modo privilegiado

Hacer lo mismo con los otros dos routers (B1 e ISP), con los switches y las PC´S.

Paso 4: *Configurar el enrutamiento ospf en los tres routers.* Configurar en cada router el enrutamiento OSPF para poder comunicarse con todas las redes del diagrama de topología.

HQ
HQ**#config t**
HQ(config)**#router ospf 1**
Levanta el protocolo ospf para enrutar las redes conectadas a el router
El 1 significa el ID del proceso, en los tres routers se debe poner el mismo ID si se coloca otro ID diferente no habrá comunicación.

HQ(config-router)**#network 10.1.1.0 0.0.0.3 area 0**
10.1.1.0 Es la red en la que se encuentra el router
0.0.0.3 Es el wildcard de la red (la wildcard es lo contrario de la máscara de subred, por ejemplo en la máscara de subred 255.255.255.0 la wildcard sería 0.0.0.255).
Área 0 Es el tipo de área que se le coloca a este red, al igual que el ID el área debe ser la misma en los tres routers.

Hacer lo mismo con las otras redes de las interfaces de cada router (B1 e ISP) para poder tener comunicación entre todas las redes.
Paso 5: *Probar la conectividad en todas las redes***.** Probar que todas las redes se puedan comunicar entre sí, mandando ping de:

- PC1 AL SERVIDOR WEB.
- PC2 A PC5
- PC3 A PC4
- PC2 AL SERVIDOR DE ARCHIVOS

- PC5 AL SERVIDOR WEB

Todos los pings deben ser exitosos, si sucede lo contrario checar que la topología este bien conectada como el diagrama mostrando y que las ip estén correctas.

5.3.4.4 Configuración ACL y cuestionario

Paso 6: *Implementar políticas de seguridad con acl estándar.* Implementar una ACL estándar, para este caso bloquee la red 10.1.10.0 el acceso a la red 10.1.40.0. Se permite todo el acceso restante a 10.1.40.0.
Configure la ACL en el router HQ.

HQ# **config t**
HQ(config)#**access-list 10 deny 10.1.10.0 0.0.0.255**
Negara el acceso a la red 10.1.10.0 con mascara 255.255.255.0
HQ(config)#**access-list 10 permit any**
Y permitica el acceso a cualquier otra red que no sea la antes negada
HQ(config)#**int ser 0/0/0**
HQ(config-if)#**ip access-group 10 in**
Se le asignan los permisos y negaciones de acceso declarados en la lista 10 a la interfaz en la que se encuentra en este caso la serial 0/0/0

Paso 7: *Probar la conectividad de la acl***.** Realizar un ping de la PC1 a la PC5, este ping debe fallar.

Paso 8: *Implementar políticas de seguridad con acl extendidas.* Configurar una ACL extendida, para este caso el host 10.1.10.5 no tiene permitido el acceso al host 10.1.50.7. Todos los host restantes pueden acceder a 10.1.50.7
Configure la ACL en B1.

B1#**config t**
B1(config)#**access-list 115 deny tcp host 10.1.10.5 10.1.50.7 0.0.0.255**
Con la lista extendida se niega el acceso algunos host sin tener que abarcar toda la red
B1(config)#**access-list 115 permit tcp any any**
De la misma manera se permite el acceso de forma específica o general

Paso 9: *Verificar la implementación de las acl***.** Realizar un ping de la PC5 a la PC3, este ping debe fallar.

Paso 10: *Implementar una política de seguridad con acl***.** Configurar una ACL para el siguiente caso, el host 10.1.50.75 no tiene permitido el acceso al servidor WEB 209.165.202.130. Se permite el todo el acceso restante.
Configure la ACL .

router(config)#access-list 99 deny host 209.165.202.130
Niega el acceso a un host en especifico

router(config)#access-list 99 permit any
Permite cualquier otro host
router(config)#int ser 0/0/0
router(config)#ip access-group 99 in
Asigna el filtro de esta lista de acceso a una interface

Paso 11: *Verificar la implementación de las acl*. Realizar un ping de la PC2 al SERVIDOR WEB, este ping debe fallar.

CUESTIONARIO

¿En este caso que tipo de ACL usaría Estándar o Extendida?
Estándar
¿En que router configurara la ACL?
En el router ISP
¿En qué interfaz aplicara la ACL?
En la interfaz serial 0/0/0
¿Que configuración aplicaría si quisiera eliminar la ACL en el router HQ?
router(config)#no access-list 10
¿Las ACL standar de que entre que números pertenecen estas mismas?
De la 1 a la 99
¿Y las ACL extendidas de que numero a que numero están?
De la 100 a la 199

5.3.4.5 Configuración NAT y cuestionario

Paso 12: *Construcción de la topología*

Conecte dos routers y a uno de ellos un switch y al switch dos PC tal como se muestra:

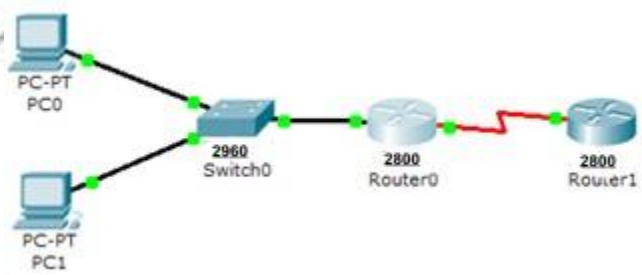

Imagen 5.10 Topología NAT-PAT

Para la conexión de esta red tenemos que conectar nuestro cable de consola para la configuración de cada router y el switch, también conectaremos con nuestros cables 1 a 1 nuestras PC´S a nuestro switch y del switch conectaremos del puerto 24 al router en el

puerto Ethernet 0/0 del mismo, y la conexión de router a router la tenemos que hacer con un cable serial de DCE a DTE.

Paso 13: *Configurar las interfaces*

Al router0 se le asigna el nombre de ESIME y al router1 en nombre de IPN, IPN será la red externa y ESIME la interna.

IPN (config)# **interface serial 0/0**
IPN (config-if)# **ip address 192.168.1.2 255.255.255.0**
Se le asiga una ip y mascara de red a la interface serial
IPN (config-if)# **no shutdown**
Habilita la interfaz
IPN (config-if)# **exit**

Se repite el proceso en el resto de las interfaces con la excepción de los seriales tipo DCE que llevan el reloj tal como se muestra continuación
ESIME# **configure terminal**
ESIME (config)# **interface fastethernet 0/0**
ESIME (config-if)# **ip address 10.10.1.1 255.255.255.0**
ESIME (config-if)# **no shutdown**
ESIME (config-if)# **exit**
Configuracion para un serial con DCE
ESIME (config)# **interface serial 0/0**
ESIME (config-if)# **ip address 192.168.1.1 255.255.255.0**
ESIME (Config-if)# **clock rate 56000**
ESIME (config-if)# **no shutdown**
ESIME (config-if)# **exit**

Configuración de las PC's

PC1
IP: 10.10.1.2
MASCARA: 255.255.255.0
GATEWAY: 10.10.1.1
PC2
IP: 10.10.1.3
MASCARA: 255.255.255.0
GATEWAY: 10.10.1.1

Paso 14: *Creación de una ACL*

ESIME(config)# **access-list 1 permit 10.10.1.0 0.0.0.255**

Creacion de la lista de acceso, en este caso debe contener el rango de direcciones internas

Donde:
List 1; es el nombre de la lista
Permit; es para dar acceso / Deny; es para negar acceso
10.10.1.0; es la red a la cual se le da el acceso
0.0.0.255; es la wildcard de la red.

Paso 15: *Implementación del NAT*

Se crea un pool de direcciones que será las direcciones dinámicas con las que saldrá a la red representada por el router IPN y después se define cual será la interfaz de entrada del NAT y la interfaz de salida del NAT

ESIME(config)# **ip ant pool P 199.99.9.40 199.99.9.62 netmask 255.255.255.0**
El pool es un conjunto de direcciones en este caso las que se utilizaran para hacer la traduccion de direcciones externas
ESIME(config)# **ip nat inside source list 1 pool P**
Active el NAT indicando primero las direcciones a traducir y des pues las direcciones en las que serán traducidas en este caso primero list 1 que son las direcciones internas de nuestra rede y después el pool P que serán las direcciones para mostrar en el exterior
ESIME(config)# **interface fastethernet 0/0**
ESIME(config-if)# **ip nat inside**
Declara que esta será la interfaz de entrada para el NAT donde se utilizara la lista 1 para direccionar
ESIME(config-if)# **exit**
ESIME(config)# **interface serial 0/0**
ESIME(config-if)# **ip nat outside**
Declara que esta será la interfaz de salida para el NAT donde se utilizara el pool P para direccionar
ESIME(config-if)# **exit**

Paso 16: *Se declara la interfaz loopback que es el enlace externo.*

IPN(config)# **interface loopback 0**
Se ingresa a una interfaz loopback que es lógica en este caso la 0
IPN(config-if)# **ip address 172.16.1.1 255.255.255.255**
Y esta tendra un direccion ip y mascara de red y solo servira como enlace para el exterior de nuestra red
IPN(config-if)# **no shutdown**
IPN(config-if)# **end**

Paso 17: *Se establecen las rutas en cada uno de los routers*

ESIME(config)# **ip route 0.0.0.0 0.0.0.0 serial 0/0**
Se establecen las rutas de default ya que como la implementacion de NAT es por seguridad no conviene establecer las rutas con la ip de nuestra red
IPN(config)# **ip route 0.0.0.0 0.0.0.0 serial 0/0**

Se declara como ruta y mascara 0.0.0.0 porque esta va a ser dinámica así que no podemos definir una estática más que esta de default.

Cuestionario

¿Cuando es necesario implementar una NAT?
Cuando son insuficientes las direcciones IP y cuando se desea mantener oculto el direccionamiento interno de nuestra red
¿Cómo se determina la interfaz NAT de entrada y de salida?
La de salida debe ser el puerto serial que nos conecta con el exterior y la interna puede ser una Ethernet o serial que conecta a toda la red interna.
¿Para qué sirve la interfaz loopback?
Es la que nos sirve de enlace externo y esa la configura la red externa
¿Porque la lista de acceso y el pool son de diferentes dominios de red?
Porque la lista contiene el direccionamiento interno de la red y el pool el direccionamiento al que será traducido para el exterior y es de esta manera como proporciona la seguridad

5.3.4.6 Configuración PAT y cuestionario

Paso 18: *Creación de PAT*

ESIME(config)#**ip nat inside source list 1 interface serial 0/0 overload**
Es muy similar ya que el PAT es un tipo de NAT, la diferencia es que asigna varias IP internas a una externa.
Y al igual que NAT se debe declarar cual será la interfaz de salida y cual la interfaz de entrada.

ESIME(config)# **interface fastethernet 0/0**
ESIME(config-if)# **ip nat inside**
Declara que esta será la interfaz de entrada para el NAT donde se utilizara la lista 1 para direccionar
ESIME(config-if)# **exit**
ESIME(config)# **interface serial 0/0**

ESIME(config-if)# **ip nat outside**
Declara que esta será la interfaz de salida para el NAT donde se utilizara el pool P para direccionar
ESIME(config-if)# **exit**

Paso 19: *Comprobar los parámetros del NAT*

ESIME# **show ip nat translation**
Muestra las transmisiones de direcciones IP

```
ESIME#show ip nat translation
Pro  Inside global     Inside local       Outside local      Outside global
---  199.99.9.41       10.10.1.2          ---                ---
---  199.99.9.40       10.10.1.3          ---                ---
```

5.11 Show IP NAT translation

ESIME# **show ip nat statistics**
Muestra las estadisticadas NAT

```
ESIME#show ip nat statistics
Total translations: 2 (0 static, 2 dynamic, 0 extended)
Outside Interfaces: Serial0/0
Inside Interfaces: FastEthernet0/0
Hits: 12  Misses: 6
Expired translations: 0
Dynamic mappings:
-- Inside Source
access-list 1 pool P refCount 2
 pool P: netmask 255.255.255.0
       start 199.99.9.40 end 199.99.9.62
       type generic, total addresses 23 , allocated 2 (8%), misses 0
```

Imagen 5.12 Show IP NAT statistics

Cuestionario

¿Cuál es la diferencia entre NAT y PAT?
PAT es un subtipo de NAT dinámica que asigna varias direcciones IP internas a una sola externa
Por que utiliza números de puerto de origen únicos?
Para distinguir entre las diferentes direcciones
Como le llama cisco al PAT?
NAT overload

Anexos

Esquema de laboratorio

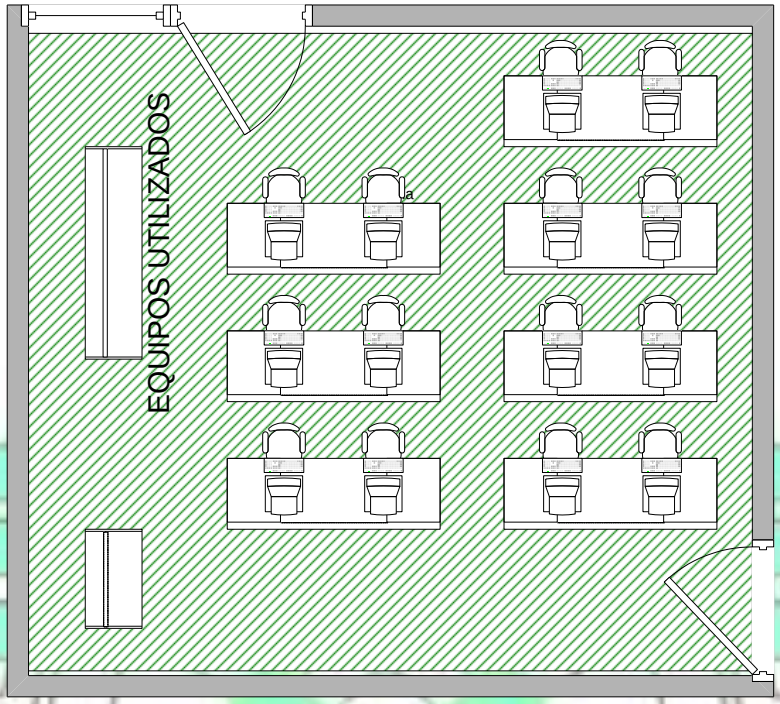

Figura 6.1 Laboratorio

Esquema de equipos utilizados.

Todos los equipos utilizados son Cisco

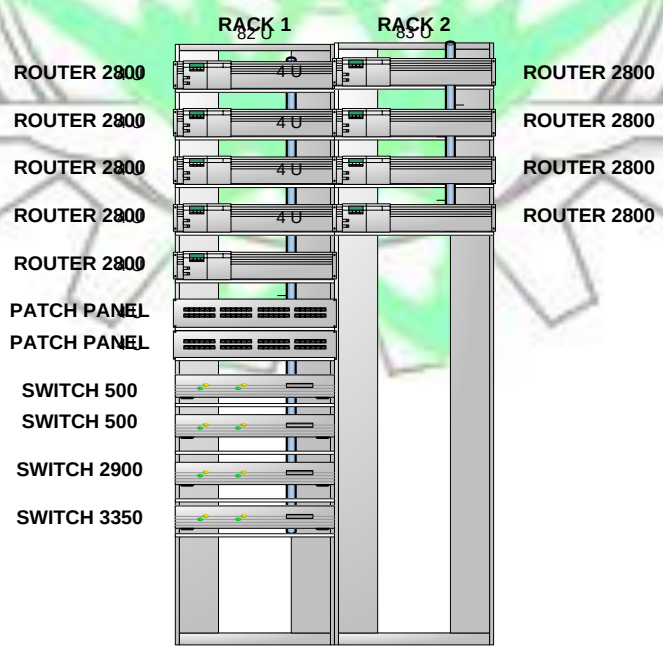

Imagen 6.2 Equipos

Router's 2800

Imagen 6.3 Router 2800

Switch 2960

Imagen 6.4 Switch 2900

Switch 3550

Imagen 6.5 Switch 3550

Switch 500

Imagen 6.6 Switch 500

- **SWITCH CISCO CATALYST EXPRESS 500:**

Configuración inicial:

- Se enchufa el switch, los LEDS del puerto y SYSTEM destellan, luego se vuelve completamente verde.
- Se pulsa el botón SETUP, el LED del puerto del switch parpadear de color verde.
- En ese momento se conecta la PC al puerto, los LEDs del Puerto en la PC y en el switch, estos parpadean de color verde.
- Cuando el LED de SETUP se vuelva verde, se puede iniciar una sesión en el navegador en la PC y aparece automáticamente la ventana de configuración
- En esta se introducen los siguientes parámetros:

Interfaz de administración vlan: 1
Modo de asignación IP: Estatico
Dirección IP: 172.17.1.1
Mascara de subred: 255.255.0.0
Puerta de enlace: 172.17.1.254
Nombre de usuario: ESIME
Contraseña: cisco
Nombre del host: switch1

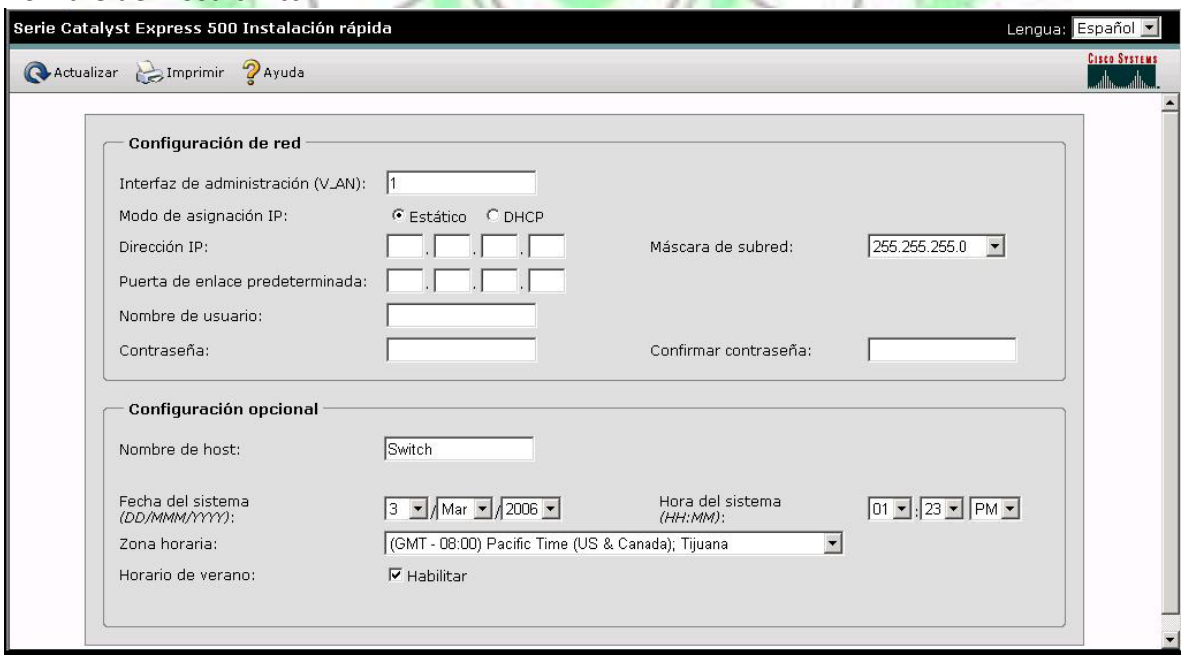

Imagen 6.7 500-1

Se le da un click en enviar y se procede a realizar el resto de la configuración indicada en las prácticas.

En caso de que el switch ya cuente con un usuario y contraseña que desconozcamos es necesario eliminar estos y el switch mantendrá su configuración.

Para restaurar contraseña:

1. Ver que no se encuentre conectado ningún dispositivo al switch y esté conectado a la toma de corriente de modo que el LED de system se encuentre encendido de manera solida de color verde.
2. Oprimir el botón de setup este empezara a destellar en color verde junto con uno de los puertos del switch. Debera conectar el cable de la PC (cable straigth Trough, "cable recto") al puerto que esta destellando y mantener oprimido el botón de setup por lo menos otros 5 segundos.
3. Después el puerto al que se conecto tornara color ámbar y nuevamente verde solido y con la ip del switch podrá iniciar sesión en el navegador y reconfigurar el usuario y la contraseña.
4. En la siguiente pantalla en el menú de la izquierda seleccionar configurar, después usuarios y contraseñas, dentro de la ventana deberá dar click en la opción crear:

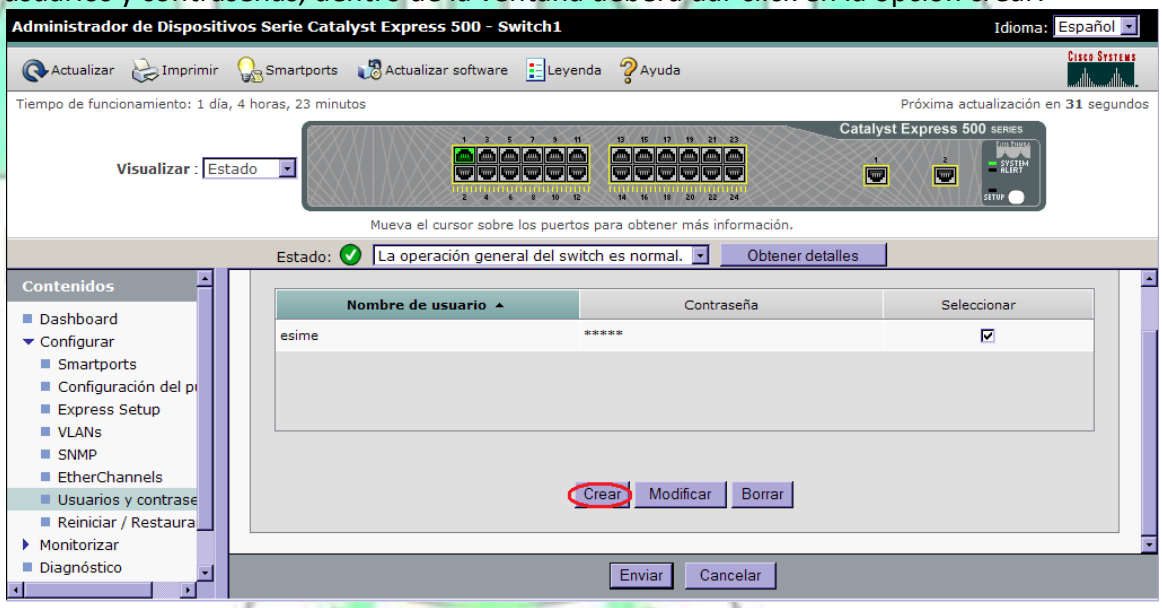

Imagen 6.8 500-2

Y aparecerá la siguiente pantalla:

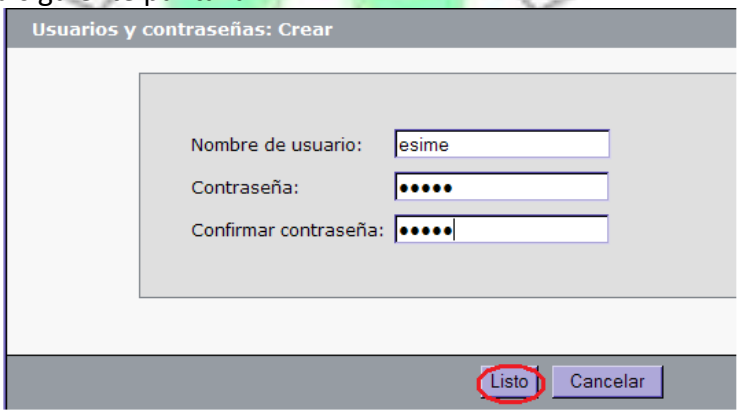

Imagen 6.9 500-3

En la cual se introduce el usuario: esime, y la contraseña: cisco y damos click en listo. Esto nos llevará a la pantalla anterior donde daremos click en enviar.

Configuración de VLAN's:

1. Primero debemos configurar los puertos dentro del switch, para esto en el menú de lado izquierdo debemos seleccionar la opción de configurar y luego smartports, dentro de este deberemos seleccionar un puerto o un grupo de ellos y seleccionar un perfil de puerto para asignarles.

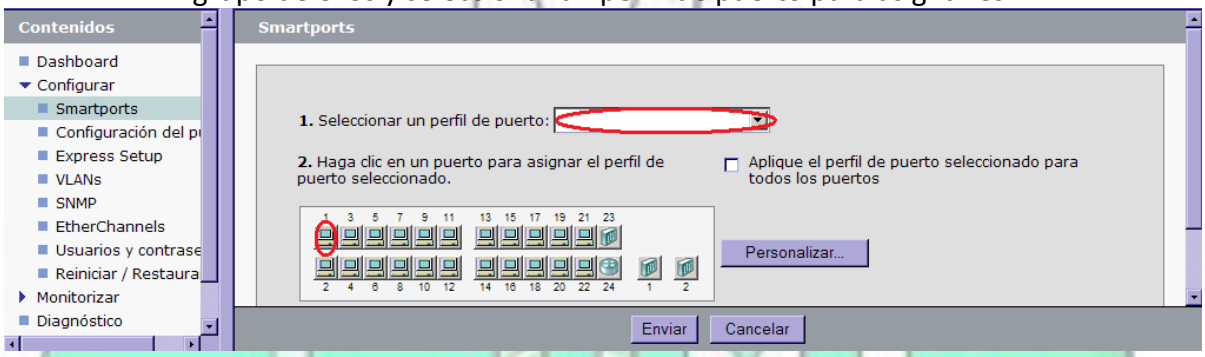

Imagen 6.10 500-4

Los perfiles de puerto son los siguientes:

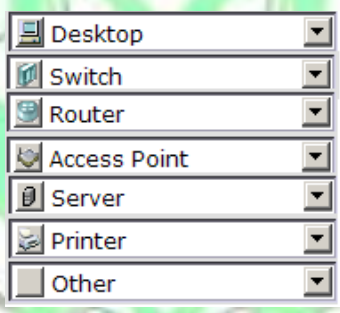

Imagen 6.11 500-5

Y este se selecciona en base a lo que se desea conectar a dicho puerto, para la práctica de VLAN's se seleccionan todos para conectar PC's a excepción del puerto 23 y 24 ya que el 23 ira conectado al otro switch y el 24 ira conectado al router.

Configuración de VTP:

Una vez que se selecciona en el perfil del puerto un switch o un router este se configura automáticamente como un "port trunk", es decir levanta el VTP y no hay que realizar ninguna configuración extra, más que conectar dicho dispositivo.

Cada vez que se oprime el botón enviar los cambios realizados son guardados en el equipo y es recomendable hacerlo cada vez que se cambia de pantalla o se realiza algún cambio.

Una vez realizado esto podemos personalizar los puertos esto nos sirve para modificar, la velocidad, la descripción, habilitarlo, etc. Tal y como se muestra en la siguiente pantalla, este es un paso opcional ya que no es necesario por default nos da en auto todos los puertos y habilitados.

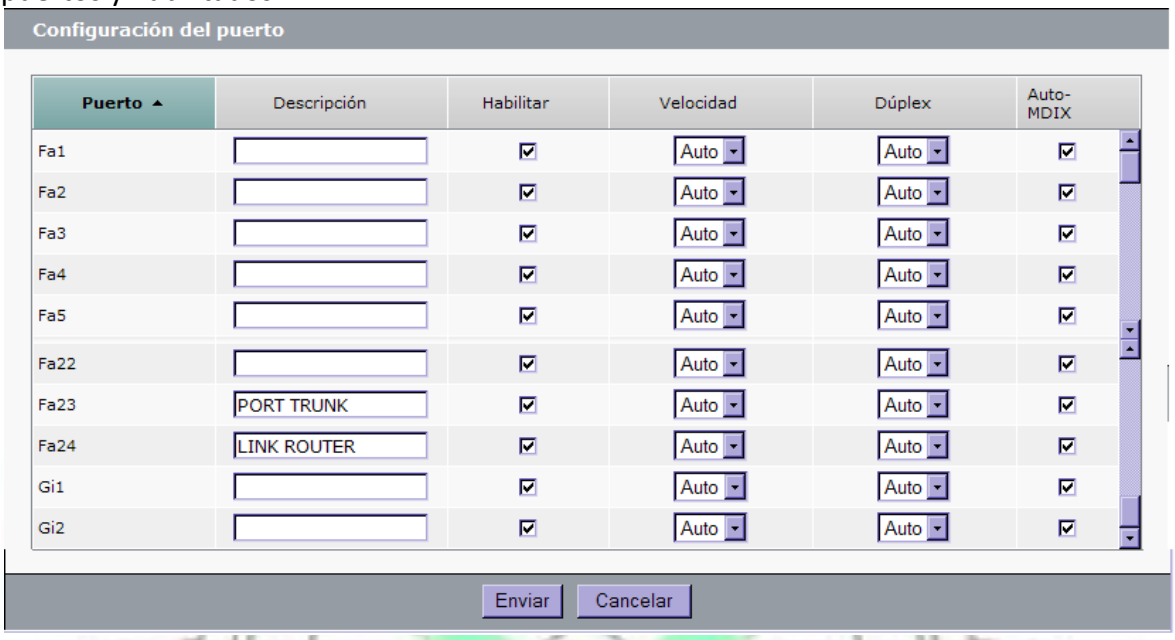

Imagen 6.12 500-6

Una vez configurados los puertos, se crean las VLAN's por lo que en el menú izquierdo seleccionamos la opción configurar y luego VLANs. Donde nos aparecerá la siguiente pantalla (inicialmente sin ninguna VLAN mas que la nativa) y hay oprimiremos el botón crear.

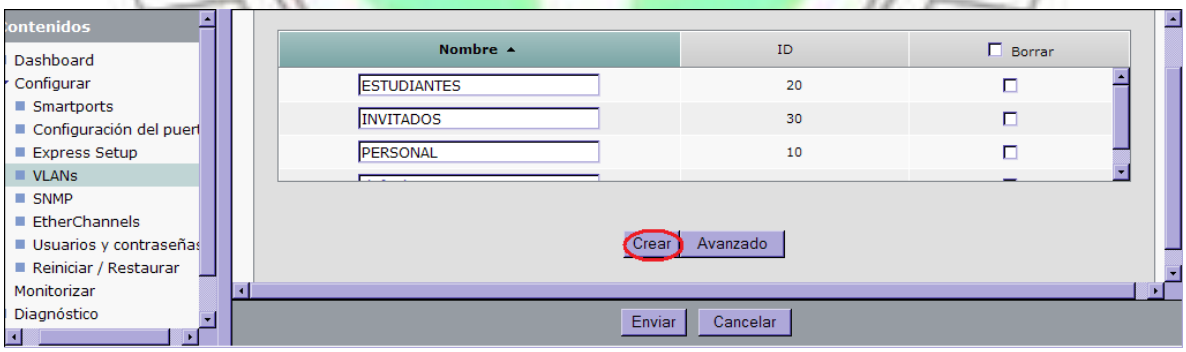

Imagen 6.13 500-7

Lo cual nos enviara a la siguiente pantalla en la cual deberemos ingresar un nombre para la VLAN y un ID o identificador y se oprime el botón listo:

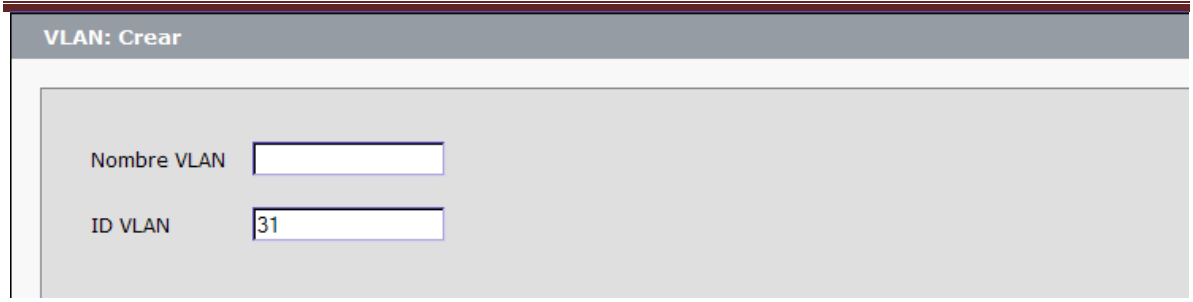

Imagen 6.14 500-8

Se repite el proceso de la ventana anterior según el numero de VLAN's a crear en nuestro caso según las mostradas en la tabla de direccionamiento en la práctica (2) de VLAN's.

Configuración de STP:

Si oprimimos el botón avanzado dentro de la pantalla descrita en el menú configurar, VLAN's nos mostrara la siguiente pantalla:

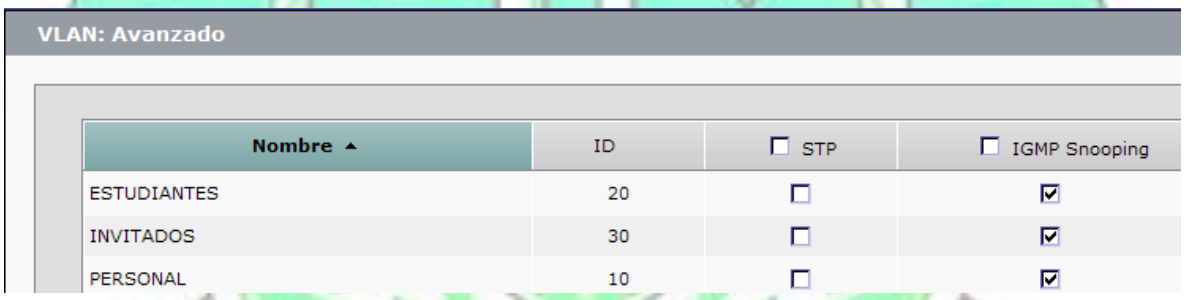

Imagen 6.15 500-9

En la cual solo debemos marcar la casilla STP y esto nos levantara el protocolo spanning tree en la VLAN o VLAN's seleccionadas. Al igul que en las pantallan anteriores se debe dar click en listo y enviar para guardar las configuraciones.

Una vez hecho esto regresamos en el menú izquierdo a configurar, smartports y dentro de la pantalla damos click en personalizar, esta vez sin seleccionan ningún puerto en especial. Para asignar cada uno de los puertos a la VLAN correspondiente (ver tabla de direccionamiento en práctica (2), VLAN) y nos mostrara la siguiente pantalla:

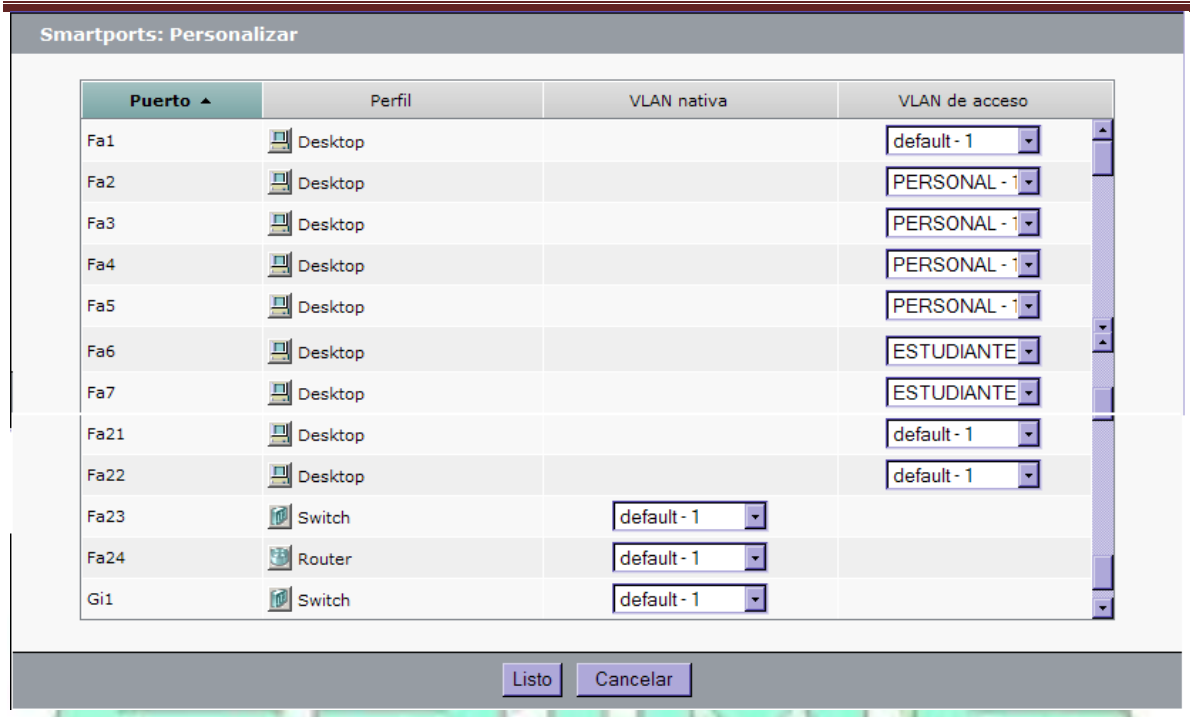

Imagen 6.16 500-10

Para verificar que se tenga la configuración deseada en el menú izquierdo seleccionamos monitorizar y después estado del puerto y nos mostrara una pantalla similar a la siguiente:

Imagen 6.17 500-11

Y para verificar la conectividad, se realiza ping entre los equipos de la misma VLAN y estos deben responder. Si no responden el ping entre diferentes VLAN' el problema de configuración debe revisarse en el router.

Por el protocolo VTP, ya no es necesario repetir el procedimiento solo realizar la asignación de puertos a cada una de las VLAN's ya existentes.

Para resolución de dudas se puede consultar en el menú izquierdo el Networs Assisment, el cual nos proporciona una guía detallada de cisco.

Conclusiones

Podemos concluir que todas las practicas aquí expuestas fueron realizadas exitosamente comprobando que el laboratorio de la ESIME “Culhuacan” cumple con los requerimientos necesarios para el desarrollo integran de los conocimientos adquiridos.

Así como también se logro observar la influencia destacada de la tecnología sobre las nuevas generaciones de dispositivos ya que aun cuando cuentan con una interfaz más amigable, son aun poco comunes en el ámbito estudiantil. Por lo que dificulta en una ligera proporción la adquisición de los nuevos esquemas a utilizar.

Por otro lado también se logro comprobar que la metodología descrita aplica para equipos cisco de diferentes modelos.

Y por último que la práctica es una parte fundamental en el estudio ya que aporta conocimientos más significativos para el estudiante logrando que estos tengan una permanencia más prolongada es su memoria y sobre todo enfrentándonos a problemáticas reales que tiene una solución bajo la misma metodología vista pero no antes considerada, sino hasta el momento de llevarlo a la práctica.

Índice de tablas

Índice de figuras

Bibliografía

"Redes de comunicación", Enciclopedia Microsoft(R) Encarta(R) 98. (c) 1993-1997 Microsoft Corporation. Reservados todos los derechos.
http://www.ts.es/doc/area/produccion/ral/BANDA.HTM
http://ccdis.dis.ulpgc.es/ccdis/laboratorios/redes.html
http://www.ts.es/doc/area/produccion/ral/CABLE.HTM
http://usuarios.lycos.es/aledomiisa/historia.php
http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/REDES02.htm
http://www.monografias.com/trabajos29/modelo-osi/modelo-osi.shtml
http://www.monografias.com/trabajos/protocolotcpip/protocolotcpip.shtml
http://www.tech-faq.com/lang/es/ethernet-switch.shtml&usg=ALkJrhg52W9zaQq0FlnU9Y8QSBX6wsFhvg
http://es.wikipedia.org/wiki/Conmutaci%C3%B3n_de_paquetes
http://eveliux.com/mx/index.php?option=content&task=view&id=173
http://es.wikipedia.org/wiki/NAT
http://www.adslfaqs.com.ar/que-es-pat-port-address-translation/
http://www.geocities.com/hilmarz/cisco/acl.htm
http://es.wikipedia.org/wiki/VLAN
http://es.kioskea.net/contents/internet/vlan.php3
http://www.textoscientificos.com/redes/redes-virtuales
http://networking.ringofsaturn.com/Cisco/vtp.php
http://es.wikipedia.org/wiki/VTP
http://es.wikipedia.org/wiki/Spanning_tree
http://es.wikipedia.org/wiki/Rapid_Spanning_Tree_Protocol
http://es.wikipedia.org/wiki/OSPF
http://es.wikipedia.org/wiki/RIP_(protocolo)
http://www.gratisweb.com/gulle79/network/rip/intro_rip.htm
http://www.monografias.com/trabajos16/seguridad-informatica/seguridad-informatica.shtml#redes
http://www.cisco.com/en/US/docs/switches/lan/catalystexpress500/release_12.2_25_fy/user/guide/trouble.html#wp78788