ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"*Diseño de Practicas de Configuración de Routers HUAWEI para Redes de Datos*."

INFORME DE PROYECTO DE GRADUACIÓN

Previo la obtención del título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentado por:

Elías Alberto Suárez Pincay

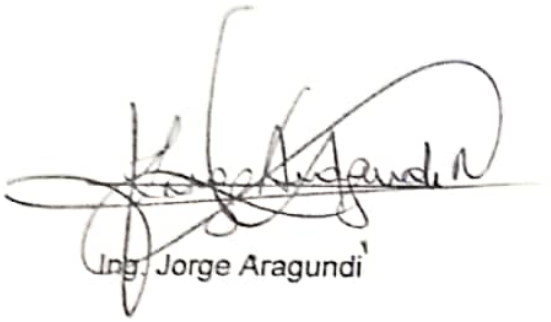
GUAYAQUIL – ECUADOR

2010

AGRADECIMIENTO

Agradezco primeramente a Dios por permitirme llegar a este punto en mi vida y lograr conseguir esta meta propuesta, a mis padres por estar siempre conmigo dándome apoyo para que esto fuese posible, a mis hermanos por su ayuda brindada, a mis amigos por ser quienes son, dándome su sincera amistad y apoyo cuando lo he necesitado, a mi directora Ing. María Antonieta Álvarez y a la Ing. Rebeca Estrada Pico por su respaldo incondicional en este proyecto de grado para la culminación del mismo.

TRIBUNAL DE SUSTENTACIÓN



Ing. Jorge Aragundi

SUB-DECANO DE LA FIEC

PRESIDENTE

Ing. María Antonieta Álvarez

DIRECTORA DE TESIS

Ing. Albert Espinal S.

VOCAL PRINCIPAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Trabajo de Grado, me corresponden exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de Graduación de la ESPOL)

Elías Alberto Suárez Pincay.

RESUMEN

El presente trabajo consiste en la creación de prácticas para routers HUAWEI Quidway AR 28-30, con una descripción clara del manejo y las características de cada uno de los equipos e instrumentos a utilizarse, el cual nos permite complementar de manera práctica los conocimientos adquiridos, colaborando a la parte didáctica en el estudio de los equipos existentes en el Laboratorio de Telecomunicaciones de la facultad, enfocado principalmente al desarrollo de redes de datos.

Además, las prácticas elaboradas serán la principal herramienta de estudio para los futuros estudiantes que cursarán por este laboratorio.

En la práctica, los estudiantes analizarán, configurarán, verificarán los protocolos de enrutamiento principales: RIPv1, RIPv2, y OSPF. Además podrán reconocer y corregir fallas y problemas de enrutamiento comunes.

INDICE GENERAL

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

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. 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.

Las redes en general, consisten en "compartir recursos", y uno de sus objetivos es hacer que todos los programas, datos y equipo estén disponibles para cualquiera de la red que así lo solicite, sin importar la localización física del recurso y del usuario. En otras palabras, el hecho de que el usuario se encuentre a 1000 km de distancia de los datos, no debe evitar que este los pueda utilizar como si fueran originados localmente.

Un enrutador o encaminador (en inglés: router) es un dispositivo hardware o software de interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red.

El enrutador toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirige los paquetes hacia el segmento y el puerto de salida adecuados. Sus decisiones se basan en diversos parámetros. Una de las más importantes es decidir la dirección de la red hacia la que va destinado el paquete. Otras decisiones son la carga de tráfico de red en las distintas interfaces de red del enrutador y establecer la velocidad de cada uno de ellos, dependiendo del protocolo que se utilice.

El diseño propuesto se desarrolla en base a los equipos obtenidos por la universidad mediante el acuerdo ESPOL- HUAWEI entre los cuales tenemos los routers antes mencionados los Quidway AR 28-30. Se ha definido un esquema de direccionamiento según lo indicado. Para ello, se entregará una

ilustración en cada unas de las prácticas propuestas, donde aparecen claramente indicadas tanto las subredes definidas como las direcciones IP asignadas a cada interfaz. Se muestra de forma detallada, los pasos que se deben seguir para la realización de la práctica.

En un principio, se debe configurar el router a través del puerto serial. Se debe asignar la dirección IP y máscara al interfaz Ethernet del mismo. Por otro lado, debe modificar adecuadamente la configuración IP de su equipo (dirección, máscara y router por defecto).

Las redes que son configuradas son redes claras y sencillas, ya que la principal idea es de establecer prácticas que muestre al estudiante el funcionamiento de los equipos así como también las principales funciones de un router y todos sus principales beneficios de manera clara y objetiva.

Se describe la arquitectura, los componentes y el funcionamiento de los routers y se explica los principios de enrutamiento y de los protocolos de enrutamiento.

CAPITULO 1

1. Fundamentos teóricos de Enrutamiento

En este capítulo denominado Fundamentos teóricos de Enrutamiento, se desarrolla primeramente los conceptos básicos de internetworking, explicando de manera general sus aspectos principales.

Luego se expone dos tipos de conexiones que un ruteador utiliza para la implementación de una red, sean estas; conexión LAN y conexión WAN, así como también los dispositivos que se utilizan en cada una de ellas.

Además se explica una descripción del enrutamiento, así como también los dispositivos de ruteo, exponiendo sus principales características.

Finalmente se plantea los tipos de topología que se utilizan en la implementación o diseño de una estructura de red.

1.1 CONCEPTOS BÁSICOS DE INTERNETWORKING

Internetworking comprende la conexión de dos o más redes de computadores diferentes o redes que se dividen en forma conjunta para formar un internetwork (con frecuencia acortado Internet), usando dispositivos los cuales operan en la capa tres del modelo básico de referencia OSI (como enrutadores o switches de la capa tres) para conectarlos juntos y permitir tráfico de ida y vuelta por ellos. Los dispositivos de ruteo de la capa tres guían el tráfico a un camino correcto a través de la Internet completa para completar su destino. [1]

Es interesante notar que muchas veces se refiere a la conexión de redes con puentes como internetworking, sin embargo el resultado es un sistema que imita una subred, y no se requiere un protocolo de internetworking (tal como IP) para recorrerlas.

Internet es una red de redes corriendo diferentes protocolos de bajo nivel, unificada por un protocolo de internetworking, el Protocolo de Internet (IP). En la figura 1.1 podemos observar una representación de Internetwork.

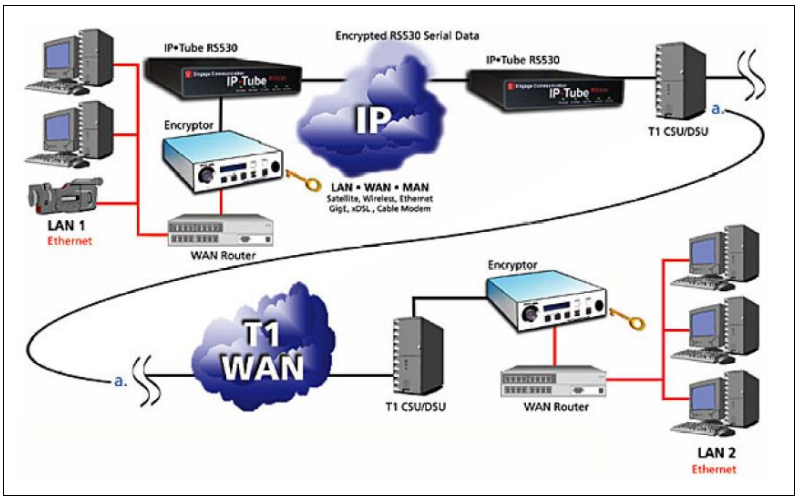


Figura 1.1.- Internetwork. [2]

Internetwork empezó como una forma para conectar tipos de tecnologías de redes distintas, pero este se convirtió en una necesidad de desarrollo de medios de alta difusión para conectar dos o más LANs vía algún tipo de WAN. Hoy en día incluye la conexión de otros tipos de redes de computadora tales como redes de área personal.

Las primeras redes eran redes de tiempo compartido que usaban mainframes y terminales cercanos. Dichos ambientes fueron implementados por IBM's Systems Network Architecture (SNA) y Digital's network architecture.

Internetworking evolucionó como una solución a tres grandes problemas:

- LANs aisladas. Hacen las comunicaciones electrónicas entre diferentes oficinas o departamentos imposibles.

- Duplicación de recursos. Significa que el mismo hardware y software tenga que ser proporcionado a cada oficina o departamento.
- Falta de administración de red. Significa que no existe un método centralizado de administración y soluciones de problemas de redes.[1]

Por más de dos décadas una nueva tecnología ha evolucionado para ser posible interconectar muchas redes físicas heterogéneas y hacerlas funcionar como una unidad funcional. La tecnología, llamada Internetworking acomoda múltiples y diversas tecnologías de hardware fundamental proveyendo una forma de interconectar redes heterogéneas y configurar convenciones de comunicación que las hace interoperar. La tecnología de Internet esconde los detalles del hardware de red y permite a las computadoras comunicarse independientemente de sus conexiones físicas de red.

1.2 CONEXIONES LAN/WAN Y DISPOSITIVOS

Las Redes de Área Local (LANs) evolucionaron alrededor de la revolución de la PC.Habilitaban a múltiples usuarios en un área geográfica relativamente pequeña para intercambiar archivos y mensajes, así como también acceder a recursos compartidos tales como servidores de archivos e impresoras.

Las LAN constan de los siguientes componentes:

- Computadores
- Tarjetas de interfaz de red

- Dispositivos periféricos
- Medios de networking
- Dispositivos de networking [3]

Las LAN permiten a las empresas aplicar tecnología informática para compartir localmente archivos e impresoras de manera eficiente, y posibilitar las comunicaciones internas. Un buen ejemplo de esta tecnología es el correo electrónico. Los que hacen es conectar los datos, las comunicaciones locales y los equipos informáticos.

Algunas de las tecnologías comunes de LAN son:

- *Ethernet*: Ethernet es un estándar de redes de computadoras de área local. Ethernet se tomó como base para la redacción del estándar internacional IEEE 802.3. En el caso del protocolo Ethernet/IEEE 802.3, el acceso al medio se controla con un sistema conocido como CSMA/CD (Carrier Sense Multiple Access with Collision Detection, Detección de Portadora con Acceso Múltiple y Detección de Colisiones), cuyo principio de funcionamiento consiste en que una estación, para transmitir, debe detectar la presencia de una señal portadora y, si existe, comienza a transmitir. Si dos estaciones empiezan a transmitir al mismo tiempo, se produce una colisión y ambas deben repetir la transmisión, para lo cual esperan un tiempo aleatorio antes de repetir, evitando de este modo una nueva colisión, ya que ambas no escogerán el mismo tiempo de espera.

- *Token Ring*: Las redes basadas en protocolos de paso de testigo (token passing) basan el control de acceso al medio en la posesión de un testigo. Éste es un paquete con un contenido especial que permite transmitir a la estación que lo tiene. Cuando ninguna estación necesita transmitir, el testigo va circulando por la red de una a otra estación. Cuando una estación transmite una determinada cantidad de información debe pasar el testigo a la siguiente. Las redes de tipo token ring tienen una topología en anillo y están definidas en la especificación IEEE 802.5 para la velocidad de transmisión de 4 Mbits/s. Existen redes token ring de 16 Mbits/s, pero no están definidas en ninguna especificación de IEEE.

- *FDDI*: (Fiber Distributed Data Interface; Interfaz de datos distribuidos por fibra) es un estándar para transmisión de datos en LAN que opera sobre fibra óptica a 100 Mbps. Fue definido en los años 80 por la ANSI (America National Standards Institute; Instituto de Estándares Nacionales de América) ante la necesidad de contar con una tecnología para LAN de gran ancho de banda. Para alcanzar este objetivo fue necesaria la adopción de la fibra óptica como medio físico, a pesar de que se elevaran demasiado los costos de instalación. La topología de la red es de anillo similar al Token Ring. El cableado de la FDDI está constituido por dos anillos de fibras, uno transmitiendo en el sentido de las agujas del reloj y el otro en dirección contraria. El primero funciona como anillo principal y el segundo como respaldo o back up. El hecho de poseer dos anillos hace que la red FDDI sea altamente tolerante a

fallas. El control de la red es distribuido, razón por la cual si falla un nodo real, el resto recompone la red automáticamente.

Las LANs se encuentran diseñadas para:

- Operar dentro de un área geográfica limitada.
- Permitir el acceso múltiple con gran ancho de banda..
- Controlar la red con administración local.
- Proporcionar conectividad a los servidores locales.
- Conectar dispositivos físicamente adyacentes.

Entre los dispositivos que se usan en una LANs tenemos:

- *Routers*: Los routers son los responsables de enrutar paquetes de datos desde su origen hasta su destino en la LAN, y de proveer conectividad a la WAN. En la figura 1.2 se observa un router HUAWEI Quidway AR 28-30.

Figura 1.2.- Router Huawei.

- *Switch*: Los switches aprenden determinada información sobre los paquetes de datos que se reciben de los distintos computadores de la red. Los switches utilizan esa información para crear tablas de envío para determinar el destino de los datos que se están mandando de un

computador a otro de la red. En la figura 1.3 se observa un switch HUAWEI.

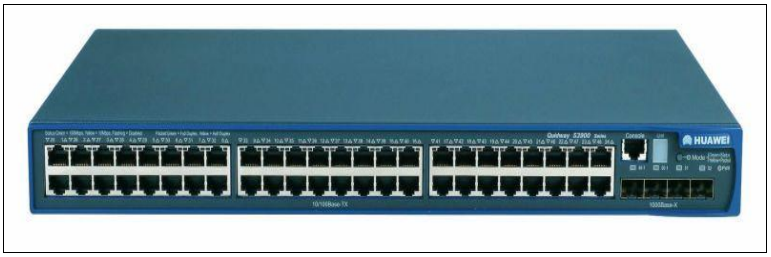


Figura 1.3.- Switch Huawei 48 puertos.

- *Hub*: En un hub, los datos que llegan a un puerto del hub se transmiten de forma eléctrica a todos los otros puertos conectados al mismo segmento de red, salvo a aquel puerto desde donde enviaron los datos.

- *Repetidoras*: El propósito de un repetidor es regenerar y retemporizar las señales de red a nivel de los bits para permitir que los bits viajen a mayor distancia a través de los medios.

- *Puentes*: La función del puente es tomar decisiones inteligentes con respecto a pasar señales o no al segmento siguiente de la red.

Los dispositivos de conectividad que permiten enlazar sistemas de cómputo separados por grandes distancias con medios de transmisión públicos o privados para formar una WAN se conocen como dispositivos de conectividad WAN. Las redes WAN permiten que las empresas se comuniquen entre sí a través de grandes distancias. Las redes WAN permiten que los computadores, impresoras y otros dispositivos de una

LAN compartan y sean compartidas por redes en sitios distantes. Las redes WAN proporcionan comunicaciones instantáneas a través de zonas geográficas extensas. [4]

Networking de área amplia también dio lugar a una nueva clase de trabajadores, los empleados a distancia, que no tienen que salir de sus hogares para ir a trabajar.

Las WAN están diseñadas para realizar lo siguiente:

- Operar entre áreas geográficas extensas y distantes.
- Posibilitar capacidades de comunicación en tiempo real entre usuarios.
- Brindar recursos remotos de tiempo completo, conectados a los servicios locales.
- Brindar servicios de correo electrónico, World Wide Web, transferencia de archivos y comercio electrónico.

Las Redes de Área Amplia (WANs) interconectan LANs con usuarios geográficamente dispersos para crear conectividad. Algunas de las tecnologías usadas para conectar LANs incluyen T1, T3, ATM, ISDN, Frame Relay, enlaces de radio y otros. Nuevos métodos de conexión de LANs dispersas están apareciendo todos los días.

Entre los dispositivos que se usan en una WAN tenemos:

- *Routers*

- *Servidores de comunicación*: El servidor responde a las peticiones de los clientes. El servidor es un computador central que se encuentra disponible de forma continua para responder a las peticiones de los clientes, ya sea de un archivo, impresión, aplicación u otros servicios. La mayoría de los sistemas operativos adoptan la forma de relación cliente/servidor. En general, los computadores de escritorio funcionan como clientes y uno o más computadores con potencia de procesamiento adicional, memoria y software especializado funcionan como servidores. En la figura 1.4 se observa la conexión de un servidor dentro de una red.

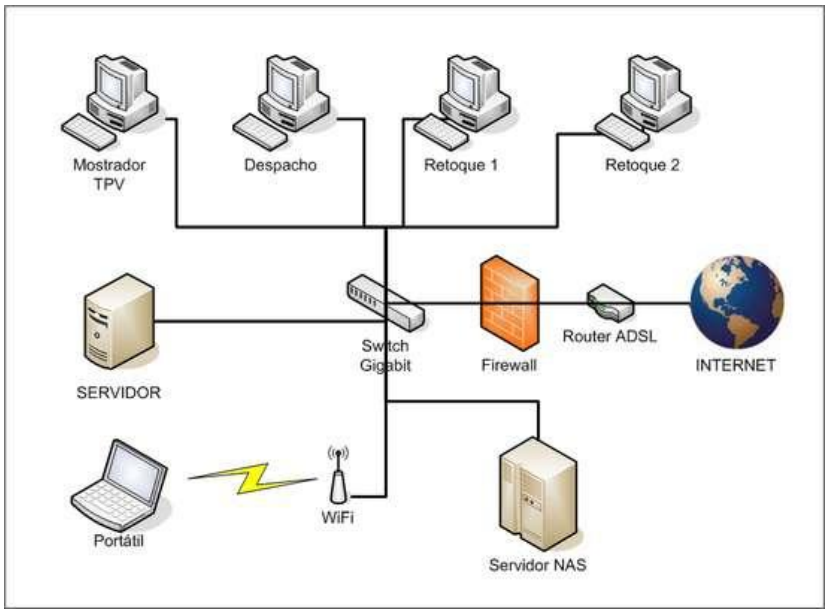


Figura 1.4.- Servidores de red.

- *MODEM*: Es un dispositivo que ofrece al computador conectividad a una línea telefónica, como se observa en la figura 1.5. El módem convierte (modula) los datos de una señal digital en una señal analógica compatible con una línea telefónica estándar. El módem en el extremo

receptor demodula la señal, convirtiéndola nuevamente en una señal digital. Los módems pueden ser internos o bien, pueden conectarse externamente al computador una interfaz de puerto serie ó USB.[4]

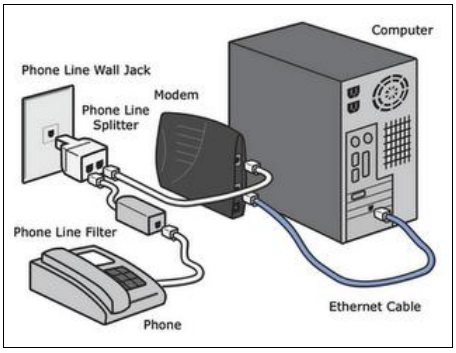


Figura 1.5.- Modem.

- *CDU/DSU:* Las líneas digitales necesitan una unidad de servicio de canal (CSU, channel service unit) y una unidad de servicio de datos (DSU, data service unit). Con frecuencia, las dos se encuentran combinadas en una sola pieza del equipo, llamada CSU/DSU. La CSU proporciona la terminación para la señal digital y garantiza la integridad de la conexión mediante la corrección de errores y la supervisión de la línea. La DSU convierte las tramas de la línea Portadora T en tramas que la LAN puede interpretar y viceversa.[5]

1.3 DESCRIPCIÓN DEL ENRUTAMIENTO

Un router tiene como principal característica conectar múltiples redes y enviar paquetes destinados ya sea a sus propias redes o a otras redes. Es considerado como un dispositivo de capa tres, porque su decisión principal de envío se basa en la información del paquete IP de capa tres,

específicamente la dirección IP de destino. Este proceso se conoce como enrutamiento.

El enrutamiento es un esquema de organización jerárquico que permite que se agrupen direcciones individuales. Estas direcciones individuales son tratadas como unidades únicas hasta que se necesita la dirección destino para la entrega final de los datos. El enrutamiento es el proceso de hallar la ruta más eficiente desde un dispositivo a otro. El dispositivo primario que realiza el proceso de enrutamiento es el Router. [4]

Las siguientes son las dos funciones principales de un Router:

- Los Routers deben mantener tablas de enrutamiento y asegurarse de que otros Routers conozcan las modificaciones a la topología de la red. Esta función se lleva a cabo utilizando un protocolo de enrutamiento para comunicar la información de la red a otros Routers.
- Cuando los paquetes llegan a una interfaz, el Router debe utilizar la tabla de enrutamiento para establecer el destino. El Router envía los paquetes a la interfaz apropiada, agrega la información de entramado necesaria para esa interfaz, y luego transmite la trama.

Un Router es un dispositivo de la capa de red que usa una o más métricas de enrutamiento para determinar cuál es la ruta óptima a través de la cual se debe enviar el tráfico de red. Las métricas de enrutamiento son valores que se utilizan para determinar las ventajas de una ruta sobre otra. Los

protocolos de enrutamiento utilizan varias combinaciones de métricas para determinar la mejor ruta para los datos.

Los routers interconectan segmentos de red o redes enteras. Pasan tramas de datos entre redes basándose en la información de Capa tres. Los Routers toman decisiones lógicas con respecto a cuál es la mejor ruta para la entrega de datos. Luego dirigen los paquetes al puerto de salida adecuado para que sean encapsulados para la transmisión. Los pasos del proceso de encapsulamiento y desencapsulamiento ocurren cada vez que un paquete atraviesa un router.

El router debe desencapsular la trama de capa dos y examinar la dirección de capa tres. El proceso completo del envío de datos de un dispositivo a otro comprende encapsulamiento y desencapsulamiento de las siete capas OSI. Este proceso divide el flujo de datos en segmentos, agrega los encabezados apropiados e información final y luego transmite los datos. El proceso de desencapsulamiento es el proceso inverso: quita los encabezados e información final, y luego combina los datos en un flujo continuo. En la figura 1.6 se observa la representación del proceso de enrutamiento a través de las capas del modelo OSI.

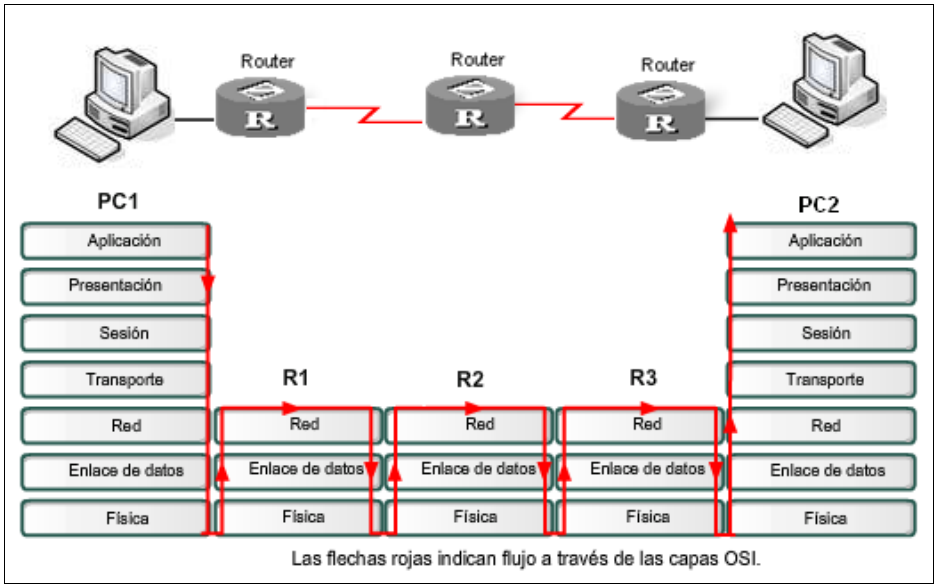


Figura 1.6.- Proceso de Enrutamiento. [4]

1.4 DISPOSITIVOS DE RUTEO

Los routers tienen muchos de los mismos componentes de hardware y software que se encuentran en otras computadoras, entre ellos:

- CPU
- RAM
- ROM
- Sistema operativo.

Un router tiene varias interfaces, cada una de las cuales pertenece a una red IP diferente. Cuando un router recibe un paquete IP en una interfaz, determina qué interfaz usar para enviar el paquete hacia su destino. La interfaz que usa el router para enviar el paquete puede ser la red del destino final del paquete (la red con la dirección IP de destino de este paquete), o puede ser una red conectada a otro router que se usa para alcanzar la red de destino.

Las interfaces se usan para conectar una combinación de redes de área local (LAN) y redes de área extensa (WAN). Por lo general, las LAN son redes Ethernet que contienen dispositivos como PC, impresoras y servidores. Las WAN se usan para conectar redes a través de un área geográfica extensa. Por ejemplo, una conexión WAN comúnmente se usa para conectar una LAN a la red del proveedor de servicios de Internet (ISP).

La principal responsabilidad de un router es dirigir los paquetes destinados a redes locales y remotas al:

- Determinar la mejor ruta para enviar paquetes.
- Enviar paquetes hacia su destino.

El router usa su tabla de enrutamiento para determinar la mejor ruta para reenviar el paquete. Cuando el router recibe un paquete, examina su dirección IP de destino y busca la mejor coincidencia con una dirección de red en la tabla de enrutamiento del router. La tabla de enrutamiento también incluye la interfaz que se utilizará para enviar el paquete. Cuando se encuentra una coincidencia, el router encapsula el paquete IP en la trama de enlace de datos de la interfaz de salida. Luego, el paquete se envía hacia su destino. [4]

Las interfaces de router pueden dividirse en dos grupos principales:

- Interfaces LAN, como Ethernet y FastEthernet.
- Interfaces WAN, como serial, ISDN y Frame Relay.

La interfaz Ethernet del router normalmente usa un jack RJ-45 que admite un cableado de par trenzado no blindado (UTP). Cuando un router se conecta a un switch, se usa un cable de conexión directa. Cuando se conectan dos routers directamente a través de las interfaces Ethernet, o cuando una NIC de PC se conecta directamente a una interfaz Ethernet del router, se usa un cable cruzado.

Las interfaces WAN se usan para conectar los routers a redes externas, generalmente a través de distancias geográficas más extensas. La encapsulación de capa dos puede ser de diferentes tipos, como PPP, Frame Relay y HDLC (Control de enlace de datos de alto nivel). Al igual que las interfaces LAN, cada interfaz WAN tiene su propia dirección IP y máscara de subred, que la identifica como miembro de una red específica.

Los routers tienen conectores físicos que se usan para administrar el router, los llamados puertos de administración. A diferencia de las interfaces seriales y Ethernet, los puertos de administración no se usan para el envío de paquetes. El puerto de administración más común es el puerto de consola. El puerto de consola se usa para conectar una terminal, o con más frecuencia una PC que ejecuta un software emulador de terminal, para configurar el router sin la necesidad de acceso a la red para ese router. El puerto de consola debe usarse durante la configuración inicial del router.

Otro puerto de administración es el puerto auxiliar. No todos los routers cuentan con un puerto auxiliar. A veces el puerto auxiliar puede usarse de maneras similares al puerto de consola. También puede usarse para conectar un módem. [4]

1.5 TOPOLOGÍAS DE RED

La topología de red es la configuración o relación de los dispositivos de red y las interconexiones entre ellos. Estas son al nivel físico y nivel lógico.

La topología física es una configuración de nodos y las conexiones físicas entre ellos. La representación de cómo se usan los medios para interconectar los dispositivos es la topología física.

Una topología lógica es la forma en que una red transfiere tramas de un nodo al siguiente. Esta configuración consiste en conexiones virtuales entre los nodos de una red independiente de su distribución física. Los protocolos de capa de enlace de datos definen estas rutas de señales lógicas. La capa de enlace de datos ve la topología lógica de una red al controlar el acceso de datos a los medios. Es la topología lógica la que influye en el tipo de trama de red y control de acceso a medios utilizados. [3]

La topología lógica de una red está estrechamente relacionada con el mecanismo utilizado para administrar el acceso a la red. Los métodos de acceso proporcionan los procedimientos para administrar el acceso a la red para que todas las estaciones tengan acceso. Cuando varias entidades

comparten los mismos medios, deben estar instalados algunos mecanismos para controlar el acceso. Los métodos de acceso son aplicados a las redes para regular este acceso a los medios.

Las topologías lógica y física generalmente utilizadas en redes son:

Punto a Punto: Esta topología conecta dos nodos directamente entre sí, como se observa en la figura 1.7. En redes de datos con topologías punto a punto, el protocolo de control de acceso al medio puede ser muy simple. Todas las tramas en los medios sólo pueden viajar a los dos nodos o desde éstos. El nodo en un extremo coloca las tramas en los medios y el nodo en el otro extremo las saca de los medios del circuito punto a punto.

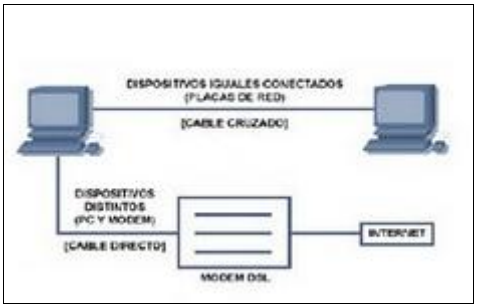


Figura 1.7.- Topología Punto a Punto

Multi-Acceso: Tal como se observa en la figura 1.8, esta topología permite a una cantidad de nodos comunicarse utilizando los mismos medios compartidos. Los datos desde un sólo nodo pueden colocarse en el medio en cualquier momento. Todos los nodos ven todas las tramas que están en el medio, pero sólo el nodo al cual la trama está direccionada procesa los contenidos de la trama.

Hacer que varios nodos compartan el acceso a un medio requiere un método de control de acceso al medio de enlace de datos que regule la transmisión de datos y, por lo tanto, reduzca las colisiones entre las diferentes señales.

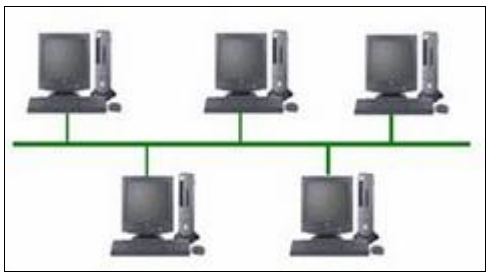


Figura 1.8.- Topología Multi-acceso

Anillo: En una topología lógica de anillo, representada en la figura 1.9, cada nodo recibe una trama por turno. Si la trama no está direccionada al nodo, el nodo pasa la trama al nodo siguiente. Esto permite que un anillo utilice una técnica de control de acceso a la media llamada paso de tokens. Los nodos en una topología lógica de anillo retiran la trama del anillo, examinan la dirección y la envían si no está dirigida para ese nodo. En un anillo, todos los nodos alrededor del anillo entre el nodo de origen y de destino examinan la trama. [3]

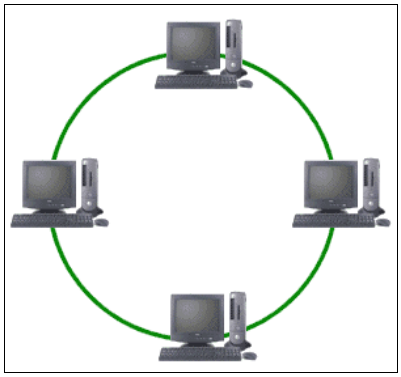


Figura 1.9.- Topología Anillo

Actualmente existe una gran variedad de topologías, como son la topología en bus, en estrella, en anillo; y en el caso de redes complejas, topologías mixtas o híbridas, dependiendo de la flexibilidad y/o complejidad que se quiera dar al diseño. A continuación mencionaremos las principales:

Topología de Bus: La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre sí. Físicamente cada host está conectado a un cable común, por lo que se pueden comunicar directamente. La ruptura del cable hace que los host queden desconectados.

En esta topología los elementos que constituyen la red se disponen linealmente, es decir, en serie y conectados por medio de un cable; el bus, tal como lo podemos observar en la figura 1.10. Las tramas de información emitidas por un nodo (terminal o servidor) se propagan por todo el bus (en ambas direcciones), alcanzando a todos los demás nodos. Cada nodo de la red se debe encargar de reconocer la información que recorre el bus, para así determinar cuál es la que le corresponde, la destinada a él.

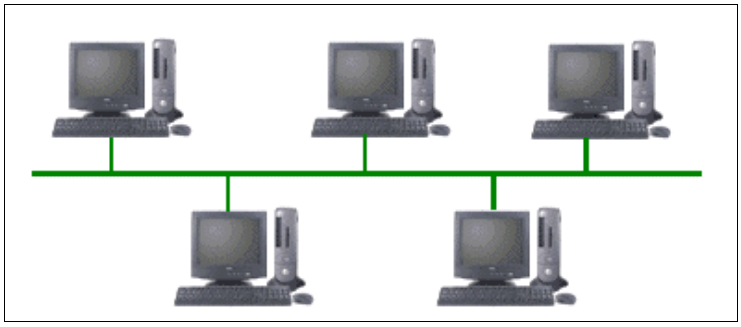


Figura 1.10.- Topología de Bus.

La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si desea que todos los dispositivos obtengan esta información. Sin embargo, puede representar una desventaja, ya que es común que se produzcan problemas de tráfico de colisiones, que se pueden disminuir segmentando la red en varias partes. Es la topología más común en pequeñas LAN, con hub o switch final en uno de los extremos.

Topología de anillo y anillo doble: Una topología de anillo se compone de un solo anillo cerrado formado por nodos y enlaces, en el que cada nodo está conectado solamente con los nodos adyacentes. Los dispositivos se conectan directamente entre sí por medios de cables. Para que la información pueda circular, cada estación debe transferir la información a la estación adyacente.

Una topología en anillo doble consta de dos anillos concéntricos, donde cada host de la red está conectado a ambos anillos, aunque los dos anillos no están conectados directamente entre sí.

En un anillo doble, dos anillos permiten que los datos se envíen en ambas direcciones. Esta configuración crea redundancia (tolerancia a fallos), lo que significa que si uno de los anillos falla, los datos pueden transmitirse por el otro. Esta topología se muestra en la figura 1.11.

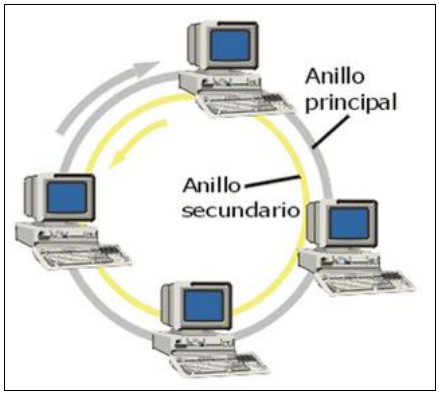


Figura 1.11.- Topología de Anillo Doble.

Topología de Estrella: Una red estrella es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de este. Se utiliza sobre todo para redes locales. La mayoría de las redes de área local que tienen un enrutador (router), un conmutador (switch) o un concentrador (hub) siguen esta topología. El nodo central en estas seria el enrutador, como se muestra en la figura 1.12, el conmutador o el concentrador, por el que pasan todo los paquetes.

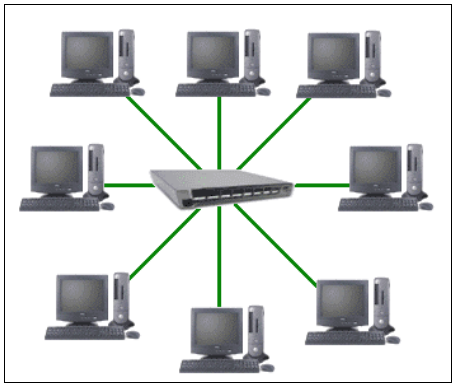


Figura 1.12.- Topología de Estrella.

Topología de árbol: Topología en árbol La topología en árbol es similar a la topología en estrella extendida, salvo en que no tiene un nodo central. En cambio, un nodo de enlace troncal, generalmente ocupado por un hub o switch, desde el que se ramifican los demás nodos. La figura 1.13 representa esta topología.

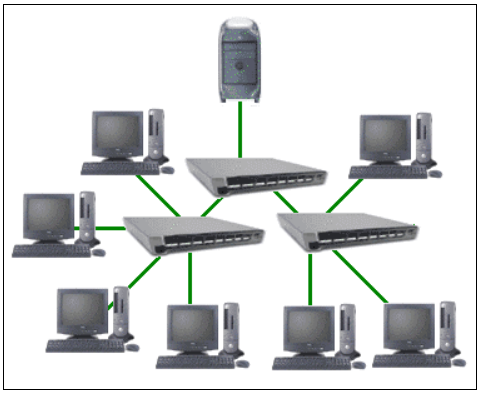


Figura 1.13.- Topología de Árbol

Topología de Malla: Topología en malla completa. En una topología de malla completa, cada nodo se enlaza directamente con los demás nodos. Las ventajas son que, como cada todo se conecta físicamente a los demás, creando una conexión redundante, si algún enlace deja de funcionar la información puede circular a través de cualquier cantidad de enlaces hasta

llegar a destino. Además, esta topología permite que la información circule por varias rutas a través de la red, tal como se muestra en la figura 1.14.

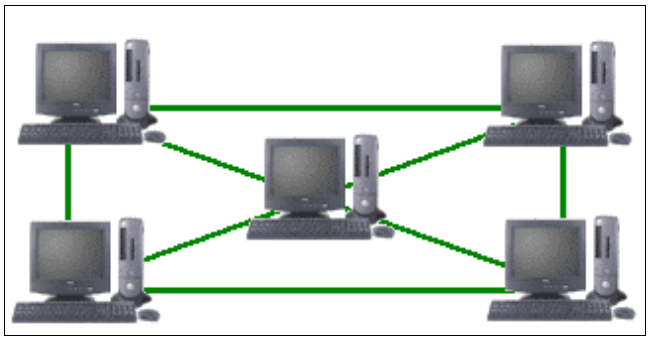


Figura 1.14.- Topología de Malla

La desventaja física principal es que sólo funciona con una pequeña cantidad de nodos, ya que de lo contrario la cantidad de medios necesarios para los enlaces, y la cantidad de conexiones con los enlaces se torna abrumadora.

CAPITULO 2

2. Direccionamiento y Enrutamiento IP

En este capítulo denominado Direccionamiento y Enrutamiento IP, se muestra una explicación precisa sobre cómo está estructurada una dirección IP, así también se explica los distintos tipos de direcciones IP y la direcciones IP por clases.

Además se expone sobre los principios en la división de subredes, se explica sobre los dos tipos de enrutamiento: estático y dinámico; y además se muestra la tabla de enrutamiento con una breve descripción de su estructura.

Finalmente se explica sobre los protocolos de enrutamiento de manera general, explicándose más a detalle los protocolos de vector distancia y estado de enlace.

2.1 ESTRUCTURA DE UNA DIRECCIÓN IP

El direccionamiento es una función clave de los protocolos de capa de Red que permite la transmisión de datos entre hosts de la misma red o en redes diferentes. [3]

Una dirección IP es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del protocolo TCP/IP. Dicho número no se ha de confundir con la dirección MAC que es un número hexadecimal fijo que es asignado a la tarjeta o dispositivo de red por el fabricante, mientras que la dirección IP se puede cambiar. Esta dirección puede cambiar cada vez que se conecta; y a esta forma de asignación de dirección IP se denomina una dirección IP dinámica (normalmente se abrevia como IP dinámica).

El Protocolo de Internet versión cuatro (IPv4) ofrece direccionamiento jerárquico para paquetes que transportan datos.

Diseñar, implementar y administrar un plan de direccionamiento IPv4 efectivo asegura que las redes puedan operar de manera eficaz y eficiente.

En la capa de red es necesario identificar los paquetes de la transmisión con las direcciones de origen y de destino de los dos sistemas finales. Con IPv4, esto significa que cada paquete posee una dirección de origen de treinta y dos bits y una dirección de destino de treinta y dos bits en el encabezado de capa tres.

Dentro de los dispositivos, la lógica digital es aplicada para su interpretación. Para quienes formamos parte de la red humana, una serie de treinta y dos bits es difícil de interpretar e incluso más difícil de recordar. Por lo tanto, representamos direcciones IPv4 utilizando el formato decimal punteada.

Los patrones binarios que representan direcciones IPv4 son expresados con puntos decimales separando cada byte del patrón binario, llamado octeto, con un punto. Se le llama octeto debido a que cada número decimal representa un byte u 8 bits.

Ejemplo de representación de dirección IPv4: 164.12.123.65

En cada dirección IPv4, alguna porción de los bits de orden superior representa la dirección de red. En la capa tres, se define una red como un grupo de hosts con patrones de bits idénticos en la porción de dirección de red de sus direcciones. [3]

A pesar de que los treinta y dos bits definen la dirección host IPv4, existe una cantidad variable de bits que conforman la porción de host de la dirección. El número de bits usado en esta porción del host determina el número de hosts que podemos tener dentro de la red.

En el sistema de numeración binaria la raíz es dos. Por lo tanto, cada posición representa potencias incrementadas de dos. Ver tabla I.

En números binarios de 8 bits, las posiciones representan estas cantidades:

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

Tabla I.- Sistema de numeración binaria.

Cuando se interpreta un byte como un número decimal, se obtiene la cantidad que esa posición representa si el dígito es 1 y no se obtiene la cantidad si el dígito es 0, como se muestra en la tabla II y tabla III. [3]

Un 1 en cada posición significa que el valor para esa posición se suma al total. Un 0 en cada posición indica que el valor para esa posición no se suma al total.

Valor de posiciones	128	64	32	16	8	4	2	1
------	1	1	1	1	1	1	0	0

Tabla II.- Valores correspondientes a posiciones.

Valor de posiciones	128	64	32	16	8	4	2	1
------	1	1	1	1	1	1	0	0
-------	128 + 64 + 32 + 16 + 8 + 4 + 0 + 0							

Tabla III.- Resultado de un octeto.

Así la dirección IPv4 para el siguiente ejemplo mostrado en la tabla IV.

192.168.0.3 = 11000000.10101000.00000000.00000011

		128	64	32	16	8	4	2	1
192	=	1	1	0	0	0	0	0	0
168	=	1	0	1	0	1	0	0	0
0	=	0	0	0	0	0	0	0	0
3	=	0	0	0	0	0	0	1	1

Tabla IV.- Conversión de octetos

2.2 TIPOS DE DIRECCIONES IP.

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

- **Dirección de red:** Se utiliza para referirse a la red en su totalidad.

- **Dirección de broadcast:** Una dirección especial utilizada para enviar datos a todos los hosts de la red.

- **Direcciones host:** Son las direcciones asignadas a los dispositivos finales de la red. [3]

Un ejemplo de tipos de direcciones seria:

192.168.0.0 → dirección de red

192.168.0.1 → dirección de host

192.168.0.255 → dirección de broadcast

Las direcciones IP se clasifican en:

Direcciones IP públicas. Son visibles en todo Internet. Un ordenador con una IP pública es accesible (visible) desde cualquier otro ordenador conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.

Direcciones IP privadas (reservadas). Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los puestos de trabajo. Los ordenadores con direcciones IP privadas pueden salir a Internet por medio de un router (o proxy) que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a ordenadores con direcciones IP privadas.

A su vez, las direcciones IP pueden ser:

Direcciones IP estáticas (fijas). Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto

de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas.

Direcciones IP dinámicas. Un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem. Los proveedores de Internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP (es muy improbable que todos se conecten a la vez).

Dependiendo del número de hosts que se necesiten para cada red, las direcciones de Internet se han dividido en las clases primarias A, B y C. La clase D está formada por direcciones que identifican no a un host, sino a un grupo de ellos. Las direcciones de clase E no se pueden utilizar (están reservadas).

Para saber a qué clase pertenece una IP (ver figura 2.1), basta sólo con ver sus primeros bits:

- Si el primer bit es 0, entonces la IP es de clase A
- Si el primer bit es 1 y el siguiente es 0, entonces es de clase B
- Si los dos primeros son 1, y el tercero es 0, entonces es de clase C.

La **clase C** utiliza sus primeros tres octetos (los primeros 24 bits) para definir su dirección de red, dejando los últimos ocho (el último octeto) para definir su dirección de host. Esto nos dejaría, teóricamente, la posibilidad de

conectar 256 dispositivos pero, debido a que hay dos números reservados para la dirección de red y para la dirección de broadcast, nos deja un total de 254 dispositivos conectados con la misma dirección de red. Esta es la clase utilizada en la mayoría de las redes hogareñas y de las pequeñas o medianas empresas.

La **clase B** utiliza sus primeros dos octetos (16 bits) para definir la dirección de red y los dos restantes para la dirección del host, lo que nos da, quitando las dos direcciones mencionadas anteriormente, 2^16 – 2 = 65.534 host.

La **clase A**, al utilizar su primer octeto (8 bits) para definir la dirección de red, deja los 3 restantes para la dirección del host, o sea, 2^24 – 2 = 16.777.214 dispositivos por red.

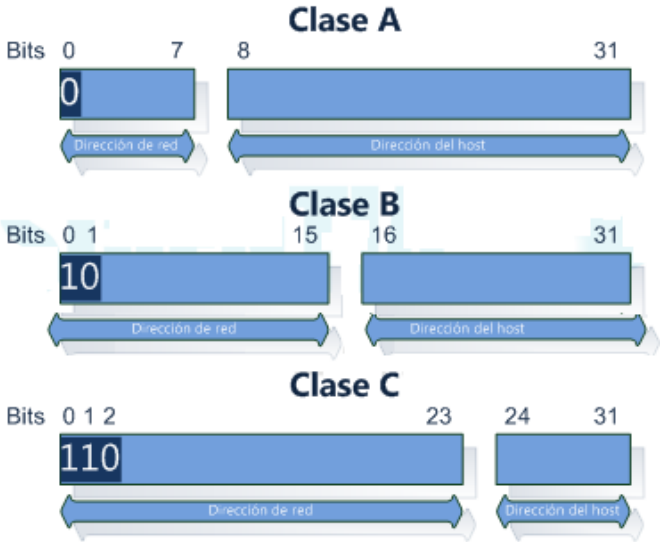


Figura 2.1.- Clase de IP

Cabe mencionar que aunque las direcciones IP de clase A tengan en su primer octeto el primer dígito binario en 0, no se pueden utilizar direcciones IP donde su primer octeto sea 0, o sea, la dirección siempre debe comenzar con un número mayor o igual a 1.

Ya que la clase A posee el primero octeto para la dirección de red, la B los dos primeros, y la C los tres primeros, éstas direcciones también son conocidas como “/8”, “/16” y “/24” respectivamente por la cantidad de bits utilizados para el prefijo.

Con el uso de redes con clases, la máscara estaba implícita en la dirección de clase, pues se conocía a priori los bits para red y los bits para host.
Para definir las porciones de red y de host de una dirección, los dispositivos usan un patrón separado de 32 bits llamado máscara de subred.

La máscara de subred se expresa con el mismo formato decimal punteado que la dirección IPv4. La máscara de subred se crea al colocar un 1 binario en cada posición de bit que representa la porción de red y un 0 binario en cada posición de bit que representa la porción de host. [3]
Por ejemplo:
172.16.20.35 / 27
Dirección
172.16.20.35 → 10101100.00010000.00010100.00100011
Máscara de subred
/27 → 11111111.11111111.11111111.11100000 → 255.255.255.224

2.3 PRINCIPIOS DIVISIÓN EN SUBREDES

Cuando se crearon las direcciones IPv4 se las dividió en cinco clases, con la intención de asignar redes de cada clase según las necesidades de direccionamiento de cada usuario. Así, la siguiente tabla (tabla V):

Clase	1er octeto	Rango	Objetivo	red	host
A	0xxxxxxx	1.0.0.0 - 127.255.255.255	Grandes cantidades de hosts	2^7	2^24 - 2
B	10xxxxxx	128.0.0.0 - 191.255.255.255	Tamaño mediano y grande	2^14	2^16 - 2
C	110xxxxx	192.0.0.0 - 223.255.255.255	Pequeñas redes	2^21	2^8 - 2
D	1110xxxx	224.0.0.0 - 239.255.255.255	Direcciones de multicast	-	-
E	1111xxxx	240.0.0.0 - 255.255.255.255	Reservadas	-	-

Tabla V.- Clases de IP.

El problema que surgió fue que las clases A y B se agotaron muy rápidamente, con lo cual el número de direcciones IP disponibles se redujo drásticamente. El gran problema de las clases es que la diferencia de hosts que cada una admite es muy grande entre sí.

Si se tiene una organización con 1000 hosts en su red. Una red de clase C no satisface sus necesidades, dado que admite como máximo 254 hosts. Entonces, la siguiente opción es una clase B, que tiene una capacidad de direccionamiento de 65534 hosts. Por lo tanto la organización desperdiciará 64534 direcciones IP, lo que representa el 98,47% de las direcciones.

Básicamente, la división en subredes plantea que si una red de clase desperdicia muchas direcciones IP entonces la misma sea dividida en N

subredes más pequeñas que aprovechen mejor el espacio de direccionamiento.

Suponiendo el caso de la organización anterior para la cual una red de clase C es muy chica y, a su vez, una red de clase B es demasiado grande, entonces se puede dividir la red de clase B en redes más chicas que se ajusten más a las realidades de la organización. De esta manera se podría, por ejemplo, dividir una red de clase B en 64 subredes de 1024 hosts cada una (en realidad 1022, pues la primer y última dirección no pueden utilizarse para hosts). De esta forma, la organización que antes desperdiciaba el 98,47% de sus direcciones IP ahora desperdiciará sólo el 2,34% y quedará la posibilidad de tener direcciones para 63 organizaciones más de similar tamaño.

Partiendo de una red dada, para obtener dos subredes será necesario un único bit, ya que con él pueden representarse dos números. Si fueran necesarias tres subredes ya se necesitaría un bit más, que daría como resultado la posibilidad de obtener cuatro subredes. Lógicamente, al utilizar bits de hosts para crear subredes, cuantas más subredes se necesiten menos hosts podrá albergar cada una.

Con la pequeña introducción teórica ya vista se analizará el procedimiento de subnetting utilizando un ejemplo. Para ello, se utilizará una empresa ficticia que está dividida en 4 áreas con 55 hosts cada una y cuenta con la red 192.10.10.0.

En primera instancia lo conveniente es tomar la red asignada y escribirla, junto con su máscara, en números binarios. Así, la red anterior, que según la tabla es una clase C y su máscara es 255.255.255.0 se escribe como:

11000000 00001010 00001010 00000000 → Dirección de red

11111111 11111111 11111111 00000000 → Máscara

r r r r r r r r r r r r r r r r r r r r r r r r hhhhhhhh → r: red; h: host

Ahora bien, según los requerimientos se necesitan cuatro subredes (una para cada área de la empresa) por lo cual deberán tomarse dos bits de la parte de host para representarlas. Entonces lo anterior se podría dividir de la siguiente manera:

11000000 00001010 00001010 **00**000000 → Dirección de red

11111111 11111111 11111111 **11**000000 → Máscara

r r r r r r r r r r r r r r r r r r r r r r r r **ss**hhhhhh → r: red; h: host; s: subred

Podemos notar que ahora, los dos bits más significativos de la parte de host forman parte de la máscara de subred. Con ello, hay 2 bits para subred lo que hace un total de 4 subredes y 6 bits para hosts, lo que significa un total de 64 hosts (62 en realidad).

Un cálculo muy común al realizar subnetting es el de computar la cantidad de hosts y de subredes que pueden obtenerse cuando se subnetea.

Las cuentas son realmente simples y se basan en las siguientes fórmulas:

2^bs - Cantidad de subredes utilizando; bs bits para subred.

(2^bh - 2) - Cantidad de hosts utilizando; bh bits para hosts.

El motivo por el cual se restan los dos bits en la última fórmula es porque la primer y última IP de una subred no puede utilizarse, debido a que la primera dirección es la dirección de subred y la última la de broadcast.

A continuación se presenta una tabla (tabla VI) con los resultados para cada potencia de 2, abarcando desde el 1 hasta el 12. Será de gran utilidad para los primeros cálculos y con la práctica ya no será necesaria.

Bits	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**
Resultados	2	4	8	16	32	64	128	256	512	1024	2048	4096

Tabla VI.- Bits vs Potencia dos.

Cálculo de máscara de subred sabiendo la cantidad de subredes necesarias: El primer caso simple es dada una cantidad de subredes obtener la cantidad de bits necesarios para la máscara de subred. Por ejemplo, si se tiene la subred 170.25.0.0 y se necesitan crear 27 subredes es necesario calcular cuántos bits se necesitan para representar el número 27.

Para ello se puede buscar en la tabla anterior encontrando que con 4 bits es posible representar 16 direcciones (no alcanza) y con 5 bits se obtienen 32 direcciones. Entonces, la máscara se transformará en:

10101010 00011001 00000000 00000000 → 170.25.0.0

11111111 11111111 00000000 00000000 → Máscara original

11111111 11111111 **11111**000 00000000 → Máscara de subred

La máscara anterior en decimal sería 255.255.248.0.

Cálculo de máscara de subred sabiendo la cantidad de hosts: Para calcular la máscara en base a la cantidad de hosts el mecanismo es muy similar al anterior con una consideración más y es que al valor de la tabla es necesario restarle 2 unidades (por las direcciones de subred y de broadcast).

Tomando como ejemplo una organización que cuenta con la clase B 181.67.0.0 y está dividida en varias áreas donde la más grande de ellas tiene 500 hosts, se debe calcular cuántos bits destinar a host. Buscando en la tabla se ve que la opción adecuada es utilizar 9 bits que nos da un total de 510 hosts. Lo que nos daría lo siguiente 181.67.0.0 / 255.255.254.0

2.4 RUTEO ESTÁTICO Y RUTEO DINÁMICO

El enrutamiento es fundamental para cualquier red de datos, ya que transfiere información a través de una internetwork de origen a destino. Los routers aprenden sobre redes remotas ya sea de manera dinámica o utilizando protocolos de enrutamiento o de manera manual, utilizando rutas estáticas.

Las rutas estáticas son muy comunes y no requieren la misma cantidad de procesamiento y sobrecarga que requieren los protocolos de enrutamiento dinámico. [4]

Las rutas a redes remotas con los siguientes saltos asociados se pueden configurar manualmente en el router. Esto se conoce como enrutamiento estático.

Las rutas estáticas se utilizan generalmente cuando se enruta desde una red a una red de conexión única. Una red de conexión única es una red a la que se accede por una sola ruta. La ejecución de un protocolo de enrutamiento en este tipo de casos es un desperdicio de recursos porque sólo tiene una manera de enviar tráfico que no sea local. Por lo tanto, las rutas estáticas se configuran para obtener conectividad a redes remotas que no están conectadas directamente al router.

Además existen rutas estáticas por defecto. Una ruta estática por defecto es una ruta que coincidirá con todos los paquetes. Las rutas estáticas por defecto se utilizan en los siguientes casos:

- Cuando ninguna otra ruta de la tabla de enrutamiento coincide con la dirección IP de destino del paquete. En otras palabras, cuando no existe una coincidencia más específica. Se utilizan comúnmente cuando se conecta el router extremo de una empresa a la red ISP.

- Cuando un router sólo tiene otro router más al que está conectado. Esta condición se conoce como router de conexión única.

Básicamente el enrutamiento estático se utiliza en los siguientes casos:

- La red es pequeña.
- Solo hay un punto de unión hacia el resto de la red.
- No hay rutas redundantes.

Si no se cumple una de las tres condiciones antes mencionadas se suele usar enrutamiento dinámico.

Aunque es esencial que todos los routers en una internetwork posean conocimiento actualizado, no siempre es factible mantener la tabla de enrutamiento por configuración estática manual. Por eso, se utilizan los protocolos de enrutamiento dinámico.

Los protocolos de enrutamiento se usan para facilitar el intercambio de información de enrutamiento entre los routers. Estos protocolos permiten a los routers compartir información en forma dinámica sobre redes remotas y agregar esta información automáticamente en sus propias tablas de enrutamiento. [4]

Los protocolos de enrutamiento determinan la mejor ruta a cada red que luego se agrega a la tabla de enrutamiento. Uno de los principales beneficios de usar un protocolo de enrutamiento dinámico es que los

routers intercambian información de enrutamiento cuando se produce un cambio de topología. Este intercambio permite a los routers aprender automáticamente sobre nuevas redes y también encontrar rutas alternativas cuando se produce una falla de enlace en la red actual.

En comparación con el enrutamiento estático, los protocolos de enrutamiento dinámico requieren menos sobrecarga administrativa. Sin embargo, el costo de usar protocolos de enrutamiento dinámico es dedicar parte de los recursos de un router para la operación del protocolo.

Un protocolo de enrutamiento es un conjunto de procesos, algoritmos y mensajes que se usan para intercambiar información de enrutamiento y completar la tabla de enrutamiento con la selección de las mejores rutas del protocolo de enrutamiento.

El propósito de un protocolo de enrutamiento incluye:

- Descubrimiento de redes remotas.
- Mantenimiento de información de enrutamiento actualizada.
- Selección de la mejor ruta hacia las redes de destino y
- Capacidad de encontrar una mejor nueva ruta si la ruta actual deja de estar disponible. [4]

Las operaciones de un protocolo de enrutamiento dinámico varían según el tipo de protocolo de enrutamiento y el protocolo de enrutamiento en sí.

En general, las operaciones de un protocolo de enrutamiento dinámico pueden describirse de la siguiente manera:

- El router envía y recibe mensajes de enrutamiento en sus interfaces.
- El router comparte mensajes de enrutamiento e información de enrutamiento con otros routers que están usando el mismo protocolo de enrutamiento.
- Los routers intercambian información de enrutamiento para aprender sobre redes remotas.
- Cuando un router detecta un cambio de topología, el protocolo de enrutamiento puede anunciar este cambio a otros routers.[4]

2.5 ELABORACIÓN DE TABLAS DE RUTEO

Si sabe qué direcciones de red (o identificadores de red) se encuentran disponibles en la interconexión de redes, le resultará más fácil decidir si debe realizar un enrutamiento. Esta información se obtiene a partir de una base de datos denominada tabla de enrutamiento.

La tabla de enrutamiento está constituida por una serie de entradas denominadas rutas que contienen información acerca de dónde están situados los identificadores de red de la interconexión de redes. La tabla de enrutamiento no es exclusiva de un solo enrutador.

Las tablas de enrutamiento generalmente pueden mantenerse manualmente cuando la red es pequeña y estática. La tablas de

enrutamiento para todos los dispositivos de red nunca cambian a menos que y hasta que el administrador de la red de los cambios manualmente. En el enrutamiento dinámico, los dispositivos automáticamente construyen y mantienen sus propias tablas de enrutamiento. Lo hacen mediante el intercambio de información relativa a la topología de red utilizando protocolos de enrutamiento. Esto permite a los dispositivos de la red de adaptarse automáticamente a los cambios en la red como dispositivo de fallas y congestión de la red cuando se produzcan. Para ver la tabla de enrutamiento de nuestro router podemos acceder al perfil de administración que poseen los router o bien desde el comando "route print" desde el cmd.exe de Windows.

Tipos de entrada de la tabla de enrutamiento: Cada entrada de la tabla de enrutamiento se considera una ruta y pertenece a uno de los tipos siguientes:

Ruta de red: Una ruta de red proporciona la ruta de un determinado identificador de red de la interconexión de redes.

Ruta de host: Una ruta de host proporciona la ruta de una dirección de la interconexión de redes (identificador de red). Las rutas de host se utilizan normalmente para crear rutas personalizadas a hosts específicos a fin de controlar u optimizar el tráfico de la red.

Ruta predeterminada: Se utiliza cuando no se encuentra ninguna otra ruta en la tabla de enrutamiento. Por ejemplo, si un enrutador o host no puede encontrar una ruta de red o de host para el destino, se utilizará la ruta predeterminada. La ruta predeterminada simplifica la configuración de los hosts. En vez de configurar hosts con rutas para todos los identificadores de red de la interconexión de redes, se utiliza una única ruta predeterminada para reenviar todos los paquetes con una dirección de red o de interconexión de redes de destino que no se encontró en la tabla de enrutamiento.

Estructura de la tabla de enrutamiento: La figura 2.2 muestra la estructura de la tabla de enrutamiento.

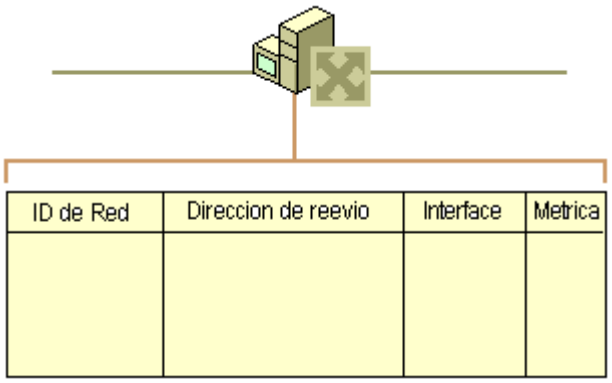


Figura 2.2.- Estructura de la tabla de enrutamiento

Cada entrada de la tabla de enrutamiento consta de los siguientes campos de información:

Identificador de red: Identificador de red o dirección de la interconexión de redes correspondiente a una ruta de host. En los enrutadores IP, hay un

campo de máscara de subred adicional que determina el identificador de red IP desde una dirección IP de destino.

Dirección de destino: dirección IP de un host o una red.

Siguiente dirección del salto: La dirección del router siguiente que un router pasará a través para llegar a su destino.

Interfaz: La interfaz de red que se utiliza cuando se reenvían los paquetes al identificador de red. Se trata de un número de puerto u otro tipo de identificador lógico, que se va a utilizar para alcanzar el siguiente enrutador.

Métrica: La métrica indica el costo relativo por utilizar la ruta para alcanzar el destino. La métrica típica son los saltos, o número de enrutadores que se atraviesan para alcanzar el destino. Si existen varias rutas al mismo destino, la ruta con menor métrica es la ruta más adecuada

Protocolo: El protocolo muestra cómo se aprendió la ruta. Si en la columna protocolo se enumeran los protocolos RIP u OSPF (o cualquier otro que no sea Local), el enrutador está recibiendo las rutas.

2.6 PROTOCOLOS DE RUTEO

Los protocolos de enrutamiento son el conjunto de reglas utilizadas por un router cuando se comunica con otros router con el fin de compartir información de enrutamiento.

Dicha información se usa para construir y mantener las tablas de enrutamiento.

Los protocolos de enrutamiento pueden clasificarse en diferentes grupos según sus características. Los protocolos de enrutamiento que se usan con más frecuencia son:

- RIP: un protocolo de enrutamiento interior por vector de distancia.
- OSPF: un protocolo de enrutamiento interior de estado de enlace.
- IS-IS: un protocolo de enrutamiento interior de estado de enlace.
- BGP: un protocolo de enrutamiento exterior de vector de ruta.[4]

Debido a que Internet se basa en el concepto de sistema autónomo, se requieren dos tipos de protocolos de enrutamiento. Estos protocolos son:

- *Interior Gateway Protocols (IGP)*: se usan para el enrutamiento de sistemas intrautónomos (el enrutamiento dentro de un sistema autónomo).
- *Exterior Gateway Protocols (EGP)*: se usan para el enrutamiento de sistemas interautónomos (el enrutamiento entre sistemas autónomos).

Un sistema autónomo (AS), conocido también como dominio de enrutamiento, es un conjunto de routers que se encuentran bajo una administración en común. Un sistema autónomo está comúnmente compuesto por muchas redes individuales que pertenecen a empresas, escuelas y otras instituciones.

Un IGP se usa para enrutar dentro de un sistema autónomo, y también se usa para enrutar dentro de las propias redes individuales. Los IGP para IP incluyen RIP, OSPF e IS-IS.

Los protocolos de enrutamiento, y más específicamente el algoritmo utilizado por ese protocolo de enrutamiento, utilizan una métrica para determinar la mejor ruta hacia una red. La métrica utilizada por el protocolo de enrutamiento RIP es el conteo de saltos, que es el número de routers que un paquete debe atravesar para llegar a otra red. OSPF usa el ancho de banda para determinar la ruta más corta.

Estos dos protocolos serán objeto de nuestro estudio razón por la cual analizaremos a detalle los protocolos de Gateway interiores (IGP).

Los protocolos de gateway interiores (IGP) pueden clasificarse en dos tipos:

2.6.1. Protocolos de enrutamiento por vector de distancia

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

Los protocolos por vector de distancia utilizan routers como letreros a lo largo de la ruta hacia el destino final. La única información que conoce el router sobre una red remota es la distancia o métrica para llegar a esa red y qué ruta o interfaz usar para alcanzarla. Los protocolos de enrutamiento por vector de distancia no tienen un mapa en sí de la topología de la red.

Los protocolos por vector de distancia funcionan mejor en situaciones donde:

- La red es simple y plana, y no requiere de un diseño jerárquico especial.
- Los administradores no tiene suficientes conocimientos como para configurar protocolos de estado de enlace y resolver problemas en ellos.
- Se están implementando tipos de redes específicos.

- Los peores tiempos de convergencia en una red no son motivo de preocupación.

Los protocolos de enrutamiento por vector de distancia incluyen RIP.

RIP (Routing Information Protocol) es un relativamente simple Interior Gateway Protocol (IGP), y se aplica principalmente a las redes relativamente pequeñas.

Desde la aplicación RIP es relativamente sencillo, el impacto del costo del propio protocolo sobre el rendimiento de las redes es relativamente pequeña, y la configuración y el mantenimiento de la RIP es más fácil que la de OSPF e IS-IS, RIP es aún ampliamente utilizado en la práctica.

RIP es una especie de vector distancia, algoritmo basado en el protocolo y el intercambio de información de enrutamiento a través de paquetes UDP. Emplea el número de saltos para medir la distancia al host de destino, esto se llama Reducción de costos. En RIP, el número de saltos de un router a su red conectada directamente es 0, y a una red que se puede llegar a través de otro router es 1, y así sucesivamente. Para limitar el tiempo para convergencia, RIP establece que el costo es un número entero entre 0 y 15. El número de saltos igual o superior a 16 se define como infinito, es decir, la red de destino o el host es inalcanzable.

Para mejorar el rendimiento y evitar la creación de bucles de enrutamiento, RIP es compatible con horizonte dividido y Poison Reverse. Además, RIP, puede redistribuir las rutas de los protocolos de enrutamiento.

RIP se describe como controlada por tres temporizadores, actualización de época, tiempo de espera y recolector de basura.

- Temporizador de período de actualización es enviar toda la información de enrutamiento RIP a todos los vecinos.

- Si una ruta RIP no se actualiza en el plazo de tiempo de espera configurado en el temporizador (es decir, el router local no recibe el paquete de actualización de la ruta de los vecinos), la ruta será considerada como inalcanzable.

- Si el router local aún no recibe ningún paquete de actualización de la ruta de los vecinos, es decir, si la ruta es inalcanzable aún no actualizados, la ruta se quita de la tabla de enrutamiento.

Actualmente, dos versiones están disponibles RIP: RIP-1 y RIP-2.

RIP-1 es un protocolo de enrutamiento con clases. Se anuncia paquetes de protocolo de la radiodifusión. Como RIP-1 no incluyen información de la máscara de subred, RIP sólo puede reconocer los

segmentos de la red de rutas naturales, como las rutas de la clase A, B o C. Por esta razón, RIP-1 no es compatible con resumen de la ruta y subredes no contiguas.

RIP-2 es un protocolo de enrutamiento sin clases. En comparación con RIP1, tiene las siguientes ventajas:

- Separación interna rutas RIP (rutas de las redes en el dominio de enrutamiento RIP) de las rutas externas de RIP, que pueden haber sido importados de un EGP u otro IGP. Usted puede utilizar etiqueta de ruta de enrutamiento con políticas de gestión de rutas de manera flexible.
- Máscara de subred, resumen de la ruta de apoyo y otras cosas sin clases-Domain Routing (CIDR).
- Especificado de siguiente salto, la dirección óptima del siguiente salto se puede encontrar en la red de difusión.
- Multidifusión para el envío de actualizaciones periódicas, reduciendo el consumo de recursos.
- Autenticación de mensajes RIP para mayor seguridad. [6]

2.6.2. Protocolos de enrutamiento de estado de enlace

A diferencia de la operación del protocolo de enrutamiento por vector de distancia, un router configurado con un protocolo de enrutamiento de estado de enlace puede crear una "vista completa" o topología de la red al reunir información proveniente de todos los demás routers.

Haciendo una analogía con letreros, el uso de un protocolo de enrutamiento de estado de enlace es como tener un mapa completo de la topología de la red. Los letreros a lo largo de la ruta desde el origen al destino no son necesarios, porque todos los routers de estado de enlace usan un "mapa" idéntico de la red. Un router de estado de enlace usa la información de estado de enlace para crear un mapa de la topología y seleccionar la mejor ruta hacia todas las redes de destino en la topología.

Los protocolos de estado de enlace funcionan mejor en situaciones donde:

- El diseño de red es jerárquico, y por lo general ocurre en redes extensas.
- Los administradores conocen a fondo el protocolo de enrutamiento de estado de enlace implementado.
- Es crucial la rápida convergencia de la red.

Los protocolos de enrutamiento de estado de enlace incluyen OSPF.

OSPF (Open Shortest Path First) es un protocolo de puerta de enlace interna, permite de las siguientes características:

- *Alcance de aplicación*: Se puede apoyar a las redes de distintos tamaños y puede soportar varios cientos de routers como máximo.
- *Rápida convergencia*: Puede transmitir los paquetes de actualización inmediatamente después de los cambios de topología de red.

- *Libre de bucle*: Desde el OSPF calcula las rutas con el algoritmo de árbol de ruta más corta de acuerdo a la relación de estados de enlace, se garantiza que ninguna ruta de bucle será generado por el propio algoritmo.
- *Área de partición*: Se permite a la red se divida en diferentes áreas para la comodidad de gestión, a fin de que la información transmitida entre las áreas es la más abstracta, por lo tanto, para reducir el consumo de ancho de banda de red.
- *Igual-costo múltiples-ruta*: Soporte de múltiples rutas de igual coste a un destino.
- *Jerarquía de enrutamiento*: OSPF tiene una jerarquía de enrutamiento de nivel cuatro. Se da prioridad a las rutas a ser dentro del área, entre el área, tipo externo-1, y de tipo externo-2 rutas.
- *Autenticación*: Es compatible con la interfaz de autenticación basada en paquetes con el fin de garantizar la seguridad del cálculo de la ruta.
- *Transmisión de multidifusión*: dirección de multidifusión de apoyo para recibir y enviar paquetes.

Entre los principales conceptos relacionados con OSPF tenemos:

Router ID: Cada enrutador OSPF debe tener un ID de router. Puede asignar una a un enrutador OSPF manualmente. Este ID Router es preferentemente la dirección de una interfaz de bucle invertido, ya que

una interfaz de bucle invertido está siempre hasta que se apague manualmente. Si no se especifica ningún ID de router, el sistema selecciona automáticamente una para el router de la siguiente manera:

- Si la dirección de la interfaz de bucle invertido está disponible, selecciona la configurada recientemente.
- Si no, seleccione la dirección IP de la primera interfaz física que está configurada y levantada.

DR y BDR:

DR (Designated Router): En la red de transmisión, para que cada enrutador pueda transmitir su información de estado local para la totalidad de AS (Sistema Autónomo), múltiples relaciones de vecinos deben crearse entre los routers. Esto, sin embargo, hace posible que la variación de la ruta de cualquier router resulte en un envío repetido, lo que desperdicia el recurso de ancho de banda. Para resolver el problema, OSPF define el "Designated Router" (DR). Todos los routers sólo tendrán que transmitir información a la DR para la transmisión de la red de estados de enlace. La relación de vecinos no se establece entre dos routers de otros DRs (llamado como otros DR), ni tampoco los otros DR intercambiarán toda la información de enrutamiento. No es especificado manualmente qué router será la DR del segmento de red local, pero comúnmente es elegido por todos los routers en el segmento de red.

BDR (Backup Designated Router): Si el DR deja de ser válido debido a una falla, debe ser reelegidos y sincronizados. Se necesita tiempo y mientras tanto el cálculo de la ruta es incorrecta. Con el fin de acelerar este proceso, OSPF propone el concepto de BDR. De hecho, BDR es una copia de seguridad de DR. DR y BDR son elegidos en ese plazo. Las adyacencias también se ha establecido entre el BDR y todos los routers de la serie de sesiones, y la información de enrutamiento se intercambiaron entre ellos. Una vez que el DR deja de ser válida, la BDR de inmediato se convertirá en un DR, y un nuevo BDR será reelegido.

Área: Cuando un gran número de routers OSPF están presentes en una red, LSDBs (Link-State Database) puede llegar a ser tan grande que una gran cantidad de espacio de almacenamiento estará ocupado y los recursos de CPU agotaran realizando el cálculo de SPF (Sender Policy Framework). Además, como la topología de una gran red es propenso a los cambios, gran cantidad de paquetes OSPF se pueden crear, disminuyendo la utilización de ancho de banda.

Para resolver este problema, OSPF divide un AS en múltiples áreas, que son identificadas por identificadores de área. En un sentido lógico, las áreas ponen routers en diferentes grupos. El área 0, también conocida como área de red troncal, es una de más importancia.

El área de red troncal de enrutamiento alcanza el intercambio de información entre las áreas de red no troncal. El área de red troncal y otras áreas de red no troncal deberá estar físicamente consecutiva. De lo contrario, usted tiene que configurar los enlaces virtuales para que sean consecutivos.

El router que conecta el área de red troncal y otra área se denomina enrutador de borde de área (ABR), también existe el router límite de sistema autónomo (ASBR) en OSPF.

Agregación de ruta: Un AS se divide en áreas que están interconectados a través de OSPF ABRs. La información de enrutamiento entre las áreas se puede reducir mediante la agregación de ruta. Así, el tamaño de las tablas de enrutamiento pueden ser reducidas y la velocidad de cálculo del router puede ser mejorado.

Después de calcular una intra-area de una ruta de un área, la ABR buscará la tabla de enrutamiento y encapsular cada ruta OSPF en un LSA y lo envía fuera del área. [7]

CAPITULO 3

3. Configuración del ruteador

En este tercer capítulo denominado Configuración del ruteador, se realiza un estudio de las configuraciones básicas y principales en estos dispositivos, ya q se explica la configuración inicial que se debe realizar en estos dispositivos, así como también la configuración de las interfaces con sus respectivas direcciones IP.

Además se muestra los distintos comandos que se utilizan para la configuración de los protocolos de ruteo.

Finalmente se expone sobre las posibles soluciones a los problemas comunes que se puedan presentar en la configuración de los protocolos de enrutamiento en una red.

3.1 CONFIGURACIONES BÁSICAS

La interfaz de usuario como los modos de configuración de usuario permite al administrador del sistema configurar las distintas características en los equipos HUAWEI.

Los equipos HUAWEI definen cuatro tipos de interfaces de usuarios asociados con los modos de configuración, estos son:

- *Puerta de Consola (CON):* El puerto de consola es un puerto del tipo dispositivo de línea. En un router, el puerto de consola EIA/TIA-232 se utiliza para permitirle a los usuarios realizar configuraciones.
- *Puerto Auxiliar (AUX):* El puerto auxiliar es un puerto del tipo dispositivo de línea. En un router, el puerto auxiliar EIA/TIA-232 DTE entrega la capacidad de conexiones de discado vía MODEM. (no aplicable para este modelo).
- *Puerto Asincrónico (TTY):* La interfaz de usuario TTY es empleado cuando un usuario desea conectarse al router a través de un puerto serial asincrónico o a través de un puerto sincrónico/asincrónico (trabajando en modo asincrónico).

- *Línea Virtual (VTY):* Un puerto virtual es una línea Terminal lógica empleada para el acceso mediante telnet al router y es generalmente conocido como VTY (Virtual Type Line). [8]

Configuración a través de Consola

Para ingresar al ambiente de configuración local, conecte el puerto serial de su PC (o terminal) al puerto de consola del Switch usando el cable consola estándar RS-232 como se muestra en la figura 3.1.

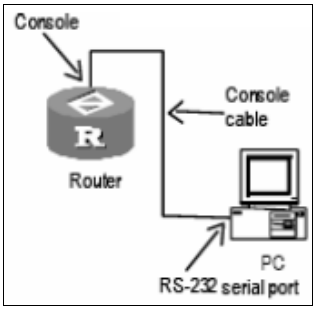


Figura 3.1.- Conexión puerto consola

Corra el programa de emulación de terminal (por ejemplo Win9x o Hyper Terminal) en el PC, y configure los parámetros de comunicación como se muestra en las figuras 3.2 y 3.3.

Figura 3.2.- Nueva conexión y puerto de conexión

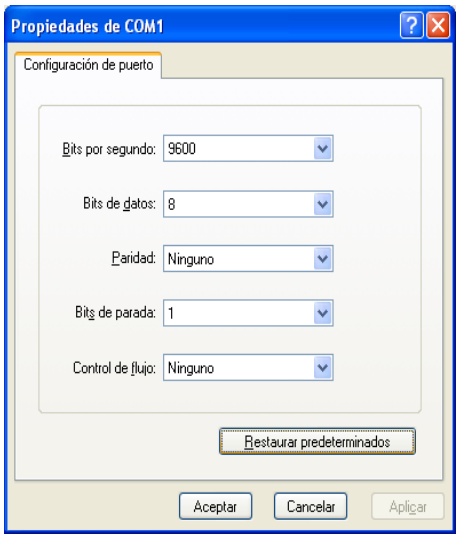


Figura 3.3.- Configurar los parámetros de comunicación

Una vez completada esta etapa presiona **`aceptar`** hasta que el símbolo de la línea de comando, **`<Quidway>`** aparezca. [9]

A. *Modo de Vista Usuario*

Cuando se hace la conexión al router (como en la actividad anterior) se ingresa al prompt en el modo de vista de usuario.

La petición de entrada aparece de la siguiente forma:

```
<Quidway>
```

B. Modo de Vista de sistema

Se puede ingresar al modo de vista de sistema a partir del modo de vista de usuario digitando el comando **system-view** como se muestra a continuación:

```
<Quidway>system-view
System View: return to User View with Ctrl+Z.
[Quidway]
```

Vea que el nombre **Quidway** (nombre del router) quedó encerrado entre corchetes.

Para regresar al modo inmediato anterior se digita el comando **quit**. Lo puede utilizar desde cualquier vista.

```
[Quidway]quit
<Quidway>
```

Además del comando **quit** existe **return** que nos permite salir de cualquier modo hacia el modo de vista de usuario, como por ejemplo cuando configuramos las interfaces (ver 3.2), podemos regresar a la vista de usuario con **return**. También puede regresar directamente al modo de vista de usuario usando **<Ctrl + Z>.**

```
[Quidway-Ethernet0/0]return
<Quidway>
```

3.1.1 Nombre de dispositivo

Desde el modo de vista de usuario ingrese al modo de vista de sistema con **system-view**

```
<Quidway>
<Quidway>system-view
System View: return to User View with Ctrl+Z.
```

Ingrese el comando **sysname** y a continuación el nombre que desea ponerle al router Router_1.

```
[Quidway]sysname Router_1
[Router1]
```

Note que el nombre por defecto cambió por el que ingresó.

3.1.2 Mensaje de Inicio

El comando **header motd** le permite configurar un mensaje al ingresar en el router según crea conveniente. Además debe ingresar algún otro caracter que le indique a este comando que al ser ingresado dicho caracter termina el mensaje. Por conveniencia usaremos %.

Desde el modo de vista de sistema ingrese el comando **header motd** además del caracter de fin de texto %. Cuando le indique, ingrese su mensaje, y al final del mismo, el carácter %. [10]

```
[Router1]
[Router1]header motd %
Input banner text, and quit with the character '%'.
***** MENSAJE DE INICIO ******
%
[Router1]
```

Digite el comando **quit** para salir del modo de vista de sistema. Nuevamente digite **quit** para salir del modo de vista de usuario. Le aparecerá en la pantalla una petición de ENTER, y al presionar verá el mensaje de inicio que escribió. Esto se muestra en la figura 3.4.

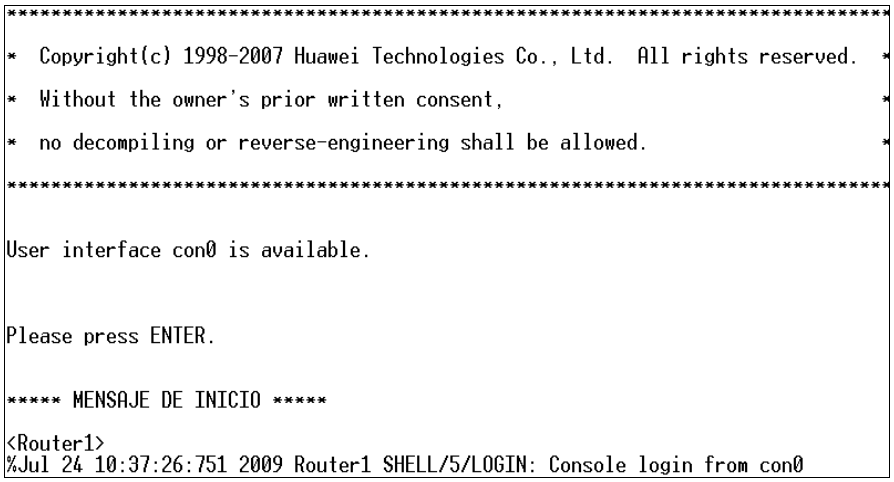


Figura 3.4.- Configurar Mensaje de de inicio

3.1.3 Contraseñas

Un router no posee una contraseña de usuario cuando se enciende por primera vez. Bajo esas condiciones, cualquier usuario puede realizar configuraciones en el equipo mientras se conecte a través de consola.

Un usuario remoto puede acceder vía telnet si el router ha sido configurado con dirección IP.

Para asegurar seguridad en la red, es necesario configurar un usuario y una contraseña para el router con el fin de permitir la administración de estos.

El sistema maneja jerarquías para los usuarios Telnet e HyperTerminal. De acuerdo con esta jerarquía, los usuarios se clasifican en 4 niveles: visitante, monitor, sistema y administración. Todos estos identificados con números del 0 al 3.

Después de que los usuarios de los distintos niveles ingresan, sólo pueden emplear comandos de su mismo nivel o inferiores. Si el tipo de autentificación que se está utilizando es mediante contraseña o si simplemente no se utiliza autentificación, el nivel de comandos al que el usuario puede acceder depende del nivel configurado en la interfaz de usuario. [8]

Por ejemplo, si el nivel de prioridad de un usuario es 2, él solo puede acceder a comandos de nivel 0 hasta 2.

El usuario con nivel de prioridad 3 puede acceder a todos los comandos. Los comandos que los usuarios de cada nivel pueden acceder se muestran en la tabla VII:

Prioridad de Usuario	Nombre	Comando
0	Visit	Ping, tracert, telnet
1	Monitor	Ping, tracert, telnet, display, debugging
2	System	Todos los commandos de configuración (excepto los de administración) y los comandos con nivel de prioridad 0 y 1
3	Manage	Todos los comandos

Tabla VII.- Prioridad de Usuario

El sistema autentifica a los usuarios cuando estos se conectan. Existen 4 tipos de métodos de autentificación:

- Autentificación local;
- Autentificación en servidor AAA;
- Autentificación mediante contraseña;
- Sin autentificación.

No se recomienda no utilizar autentificación, debido a que usuarios pueden acceder al router sin nombre de usuario ni contraseña.

La autentificación mediante contraseña es levemente segura, debido a que requiere a cada usuario que se conecte el ingreso de la contraseña asociado.

Cuando se emplea autentificación local o mediante un servidor AAA, se debe ingresar un nombre de usuario y contraseña que correspondan a los configurados en el router o en el servidor AAA. Los usuarios de

discado se autentifican usualmente a través de servidores AAA mientras que los usuarios telnet y de terminal lo realizar de forma local. Al configurar el modo de autentificación de usuario, se puede configurar el método de autentificación que se empleará cuando un usuario acceda el router a través de la interfaz de usuario especificada. [8]

authentication-mode { password | scheme [command-authorization] }

None: Indica que no se emplea autentificación.

Password: Autentificación empleando contraseña pero no usuario.

Scheme: Autentificación empleando el esquema AAA (autentificación local, RADIUS/HWTACACS).

Autentificación mediante password

Esta configuración se realiza en el modo de visualización de la interfaz.

set authentication password { cipher | simple } clave

Simple: Se configure el password en texto plano.

Cipher: Se configura el password con texto encriptado.

Autentificación local con nombre de usuario y password

Si se elige autentificación local, será necesario emplear nombre de usuario y contraseña. En la tabla VIII se muestra los comandos para establecer un usuario y contraseña.

Operación	Comando
Configurar nombre de usuario (en system view)	**local-user** nombre-usuario
Eliminar usuario (en system view)	**undo local-user** { nombre-usuario | all }
Configurar una contraseña para el usuario local (en local user view)	**password** { cipher | simple } password
Cancelar la contraseña del usuario local (en local user view)	**undo password**

Tabla VIII.- Nombre de usuario y password

El comando **`service-type`** permite configurar el nivel de comandos que un usuario puede utilizar en un determinado servicio.

Los servicios a los cuales pueden acceder los usuarios se muestran en la tabla IX a continuación:

ftp	Servicio FTP
lan-access	Servicio LAN-ACCESS
ssh	Servicio Secure Shell
telnet	Servicio TELNET
terminal	Servicio TERMINAL

Tabla IX.- Tipo de servicio

En el ejemplo de configuración que se muestra, se configura el usuario local **prueba**, con clave encriptada **huawei123**, que tendrá acceso al servicio telnet con un nivel de prioridad **0**.

Ejemplo de configuración:

```
[Router_1] local-user prueba
[Router_1-luser-prueba] password cipher huawei123
[Router_1-luser-prueba] service-type telnet level 0
```

3.2 CONFIGURACIÓN DE INTERFACES

Interfaz se refiere a la parte a través de la cual un sistema del router intercambia datos e interactúa con otros dispositivos en la red. Su función es lograr el intercambio de datos entre el router y otros dispositivos de red.

La vista de la interfaz está diseñada en el software VRP (Versatile Routing Platform) para la comodidad de la configuración y mantenimiento. Todos los comandos relacionados con una interfaz puede ser válido sólo cuando se utilizan en la vista de la interfaz. [11]

El comando de **`Interface`** permite entrar en la vista de la interfaz especificada (ver tabla X).

Operación	Comando
Entra en la vista de una interface especificada	**interface** *type number*

Tabla X.- Vista de una interface

Hay una entrada de configuración de descripción de la interfaz, para cada interfaz física en los routers para identificar la función de esa interfaz Esto se muestra en la tabla XI, además en la tabla XII se muestra unos comando de mucha importancia a la hora de configurar una interface.

Operation	Command
Configuración de descripción de interface	**description** *interface-description*
Restaurar la descripción de la interface por default	**undo description**

Tabla XI.- Configuración de descripción de interface

Operación	Comando	Observación
Borrar la estadística de la interfaz	**reset counters interface** [*type number*]	Ejecute este comando en la vista del usuario.
Cierre de una interfaz	**shutdown**	Ejecutar estos comandos en la vista de la interfaz.
Enciende una interfaz	**undo shutdown**	
Reinicia uan interface	**restart**	

Tabla XII.- Comando de interface

3.2.1 Interface Ethernet

Para configurar la interface Ethernet se utiliza los principales comandos que se muestran paso a paso en esta sección.

Primero se ingresa al modo de configuración de interface para configurar la interface LAN. Se realiza la configuración en la vista del sistema como se observa en la tabla XIII.

Operation	Command
Introduzca a la vista de interfaz Ethernet especificada	**interface ethernet** *number*

Tabla XIII.- Vista de interfaz Ethernet especificada

Luego se configura la dirección IP, en la vista de interfaz Ethernet, utilizando los comandos de la tabla XIV.

Operación	Comando
Asigna una dirección IP a la interfaz	**ip address** *ip-address mask* [**sub**]
Quita la dirección IP de la interfaz	**undo ip address** [*ip-address mask*] [**sub**]

Tabla XIV.- Vista de interfaz Ethernet especificada

A veces, se necesita habilitar bucle local en una interfaz para probar algunas funciones especiales. La siguiente configuración en la vista de interfaz Ethernet, mostrada en la tabla XV, permite en una interfaz habilitar el bucle local.

Operación	Comando
Habilita el Bucle local	**loopback**
Deshabilita el Bucle local	**undo loopback**

Tabla XV.- Bucle local

Para mostrar el estado de una interfaz Ethernet especificada, se configura el comando de la tabla XVI en cualquier vista.

Operación	Comando
Mostrar el estado de una interfaz Ethernet especificada	**display interface** { **ethernet** | **gigabitethernet** } [*interface-number*]

Tabla XVI.- Mostrar el estado de una interfaz Ethernet especificada

3.2.2 Interface Serial

Para configurar la interface Serial se utiliza los principales comandos que se muestran a detalle en esta sección.

Se ingresa al modo de configuración de interface para configurar la interface WAN. Luego en la vista del sistema se configura el comando mostrado en la tabla XVII.

Operation	Command
Introduzca a la vista de interfaz Serial especificada	**interface serial** *number*

Tabla XVII.- Vista de interfaz serial especificada

Se configura la dirección IP, utilizando los comandos que se muestra en tabla XVIII, dentro de la vista de interfaz Serial.

Operación	Comando
Asigna una dirección IP a la interfaz	**ip address** *ip-address mask* [**sub**]
Quita la dirección IP de la interfaz	**undo ip address** [*ip-address mask*] [**sub**]

Tabla XVIII.- Vista de interfaz serial especificada

Para mostrar el estado de una interfaz serial especificado se establece el comando que se observa en la tabla XIX.

Operación	Comando
Mostrar el estado de una interfaz Ethernet especificada	**display interface** { **serial** } [*interface-number*]

Tabla XIX.- Mostrar el estado de una interfaz serial especificado

3.2.3 Interface GigabitEthernet

Para configurar la interface GigabitEthernet se ultiliza los principales comandos detallados en esta sección.

Se ingresa al modo de configuración de interface para configurar la interface LAN. El comando mostrado en la tabla XX se configura en la vista del sistema.

Operation	Command
Introduzca a la vista de interfaz Gigabitethernet especificada	**interface gigabitethernet** *number*

Tabla XX.- Vista de interfaz gigabitethernet especificada

Se configura la dirección IP en la vista de interfaz gigabitethernet, utilizando los comandos que se muestra en tabla XXI.

Operación	Comando
Asigne una dirección IP a la interfaz	**ip address** *ip-address mask* [**sub**]
Quite la dirección IP de la interfaz	**undo ip address** [*ip-address mask*] [**sub**]

Tabla XXI.- Vista de interfaz gigabitethernet especificada

Se ejecuta el comando que se puede observar en la tabla XXII, para mostrar el estado de una interfaz gigabitethernet especificada

Operación	Comando
Mostrar el estado de una interfaz Ethernet especificada	**display interface** { **ethernet** | **gigabitethernet** } [*interface-number*]

Tabla XXII.- Mostrar el estado de una interfaz gigabitethernet especificado

3.3 IMPLEMENTACIÓN DE PROTOCOLOS DE RUTEO

3.3.1 Implementar rutas estáticas

Rutas Estáticas es un tipo especial de ruta configurado manualmente por un administrador. Se puede crear una red de interconexión con la configuración de rutas estáticas. El problema de esta configuración es cuando se produce un fallo en la red, la ruta estática no puede cambiar de forma automática para mantenerse lejos del nodo causando el error, sin la ayuda del administrador.

En una red relativamente sencilla, sólo necesita configurar las rutas estáticas para hacer que el router trabaje normalmente. La configuración adecuada y el uso de rutas estáticas pueden mejorar el rendimiento de la red y garantizar el ancho de banda de aplicaciones importantes.

Una ruta por defecto es una especie de ruta especial, configurada por la ruta estática o algunos protocolos de enrutamiento dinámico, como OSPF.

La configuración de enrutamiento estático incluye:

- Configurar una ruta estática.
- Configurar la ruta por defecto.
- Configurar la prioridad de una ruta estática.
- Eliminar una ruta estática.[12]

Configurando una Ruta Estática:

Se realiza la configuración de la tabla XXIII en la vista del sistema.

Operación	Comando
Agrega una ruta estática	**ip route-static** *ip-address* { *mask* | *mask-length* } [*interface-type interface-number*] [*nexthop-address*] [**preference** *value*] [**reject** | **blackhole**]
Elimina una ruta estática	**undo ip route-static** *ip-address* {*mask* | *mask-length* } [*interface-name*] [*nexthop-address*] [**preference** *value*]

Tabla XXIII.- Configuración de una ruta estática

Configuración de la ruta predeterminada:

Se realiza la configuración de la tabla XXIV en la vista del sistema.

Operation	Command
Configurar la ruta por defecto	**ip route-static** 0.0.0.0 { 0.0.0.0 | 0 } {*interface-type interface-number* | *nexthop-address* } [**preference** *value*] [**tag** *tag-value*] [**description** *string*]
Eliminar la ruta por defecto	**undo ip route-static** 0.0.0.0 { 0.0.0.0 | 0 } {*interface-type interface-number* | *nexthop-address*} [**preference** *value*]

Tabla XXIV.- Configurar la ruta por defecto

Borrar todas las rutas estáticas:

Para borra las rutas estáticas, se configura en la vista del sistema el siguiente comando que observamos en la tabla XXV.

Operacion	Comando
Eliminar todas las rutas estáticas	**delete static all**

Tabla XXV.- Eliminar todas las rutas estáticas

Ejemplo de configuración de enrutamiento estático:

En la siguiente figura 3.5, es necesario configurar las rutas estáticas a fin de lograr el funcionamiento entre dos ordenadores o routers.

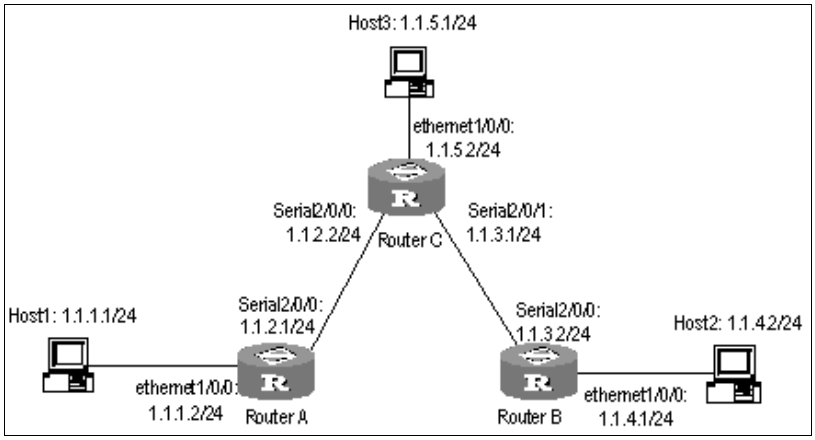


Figura 3.5.- Diagrama de red (rutas estáticas)

Procedimiento de configuración:

 # Configurar la ruta estática para Router A

```
[Router] ip route-static 1.1.3.0 255.255.255.0 1.1.2.2
[Router] ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
[Router] ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
```

O simplemente configurar la ruta por defecto

```
[Router] ip route-static 0.0.0.0 0.0.0.0 1.1.2.2
```

 # Configurar la ruta para Router B

```
[Router] ip route-static 1.1.2.0 255.255.255.0 1.1.3.1
[Router] ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
[Router] ip route-static 1.1.1.0 255.255.255.0 1.1.3.1
```

O simplemente configurar la ruta por defecto

```
[Router] ip route-static 0.0.0.0 0.0.0.0 1.1.3.1
```

 # Configurar la ruta para Router C

```
[Router] ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
[Router] ip route-static 1.1.4.0 255.255.255.0 1.1.3.2
```

Una vez configuradas las PC con sus correspondientes puertas de enlace, los hosts o routers en la Figura 3.5, pueden trabajar conjuntamente.

3.3.2 Implementar el protocolo RIP

Antes de poder configurar RIP, se debe habilitarlo. Sin embargo, esto no es necesariamente el caso cuando se configura características relacionados con la interface. Hay que tener en cuenta que al deshabilitar RIP puede deshabilitar los parámetros relacionados con la interfaz.

Configuración básica de RIP incluye:

- Habilitar RIP.
- Habilitar RIP en un segmento de red.

Habilitación de RIP:

Después de que se habilita RIP, se puede entrar a la vista de RIP.

Para ello se realiza la configuración de la tabla XXVI en la vista del sistema.

Operación	Comando
Habilita RIP e ingresa a la vista RIP	**rip**
Deshabilita RIP	**undo rip**

Tabla XXVI.- Habilitar RIP y entrar en la vista de RIP

Habilitación de RIP en un segmento de red:

Para controlar el funcionamiento flexible RIP, se puede especificar algunas interfaces y configurar la red donde se encuentran las redes RIP, de modo que estas interfaces pueda enviar y recibir paquetes RIP. Para ello en la vista RIP se utilizan los comandos de la tabla XXVII.

Operación	Comando
Habilitar RIP en la red especificada	**network** *network-address*
Deshabilitar RIP en la red especificada	**undo network** *network-address*

Tabla XXVII.- Habilitar red RIP

Configuración de la redistribución de la ruta de RIP:

RIP permite que las rutas de otros protocolos de enrutamiento puedan ser redistribuidos en la tabla de enrutamiento RIP. También permite configurar la métrica por defecto usado para su redistribución.

RIP puede redistribuir estos tipos de rutas: directo, estático, OSPF, BGP, y IS-IS. Para esto se realiza la configuración en la vista RIP, se utiliza los comandos mostrados en la tabla XXVIII.

Operación	Comando
Redistribuir las rutas de otros protocolos	**import-route** *protocol* [**allow-ibgp**] [**cost** *value*] [**route-policy** *route-policy-name*]

Operación	Comando
Cancelar la redistribución de las rutas de otros protocolos	**undo import-route** *protocol*
Configurar el predeterminado costo de enrutamiento	**default cost** *value*
Restaurar el valor predeterminado de costo de enrutamiento	**undo default cost**

Tabla XXVIII.- Configuración de la redistribución de la ruta de RIP

Especifica la versión RIP de una interfaz:

RIP tiene dos versiones, RIP-1 y RIP-2. Se puede especificar la versión de los paquetes RIP procesado por una interfaz, utilice los comandos q se muestran en la tabla XXIX.

Operación	Comando
Especifique la versión de interfaz como RIP-1	**rip version 1**
Especifique la versión de interfaz como RIP-2	**rip version 2** [**broadcast** | **multicast**]
Restaurar el operativo por defecto la versión RIP en una interfaz de	**undo rip version** { **1** | **2** }

Tabla XXIX.- Específica la versión RIP de una interfaz

Especificar el estado de funcionamiento de la interfaz:

En vista de interfaz, se puede especificar el estado de funcionamiento de RIP en la interfaz. Por ejemplo, si RIP es habilitado en la interfaz, es decir, si los paquetes de actualización RIP son enviados y recibidos en la interfaz. También se puede especificar por separado una interfaz para enviar (o recibir) paquete de actualización RIP.

Se realiza, en la vista de la interfaz, la siguiente configuración mostrada en la tabla XXX, según el estado de funcionamiento que se desee llevar a cabo. [6]

Operación	Comando
Habilitar RIP en una interfaz	**rip work**
Deshabilitar RIP en una interfaz	**undo rip work**
Habilitar una interfaz para recibir paquetes de actualización RIP	**rip input**
Desactivar una interfaz para recibir paquetes de actualización RIP	**undo rip input**
Habilitar una interfaz para enviar paquetes de actualización RIP	**rip output**
Desactivar una interfaz para enviar paquetes de actualización RIP	**undo rip output**

Tabla XXX.- Específica el estado de funcionamiento de la interfaz

Ejemplo de configuración de RIP:

Una intranet es conectado a Internet a través de Router A. Los host de la intranet están conectados directamente a Router B o Router C, como se muestra en la figura 3.6.

Habilitar RIP en estos tres routers y configurar de la siguiente manera:

- Router A pueden recibe la información de enrutamiento de redes externas, pero no se puede anunciar la información de enrutamiento de la intranet a las redes externas.
- Routers A, B y C pueden intercambiar información RIP entre ellos para permitir que los host en la intranet puedan acceder a Internet.[6]

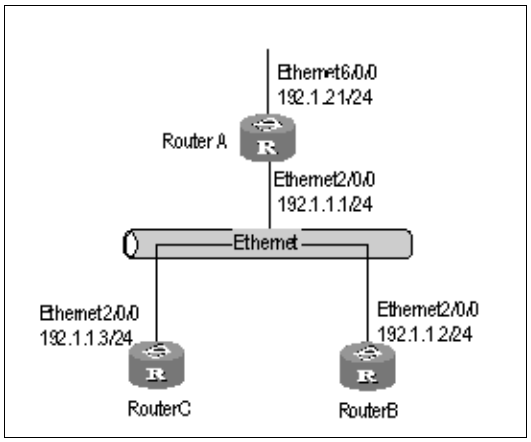


Figura 3.6.- Diagrama de red (RIP)

Procedimiento de configuración:

 # Configurar Router A

 # Configurar las interface Ethernet 2/0/0 y Ethernet 6/0/0.

```
[Router] interface ethernet 2/0/0
[Router-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[Router-Ethernet2/0/0] quit
[Router] interface ethernet 6/0/0
[Router-Ethernet6/0/0] ip address 192.1.2.1 255.255.255.0
```

 # Configuración de RIP, y configurar Ethernet 2/0/0 y Ethernet 6/0/0 para ejecutar RIP.

```
[Router] rip
[Router-rip] network 192.1.1.0
[Router-rip] network 192.1.2.0
```

 # Configure el interfaz Ethernet 6/0/0 del Router para recibir paquetes RIP solamente.

```
[Router] interface ethernet 6/0/0
[Router-Ethernet6/0/0] undo rip output
[Router-Ethernet6/0/0] rip input
```

 # Configurar Router B

 # Configurar el interfaz Ethernet 2/0/0.

```
[Router] interface Ethernet 2/0/0
[Router-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
```

 # Configuración de RIP, y configurar Ethernet 2/0/0 para ejecutar RIP.

```
[Router] rip
[Router-rip] network 192.1.1.0
[Router-rip] import direct
```

 # Configurar Router C

 # Configure el interfaz Ethernet 2/0/0.

```
[Router] interface Ethernet 2/0/0
[Router-Ethernet2/0/0] ip address 192.1.1.3 255.255.255.0
```

 # Configuración de RIP, y configurar Ethernet 2/0/0 para ejecutar RIP.

```
[Router] rip
[Router-rip] network 192.1.1.0
[Router-rip] import direct
```

3.3.3 Implementar el protocolo OSPF

Entre todas las tareas de configuración, sólo después de habilitar OSPF, el número de la interfaz y el área de número, otras funciones pueden ser configuradas. Sin embargo, la configuración de las funciones relacionadas con la interfaz no está restringida por si el OSPF está habilitado o no.

Configuración básica de OSPF

- Configurar Router ID
- Habilitar el proceso de OSPF
- Introduzca vista área OSPF
- Especifique el segmento de la red.

Configurando Router ID:

Router ID es un entero de 32 bits sin signo que identifica un router dentro de un AS. Router ID se puede configurar manualmente. Si el ID de router no está configurado, el sistema seleccionará automáticamente la más pequeña de las direcciones IP de las interfaces actuales, como el ID de router. Cuando se realice manualmente, debe garantizar que los identificadores de cualquiera de los dos routers en el sistema autónomo son únicos. Una práctica común para establecer el router ID es la dirección IP de una interfaz en el router Con el comando mostrado en la tabla XXXI podemos configurar el router ID. [7]

Operación	Comando
Configurar un router ID	**router id** *router-id*
Remover un router ID	**undo router id**

Tabla XXXI.- Configuración del router ID

Proceso de Habilitación de OSPF:

OSPF soporta múltiples-proceso. Cuando varios procesos están habilitados en un router, es necesario especificar un número diferente para ellos.

El número de proceso OSPF es un concepto local, sin ningún efecto sobre su intercambio de paquetes con otros routers. Por lo tanto, aunque el número de proceso de diferentes routers es diferente, el intercambio de paquetes está disponible.

Se realiza la configuración de la tabla XXXII en la vista del sistema.

Operación	Comando
Habilitar OSPF e ingresa a vista OSPF	**ospf** [*process-id* [[**router-id** *router-id*] **vpn-instance** *vpn-instance-name*]]
Deshabilitar proceso de protocolo de enrutamiento OSPF	**undo ospf** [*process-id*]

Tabla XXXII.- Activar / desactivar OSPF

Entrando en la vista de área OSPF:

OSPF divide un sistema autónomo en áreas más pequeñas y asigna a los routers a diferentes grupos lógicamente.

Se realiza la siguiente configuración de la tabla XXXIII, en la vista de OSPF.

Operation	Command
Entrar en la vista de área OSPF	**area** *area-id*
Eliminar un área OSPF designados	**undo area** *area-id*

Tabla XXXIII.- Entrar en la vista de área OSPF

Especificación de un segmento de red para ejecutar OSPF

Después de habilitar OSPF en vista de sistema, se debe especificar en qué segmento de la red OSPF debe ser aplicado. Para ello en la vista área OSPF se ejecuta el comando de la tabla XXXIV.

Operación	Comando
Especifique un segmento de red para ejecute OSPF	**network** *ip-address wildcard-mask*
Deshabilitar OSPF en el segmento de red.	**undo network** *ip-address wildcard-mask*

Tabla XXXIV.- Entrar en la vista de área OSPF

Configurar el costo de envío de paquetes en una interfaz:

Puede configurar el costo de envío de paquetes en las interfaces para interferir en el cálculo de la ruta.

Se realiza la configuración en la vista de la interfaz, tal como se observa en la tabla XXXV.

Operación	Comando
Configurar el costo de envío de paquetes en una interfaz	**ospf cost** *value*
Restaurar el coste por defecto para la transmisión de paquetes de la interfaz	**undo ospf cost**

Tabla XXXV.- Entrar en la vista de área OSPF

Reinicio de un proceso de OSPF

Si el comando **undo ospf** se ejecuta en un router y después el comando **ospf** se utiliza para reiniciar un proceso de OSPF, la configuración de OSPF anterior se perderá.

Con el comando **reset ospf all**, se puede restablecer el proceso de OSPF, sin perder la configuración de OSPF anterior. Este comando se muestra en la tabla XXXVI.

Operación	Comando
Reiniciar un proceso OSPF	**reset ospf** [**statistics**] { **all** | *process-id* }

Tabla XXXVI.- Reiniciar un proceso OSPF

Ejemplo de configuración de OSPF:

Router A y Router B están conectados por interfaces seriales, y Router B Router C están conectados por interfaces Ethernet.

Router A pertenece a área 0, Router C pertenece a area1, y Router B pertenece a las dos área 0 y área 1, tal como podemos ver en la figura 3.7. [8]

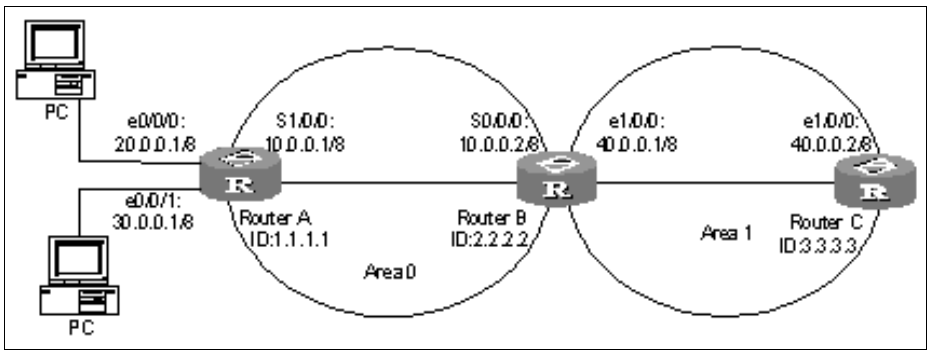


Figura 3.7.- Diagrama de red (OSPF)

Procedimiento de configuración:

 # Configurar Router A

```
<Router> system-view
[Router] router id 1.1.1.1
[Router] interface serial1/0/0
[Router-serial1/0/0] ip address 10.0.0.1 255.0.0.0
[Router-serial1/0/0] interface ethernet0/0/0
[Router-ethernet 0/0/0] ip address 20.0.0.1 255.0.0.0
[Router- ethernet 0/0/0] interface ethernet0/0/1
[Router- ethernet 0/0/1] ip address 30.0.0.1 255.0.0.0
[Router- ethernet 0/0/1] quit
[Router] ospf
[Router-ospf-1] area 0
[Router-ospf-1-area-0.0.0.0] network 10.0.0.1
0.255.255.255
[Router-ospf-1 -area-0.0.0.0] network 20.0.0.1
0.255.255.255
[Router-ospf-1 -area-0.0.0.0] network 30.0.0.1
0.255.255.255
```

 # Configurar Router B

```
<Router> system-view
[Router] router id 2.2.2.2
[Router] internet serial0/0/0
[Router-serial0/0/0] ip address 10.0.0.2 255.0.0.0
[Router-serial0/0/0] Interface ethernet 1/0/0
[Router-ethernet 1/0/0] ip address 40.0.0.1 255.0.0.0
[Router-ethernet 1/0/0] quit
```

```
[Router] ospf
[Router-ospf-1] area 0
[Router-ospf-1-area-0.0.0.0] network 10.0.0.2
0.255.255.255
[Router-ospf-1-area-0.0.0.0] area 1
[Router-ospf-1-area-0.0.0.1] network 40.0.0.1
0.255.255.255
```

 # Configurar Router C

```
<Router> system-view
[Router] router id 3.3.3.3
[Router] interface ethernet 1/0/0
[Router-ethernet 1/0/0] ip address 40.0.0.2 255.0.0.0
[Router-ethernet 1/0/0] quit
[Router] ospf
[Router-ospf-1] area 1
[Router-ospf-1-area-0.0.0.1] network 40.0.0.2
0.255.255.255
```

3.4 TROUBLESHOOTING Y MONITOREO DE LA RED

3.4.1 Respaldo TFTP

TFTP (Trivial File Transfer Protocol) es un tipo de protocolo simple de transferencia de archivos.

En comparación con otro protocolo de transferencia de archivos FTP, TFTP no tiene una interfaz compleja de acceso interactivo y control de autenticación, que es aplicable en el entorno en el que no se requiere una compleja interacción entre el cliente y el servidor. Por ejemplo, el protocolo TFTP se utiliza para obtener el espejo de la memoria del sistema cuando se inicie el sistema. En general, el protocolo TFTP se realiza basado en UDP.

En TFTP, la transferencia de archivos es originado por el cliente. Cuando es necesario para descargar archivos, al final el cliente enviará un paquete de petición de lectura para el servidor TFTP, se recibe el paquete respuesta del servidor, y se enviar la contestación de recibo al servidor.

Cuando sea necesario cargar archivos, el cliente enviará por escrito paquete de solicitud al servidor de TFTP y luego envía paquetes al servidor y recibe la confirmación desde el servidor. El router funciona como cliente y servidor TFTP.

Uso de TFTP para descargar archivos:

Los comandos de la tabla XXXVII permiten la descarga de archivos mediante TFTP, esto se realiza en la vista del usuario

Operación	Comando
Uso TFTP para descargar archivos	**tftp** *host* **get** *source-filename* [*destination-filename*]
Descarga de archivos en el modo seguro.	**tftp** *host* **sget** *source-filename* [*destination-filename*]

Tabla XXXVII.- Uso TFTP para descargar archivos

Uso de TFTP para cargar archivos:

En la tabla XXXVIII se muestra la descripción del comando para cargar archivos usando TFTP.

Operation	Command
Uso TFTP para cargar archivos	**tftp** *X.X.X.X* **put** *source-filename* [*destination-filename*]

Tabla XXXVIII.- Uso TFTP para cargar archivos

Ejemplo de respaldo TFTP:

El router trabaja como TFTP cliente y está configurado de acuerdo al diagrama de topología que se muestra en la figura 3.8 [14]

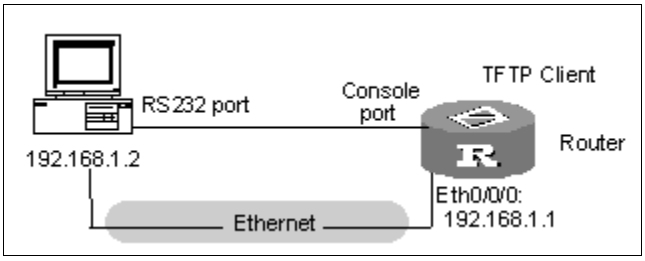


Figura 3.8.- Diagrama de red (respaldo TFTP)

Una vez configuradas las interfaces se procede a copiar un archivo que se encuentra en la PC, para ello se necesita ejecutar el programa Dlink TFTP Server, que es comúnmente utilizado para cargar y / o descargar configuraciones de routers, switches, hubs, etc., también se puede utilizar otro programa que nos permita ejecutar la PC como servidor TFTP (este programa se adjuntará en el cd anexo del manual de prácticas). En la figura 3.9 se muestra la imagen del programa D-Link TFTP Server utilizado para la trasferencia TFTP.

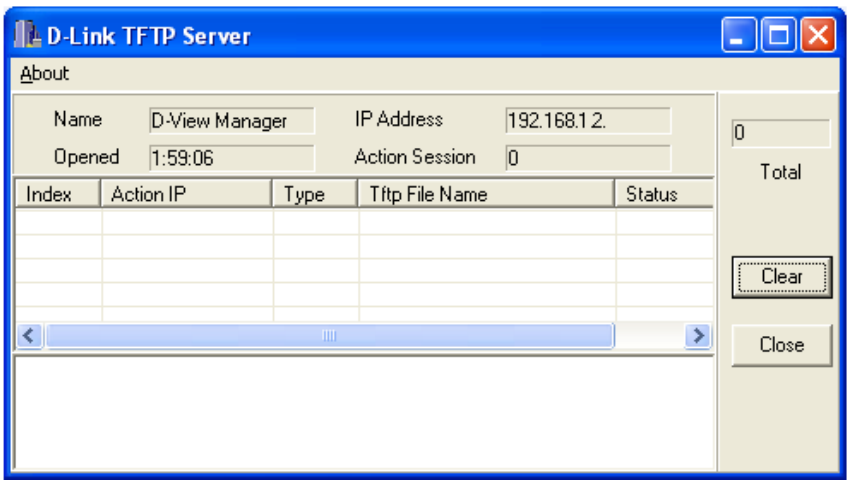


Figura 3.9.- D-Link TFTP Server en PC

Ahora bien, desde el promp en el router se ejecuta lo siguiente, tal como vemos en la figura 3.10.

```
<router_1>ftp 192.168.1.2 get C:/config

 % Wrong parameter found at '^' position.
<router_1>tftp 192.168.1.2 get C:/config
  File will be transferred in binary mode.
  Downloading file from remote tftp server, please wait.....
  TFTP:     1470 bytes received in 0 second(s).
  File downloaded successfully.

<router_1>dir
Directory of flash:/

   1   -rw-  11941732  Apr 01 2003 12:47:58   main.bin
   2   drw-         -  Jun 26 2009 00:51:05   practicas
   3   -rw-      1470  Oct 15 2009 16:31:52   config.cfg

31877 KB total (20196 KB free)

<router_1>
```

Figura 3.10.- Copia de archivo al router

Como vemos se ha logrado transferir un archivo desde la PC hacia el router con la ayuda del programa antes mencionado (D-link Server).

3.4.2 Utilerías de monitoreo: Display, Debugs, Telnet

La tabla XXXIX muestra los diferentes comandos que nos permiten ver el estado y cierta información de interfaces.

operación	Comando	Observación
Muestra el estado del funcionamiento actual y las estadísticas de una interfaz	**display interface** [*type number*]	Estos comandos se pueden ejecutar en cualquier vista.
Muestra la información breve sobre determinada o todas las interfaces	**display brief interface** [*type* [*number*]] [| { **begin** | **include** | **exclude**} *text*]	
Muestra la información principal de configuración de una interfaz	**display ip interface** [*type number*]	
Muestra el estado de una interfaz	**display status interface** *interface-type interface-number*	
Habilitar el tipo específico de depuración de una interfaz.	**debugging physical** { **all** | **error** | **event** | **packet** } [**interface** *interface-type interface-number*]	Ejecutar estos dos comandos en la vista del usuario.
Deshabilitar el tipo específico de depuración de una interfaz.	**undo debugging physical** { **all** | **error** | **event** | **packet** } **interface** *interface-type interface-number*	

Tabla XXXIX.- Mostrar detalles de interfaces

Problemas de rutas estáticas

El router no está configurado con el protocolo de enrutamiento dinámico. Tanto el estado físico de la interfaz y el protocolo de capa de

enlace se encuentran en estado de UP, pero el paquete IP no pueden ser remitidos normalmente.

Resolución de problemas:

- Usar el comando **`display ip routing-table protocol static`** para ver si la ruta estática correspondiente está correctamente configurado.
- Usar el comando **`display ip routing-table`** para ver si la ruta es válida.
- Ver si la siguiente dirección de salto no se especifica o está mal especificada en la interfaz.

La tabla XL nos muestra los distintos comandos de **`display`** que se utiliza para poder observar los detalles de la tabla de ruta. [12]

Operación	Comando
Ver resumen de la tabla de enrutamiento	**display ip routing-table**
Ver los detalles de la tabla de enrutamiento	**display ip routing-table verbose**
Ver la ruta de un destino específico de direcciones	**display ip routing-table** *ip-address* [*mask*] [**longer-match**] [**verbose**]
Ver las rutas dentro del rango especificado de direcciones de destino	**display ip routing-table** *ip-address1 mask1 ip-address2 mask2* [**verbose**]
Ver las rutas por filtrado de lista de direcciones IP especificado de prefijo	**display ip routing-table ip-prefix** *ip-prefix-number* [**verbose**]
Ver las rutas descubiertas por el protocolo especificado	**display ip routing-table protocol** *protocol* [**inactive** | **verbose**| **vpn-instance** *vpn-instance-name*]
Ver el árbol de la tabla de rutas	**display ip routing-table radix**

Operación	Comando
Ver las estadísticas en una tabla de enrutamiento	**display ip routing-table** [**vpn-instance** *vpn-instance-name*] **statistics**
Ver los detalles de la tabla de enrutamiento	**display ip routing-table vpn-instance** *vpn-instance-name* [*ip-address*] **verbose**
Borrar la tabla de enrutamiento	**reset ip routing-table** [**vpn-instance** *vpn-instance-name*] **statistics protocol** *protocol-type*

Tabla XL: Mostrar detalles de tabla de enrutamiento

Problemas de RIP

El paquete de actualización no se puede recibir cuando la conexión física es normal.

Resolución de problemas:

Puede ser causado por lo siguiente:

- RIP no está habilitado en la interfaz correspondiente (por ejemplo, el comando **`undo rip work`** se ejecuta) o de esta interfaz no está habilitada a través del comando **`network.`**

La tabla XLI nos muestra los distintos comandos que se utiliza para poder observar los detalles en el protocolo RIP. [6]

Operación	Comando
Muestra el funcionamiento del estado actual RIP y la configuración de la información	**display rip**
Muestra información sobre RIP interfaces.	**display rip interface** [**vpn-instance** *vpn-instance-name*]
Mostrar la tabla de enrutamiento RIP	**display rip routing** [**vpn-instance** *vpn-instance-name*]
Habilitar la depuración de paquetes de RIP.	**debugging rip packets** [**interface** *type number*]
Deshabilitar la depuración de paquetes de RIP	**undo debugging rip packets**
Habilitar la recepción de paquetes de depuración de RIP	**debugging rip receive**
Deshabilitar la depuración de recibir el paquete de RIP	**undo debugging rip receive**
Habilitar el envío de paquetes de depuración de RIP	**debugging rip send**
Desactivar el envío de paquetes de depuración de RIP	**undo debugging rip send**

Tabla XLI.- Vista y depuración RIP

Problemas de OSPF:

OSPF se configura de acuerdo a los procedimientos anteriores, pero el OSPF no puede funcionar normalmente.

Resolución de problemas:

Consulte paso a paso los siguientes procedimientos:

- En primer lugar, comprobar si el protocolo entre dos routers conectados directamente en el funcionamiento normal.

- Ejecutar **`display ospf peer`** para ver la información acerca de pares de OSPF.
- Ejecutar el comando **`display ospf interface`** para ver la información de OSPF en la interfaz.
- Comprobar si las conexiones físicas y de los protocolos de nivel inferior funcionar normalmente. Ejecutar comando **`ping`** para probar. Si el router local no puede llegar el router remoto, indica que las conexiones físicas y de los protocolos de nivel inferior no pueden funcionar normalmente.
- Si las conexiones físicas y de los protocolos de nivel inferior son normales, comprobar los parámetros OSPF configurados en la interfaz, pero debe garantizar la coherencia de los parámetros de su router adyacentes. Los identificadores de área debe ser el mismo, y los segmentos de la red y las máscaras también debe ser coherente.
- Si un área está definida como el área de rutas, entonces el área se debe establecer en el cabo de todos los routers conectados a esta área.
- Los tipos de interfaz de dos routers adyacentes deben ser coherentes.
- Si más de dos zonas están configuradas, entonces por lo menos un área debe ser configurada como el área de red troncal (es decir, el área de identificación es 0).
- Asegurar el área de red troncal se conecta con todas las otras áreas.

La tabla XLII nos muestra los distintos comandos que se utiliza para poder observar los detalles en el protocolo OSPF. [7]

Operación	Comando
Mostrar la breve información del proceso de enrutamiento OSPF	**display ospf** [*process-id*] **brief**
Mostrar las estadísticas de OSPF	**display ospf** [*process-id*] **cumulative**
Muestra información de vecinos OSPF	**display ospf** [*process-id*] **peer** [**brief**]
Mostrar siguiente salto información OSPF	**display ospf** [*process-id*] **nexthop**
Mostrar la tabla de enrutamiento OSPF	**display ospf** [*process-id*] **routing**
Muestra la información de interfaz OSPF	**display ospf** [*process-id*] **interface** [*interface-type interface-number*]
Mostrar los errores OSPF	**display ospf** [*process-id*] **error**
Mostrar el proceso de depuración de OSPF	**display debugging ospf**
Habilitar la depuración de paquetes OSPF	**debugging ospf packet** [**ack** | **dd** | **hello** | **interface** *type num* | **request** I **update**]
Deshabilitar la depuración de paquetes OSPF	**undo debugging ospf packet** [**ack** | **dd** | **hello** | **interface** *type num* | **request** I **update**]

Tabla XLII.- Vista y depuración OSPF

Telnet Servicios de Terminal

El protocolo Telnet pertenece al protocolo de capa de aplicación en los protocolos TCP / IP, que proporciona la función de inicio de sesión remoto y de la terminal virtual a través de la red.

Los servicios de Telnet proporcionada por el sistema son:

- El servidor Telnet

  Los servicios del servidor Telnet como se muestra en la figura 3.11.

  El usuario puede ejecutar el programa cliente de Telnet en un equipo para iniciar sesión en el router para la configuración y gestión.

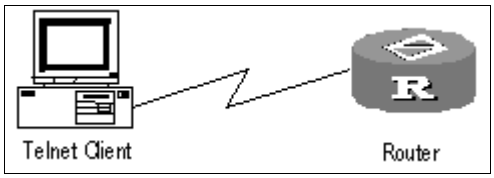


Figura 3.11.- Servicios de servidor Telnet

- Cliente Telnet

  Los servicios de cliente Telnet como se muestra en la figura 3.12.

  Después de configurar la conexión al router mediante la ejecución del programa de emulación de terminal o el programa de Telnet en el equipo, el usuario ingresa el comando **`telnet`** para acceder a otros routers de configuración y administración. [13]

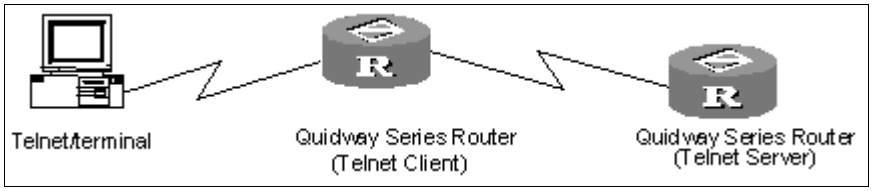


Figura 3.12.- Servicios de cliente Telnet

Establecer una conexión Telnet

Se realiza la siguiente configuración de la tabla XLIII en la vista del usuario.

Operación	Comando
Telnet a otro router para la gestión	**telnet** [**vpn-instance** *vpn-instance-name*] *host-ip-address* [*service-port*]

Tabla XLIII.- Establecer una conexión Telnet

Por ejemplo, una PC es conectada al puerto de consola en el router1. A continuación, puede utilizar el siguiente comando telnet al router router2 en 129.102.0.1.

```
<Router1> telnet 129.102.0.1
Trying  129.102.0.1 ...
Connected to 129.102.0.1 ...
<Router2>
```

Capítulo 4

4. Prácticas de configuración de los equipos Quidway AR 28-30

En este ultimo capitulo se explica de manera general cada una de las practicas que se han implementado para su estudio y desarrollo dentro de las actividades de laboratorio.

Se describe cada uno de los puntos que se lleva a cabo en la respectiva práctica, es decir, una breve descripción de lo que se ha configurado para la realización de dicha práctica.

4.1 CONFIGURACIÓN BÁSICA

En la práctica #1 denominada “Configuración básica del router” se establece la configuración básica para la utilización y familiarización de los routers Quidway Ar 28 – 30.

Inicialmente se expone sobre cómo se debe conectar el router mediante el terminal de consola, así como los pasos necesarios para realizar una buena conexión.

Una vez que se establece la correcta conexión del router, se explica los distintos modos de vista que el router nos provee para la configuración del mismo.

Ya que se ha familiarizado con los modos de vista del router, se enfoca en la configuración básica propiamente dicha, para ello se muestra como borrar la configuración existente para así poder configurar todo desde inicio.

Se indica cómo establecer el nombre del router la hora y el mensaje de inicio. Se realiza la conexión de la topología propuesta y se procede a explicar cómo realizar la configuración de cada una de las interfaces y medios de interconexión entre los dispositivos utilizados.

Una vez realizado todo lo antes expuesto, se expone como verificar que cada una de las conexiones esté establecida correctamente mediante el uso de comandos de verificación como son display y ping.

4.2 CONFIGURACIÓN DE RUTAS ESTÁTICAS

En la práctica # 2 denominada “Configuración de rutas estáticas” se enfoca en la configuración de rutas estáticas, para ello se establece una topología de red sencilla pero que se acoge a la necesidad didáctica.

Se procede a establecer la conexión de los dispositivos de red. Luego se procede a hacer el borrado de la configuración existente en cada routers, así como también mostrar cómo establecer un archivo predeterminado tanto para cargar como para guardar la configuración en el router.

Se realiza la configuración básica como es nombre del router, mensaje de inicio y hora. Una vez realizado esto se configurar cada una de las interfaces según el diagrama y tabla de direccionamiento.

Se configura las interface Ethernet, Serial y la interface Gigabitethernet según sea necesario y según el requerimiento en la topología.

Así mismo se configura las PC para la red LAN en cada router.

Finalmente se comprueba que todas las conexiones y la comunicación entre todos los dispositivos que interactúan en la red sean satisfactorias, para ello se utiliza comandos que nos proveen esa información.

4.3 CONFIGURACIÓN DE RIPV1

El objetivo de la práctica # 3 denominada “Configuración de RIP verison1“, es aprender a configurar RIP. Se establece una topología de red sencilla pero que se adapta a las necesidades didácticas.

De igual manera que en la práctica anterior se procede a conectar cada uno de los dispositivos de acuerdo a la topología establecida .Se realiza el borrado de la configuración existente en cada routers, así como también mostrar cómo establecer un archivo predeterminado tanto para cargar como para guardar la configuración en el router.

Se establece el nombre de los routers así como su mensaje de inicio y la hora. Luego de esto de acuerdo al diagrama de red y a la tabla de direcciones IP correspondiente se configura cada una de las interfaces que se utilizaran en los respectivos routers.

Una vez configuradas las interfaces, el siguiente objetivo es habilitar el protocolo RIP en cada routers así como definir cada segmento de red para este tipo de protocolo.

Finalmente como en todas las anteriores prácticas, se verifica que cada conexión sea satisfactoria así como también que el protocolo RIP este habilitado e intercomunicando a la red.

4.4 REDISTRIBUCIÓN DE RUTAS EN RIP

La práctica #4 denominada “Redistribución de rutas dentro de RIP” se enfoca en un caso muy particular en RIP, lo que se lo refiere con el nombre de redistribución de rutas.

Se establece la conexión de los respectivos dispositivos de red. De la misma forma que en las prácticas anteriores se borra la configuración inicial y se procede con la configuración básica de cada router, es decir, nombre, mensaje de inicio y hora.

Básicamente la topología de red es similar a la que se configuro para RIP, con la única variante en sus direcciones de red.

El objetivo de esta práctica es de mostrar cómo hacer que por medio de RIP se puede redistribuir una ruta, al redistribuir la ruta estática por defecto se logra que el resto de routers sepan también donde enviar los paquetes que no estén destinados a su red.

Se muestra que la redistribución se lleve a cabo al verificar la tabla de rutas correspondiente en cada uno los routers utilizados en la topología expuesta.

4.5 CONFIGURACIÓN DE RIPV2

En la práctica # 5 denominada “Configuración de RIP versión 2” se ha establecido una topología de red sencilla.

Se borra la configuración inicial y se procede a la configuración básica de cada router, es decir, nombre, mensaje de inicio y hora.

Según en el diagrama de red y la tabla de direcciones IP correspondiente, se configura cada una de las interfaces que se utilizaran en los respectivos routers.

Una vez que se configura las interfaces se habilita en cada una de ellas el protocolo RIP V2, y luego en cada router se define cada segmento de red para este tipo de protocolo.

Finalmente se procede a verificar que cada conexión sea satisfactoria así como también que el protocolo RIPV2 este habilitado e intercomunicando a la red establecida.

4.6 CONFIGURACIÓN DE OSPF

En la práctica #6 denominada “Configuración OSPF”, se la establece sobre una red de topología, la cual al igual que las prácticas anteriores está conformada por tres routers a los cuales están conectados una PC respectiva

De la misma forma que se ha hecho en las prácticas anteriores, se borra la configuración inicial y se procede con la configuración básica de cada router, es decir, nombre, mensaje de inicio y hora.

Se establece la configuración de las interfaces que utilizan cada routers así como también se configura las direcciones correspondientes a los host en cada PC.

Luego de esto se procede a establecer el protocolo de enrutamiento así como el área y la asignación de los segmentos de red a este protocolo.

Además se muestra como definir un ID en el router, así como establecer el costo y el ancho de banda en una interfaz

Finalmente se verifica la interface y protocolo de enrutamiento para la comprobar satisfactoriamente la comunicación entre cada uno de los dispositivos utilizados.

4.7 CONFIGURACIÓN DE SEGURIDAD ACCESO (SSH)

La practica # 7 denominada “Configuración de seguridad de acceso” , es una de las prácticas en que su topología de red se basa en la conexión de un router a una PC.

Se muestra como borrar la configuración establecida, así como también como establecer un archivo predeterminado tanto para cargar como para guardar la configuración en el router.

Luego se establece la configuración básica como nombre, hora y mensaje de inicio.

Se establece como se configura la interface, en este caso solo la interfaz Ethernet así como también se establece la dirección del host.

Se define como establecer la configuración ssh servidor así como ssh cliente y la utilización de un software para dicha comunicación.

Se verifica mediante el comando de visualización para ver el estado de la interfaz y la conectividad entre router y PC.

4.8 CONFIGURACIÓN PARA UNA RED WAN UTILIZANDO EQUIPOS SDH Y ROUTERS HUAWEI.

Esta práctica # 8 denominada “Configuración para una red WAN utilizando equipos SDH y routers HUAWEI” se incluye a parte de los routers, otros equipos de conexión para redes WAN.

La topología de red que se estable está conformada por cuatros routers con las cuatros PCs respectivas y los tres equipos de conexión WAN los OSN Optix 1500 B. Se establece la conexión de cada dispositivo de acuerdo a lo establecido en la topología. Se establece el borrado de cada uno de los routers a utilizarse.

Una vez que se han borrado la configuración de los routers, se procede con la configuración básica, luego se establece la configuración de cada una de las interfaces y de las respectivas PCs conectadas a cada router.

Se explica además como configurar los equipos OSN para poder establecer la conexión entre los dispositivos. Luego de esto se realiza la configuración de un tipo de enrutamiento, en este caso mostramos dos configuraciones antes establecidas, rutas estáticas y el protocolo RIPV1.

Finalmente se verifica que todos los dispositivos interactúen entre sí, mediante la verificación por medio de los comandos necesarios.

Conclusiones y Recomendaciones

Conclusiones:

1. El presente estudio se desarrolló en el campo de routers HUAWEI. Este proyecto sirve como introducción a los conceptos y da un acercamiento o familiarización a estos dispositivos.

2. Los routers HUAWEI destacan por su facilidad de configuración. Esta facilidad de configuración los convierte en una buena herramienta para la docencia. Es la falta de conocimiento o no familiarización lo que dificulta el entendimiento y configuración de los mismos, para ello se ha implementado las prácticas.

3. Otra característica que ha sido descrita y que es de suma importancia de los protocolos de enrutamiento, es si deben enrutar dentro o fuera de la subred donde se encuentran.

4. Los protocolos de enrutamiento internos se utilizan para actualizar routers bajo el control de un sistema autónomo; mientras que los exteriores se emplean para permitir que dos redes con distintos sistemas autónomos se comuniquen; el ejemplo más actual es el de Internet: OSPF para ruteo interno, BGP para externo.

5. No se intenta profundizar en aspectos que si bien son importantes, representa un estudio en demasía extenso y en todo caso es mejor referirse a los documentos originales para conocer estos aspectos con mejor detalle; ejemplo de estos aspectos no tomados muy en cuenta es uno de los protocolos para sistemas autónomos externos como es BGP.

Recomendaciones:

1. El estudio de los protocolos de la capa de red está en permanente evolución, siendo un tema de gran interés y expectativa de futuros desarrollos teniendo presente la continua evolución de las redes de comunicaciones de datos, cada vez sometidas a mayores requerimientos en cuanto a sus prestaciones, las que están directamente relacionadas con el desempeño de los protocolos de red. Sólo dependerá de qué recurso o criterio se elija como prioritario para el envío de los paquetes de datos.

2. Muchas instituciones mantienen estructuras de comunicaciones complejas, debido a la necesidad de mantenerse comunicados; por lo que deben precisar una buena administración de red que permita un mejor manejo y control de los elementos que la conforman.

3. Es necesario conocer en profundidad los dispositivos para poder comprender lo que sucede con los mismos y como se pueden configurar adecuadamente.

4. La administración de red debe proporcionar herramientas automatizadas y manuales de administración al usuario de red, para que éste pueda detectar posibles fallas o degradaciones en el

desempeño de la misma. Así le permitirá contar con estrategias de administración para optimizar la infraestructura existente y mejorar el rendimiento de aplicaciones y servicios.

Anexos

Anexo A:

Se adjuntara en formato digital cada una de las prácticas mencionadas en el capítulo 4, completamente desarrolladas, tanto la versión instructor como la versión estudiante a fin de que se cumpla con el objetivo de ser utilizadas para fines académicos. Además de unos programas utilizados en las practicas mencionadas como son D-link server y el Putty 0.60.

Anexo B:

Para todo aquel que tiene problemas para subnetear puede tomar el siguiente gráfico como guía.

Dicho cuadro contiene las máscaras de subred de tamaño variable (variable length subnet mask, VLSM) contiene ejemplos de varias subredes soportando diferente cantidad de host y sus octetos correspondientes.

Class C Subnet Table	/24 .0 (00000000) 0 subnets/254 hosts	/25 .128 (10000000) 0 subnet 126 hosts	/26 .192 (11000000) 2 subnets 62 hosts	/27 .224 (11100000) 6 subnets 30 hosts	/28 .240 (11110000) 14 subnets14 hosts	/29 .248 (11111000) 30 subnets 6 hosts	/30 .252 (11111100) 62 subnets 2 hosts
.0	.0	.0	.0	.0	.0	.0	.0 (.1 -.2)
.4						(.1 - .6)	.4 (.5 - .6)
.8					(.1 - .14)	.8	.8 (.9 - .10)
.12				(.1 - .30)		(.9 - .14)	.12 (.13 - .14)
.16					.16	.16	.16 (.17 - .18)
.20						(.17 - .22)	.20 (.21 - .22)
.24					(.17 - .30)	.24	.24 (.25 - .26)
.28			(.1 - .62)			(.25 - .30)	.28 (.29 - .30)
.32				.32	.32	.32	.32 (.33 - .34)
.36						(.33 - .38)	.36 (.37 - .38)
.40					(.33 - .46)	.40	.40 (.41 - .42)
.44				(.33 - .62)		(.41 - .46)	.44 (.45 - .46)
.48					.48	.48	.48 (.49 - .50)
.52						(.49 - .54)	.52 (.53 - .54)
.56					(.49 - .62)	.56	.56 (.57 - .58)
.60		(.1 - .126)				(.57 - .62)	.60 (.61 - .62)
.64			.64	.64	.64	.64	.64 (.65 - .66)
.68						(.65 - .70)	.68 (.69 - .70)
.72					(.65 - .78)	.72	.72 (.73 - .74)
.76				(.65 - .94)		(.73 - .78)	.76 (.77 - .78)
.80					.80	.80	.80 (.81 - .82)
.84						(.81 - .86)	.84 (.85 - .86)
.88					(.81 - .94)	.88	.88 (.89 - .90)
.92			(.65 - .126)			(.89 - .94)	.92 (.93 - .94)
.96				.96	.96	.96	.96 (.97 - .98)
.100						(.97 - .102)	.100 (.101 - .102)
.104					(.97 - .108)	.104	.104 (.105 - .106)
.108				(.97 - .126)		(.105 - .108)	.108 (.107 - .108)
.112					.112	.112	.112 (.113 - .114)
.116						(.113 - .118)	.116 (.117 - .118)
.120					(.113 - .126)	.120	.120 (.121 - .122)
.124						(.121 - .126)	.124 (.125 - .126)
.128	(.1 - .254)	.128	.128	.128	.128	.128	.128 (.129 - .130)
.132						(.129 - .130)	.132 (.133 - .134)
.136					(.129 - .142)	.136	.136 (.137 - .138)
.140				(.129 - .158)		(.137 - .142)	.140 (.141 - .142)
.144					.144	.144	.144 (.145 - .146)
.148						(.145 - .150)	.148 (.149 - .150)
.152					(.145 - .158)	.152	.152 (.153 - .154)
.156			(.129 - .191)			(.153 - .158)	.156 (.157 - .158)
.160				.160	.160	.160	.160 (.161 - .162)
.164						(.161 - .166)	.164 (.165 - .166)
.168					(.161 - .174)	.168	.168 (.169 - .170)
.172				(.161 - .190)		(.169 - .174)	.172 (.173 - .174)
.176					.176	.176	.176 (.177 - .178)
.180						(.177 - .182)	.180 (.181 - .182)
.184					(.177 - .190)	.184	.184 (.185 - .186)
.188						(.185 - .190)	.188 (.189 - .190)
.192		(.129 - .254)	.192	.192	.192	.192	.192 (.193 - .194)
.196						(.193 - .198)	.196 (.197 - .198)
.200					(.193 - .206)	.200	.200 (.201 - .202)
.204				(.193 - .222)		(.201 - .206)	.204 (.205 - .206)
.208					.208	.208	.208 (.209 - .210)
.212						(.209 - .214)	.212 (.213 - .214)
.216					(.209 - .222)	.216	.216 (.217 - .218)
.220			(.191 - .254)			(.217 - .222)	.220 (.221 - .222)
.224				.224	.224	.224	.224 (.225 - .226)
.228						(.225 - .230)	.228 (.229 - .230)
.232					(.225 - .238)	.232	.232 (.233 - .234)
.236				(.225 - .254)		(.233 - .238)	.236 (.237 - .238)
.240					.240	.240	.240 (.241 - .242)
.244						(.241 - .246)	.244 (.244 - .246)
.248					(.241 - 254)	.248	.248 (.249 - .250)
.252						(.249 - .254)	.252 (.253 - .254)

Bibliografía

[1] Internetworking Basics, CISCO
http://www.cisco.com/en/US/docs/internetworking/technology/handbook/Intro-to-Internet.html

Último Acceso: Junio del 2010.

[2] Roffé Vanesa, "*Interconexión de Redes (Internetworking)",* Trabajo Monografico de Adscripcion, Argentina, 2008, *http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/Informe_SO_08.pdf*

Último Acceso: Junio del 2010.

[3] Cisco System, CCNA1 Exploration v4.0- Network Fundamentals, http://atodocisco.com/index.php?p=curricula

Último Acceso: Julio del 2010.

[4] Cisco System, CCNA2 Exploration v4.0- Routing Protocols and Concepts. http://atodocisco.com/index.php?p=curricula

Último Acceso: Julio del 2010.

[5] Cisco System, CCNA4 Exploration v4.0- Routing Protocols and Concepts. http://atodocisco.com/index.php?p=curricula

Último Acceso: Julio del 2010.

[6] HUAWEI, Documentación de CD-ROM, "*Low-End and Mid-Range Series Routers Electronic Documentation-(V3.16)".* 2007.

3611A024-VRP3.4 Operation Manual (V3.47)/06-Routing Protocol Operation/Chapter 3 RIP Configuration.

[7] HUAWEI, Documentación de CD-ROM, "*Low-End and Mid-Range Series Routers Electronic Documentation-(V3.16)".* 2007.

3611A024-VRP3.4 Operation Manual(V3.47)/06-Routing Protocol Operation/Chapter 4 OSPF Configuration.

[8] HUAWEI, "*Configuración de Interfaces y Aprovisionamiento Básico",* http://www.comten.cl/documentacion/pdfs/tips_config_min.pdf.

Último Acceso: Junio del 2010.

[9] HUAWEI, Documentación de CD-ROM, "*Low-End and Mid-Range Series Routers Electronic Documentation-(V3.16)".* 2007.

3611A024-VRP3.4 Operation Manual (V3.47)/01-Getting Started Operation/Chapter 2 User Configuration Interface.

[10] HUAWEI, Documentación de CD-ROM, "*Low-End and Mid-Range Series Routers Electronic Documentation-(V3.16)".* 2007.

3611A024-VRP3.4 Command Manual (V3.47)/01-Getting Started Command/Chapter 1 Basic Configuration Command.

[11] HUAWEI, Documentación de CD-ROM, "*Low-End and Mid-Range Series Routers Electronic Documentation-(V3.16)".* 2007.

3611A024-VRP3.4 Operation Manual (V3.47)/03-Interface Operation

[12] HUAWEI, Documentación de CD-ROM, "*Low-End and Mid-Range Series Routers Electronic Documentation-(V3.16)".* 2007.

3611A024-VRP3.4Operation Manual (V3.47)/06-Routing Protocol Operation/Chapter 2 Static Route Configuration.

[13] HUAWEI, Documentación de CD-ROM, "*Low-End and Mid-Range Series Routers Electronic Documentation-(V3.16)".* 2007.

3611A024-VRP3.4 Operation Manual (V3.47)/02-System Management Operation/Chapter 12 Terminal Services.

[14] HUAWEI, Documentación de CD-ROM, "*Low-End and Mid-Range Series Routers Electronic Documentation-(V3.16)".* 2007.

3611A024-VRP3.4 Operation Manual (V3.47)/02-System Management Operation/Chapter 5 TFTP Configuration.

[15] SSH 2.0 Configuration, http://www.h3c.com/portal/download.do?id=817108

Último Acceso: Junio del 2010.