# CAPITULO 1

# INTRODUCCIÓN

## 1.1 Objetivo

El objetivo de la tesis es explicar como se diseña e implementa el protocolo OSPF, que esta orientado para redes grandes, proporcionando también un respaldo de conocimiento de cómo es el protocolo OSPF, un protocolo de estado de enlace, sus funcionamientos, así como un conocimiento del Diseño y la implementación del Protocolo OSPF, en la red a diseñar e implementar. Con esto se espera proveer suficiente información para la selección de dicho protocolo, para su implementación en una red con direccionamiento clase B. Con un respaldo confirmado en cada uno de sus capítulos ya que en sus capítulos se busca, como primordial objetivo proporcionar buenas bases para el diseño e implementación de una red de OSPF. Así como la selección de este protocolo para grandes redes, ya

que las tecnologías alternativas a OSPF, tales como son los protocolos de Vector de Distancia, es decir: RIP, IGRP, etc. Las limitaciones de esta investigación serian las configuraciones de cada ruteador en toda la red, tan solo se mostrarán configuraciones de ruteadores, los cuales se considere clave en la arquitectura de la Red de OSPF. Así también otra limitación importante sería la del análisis de la implementación y diseño en un tipo de Red, es decir a un solo tipo de direccionamiento de Red Homologada clase B. Cabe mencionar también, que en esta investigación se utilizan diversas tecnologías que requerirían ser investigadas a parte si se requiere una completa profundidad de conocimientos de la tales como Frame Relay, etc. Para esto se requiere de una publicación especializada que esta fuera de la intención de esta investigación.

## 1.2 Justificación

Mediante esto se quiere dar merito a la elaboración de la tesis "Diseño de una Red en OSPF", que busca dar un panorama nuevo y diferente en la implementación y diseño de redes grandes de alta confiabilidad. En redes grandes cuyos sistemas y recursos tecnológicos existentes son ya de poco fiar debido a su crecimiento, y a su exigencia de confiabilidad y de la necesidad de la alta disponibilidad de sus recursos de red, dado que las redes en OSPF son por zonas independientes, si una ruta se vuelve indisponible solo en su área se escucha su indisponibilidad, no disparando el mecanismo de avisos a toda la red; cosa que hacen otros protocolos.

Como sabemos las redes digitales, se han convertido con el tiempo en redes vitales para el desarrollo de las empresas, debido a la transparencia de las redes de datos ya que pueden transportar tanto voz datos o video. Y debido a la exigencia de estos recursos se requiere de un buen diseño a nivel ruteadores ya que ellos son los que transportan y en un momento dado filtran el trafico que pasa a través de ellos. También en un buen diseño influye mucho la redistribución de

las rutas alternativas, para la disponibilidad total en caso de un siniestro, que haga que las rutas primarias en un momento dado se conviertan en indisponibles. Un buen diseño en OSPF, hace que las redes con exigencia de alta disponibilidad sean totalmente confiables, ya que un buen diseño de OSPF brinda la confiabilidad de un protocolo de Estado de Enlace, para ello lo que no pueden hacer los protocolos como RIP, IGRP u otros cuyos algoritmos son confiables pero no lo suficiente para las grandes redes de alta disponibilidad, por que muchos de estos no tienen las bondades de un sistema jerárquico de encaminamiento que hace que OSPF sea la mejor opción de diseño e implementación de una red.

Con esto ultimo se comprueba, que la implementación del protocolo OSPF, para una red grande es la mejor opción, dado que las redes están constantemente creciendo en México y un buen diseño de un protocolo es lo que pocas veces existe en las redes mexicanas. Es una excelente opción esta tesis para que sirva de guía para el diseño e implementación correcta de una red grande cuyo direccionamiento es de clase B, pero el estudio también es fundamental para la implementación de otro tipo de redes, con otros direccionamientos y necesidades y que requieran un protocolo confiable para su red. Esto se dejará para otras investigaciones, que los investigadores requieran realizar.

## 1.3 Metodología

Como, objeto muestra se seleccionará una red de gran volumen cuya dirección homologada por el NIC será de clase B, y sus dispositivos de Red a usar serán ruteadores marca Cisco serie 2600 y 7200 según donde el punto de interconexión lo necesite. Cabe aclarar que para fines explicativos, se utilizarán direccionamientos diferentes al utilizado por la implementación final de esta investigación. A través de la documentación en los capítulos se mostrara la tecnología OSPF para que se proceda a la instalación e implementación de OSPF, con el tipo de Red y dispositivos ya antes mencionados.

La red que se implementara será una red académica universitaria (UANL), que es una red regional en el Estado de Nuevo León, esta tendrá un direccionamiento de 168.130.0.0 y será redistribuido según los pasos a seguir para su correcta implementación en el protocolo la metodología de implementación se cita en el capitulo 6 y no esta demás mencionarla en estos 6 posos:

- Paso 1: Analice los Requerimientos
- Paso 2 Desarrollo de la Topología de la Red
- Paso 3: Determinación del Direccionamiento y la Convención de los Nombres
- Paso 4: Provisión del Hardware
- Paso 5: Aprovechamiento del Protocolo y las Características del IOS
- Paso 6: Implementación Monitoreo y Manejo de la Red

Esta red en particular constará de 3 campus uno será el principal, en el cual residirá la espina dorsal de esta red, este es Ciudad Universitaria. Los otros dos son Campus Medico y Campus Mederos, cada uno de estos con dependencias que necesitan estar conectadas con la red constantemente. También la red necesita conectar a diversas dependencias foráneas situadas en todo el estado de Nuevo León, mediante enlaces dedicados, en la WAN, permitiendo una conexión punto a punto con cada dependencia desde el campus principal d la ciudad Universitaria. Así también se conectara esta red con la red global, a través del protocolo BGP – 4, permitiendo así que la red en cuestión tenga posibilidades infinitas dentro del ciberespacio. Cabe mencionar que la limitante importante en esta investigación es el despliegue completo de todas las configuraciones de nuestra red, dado que se trata de una red muy grande, se necesitarían de mas de 1000 hojas para mostrar cada una de las configuraciones de nuestra red. En vez de esto se opto por resumir de alguna manera, las configuraciones de la red en cuestión, mostrando y explicando cada porción de las configuraciones de la red en cuestión.

# CAPITULO 2

# INTRODUCCIÓN A LAS TECNOLOGÍAS

## 2.1 Modelo De Referencia Del Sistema de Interconexión Abierto

El sistema de interconexión abierto (OSI) describe cómo la información de una Aplicación de software en una computadora se mueve a través de la red a otra computadora. El modelo de referencia OSI es un modelo conceptual integrado por siete capas, con funciones particulares de cada una. El modelo fue desarrollado por la Organización de Estandarización Internacional (ISO) en 1984, y ahora se considera el modelo arquitectónico primario para las comunicaciones entre computadoras. El modelo OSI divide las tareas implicadas con la transmisión de información entre computadoras en siete tareas más pequeñas, siendo este grupos de tarea más manejables. Una tarea o un grupo de tareas entonces se asigna a cada uno de las siete capas de OSI. Cada capa es razonablemente autónoma para poder poner en ejecución las tareas asignadas a cada capa independientemente. Esto permite que las soluciones ofrecidas por una capa sean

actualizables cada una, sin afectar las otras capas. La lista siguiente detalla las siete capas del modelo (OSI):

- Capa 7 -- Aplicación
- Capa 6 -- Presentación
- Capa 5 -- Sesión
- Capa 4 -- Transporte
- Capa 3 -- Red
- Capa 2 -- Trasmisión de datos
- Capa 1 -- Física

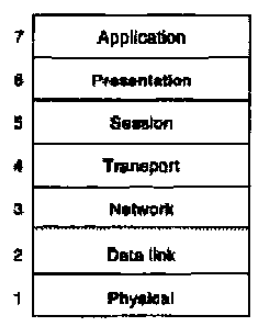



**Figura 2 -** 1 El sistema de interconexión abierto Contiene Siete Capas Independientes

## 2.2 Características de las Capas de OSI

Las siete capas del MODELO OSI se pueden dividir en dos categorías: capas superiores y capas más bajas.

*Las capas superiores* del modelo OSI son las que tratan generalmente con El software, esto es con la capa más alta, la capa de Aplicación, que está más cercana al usuario del extremo. Los usuarios y los procesos de la capa de

Aplicación interactúan recíprocamente con el software de aplicaciones que contienen los componentes de comunicaciones. El término de capa superior se utiliza a veces para referirse a cualquier capa que este sobre otra capa en el modelo de OSI.

La capa más bajas Son las encargadas de todo el proceso que implica el transporte de los datos. La capa física y la capa de trasmisión de datos se implementan en hardware y software. La capa más baja, la capa física, es la más cercana al medio físico de la red (la red de cableado, por ejemplo) y es responsable realmente de poner la información en el medio.
La Figura 2-3 ilustra la división entre las capas superiores y más bajas del OSI.

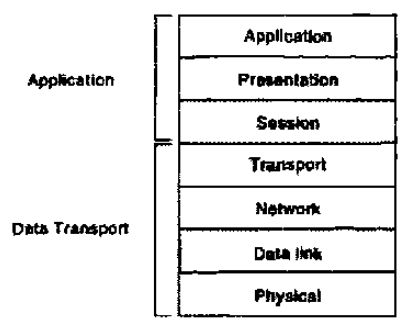



**Figura 2 - 2:** Dos sistemas de capas hacen para arriba las capas de OSI

## 2.2.1 Protocolos

El modelo de OSI proporciona un marco conceptual para la comunicación entre las computadoras, pero el modelo en sí mismo no es un método de comunicación. La comunicación real es hecha usando protocolos de comunicación. En el contexto de establecimiento de una red de datos, *un protocolo* es un sistema formal de reglas y de convenciones que gobierna, cómo

las computadoras intercambian la información sobre un medio de la red. Un protocolo pone en función una o más de las capas del OSI.

Existe una variedad amplia de protocolos de comunicación. Algunos de estos protocolos incluyen protocolos de LAN, protocolos de WAN, protocolos de red, y protocolos de la Encaminamiento. *Los protocolos de LAN* funcionan en las capas física de trasmisión y la de enlace de datos del modelo OSI y definen el intercambio de datos sobre varios medios de LAN. *Los protocolos WAN* funcionan en las tres capas más bajas del modelo de OSI y definen la comunicación sobre varios medios de Redes de Área Amplia. *Los protocolos de encaminamiento o Ruteo* son los protocolos de capa de red que son responsables de intercambiar la información entre las Ruteadores de modo que los ruteadores puedan seleccionar la trayectoria apropiada para el tráfico de la red. Finalmente, *los protocolos de red* son varios protocolos de capa superior que existen en una conjunto dado de protocolos. Muchos protocolos confían en otros para la operación. Por ejemplo, muchos protocolos de encaminamiento utilizan protocolos de red para intercambiar la información entre los Ruteadores. Este concepto de la construcción sobre las capas ya en existencia, es la función del modelo de OSI.

### 2.2.2 Modelo OSI y Comunicación Entre los Sistemas

La información que es transferida de un software de aplicación en un sistema informático a un software de aplicación en otro, debe pasar por las capas del OSI. Por ejemplo, si un software de aplicación en el sistema **A** tiene información a transmitir a un software de aplicación en el sistema **B**, el programa de aplicación en el sistema **A** pasará su información a la capa de aplicación (la capa 7) de la capa de aplicación del sistema **A**. Después pasa la información a la capa de presentación (la capa 6), que retransmite los datos a la capa de sesión (capa 5), etcétera hasta la capa física (capa 1). En la capa física, la información se pone en el medio físico de la red y se envía a través del medio al sistema **B**. Entonces la capa física del sistema **B** quita la información del medio físico, y

entonces su capa física pasa la información hasta la capa de enlace de datos (la capa 2), que la pasa a la capa de red (capa 3), etcétera, hasta que alcanza la capa de aplicación (capa 7) del sistema **B**. Finalmente, la capa de aplicación del sistema **B** pasa la información al programa de aplicación del receptor para terminar el proceso de la comunicación.

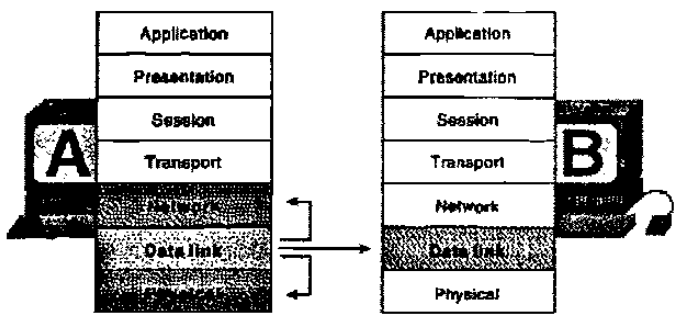



**Figura 2 - 3** Comunicación del Modelo OSI con otras Capas.

A continuación se mencionaran cada una de las capas del Modelo OSI y su función especifica dentro del modelo.

## 2.2.2.1 La Capa Física Del Modelo OSI

La capa física define las especificaciones eléctricas, mecánicas, procésales, y funcionales para activar, mantener, y desactivar el enlace físico entre los sistemas de red al comunicarse. Las especificaciones de la capa física definen características tales como niveles voltaicos, medición del tiempo en los cambios de voltaje, tarifas de datos físicas, distancias máximas de la transmisión, y

conectores físicos. Las implementaciones de la capa física se pueden categorizar como especificaciones de LAN o WAN. El Figura 1-4 ilustra algunas LAN y WAN comunes.

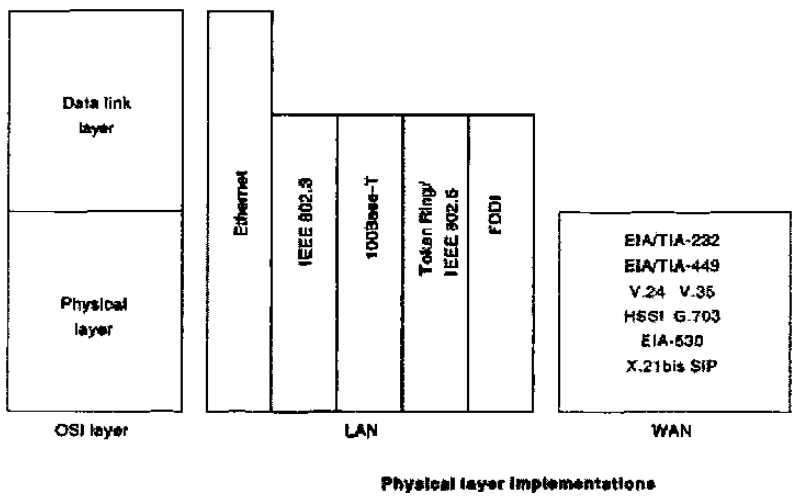



**Figura 2 - 4** La implementación de la capa física pueden ser especificaciones LAN o WAN

## 2.2.2.2 La Capa De Enlace De Datos Del Modelo OSI

La capa de enlace de datos proporciona un tránsito confiable de datos a través de un enlace físico de red. Diversas especificaciones de la capa de enlace de datos definen diversas características de red, estas hacen funciones de gestión incluyendo la dirección física, la topología de la red, la notificación del error, secuencias de tramas, y control de flujo. El direccionamiento físico (en

comparación con el direccionamiento de red) define cómo los dispositivos se tratan en la capa de enlace de datos. La topología de la red consiste en las especificaciones de la capa de enlace de datos que definen a menudo cómo los dispositivos deben ser conectados físicamente, por ejemplo adentro una topología de bus o una topología de anillo. La notificación de error, alerta a protocolos de capas superiores, que ha ocurrido un error de transmisión, y la secuencia de tramas de datos, reordena las tramas que se transmitieron fuera de secuencia. Finalmente, el control de flujo modera la transmisión de datos para no abrumar el dispositivo de recepción con más tráfico que él puede dirigir contemporáneamente.

El instituto de los ingenieros electrónicos y eléctricos (IEEE) ha subdividido la capa de trasmisión de datos en dos subcapas: Control Lógico de Enlace (LLC) y Control de Acceso al Medio (MAC). El Figura 1-5 ilustra las subcapas de IEEE de la capa de trasmisión de datos.

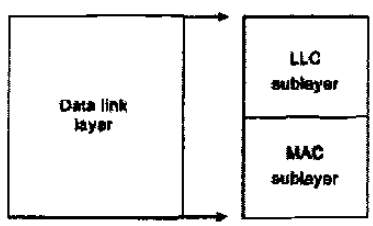



**Figura 2 - 5** La Capa De Enlace De Datos Contiene Dos Subcapas

La subcapa de control Lógico de Enlace (LLC) de la capa de enlace de datos maneja las comunicaciones entre los dispositivos sobre un solo enlace en una red. El LLC se define en la especificación de IEEE 802,2 y apoya los servicios Orientados a no conexión y los Orientados a Conexión usados por protocolos de capas mas altas. El IEEE 802,2 define un número de campos en los marcos de la capa de enlace de datos que permiten a protocolos múltiples de la capas superiores compartir un solo enlace de datos físico. La subcapa de Control de Acceso al Medio (MAC) de la capa de enlace de datos maneja el acceso del

protocolo al medio físico de la red. La especificación del MAC de IEEE define las direcciones del MAC, que permiten a los dispositivos múltiples identificarse uno del otro en la capa de trasmisión de datos.

### 2.2.2.3 La Capa De Red Del Modelo OSI

La capa de red define la dirección de red, a diferencia del MAC ADDRESS. Algunas implementaciones de la capa de red, tales como el Protocolo de Internet (IP), definen las direcciones de red de una manera que encaminan a sus destinos la información. La selección puede ser determinada sistemáticamente comparando la dirección de red de la fuente con la dirección de red de destino, y aplicando la mascara de subred. Porque esta capa define la disposición lógica de la red, los ruteadores pueden utilizar esta capa para determinar cómo enviar los paquetes. Debido a esto, mucho del trabajo del diseño y de la configuración para las redes sucede en la capa 3, la capa de red.

### 2.2.2.4 La Capa De Transporte Del Modelo OSI

La capa de transporte acepta datos de la capa de sesión y divide los datos en segmentos para el transporte a través de la red. Generalmente, la capa de transporte es responsable de cerciorarse de que los datos están sin error y en la secuencia apropiada. El control de flujo ocurre generalmente en la capa de transporte. El control de flujo maneja la transmisión de datos entre los dispositivos de modo que el dispositivo que transmite no envíe más datos que el dispositivo de recepción pueda procesar. La multiplexión permite a datos de varios usos ser transmitidos sobre un solo enlace físico. Los circuitos virtuales son establecidos, mantenidos, y terminados por la capa de transporte. El repaso de las faltas implica el crear varios mecanismos para detectar errores de la transmisión,

mientras que la recuperación de error implica el actuar, por ejemplo solicitar que los datos estén retransmitidos, para resolver cualquier error que ocurra. Los protocolos del transporte usados en el Internet son TCP y UDP.

### 2.2.2.5 La Capa De Sesión Del Modelo OSI

La capa de sesión del modelo OSI establece, maneja, y termina sesiones de comunicación. Las sesiones de comunicación consisten en peticiones de servicio y mantienen las respuestas que ocurren entre los usos, situados en diversos dispositivos de red. Estas peticiones y respuestas son coordinadas por los protocolos implementados en la capa de sesión. Algunos ejemplos de implementación de la capa sesión, incluyen el Protocolo de Información de Zona (ZIP), el protocolo de Appletalk que coordina el proceso de enlace por nombres; y el Protocolo del Control de Sesión (SCP), el protocolo de capa de sesión de DECnet fase IV.

### 2.2.2.6 La Capa De Presentación Del Modelo OSI

La capa de presentación, proporciona una variedad de funciones de codificación y de conversión que se aplican a los datos de la capa de Aplicación. Estas funciones se aseguran que la información enviada de la capa de Aplicación, de un sistema fuera legible por la capa de Aplicación de otro sistema. Algunos ejemplos de los esquemas de la codificación y de la conversión de la capa de presentación incluyen formatos comunes de la representación de datos, la conversión de los formatos de carácter de la representación, esquemas comunes de la compresión de datos, y esquemas comunes del encríptado de datos. Los formatos comunes de la representación de datos, o el uso de la imagen estándar, del sonido, y de los formatos de video, permiten el intercambio de datos y su uso entre diversos tipos de sistemas informáticos.

Los esquemas de la conversión son utilizados para intercambiar la información por los sistemas usando diversas representaciones de texto y de

datos, tales como EBCDIC y ASCII. Los esquemas estándares de la compresión de datos permiten que los datos se compriman en el dispositivo fuente y que se descompriman correctamente en la destinación. Los esquemas estándares del cifrado o encríptado de datos permiten que los datos cifrados en el dispositivo de la fuente sean descifrados correctamente en la destinación.

Las implementaciones de la capa de presentación no se asocian típicamente a un conjunto de protocolos en particular. Algunos estándares bien conocidos para el vídeo incluyendo a QuickTime y al grupo de expertos de la película (MPEG). QuickTime es una especificación en computadoras de Apple para vídeo y el audio, y el MPEG es un estándar para la compresión y la codificación video. Entre las imágenes gráficas bien conocidas existen los formatos como : el formato de intercambio de gráficos (GIF), el grupo de expertos fotográfico (JPEG), y el formato marcado con etiqueta del archivo de la imagen (tiff). El GIF es un estándar para comprimir y encríptar imágenes gráficas. El JPEG es otro estándar de la compresión y de la codificación para las imágenes gráficas, y el tiff es un formato estándar de la codificación para las imágenes gráficas.

### 2.2.2.7 La Capa De Aplicación Del Modelo OSI

La capa de Aplicación es la capa de OSI más cercana al usuario, esto significa que la capa de Aplicación del OSI y el usuario interactúan directamente con el software Aplicación

Esta capa interactúa con los softwares de Aplicación que implementan un componente de comunicación. Tales programas de Aplicación caen fuera del alcance del modelo OSI. Las funciones de la capa de Aplicación incluyen

típicamente identificar a las partes a comunicar, la determinación de disponibilidad del recurso, y sincronizar la comunicación.

Al identificar a las partes a comunicar, la capa de Aplicación determina la identidad y la disponibilidad de las partes a comunicar para una aplicación con datos para transmitir.

Al determinar disponibilidad del recurso, la capa de Aplicación debe decidir si existen los suficientes recursos de la red para la comunicación solicitada.

En sincronizar la comunicación, toda la comunicación entre las aplicaciones requiere la cooperación que es manejada por la capa de Aplicación. Algunos ejemplos de las implementaciones de la capa de Aplicación incluyen el telnet, el Protocolo de Transferencia de Archivos (ftp), y el Protocolo Simple de Correo (smtp).

## 2.3 Protocolos de Internet

Los protocolos de Internet son los protocolos (no propietarios) de sistema abierto más populares del mundo porque pueden ser utilizados para comunicarse a través de redes implementadas e interconectadas y están igualmente bien definidas para LAN y sobre las comunicaciones de WAN. Los protocolos de Internet consisten en un conjunto de protocolos de comunicación, los cuales existen dos muy conocidos que son: Protocolo de Control de Transmisión (TCP) y el Protocolo de Internet (IP). El conjunto de Protocolo de Internet, incluye no sólo protocolos de las capas bajas (tales como TCP y IP), sino que también especifica usos comunes tales como correo electrónico, emulación terminal, y transferencia de archivos.

Los protocolos del Internet primero fueron desarrollados a mediados de los años setenta, cuando el la Agencia de Defensa de investigaciones Avanzadas

(DARPA) llegó a estar interesada en establecer una red de conmutación de paquetes, que facilitaría la comunicación entre los sistemas informáticos disímiles en las instituciones de investigación. Con una meta de conectividad heterogénea en mente, DARPA financió la investigación de la Universidad de Stanford y Bolt, Beranek, y Newman (BBN). El resultado de este esfuerzo del desarrollo era de un conjunto de Protocolos de Internet, a finales de los años 70.

La documentación de los protocolos de Internet (los nuevos o los protocolos revisados) y las políticas se especifican en los informes técnicos llamados Peticiones para Comentarios ( RFC's), que son publicados y después repasados y analizados por la comunidad del Internet. Los refinamientos del protocolo se publican en los RFC's nuevos. Para ilustrar el alcance de los protocolos del Internet, el Figura 1-6 cuenta con mapas de muchos de los protocolos de Internet y de sus capas correspondientes de OSI. Este capítulo trata los elementos y las operaciones básicos de éstos y otros protocolos dominantes del Internet.

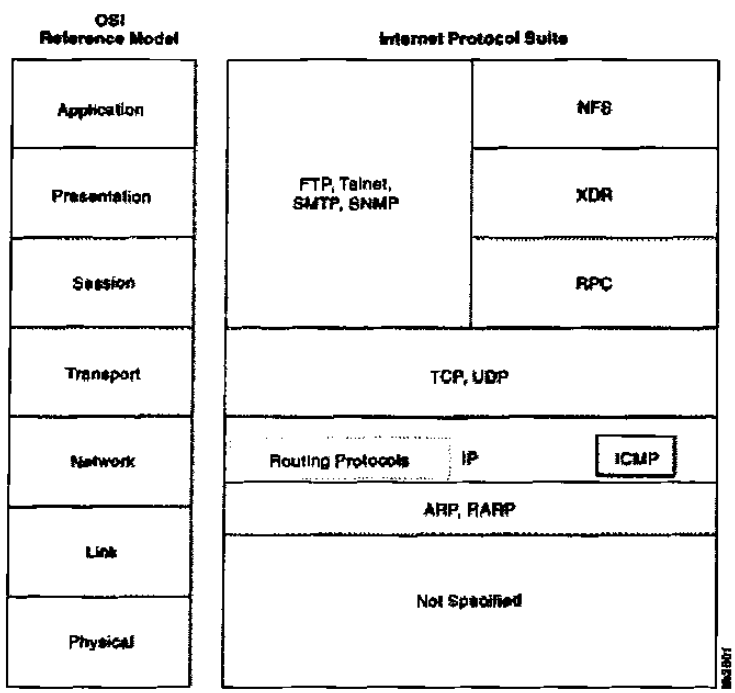



**Figura 2 - 6** El protocolo de Internet se muestra en la gama completa del modelo OSI.

El Protocolo de Internet (IP) se encuentra en la capa red (protocolo de capa 3) que contiene la dirección de información y de una cierta información de control que permita a los paquetes ser encaminados. El IP se documenta en el RFC 791 y es el protocolo primario de la capa de red. Junto con el Protocolo de Control de Transmisión (TCP), el IP representa el corazón de los protocolos de Internet. El IP tiene dos responsabilidades primarias: brindar comunicación no orientada a conexión, entrega del mejor esfuerzo de datagramas en una red; y proporciona la fragmentación y el nuevo ensamble de datagramas a los acoplamientos de los datos de apoyo de diversos tamaños de la unidad máxima de transmisión (MTU).

## 2.3.1 Formato Del Paquete del IP

Un paquete del IP contiene varios tipos de información, según lo ilustrado en el Figura 2 - 7.

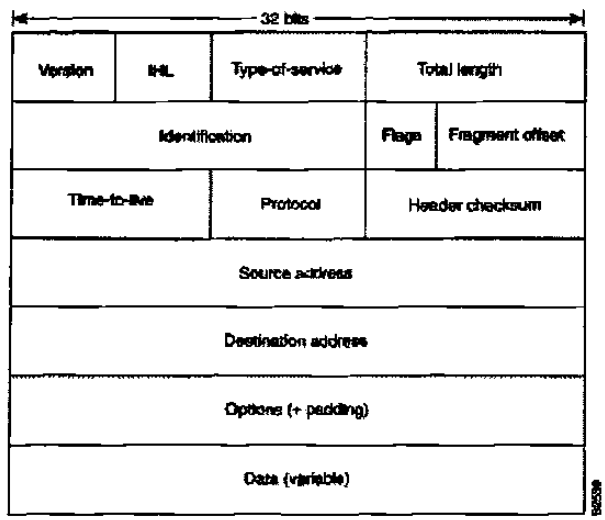



**Figura 2 - 7** Catorce campos abarcan un paquete de IP.

La discusión siguiente describe los campos del paquete del IP ilustrados en el Figura 2 - 7:

- Versión -- indica la versión del IP usada actualmente.
- Longitud del encabezado del IP *(* IHL) -- indica la longitud del encabezado del datagrama en palabras 32-bit.
- Tipo-de-Servicio -- especifica cómo un protocolo de la superior-capa quisiera que un datagrama actual fuera manejado, y asigna a los datagramas varios niveles de importancia.
- Longitud total -- especifica la longitud, en octetos, del paquete entero de IP, incluyendo los datos y el encabezado.
- Identificación -- contiene un número entero que identifica el datagrama actual. Este campo se utiliza para ayudar a ensamblar fragmentos del datagrama.
- Las banderas -- consiste en un campo de 3-bit del cual los dos bits (menos significativos) de orden inferior controlan la fragmentación. El bit de peso inferior especifica si el paquete puede ser hecho fragmentos. El bit medio especifica si el paquete es el fragmento pasado en una serie de paquetes hechos fragmentos. El bit tercero o de categoría alta no se utiliza.
- Fragmento compensado -- indica la posición de los datos del fragmento concerniente al principio de los datos en el datagrama original, que permite que el proceso de IP de destinación reconstruya correctamente el datagrama original.
- Tiempo-a-Vida -- mantiene un contador que gradualmente se decrementa hacia abajo a cero, en ese punto se desecha el datagrama. Esto guarda los paquetes de transmisión sin fin.
- Protocolo -- indica qué protocolo de la capa superior recibe los paquetes entrantes después de que el proceso de IP sea completo.
- Suma de comprobación del encabezado -- ayuda a asegurar la integridad del encabezado del IP.
- *Dirección* de fuente -- especifica el nodo que envía.
- Dirección de la destinación -- especifica el nodo de recepción.

- Las opciones -- permite que el IP apoye varias opciones, tales como seguridad.
- Los datos -- contiene la información de la capa superior.

### 2.3.2 Dirección de IP

Como con cualquier otro protocolo de capa red, el esquema de dirección del IP es integral al proceso de encaminar los datagramas de IP en una red. Cada dirección de IP tiene componentes específicos y sigue un formato básico. Estas direcciones de IP se pueden subdividirse y utilizarse para crear direcciones para las subredes.

Cada anfitrión en una red de TCP/IP se le asigna una dirección lógica de 32-bit única que se divide en dos porciones principales: el numero de red y el numero de anfitrión. El numero de Red identifica una red y se debe asignar por el Centro de información de Red (InterNIC) si la red es ser parte del Internet. Un Proveedor de Internet (ISP) puede obtener bloques de direcciones de red del InterNIC y puede por si mismo asignar el espacio de direcciones como así lo requiera. El numero de anfitrión identifica un anfitrión en una red y es asignado por el administrador local de la red.

### 2.3.3 El Formato de Dirección de IP

La Dirección IP de 32-bit se agrupa en ocho bits a la vez, y es separado por puntos, y representada en el formato decimal (conocido como *notación puntual decimal*). Cada bit en el octeto tiene un peso binario (128, 64, 32, 16, 8, 4, 2, 1). El valor mínimo para un octeto es 0, y el valor máximo para un octeto es 255. El Figura 1-8 ilustra el formato básico de una IP.

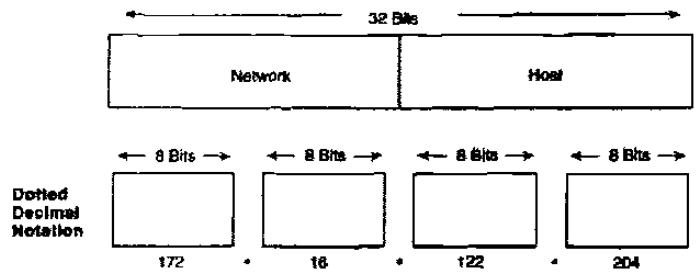



**Figura 2 - 8** Una Dirección de IP consiste en 32 bits, agrupados en cuatro octetos.

## 2.3.4 Clases de Dirección de IP

El IP soporta cinco diversas clases de las direcciones: A, B, C, D, y E. Solamente las clases A, B, y C están disponibles para el uso comercial. Los bits (de categoría alta) extremos izquierdos indican la clase de la red. La tabla 1-1 proporciona la

información de referencia sobre las cinco clases de Direcciones de IP.

| IP Clases de Red | Formato | Propósito | Orden Superior Bit(s) | Rango de Direcciones | No. Bits de Red/ anfitrión | Max. Anfitriones |
|---|---|---|---|---|---|---|
| A | N.H.H.H[1] | Pequeñas Organizaciones | 0 | 1.0.0.0 a 126.0.0.0 | 7/24 | 16,777, 214[2] ($2^{24}$ - 2) |
| B | N.N.H.H | Medianas Organizaciones | 1, 0 | 128.1.0.0 a 191.254.0.0 | 14/16 | 65, 543 ($2^{16}$ - 2) |
| C | N.N.N.H | Organizaciones relativamente pequeñas | 1, 1, 0 | 192.0.1.0 a 223.255.254.0 | 22/8 | 245 ($2^{8}$ - 2) |
| D | N/A | Grupos de Multitransmisión (RFC 1112) | 1, 1, 1, 0 | 224.0.0.0 a 239.255.255.255 | N/A (No para Uso Comercial) | N/A |
| E | N/A | Experimental | 1, 1, 1, 1 | 240.0.0.0 a 254.255.255.255 | N/A | N/A |

**Tabla 2 - 1** Información de referencia sobre las cinco clases de Direcciones IP

[1] N = Numero de Red, H = Numero de Anfitrión

[2] una dirección es reservada para la dirección de difusión, y una dirección es reservada para la red.

El Figura 2-9 ilustra el formato de las clases comerciales de las Direcciones de IP. (observe los bits de categoría alta en cada clase.)

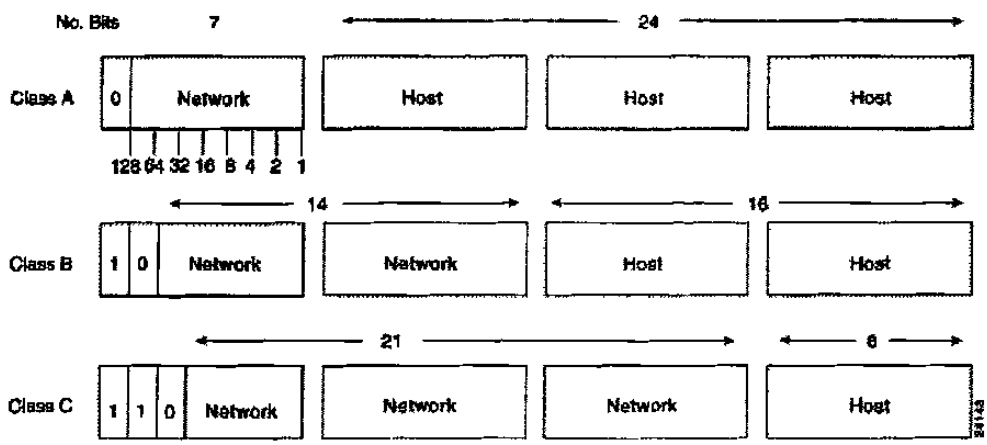



**Figura 2 - 9** La Dirección de IP se ajusta al formato A, B, y C, que está disponible para el uso comercial.

Las clases de dirección puede ser determinada fácilmente examinando al primer octeto de la dirección y ubicando ese valor a un rango de clases en la tabla siguiente. En una Dirección IP de 172.31.1.2, por ejemplo, el primer octeto es 172. Dado que 172 cae entre 128 y 191, 172.31.1.2 es una dirección de la clase B. El

Figura 2-10 resume los rangos de valores posibles para el primer octeto de cada clase de la dirección.

| Address Class | First Octet In Decimal | High-Order Bits |
|---|---|---|
| Class A | 1 Ð 126 | 0 |
| Class B | 128 Ð 191 | 10 |
| Class C | 192 Ð 223 | 110 |
| Class D | 224 Ð 239 | 1110 |
| Class E | 240 Ð 254 | 1111 |

**Figura 2 - 10** Rango de valores posibles que existen para el primer octeto de cada clase de dirección.

## 2.3.5 Dirección De Subred de IP

Las redes de IP se pueden dividir en redes más pequeñas llamadas Subredes. Las Subredes brindan al administrador de red varias ventajas, incluyendo flexibilidad adicional, un uso más eficiente de direcciones de red, y la capacidad de contener tráfico de difusión (una difusión no cruzará un ruteador).

Las Subredes están bajo administración local. Así que, el mundo exterior ve una organización como una sola red y no tiene ningún conocimiento detallado de la estructura interna de la organización.

Una dirección de red dada se puede segmentar en muchas subredes. Por ejemplo, 172.16.1.0, 172.16.2.0, 172.16.3.0, y 172.16.4.0 son todas las subredes dentro de la red 171.16.0.0. (todo en 0s en la porción del anfitrión de una dirección especifica de la red entera).

## 2.3.5.1 Mascara de Subred de IP

Una Dirección de subred es creada "pidiendo prestados" bits del campo del anfitrión y señalándolos como el campo de Subred. El número de bits prestados varía y es especificado por la mascara de Subred. El Figura 1-11 demuestra cómo los bits se piden prestados del campo de la dirección del anfitrión para crear el campo de dirección de Subred.

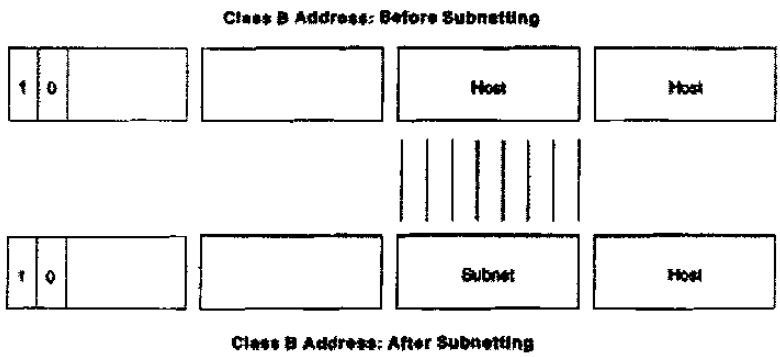



**Figura 2 - 11** Los bits se piden prestados del campo de dirección del anfitrión para crear el campo de dirección de red.

Las máscaras de subred utilizan la misma técnica de formato y de representación de direcciones de IP. La mascara de subred, sin embargo, tiene 1s binarios en todos los bits que especifican los campos de red y de subred, y 0s binarios en todos los bits que especifiquen el campo del anfitrión. El Figura 1-12 ilustra un ejemplo de la mascara de subred.

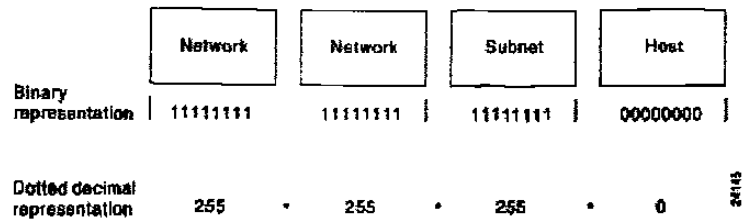



**Figura 2 - 12** Un ejemplo de mascara de subred consiste en todos 1s y 0s binarios.

Los bits de la mascara de subred deben venir de los bits (extremos izquierdos) de categoría alta del campo del anfitrión, pues el Figura 1-13 los ilustra. Los detalles de los tipos de mascara de subred de la clase B y de C a continuación se presentan. Las direcciones de la clase A no se discuten en este capítulo porque están generalmente en la subred en un límite de 8-bits.

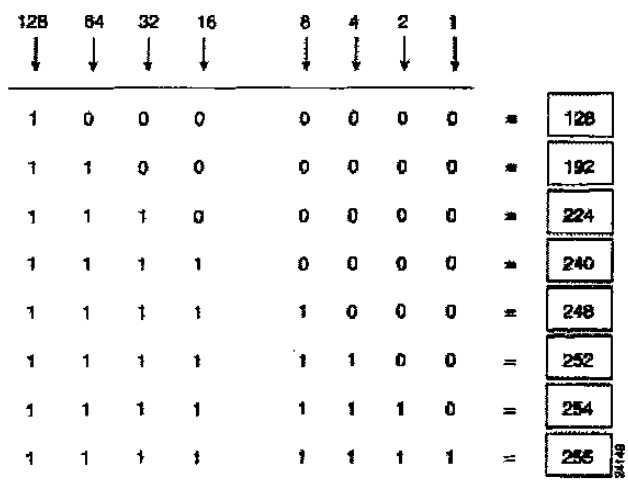



**Figura 2 - 13** Los bits de la mascara de subred vienen en los bits de categoría alta del campo del anfitrión.

Varios tipos de máscaras de subred existen para las subredes de la clase B y de la C.

La Mascara de subred por defecto para una dirección de la clase B que no tenga ninguna subred es 255.255.0.0, mientras que la mascara de subred para una dirección 171.16.0.0 de la clase B que especifique ocho bits de subred es 255.255.255.0. La razón de esto es que existen ocho bits para subred (1 para la

dirección de red y 1 para la dirección de difusión) = 254 posibles subredes, con $2^8 - 2 = 254$ anfitriones posibles por subred.

La mascara de Subred para una dirección 192.168.2.0 de clase C que especifica cinco bits de subred es 255.255.255.248. Con cinco bits disponibles para segmentar, $2^5 - 2 = 30$ subredes posibles, con $2^3 - 2 = 6$ anfitriones por subred.

Las tablas de referencia mostradas en la tabla 1-2 y la tabla 1-3 pueden ser utilizadas para planear redes de la clase B y de C, para determinar el número de subredes requeridas y de anfitriones, y la mascara de subred apropiada.

**Tabla 2 - 2** Tabla De Referencia De la Subred Clase B

| Numero de Bits | Mascara de Subred | Numero de Subred | Número de Anfitriones |
|---|---|---|---|
| 2 | 255.255.192.0 | 2 | 16382 |
| 3 | 255.255.224.0 | 6 | 8190 |
| 4 | 255.255.240.0 | 14 | 4094 |
| 5 | 255.255.248.0 | 30 | 2046 |
| 6 | 255.255.252.0 | 62 | 1022 |
| 7 | 255.255.254.0 | 126 | 510 |
| 8 | 255.255.255.0 | 254 | 254 |
| 9 | 255.255.255.128 | 510 | 126 |
| 10 | 255.255.255.192 | 1022 | 62 |
| 11 | 255.255.255.224 | 2046 | 30 |
| 12 | 255.255.255.240 | 4094 | 14 |
| 13 | 255.255.255.248 | 8190 | 6 |
| 14 | 255.255.255.252 | 16382 | 2 |

**Tabla 2 - 3** Tabla De Referencia De Subred en Direcciones Clase C

| Número de Bits | Mascara de Subred | Numero de Subred | Número de Anfitriones |
|---|---|---|---|
| 2 | 255.255.255.192 | 2 | 62 |
| 3 | 255.255.255.224 | 6 | 30 |
| 4 | 255.255.255.240 | 14 | 14 |
| 5 | 255.255.255.248 | 30 | 6 |
| 6 | 255.255.255.252 | 62 | 2 |

### 2.3.5.2 ¿Cómo las máscaras de Subred se utilizan para determinar el número de Subred?

Los Ruteadores realizan un proceso para determinar la dirección de red (o más específicamente, de Subred). Primero, los ruteadores extraen la dirección de la destinación de IP del paquete entrante y recupera la mascara de subred interna. Entonces se realiza un AND lógico, una operación para obtener el numero de red. Esto hace que la porción del anfitrión de la dirección de destinación de IP pueda ser removida, mientras que sigue habiendo el numero de Red de destinación. Los

ruteadores entonces ven el numero de Red y la envía a la interfaz saliente. Finalmente, transmite la trama a la Dirección IP de destinación.

### 2.3.5.3 Operación Lógica AND

Tres reglas básicas gobiernan la operación lógica "AND" de dos números binarios. Primera, 1 "AND" con 1 produce 1. En segundo lugar, 1 "AND" con 0 produce 0. Finalmente, 0 "AND" con 0 produce 0. La tabla de verdad proporcionada en la tabla 2-4 ilustra las reglas para las operaciones lógicas AND.

**Tabla 2 - 4** Reglas para las operaciones lógicas AND

| Entrada | Entrada | Salida |
|---|---|---|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 0 |

Dos pautas simples existen para recordar las operaciones lógicas del AND : La AND lógica de un 1 con un 1 produce el valor original, y lógicamente un "AND" de un 0 con cualquier número produce un 0.

El Figura 2-14 ilustra que cuando un AND lógico de una Dirección de IP de destinación y de su mascara de Subred se realiza, el número de Subred se conserva, lo cual el ruteador utiliza para transmitir al paquete.

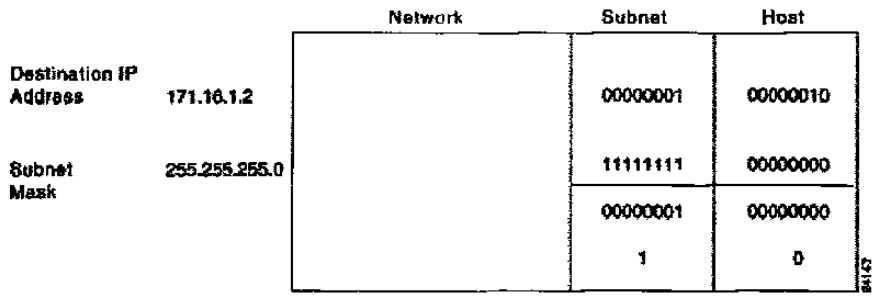



**Figura 2 - 14** La aplicación de un AND lógico a la IP de destinación con su mascara de subred produce el número de subred.

## 2.3.6 Protocolo de resolución de Direcciones (ARP)

Para que dos máquinas en una red dada se comuniquen, deben saber las direcciones físicas de la máquina (o MAC). Difundiendo el protocolo de resolución de direcciones (ARP's), un anfitrión puede descubrir dinámicamente la dirección de la capa MAC que corresponde a una dirección en particular de la capa de red de IP.

Después de recibir una dirección de la capa MAC, los dispositivos de IP crean una memoria de ARP para almacenar la dirección recientemente adquirida de la relación IP-a-MAC, así evitando tener que difundir ARPS cuando desean reconectarse a un dispositivo. Si el dispositivo no responde dentro de un marco de tiempo especificado, se limpia la memoria.

Además el Protocolo reverso de resolución de direcciones (RARP) se utiliza para ubicar las direcciones de la capa MAC a las direcciones del IP. El RARP, que es lo contrario lógicamente de ARP, se pude utilizar por las estaciones de

trabajo sin disco duro que no saben sus direcciones de IP cuando son encendidas. El RARP confía en la presencia de un servidor de RARP con una tabla de ubicación de las direcciones de la capa MAC-a-IP.

## 2.4 Encaminamiento de Internet

Los dispositivos de encaminamiento de Internet tradicionalmente se han llamado puertas de enlaces. En terminología de hoy, sin embargo, las puertas de enlace se refieren específicamente a un dispositivo que realice la traducción de protocolos de la capa aplicación entre los dispositivos. Las puertas de enlace interiores se refieren a los dispositivos que realizan estas funciones, que se encuentran bajo el mismo control de administración o autoridad de red, tal como una red interna de una corporación. Éstos se conocen como sistemas autónomos. Las puertas de enlace realizan funciones del protocolo entre las redes independientes.

Los ruteadores dentro del Internet se organizan jerárquicamente. Los ruteadores usados para el intercambio de información dentro de sistemas autónomos se llaman ruteadores interiores, que utilizan una variedad de protocolos interiores (IGPs) para lograr este propósito. El Protocolo de encaminamiento de información (RIP) es un ejemplo de un IGP.

Los ruteadores que mueven la información entre los sistemas autónomos se llaman ruteadores exteriores. Estos ruteadores utilizan un Protocolo Exterior de puerta de enlace para intercambiar la información entre los sistemas autónomos. El Protocolo de Puerta de Enlace Fronterizo (BGP) es un ejemplo de un Protocolo de Puerta de Enlace exterior.

### 2.4.1 Encaminamiento de IP

Los protocolos de encaminamiento de IP son dinámicos. El encaminamiento dinámico busca calcular rutas automáticamente en los intervalos regulares por el software en dispositivos de encaminamiento. Esto se pone en contraste con el encaminamiento estático, donde las rutas son establecidas por el administrador de red y no cambian hasta que el administrador de la red las cambie.

Una tabla de encaminamiento de IP, consiste en la dirección de destinación/ siguiente salto, se utiliza para permitir la encaminamiento dinámico. Una entrada en esta tabla, por ejemplo, sería interpretada como sigue: para conseguir a la red 172.31.0.0. envíe el paquete fuera de la interfaz 0 (E0) de Ethernet.

El encaminamiento de IP especifica que los datagramas de IP viajan a través de la red un salto a la vez. La ruta entera no se sabe en el inicio del viaje. En lugar, en cada parada, la destinación siguiente es calculada emparentando la dirección de destinación dentro del datagrama con una entrada en la tabla de encaminamiento del nodo actual.

La implicación de cada nodo en el proceso de encaminamiento se limita a la expedición de paquetes basados en la información interna. Los nodos no supervisan si los paquetes consiguen su destinación final, ni el IP prevé el error para divulgarlo de nuevo a la fuente al ocurrir anomalías. Esta tarea se deja a otro Protocolo de Internet, el protocolo de control de mensaje de Internet (ICMP).

## 2.5 Protocolo de control de mensaje del Internet (ICMP)

El protocolo de control de mensaje de Internet (ICMP), es un Protocolo de Internet de la capa red que proporciona mensajes de paquetes para informar errores y otra información con respecto al paquete de IP que se procesa de nuevo a la fuente. El ICMP se documenta en el RFC 792.

### 2.5.1 Mensajes de ICMP

Los mensajes ICMP's generan varias clases de mensajes útiles, incluyendo la destinación inalcanzable, petición del eco y la contestación, redireccionamiento, tiempo excedido, y de anuncio de ruteadores y de solicitación de ruteador. Si un mensaje de ICMP no puede ser entregado, ningún otro será generado. Éste debe evitar una inundación sin fin de mensajes de ICMP.

Cuando un mensaje de destinación inalcanzable del ICMP es enviado por un ruteador, significa que el ruteador no puede enviar el paquete a su destinación final. EL ruteador entonces desecha el paquete original. Dos razones existen para que una destinación pueda ser inalcanzable. Lo más comúnmente posible, es que el anfitrión de la fuente ha especificado una dirección no existente. Con menos frecuencia, el ruteador no cuenta con una ruta a la destinación.

Los mensajes de Destinación inalcanzables incluyen cuatro tipos básicos: la red inalcanzable, anfitrión inalcanzable, el protocolo inalcanzable, y el puerto inalcanzable. los mensajes de Red inalcanzable significan generalmente que una falta ha ocurrido en el encaminamiento o la dirección de un paquete. los mensajes Anfitrión inalcanzables indican generalmente la falta de entrega, tal como una mascara de subred incorrecta. Los mensajes de Protocolo inalcanzables significan generalmente que la destinación no soporta el protocolo de la capa superior especificada en el paquete. Los mensajes de Puerto inalcanzables implican que el socket o el puerto del TCP no está disponible.

Un mensaje de ICMP de petición de eco, que es generado por el comando del Ping, es enviado por cualquier anfitrión para probar si el nodo es alcanzable a través de una red. El ICMP eco contesta el mensaje indicando que el nodo puede ser alcanzado con éxito.

Un mensaje de ICMP de redireccionamiento es enviado por el ruteador al anfitrión fuente para estimular un encaminamiento más eficiente. El ruteador todavía remite el paquete original a la destinación. El mensaje de

redireccionamiento de ICMP permite que las tablas de encaminamiento del anfitrión sigan siendo pequeñas porque es necesario saber la dirección de solamente un ruteador, incluso si este ruteador no proporciona la mejor trayectoria. Incluso después de recibir un mensaje de redireccionamiento de ICMP, algunos dispositivos pueden continuar usando la ruta menos eficiente.

Un mensaje de Tiempo excedido ICMP es enviado por el ruteador si el Tiempo de vida de un paquete de IP alcanza un cero (expresado en saltos o segundos). El tiempo de Vida evita que los paquetes circulen continuamente en la red si la red contiene un bucle de encaminamiento. El ruteador entonces desecha el paquete original.

### 2.5.2 ICMP Protocolo descubridor de Ruteadores (IDRP)

Los mensajes de Anuncio de ruteador y de Solicitación de Ruteador en las aplicaciones de IDRP se utiliza para descubrir las direcciones, en los ruteadores en subredes directamente unidas. Cada ruteador periódicamente, transmite Anuncios de Ruteador en cada una de sus interfaces. Los anfitriones entonces descubren direcciones de ruteadores en subredes directamente unidas escuchando estos mensajes. Los anfitriones pueden utilizar mensajes de Solicitación de Ruteador para más bien solicitar los anuncios inmediatos, que para esperar mensajes no solicitados.

IRDP ofrece varias ventajas sobre otros métodos de descubrir direcciones de ruteadores vecinos. Sobre todo, no requiere que los anfitriones reconozcan los protocolos de encaminamiento, ni requiere la configuración manual de un administrador.

Los mensajes de Anuncios de Ruteador permiten a los anfitriones descubrir la existencia de las ruteadores vecinos, pero no que el ruteador es la mejor trayectoria para alcanzar una destinación particular. Si un anfitrión utiliza un ruteador pobre de primero salto para alcanzar una destinación particular, recibe un mensaje de redireccionamiento que identifica una opción mejor.

## 2.6 Protocolo de Control de Transmisión (TCP)

El TCP proporciona una transmisión confiable de datos en un ambiente de IP. El TCP corresponde a la capa de transporte (capa 4) del MONDELO DE REFERENCIA OSI. Entre los servicios que el TCP proporciona están la transferencia de datos, la confiabilidad, el control de flujo eficiente, la operación full-duplex, y la multiplexión.

Con la transferencia de datos, el TCP entrega un flujo datos no estructurado de los octetos identificados por una secuencia de números. Este servicio beneficia en usos, porque no tienen que dividir los datos en bloques antes de detener el TCP. En ves de eso, TCP agrupa octetos en segmentos y los pasa al IP para la entrega.

El TCP ofrece confiabilidad proporcionando una entrega confiable en una conexión orientada punto a punto, del paquete en la red. Hace esto ordenando octetos con un número del reconocimiento de expedición que indique la destinación del octeto siguiente que la fuente espera recibir. Los octetos no reconocidos dentro de un período especificado se retransmiten. El mecanismo de la confiabilidad del TCP permite que los dispositivos traten el perdido, retraso, la duplicación, o los paquetes de la mala interpretación. Un mecanismo de temporalización permite que los dispositivos detecten los paquetes perdidos y que soliciten la retransmisión.

El TCP ofrece el control de flujo eficiente, que significa que, al enviar reconocimientos de nuevo a la fuente, el proceso de recepción del TCP indica el número de trama más alto que se puede recibir sin desbordar sus almacenadores intermedios internos.

La operación full-duplex significa que los procesos del TCP se pueden enviar y recibir al mismo tiempo.

Finalmente, la multiplexión de TCP significa que numerosas conversaciones simultáneas de la capa superior se pueden multiplexar sobre una sola conexión.

## 2.7 ¿Qué Es encaminamiento?

El encaminamiento es el acto de mover la información a través de una red de una fuente a una destinación. A lo largo de la red, por lo menos un nodo intermedio se encuentra. El encaminamiento se pone en contraste a menudo con la conmutación por puente, que pude parecerse para lograr la misma cosa a un observador ocasional. La diferencia primaria entre los dos es que la conmutación por puente ocurre en la capa 2 (la capa de acoplamiento) del MODELO DE REFERENCIA OSI, mientras que el encaminamiento ocurre en la capa 3 (la capa de red). Esta distinción provee al encaminamiento y a la conmutación por puente sobre diversa información en el uso en el proceso de mover la información desde la fuente a la destinación, así que las dos funciones logran sus tareas de diversas maneras.

El asunto del encaminamiento se ha cubierto en la literatura de la informática por más de dos décadas, pero el encaminamiento alcanzó renombre comercial a mediados de los años ochenta. La razón primaria de este retraso de tiempo es que las redes en los años 70 eran ambientes simples, homogéneos. Hace solamente relativamente poco tiempo la redes grandes llegaron a ser popular.

### 2.7.1 Componentes Del Encaminamiento

El encaminamiento implica dos actividades básicas: determinación de las trayectorias óptimas de encaminamiento y el transporte de los grupos de información (típicamente llamados paquetes) en una red. En el contexto del proceso de encaminamiento, el último de éstos se refiere como conmutación de conjunto de bits. Aunque la conmutación de conjunto de bits es relativamente directa, la determinación de la trayectoria puede ser muy compleja.

## 2.7.2 Determinación De la Trayectoria

Los protocolos de encaminamiento utilizan métricas para evaluar qué trayectoria será la mejor para que viaje un paquete. Una métrica es un estándar de medida, tal como el ancho de banda de la trayectoria, que es utilizada por algoritmos para encaminar y para determinar la trayectoria óptima a una destinación. Para ayudar al proceso de la determinación de trayectoria, los algoritmos de encaminamiento inicializan y mantienen las tablas de encaminamiento, que contienen la información de la ruta. La información de la ruta varía dependiendo del algoritmo de encaminamiento usado.

Los algoritmos de encaminamiento llenan las tablas de encaminamiento de una variedad de información. Las asociaciones de Destilación/ siguiente salto dicen al ruteador que una destinación particular pueda ser alcanzada óptimamente, enviando el paquete a un ruteador en particular, que representa el "salto siguiente" en la manera de la destinación final. Cuando un ruteador recibe un paquete entrante, comprueba la dirección de destinación y procura asociar esta dirección a un salto siguiente. El Figura 1-15 representa una tabla de encaminamiento de destilación/ siguiente salto

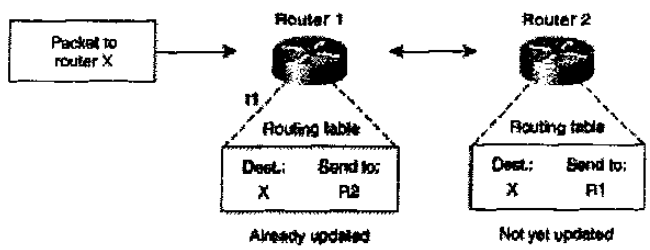



**Figura 2 - 15** Las asociaciones de destinación/ Siguiente salto determinan la trayectoria óptima de los datos

Las tablas de encaminamiento también pueden contener la otra información, tal como datos sobre la trayectoria mas deseable. Los ruteadores comparan métricas para determinar las rutas óptimas, y estas métricas se diferencian dependiendo del diseño del algoritmo de encaminamiento usado. Una

variedad de métricas común será introducida y descrita más adelante en este capítulo.

Los ruteadores se comunican el uno con el otro y mantienen sus tablas de encaminamiento a través de la transmisión de una variedad de mensajes. El mensaje de actualización de encaminamiento es un mensaje que consiste generalmente de toda o una porción de una tabla de encaminamiento. Analizando actualizaciones de encaminamiento el resto de los ruteadores, que pueden construir un Figura detallado de la topología de la red. Un anuncio de estado de enlace, es otro ejemplo de un mensaje enviado entre los ruteadores, que informa a otros ruteadores el estado de los enlaces del remitente. La información de enlace también se puede utilizar para construir un Figura completo de la topología de la red para permitir a los ruteadores determinar las rutas óptimas en las destinaciones de red.

### 2.7.3 Conmutación

Los algoritmos de Conmutación es relativamente simple; es igual para la mayoría de los protocolos de la encaminamiento. En la mayoría de los casos, un anfitrión para determinar como enviar un paquete a otro anfitrión, adquiere la dirección de un ruteador por algunos medios, el anfitrión fuente envía un paquete enviado específicamente a un ruteador de dirección física (capa de Control de Acceso al Medio [ MAC]), este a su vez con la dirección del protocolo (capa de red) del anfitrión de destinación.

Pues examina la dirección del protocolo de la destinación del paquete, el ruteador se determina que sabe o no sabe remitir el paquete al salto siguiente. Si el ruteador no sabe remitir el paquete, cae típicamente el paquete. Si el ruteador sabe remitir el paquete, sin embargo, cambia la dirección física de la destinación al salto siguiente y transmite el paquete.

El salto siguiente puede ser el último anfitrión de destinación. Si no, el salto siguiente es generalmente otro ruteador, que ejecuta el mismo proceso de decisión de conmutación. Mientras que el paquete se mueve en la red, su

dirección física cambia, solamente su constante es la dirección de protocolo, según lo ilustrado en el Figura 5-16.

La discusión precedente describe el cambiar entre una fuente y un sistema extremo de destinación. La Organización Internacional de Estándares (ISO) ha desarrollado una terminología jerárquica que es útil en describir este proceso. Usando esta terminología, los dispositivos de red tienen la capacidad para remitir los paquetes entre las subredes y se llaman *sistemas de extremos (ES's),* mientras que los dispositivos de red con estas capacidades se llaman *sistemas intermedios (IS's)* . Los IS's se dividen más a fondo en los que pueden comunicarse dentro de los dominios de encaminamiento ( los *IS del intradominio* ) y los que comunican a ambos en y entre los dominios de encaminamiento (*IS's de interdominio* ). Un dominio de encaminamiento generalmente se considera una porción de una red bajo autoridad administrativa común que es regulada por un sistema particular de pautas administrativas. Los dominios de encaminamiento también se llaman sistemas autónomos. Con ciertos protocolos, encaminamientos de dominios se puede dividir en áreas de encaminamiento, pero los protocolos de encaminamiento de intradominio todavía se utilizan para transmitir en y entre áreas.

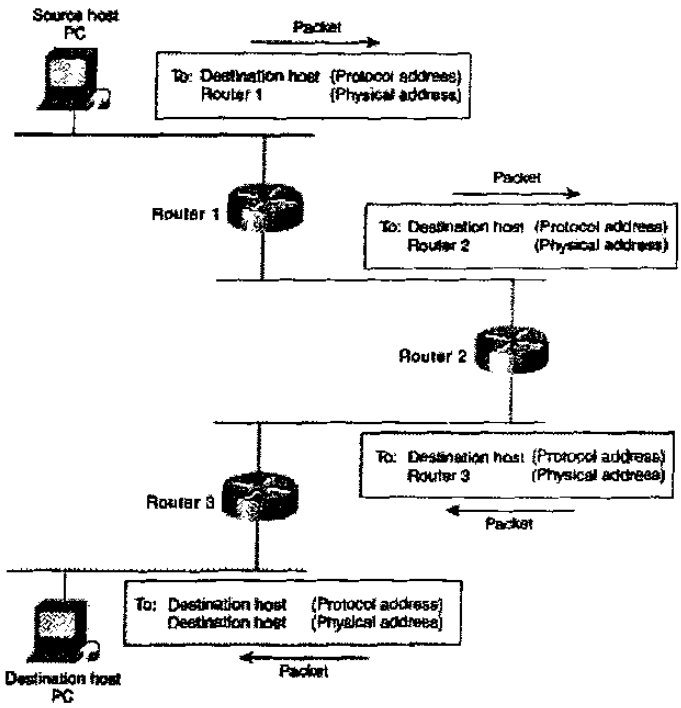



**Figura 2 - 16** Numerosos ruteadores pueden entrar en funciones durante el proceso de la Conmutación

## 2.7.4 Algoritmos De Encaminamiento

Los algoritmos de encaminamiento se pueden distinguir basándose en varias características dominantes. Primero, las metas particulares del diseñador del algoritmo afectan la operación del protocolo de la encaminamiento que resulta. En segundo lugar, varios tipos de algoritmos de encaminamiento existen, y cada algoritmo tiene un diverso impacto en los recursos de la red y del ruteador. Finalmente, los algoritmos de encaminando utilizan una variedad de métricas que afecten el cálculo de rutas óptimas.

### 2.7.4.1 Metas Del Diseño

Los algoritmos de encaminamiento tienen a menudo una o más, de las metas de diseño siguientes:

- Optimización
- Simplicidad y gastos indirectos bajos
- Robustez y estabilidad
- Convergencia rápida
- Flexibilidad

La Optimización refiere a la capacidad del algoritmo de encaminamiento para seleccionar la mejor ruta, que depende de la métrica y del peso de las métricas usadas para hacer el cálculo. Por ejemplo, un algoritmo de encaminamiento puede utilizar un número de saltos y pausas, pero puede tener pausas más pesadas en el cálculo. Naturalmente, los protocolos encaminamiento debe definir sus algoritmos métricos del cálculo terminantemente.

Los algoritmos de encaminamiento también se diseñan para ser tan simples como sea posible. Es decir el algoritmo de encaminamiento debe ofrecer una funcionalidad eficientemente, con un mínimo de software y de utilización. La eficacia es particularmente importante cuando el software que pone el algoritmo de encaminamiento en ejecución debe funcionar en una computadora con recursos físicos limitados.

Los algoritmos de encaminamiento deben ser *robustos* , que significa que él debe de encarar y realizar correctamente sus funciones, adentro de circunstancias inusuales o imprevistas, tales como fallas de hardware, condiciones de cargas altas, e implementaciones incorrectas. Porque los ruteadores están situados en los puntos centrales de la red, y pueden causar problemas considerables cuando fallan. Los mejores algoritmos de encaminamiento son a menudo los que han

soportado la prueba del tiempo y que han probado su estabilidad bajo una variedad de condiciones de red.

Además, los algoritmos de encaminamiento deben converger rápidamente. La convergencia es el proceso de poner de acuerdo a todos los ruteadores, en las rutas óptimas. Cuando sucede un acontecimiento en la red que causa que las rutas se caigan o se hagan indisponibles, los ruteadores distribuyen los mensajes de actualización de encaminamiento en las redes involucradas, estimulando el recálculo de rutas óptimas y haciendo eventualmente que todas los ruteadores convengan en estas rutas. Los algoritmos de encaminamiento que convergen lentamente pueden causar bucles de encaminamiento o interrupciones de la red.
En el bucle de encaminamiento exhibido en el Figura 5-17, un paquete llega al ruteador 1, el ruteador 1 del T1 del tiempo se ha puesto al día ya se sabe así que la ruta óptima a la destinación es llamada para el ruteador 2 para ser la parada siguiente. El ruteador 1 por lo tanto remite el paquete al ruteador 2, pero porque este ruteador todavía no se ha puesto al día, se cree que el salto siguiente óptimo es el ruteador 1. El ruteador 2 por lo tanto remite el paquete de nuevo al ruteador 1, y el paquete continúa transmitiéndose hacia atrás entre los dos ruteadores hasta que el ruteador 2 recibe su actualización de encaminamiento o hasta que el paquete se ha pasado del tiempo de espera permitido.

| To reach network: | Send to: |
|---|---|
| 27 | Node A |
| 57 | Node B |
| 17 | Node C |
| 24 | Node A |
| 52 | Node A |
| 16 | Node B |
| 26 | Node A |
| . . . | . . . |

**Figura 2 - 17** Los bucles lentos de convergencia y de encaminamiento pueden obstaculizar progreso

Los algoritmos de encaminamiento deben también ser flexibles, que significa que él debe adaptarse rápidamente y exactamente a una variedad de circunstancias de red. Asuma, por ejemplo, que ha ido de un segmento de red abajo, tantos como que los algoritmos de encaminamiento son enterados del problema, ellos seleccionarán rápidamente la trayectoria más conveniente a ese segmento. Los algoritmos de encaminamiento se pueden programar para adaptarse a los cambios en la ancho de banda de la red, el tamaño de la cola del ruteador, y la retraso de red , entre otras variables.

## 2.7.4.2 Tipos de Algoritmos

Los algoritmos de encaminamiento se pueden clasificar por el tipo. Las diferencias dominantes incluyen éstas:

- Estático contra Dinámico
- Unicamino contra caminos múltiples
- Plano contra jerárquico
- Huéspedes inteligentes contra ruteadores inteligentes.
- Intra dominio contra ínter dominio.
- Estado de enlace contra Vector de Distancia

### 2.7.4.2.1 Estático Contra Dinámico

Los algoritmos estáticos de encaminamiento son apenas algoritmos del todo, pero son mapas de la tabla establecidos por el administrador de red desde el principio del encaminamiento. Estos mapas no cambian a menos que el administrador de red los altere. Los algoritmos que utilizan las rutas estáticas son simples de diseñar y trabajar bien en ambientes donde es relativamente fiable el tráfico de red y donde es relativamente simple el diseño de la red.

Porque los sistemas estáticos de encaminamiento no pueden reaccionar a los cambios de la red, generalmente se consideran inadecuados para las redes grandes, que constantemente cambian. La mayoría de los algoritmos dominantes de encaminamiento en la actualidad son los algoritmos dinámicos de encaminamiento, que se ajustan a las circunstancias de red cambiantes, analizando mensajes entrantes de actualización de encaminamiento. Si el mensaje indica que ha ocurrido un cambio en la red, el software de encaminamiento recalcula las rutas y envía nuevos mensajes de actualización de encaminamiento. Estos mensajes impregnan la red, estimulando los ruteadores para volver a efectuar sus algoritmos y para cambiar sus tablas de encaminamiento por consiguiente.

Los algoritmos dinámicos de encaminamiento se pueden suplir con las rutas estáticas cuando sea apropiado. Un ruteador de ultimo recurso (un ruteador al cual se envían todos los paquetes no encaminables), por ejemplo, se puede señalar para actuar como depósito para todos los paquetes encaminables, asegurándose de que todos los mensajes están manejados por lo menos de una cierta manera.

### 2.7.4.2 Unicamino contra caminos múltiples

Algunos protocolos sofisticados de encaminamiento apoyan las trayectorias múltiples a la misma destinación. De distinta manera de los algoritmos de Unicamino, estos algoritmos multidireccionales permiten el tráfico y se multiplexan en líneas múltiples excesivas. Las ventajas de algoritmos multidireccionales son obvias: Pueden proporcionar un rendimiento de procesamiento y una confiabilidad substancialmente mejores. Esto se llama generalmente el compartir carga.

### 2.7.4.3 Plano contra jerárquico

Algunos algoritmos de encaminamiento funcionan en un espacio plano, mientras que otros utilizan encaminamiento por jerarquías. En un sistema plano de encaminamiento, los ruteadores son punto a punto de todos los demás. En un sistema del encaminamiento jerárquico, la forma en que algunas ruteadores que forman una espina dorsal de encaminamiento (backbone). Los paquetes de los ruteadores que no pertenecen a la espina dorsal viajan a los ruteadores de la espina dorsal (backbone), donde se envían a través de la espina dorsal hasta que alcanzan el área general de destinación. En este punto, viajan de los ruteadores pasando de la espina dorsal a través de uno o más ruteadores que no pertenecen al backbone hasta la destinación final.

Los sistemas de encaminamiento señalan a menudo los grupos lógicos de nodos, llamados dominios, de sistemas autónomos, o de áreas. En sistemas jerárquicos, algunos ruteadores en un dominio pueden comunicarse con los ruteadores en otros dominios, mientras que otros pueden comunicarse solamente con los ruteadores dentro de su dominio. En redes muy grandes, los niveles jerárquicos adicionales pueden existir, con los ruteadores en el nivel jerárquico más alto que forma la espina dorsal de encaminamiento.

La ventaja primaria del ruteo jerárquico es que mimetiza la organización de la mayoría de las compañías y por lo tanto apoya sus patrones de tráfico bien. La

mayoría de la comunicación de red ocurre dentro de los grupos de compañías pequeñas (dominios). Porque los ruteadores de interdominio necesitan saber solamente sobre otros ruteadores dentro de su dominio, sus algoritmos de encaminamiento pueden ser simplificados, dependiendo del algoritmo de encaminamiento que es utilizado, el tráfico de actualización de encaminamiento se puede reducir por consiguiente.

### 2.7.4.4 Huéspedes inteligentes contra ruteadores inteligentes.

Algunos algoritmos de encaminamiento asumen que el nodo del final de la fuente determinará la ruta entera. Esto se refiere generalmente como encaminamiento de fuente. En sistemas de encaminamiento fuente, los ruteadores actúan simplemente como dispositivos de colocación y transmisión, enviando el paquete a la parada siguiente.

Otros algoritmos asumen que los anfitriones no saben nada sobre las rutas. En estos algoritmos, los ruteadores determinan la trayectoria con la red basada en sus propios cálculos. En el primer sistema, los anfitriones tienen la inteligencia de encaminamiento

### 2.7.4.5 Intradominio Contra Ínter Dominio.

Algunos algoritmos de encaminamiento trabajan solamente dentro de dominios; otros trabajan en y entre dominios. La naturaleza de estos dos tipos de algoritmos es diferente. Está parada para razonar, por lo tanto, que un algoritmo óptimo de intradominio de encaminamiento no sería necesariamente un algoritmo óptimo de encaminamiento de interdominio.

### 2.7.4.6 Estado de enlace contra Vector de Distancia

Los algoritmos de estado de enlace (también conocidos como algoritmos de primer trayectoria más corta) se involucran en la información de encaminamiento a todos los nodos en la red. Cada ruteador, sin embargo, envía solamente la porción de la tabla de encaminamiento que describe el estado de sus propios enlaces. En algoritmos de estado de enlace, cada ruteador construye una pictografía de la red entera en sus tablas de encaminamiento. Los algoritmos de vector de distancia (también conocidos como algoritmos de Bellman-Ford) llaman a cada ruteador para que envíe toda o una cierta porción de su tabla de encaminamiento, pero solamente a sus vecinos. Esencialmente, los algoritmos de estado de enlace envían actualizaciones pequeñas por todas partes, mientras que los algoritmos de vector de distancia envían actualizaciones más grandes solamente a las ruteadores vecinos. Los algoritmos del vector de distancia saben solamente sobre sus vecinos.

Porque convergen más rápidamente, los algoritmos de estado de enlace son algo menos propensos a los bucles de encaminamiento que los algoritmos del vector de distancia. Por otra parte, los algoritmos de estado enlace- requieren más energía y memoria del CPU que algoritmos del vector de distancia. los algoritmos del estado de enlace, por lo tanto, pueden ser más costosos en implementar y soportar. Los protocolos de estado de Enlace que son generalmente más escalables que los protocolos de vector de distancia.

## 2.7.5 Métricas de Encaminamiento

Las tablas de encaminamiento contienen la información usada para conmutar y seleccionar la mejor ruta. ¿Pero cómo, las tablas de encaminamiento se construyen específicamente? ¿Cuál es la naturaleza específica de la información que contiene? ¿Cómo los algoritmos de encaminamiento determinan que una ruta es preferible a otras?

Los algoritmos de encaminamiento han utilizado muchas métricas para determinar la mejor ruta. Los algoritmos sofisticados de encaminamiento pueden basar la selección de ruta en la métrica múltiple, combinándola en una sola métrica (híbrida). Se han utilizado todas las métricas siguientes:

- Longitud de trayectoria
- Confiabilidad
- Retardo
- Ancho de Banda
- Carga
- Costos de Comunicación

La longitud de trayectoria es la métrica más común de encaminamiento. Algunos protocolos de encaminamiento permiten que los administradores de red asignen costos arbitrarios a cada enlace de red. En este caso, la longitud de trayectoria es la suma de los costos asociados a cada enlace. Otros protocolos de encaminamiento definen la cuenta de los saltos, una métrica que especifica el número de pasos a través de dispositivos de red, tales como ruteadores, que un paquete debe tomar de camino desde una fuente a una destinación.

La confiabilidad, en el contexto de los algoritmos de encaminamiento, se refiere a la formalidad (descrita generalmente en los términos del rango del bit-error) de cada enlace de red. Algunos enlaces de red pudieran caerse más a menudo que otros. Después de que una red falle, ciertos enlaces de red se pudieran reparar más fácilmente o más rápidamente que otros enlaces. Cualquier factor de confiabilidad se puede considerar como la asignación de los grados de confiabilidad, que son valores numéricos arbitrarios asignados generalmente a los enlaces de red por los administradores de red.

El retraso de encaminamiento se refiere a la cantidad del tiempo requerido para mover un paquete desde la fuente a la destinación con la red interna. El

retraso depende de muchos factores, incluyendo el ancho de banda de la red del enlace, el puerto hace una cola en cada ruteador de manera que, crea congestión de red en todos los enlaces de red, y de la distancia física de transmisión. Porque el retraso es una conglomeración de varias variables importantes, es una métrica común y útil.

El ancho de banda se refiere a la capacidad disponible del tráfico de un enlace. En igualdad de circunstancias, un enlace de Ethernet 10-Mbps sería preferible a una línea arrendada de 64-kbps. Aunque el ancho de banda es un grado de rendimiento de procesamiento alcanzable máximo en un enlace, las rutas con enlaces con mayor ancho de banda no proporcionan necesariamente rutas mejores que las rutas con enlaces más lentos. Por ejemplo, si un enlace más rápido está más ocupado, el tiempo real requerido para enviar un paquete a la destinación podría ser mayor.

La carga se refiere al grado a el cual un recurso de red, tal como un ruteador, está ocupado. La carga se puede calcular en una variedad de maneras, incluyendo la utilización del CPU y los paquetes procesados por segundo. La supervisión de estos parámetros sobre una base continua puede ser recurso intensivo por sí mismo.

El costo de la comunicación es otra métrica importante, especialmente porque algunas compañías pueden no cuidar sobre funcionamiento tanto como cuidan sobre gastos de funcionamiento. Aunque el retraso de línea puede ser más larga, ellos enviará excedente de los paquetes sus propias líneas más bien que a través de las líneas públicas que cuestan el dinero por tiempo de uso.

## 2.7.6 Protocolos de Red

Los protocolos encaminados son transportados por protocolos de encaminamiento a través de una red. En general los protocolos encaminados, en este contexto también se refiere como protocolos de red. Estos protocolos de red realizan una variedad de funciones requeridas para la comunicación entre las aplicaciones de usuario, entre los dispositivos de fuente y de destinación, y estas funciones pueden diferenciarse extensamente entre los protocolo. Los protocolos de red ocurren en las cinco capas superiores del MODELO DE REFERENCIA OSI: la capa de red, la capa de transporte, la capa de sesión, la capa de presentación, y la capa de Aplicación.

La confusión sobre los términos protocolo encaminado y protocolo de encaminamiento es común. Los protocolos encaminados son los protocolos que se encaminan sobre una red interna. Por ejemplos como los protocolos Internet Protocol (IP), DECnet, Appletalk, Novell NetWare, OSI, VIDES de Banyan, y el Xerox Network System (XNS). El protocolo encaminamiento, por otra parte, son los protocolos que implementan algoritmos de encaminamiento. Puesto que simplemente, los protocolos de encaminamiento son utilizados por los sistemas intermedios para construir las tablas usadas en la determinación y selección de trayectorias de protocolos encaminados. Los ejemplos de estos protocolos incluyen el protocolo interior de la encaminamiento de puerta de enlace (IGRP), el protocolo interior mejorado de encaminamiento de puerta de enlace (IGRP mejorado), la primera trayectoria más corta abierta (OSPF), Los Protocolos de Puertas de Enlace Exteriores (EGP), el Protocolo de Puerta de enlace de Frontera (BGP), Sistema intermedio – Sistema intermedio (IS-IS), y el Protocolo de Encaminamiento de Información (RIP).

# Conclusiones

Como pudimos observar el encaminamiento existe y se debe e diversas causas y estándares que se explicaron brevemente en este capitulo, ahora podemos diferenciar con exactitud como trabajan los protocolos de encaminamiento y que información manejan para que la información llegue de la fuente a su destino, dado que los protocolos TCP/IP, son los protocolos generalmente usados para estas labores, que en conjunción con los protocolos de encaminamiento nos muestran un panorama claro de que es una red con protocolos de encaminamientos implementados, así como también podemos ver que entre mas grande sea la red, mas cuidado hay que tener al seleccionar el tipo de protocolos , tratando de lograr los objetivos de simplicidad y optimización, pudimos observar que para los protocolos de vector de distancia son ideales para redes pequeñas pero la naturaleza de sus algoritmos se complica al implementarlos en una red grande y complicada, para estos casos podemos ver que protocolos como OSPF, son los que llevan la delantera en funcionabilidad y tecnología.

# CAPITULO 3

# OSPF

## 3.1 OSPF (La Primera Trayectoria Más Corta Abierta)

OSPF (Open Short Firt Path) es un protocolo de encaminamiento de estado de enlace. Se diseño para ser de funcionamiento interno en solo Sistema Autónomo. Cada Ruteador de OSPF mantiene una base de datos idéntica que describe la topología del sistema autónomo. De esta base de datos, una tabla de encaminamiento es calculada construyendo un camino más corto de trayectoria.

OSPF recalcula las rutas rápidamente cuando encara cambios topológicos, utilizando un mínimo de tráfico de protocolo de encaminamiento. OSPF proporciona ayuda para la repartición equitativa de costos multidireccionales. Se proporciona una capacidad de encaminamiento de área, permitiendo un nivel adicional de protección de encaminamiento y de una reducción en el tráfico de

protocolo de encaminamiento. Además, se autentifican todos los intercambios del protocolo de encaminamiento de OSPF.

OSPF se clasifica como Protocolo de Puerta de Enlace Interior (IGP). Esto significa que distribuye la información de encaminamiento entre los ruteadores que pertenecen a un solo Sistema Autónomo. El protocolo OSPF se basa en un protocolo de estado de enlace o tecnología de SPF. Esto es, una variación con los en base a Bellman-Ford usado por protocolos tradicionales de encaminamiento del Internet de TCP/IP. El protocolo de OSPF fue desarrollado por el grupo de trabajo de OSPF del Internet Engineering Task Force. Se ha diseñado expresamente para el ambiente del Internet de TCP/IP, incluyendo para ayudar explícitamente al CIDR y marcar una etiqueta a la información de encaminamiento externa derivada. OSPF también prevé la autentificación de las actualizaciones de encaminamiento, y utiliza la multitransmisión (multicast) de IP cuando transmite y recibe las actualizaciones. Además, mucho trabajo se ha hecho para producir un protocolo que responda rápidamente a los cambios de la topología, todo esto implica cantidades pequeñas de tráfico del protocolo de encaminamiento.

La publicación de la versión 1 de OSPF, fue publicada como Request For Comments (RFC) 1131 en octubre de 1989 por Juan T. Mayo y el grupo de trabajo de OSPF. OSPF hizo uso el algoritmo famoso de Dijkstra. Este algoritmo no era nuevo y no había sido creado específicamente para llenar la demanda de la comunidad establecida en una red. ¡En realidad, este fórmula matemática fue creada inicialmente para ser mostrado en la computadora de ARMAC en 1956, hace mas de 30 años antes de que el OSPF era considerado!

Edsger W. Dilkstra nació en 1930 en la ciudad de Rotterdam en los Países Bajos. Encontrándose en una familia orientada a la ciencia, él sobresalió y alcanzó rápidamente su Ph.D. en informática en 1959 de la universidad de Amsterdam, Holanda. Para el momento en que él tenia 32 años, él había

alcanzado un profesorado en matemáticas en la Universidad de Eindhoven. Su logro sigue siendo extremadamente impresionante hasta la actualidad.

Su contribución recordada al mundo de las computadoras, son sus algoritmos, específicamente el algoritmo de la trayectoria más corta. Dilkstra no consideraba su algoritmo muy notable en ese entonces, y hasta años después de que él lo publicara. Hoy, su algoritmo se está aplicando a la edificación de caminos, a el encaminamiento de comunicaciones, y en la industria de la líneas aéreas. Su algoritmo incluso fue alterado levemente para determinar la manera más barata de enlazar con cables una computadora. La meta común más conocida del algoritmo Dijkstra es encontrar la ruta más corta entre dos puntos.

La meta del algoritmo de la trayectoria más corta de Edsger Dijkstra es encontrar la ruta más corta entre dos puntos con una serie. Para describir la operación de su algoritmo en los términos del claros, mire el ejemplo siguiente. Suponga que usted está intentando encontrar la trayectoria más corta entre dos ciudades: Atlanta y Boston (un sistema base de ruteadores). El propósito en este ejemplo es determinar el tiempo mínimo necesario para conducir a cada ciudad (ruteador) en una base expandida de ciudades (red). La secuencia para encontrar este valor mínimo de tiempo es como sigue:

1. Comience en la ciudad de origen (ruteador). El tiempo (distancia) necesitó para alcanzar esta ciudad es, por supuesto, cero porque es su origen.

2. Entonces usted descubre una ciudad nueva, que usted llamará la ciudad X (ruteador), que usted desea alcanzar.

    - Si el tiempo de conducir (distancia) a la ciudad X es más corto que el tiempo de conducir a cualquier otra ciudad fuera del sistema base.

- Si el tiempo de conducir a la ciudad X es el tiempo mínima de conducir a la ciudad Y en la base fijada de Atlanta, más el tiempo de conducir de Y a X.

3. Entonces agregue la ciudad X al sistema de la base (red), y registre el tiempo es computado (distancia)

4. Si es una ciudad es llamada Boston entonces listo, si no, se repite.

Este ejemplo ayuda a demostrar la razón detrás del nombre del algoritmo. Otro factor importante en su operación es cómo converge el SPF. Esencialmente, convergerá en iteraciones de 0(M.log M), donde está el número M de enlaces. Esto es superior al algoritmo del Bellman-Ford, que convergen en 0(N.M) las iteraciones donde N, es el número de nodos.

Estas características y porque la especificación fue desarrollada en una manera abierta por el IETF explican el nombre del protocolo OSPF " la primera trayectoria más corta abierto ". También, el protocolo de OSPF es un estándar abierto que permite la publicación de todos los datos referente a su diseño y función. Esta información se ha publicado en una serie de RFCs.

OSPF encamina los paquetes de IP basados solamente en la Dirección IP de destinación encontrada en el encabezado del paquete de IP. Se encaminan los paquetes de IP "como son" -- no se encapsulan en cualquier otro encabezado de otro protocolo como para transitar en el Sistema Autónomo. El OSPF es un protocolo dinámico de encaminamiento. Detecta rápidamente cambios topológicos en el AS (por ejemplo las fallas de interfaz del ruteador) y calcula las rutas libres de bucles, nuevas después del período de la convergencia. Este período de convergencia es de cortocircuito e implica un mínimo de tráfico de encaminamiento. En un protocolo de encaminamiento de estado de enlace, cada

ruteador mantiene una base de datos que describe la topología del sistema autónomo. Esta base de datos se refiere como la base de datos de estado de enlace. Cada ruteador participa y tiene una base de datos idéntica. Cada fragmento individual de esta base de datos es el estado local de un ruteador en particular (por ejemplo, las interfaces activas y los vecinos accesibles del ruteador) Los ruteadores distribuyen su estado local a través del Sistema Autónomo por flooding (inundamiento de avisos).

Todos los ruteadores ejecutan exactamente el mismo algoritmo, en paralelo. La base de datos de estado de enlace, de cada ruteador construye un árbol de las trayectorias más cortas consigo mismo como raíz. Este árbol de trayectorias cortas da ruta a cada destinación en el Sistema Autónomo. La información de encaminamiento externamente derivada aparece en el árbol como va.

Cuando existen varias rutas de igual costo a una destinación, el tráfico se distribuye igualmente entre ellos. El costo de una ruta es descrito por una sola métrica sin dimensiones.

OSPF permite que los sistemas de redes sean agrupados juntos. Tal agrupamiento se llama área. La topología de un área se oculta del resto del Sistema Autónomo. El este ocultar de la información permite una reducción significativa en tráfico de la encaminamiento. También, encaminando dentro del área es determinado solamente por propia topología del área, prestando la protección del área contra malos datos de la encaminamiento. Un área es una generalización de un IP segmentar la red.

OSPF permite la configuración flexible de las Subredes de IP. Cada ruta distribuida por OSPF tiene una destinación y una máscara. Dos diversas Subredes del mismo número de red de IP pueden tener diversos tamaños (es decir, diversas máscaras) Esto se refiere comúnmente como mascara de subred de longitud variable. Un paquete se encamina mejor (es decir, lo más largo posible o más

específico) Las rutas del anfitrión se consideran ser las subredes y las máscaras son "de difusión" (0xffffffff). Se autentifican todos los intercambios del protocolo de OSPF. Esto significa que solamente los rutedores confinados en el AS pueden participar en la encaminamiento del sistema autónomo. Una variedad de esquemas de autentificación pueden ser utilizados. De hecho, los esquemas separados de autentificación se pueden configurar para cada subred de IP. El encaminamiento externamente derivando de datos (Por ejemplo, las rutas se pueden aprender de un Protocolo de Puerta de Enlace Exterior tal como BGP; vea que [ Ref23 ]) se anuncia a través del Sistema Autónomo. Estos datos externamente derivados se guardan a parte de los datos del protocolo de estado de enlace de OSPF. Cada ruta externa se puede también marcar con etiqueta por el ruteador de publicidad, permitiendo pasar la información adicional entre los Ruteadores de Frontera del Sistema Autónomo.

### 3.1.1 Breve Historia de la Tecnología de Encaminamiento de Estado de Enlace

OSPF es un protocolo de encaminamiento de estado de enlace. Tales protocolos también se refieren en la literatura como protocolos basados en SPF o de base de datos distribuidos. Esta sección da una breve descripción de los progresos en la tecnología de estado de enlace que han influenciado el protocolo de OSPF. El primer protocolo de encaminamiento de estado de enlace fue desarrollado para el uso de la red de conmutación de conjunto de bits de ARPANET. Este protocolo se describe adentro de [ Ref3 ]. Esto ha formado el punto de partida para el resto de los protocolos de estado de enlace. El ambiente homogéneo de ARPANET, es decir, los conmutadores de paquete solo comerciales conectados por las líneas seriales síncronas, simplifican el diseño y la implementación del protocolo original. Las modificaciones a este protocolo fueron

propuestas adentro de [ Ref4 ]. Estas modificaciones se repartieron con el aumento de la tolerancia de fallas del protocolo de encaminamiento, entre otras cosas, agregando en suma una comprobación al LSAs (de tal modo que detecta la corrupción de la base de datos). El papel también incluyó los medios para reducir los gastos indirectos del tráfico de encaminamiento en un protocolo de estado de enlace. Esto fue logrado introduciendo los mecanismos que permitieron un intervalo entre los transmisores de los LSA para ser aumentados en una orden de la magnitud. El protocolo incluye los métodos para la reducción el tráfico de datos y de encaminamiento al trabajar en redes excesivas de difusión. Esto es logrado por la elección de un un ruteador designado, para cada red de difusión, que entonces origina un LSA para la red.

El grupo de trabajo de OSPF del IETF ha extendido este trabajo para desarrollar el protocolo de OSPF. El concepto señalado del ruteador se ha realzado grandemente para reducir más la cantidad de tráfico de encaminamiento requerido. Las capacidades de la multitransmisión se utilizan para la reducción adicional del ancho de banda de encaminamiento. Se ha desarrollado un esquema de encaminamiento de área permitiendo que la información se oculte /proteja /reduzca. Finalmente, los algoritmos se han adaptado para la operación eficiente en interedes de TCP/IP

## 3.2 Ambiente Funcional del OSPF

Esta sección describe las características básicas y las características del ambiente funcional de OSPF. El ambiente en el cual OSPF funciona es definido por las características de su operación y de diseño. Puesto simplemente, que el ambiente funcional de OSPF define pues la arquitectura de red, en la cual el protocolo funcionará correctamente.

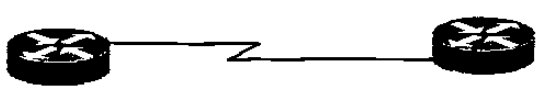
El RFC 1793 proporciona un ejemplo que trata la extensión de OSPF para tener la capacidad de funcionar dentro de circuitos basados en demanda. Hasta que este el RFC fue publicado e implementado, OSPF no funcionó correctamente al ocuparse de tales circuitos de ISDN. Ahora que el protocolo se ha ajustado para funcionar correctamente cuando trata circuitos basados en demanda, usted puede decir que el ambiente funcional del protocolo se ha mejorado.

Con ese ejemplo en mente, aquí se presentan los tres tipos de red que OSPF reconoce.

### 3.2.1 Tipos de Redes en OSPF

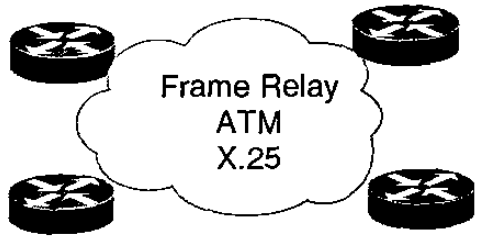
La figura 3-1 ilustra los tres diversos tipos de la red dentro de los cuales OSPF funciona.

La lista siguiente explica las características físicas de los tipos de red de OSPF ilustrados en la figura 3-1:



Punto a Punto

Multiacceso




Multiacceso de no Difusión (NBMA)

**Figura 3 - 1** Tipos de Red en OSPF

Punto a Punto. Un solo circuito que conecta dos ruteadores de OSPF, que permitirán que una sola relación vecina sea construida.

Multiacceso: Un circuito que tiene por lo menos dos ruteadores de OSPF conectados con él y les permite comunicarse uno a otro. Esto proporciona el potencial para las relaciones vecinas múltiples y para ser formadas las adyacencias, pero de prevenir esto, un ruteador designado como (DR) construye todas las adyacencias y las distribuye hacia fuera a todos los ruteadores conectados.

## 3.2.2 Redes de Multiacceso de no Difusión

En un medio de Multiacceso de no Difusión (NBMA) Las redes de NBMA son muy similares a las redes de multiacceso, con la excepción que no permiten el tráfico de difusión (por ejemplo, X.25) Las redes de NBMA también tienen el potencial para las adyacencias múltiples, pero los circuitos virtuales pueden no conectar todos los ruteadores. En algunos casos, esto requeriría que las adyacencias sean configuradas manualmente.

El estándar de ITU-T define cómo las conexiones entre el DTE y el DCE son de acceso mantenido por la terminal remota y las comunicaciones de la computadora en PDNs. X.25 especifica LAPB, un protocolo de capa del enlace de datos, y PLP, un protocolo de capa de red.

Si usted se preguntara por las redes punto Multipunto el RFC de OSPF lo explica mejor: en una de dos redes grandes de modos de no difusión. El primer modo, llamado de no difusión, de multiacceso o NBMA, simula la operación de OSPF en una red de difusión. El otro modo, llamado punto a multipunto, trata la red de no difusión como enlaces colectivos de un punto a punto Las redes de no difusión se refieren como red de NBMA

### 3.2.3 Identificación De Ruteador

Cada ruteador que funciona en OSPF dentro de una red debe tener una identificación única de ruteador. Éste es el número de ficción que es de 32-bit, un número con el cual se identifica un ruteador de otro, en el Sistema Autónomo (AS). La identificación del ruteador es utilizada por la base de datos de estado de enlace de OSPF (como método a seguir para cada ruteador en el AS y la asociación de los enlaces a él)

Este número de identificación es único en cada ruteador de OSPF. Para asignar la identificación del ruteador, OSPF utiliza el método por defecto de determinar la dirección más alta de las interfaces activas del ruteador.

El otro método implica manualmente el asignar el número de identificación del ruteador, configurando una dirección de loopback en el ruteador Cisco. Este método tiene la ventaja de ser mucho más estable, que el método por defecto porque una dirección de loopback no puede caerse o perder la conectividad, que daría lugar a la necesidad de poner al día las tablas de encaminamiento

Los ruteadores marca Cisco actualmente tienen un nuevo comando para permitir explícitamente el ajuste de la identificación del ruteador.

La configuración de una dirección del loopback como la identificación del ruteador de OSPF tiene una ventaja muy significativa en su estabilidad. La interfaz es esencialmente una interfase basada en software que se puede utilizar para muchos propósitos adicionales tales como resumir rangos de Direcciones IP o localización de averías. Son accesibles, con tal que caigan dentro de la categoría de anunciación de Direcciones de IP.

Al configurar la Dirección de IP para su interfaz de loopback, tenga presente que no debe ser una dirección IP "verdadera", que utiliza un espacio de dirección valioso. La alternativa es utilizar una Dirección de IP "falsa", que es esencialmente una Dirección IP hecha que no es parte del rango normal de Direcciones IP de su red. El RFC 1597 pude ser un buen lugar para comenzar si usted decide utilizar este método de hacer que el primer octeto dure.

### 3.2.4 Vecinos

OSPF considera que dos ruteadores tengan una interfaz situada en una red común como vecinos. Cuando OSPF descubre a sus vecinos, éste es el primer paso de descubrir la red y de construir una tabla de encaminamiento. Este proceso comienza por el ruteador que aprende los números de identificación de los ruteadores. En redes de multiacceso, el protocolo de OSPF descubre a estos vecinos dinámicamente mediante los Hellos, que serán discutidos más tarde.

Para construir las relaciones de vecinos estables de OSPF, asegúrese de que el número de ruteadores por LAN sea pequeño. Utilice el comando de prioridad para organizar quien es el DR y de evitar de tener el mismo ruteador de DR para más de un enlace, con el uso del comando de prioridad de OSPF.

### 3.2.5 Adyacencias

Para las adyacencias, OSPF debe primero haber descubierto a sus vecinos. Las adyacencias se forman con el fin de intercambiar información de encaminamiento. No cada ruteador vecino formaría una adyacencia. Las seis condiciones bajo las cuales el OSPF formará adyacencias son las siguientes:

- La conectividad de la red es punto a punto
- El Ruteador es el Ruteador Designado (DR)
- El Ruteador vecino es el Ruteador Designado (DR)
- El Ruteador es el ruteador DR de respaldo
- El Ruteador vecino es el ruteador DR de respaldo

Las adyacencias controlan la distribución de las actualizaciones de encaminamiento en el sentido de que solamente los ruteadores adyacentes a este solo envían actualizaciones y las procesan.

### 3.3.6 Ruteadores Designados

OSPF construye adyacencias entre los ruteadores para propósitos de intercambiar la información de encaminamiento. Cuando OSPF tiene que ocuparse de ambientes de multiacceso de no difusión (NBMA) o redes de Difusión, sin embargo, estos representan un problema en sí mismo. En estos

tipos de redes, existen ruteadores múltiples, que darían lugar enteramente también a muchas adyacencias. Para combatir adyacencias superfluas el ruteador designado es introducido.

OSPF señalará un solo ruteador por red de multiacceso para construir adyacencias entre el resto de los ruteadores. Un DR es elegido por el protocolo de Hello de OSPF (que se discute más adelante) La presencia de un DR reducirá el número de las adyacencias que se forman, y que alternadamente reduce la cantidad de tráfico del protocolo de encaminamiento, del ruteador de superior, y el tamaño de la base de datos de estados de enlace de OSPF.

¿Los ruteadores designados son muy beneficiosos, pero cómo OSPF calcula quien será el ruteador designado (DR) en una red? La secuencia siguiente describe cómo OSPF determina qué ruteador será el DR:

Los pasos descritos en cómo se elige un DR, asumen que ninguno existe en esa red. Si éste no es el caso, el proceso se altera levemente y usted debe referirse al RFC 2328 para información adicional.

1. OSPF selecciona un ruteador al azar y examina su lista de vecinos; llame a este ruteador T. Esta es una lista de vecinos de ruteadores, que consiste en todos los ruteadores que han comenzado la comunicación bidireccional entre ellos mismos. Esta comunicación, se refiere como de "2 vías " y es el estado más avanzado de la comunicación, que los ruteadores vecinos pueden alcanzar sin realmente la formación de una adyacencia.

2. El ruteador T, quita de esa lista a todos los ruteadores que son inelegibles para ser DR. Esto consistiría en que los ruteadores que tiene una prioridad otorgada por el protocolo OSPF de 0. Se procede al siguiente paso con los ruteadores restantes en la lista.

3. El DR de respaldo se elige realmente primero, y se determina con los cálculos en los cuales el ruteador tiene la prioridad más alta. Si más de un ruteador tiene el mismo valor de prioridad, esencialmente se han enlazado. Los valores de la prioridad pueden ser definidos, o permitir los valores por defecto. OSPF tomará el ruteador con la identificación más alta de ruteador para romper el lazo. Si hay ya un DR en existencia, entonces cualquier otro ruteador es inelegible para la elección en este punto.

4. Si ningún otro ruteador se ha declarado para ser el DR, entonces es asignado el de respaldo nuevamente para ser el DR.

5. Si el ruteador T ahora es el nuevo DR, después repita los pasos 3 y 4 para conseguir un DR de respaldo y para proceder al paso 6. Por ejemplo, si el ruteador T es el DR, no será elegible para la elección cuando se repita el paso 3. Esto se asegura, de que ninguna ruteador se declare DR y el respaldo DR.

6. Como resultado de estos cálculos, el ruteador T se ha convertido en DR y el ruteador de OSPF y el estado del sus interfaces se fija por consiguiente. Por ejemplo, el DR tiene un nuevo estado de interfaz de DR y el DR de respaldo tiene un estado de interfaz de DR diferente.

7. El DR ahora comenzará a enviar los paquetes Hello, para comenzar el proceso de construir las adyacencias necesarias, con el resto de los ruteadores de la red

## 3.3 Protocolos en OSPF

Los ruteadores de OSPF se comunican con cada uno usando el protocolo de OSPF. OSPF funciona sobre IP, aunque OSPF se compone de tres

subprotocolos: el Hello, el de Intercambio, y el flooding. Las secciones siguientes discuten estos tres subprotocolos con mayor detalle. Todos los paquetes de OSPF comienzan con un encabezado común. La figura 3-2 ilustra una porción (por campo) del encabezado común, encontrado al principio de cada paquete publicado por un subprotocolo de OSPF.

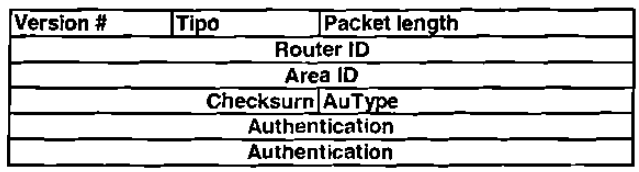



**Figura 3 - 2** Encabezado Común del Subprotocolo de OSPF

### 3.3.1 Protocolo Hello

El protocolo Hello es usado para tres principales tareas:

- Para verificar que los enlaces estén operando.
- Para Elegir el DR o el DR de respaldo, en redes de difusión o de no difusión.
- Para descubrir, establecer y mantener las relaciones entre los vecinos.

Además, el protocolo Hello, es responsable de asegurarse de que la comunicación entre los vecinos de OSPF sea bidireccional (dos vías) Este tipo de comunicación se establece cuando el ruteador ve por sí mismo, la lista de los paquetes hellos de sus vecinos. La figura 3-3 muestra, cómo los ruteadores de OSPF publican los paquetes hello en la red, para descubrir a sus vecinos.

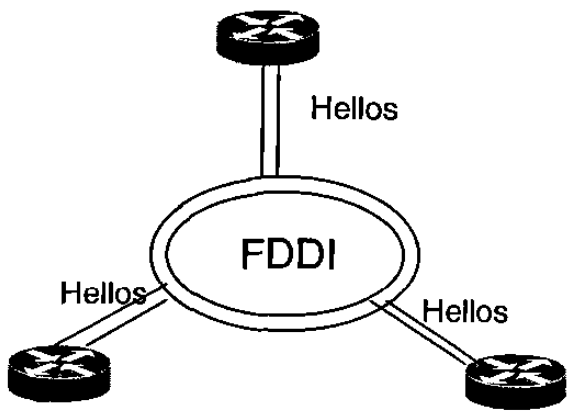



**Figura 3 - 3** Operación del protocolo Hello

La operación básica del protocolo Hello, puede ser mostrada brevemente como sigue

- Los ruteadores de OSPF envían paquetes hellos como difusiones
- El paquete hello es recibido por el nuevo ruteador de OSPF
- El ruteador nuevo contesta los paquetes, con sus propios paquetes hellos

### 3.3.2 Variación de Operación del Protocolo Hello Tipos de Redes en OSPF

El protocolo Hello trabaja diferentemente en redes: punto a punto, multiacceso, y de Multi Acceso por No Difusión NBMA en OSPF. En redes de difusión, cada ruteador se anunciará periódicamente enviando multitrasmisiones de paquetes hello, que permiten descubrir a sus vecinos dinámicamente.

En redes de NBMA, los ruteadores de OSPF pueden requerir una cierta orden de información de configuración para que el protocolo hello funcione correctamente. Esta configuración es realmente del protocolo que sale sobre la red a encontrar o elegir el ruteador designado, según lo discutido previamente en la sección, "los tipos de red de OSPF."

A menos que estén configurados de otra manera, los paquetes hello se omiten en un lapso de transmisión una vez cada 10 segundos o de 30 segundos para las redes de NBMA. Alternativamente, esto se puede fijar con un comando

En redes punto a punto o de punto a multipunto, el ruteador de OSPF enviará los paquetes hellos a cada vecino con quien pueda comunicarse directamente.

En redes de punto a punto, un paquete Hello de OSPF se envía como paquete de multitransmisión. En redes de punto a multipunto, podrían ser enviados como multitransmisión, si la capa de enlace de datos repliega el paquete. O la información del vecino pudiera configurarse para indicar quién envía las réplicas de los hellos cuando la capa de enlace de datos no aplica, por ejemplo el modelo del servidor de ATM ARP.

### 3.3.3 Formato del paquete del Protocolo Hello

Los paquetes del protocolo Hello de OSPF se ajustan al formato solamente en una dirección. Todos los paquetes de OSPF comienzan con un encabezado estandardizado de 24-bytes, que contenga la información que determina, si el proceso ocurrirá en el resto del paquete. Los paquetes contienen campos mostrados en la figura 3 – 4, siempre en el mismo orden. Todos los campos en este formato son de 32 bits, a excepción de los campos siguientes: Intervalo Hello, que es 16 bit; Opciones, el cual es 8 bits; y el de prioridad, que es 8 bits.

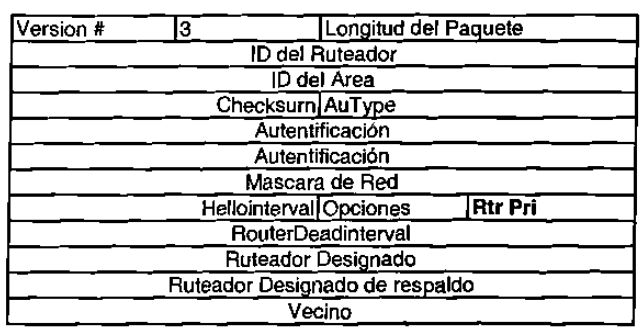



**Figura 3 - 4** El Paquete Hello con Detalle

La siguiente lista describe lo que cada campo del paquete representa

- Numero de Versión: Identifica la versión de OSPF que corre en el ruteador que da origen a los paquetes hellos.

- Longitud de paquetes: Brinda la longitud total del paquete hello.

- ID del ruteador: Identificación del ruteador.

- ID del Área: Contiene el número de Área al cual el ruteador pertenece.

- Checksum: Esta sección es, por supuesto, es utilizada para asegurar la integridad de los paquetes no se han comprendido durante la transmisión.

- Mascara de Red: Mascara de Subred que se asoció a la interfaz. Si la subred se utiliza, será fijada por valor hexadecimal apropiado para cada clase del Dirección IP.

- Intervalo de Hello: El número de segundos en el cual el ruteador transmite los paquetes Hello.

- Rtr PRI: Éste es donde la prioridad del ruteador puede ser anotada si se utiliza esta opción, si no por defecto es 1.

- Intervalo Muerto de Ruteador: Número de segundos desde que el último paquete de hellos fue recibido, antes de declarar que el silencio de un ruteador se convierta en inaccesible

- Ruteador Designado: La Dirección de IP del ruteador designado de la red(si se utiliza). Este campo omite 0.0.0.0 cuando un ruteador designado no está presente, como en los circuitos en demanda.

- Ruteador designado de Respaldo: La Dirección IP del ruteador designado de la red, el ruteador (si está presente) Este campo omite 0.0.0.0 cuando un Ruteador designado no está presente, como circuitos en demanda.

- Vecinos: Contiene las identificaciones de ruteador de cada ruteador que ha enviado un paquete válido de hello. Este campo puede tener entradas múltiples.

### 3.3.4 Protocolo de Intercambio

Cuando dos ruteadores de OSPF han establecido una comunicación bidireccional, o comunicación de dos vías, sincronizarán sus bases de datos de encaminamiento (estado de enlace). Para los enlaces de punto a punto, los dos ruteadores se comunicarán la información directamente entre sí mismos. En los enlaces de red (es decir, redes de multiacceso por difusión o de no difusión) esta sincronización ocurrirá entre el nuevo ruteador de OSPF y el DR. El protocolo de intercambio primero se utiliza para sincronizar las bases de datos de encaminamiento (estado de enlace) Después de la sincronización, cualquier cambio en los enlaces del ruteador utilizarán el protocolo de flooding para poner al día todos los ruteadores de OSPF.

Una nota interesante sobre la operación de este protocolo es que es asimétrico. El primer paso en el proceso del intercambio es determinarse quién es el amo y quién es el esclavo. Después de convenir en estos papeles, los dos ruteadores comenzarán a intercambiar la descripción de sus bases de datos respectivas de estado de enlace. Esta información se pasa entre las dos ruteadores vía la disposición del paquete del protocolo del intercambio según lo mostrado en la figura 3 – 5.

Entonces reciben y procesan estos paquetes de descripción de la base de datos, los ruteadores harán una lista separada que contenga los expedientes que necesitarán intercambiar más adelante. Cuando las comparaciones son completas, los ruteadores entonces intercambiarán las actualizaciones necesarias

que fueron puestas en la lista para poder continuar sus bases de datos actualizadas.

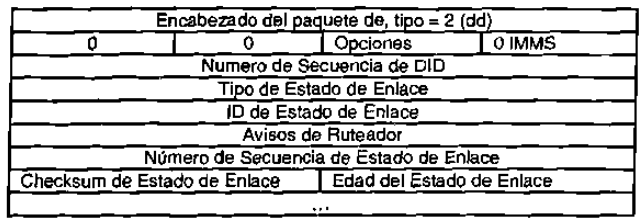



**Figura 3 - 5** Campos del Protocolo de Intercambio

## 3.3.5 Protocolo de Flooding

El subprotocolo de flooding de OSPF es responsable de distribuir y de sincronizar la base de datos de estado de enlace, siempre que un cambio ocurra a un enlace. Cuando un enlace cambia de estado (se cae), el ruteador que experimentó el cambio publicará un paquete de flooding que contiene el cambio de estado. Esta actualización inunda todo hacia todas las interfaces de los ruteadores. Con la tentativa de asegurarse de que el paquete de flooding haya sido recibido por todos sus vecinos, el ruteador continuará retransmitiendo la actualización hasta que recibe un reconocimiento de sus vecinos.

Un enlace es cualquier tipo de conexión (Frame Ralay, Ethernet, etc) entre los ruteadores de OSPF.

Hay dos maneras en las cuales OSPF puede reconocer una actualización. La primera es cuando el ruteador de destinación envía un reconocimiento directamente al ruteador fuente. En este caso, no hay un DR en uso de OSPF si está ocurriendo esto. La segunda manera es cuando un DR está en uso y recibe la actualización; retransmitirá inmediatamente esta actualización al resto de los

ruteadores. Por lo tanto, cuando el ruteador que envía oye esta retransmisión, se considera que no se tomará un reconocimiento, y ninguna otra acción.

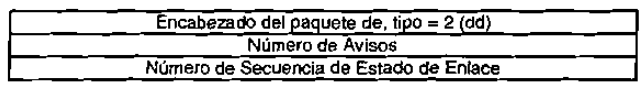



**Figura 3 - 6** Muestra los nombres de los campos, disposición del paquete para el subprotocolo de flooding.

## 3.4 Aviso Estado de Enlace (LSA)

Un enlace es cualquier tipo de conexión entre dos ruteadores de OSPF, como una interfaz en serial. El estado es la condición del enlace, si está arriba o abajo. Un anuncio son las aplicaciones que OSPF usa como método para proporcionar información a otros ruteadores de OSPF. Usted podría decir que los anuncios de estado de enlace son los paquetes que OSPF utiliza, para anunciar cambios en la condición de un enlace específico a otros ruteadores de OSPF.

Hay seis diferentes y distintivos formatos de paquetes de estado de enlace que usa OSPF, cada uno para un diverso propósito que ayude a la subsistencia intacta y exacta de la tabla de encaminamiento de red de OSPF. Aunque hay seis diversos tipos de paquetes, éstos se muestran más adelante en esta sección. Cuando un ruteador recibe un LSA, comprueba su base de datos de estado de enlace. Si el LSA es nuevo, el ruteador hace un LSA de flooding hacia sus vecinos. Después de que el LSA nuevo se agregue a la base de datos de LSA, el ruteador volverá a efectuar el algoritmo de SPF. Este recálculo por el algoritmo de SPF es absolutamente esencial para preservar las tablas de encaminamiento exactas. El algoritmo de SPF es responsable de calcular la tabla de encaminamiento y cualquier cambio de LSA que pude también causar un cambio en la tabla de encaminamiento. La figura 3 – 7 demuestra esta transacción donde

el ruteador A pierde un enlace y recalcula el primer algoritmo de la trayectoria más corta y después hace un flooding el LSA cambia las interfaces restantes. Este LSA nuevo entonces es analizado por los ruteadores B y C, que recalculan y continúan inundando con LSA hacia fuera de las otras interfaces al ruteador D.

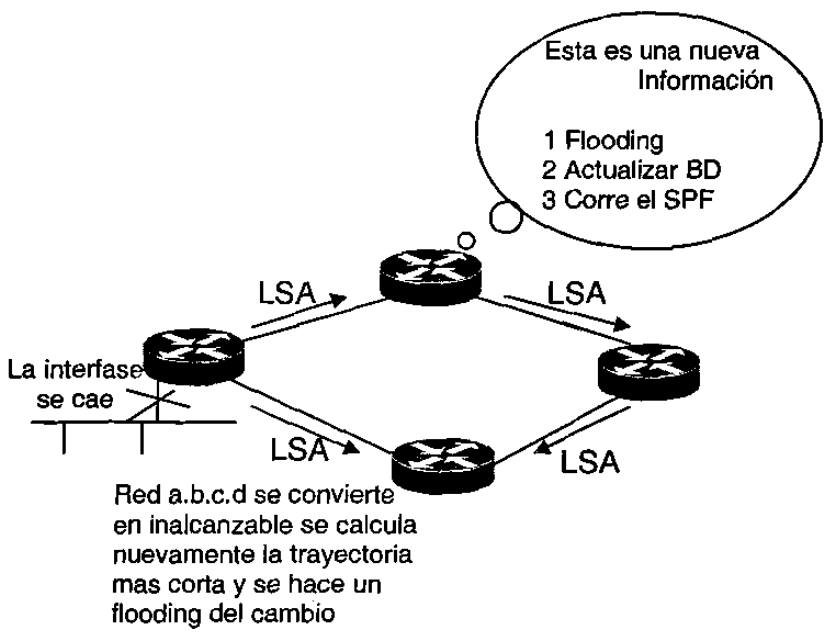



**Figura 3 - 7** Ejemplo de un ruteador enviando un Nuevo LSA y haciendo un flooding

Si no hay cambios, después de cada 30 minutos, los LSAs se envían a todas los ruteadores vecinos; para asegurarse de que los ruteadores tengan la misma base de datos de estado de enlace..

### 3.4.1 Sincronización de las Bases de Datos de Estado de Enlace

La figura 3 – 8 ilustra la sincronización inicial de la base de datos de estado de enlace, que ocurre en cinco pasos mientras es detallada la secuencia numerada después en la figura.

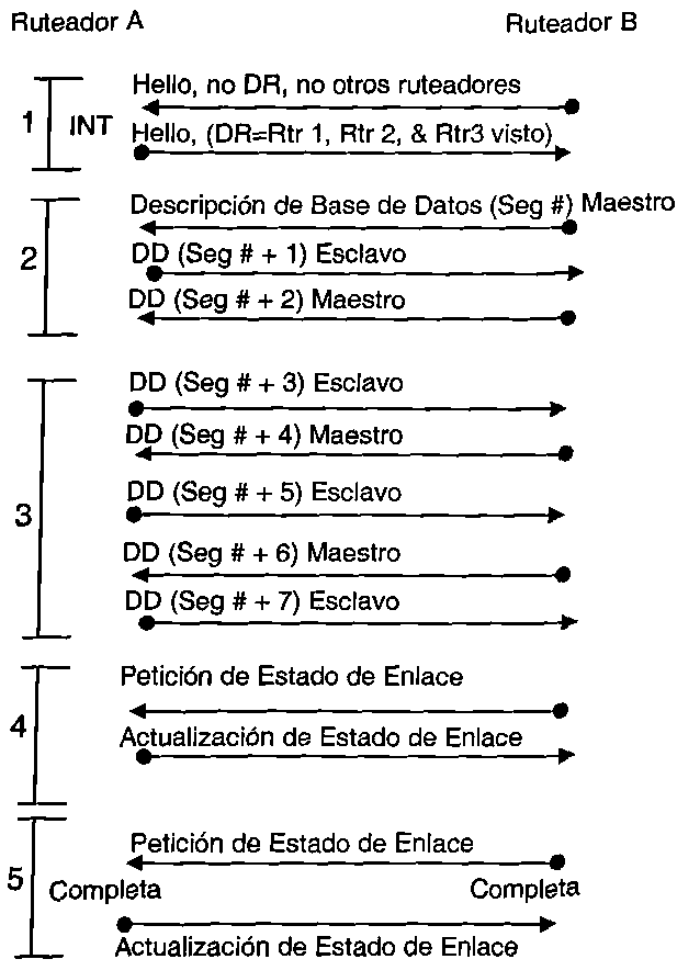



**Figura 3 - 8** Sincronización de la Base de Datos

Los estados para la sincronización de la base de datos de estado de enlace según lo ilustrado en la figura 3 – 8 son como sigue:

1. Estableciendo de la comunicación bidireccional (2 vías): Logrado por los hellos de descubrimiento de los ruteadores y de elección de un DR.

2. Estado de Exstart: Dos ruteadores vecinos forman una relación maestro/ esclavo y convienen en una secuencia que comienza y que se incrementada para asegurar que los LSAs se reconozcan correctamente y ninguna duplicación ocurra. Los paquetes de descripción de base de datos (DD) son los que comienzan.

3. Estado de Intercambio. Los paquetes de descripción de la base de datos (DD) continúan fluyendo mientras que el ruteador auxiliar reconoce los paquetes del amo. En este paso, OSPF se considera operacional porque los ruteadores pueden enviar y recibir LSAs.

4. Estado de carga. Las peticiones de Estado de Enlace se envían a los vecinos que piden los anuncios recientes que todavía no se han descubierto. En esta etapa, el ruteador construye varias listas para asegurar que todos los enlaces estén actualizados y para ser reconocidos correctamente. La figura 3 – 9 muestra los campos y la información contenida dentro del formato del paquete de la petición del estado de enlace.

5. Estado completo: Los ruteadores vecinos son completamente adyacentes porque sus bases de datos de estado de enlace se sincronizan completamente.

Durante los cinco pasos de la sincronización de la base de datos de estado de enlace, los LSAs normales no se envían. En lugar de ello, los ruteadores intercambian paquetes conocidos como paquetes de descripción de la base de datos (DD), que son los paquetes de tipo 2 que se utilizan cuando se están inicializando una adyacencia y los dos ruteadores en cuestión intercambian y sincronizan sus bases de datos de estado de enlace.

Estos paquetes de DD consisten en el contenido de la base de datos del estado de enlace. La figura 3 – 9 muestra los campos e información contenida dentro de cada paquete de DD.

| Version # | 3 | Longitud del Paquete |
|---|---|---|
| ID del Ruteador | | |
| ID del Area | | |
| Checksum | AuType | |
| Autentificación | | |
| Autentificación | | |
| Tipo de LS | | |
| IP de Estado de Enlace | | |
| Aviso del Ruteador | | |

**Figura 3 - 9** Formato del Paquete de Petición e Estado de Enlace

Por supuesto, los paquetes múltiples se pudieran necesitar para terminar la sincronización y en ese caso un procedimiento de respuesta de polleo es utilizado con un ruteador para que se convierta en amo y el otro en el esclavo.

| Version # | 3 | Longitud del Paquete |
|---|---|---|
| ID del Ruteador | | |
| ID del Area | | |
| Checksum | AuType | |
| Autentificación | | |
| Autentificación | | |
| Interface MTU | Opciones 1010101010111M 1MS | |
| Número de Secuencia DD | | |
| Un Encabezado de LSA | | |

**Figura 3 - 10** Descripción del Formato del Paquete de la Base de Datos

## 3.4.2 Tipos de Paquete de LSA

Distintamente a los protocolos de vector de distancia (RIP o IGRP), OSPF no envía realmente su tabla de encaminamiento a otros ruteadores. En lugar, las tablas de encaminamiento se derivan de la base de datos de LSA. La Tabulación de la tabla 3-1 se describe en seis diversos tipos de paquetes de LSA que se pueden generarse por el ruteador de la fuente y entrar en la base de datos de LSA del ruteador de destinación.

**Tabla 3 - 1** Tipos de Paquetes LSA

| Tipo de paquete de LSA | Descripción |
|---|---|
| 1 | Avisos de Enlace de Ruteador |
| 2 | Avisos de enlaces de Red |
| 3 | Aviso Sumarios de Enlaces (ABRs) |
| 4 | Avisos Sumarios de Enlace (ASBRs) |
| 5 | Avisos de enlaces externos de Sistemas Autónomo (AS) |
| 7 | Areas Not-So-Stubby(NSSA) |

Aunque hay diversos tipos de LSAs y cada uno tiene una estructura única de paquete para reflejar la información que contiene, todos comparten un encabezado común según lo mostrado en la figura 3-11.

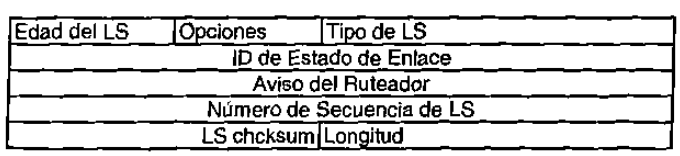



**Figura 3 - 11** Encabezado Común de Aviso de Estado de Enlace

Las secciones que siguen proporcionan descripciones generales de los seis diversos tipos de paquetes de LSA.

## 3.4.3 Tipo 1 de LSA de Ruteador

El LSA de ruteador es generado por cada ruteador de cada área a la cual pertenezca. Estos paquetes describen los estados de los enlaces del ruteador al área y hacen flooding solamente dentro de una área especifica. La identificación del estado de enlace es la identificación del ruteador originario. La figura 3 –12 muestra la disposición de cada paquete de LSA del ruteador.

| - - - 0 - - - EB | - - - 0 - - - - | Numero de Enlaces |
|---|---|---|
| ID del Enlace | | |
| Datos del Enlace | | |
| Tipo | # TOS | TOS 0 métrica |
| TOS = x | 0 | TOS x métrica |
| TOS = y | 0 | TOS y métrica |
| - - - - - - | - - - - - - - - | - - - - - - - - |
| TOS = z | - - - 0 - - - - | TOS z métrica |

**Figura 3 - 12** Descripción del paquete LSA del Ruteador

## 3.4.4 Tipo 2 de LSA de Redes

Los LSA de red son generados por los ruteadores designados (DR) y describen el sistema de ruteadores unidas a una red en particular. Hacen flooding en el área que contiene su red. La identificación de estado de enlace, es la dirección de la interfaz de IP del DR. La figura 3 –13 muestra la disposición de cada estructura del paquete de LSA la red.

| Mascara de Red | | |
|---|---|---|
| E TOS = 0 | 0 | TOS 0 métrica |
| Etiqueta (0) de Ruta Externa | | |
| TOS = x | 0 | TOS x métrica |
| Etiqueta (1) de Ruta Externa | | |
| ------ | -------- | -------- |
| TOS = z | ---0---- | TOS z métrica |
| Etiqueta (z) de Ruta Externa | | |

**Figura 3 - 13** Descripción del paquete LSA de Red

## 3.4.5 Tipo 3 de LSA's Sumarios para ABR

Los LSA son generados por los Ruteadores de Frontera de Area (ABRs) y describen las rutas de inter-área para varias redes. Pueden también ser usadas para agregación de rutas. La ID de Estado de Enlace es el número de Red de Destinación. La Figura 3 –14 muestra la descripción de este paquete sumario

| Mascara de Red | | |
|---|---|---|
| TOS = 0 | 0 | TOS 0 métrica |
| TOS = x | 0 | TOS x métrica |
| ------ | -------- | -------- |
| TOS = z | 0 | TOS z métrica |

**Figura 3 - 14** Descripción del paquete LSA Tipo 3 y 4

## 3.4.6 Tipo 4 de LSA's Sumarios para ASBR

Los LSA sumarios describen los enlaces a los ruteadores de frontera de los Sistemas Autónomos (ASBR) y también es generado por los ruteadores fronterizos de Area (ABRs). La identificación del estado de enlace es la identificación del ruteador del ASBR descrito. La figura 3-17 (mostrada previamente) ilustra la disposición de cada paquete.

### 3.4.7 Tipo 5 de LSA para sistemas Autónomos externos

El tipo 5 de LSA es generado por los ruteadores Frontera del Sistema Autónomo (ASBR). Describen las rutas a las destinaciones externas al Sistema Autónomo. Harán flooding por todas partes a excepción de las áreas Stub. La identificación del estado de enlace es el numero de red externo.

### 3.4.8 Tipo 7 de LSA Not So Stub by Area (NSSA)

El tipo 7 de LSA es generado por los ruteadores de Fronterizos de Área (ABR) Describen las rutas dentro del NSSA. Pueden ser resumidas y ser convertidas en el tipo 5 de LSA por el ABR. Después de que se conviertan al tipo 5 de LSA, serán distribuidas a las áreas que pueden soportar el tipo 5 de LSA. Refiérase al RFC 1587 para otros detalles en cómo se hace esta conversión.

### 3.4.9 Ejemplo de la Operación de Avisos de Estado de Enlace

Ahora que se han discutido los seis LSA y usted entiende cómo funcionan dentro del ambiente funcional de OSPF, refiérase a la figura 3 – 5 para una representación visual para la operación y la interacción entre los varios tipos de LSA dentro de una red del OSPF.

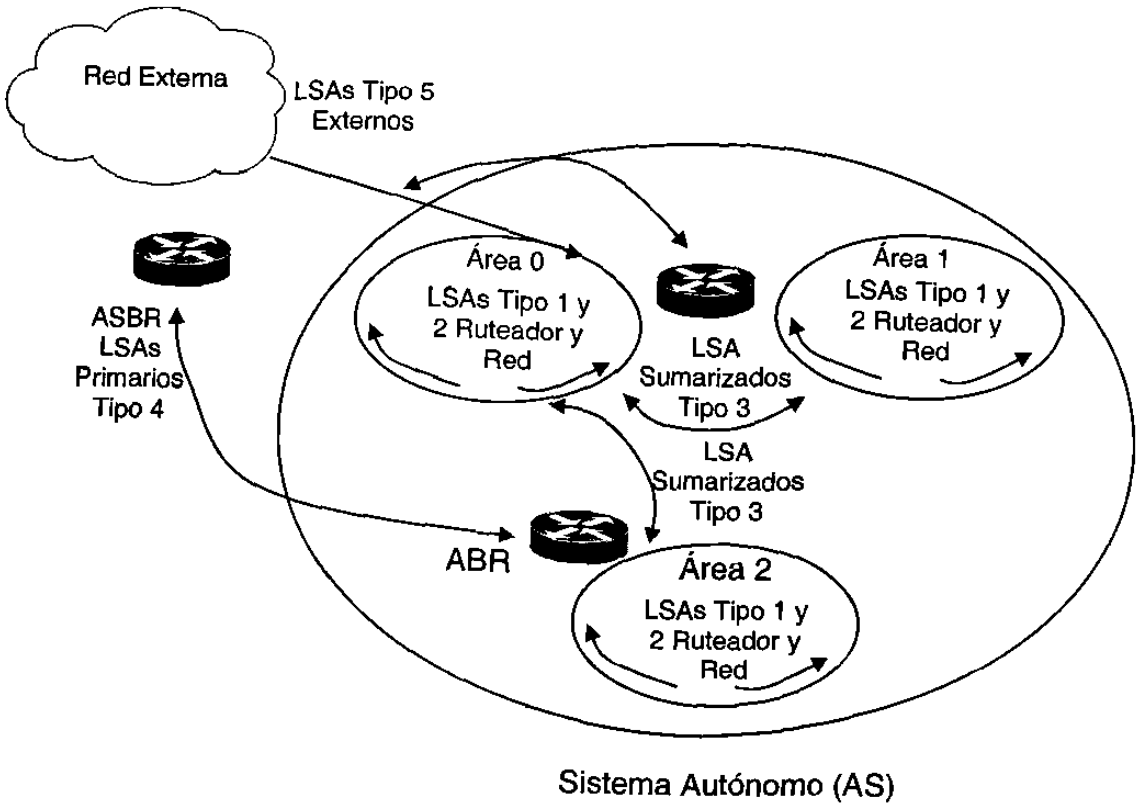



**Figura 3 - 15** Operación de los Avisos de Estado de Enlace

## 3.5 Base de Datos de estado de Enlace

Los ruteadores de OSPF en la misma área todos tendrán la misma base de datos de estado de enlace y ejecutarán el mismo algoritmo de SPF. Los expedientes en esta base de datos son utilizados por el algoritmo de SPF para determinar la topología de la red y para computar la trayectoria más corta a una destinación. Las características de la base de datos de estado de enlace son como sigue:

- Todos los ruteadores que pertenezcan a la misma área tienen la base de datos de estado de enlace idéntica.

- Calcular las rutas usando el SPF que se realiza por separado para cada área

- El flooding de LSA se contiene dentro del área que experimentó el cambio

- La base de datos de estado de enlace se compone de los seis diversos tipos de LSA

- Un ruteador tiene una base de datos de estado de enlace separada para cada área a la cual pertenezca.

## 3.6 Ruteadores y Redes

### 3.6.1 Sistemas Autónomos (AS)

La base de datos de estado de enlace es la fuente de datos para computar las rutas de red, que deben ser computadas otra vez después de que cualesquier cambio ocurra o cambio potencial en la topología de la red, como pude ser el causante de que las rutas cambien. Cada ruteador de OSPF construirá una tabla de encaminamiento con sí mismo como el centro de la red. Una topología que representa la red, que se extrae de los expedientes contenidos dentro de la base de datos de estado de enlace.

El algoritmo de SPF entonces se utiliza para computar la trayectoria más corta del ruteador local de OSPF a cada destinación dentro de la red. Mientras que estos cómputos funcionan y la trayectoria más corta es determinada, esta información se pone en una tabla de encaminamiento. De estos cómputos el ruteador deriva el ruteador del siguiente (salto) que se debe utilizar para alcanzar

la destinación. Esta información es utilizada por el ruteador para encaminar los paquetes a su destinación.

Hay muchos factores que pueden afectar a los resultados de estos cálculos tales como, el tipo de servicio (TOS)

### 3.6.2 Ruteo Jerárquico en OSPF

Una de las características mas importantes dentro del protocolo OSPF es su capacidad para utilizar una estructura del ruteo jerárquico. Hay dos características, que usted debe tener presente al considerar cómo OSPF funciona dentro de este tipo de estructura jerárquica.

- La estructura debe existir o crear un orden para que OSPF funcione correctamente

- La topología explícita tiene precedencia sobre la dirección

Las secciones siguientes discuten tipos de ruteadores de OSPF, técnicas de diseño jerárquicas de red, del Sistema Autónomo, de áreas, y de encaminamiento dentro de una estructura jerárquica. Esta información será presentada y cómo todas obran recíprocamente para que una red de OSPF funcione.

### 3.6.3 Tipos de Ruteadores en OSPF

La estructura de encaminamiento jerárquico usada por OSPF señala cuatro diversos tipos de ruteadores. Cada uno tiene un papel único y características definidas dentro de la jerarquía. La figura 3 –16 muestra una red típica de OSPF con áreas múltiples que contienen los diversos tipos de ruteadores de OSPF.

Las secciones que siguen proporcionan las descripciones generales para los cuatro diversos tipos de ruteadores de OSPF.

### 3.6.3.1 Ruteadores Internos (IR)

Las ruteadores internos (IR) son los ruteadores que tienen conexión directa a red, todos pertenecen a la misma área de OSPF. Estos tipos de ruteadores, tendrán una sola base de datos de estado de enlace, porque pertenecen solamente a una área.

### 3.6.3.2 Ruteadores Fronterizos de Área (ABR)

Los ABR se unen a las áreas múltiples de OSPF, allí pueden ser ABR múltiples dentro de una red. Los ABR tendrán copias múltiples de la base de datos de estado de enlace debido a esto. El ruteador utiliza una base de datos para cada área que será resumida, y entonces será presentada a la espina dorsal (backbone) para la distribución a otras áreas. Los ruteadores situadas en la frontera de una o más áreas de OSPF y conectan esas áreas con la red de la espina dorsal (backbone) y se conocen como ABR. Los ABR se consideran como miembros de la espina dorsal de OSPF y sus áreas unidas. Los ABR por lo tanto mantiene las tablas de encaminamiento que describen la topología de la espina dorsal y la topología de las otras áreas. Recuerde que un ABR envía solamente la información resumida al área de la espina dorsal, para ser considerado un ABR el ruteador debe conectarse con la espina dorsal.

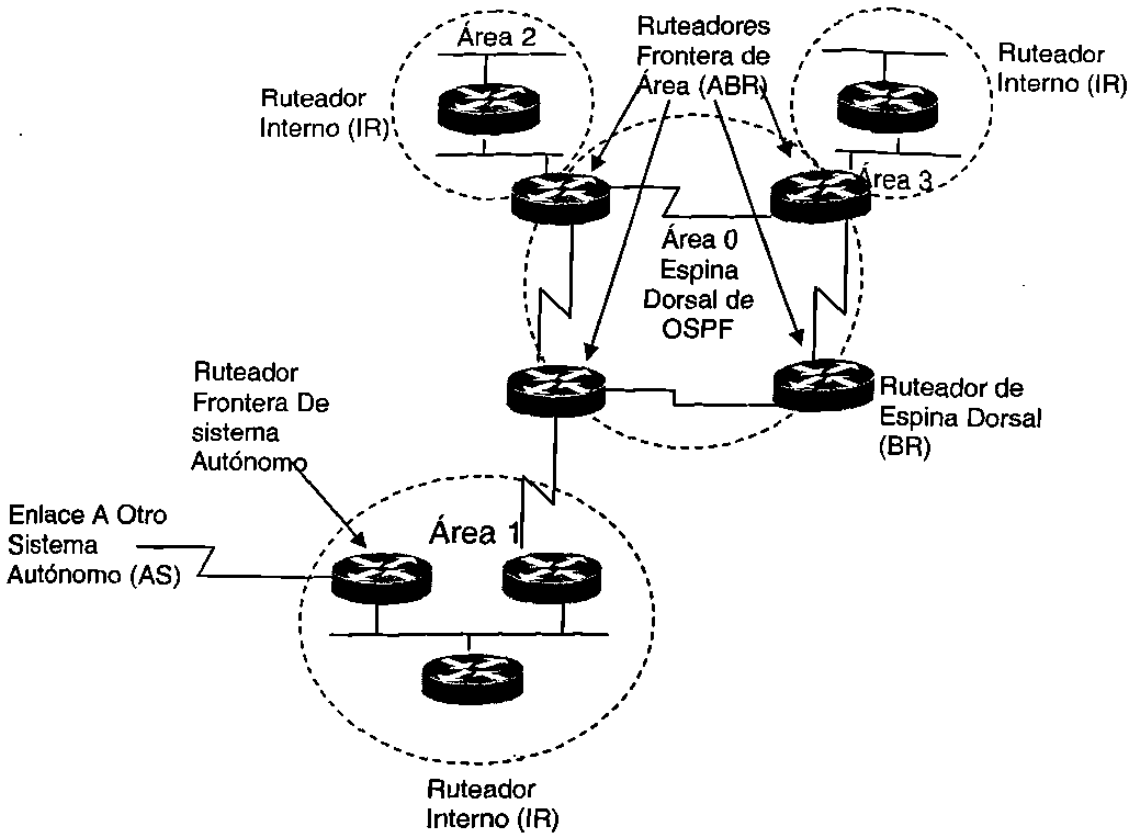



**Figura 3 - 16** Tipos de Ruteadores en OSPF

### 3.6.3.3 Ruteadores Fronterizos de Sistemas Autónomos (ASBR)

El ASBR está conectado con más de un Sistema Autónomo e intercambia la información de encaminamiento con los ruteadores de otro Sistema Autónomo. EL ASBR anuncia la información de encaminamiento externa intercambiada a través de su Sistema Autónomo. Cada ruteador dentro de un Sistema Autónomo sabrá conseguir a cada ASBR con su AS. El ASBR utiliza OSPF y otro protocolo de encaminamiento, tal como RIP o BGP. Los ASBR's debe residir en un área de OSPF que no sea Stub.

Al utilizar ruteadores Cisco, el comando de la redistribución se utiliza a menudo para traer dos protocolos de encaminan juntos. El Protocolo de Puerta de

Enlace Fronterizo (BGP) se puede también utilizar para traer sistemas autónomos múltiples juntos.

### 3.6.3.4 Ruteador de Espina Dorsal (Backbone)

El BR tiene típicamente una interfaz al área de la espina dorsal y una o dos a otras áreas de OSPF. Los ruteadores de espina dorsal no tienen que tener ABR. Los ruteadores que tienen sus interfaces solamente conectadas a la espina dorsal también se consideran BR.

### 3.6.3.5 Técnicas de Diseño de Red Jerárquico

Al considerar cómo diseñar su red de OSPF, recuerde los factores siguientes que son soportados por OSPF y las teorías actualmente aceptadas de diseño de red:

- Una espina dorsal basada en árbol unido, permitirá rápida convergencia y economía en gran escala.
- Nunca más de seis saltos de ruteador de fuente a la destinación.
- 30 a 100 ruteadores por área.
- El espacio de dirección de IP debe estar contiguo.
- Todas las áreas se conectan con el área 0.
- Mantenga la espina dorsal /área 0 simple, simétrica, y restrinja el acceso de los usuarios finales.

- No permita más de dos áreas por ABR, además de su conexión al área 0. Si no, tendrá que no perder de vista a muchas bases de datos de estado de enlace.

## 3.7 Entendiendo un Sistema Autónomo (AS)

Un Sistema Autónomo (AS) es un grupo de áreas que comparten una estrategia común de encaminamiento. Para los propósitos de OSPF, cada Sistema Autónomo (AS) se debe asignar un número único de 16-bit por la Autoridad de Números de Asignación de Internet (IANA).

La autoridad de Asignación de Número de Internet (IANA) es una organización que trabaja bajo auspicios del ISOC a pues una parte del IAB. IANA delega la autoridad para la asignación de espacio de direcciones de IP y la asignación de los nombres de dominios del NIC y otras organizaciones. El IANA también mantiene una base de datos de los identificadores asignados del protocolo usados en el TCP/IP, incluyendo números de Sistema Autónomo.

El encaminamiento real de la información dentro de un Sistema Autónomo ocurre en una de tres maneras:

- Si la fuente y las direcciones de destinación de un paquete residen dentro de la misma área, después se utiliza el encaminamiento de intra-área.

- Si la fuente y las direcciones de destinación de un paquete residen dentro de diversas áreas pero aún dentro del AS, después se utiliza el encaminamiento del Inter-área

- Si residen la fuente y las direcciones de destinación de un paquete en un AS externo, entonces el encaminamiento externo se utiliza.

- Estos diversos tipos de encaminamiento serán discutidos más adelante bajo la sección, "encaminamiento dentro de una estructura jerárquica."

## 3.8 Entendiendo las Áreas

Un panorama típico para muchas redes es que como crecen y más sitios se agregan, las ventajas de OSPF comenzarán a degradarse. Por ejemplo, la base de datos de estado de enlace continuará creciendo de tamaño mientras que el número de ruteadores crece. En un cierto punto llegará a ser ineficaz. El flooding de LSA de una gran cantidad de ruteadores puede también causar problemas de congestión. Para solucionar estos problemas, usted comience dividiendo sus Sistemas Autónomo(AS) en segmentos de áreas múltiples. Como usted agrupa los ruteadores en áreas, considere el limitar el número de ruteadores por área. Cada ruteador entonces tendrá una base de datos de estado de enlace con las entradas para cada ruteador en su área.

Las áreas son similares a la idea de una subred en que las rutas y las redes contenidas dentro pueden ser sumariadas fácilmente. Es decir las áreas son los segmentos lógicos contiguos de red que se han agrupado juntos. Con el uso de las áreas dentro de OSPF, la red será más fácil de manejar y proporcionará una reducción marcada en el tráfico de encaminamiento. Esto adquiere ventajas porque la topología real de una área es invisible a otros ruteadores fuera del área.

Las áreas también permiten a los ruteadores contenidos dentro de ellas Funcionar con su propia base de datos de estado de enlace y el algoritmo de SPF. En verdad, un ruteador trabaja con una copia de la base de datos del estado de enlace para cada área con la cual esté conectado.

### 3.8.1 Característica de una Área de OSPF

La lista siguiente proporciona algunas características generales de una área de OSPF.

- Las áreas contienen un grupo de anfitriones y de redes contiguas
- Las ruteadores tienen una base de datos de la topología del área y utilizan el mismo algoritmo de SPF.
- Cada área está conectada con el área de espina dorsal conocida como área 0.
- Los Enlaces Virtuales pueden ser usados.
- Permite encaminamiento de Inter-áreas.

Las características contorneadas en la lista precedente, necesitan ser consideradas para trabajar dentro de una red del OSPF.

### 3.8.2 Reglas de Diseño de Red

Al diseñar una área de OSPF, usted debe tener algunos de los requisitos siguientes presente:

- Una Área de Espina Dorsal (Backbone) debe de estar presente

- Todas las Áreas deben de tener conexión la Espina Dorsal, aun y las áreas Stub.

- El área Espina Dorsal debe de ser continua.

### 3.8.3 El Área Espina Dorsal (Backbone)

Una área de la espina dorsal es una estructura lógica y física para el Sistema Autónomo y se une a las áreas múltiples. El área de la espina dorsal es responsable de distribuir la información de encaminamiento entre las áreas que no pertenecen a la Espina dorsal (non-backbone) La espina dorsal debe ser contigua, pero no necesite estar físicamente contigua; la conectividad de la espina dorsal se puede establecer y mantener con la configuración de los enlaces virtuales.

### 3.8.4 Áreas Stub

Un área se podría referir como área Stub cuando hay un solo punto de la salida de esa área, o si el encaminamiento externo fuera del área no tiene que tomar una trayectoria óptima. Un Stub es justo como qué suena en inglés, un callejón sin salida dentro de la red. Los paquetes pueden entrar e irse solamente a través del ruteador fronterizo de área. ¿ Algo que se preguntará, eso se lo garantizo es, porqué usted necesitaría tal área? La razón es el mismo viejo fastidio de considerar siempre el tamaño de la red. Mediante la construcción de áreas Stub, usted puede reducir el tamaño total de las tablas dentro de los ruteadores que están dentro del área de Stub.

Las redes externas, tales como ésas que vienen redistribuidas por otros protocolos en OSPF, no se les permiten hacer un flooding en un área stub.

La configuración de un área de Stub, reduce el tamaño de la base de datos del estado de enlace dentro de un área, y reduce los requisitos de la memoria de los ruteadores que se encuentran en el interior del área.

El encaminamiento de estas áreas del mundo, se basa en unas rutas por defecto. Contienen las rutas del Inter-área y del intra-área.

Las áreas de stub deben tener un ruteador de Frontera de área.

Todas los ruteadores del OSPF dentro de un área del Stub, tienen que ser configurados como ruteadores del stub, porque siempre que un área se configure como stub, todos las interfaces que pertenecen a esa área, comenzarán a intercambiar los paquetes del hello como una bandera, que indique que el interfaz es stub. Esto es realmente justo un bit en el paquete hello ("E "bit) que toma al sistema a 0. Todos las ruteadores que tienen un segmento común tuvieron que convenir en esa bandera. Si los ruteadores no convienen, después no sentirán bien a sus vecinos y el encaminamiento no tomará efecto.

### 3.8.5 Restricciones de una Área Stub

Las áreas de Stub tienen ciertas restricciones aplicadas a su operación. Esto es porque se han diseñado para no llevar rutas externas y cualesquiera de las situaciones en la lista siguiente podrían hacer que enlaces externos puedan ser inyectados en el área stub.

- Las Áreas Stub no pueden ser usadas como área de transito para los enlaces virtuales.

- Un ASBR no puede estar internamente en una Stub área.

- El OSPF permite que ciertas áreas sean configuradas como áreas stub.

Una extensión para áreas Stub, son las llamadas áreas totalmente stubby. Los Sistemas Cisco indican este tipo de área de Stub agregando un comando "no-summary" de a la configuración del área de Stub dentro del ruteador. Un área totalmente Stubby es una que bloquea las rutas externas y el encaminamiento sumario (las rutas de Inter-área) entrar el área. De esta manera, solamente las rutas del intra-área y la ruta por defecto de 0.0.0.0 se inyectan en el área.

## 3.9 Encaminamiento en una estructura jerárquica

Hay tres tipos de rutas que se puedan utilizar por OSPF: intra-área, Inter-área, y rutas externas. Las secciones que siguen, proporcionan descripciones generales de estos tipos de rutas.

### 3.9.1 Encaminamiento en una intra-área

El encaminamiento de Intra-área es el nombre usado para describir el encaminamiento dentro de un área lógica. Estos tipos de rutas son descritos por los LSA tipo 1. Para que los paquetes sean encaminados en orden dentro de una sola área, se utiliza el encaminamiento de intra-área. Cuando están exhibidos en la tabla de encaminamiento de OSPF estos enlaces destinos se señalan con un "0."

### 3.9.2 Encaminamiento en Inter-área

El encaminamiento es el nombre usado para describir el encaminamiento entre dos o más áreas lógicas que estén dentro del Sistema Autónomo fuente.

Estos tipos de ruteadores son descritos por los LSA sumarios (tipos 3 y 4). Al encaminar los paquetes entre dos áreas de no difusión, la espina dorsal será utilizada. Esto significa que el encaminamiento de Inter-rea tiene pedazos de encaminamiento de Inter-área a lo largo de su trayectoria, por ejemplo:

Una trayectoria del intra-área se utiliza desde el ruteador fuente al ruteador de frontera de área.

La espina dorsal (backbone) entonces utiliza el área de fuente al área de destinación.

Una trayectoria del intra-área se utiliza desde el ruteador frontera de área a la área de destinación.

Ponga estas tres rutas juntas y usted tendrá una ruta del Inter.-área. Por supuesto, el algoritmo de SPF calculará el costo más bajo entre estos dos puntos. Cuando estos tipos de rutas se exhiben en la tabla de encaminamiento de OSPF, estos tipos de rutas se indican con un IA.

### 3.9.3 AS (Sistemas Autónomos) Rutas Externas

La información de encaminamiento externa se puede obtener por OSPF mediante diversos medios según lo discutido. Esta información debe entonces hacerse disponible a través del Sistema para ser utilizada. Los ruteadores de ASBR sumarizan la información y harán un flooding a esta información a través del AS. Cada ruteador recibirá esta información a excepción de áreas del Stub.

Hay dos tipos específicos de rutas externas, que son las siguientes:

- Rutas E1. Las rutas del E1 son la suma de la métrica interna y externa de OSPF. Son identificadas por la designación de E1 dentro de la tabla de encaminamiento de OSPF. Por ejemplo, si un paquete es destinado para otro Sistema Autónomo, E1 agrega todas las métricas para ambos sistemas autónomos asociados a alcanzar la destinación.

- Rutas E2. Las rutas E2 son las preferidas por defecto para OSPF ya que no agregan la métrica interna de OSPF. Por ejemplo, si un paquete es destinado para otro Sistema Autónomo, las rutas E2 agregan solamente las métricas del AS de destinación asociado para alcanzar la destinación.

Las rutas múltiples a la misma destinación utilizarán la orden siguiente de preferencia para encaminar: intra-área, inter-área, E1, y E2.

# Conclusiones

Aquí pudimos ver las ventajas del encaminamiento jerárquico, y como funcionan los LSA, así como también pudimos ver cuales son los distintos subprotocolos, por lo cueles se componen OSPF. Los tipos de Ruteadores, lo cual nos da herramientas para poder hacer un diseño más acorde con la tecnología OSPF.

# CAPITULO 4

# CONCEPTOS BÁSICOS DE DISEÑO DE OSPF

## 4.1 Conceptos de Diseño de OSPF

- Algoritmos de OSPF. El algoritmo de OSPF será discutido en mayor detalle con la introducción de costos. Con la adición de costos, las tablas de encaminamiento de OSPF se alteran, y esta sección explica cómo y porqué.

- Convergencia de OSPF. Esta sección cubre las ediciones que rodean la convergencia con el protocolo, incluyendo las ventajas de OSPF y de su capacidad de converger muy rápidamente.

- Pautas Del Diseño del OSPF. Esta sección comienza la introducción para diseñar redes del OSPF y se concentra en dos puntos principales: topología y escabilidad de la red. Esta sección comienza a examinar los requisitos y la disposición físicas necesaria antes de que el trabajo real comience.

- Consideraciones Del Diseño Del Área. Los fundamentos verdaderos de cualquier red de OSPF son sus áreas. El diseño apropiado de estas áreas es absolutamente esencial y se discuten muy diversas áreas: la espina dorsal, non-stub, y todas las variaciones del área de Stub.

- Selección De Ruta de OSPF. El encaminamiento es la esencia de cada protocolo, y cómo el protocolo determina sus rutas es el área primaria el foco en esta sección. Se incluye dentro de este capítulo la capacidad inherente de OSPF para conducir balancear la carga. La derivación de rutas externas también se discute extensamente.

- Direccionamiento de IP y Sumarización de Ruta en OSPF. Las técnicas generales y los procedimientos de sumarización de ruta usados por OSPF se examinan y se demuestran a través de diversos panoramas con los cuales un ingeniero de red puede tener contacto. Esta sección concluye con una discusión a profundidad de VLSM y las ventajas de su uso en su red de OSPF.

## 4.2 Algoritmos de OSPF

OSPF es un protocolo de estado de enlace que utiliza una base de datos de estado de enlace (LSDB) para construir y calcular la trayectoria más corta a todas las destinaciones conocidas. Está con el uso del algoritmo del SPF con la información contenida dentro del LSDB que calcula las rutas.

El algoritmo de la trayectoria más corta por *sí* mismo es absolutamente complicado, y sus funcionamientos internos están realmente más allá del alcance de este investigación. Pero entender su lugar y operación es esencial para la realización de una comprensión completa de OSPF el texto sigue revisiones de la operación de calcular la trayectoria más corta y después aplica eso a un ejemplo.

Lo que sigue es un nivel muy alto, en una manera simplificada de mirar varios pasos usados por el algoritmo:

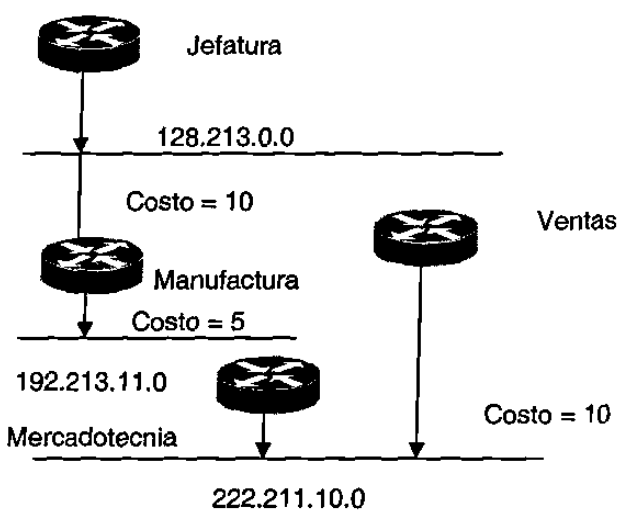
1. Sobre la inicialización o debido a cualquier cambio en la información de encaminamiento, un ruteador generará un anuncio del estado de enlace (LSA). Este anuncio representará la colección de todos los estados de enlace en ese ruteador.

2. Todas los ruteador intercambiarán LSA por medio del protocolo del flooding de OSPF. Cada ruteador que recibe una actualización de estado de enlace la almacenará en su LSDB y después hace un flooding de la actualización a otros ruteadores.

3. Después de que la base de datos de cada ruteador sea actualizada, cada ruteador recalculará un árbol más corto de la trayectoria a todas las destinaciones. El ruteador utiliza algoritmo (Dijkstra) de la primera trayectoria más corta para calcular el árbol más corto de la trayectoria

basado en el LSDB. Las destinaciones, sus costos asociados, y el salto siguiente para alcanzar esas destinaciones que formarán la tabla de encaminamiento de IP.

Se calcula la trayectoria más corta usando el algoritmo Dijkstra. El algoritmo coloca cada ruteador en la raíz de un árbol y calcula la trayectoria más corta a cada destinación basada en el costo acumulativo requerido para alcanzar esa destinación. Cada ruteador tendrá su propia opinión de la topología de la red aunque todas los ruteadores construirán un árbol de la trayectoria más corta usando la misma LSDB. Esta visión consiste en cuáles trayectorias están disponibles y sus costos asociados para alcanzar destinaciones a través de la red. En la figura 4-1, el ruteador de las jefaturas está en la base del árbol (mire hacia arriba de la figura). Las secciones siguientes indican qué está implicada en la construcción de un árbol de la trayectoria más corta.




Vista A: Topologia de Red

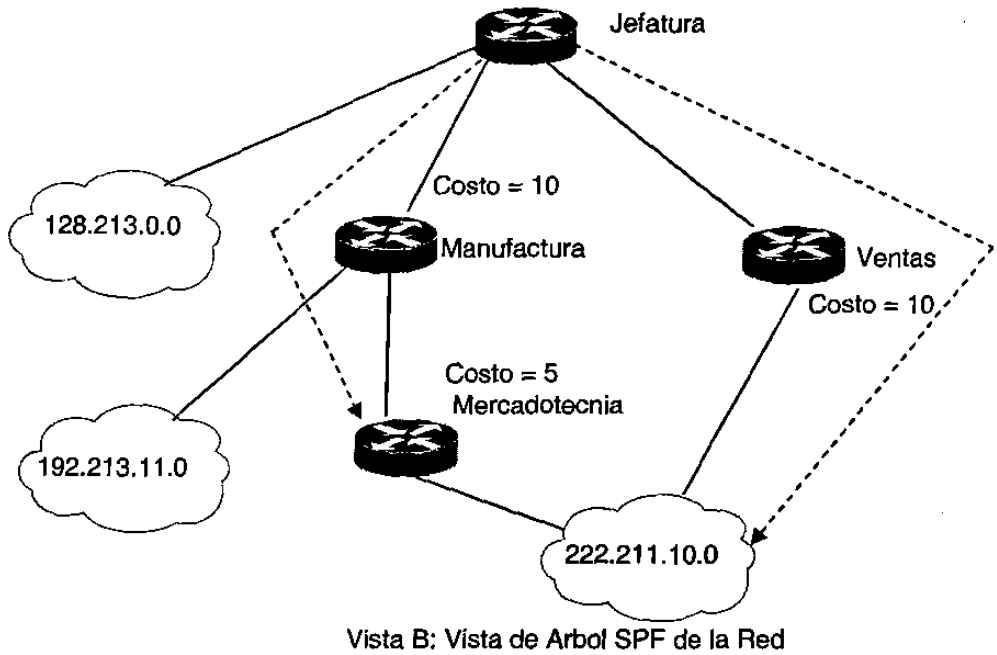



**Figura 4 - 1** Calculo de la trayectoria más corta: Cómo La red busca desde la perspectiva de la jefatura

## 4.3 Costos de OSPF

El costo o la métrica asociada con un interfaz en OSPF es una indicación de los gastos indirectos requeridos para enviar los paquetes a través de ese interfaz. Por ejemplo, en la figura 5-1, para que la jefatura alcancen la red 192.213.11.0, es de un costo de 20 (10+5+5) que se asocia a la trayectoria más corta.

El costo de un interfaz es inversamente proporcional a la ancho de banda de ese interfaz. Un ancho de banda más alta indica un costo más bajo. Hay más gastos indirectos (un costo más alto) y un retraso que implica cruzar una línea serial de 56K, que si se cruza una línea de Ethernet de 10 Mbps. La fórmula usada por OSPF para calcular el costo es:

Costo = 1 00,000,000/ancho de banda en bps

O por ejemplo, costará 10 EXP8/1 0 EXP7 = 10 cruzar una de línea 10Mbps Ethernet y constará 10 EXP8/1544000=64 para cruzar una línea del TI. Por defecto, el costo de un interfaz está mencionado basándose en la ancho de banda, pero usted puede poner un costo en un interfaz con el comando **ip ospf cost [value]** para el costo de la interfase de OSPF.

En el lanzamiento del Cisco IOS 10,2 y anteriores, OSPF asignó métricas por defecto a la interfaz de un ruteador, sin importar el ancho de banda unida realmente al interfaz. Por ejemplo, daría a un enlace de 64K y a un enlace de T1 iguales métricas. Esto requería que el usuario elimine el valor prefijado para aprovecharse del enlace más rápido. Esta eliminación fue lograda con el uso del comando de OSPF **ip ospf cost [value]**, que sería puesto en cada interfaz según lo deseado.

En Cisco IOS 10,3 y posteriores, el OSPF por defecto ahora calcula el costo (métrica) para una interfaz según el ancho de banda de la interfaz. Si necesario, esta característica puede también ser deshabilitada con el uso del comando **no ospf auto-cost -determination** de OSPF. Usted entonces podrá modificar los costos de encaminamiento para requisitos particulares según lo necesitado.

## 4.4 Árbol de la Trayectoria Mas corta

Asuma que usted tiene el diagrama de la red según lo mostrado en la figura 4-1 con los costos indicados de la interfaz. Para construir el árbol de la trayectoria más corta para el ruteador de jefaturas, usted tendría que hacer la raíz del árbol y calcular el costo más pequeño para cada destinación.

Las direcciones de las flechas en esta figura se utilizan para calcular el costo de la ruta. Por ejemplo, el costo del interfaz del ruteador de manufactura a la red 128.213.0.0 no es relevante al calcular el costo a 192.213.11.0.

Las jefaturas pueden alcanzar 192.213.11.0 vía el ruteador de manufactura con un costo de 20 (10+5+5). Las jefaturas pueden también alcanzar 222.211.10.0 vía el ruteador de las ventas con un costo de 25 (10+15) o vía el ruteador de la manufactura con un costo de 20 (10+5+5)

En caso de que existan las trayectorias iguales de costo a la misma destinación, la implementación del Cisco de OSPF no se perderá de vista hasta seis saltos siguientes a la misma destinación.

Para construir el árbol de la trayectoria más corta para las jefaturas, usted tendría que hacer las jefaturas la raíz del árbol y calcular el costo más pequeño para cada destinación. Después de que el ruteador construya el árbol de la trayectoria más corta, comenzará a construir la tabla de encaminamiento por consiguiente. Las redes directamente conectadas serán alcanzadas vía una métrica (costo) de 0 y otras redes serán alcanzadas según el costo según lo calculado en el árbol.

## 4.5 Convergencia en OSPF

Una de las características más atractivas sobre el OSPF es su capacidad a adaptarse rápidamente a los cambios de la topología. Los dos componentes esenciales a la convergencia de encaminamiento son:

- Detección de cambios a la topología de la red

- Recálculo rápido de rutas.

### 4.5.1 Detectando cambios a la Topología de la Red

El OSPF utiliza dos mecanismos para detectar cambios de la topología. Los cambios del estado del interfaz (tales como falta del portador en un enlace serial) es el primer mecanismo. El segundo mecanismo es la falta de recepción de paquetes hello de OSPF de su vecino dentro de una ventana de la sincronización llamada contador de tiempo muerto. Después de que expire este contador de tiempo, el ruteador asume que el vecino está caído. Se configura el contador de tiempo muerto usando el comando ip ospf dead -interval de la configuración OSPF. El valor prefijado del contador de tiempo muerto es cuatro veces el valor del intervalo Hello, que los resultados en un defecto muerto del contador de tiempo de 40 segundos para las redes de difusión y 2 minutos para las redes de no difusión.

Para resumir, la detección de avería de OSPF puede diferenciar levemente dependiendo del tipo de medios. En general, la falta hola de un paquete puede reemplazar la falta de paquetes keepalive (vida). El tipo de medios afectará cómo el OSPF detecta una falta según lo demostrado en la lista siguiente:

- Las averías de la interfaz seriales se detectan de una de dos maneras.
- Detección inmediata de pérdidas de portador (lmi).
- Dos a tres veces el tiempo del paquete de keepalive (vida) por defecto 10 segundos.
- El token ring y el FDDI se detectan inmediatamente.
- Se detecta Ethernet después de que se caiga el paquete keepalive de dos a tres veces.

### 4.5.2 Rápida Recalculación de Rutas

Después de que se haya detectado una falta, el ruteador que detectó la falla un manda un paquete de Flooding de LSA con la información del cambio a todas las ruteadores con las cuales esté conectada directamente. El ruteador de detección continuará haciendo un flooding, de esta información hasta que cada ruteador con el cual está conectada directamente reconoce su recepción.

Todos las ruteadores recalcularán sus rutas usando el algoritmo de Dijkstra (o SPF). Recuerde que cada ruteador construye su tabla de encaminamiento basada sobre la LSDB, y este cambio altera el contenido de esa base de datos. Por lo tanto, el ruteador reconstruirá sus tablas de encaminamiento con ella como la base del árbol de la ruta. El tiempo requerido para funcionar el algoritmo depende de una combinación del tamaño del área y del número de rutas en la base de datos.

OSPF balancea la carga a lo largo de las trayectorias con igual costo, esto tiene en cuenta una convergencia casi inmediata. El OSPF puede también balancear cargas a través de cuatro trayectorias de igual costo.

## 4.6 Guía de Diseño de OSPF

El protocolo OSPF, según lo definido en RFC 1583 y RFC 2178, proporciona un protocolo abierto de la alta funcionalidad que permite a redes de múltiples fabricantes comunicarse con la familia de protocolos de JCPAP. Algunas de las ventajas del OSPF son: convergencia rápida, VLSM, autentificación, segmentación jerárquica, sumarización de ruta, y agregación, que son necesarios para manejar redes grandes y complicadas.

Si usted está construyendo una red interna de OSPF de abajo para arriba o está convirtiendo su red interna al OSPF, las pautas del diseño destacadas en las secciones siguientes proporcionan una fundación de la cual usted pueda construir un ambiente confiable, escalable basado en OSPF.

Diversa gente tiene diversos acercamientos para diseñar redes de OSPF. La cosa importante a recordar es que cualquier protocolo puede fallar bajo presión. La idea no es desafiar el protocolo para trabajar algo con él para conseguir el mejor funcionamiento posible de su red.

El OSPF RFC 1583 y 2178 no especifica varias consideraciones muy importantes que son esenciales para el diseño correcto de una red de OSPF. Pero el RFC 2178 es un recurso muy bueno a consultar al presentar al diseño de su red de OSPF. Es también compatible posterior al RFC 1583.

Las dos actividades de diseño que son críticamente importantes para una implementación acertada de OSPF son definir los límites de área y la asignación de direcciones. Asegurarse de que estas actividades estén planeadas y ejecutadas correctamente esto hará la diferencia en su puesta en práctica de OSPF.

## 4.7 Topología de Red de OSPF

El OSPF trabaja lo mejor posible en un ambiente de encaminamiento jerárquico. La primera y la más importante decisión cuando diseña una red en OSPF es de determinar qué ruteadores y enlaces deben ser incluidos en la espina dorsal (área 0) y cuáles son incluidos en cada área. Lo siguiente son las tres características importantes de OSPF y su necesidad de una estructura de una estructura jerárquica:

La estructura jerárquica de encaminamiento debe existir o ser creada.

Un área contigua de espina dorsal debe estar presente y todas las áreas deben tener una conexión a la espina dorsal.

La topología explícita tiene precedencia cualesquiera a esquemas de dirección de IP que pudieran haber sido aplicados.

Varios artículos importantes para considerar cuando se diseña la topología para una red de OSPF (serán discutidas largamente en las secciones que siguen) son como sigue:

- El número de ruteadores en un área.
- El número de áreas conectadas a un ruteador frontera de área (ABR).
- El número de vecinos para cualquier ruteador.
- El número de las áreas soportadas por cualquier ruteador.
- Seleccionar el ruteador designado (DR).
- EL LSDB.

### 4.7.1 El Número de Ruteadores en un Área.

El OSPF utiliza intensivamente el CPU con el algoritmo de SPF. La experiencia ha demostrado que 40 a 50 ruteadores por área son el límite superior óptimo para OSPF, el número de los cálculos que se deben realizar por el ruteador dado los paquetes de n estados de enlaces (LSP's) y es proporcional a n(log)n. Consecuentemente, entre más grande y más inesTabla sean las áreas, mayor es la probabilidad para los problemas de funcionamiento asociados al recálculo del encaminamiento del OSPF.

Generalmente, un área debe tener no más de 50 ruteadores. ¿Eso no significa que no funcionarán las redes con 60 o 70 ruteadores en un área, pero

para porqué experimentar con la estabilidad si usted no lo necesita? Las áreas con enlaces inestables deben ser más pequeñas.

Uno de los problemas principales con las áreas es que los administradores de la red dejan su área de espina dorsal crecer demasiado grande. Intente controlar la vista lógica de la red desde el comienzo, y recuerde que no lastima comenzar a crear otra área antes de que ella es necesaria. Una buena regla del pulgar es planear para el crecimiento máximo a la par con la planificación a largo plazo. Esto tiene un ventaja agregada para asegurar que su red pueda manejar el crecimiento rápido. En este caso, el planear para demasiado nunca es una mala idea.

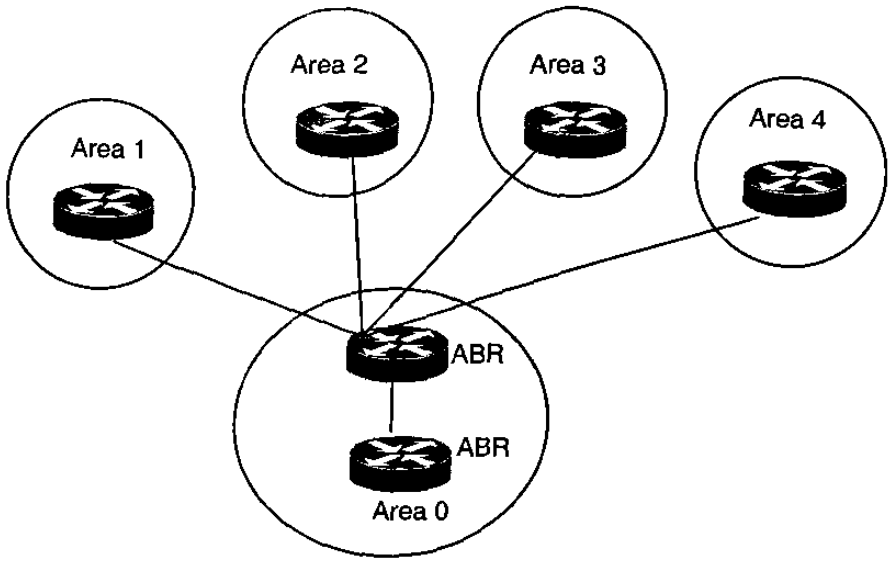
Sin embargo, esas recomendaciones se hacen de acuerdo con recomendaciones "oficiales" de Cisco con respecto a redes del OSPF. Los estudios y las implementaciones verdaderas en el mundo han ido más lejos. Por ejemplo, la estadística en la tabla 4-1 vine "del informe de estándar del OSPF del IETF."

Tabla 4 – 1 informe de estándar del OSPF del IETF

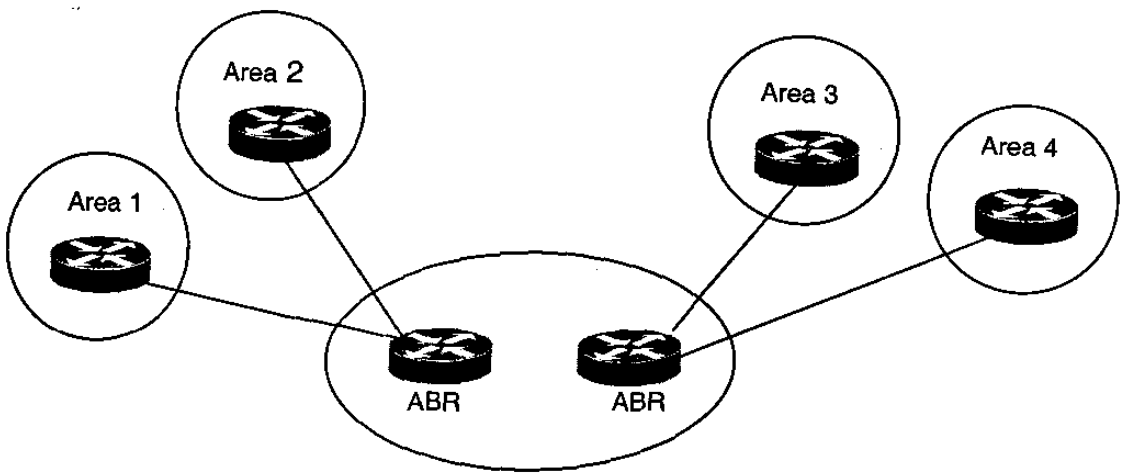
| **Parámetro** | **Mínimo** | **Media** | **Máximo** |
|---|---|---|---|
| Ruteador en un Dominio | 20 | 510 | 1000 |
| Ruteador por una sola area | 20 | 160 | 350 |
| Áreas por Dominio | 1 | 23 | 60 |

Es bueno saber que OSPF se ha probado y puede a fondo soportar el escalamiento a un tamaño fenomenal.

El ABR guardará una copia de la base de datos para todas las áreas que se mantienen. Si una ruteador está conectado con cinco áreas, por ejemplo, tendrá que guardar una lista de cinco diversas bases de datos. Es mejor para no sobrecargar un ABR; que usted intente separar las áreas sobre otros ruteadores. El diseño ideal es tener cada ABR conectado con dos áreas solamente, la espina dorsal, y otra área, con tres áreas siendo el límite superior. La figura 4-2 demuestra la diferencia entre un ABR que lleva a cabo cinco diversas bases de datos, incluyendo el área 0 (parte a) y dos ABRs que lleva a cabo tres bases de datos cada uno (la parte b).




Demaciadas Areas Por ABR
(a)




Dos Areas Por ABR es lo Óptimo
(b)

**Figura 4 - 2** ¿Cuántas Áreas pueden estar conectadas por ABR?

Éstas son pautas justas; cuanto más áreas que usted una por ABR, más bajo es el rendimiento que usted pueda conseguir de esa ruteador. En algunos casos, el rendimiento más bajo puede ser tolerado, pero los usuarios finales no lo verán probablemente de esa manera.

## 4.7.2 El Numero De Vecinos Para Cualquier Ruteador.

El Flooding de OSPF transmite todos los cambios de estado de enlace a todas las ruteadores en un área. Los ruteadores con muchos vecinos tienen la mayoría del trabajo a hacer cuando ocurren los cambios de estado de enlace. En general, cualquier ruteador debe tener no más de 60 vecinos.

El número de ruteadores conectados en la misma LAN es también importante. Cada LAN tiene un DR y BDR que construyan adyacencias con el resto de los ruteadores. Cuanto menos vecinos existan en la LAN, más pequeño es el número de adyacencias que un DR o BDR tiene que construir. Usted puede ver en la figura 4-3 que cuanto más vecinos el DR o el BDR tiene, más es el trabajo que deben hacer.

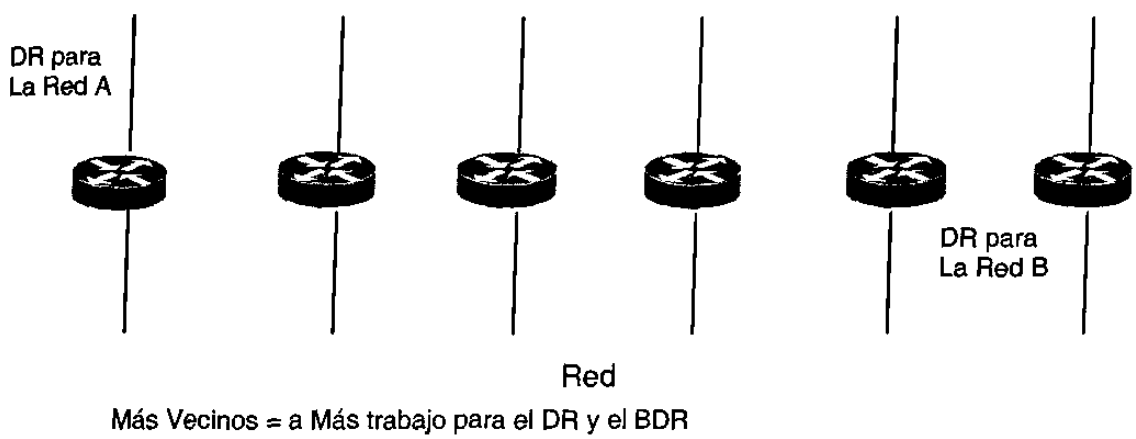



**Figura 4 - 3** Más Vecinos = a Más trabajo para el DR y el BDR

Esto, por supuesto, depende de cuánta energía tenga el proceso en su ruteador. Usted podría cambiar siempre la prioridad de OSPF para seleccionar a su DR. también, si es posible, intentar evitar de tener el mismo ruteador DR en más de un segmento. Si la selección del DR se basa en la prioridad más alta, entonces un ruteador podría convertirse en accidentalmente un DR sobre todos los segmentos con los cuales está conectado. Esta ruteador estaría haciendo esfuerzo adicional mientras que otras ruteadores están ociosos.

### 4.7.3 Número de Área Soportadas por cualquier otro Ruteador

Un ruteador debe utilizar el algoritmo del estado de enlace para cada cambio del estado de enlace que ocurra para cada área en la cual la ruteador resida. Cada ruteador frontera de área está en por lo menos dos áreas (la espina dorsal y una área). En general, par maximizar estabilidad, un ruteador no debe estar en más de tres áreas.

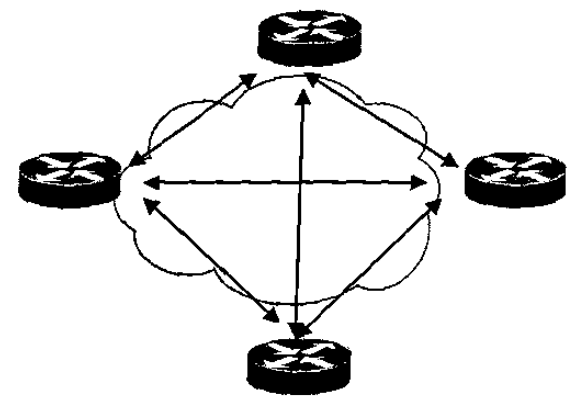
### 4.7.4 Seleccionando el Ruteador Designado

En general, el DR y los BDR en una LAN hacen la mayoría del trabajo de OSPF. Es una buena idea seleccionar los ruteadores para que ya no se cargan pesadamente con actividades de intensivas del CPU para los DR y los BDR. Esto se puede lograr usando **ip ospf priority,** l comando de la prioridad l, que permitirá que usted organice los DR's según lo necesario.

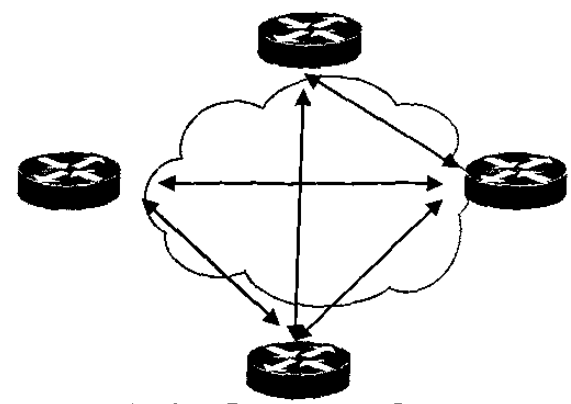
Además, no es generalmente una buena idea seleccionar el mismo ruteador para ser el DR en más de una LAN simultáneamente. Estas pautas ayudarán a asegurarse de que ningún enlace de difusión tendrá también muchos vecinos con demasiado tráfico de paquetes Hello.

### 4.7.5 Topologías de Red Totalmente Conectada contra Parcialmente Interconectado

Las nubes de Multiacceso de no Difusión (NBMA), tales como Frame Relay o X.25, son siempre un desafío. La combinación de bajo ancho de banda y muchos LSA's es también perjudicial incluso para OSPF .Una topología parcialmente enlazada se ha demostrado que se comporta mucho mejor que una topología de la red totalmente enlazada. La figura 4-4 demuestra las ventajas y las diferencias entre las dos topologías.



Una Red Totalmente Conectada
(no Recomendada)



Una Red Parcialmente Conectada
(Recomendada)

**Figura 4 - 4** Ejemplos de las redes totalmente Conectadas y parcialmente conectadas

Una solución cuidadosamente presentada de red de punto a punto o de punto a multipunto en algunos casos funciona mucho mejor que las redes de múltiples puntos que tienen que ocuparse de las muchas funciones de DR.

## 4.8 La Base de Datos de Estado de Enlace

Aunque están cubiertas en capítulos anteriores, estas ediciones con respecto al LSDB son muy importantes y tratan directamente con su operación en lo referente a la topología de la red:

- Un ruteador tiene una LSDB separada para cada área a la cual pertenece
- Un ruteador tiene un LSDB separado para cada área a la cual los ruteadores pertenecen. Todos los que pertenecen a la misma área tienen el LSDB idéntico.
- El cálculo del SPF es utilizado separadamente para cada área y para su LSDB asociado.
- El flooding de LSA ocurre solamente en el área que envía el aviso.

## 4.9 Escabilidad de Red de OSPF

Su capacidad de escalar una red interna de OSPF depende de su esquema total, de la estructura de la red y de la dirección del IP. Conforme a las discusiones referentes la topología de la red y a la sumarización de la ruta, adoptar un ambiente jerárquico de las direcciones y una asignación de direcciones estructuradas, serán los factores más importantes de determinar en la escabilidad de su red interna. La escabilidad de la red es afectada por consideraciones operacionales y técnicas.

Operacionalmente, las redes del OSPF deben ser diseñadas de modo que las áreas no necesiten estar partidas para acomodar el crecimiento. El espacio de direcciones se debe reservar para permitir la adición de nuevas áreas. La escabilidad se debe tomar siempre en consideración al diseñar su red. Todas las ruteadores guardan una copia del LSDB. Pues la red crece, alcanzando eventualmente un punto a donde la base de datos llega a ser demasiado grande, dando por resultado la ineficacia en su encaminamiento. Además, los LSA's harán un flooding a través de la red, dando por resultado un problema de la congestión. La capacidad de su red de OSPF a escalar correctamente es determinada por una multiplicidad de factores, incluyendo lo siguiente:

- Requerimientos de Memoria del Ruteador.
- Requerimientos de CPU.
- Ancho de Banda Disponible.
- Seguridad de OSPF.

En muchos casos, el personal que trabaja directamente con las redes no está siempre en el control completo de algunos de los factores discutidos en esta sección. Por supuesto, entre más grande es mejor; desafortunadamente, es también más costosa.

### 4.9.1 Determinando los Requerimientos de Memoria del Ruteador

Un ruteador de OSPF almacena todos los estados de enlace para todas las áreas a las que pertenece. Además, puede almacenar las rutas sumarizadas y

externas. El uso cuidadoso de las técnicas del sumarización de ruta y de la creación de las áreas del Stub puede reducir el uso de la memoria substancialmente.

No es fácil determinar la cantidad exacta de memoria necesitada para una configuración en particular de OSPF. Los recursos de la memoria generalmente se elevan cuando muchas rutas externas se inyectan también en el dominio de OSPF. Un área de la espina dorsal con 40 ruteadores y un una ruta por defecto a, el mundo exterior tendría menos consumo de memoria comparadas con un área de la espina dorsal con 4 ruteadores y 33.000 rutas externas que fuesen inyectadas en memoria del ruteador de OSPF, podrían también ser conservadas usando un buen diseño de OSPF. La Sumarización en las ruteadores frontera de área y el uso de las áreas de Stub podrían reducir al mínimo el número de las rutas intercambiadas.

La memoria total usada por OSPF es la suma de la memoria usada en la tabla de encaminamiento (**show ip route summary**) y la memoria usada en el LSDB. Los números siguientes son "regla de pulgar". Cada entrada en la tabla de encaminamiento consumirá entre aproximadamente 200 y 280 octetos más 44 octetos por la trayectoria adicional. Cada LSA consumirá gastos indirectos de 100 octetos más el tamaño del LSA real, posiblemente otros 60 a 100 octetos (para el ruteador de enlace, esto depende del número de interfaces en la ruteador). Estas cantidades se deben agregar a la memoria usada ya por otros procesos y por el IOS sí mismo.

Si usted realmente desea saber el número exacto, usted puede hacer una show memory con y sin su activación en OSPF. La diferencia en la memoria del procesador usada sería la respuesta.

Considere el conseguir y el guardar una copia de reserva de la configuración del ruteador de antemano, por supuesto.

Normalmente, una tabla de encaminamiento que use menos octetos de 500K se podría acomodar con 2 a 4MB de RAM; las redes grandes que tienen tablas de encaminamiento mayores de 500K pudieron necesitar de 8 a 16MB. Puede ser que incluso necesiten 32 a 64MB si las rutas se llenan y se inyectan del Internet.

### 4.9.2 Requerimientos de CPU

Un ruteador de OSPF utiliza ciclos del CPU siempre que ocurra un cambio de estado de enlace. Así, que mantenga las áreas de OSPF pequeñas y use la sumarización de ruta para reducir dramáticamente el uso del CPU del ruteador y así se crea un ambiente dentro del cual el OSPF pueda funcionar.

### 4.9.3 Ancho de Banda Disponible

El OSPF envía actualizaciones parciales de LSA cuando ocurre un cambio del estado de enlace. Las actualizaciones inundan a todos las ruteadores en el área. En una red reservada, el OSPF es un protocolo reservado, ¿no son todos los protocolos de esa manera? Lo siento, se tuvo que ser decir. En una red con los cambios substanciales de la topología, OSPF reduce al mínimo la cantidad de ancho de banda usado para el tráfico del cliente.

### 4.9.4 Seguridad en OSPF

Las dos clases de seguridad aplicables a los protocolos de encaminamiento están como siguen:

- Las ruteadores que participan en una red de OSPF son controlados
- El OSPF contiene un campo opcional de autentificación.

Todas las ruteadores dentro de un área deben convenir en el valor del campo de la autentificación. Porque el OSPF es un protocolo estándar disponible en muchas plataformas, incluyendo algunos anfitriones, usando el campo de la autentificación previene el arranque inadvertido de OSPF en una plataforma incontrolada en su red y reduce el potencial para la inestabilidad.

Usted puede ser que piense que es posible controlar la información de encaminamiento dentro de un área de OSPF. Recuerde sin embargo, esto para que el OSPF funcione correctamente, todas las ruteadores dentro de un área debe tener los mismos datos. Consecuentemente, no es posible utilizar los filtros de ruta en una red de OSPF para proporcionar la seguridad porque los intercambios de OSPF encaminan la información con el uso de LSA's, no rutas. OSPF entonces calcula la ruta a una destinación basada sobre el LSA.

## 4.10 Consideraciones para el Diseño de Áreas en OSPF

Al crear redes internas de OSPF a gran escala, la definición de áreas y la asignación de recursos dentro de áreas se deben hacer con una vista pragmática de su red interna de OSPF. Esta asignación de recursos incluye componentes físicos y lógicos del establecimiento de una red de modo que resulte en un funcionamiento óptimo.

### 4.10.1 Justificando el Uso de Áreas y de Áreas Múltiples

Las áreas son esencialmente pequeñas redes dentro de una red más grande, y como tales, ellos encaminan solamente tráfico necesario dentro de sí mismos, de tal modo reduciendo tráfico total de la red. Hay muchas razones para usar la capacidad de OSPF para crear áreas y darle lugar a las ventajas para su red. El uso de áreas es necesario así que la estructura jerárquica requerida de OSPF se puede poner en su lugar. La topología de red dentro de un área es

invisible a cualquier cosa afuera de esa área, según lo demostrado en la figura 4-5.

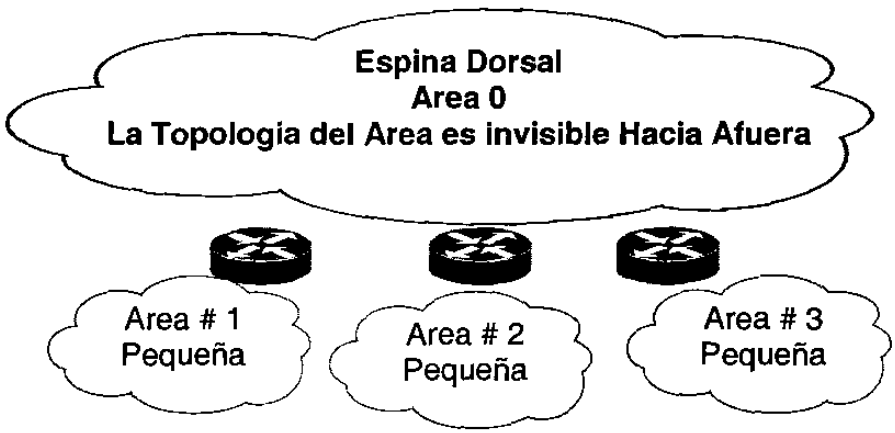



**Figura 4 - 5** Las Áreas sirven como pequeñas Redes, por consecuencia resultan en una reducción del trafico de la red

## 4.10.2 Características de Un Área No Stub

Las áreas de Non Stub llevan una ruta por defecto, rutas de los estáticas, rutas de intra-área, y rutas externas. Una área debe ser un área de non stub cuando contiene un ruteador que utilice el OSPF y cualquier otro protocolo, tal como el Protocolo de Encaminamiento de Información (RIP). Tal ruteador se conoce como ruteador de la frontera de Sistema Autónomo (ASBR). Una área debe también ser una área del non stub, cuando un enlace virtual se configura a través del área. Las áreas de Non stub son el tipo más intensivamente socorridas de las áreas.

## 4.10.3 EL LSDB en un Área

El LSDB está por todas partes dentro de una red de OSPF. Cuando está se encuentra en un área, el LSDB será idéntico en cada ruteador dentro del área. El LSDB también contendrá una variedad de LSA, como sigue:

- Anuncios de enlace de ruteador

- Anuncios de enlace de red.
- Anuncios sumarios del acoplamiento (red del IP y ASBR)
- Sistema Autónomo, (AS) anuncios externos (áreas del non stub solamente)

### 4.10.4 Particiones Del Área: ¿Interrupciones o crecimiento de la red?

Las particiones del área ocurrirán típicamente dentro de un área. OSPF no procura activamente las reparaciones de particiones de área. Cuando se convierte una área particionada, las nueva sección se hace simplemente en una áreas separada. Mientras la espina dorsal puede alcanzarlas a ambas, se continuará encaminando la información a ellos.

Para mantener el encaminamiento, un rango de Direcciones de IP no se debe separar a través del área particionada. Esto asume que algunas destinaciones ahora requerirán el encaminamiento de Inter.-área consecuentemente. Si ocurre esto, después algunas destinaciones llegarán a ser inalcanzables y los lazos de encaminamiento podrían ocurrir. Una condición de interrupción de esta información no es muy provechosa, pero cuando se diseñan áreas, asigne los rangos de Direcciones IP por consiguiente de modo que el crecimiento pueda ser más fácil dirigido en el futuro si una nueva área es necesaria.

La espina dorsal nunca se debe repartir, pero si ocurre, después considere el usar de un enlace virtual para reparar temporalmente la espina dorsal. Los enlaces virtuales se discuten más adelante en este capítulo. Aunque partir su espina dorsal de OSPF se considera mala práctica, hay veces en que podría ser beneficioso, así que OSPF lo permite. Por ejemplo, una compañía está intentando combinar dos redes separadas de OSPF en una red con un área común 0. En otros casos, los enlaces virtuales se agregan para la redundancia en caso de que una cierta falla de ruteador haga que la espina dorsal este partida en dos. Cualesquiera que se a la razón, un enlace virtual se puede configurar entre ABR's

separados que tocan el área 0 de cada lado y tienen un área común (véase la figura 4-6).

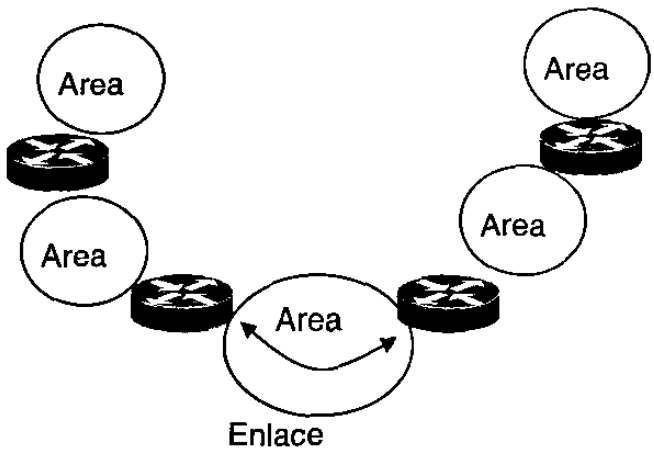



**Figura 4 - 6** Reparando o juntando 2 Áreas de Espina Dorsal

En la figura 4-6, el OSPF de dos áreas se ligan vía un acoplamiento virtual. En caso de que no exista un área común, un área adicional, tal como área 3, se podría crear para convertirse en el área del tránsito. En caso de que cualquier área que sea diferente que la espina dorsal se reparta

La espina dorsal tomará el cuidado de repartir sin usar ninguno de los enlaces virtuales. Una porción de área partida será conocida por la otra parte vía las rutas del Inter..-área más bien que por las rutas del intra-área.

## 4.10.5 Reglas de Oro para El Diseño de Áreas

Entonces usted comienza a diseñar su red de OSPF, Primero será necesario que usted comenzará con el área 0, el área de la espina dorsal de cada red del OSPF. Hay dos reglas muy importantes, que si está seguido, le consigue comenzó correctamente:

1. Un área contigua de la espina dorsal debe estar presente.

2. El resto de las áreas deben tener una conexión al área de la espina dorsal.

Los siguientes son reglas más generales y las capacidades de OSPF que ayudarán a asegurarse de que su red de OSPF siga siendo flexible y proporciona, la clase de funcionamiento necesaria para entregar el servicio confiable a todos sus usuarios:

- Considere la proximidad física al definir áreas
- Reduzca el tamaño máximo de áreas si los enlaces son inestables.
- Asegure las áreas individuales contiguas.
- Utilice los parámetros de Retoque de OSPF.

#### 4.10.5.1 Consideración de la Proximidad Física cuando se Definen las Áreas

Si una localización particular está densamente conectada, cree un área específicamente para los nodos en esa localización. Esto permitirá a OSPF manejo de un denso de número de nodos, y permitirá una gerencia y un encaminamiento más eficiente.

### 4.10.5.2 Reduciendo el tamaño Máximo de Áreas si los Enlaces son Inestables

Si su red interna incluye enlaces inestables, considere implementar áreas más pequeñas para reducir los efectos de inestabilidad de la ruta. Siempre que una ruta se caiga o se levante, cada área afectada debe converger en la nueva topología. El algoritmo de Dijkstra funcionará en todos los ruteadores afectados.

Dividiendo su red en segmentos, en áreas más pequeñas o múltiples, usted puede aislar enlaces inestables y entregar un servicio total más confiable. Esto siempre es un beneficio para todo mundo.

### 4.10.5.3 Asegurando Continuidad en Áreas Individuales

Un área contigua en OSPF es un área en la cual una trayectoria puede ser trazada de cualquier ruteador en una área a cualquier ruteador en la misma área. Esto no significa que todos los ruteadores deben compartir un mismo común medio de red (como Ethernet) Refiérase a la Figura 4- 7 para referirse a estos conceptos.

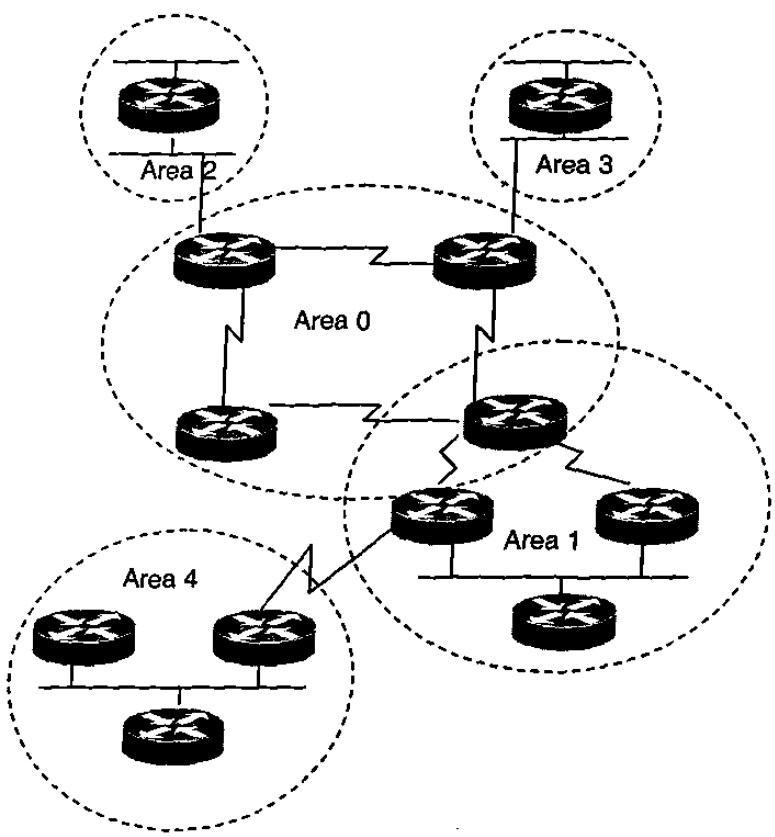



**Figura 4 - 7** Áreas contiguas en una red de OSPF

Idealmente, las áreas deben tener enlaces internos y externos redundantes múltiples para evitar particiones.

### 4.10.5.4 Usando Parámetros de Retoque de OSPF

Hay un grupo de parámetros de Retoque de OSPF que puedan ayudarle a diseñar un área, que resuelva más fácilmente las necesidades específicas de su red. Todos estos comandos y sus valores asociados son generalmente los valores por defecto, que son buenos valores. Si usted está considerando cambiarlos, es buena práctica cambiarlos en todos las ruteadores.

Recuerde, los ruteadores de Cisco no mostrarán los valores prefijados, en sus archivos de configuración.

Los Parámetros de Retoque en OSPF son los siguientes:

- `Ip ospf hello-interval (seconds)` Este comando está por defecto a 10 segundos. Modificándose este valor usted puede especificar el intervalo de la transmisión de los paquetes hello enviados de una interfaz

- `ip ospf dead interval (seconds)` Este comando omite un valor cuatro veces hola el intervalo. Este comando especifica cuánto tiempo los paquetes de una ruteador hola no deben haber sido vistos antes de que sus vecinos declaren la ruteador abajo.

- `ip ospf retransmission- interval (seconds)` Este comando omite un valor de cinco segundos. Modificando este valor, usted puede especificar el número de segundos entre las retransmisiones de LSA.

- `ip ospf transmit-delay (seconds)` Este comando omite un valor de un segundo. Modificando este valor, usted puede fijar la hora a retrasa antes de transmitir un LSA de un interfaz.

### 4.10.6 Aspectos Críticos Del Diseño De Una Área

Los dos aspectos más críticos de diseñar un área incluyen la determinación de cómo el área es tratada y la determinación de cómo el área está conectada con la espina dorsal. Las áreas deben tener un sistema contiguo de direcciones de red y/ o de subred siempre que sea posible. Usted puede tener un área con cualquier combinación de redes y de subredes, pero se desalienta fuertemente. Siempre que sea posible, usted debe hacer que un área consista en redes y subredes agrupadas para poder lograr fácilmente la sumarización de la ruta. Sin un espacio de dirección contiguo, la implementación de sumarización de ruta es imposible.

Los ruteadores que conectan un área con la espina dorsal se llaman ABR. Las áreas pueden tener un solo ABR o pueden tener ABR's múltiples. En general, usted debe tener más de un ABR por área para reducir al mínimo el riesgo de que el área sea desconectada de la espina dorsal.

#### 4.10.6.1 Diseño del Área de Espina Dorsal

La espina dorsal de OSPF (también conocida como área 0) es extremadamente importante. Si más de una área se configura en una red de OSPF, una de estas áreas tiene que ser el área 0. Al diseñar redes, es buena práctica comenzar con el área 0 y después ampliarse en otras áreas más adelante desde el inicio. Sumarizar, la espina dorsal de OSPF, es la parte de la red de OSPF que actúa como la trayectoria primaria para el tráfico que es destinado a otras áreas o redes.

La teoría aceptada de diseño de red recomienda que se acerque a tres enlaces (véase la figura 4-8). Esta teoría indica, que nunca debe haber más de tres niveles con un máximo de seis saltos de ruteador a través de los puntos más lejanos de red. Este tipo de diseño satisface a OSPF muy bien debido a sus conceptos y necesidad de área del ruteo jerárquico. Este diseño reduce tiempo de la convergencia y facilita el sumarización de ruta.

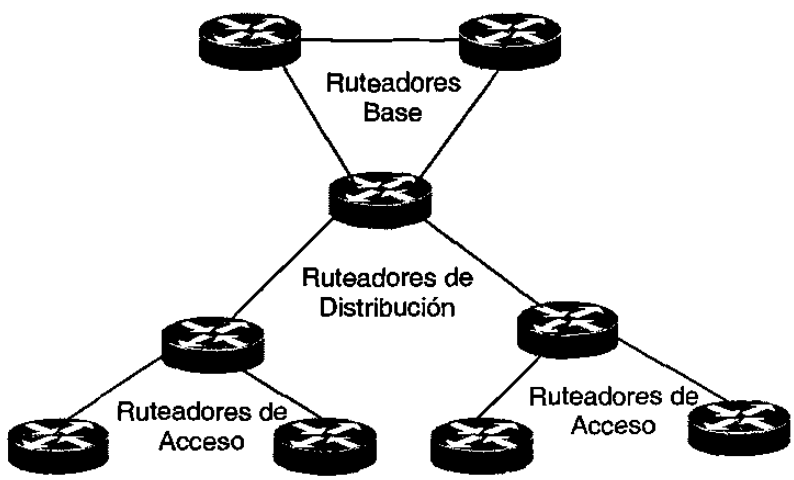



**Figura 4 - 8** Modelo del Diseño de Red del Árbol unido

Usted debe apegarse a las pautas siguientes al diseñar una espina dorsal de OSPF (área 0):

- Asegure la estabilidad de la espina dorsal
- Asegure la redundancia, como esto se llama definitivamente para en un área tan crítica.
- Asegúrese de que las espinas dorsales de OSPF estén contiguas

- Mantenga esta área simple. Entre menos ruteadores mejor

- Mantenga la ancho de banda simétrico de modo que el OSPF pueda mantener balanceo de carga.

- Asegure el resto de las áreas se conecten directamente con el área 0.

- Restrinja todos los recursos del usuario final (anfitrión) del área 0.

La espina dorsal tiene que estar en el centro del resto de las áreas, es decir, todas las áreas tienen que estar físicamente conectadas con la espina dorsal. El razonamiento detrás de esto es que OSPF espera que todas las áreas inyecten la información de encaminamiento en la espina dorsal y, alternadamente, la espina dorsal diseminará esa información de encaminamiento en otras áreas. La figura 4-9 ilustra el flujo de información de encaminamiento en una red de OSPF.

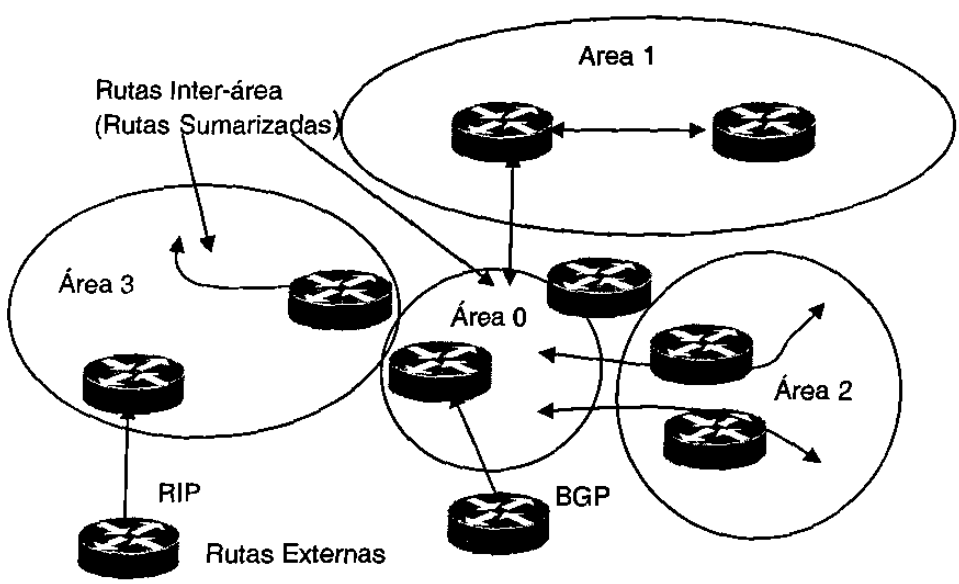



**Figura 4 - 9** La Fluctuación de la Información en una Red de OSPF, en la Cual La Espina Dorsal es la Clave

En la figura 4-9, todas las áreas están conectadas directamente con la espina dorsal. La estabilidad y la redundancia son los criterios más importantes para la espina dorsal. Mantener el tamaño de la espina dorsal, brinda resultados razonables de estabilidad. Esto es muy deseable porque cada ruteador en la espina dorsal necesita el recomputar sus rutas después de que cada cambio de estado de enlace. Manteniendo la espina dorsal pequeña reduce la probabilidad de un cambio y reduce la cantidad de ciclos del CPU requeridos al recomputo de las rutas del.

La redundancia es importante para la espina dorsal para prevenir la partición cuando se cae un enlace. Se diseña una buena espina dorsal de modo que a ninguna falla de un solo enlace pueda causar una partición (es decir, la espina dorsal se aísle). Las espinas dorsales de OSPF deben estar contiguas. Todos los ruteadores en la espina dorsal se deben conectar directamente con otros ruteadores de la espina dorsal. Evite poner a los anfitriones (tales como estaciones de trabajo, servidores de archivo, u otros recursos compartidos) en el área de la espina dorsal. Mantener a los anfitriones fuera del área de la espina dorsal simplifica la extensión de la red interna y crea un ambiente más esTabla porque la operación normal de un anfitrión (mañana/ tarde, accionan levantamiento/ caídas) y causará tráfico innecesario de LSA.

### 4.10.6.2 Enlaces Virtuales: ¿Perdición o ventaja?

El OSPF incluye el concepto de enlaces virtuales. En las situaciones raras que una nueva área sea introducida y no pueda tener un acceso físico directo a la espina dorsal, un enlace virtual tendrá que ser configurado. Un enlace virtual crea una trayectoria entre dos ABR que no estén conectados directamente. La teoría aceptada del diseño de red considera el uso de enlaces virtuales como el resultado de una espina dorsal mal diseñada.

Un enlace virtual puede conectar un ABR con la espina dorsal (área 0) aunque no esté conectada directamente (véase la figura 5-10). Con el uso de un enlace virtual, que es similar a un túnel, esto puede ser logrado.

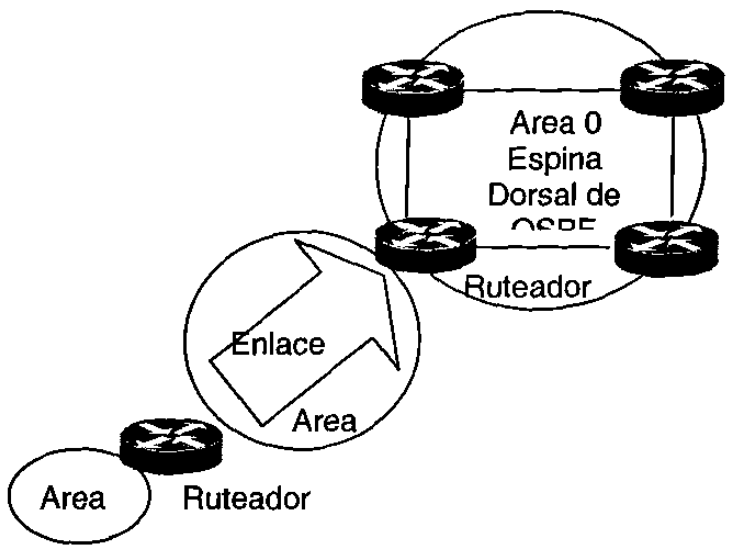



**Figura 4 - 10** Enlaces Virtuales ¿Perdición o Ventaja?

- Su estabilidad es determinada por la estabilidad del área que atravieza.
- Pueden ser configurados solamente en ABR.
- No pueden funcionar a través de áreas de Stub.
- Asisten a solucionar problemas de la conectividad de la red del a corto plazo.
- Pueden ser utilizados para asistir y proporcionar redundancia.
- El OSPF trata a dos ruteadores unidas por un acoplamiento virtual como si estuvieran conectados por una red no numerada de punto a punto.

- Los enlaces virtuales no se pueden configurar en enlaces no numerados o con áreas Stub.

Usando el comando en el modo activo (EXEC), **show ip ospf virtual –links** usted puede ver los enlaces virtuales configurados en su ruteador

### 4.10.6.3 Áreas Stub

Un área del Stub en OSPF es un área que lleva rutas por defecto, y las rutas del Inter. área pero no lleva ningunas rutas externas. Las áreas Stub reducen gastos indirectos de la red poniendo las secciones de la red en áreas de callejón sin salida, también conocidas como áreas stub. Esto reduce las rutas que son anunciadas a través de la red.

Porque se utiliza el encaminamiento por defecto, el LSDB se reduce de tamaño, que alternadamente también reduce la carga que es colocada en el CPU y la memoria del ruteador. Las actualizaciones de encaminamiento también se reducen porque las variaciones específicas de enlace no serán inyectadas a través de la red; en lugar, se confinan al área o incluso no entran en el área, dependiendo de donde ocurrieron.

Hay tres diversos tipos de áreas de Stub: Stub normal, área totalmente en Stub (TSA), y NSSA. Cada área Stub y las características correspondientes serán discutidas en las secciones que siguen.

### 4.10.6.4 Reglas de Oro para el Diseño de Áreas Stub

Muchos tropiezan reglas del diseño del área están en lugar porque un área del trozo se diseña y se configura para no llevar las ruteadores externas. Si una

situación ocurriera dentro de un área stub, los enlaces externos se inyectarán en el área, después su utilidad está arruinada. Lo siguiente son las reglas:

- Solamente un solo ABR puede estar en un área de Stub, pero si hay más de uno, entonces aceptará las trayectorias no óptimas de encaminamiento.

- Una Área Stub no puede ser ASBR.

- En una Área Stub los Enlaces Virtuales no están permitidos

- Todas los ruteadores dentro de cualquier tipo de área stub se deben configurar para reconocer su localización (es decir, qué área esta dentro y cualquier ajuste específico de OSPF para esa área). Si todos los ruteadores no convienen en su localización, entonces no se convertirán en sus vecinos y el encaminamiento no tomará efecto.

- El área de Espina Dorsal no puede ser configurada como Área Stub.

### 4.10.6.5 Áreas Stub Normales

El comando de configuración **area # stub** comienza el encaminamiento del área stub. Las rutas externas que son anunciadas en el OSPF debe ser hecho vía el comando **summary –address** esto es hecho típicamente en un ASBR.

Las áreas Stub normales tienen solamente bloques de rutas externas; sin embargo, permiten la sumarización de rutas. Por ejemplo, se permiten los tipos 1-4 de LSA y se bloquean los 5-7. Ésta es la diferencia entre las áreas Stub normales y los otros tipos de áreas Stub.

El comando que configura un área Stub es como sigue:

**area <area-id> stub [no-summary]**

El comando que configura un costo por defecto en un área es como sigue:

**area area-id default-cost cost**

Si los costos no son configurados usando el comando area area - A def ault - cost cost un costo de uno será anunciado por el ABR. La Figura 4-11 muestra un ejemplo muy bueno de las áreas Stub. En los ejemplos que siguen, los archivos de configuración del ruteador serán presentados basados sobre la disposición en la Figura 4 -11.

Asuma que el área 2 debe ser configurada como área stub. Los ejemplos siguientes muestran la tabla de encaminamiento del RTE antes y después que se configura el área 2 como área del stub.

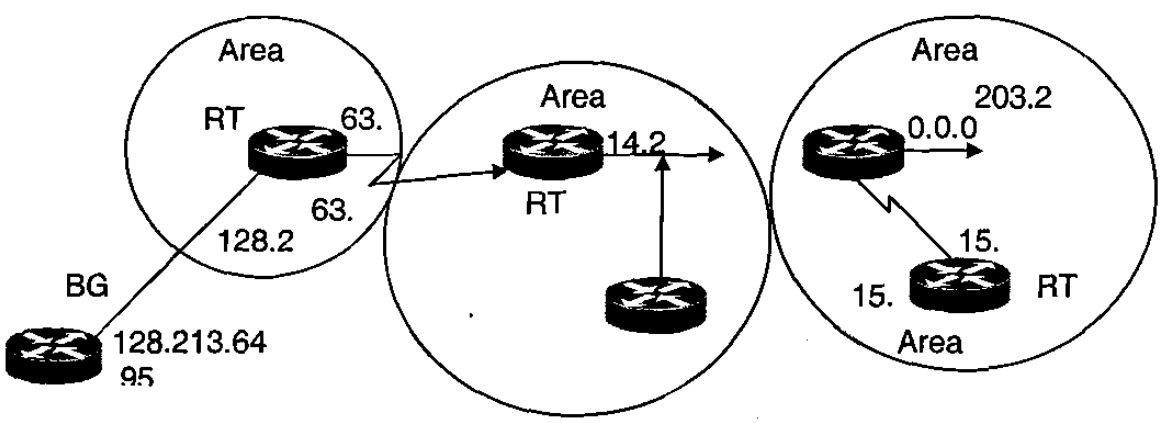



**Figura 4 - 11** Configurando un área OSPF como un área Stub

Antes de convertirse en un área Stub

```
RTC#
interface Ethernet0
ip address 203.250.14.1 255.255.255.0
 interface Serial1 ip address 203.250.15.1 255.255.255.252
router ospf 10
 network 203.250.15.0 0.0.0.255
 area 2 network 203.250.14.0 0.0.0.255 area 0

RTE#sh ip route
Codes: C - connected, S - static, I
D        EIGRP, EX - EIGRP external, 0 - OSPF, IA - OSPF inter area
El - OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, Ll - IS-IS level-1, L2 - IS-IS level-2,
Candidate default Gateway of last resort is not set
203.250.15.0 255.255.255.252 is subneted, 1 subnet
C 203.250.15.0 is directly connected, Serial0
0 IA 203.250.14.0 [110/741 via 203.250.15.1, 00:06:31, Serial0
128.213.0.0 is variably subneted, 2 subnets, 2 masks
0 E2 128.213.64.0 255.255.192.0
[110/10] via 203.250.15.1, 00:00:29, Serial0
0 IA 128.213.63.0 255.255.255.252
[110/841 via 203.250.15.1, 00:03:57, Serial0
131.108.0.0 255.255.255.240 is subneted, 1 subnets
0 131.108.79.208 [110/74] via 203.250.15.1, 00:00:10, Serial0
```

El RTE ha aprendido las rutas del Inter.-área (O - IA) 203,250,14. 0 y 128,213,63. 0, y él tiene la ruta de intra-area de (O) 131,108,79,208 y la ruta externa (O - E2) 128. 213,64. 0. Si usted configura el área 2 como Stub, usted necesita hacer lo siguiente:

*Después de convertirse en un área Stub*

```
RTC#
interface Ethernet 0
 ip address 203.250.14.1 255.255.255.0
```

```
interface Serial1
  ip address 203.250.15.1 255.255.255.252
router ospf 10
  network 203.250.15.0 0.0.0.255 area 2
  network 203.250.14.0 0.0.0.255 area 0
area 2 stub

RTE#
  interface Ethernet0
    ip address 203.250.14.2 255.255.255.0
  interface Ethernetl
    ip address 131.108.79.209 255.255.255.240
  interface Seriall
    ip address 203.250.15.1 255.255.255.252
  router ospf 10
    network 203.250.15.0 0.0.0.255
    area 2 network 203.250.14.0 0.0.0.255
    area 0 network 131.108.0.0 0.0.255.255
    area 2  area 2 stub
```

Observe que el comando de Stub está configurado en el RTE también; si no, el RTE nunca será venido un vecino a RTC. El costo por defecto no fue fijado, así que RTC anunciará 0.0.0.0 RTE con una métrica de 1.

```
RTE# sh ip route

Codes: C - connected, S - static, I IGRP, R RIP, M - mobile, B - BGP D EIGRP, EX - EIGRP
external, 0 OSPF, IA OSPF inter area El OSPF external type 1, E2 - OSPF external type 2, E - EGP
I - IS-IS, LI - IS-IS level-1, L2 -IS-IS level-2, * - candidate default
Gateway of last resort is 203.250.15.1 to network 0.0.0.0
203.250.15.0 255.255.255.252 is subneted, 1 subnets
C 203.250.15.0 is directly connected, Serial0
O -  IA 203.250.14.0 [110/74] via 203.250.15.1, 00:26:58, Serial0
128.213.0.0 255.255.255.252 is subneted, 1 subnets
O - IA 128.213.63.0 [110/84] via 203.250.15.1, 00:26:59, Serial0
131.108.0.0 255.255.255.240 is subneted, 1 subnets
O 131.108.79.208 [110/74) via 203.250.15.1, 00:26:59, Serial0
```

```
O - IA 0.0.0.0  0.0.0.0  [110/65] via 203.250.15.1, 00:26:59, Serial0
```

Observe que todas las rutas que se muestran arriba excepto las rutas externas que fueron substituidas por una ruta por defecto de 0.0.0.0. El costo de la ruta resulto ser 65 (64 para mas uno a un TI que anunciado por RTC). Usted ahora configurará el área 2 para ser totalmente stub y para cambiar el costo por defecto de 0.0.0.0 a 10:

```
RTC#
  interface Ethernet0
    ip address 203.250.14.1 255.255.255.0
  interface Serial1
    ip address 203.250.15.1 255.255.255.252
  router ospf 10
    network 203.250.15.0 0.0.0.255
    area 2 network 203.250.14.0 0.0.0.255
    area 0 area 2 stub no-summary

RTE#sh ip route
Codes: C -connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, 0 - OSPF, IA - OSPF inter area EI - OSPF
external type 1, E2 - OSPF external type 2,E – EGP I - IS-IS, LI - IS-IS level-1, L2 - IS-IS level-2,
candidate default Gateway of last resort is not set
203.250.15.0 255.255.255.252 is subneted, 1 subnets
C 203.250.15.0 is directly connected, Serial0
131.108.0.0 255.255.255.240 is subneted, 1 subnets
0 131.108.79.208 (110/741 via 203.250.15.1, 00:31:27, Serial0
O*IA 0.0.0.0 0.0.0.0 [110/74] via 203.250.15.1, 00:00:00, Serial0
```

Observe que las únicas rutas que se muestran arriba son las rutas del intra área (0) y la ruta por defecto 0.0.0.0. Se han bloqueado las rutas externas y de Inter.-área. El costo de la ruta por defecto ahora es 74 (64 mas 10 a una línea TI anunciadas por RTC). No hay configuración necesaria para RTE en este caso. El

área es ya stub, y el comando **no-summary** no afecta del todo a el paquete hello como lo hace el comando stub.

### 4.10.6.6 Áreas Totalmente Stubby

Cisco indica un TSA al configurar a los ruteadores agregando la el comando de no sumarizar a la configuración. Así, el comando de configuración necesitado es **area # stub no summary.**

Un TSA bloquea las rutas externas y las rutas sumarizadas al entrar en el área. Esto deja las rutas por defecto y las de intra. -área como los únicos tipos que son anunciados a través del área. Ésta es la técnica más completa del sumarización posible en el OSPF y los resultados son tablas de encaminamiento extremadamente pequeñas compuestas solamente de las redes encontradas en el área.

### 4.10.6.7 Áreas no-So-Stubby

Según lo mencionado en el capítulo, la "introducción al OSPF," NSSA tiene su propio RFC y es un nuevo concepto en OSPF que el advenimiento de este nuevo tipo de área híbrida stub también introdujo un LSA nuevo, el tipo 7, que es responsable de llevar la información externa de ruta.

NSSA no se soporta hasta la versión 11,2 del IOS de Cisco y más adelante.

Las dos ventajas principales del LSA Tipo - 7 son que puede ser filtrado y sumarizado flexiblemente. Generalmente hablando, el uso de un NSSA se aconseja cuando se recae entre un ASBR y un ABR, donde el ASBR está conectado con diversos protocolos de encaminamiento y el ABR conecté con el área 0 de OSPF.

En el RFC 1587 usted encontrará una descripción detallada de las razones por las cuales usted desearía utilizar un NSSA. Usted debe también leer el RFC también para la información detallada.

La operación de un NSSA es algo directa. Usted tiene un ASBR conectado a una red RIP funcionamiento. Este ruteador también se configura como parte de un NSSA. El ruteador redistribuirá las rutas aprendidas de RIP en OSPF LSA Tipo- 7 para la transmitirse dentro de NSSA. El NSSA ABR verá estos anuncios y deseará remitirlos sobre el área 0 para la distribución a través de la red. El ABR entonces redistribuirá los LSA's Tipo -7 en LSA's Tipo -5.

### 4.10.6.8 Selección de Rutas en OSPF

Al diseñar una red interna de OSPF para la selección eficiente de ruta, usted necesita considerar tres asuntos importantes:

- Retoques en las métricas de OSPF
- Controlando el tráfico de Inter.-áreas.
- Balanceo de Cargas de Inter.-redes de OSPF.

### 4.10.6.9 Retoques de métricas en OSPF

El valor prefijado para la métrica de OSPF (costo) se basa en el ancho de banda. Las características siguientes demuestran cómo se generan las métricas de OSPF:

- Cada enlace da un valor métrico basado en su ancho de banda.

- La métrica para un enlace específico es el inverso del ancho de banda para ese enlace.

- Las métricas de enlace son normalizadas para que FDDI tenga una métrica de 1.

- La métrica para una ruta es la suma de la métrica para todos los enlaces en la ruta.

En algunos casos, su red pude tener un tipo de implementación que son más rápidos que los medios más rápidos por defecto configurables para OSPF (FDDI). Un ejemplo de medios más rápidos es ATM. Por defecto, medios más rápidos serán asignados un costo igual al costo de un enlace de FDDI. Costo de la métrica de estado de enlace de 1. Dado un ambiente de FDDI y un tipo de medios más rápidos, usted debe configurar manualmente costos del enlace para configurar el enlace más rápido con una métrico más baja. Configure cualquier enlace de FDDI con un costo mayor de 1, y configure el acoplamiento más rápido con un costo menor que el costo asignado al enlace de FDDI. Utilice el comando de configuración **ip ospf** para modificar el costo de estado de enlace.

Cuando se permite la sumarización de ruta, el OSPF utiliza la métrica de la mejor ruta en la sumarización.

Se encuentra dentro de la versión 11,3 del IOS de Cisco, un nuevo comando de OSPF, **ospf auto-cost reference bandwidth**, que puede asistirle en la sumarización de la ruta.

### 4.10.6.10 Tipos de Métricas Externas : E1 y E2

Las rutas que se originan de otros protocolos de encaminamiento (o de diversos procesos de OSPF) y que se inyectan en el OSPF vía la redistribución se

llaman rutas externas. Hay dos formas de métricas externas: Tipo 1 (EL) y el Tipo 2 (E2). Estas rutas son representadas por O - E2 ó O - E2 en la tabla de encaminamiento de IP. Se examinan después de que el ruteador haga su tabla de encaminamiento interna. Después de que se examinan, se hacen flooding a través del Sistema Autónomo (AS), inalterado. La información externa podía venir de una variedad de fuentes, tales como otros protocolos de encaminamiento.

Las métricas de E1 dan lugar a las rutas a las cuales se les agrega las métricas de OSPF internas a la métrica de la ruta externa; también se expresan en los mismos términos de una métrica de estado de enlace de OSPF. La métrica de OSPF interna es el costo total para alcanzar la destinación externa, incluyendo cualesquier costo de OSPF interno de la red que se incurren para llegar allí. Estos costos son calculados por el ruteador que desea alcanzar la ruta externa.

Las E2 no agregan la métrica interna de OSPF al costo externo de las rutas, las del tipo por designación son utilizadas también por OSPF. La métrica E1 es generalmente preferida. El uso de las métricas E2 asume que el ruteador se encuentra entre un AS, por ello el costo es considerado. Esto Elimina la necesidad de métricas internas de OSPF. La Figura 4-12 Muestra bien la comparación de estas dos métricas.

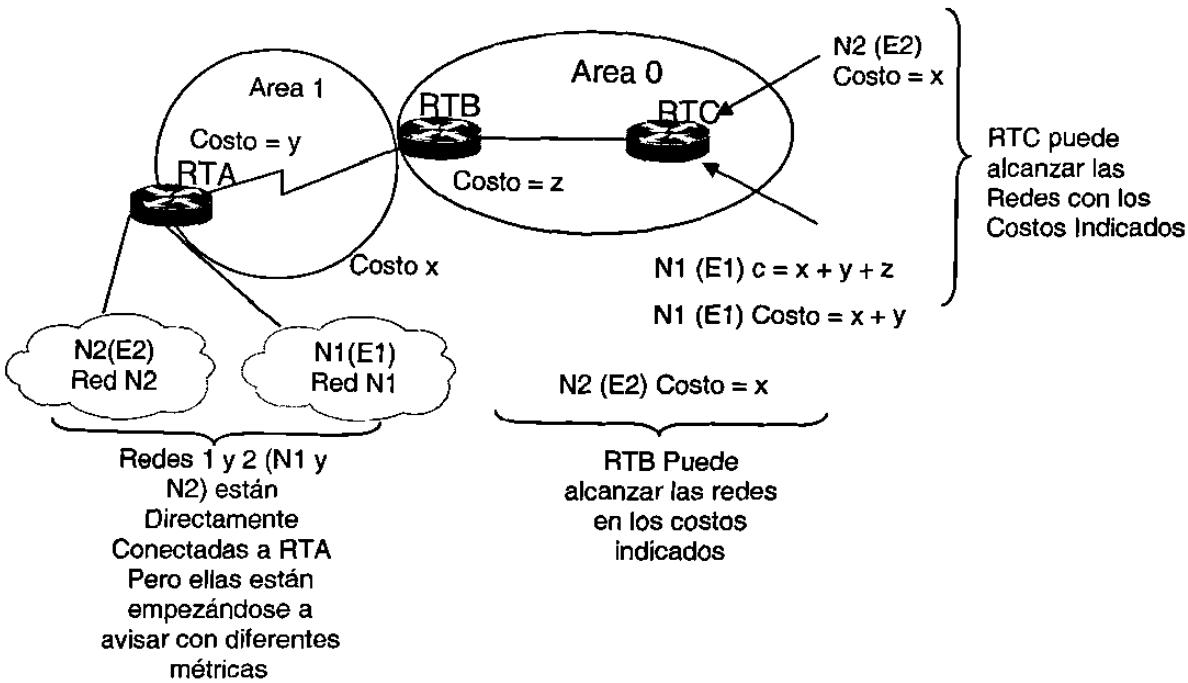



**Figura 4 - 12** E1 contra E2 Tipos de Métricas Externas

Generalmente, el último comportamiento es deseable porque la espina dorsal tiene típicamente líneas de más altos de la ancho de banda disponible. También, los paquetes más rápidos consiguen entrar allí, en un encaminamiento mas rápido a su destinación. Sin embargo, si usted quisiera que el tráfico utilizara el ABR que es el más cercano a la destinación (de modo que el tráfico deje el área tan tarde como sea posible), el ABR debe inyectar sumarizaciones de ruta en el área, en vez de inyectar la ruta designada.

La mayoría de los diseñadores de red prefieren evitar el encaminamiento asimétrico (es decir, con diferentes trayectorias para los paquetes que van de A á B y los que vienen de B á A). Es importante entender cómo el encaminamiento ocurre entre las áreas así que usted puede evitar el encaminamiento asimétrico si es del todo posible.

Las rutas que se generan dentro de una área (la destinación pertenecen al área) se llaman las rutas del intra-área. Estas rutas son representadas por la letra O en la tabla de encaminamiento de IP. Las rutas que se originan de otras áreas se llaman rutas de Inter.-área o rutas del sumarias. La notación para estas rutas es O -IA en la tabla de encaminamiento de IP.

### 4.10.6.11 Balanceo de Cargas en redes de OSPF

Como parte de su diseño, usted necesitará considerar la circulación a través de la red y si o no utilizar balancear la carga. El uso de esta característica de OSPF puede ser muy provechoso a la salud total de su red. Esta sección discute cómo a utilizar lo mejor posible la característica de balanceo de cargas de OSPF con una red.

En el encaminamiento, el balanceo de carga es la capacidad de una ruteador para distribuir el excedente de tráfico de todos sus puertos de red que tengan la misma distancia en su dirección de destinación. Los buenos algoritmos de balanceo de carga utilizan la velocidad de línea y la información de la confiabilidad. Soporta los incrementos de balanceo de carga en la utilización de los segmentos de red, así se aumenta el ancho de banda eficaz de la red.

Las topologías de red se diseñan típicamente para proporcionar rutas redundantes para prevenir una partición de red. La redundancia es también útil para proporcionar el adicional la ancho de banda para áreas con alto tráfico. Si existen las trayectorias del costos iguales entre los nodos, los ruteadores Cisco cargan automáticamente el balanceo de cargas en un ambiente de OSPF.

Fast-switching es una característica de Cisco por el que un acumulador de memoria (cache) de la ruta se utiliza para apresurar la conmutación de un conjunto

de bits a través de un ruteador. Para las velocidades de línea de 56Kbps y más rápidas, se recomienda que usted permite el Fast-switching.

Las ruteadores Cisco pueden utilizar hasta cuatro trayectorias de igual costo para una destinación dada. Los paquetes se pudieran distribuir en por destinación (al fast-switching) o por paquete. El balanceo de la cargas de por destinación es el comportamiento por defecto. El balancear de carga de por paquete puede ser permitido dando deshabilitando el Fast-switching usando **no ip route -cache** el comando de configuración de interfaz.

## 4.10.6.12 Direccionamiento de IP en OSPF y Sumarización de Rutas

La asignación de Direccionamiento de IP y la sumarización de ruta se ligan intrínsecamente al diseñar redes del OSPF. Para crear una red escalable de OSPF, usted debe implementar la sumarización de ruta. Para crear un ambiente capaz de soportar la sumarización de ruta, usted debe de implementar un esquema de direccionamiento jerárquico eficaz. La estructura de la dirección que usted implemente puede tener un impacto profundo en el funcionamiento y la escabilidad de su red de OSPF. La última meta es implementar pocas rutas como sea posible en las tablas de encaminamiento y reducir el número de actualizaciones.

La figura 4-13 ilustra las ventajas del sumarización de la ruta en una tabla de encaminamiento. Sin el sumarización, solamente tres entradas existen en la tabla de encaminamiento, y con el sumarización, sólo una entrada existe en la tabla de encaminamiento.

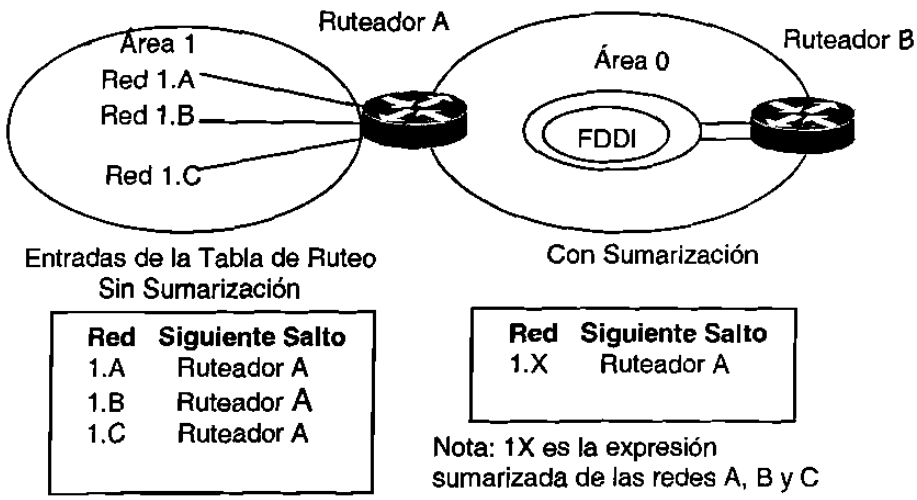



**Figura 4 - 13** Beneficios de la Sumarización de Rutas

Reglas de Oro para el Diseño del direccionamiento de IP y de la Sumarización de Rutas

Al planear su red de OSPF, considere las reglas de oro siguientes del diseño para el IP y la sumarización:

- El esquema de direccionamiento de IP de red debe ser configurado de modo que los rangos de las subredes asignadas dentro de una área estén contiguos.

- Asigne su espacio de Direcciones IP dentro de cada área de modo que permita que usted parta fácilmente las áreas mientras que su red crece.

- Siempre que sea posible, asigne las subredes según límites simples del octeto.

- Defina a fondo la estructura de la dirección de su red. Esto le permitirá asignar y planear con más eficacia y mantener su esquema de direccionamiento de IP estructurado y simple.

- Determine las localizaciones correctas de cada tipo de ruteador, área, espina dorsal, y así sucesivamente. Esto le asistirá en la determinación de qué ruteador debe sumarizar.

### 4.10.6.13 Técnicas de Sumarización de Rutas en OSPF

La sumarización de ruta es particularmente importante en un ambiente de OSPF porque aumenta la estabilidad y la eficacia de la red. La sumarización es la consolidación de rutas múltiples en un solo anuncio. Esto se hace normalmente en los ABR o de ASBR's. Aunque el sumarización se podría configurar entre cualquier dos áreas, es mejor resumir en la dirección de la espina dorsal. Esta manera la espina dorsal recibe todas las direcciones agregadas y, alternadamente, las inyectará, resumido ya, en otras áreas. Si se está utilizando el sumarización de la ruta, las rutas dentro de un área que el cambio no necesita ser cambiado en la espina dorsal o en otras áreas. Hay dos tipos de sumarización:

- Sumarización de rutas de Inter.-áreas

- Sumarización de Rutas Externas

### 4.10.6.14 Sumarización de Rutas de Inter.-áreas

La sumarización de ruta de Inter.-área se hace en los ABR's, y se aplica a las rutas dentro del AS. No se aplica a las rutas externas inyectadas en OSPF vía la redistribución. Para aprovecharse de la sumarización, los números de red en

las áreas, se deben asignar de una manera contigua de modo que usted pueda colocar estas direcciones en un rango y sumarizarlas.

Para especificar un rango de direcciones, realice la tarea siguiente en modo de la configuración del ruteador: area area-id range mascara de red.

El **area-id** es el área que contiene las redes que se sumarizan. La dirección y la máscara especificarán el rango de direcciones que se sumarizarán en un rango. La figura 4 - 14 ilustra un ejemplo de la sumarización.

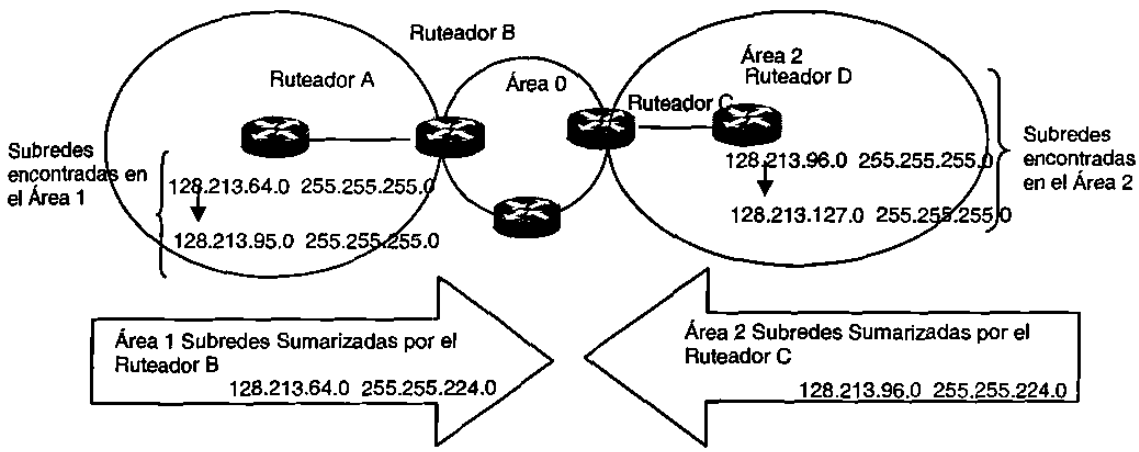



**Figura 4 - 14** Un Ejemplo de Sumarización de rutas de Inter-área

En la figura 4-14, la ruteador B está sumarizando el rango de las subredes encontrados dentro del área 1 a partir de 128,213,64,0 a 128,213,95,0 en un rango: La 128,213,64,0 con una máscara de 255,255,224,0 en la espina dorsal. Esto es alcanzada enmascarando los primeros tres bits de la extrema izquierda de 64, usando una máscara de 255,255,224,0.

De la misma manera, el ruteador C está generando la dirección sumarizada 128,213,96,0 255,255,224.0 en la espina dorsal. Observe que esta sumarización era acertada porque usted tiene dos rangos distintos de subredes, de 64-95 y de 96-127 en las áreas 1 y 2 respectivamente.

Sería difícil sumarizar si las subredes entre el área 1 y el área 2 se traslapasen. El área de la espina dorsal recibiría los rangos de sumarizaciones del traslapo y los ruteadores en el centro no sabrían dónde enviar el tráfico basado en la dirección sumaria. Lo que sigue es la configuración relativa del ruteador B, y usted puede extrapolar la configuración de la ruteador C también:

Router *B#*
router *ospf 100*
area 1 range 128.213.64.0 255.255.224.0

## 4.10.6.15 Sumarización de Rutas Externas

La sumarización externa de ruta es especificada a las rutas externas que se inyectan en OSPF vía la redistribución hecha por los ASBR's. También, cerciórese de que los rangos externos que son resumidas estén contiguos. La Sumarización que se traslapa se extiende a partir de dos diversas ruteadores, que podrían hacer que los paquetes sean enviados a la destinación incorrecta. La Sumarización se hace mediante el subcomando siguiente de OSPF en el ruteador **summary-address ip-address mask**

Este comando es eficaz solamente en ASBR's que hacen la redistribución en OSPF.

En la figura 4-15, el ruteador A y la ruteador D (ambos ASBR's) están inyectando las rutas externas en OSPF por la redistribución. El ruteador A está inyectando subredes en el rango de 128.213.64?95 y la ruteador D está inyectando subredes en el rango 128.213.96.127.

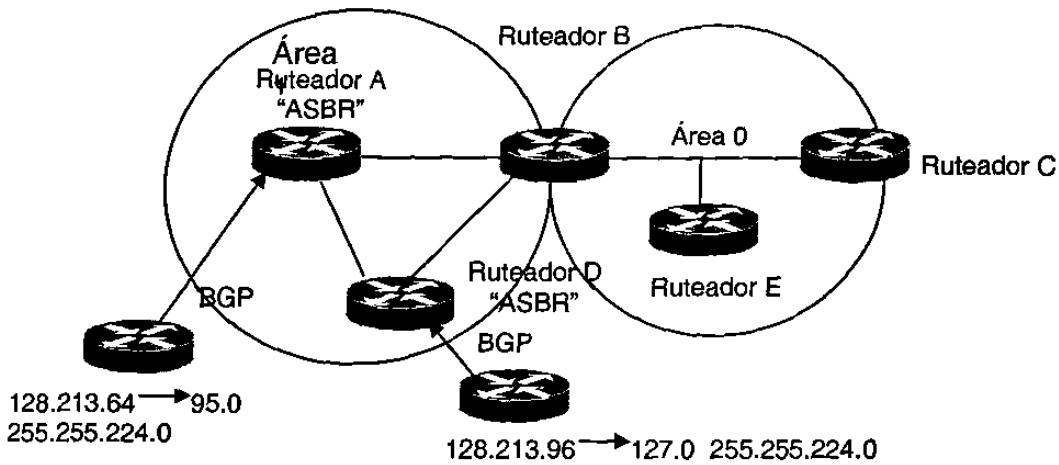



**Figura 4 - 15** Un Ejemplo de la Sumarización de Rutas Externas

Para sumarizar correctamente las subredes en una rango en cada ruteador, usted puede configurar las ruteadores como sigue:

```
Router A#
router ospf 100
summary-address 128.213.64.0 255.255.224.0
redistribute bgp 50 metric 1000 subnets

Router D#
router ospf 100
summary-address 128.213.96.0 255.255.224.0
redistribute bgp 20 metric 100 subnets
```

Esto hará que el ruteador A genere una ruta externa 128,213,64,0 con una máscara de 255,255,224,0 y hará que el ruteador D generar una ruta externa 128,213,96,0 con una máscara de 255.255.224.0. Observe que el comando de las

direcciones sumarias no tiene ningún efecto si es utilizado en el ruteador B porque el ruteador B no está haciendo la redistribución en OSPF, ni es un ASBR.

### 4.10.6.16 Sumarización de Rutas y Distribución de Rutas

La sumarización de ruta trata dos cuestiones importantes de la distribución de la información de rutas:

- **¿Qué información la espina dorsal necesita saber sobre cada área?** La respuesta a esta pregunta centra la atención en la información de encaminamiento del área a la espina dorsal.

- **¿Qué información cada área necesita saber sobre la espina dorsal y otras áreas?** La respuesta a esta pregunta se centra la atención en la información de encaminamiento de la espina dorsal a la área.

Si usted sabe las respuestas a estas preguntas, usted podrá diseñar con eficacia cómo usted necesita resumir las rutas dentro de su red del OSPF.

### 4.10.6.17 Avisos de Ruta de Área a Espina Dorsal

Hay varias consideraciones dominantes en la colocación de las áreas de OSPF para una sumarización apropiada. La sumarización de ruta de OSPF ocurre en los ABR's. El OSPF soporta las máscaras del subred de longitud variable (VLSM), así que es posible resumir en cualquier límite de bits una red o una dirección de subred. OSPF requiere la sumarización manual. Pues usted diseña las áreas, usted necesita determinar la sumarización en cada ABR.

### 4.10.6.18 Avisos de Ruta de Espina Dorsal a Área

Cuatro tipos potenciales de información de encaminamiento existen en un área y se enumeran en la tabla 4-2, que demuestra los diversos tipos de áreas según la información de encaminamiento que utilizan.

Tabla 4-2 Tipos de rutas en Areas de OSFP

| Area Type | Default | Intra-Area | Inter-Area | External |
|---|---|---|---|---|
| Non-stub | Si | Si | Si | SI |
| Stub | Si | Si | Si | No |
| TSA | Si | Si | No | No |
| NSSA | Si | Si | Si | Si |

Los tipos de rutas definidas en la tabla 4 -2 para las áreas de OSPF son como sigue:

- Rutas por Defecto. Si una ruta explícita no se puede encontrar para una red dada o una subred de IP, el ruteador remitirá el paquete a la destinación especificada en la ruta por defecto.

- Rutas De Intra-área. Las rutas explícitas de red o de subred se deben portar para todas las redes o subredes dentro de una área.

- Rutas De Inter.-área. Las áreas pueden portar las rutas explícitas de red o de subred para las redes o las subredes que están en el AS pero no en esta área.

- Rutas Externas. Cuando diversa información de encaminamiento del intercambio de AS, las rutas que se intercambian son referidas como rutas externas.

## 4.11 Escenarios de Direccionamiento y Sumarización de OSPF

Las secciones siguientes discuten el sumarización de ruta del OSPF e IP más comúnmente encontrados en tres que trata panoramas:

- Escenario 1: Asignar números únicos de red a cada área del OSPF.
- Escenario 2: Asignación de dirección compleja con solamente una sola dirección del NIC.
- Escenario 3: El Uso de Direcciones IP Privadas.

### 4.11.1 Escenario 1: Asignar números únicos de la red a cada área de OSPF

En este panorama cada área de OSPF tiene su propio rango único de Direcciones IP asignadas por el NIC. Esto puede ser tan grande como una dirección de clase A entera para una red, con múltiples clases B's asignado a cada área, o más realista, usted puede utilizar un grupo de direcciones de clase C. Este ejemplo se demuestra en la figura 4-15. Las ventajas de este método son como sigue:

- Direccionar Segmentos es muy simple
- La configuración de los ruteadores es fácil y con errores inverosímiles.
- Las operaciones de la red son dinámicas porque cada área tiene un prefijo simple único de dirección.

Los dos pasos siguientes son los pasos básicos para crear tal red:

- Defina su estructura (identifique las áreas y asigne los nodos a las áreas).

- Asigne las direcciones a las redes, a las subred, y a las estaciones finales según lo demostrado en la figura 4-16.

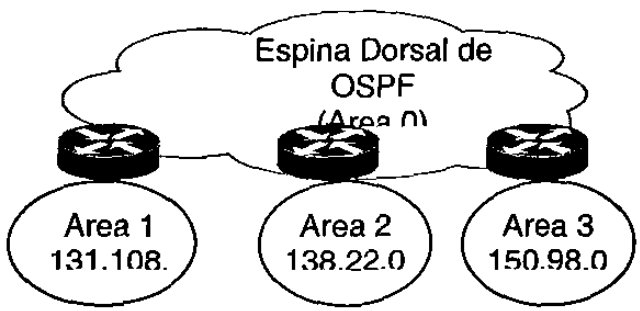



**Figura 4 - 16** Asignando únicos números de Red a cada Área de OSPF

Como ejemplo, la configuración de sumarización de ruta en los ABR's se simplifica grandemente. Las rutas del área 4 inyectadas en la espina dorsal serían sumarizadas como "todas las rutas comenzando con 150.98 que se encuentran en el área 4." Esto se puede lograr en una ruteador de Cisco con el comando siguiente:

**area 4 range 150.98.0.0 255.255.0.0**

La desventaja principal de este propuesta es que puede ser muy derrochadora con el espacio importante de Direcciones IP. Por supuesto, este espacio podría también ser muy difícil de obtener, por lo menos hasta IM.

### 4.11.2 Escenario 2: Asignación de dirección compleja con solamente una sola dirección de NIC

Puede haber una situación donde usted tenga solamente una dirección de NIC (una sola clase B por ejemplo) a asignar para todas las áreas de su red de OSPF del multiarea. Usted puede ser que también desee ahorrar un cierto espacio de dirección usando VLSM, tales que los enlaces seriales de punto a punto en cada área que tiene una mascara de subred que permita dos anfitriones por Subred.

Este ejemplo utiliza la parte del espacio de dirección para la dirección 150 100.0. 0. del NIC Se usa esto para ilustrar el concepto de " mascara de área " y también la segmentación de subredes grandes en secciones más pequeñas (VLSM's).

Los puntos que siguen listan las situaciones que se aplicaron, y describen el proceso usado para asignar direcciones:

1. Determínese cuántas áreas usted tendrá en su red de OSPF. Un valor de 500 se ha elegido para este ejemplo. (un valor de 500 áreas de red de OSPF no es realista, sino que ayudará a ilustrar la metodología usada)

2. Creé "un límite artificial de máscaras de área" en su espacio de direcciones. Las líneas punteadas en la figura 5-17 indican que usted utilizará 9 bits de la porción de subred de la dirección para identificar las áreas únicamente. Observe que èxp9=512 resuelve el requisito de 500 áreas. Solamente el espacio de dirección para dos de las 512 áreas se documenta en este ejemplo.

3. Determine el número de las subredes requeridas en cada área y el número de los anfitriones (máximo) requeridos por subred. En este ejemplo, usted

requiere siete subredes con 14 anfitriones cada uno y cuatro subredes con 2 anfitriones cada uno (las líneas de seriales).

4. El paso 3 le permite decidir a donde dibujar la línea que se divide entre la subred y el anfitrión (llamada mascara de subred) dentro de cada área. Observe que usted tiene solamente 7-bits a la izquierda a utilizar debido a la creación de la máscara artificial de área. De hecho, los 9-bits de la máscara de área son parte de la porción de la dirección de subred, pero usted ha restringido su flexibilidad de modo que usted pueda sumarizar todas las subredes de una área con un comando de rango.

La porción de espacio de dirección que tiene el campo del anfitrión de 2-bit (mascara de subred de 255,255,255,252) fue elegida arbitrariamente a partir de uno de los campos de la subred mas larga. Este método de asignar las direcciones para la porción de VLSM del espacio de dirección se hace para no garantizar ningún traslape de direcciones. Alternativamente, si el requisito había sido diferente, usted habría podido elegir cualquier número de subred más grande (con la máscara de 255.255.255.240) y segmentar rangos mas elevados a más pequeños con pocos anfitriones, o combinar varios de ellos para crear subredes con más anfitriones.

### 4.11.2.1 Pautas Realistas Del Diseño De Sumarización

Es importante observar que la muestra de direcciones y de opciones del límite de la máscara en el panorama 2 fue elegida simplemente de modo que el espacio de dirección entero de una sola área se pudiera demostrar en una sola página. No es realista tener una red de OSPF diseñada con 500 áreas. Un diseño realista pudo incluir lo siguiente:

Sobre áreas de 20 a 30 (máximo) para el AS entero.

Con las direcciones de red asignadas siguientes:

Clase B: 156. 77. 0. 0

Clase C: 198.22.33.0 198.22.34.0

### 4.11.2.2 Asignación de Áreas

Aquí, cada red de la clase C será utilizada enteramente en su propia área (similar el panorama 1) y la dirección de clase B será subdividido usando una máscara de área y distribuido entre las 16 áreas restantes. La red de clase B, 156.77.0.0, podría ser subdividido como sigue: 156, 77. x x x x y y y y .y z el límite de la máscara de área de las letras "x"," y" y "z" representan los bits de los dos octetos pasados de los bits de B. Las cuatro x de la clase se utiliza para identificar 16 áreas. Los cinco bits de "y" representan hasta 32 subredes por área. Los siete bits de z permiten 126 anfitriones (128-2) por subred.

Todos los principios usados para la sumarización y VLSM mostrados en los escenarios 1 y 2 también necesitan este ejemplo más realista.

El sumarización de la ruta es extremadamente deseable para una red interna confiable y escalable del OSPF. La eficacia del sumarización de la ruta, y su puesta en práctica del OSPF en el general, bisagras en el esquema de dirección que usted adopta. Sumarización en una red interna del OSPF ocurre entre cada área y el área de la espina dorsal. Sumarización se debe configurar manualmente en OSPF.

Debido a la asignación cuidadosa de direcciones, cada área se puede resumir con un solo comando de rango. Esto es un requisito para poder escalar una red de OSPF. El primer sistema de direcciones comenzando con 150,100.

2.0xxxxxxx (representan al octeto basado en binario) se puede sumarizar en la espina dorsal con el comando siguiente:

area 8 range 150.100.2.0 255.255.255.128

Esto significa que todas las direcciones comenzando con 150,100,2. 0xxxxxxx se pueden encontrar en el área 8.

Semejantemente, con la segunda área demostrada, la gama de direcciones comenzando con:

150.100.2.1xxxxxxx

Puede ser sumarizado como sigue:

area 17 range 150.100.2.128 255.255.255.128

Esta metodología de diseño es extensible tales que el límite de la máscara de área y las máscaras del subred se puedan dibujar en cualquier punto en el espacio de la dirección. Esto pudo ser requerido si usted habría planeado originalmente para 32 áreas en su red pero después habría decidido más adelante que usted necesitare más. Aquí, usted puede decidir tener un límite de máscara de área de longitud variable. Esto llega a ser mucho más complejo para manejar y está más allá del alcance de esta investigación. La estrategia 2 trata de simplificar un escenario que para la gente es inherentemente complicado tratar. Tenga presente que si usted hubiera mostrado el espacio de dirección entero para 150. 100.0.0, el documento tendría paginas adicionales 510.

### 4.11.2.3 Ejemplo de subred de Bit-Wise y de VLSM

Las máscaras de subred de longitud variable (VLSM) y la segmentación de red y de Bit-Wise se pueden utilizar en combinación para ahorrar espacio de

dirección. Considere una red hipotética donde se subdivide usando una máscara de área y se distribuye una dirección de clase B entre 16 áreas. La red de clase B, 156.77. 0.0, se pudo subdividir según lo ilustrado en la figura 5-16.

En la figura 5-16, las letras x, y, y z representan los pedacitos de los dos octetos pasados de la red de la clase B como sigue:

- Los cuatro bits de x se utilizan para identificar 16 áreas.
- Los cinco bits de y representan hasta 32 subredes por área.
- Los siete bits de z permiten 126 anfitriones (128-2) por subred.

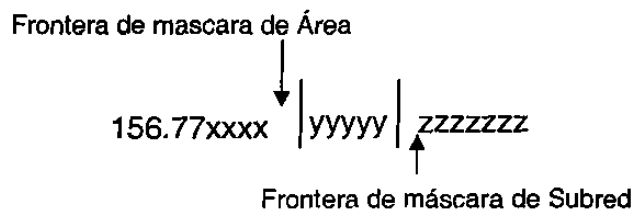



**Figura 4 - 17** Se Muestra la Frontera de Área y la Frontera de Subred

### 4.11.3 Escenario 3: El Uso de Direcciones IP Privadas

La dirección privada es otra opción citada a menudo como más simple desarrollando un esquema del área usando la segmentación de bit-wise. Aunque los esquemas privados de dirección proporcionan un nivel excelente de flexibilidad y no limitan el crecimiento de su red interna de OSPF, pero tienen ciertas desventajas.

Por ejemplo, desarrollar una red interna de gran escala de nodos privados tratados del IP limita el acceso total al Internet y asigna la implementación por comando a lo qué se refiere como zona desmilitarizada (DMZ). Si usted necesita conectarse con el Internet, la figura 5-18 ilustra la manera de la cual un DMZ proporciona un almacenador intermediario de los nodos válidos del NIC entre una red privada y el Internet.

Todos los nodos (los sistemas y las ruteadores de finales) en la red en el DMZ deben tener direcciones del IP de NIC asignadas. El NIC pudo, por ejemplo, asignarle un solo número de red de clase C. El DMZ mostrado en la figura 5-18 tiene dos ruteadores y un solo anfitrión de la entrada en uso (ApGate).

El ruteador A proporciona interfaz de entrada de DMZ y el Internet, y la ruteador B proporciona el Firewall de DMZ y el ambiente privado de la dirección. Todas los funciones que necesitan trabajar sobre el Internet deben tener acceso al Internet a través de la entrada en uso.

Los Firewalls pueden tomar muchas formas. Puede ser un ruteador configurado especialmente mediante el uso del Firewall de Cisco ature del E fijado o una máquina dedicada y diseñada en la tierra hasta realiza cluti del Firewall tal como un Fix-Firewall, Raptor Eagle, o un Firewall-1).

EL ruteador B Apgate proporciona el e-mail, la transferencia de archivo, y cualquier otro servicio al Internet requerido por los usuarios en la red privada localmente administrada de la dirección de I P
Direcciones de Red Privadas conectadas a l ruteador.

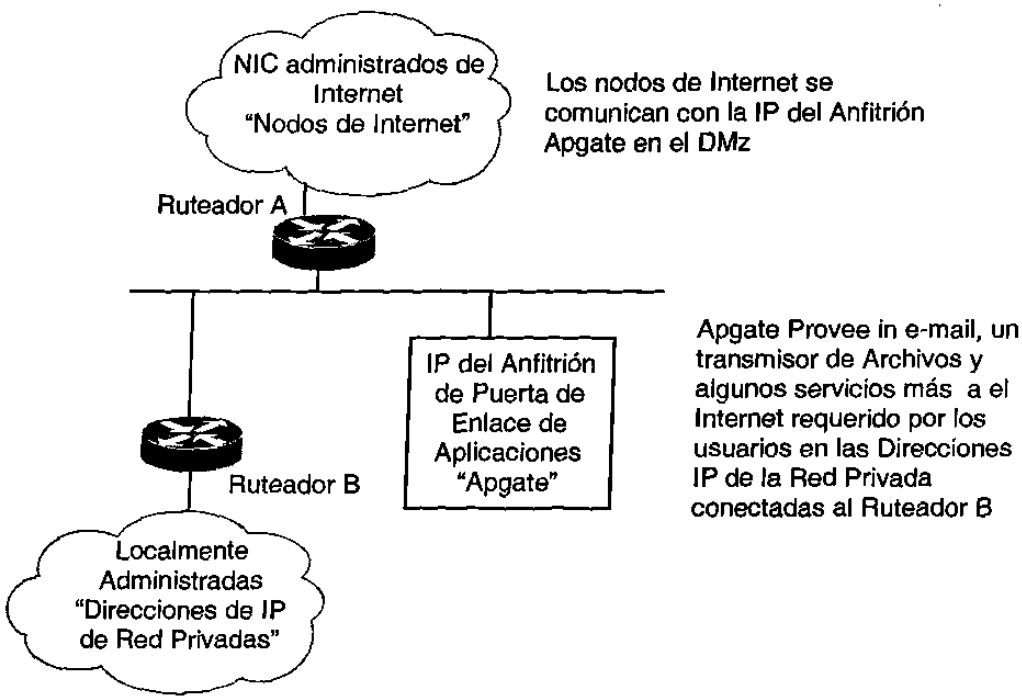



**Figura 4 - 18** Se ilustra la manera de la cual un DMZ proporciona un almacenador intermediario de los nodos válidos del NIC entre una red privada y el Internet.

## 4.12. VLSM en OSPF

Las redes de IP se dividen en direcciones de clase A, de B, y de C. Usted puede definir una máscara que especifique qué bits en la dirección definen la subred y cuáles definen el anfitrión. OSPF apoya un concepto llamado máscaras del subred de dirección variable (VLSM) que permita a un administrador utilizar diversas máscaras para el mismo número de subred en diversas interfaces.

### 4.12.1 Funcionabilidad de VLMS

Usted puede ser que desee utilizar VLSM, si usted quiere manejar el espacio de direccionamiento de IP. VLSM le permite conseguir más uso de su espacio disponible. VLSM ofrece la flexibilidad de manejar subredes con diversos números de anfitriones. Por ejemplo, un cliente que no ha puesto VLSM en ejecución tiene algunas interfaces con solamente algunos anfitriones y otras interfaces con muchos anfitriones puede elegir utilizar una máscara larga, en la primera máscara de interfaz y una mas corta en la segunda interfaz. Este espacio de dirección se debe asignar muy cuidadosamente. Es muy probable que las redes existentes necesiten el renumerar sus redes para poder aprovecharse de esta característica.

Con VLSM, usted no tiene que perder números de red en interfaces en serie, porque usted puede apoyar interfaces innumerables del IP. También, VLSM soporta subredes discontinuas. Un ejemplo de un uso de subredes discontinuas es donde un cliente tiene dos direcciones de clase B. Uno se utiliza en la espina dorsal, y otra es utilizada por los sitios. El número de red del sitio es discontinuo si hay más de un sitio con el mismo número de red. La solución existente es utilizar direcciones secundarias de IP en la misma interfaz. De esta manera, usted puede proporcionar un sistema de números de red a través de la espina dorsal y, así, conectar las subredes discontinuas.

### 4.12.2 Trampas del VLSM

Algunas de las desventajas de VLSM incluyen lo siguiente:

Es fácil incurrir en equivocaciones en la asignación de direcciones.
Es más difícil supervisar su red.

Al usar VLSM, tenga mucho cuidado sobre asignar direcciones. Por ejemplo, el numero de red interno de clase B del Cisco es 131,108.0.0.

Primero una poca ayuda de matemáticas para demostrar un cierto campo común de mascara:

Tabla 4 - *3* Mascaras Comunes y Anfitriones

| **Mask** | **Number of hosts** |
|---|---|
| *255,255.255.252* | 2 |
| *255.255.255.248* | 6 |
| *255.255.255.240* | 14 |
| *255.255.255. 224* | 30 |
| *255.255.255.192* | 62 |
| *255.255.255.128* | 126 |
| *255.255. 255. 0* | 254 |

Suponga que usted tiene dos laboratorios a los cuales usted desea asignar números de subred. El primer laboratorio es muy pequeño y nunca tendrá más de seis anfitriones. El segundo laboratorio es grande y pude necesitar soportar hasta 126 anfitriones. La cosa obvia es hacer las máscaras apropiadamente. Sin embargo, es fácil incurrir en equivocaciones al hacer esto.

Tabla 4-4 Asignación de Mascaras

| **LDs** | **Network Number** | **Mask** | **Legal Host** |
|---|---|---|---|
| Lab. A | 131.108.13.248 | 255.255.255.248 | 249-254 |
| Lab. B | 131.108.13.128 | 255.255.255.128 | 129-254 |

Esto es una configuración ilegal porque uno de los pares de red/ mascara es dependiente de la otra. Observe qué puede suceder.

Se permite a los dueños de esos laboratorios asignar sus direcciones de IP dentro de los laboratorios ellos mismos. Vamos a decir que el dueño del laboratorio A asigna un anfitrión cuya dirección de IP es 131.108.13.250 esto es con 2 anfitriones en la red 131,108,13,248. Mientras tanto, el dueño del laboratorio B asigna un anfitrión cuya dirección IP es 131.108.13.2ö esto es con 122 anfitriones en el 108.13.128. de la red 131 ambos son direcciones legales.

Sin embargo, es imposible que un ruteador diga qué anfitrión debe conseguir los paquetes que se envían a esas Direcciones IP. Peor todavía, ni unos ni otros de los dueños del laboratorio se dan cuenta que han creado un problema. Para hacer esto mas formal, la configuración siguiente de la tabla 5-5 demuestra otras posibilidades legales:

Tabla 4-5 Configuraciones de IP

| LDs | Numero de Redes | Mascara | Anfitriones Legales |
|---|---|---|---|
| Lab. A | 131.108.13.248 | 255.255.255.248 | 249-254 |
| Lab. B | 131.108.13.0 | 255.255.255.128 | 1-127 |

Una trampa final a revisar es el uso de la subred cero, que no es legal. Si usted utiliza las máscaras de subred que no caen en los límites 8-bit, usted puede terminar creando una subred no obvia en cero.

Por ejemplo, la máscara 255.255.255.0 de la red 192.111.108.0 tiene ocho anfitriones en ella (192.111.108.[1-8 ]). Usted puede intentar ampliar el número de redes estirando la máscara: de 255.255.255.240 (15 redes con 14 anfitriones cada uno) de la red 192.111.108.0.

Sin embargo, esto deja a todos los anfitriones existentes en el subred cero, que no funciona. Los anfitriones necesitan ser vueltos a numerar (17-24, por

ejemplo). Este problema existe incluso cuando VLSM no se utiliza. Sin embargo, VLSM lo hace más probablemente para ocurrir.

Según RFC 795, el único número ilegal es la subred cero. Las subredes de todos unos son legales. De hecho, el comando del IOS **ip subnet zero** brinda información acerca de la primera restricción.

### 4.12.3 Implementación Propia de VLSM

La mejor manera de utilizar VLSM es mantener el plan de enumeración existente y emigrar gradualmente algunas redes para recuperar el espacio de dirección. En la red de Cisco, la dirección de clase B es 131,108.0.0. Usted utiliza una máscara de 255,255,255. 0. Usted podría tomar una dirección y decidir utilizarla para todas las enlaces seriales, por ejemplo:

Dirección existente: número de Red : 131.108. 0. 0, máscara: 255. 255. 255. 0

Reserve una subred existente para todas las enlaces seriales: número de red: 131.108. 254. 0, máscara: 255.255. 255. 252

El uso de VLSM permite 6-bits ó 64 subredes para las líneas seriales. Estas subredes serían

131.108.254.1 y 131.108.254.2
131 .108.254.5 y 131 .108.254.6
131.108. 254.9 y 131.108. 254. 10

Observe que los números de anfitrión con todos ceros o todos unos no son soportados. Esto alcanza una mejora de 64:1 en la asignación del espacio de dirección en líneas seriales. También asume que usted está incluyendo el subred cero y la difusión.

## 4.12.4 Opciones de Interoperabilidad con VLSM

Las ruteadores en una sola área deben convenir en la máscara de red. IGRP no soporta a VLSM. Así que cuando la información se redistribuye del OSPF a IGRP, sólo una sola máscara será utilizada. La mejor manera de hacer este trabajo es ocultar todo el VLSM de IGRP. OSPF debe sumarizar las redes para alcanzar una máscara por número de red.

La idea detrás de VLSM es ofrecer más flexibilidad en tratar de dividir una red importante en subredes múltiples y todavía de poder mantener un número adecuado de anfitriones en cada subred. Sin VLSM, una mascara de subred se puede aplicar solamente a una red importante. Esto restringiría el número de anfitriones dados al número de las subredes requeridas. Si usted escoge la máscara de tal manera, de que usted tenga bastantes subredes, usted no podría asignar bastantes anfitriones en cada subred. La limitación es real para los anfitriones: una máscara que permite bastantes anfitriones no pude proporcionar bastante espacio de subred.

Por ejemplo, suponga que usted asigna una red 192 214.11.0 de clase C., y usted necesita dividir esa red con en tres subredes 100 anfitriones en una subred y 50 anfitriones para cada uno de las subredes restantes. No haciendo caso de los dos límites 0 y 255 del final, usted tiene teóricamente disponible para usted 256 direcciones (192.214.11.0 - 192.214.11.255). Esto no se puede hacer sin VLSM. La Figure 5-19 muestra un ejemplo de cómo usted puede utilizar VLSM para dividir una dirección de clase C en segmentos.

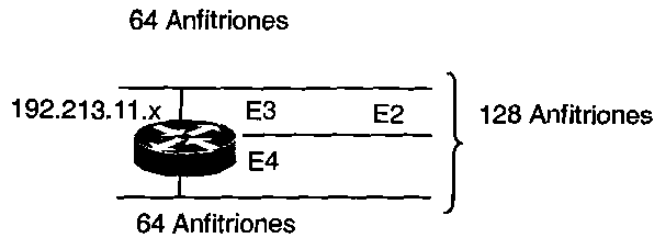



**Figura 4 - 19** Se muestra un ejemplo de cómo usted puede utilizar VLSM para dividir una dirección de clase C en segmentos

Hay un puñado de máscaras de subred que pueden ser utilizadas; recuerde que una máscara debe tener un número contiguo de unos que empiezan con la izquierda y el resto de los bits son todos ceros. Como ejemplo, algunas configuraciones comunes de VLSM incluyen lo siguiente:

- Para . . . 252 (1111 1100), El espacio de Direcciones es dividido en 64.
- Para. . . 248 (1111 1000), El espacio de Direcciones es dividido en 32.
- Para. . . 240 (1111 0000), El espacio de Direcciones es dividido en 16.
- Para. . . 224 (1110 0000), El espacio de Direcciones es dividido en 8
- Para . . .192 (1100 0000), El espacio de Direcciones es dividido en 4.
- Para . . . 128 (1000 0000), El espacio de Direcciones es dividido en 2.

Sin VLSM, usted tiene la opción de usar la máscara 255,255,255,128 y de dividir las direcciones en dos subredes con 128 anfitriones cada uno o de usar 255,255,255,192 y de dividir el espacio en cuatro subredes con 64 anfitriones cada una.

Esto no resolvería el requisito. Usando máscaras múltiples usted puede utilizar la máscara 128 y fomentar subred el segundo pedazo de direcciones con la

máscara 192. La figura 4-20 se muestra la división apropiada del espacio de dirección.

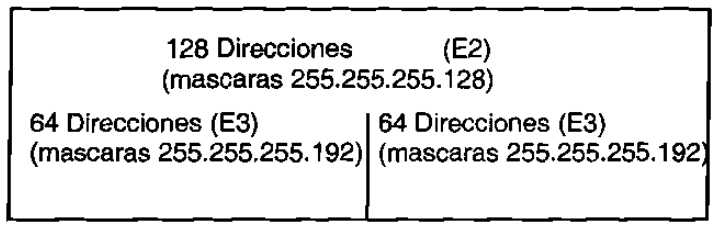



**Figura 4 - 20** Distribución de Direcciones con VLSM

Ahora, tenga cuidado en el asignación de las direcciones de IP a cada máscara. Después de que usted asigne una dirección de IP a un ruteador o a un anfitrión, usted habrá utilizado una subred entero para ese segmento. Por ejemplo, si usted asigna 192,214,11,10 255,255,255,128 a E2, el rango entero de direcciones entre 192,214. 11. 0 y 192,214,11,127 es consumido por E2. De la misma manera si usted asigna a 192,214,11 el 160 255,255,255,128 a E2, el rango entero de direcciones entre 192,214,11,128 y 192,214,11,255 es consumido por el segmento E2. Lo que sigue es una ilustración de cómo el ruteador interpretará estas direcciones. Recuerde por favor que en cualquier momento usted está utilizando una máscara diferente que la máscara natural, se quejará el ruteador si la combinación de dirección de IP y la máscara dan lugar a una subred cero. Para resolver esta edición, utilice el comando ip subnet - zero.

```
RTA#ip subnet-zero
interface Ethernet2
ip address 192.214.11.10 255.255.255.128
interface Ethernet3
ip address 192.214.11.160 255.255.255.192
interface Ethernet4
ip address 192.214.11.226 255.255.255.192
```

```
RTA# show ip route connected
192.214.11.0 is variably subneted, 3 subnets, 2 masks
C 192.214.11.0 255.255.255.128 is directly connected, Ethernet2
C 192.214.11.128 255.255.255.192 is directly connected, Ethernet3
C 192.214.11.192 255.255.255.192 is directly connected, Ethernet4
```

# Conclusiones

Este capítulo termina la discusión sobre las matemáticas que rodean el algoritmo del SPF y su operación dentro de OSPF, las diversas "reglas de oro del diseño" que fueron proporcionadas para todas las porciones esenciales de una red de OSPF. Fueron incluidas dentro de esas discusiones la capacidad de OSPF de sumarizar las rutas y las ventajas de usar una característica tan fuerte del protocolo. La discusión concluyó con una demostración de la utilidad de VLSM dentro del ambiente del OSPF.

En la conclusión, muchos de los comandos de la configuración especifica de OSPF serán presentados detalladamente en el capítulo siguiente. Todos los comandos de la configuración se agrupan juntos para su facilidad en la referencia además de la pagina de Cisco System, www.cisco.com.