UNIVERSIDAD DE LAS CIENCIAS INFORMATICAS

FACULTAD 2

DIRECCION DE GESTION TECNOLOGICA

TRABAJO DE DIPLOMA

Título: Propuesta de protocolo de enrutamiento para la Red de la UCI

Autor:

Thayli Grave de Peralta Díaz

Tutor:

Ing. Orestes Rodríguez Morales

Profesor Dpto. Sistemas Digitales.

Especialista Superior de la Dirección de Gestión Tecnológica

Cotutor

Félix Alberto Suárez Planche

Ing. Alexander Parra Yusina

Asesor

MSc. Pedro Carlos Pérez Martinto

Ciudad de La Habana, junio de 2007

"Año 49 de la Revolución"

Dedicatoria

A mi padre, que aunque ya no está,
se que estaría orgulloso de mí.
Thayli

Agradecimientos

Agradecer a todas las personas que han estado apoyándome para ser mejor cada día. A mi novio Irving Valdes Soler por ser tan comprensivo y haberme aconsejado tanto a lo largo de la carrera. A mi madre por sacrificarse tanto para que sea una profesional. A mi tutor por pelearme para que terminara la tesis. A Félix por soportarme tantas horas rectificando errores. A Pedro por darme aliento siempre. A Grisel por auxiliarme en la casa para poder adelantar este trabajo. A Yuliet por ayudarme a traducir documentos de apoyo. A todos mis amigos que siempre se preocupaban porque saliera bien. A mis profesores. En fin a todos los que siempre confiaron en mí.

Resumen

En la Universidad de la Ciencias Informáticas UCI, existen problemas con el tráfico de la red, por la topología y protocolo de enrutamiento que están implementadas. Debido a esto se hizo un estudio de un protocolo de enrutamiento nuevo para garantizar un mejor funcionamiento de la red con las nuevas proyecciones topológicas que se quieren hacer, comparándolo con el protocolo que está actualmente en la universidad, tratando de garantizar un rendimiento óptimo en la transmisión de datos a través de la red. Proponiéndose después de analizar las ventajas y las desventajas que traería consigo, un modelo de la estructura lógica del protocolo en la red de la universidad.

Índice

Introducción

La tecnología durante los últimos tiempos ha estado dominada por una gran revolución industrial y a partir de que se lanzó al mercado el computador personal, se vio la necesidad de compartir información; progresivamente los usuarios fueron reuniéndose para conectarse entre sí formando pequeños grupos para transportar, almacenar y procesar información de forma que podían intercambiar archivos y recursos físicos tales como impresoras, discos duros, unidades de disco, entre otros y con el surgimiento de Internet, esto se vio con mucho más auge. Al aumentar la demanda de procesar y obtener información, se han mejorado las técnicas de procesamiento de datos, creando así los grandes avances de la tecnología informática, que han hecho de las comunicaciones digitales una de las herramientas más importantes de la era actual.

Internet se compone de múltiples subredes interconectadas por ruteadores, los cuales utilizan la dirección IP para transportar datagramas sobre una ruta hasta la computadora destino; siendo los protocolos de enrutamiento algoritmos que permiten decidir cuál es la mejor ruta que deben seguir estos datagramas; por lo que al diseñar la red, se debe tomar una decisión importante acerca de los protocolos de enrutamiento que se utilizarán para intercambiar la información de enrutamiento.

Desde el surgimiento del protocolo de enrutamiento OSPF (Open Shortest Path First, Abrir primero la ruta de acceso más corta), ha sido pensado para el entorno de Internet como un protocolo de enrutamiento interno, es decir, que distribuye información entre ruteadores que pertenecen al mismo Sistema Autónomo. Se utiliza actualmente en la mayoría de las redes empresariales como protocolo de enrutamiento porque es muy eficiente.

Es un protocolo abierto. Responde rápidamente a cambios en la topología de la red y genera poco tráfico, proporcionando balanceo de carga entre múltiples rutas que tengan la misma distancia.

Debido a esto se quiere en este trabajo realizar una investigación detallada de este protocolo, analizando así las ventajas y desventajas que ofrece el mismo, para de esta forma hacer una propuesta de implementación para la red de la universidad.

Se propone con el objetivo de reemplazar al que se encuentra implementado actualmente, ya que con varios estudios realizados es necesario hacer un cambio de topología, que aunque únicamente determina la configuración de las conexiones entre nodos; pueden verse afectados por la misma, la distancia entre los nodos, las interconexiones físicas, las tasas de transmisión y/o los tipos de señales.

La topología en que se encuentra diseñada la red de la UCI hoy en día es en estrella; esta reduce la posibilidad de fallo de red conectando todos los nodos a un nodo central, pero todos los nodos periféricos se pueden comunicar con los demás transmitiendo o recibiendo del nodo central solamente. Sin embargo en una topología en malla, que es la topología que se quiere implementar, hay al menos dos nodos con dos o más caminos entre ellos; y aunque el número de caminos arbitrarios en las redes en malla las hace más difíciles de diseñar e implementar, su naturaleza descentralizada las hace muy útiles y son muy fiables gracias a los múltiples caminos por los que los datos pueden viajar.

Debido a este cambio necesario de topología de la red, el protocolo RIP (Routing Information Protocol, Protocolo de información de enrutamiento) v1 y 2, implementado actualmente en la universidad, cumpliría su objetivo en la transmisión de datos, pero no sería de manera óptima, ya que RIP v1 tiene lenta respuesta a los cambios que se producen en la topología de la red. Poca capacidad en las métricas utilizadas para medir la distancia entre nodos. Imposibilidad de repartir el tráfico entre dos nodos por varios caminos si estos existen por la creación de bucles que saturaban la red. Imposibilidad de discernir diferentes tipos de servicios. Imposibilidad de discernir entre host, ruteadores, diferentes tipos de redes dentro de un mismo Sistema Autónomo.

Algunos de estos puntos han sido resueltos por RIP v2, que cuenta con un mayor número de métricas, enrutamiento por subred y transmisión de multidifusión, pero no es todavía lo suficientemente óptimo.

Presentándose el problema científico siguiente:

¿Cómo atenuar los problemas de los procesos de enrutamientos con las nuevas proyecciones topológicas en la UCI mediante la implantación del protocolo de enrutamiento Open Short Path First (OSPF)?

Tomándose como objeto de estudio de la investigación a los procesos de enrutamiento en la red de la Universidad de la Ciencias Informáticas UCI.

Por tanto, se establece como objetivo general proponer un modelo de enrutamiento del protocolo OSPF, que soporte las nuevas proyecciones topológicas para la red de la UCI.

Objetivos específicos:

- Analizar ventajas del protocolo OSPF sobre RIP v1 y 2.
- Diseñar la estructura lógica del protocolo OSPF para la red de la UCI.

Tareas de investigación

1. Estudiar acerca del enrutamiento y los tipos de protocolos.
2. Estudiar acerca de la estructura funcional de los protocolos OSPF.
3. Realizar el análisis de la red actual en la UCI y su proyección futura.
4. Analizar el tráfico, cantidad de redes virtuales y características propias en la red de la UCI

Metodología a utilizar.

Métodos: Análisis y síntesis. Modelación.

Análisis y síntesis con el objetivo de buscar toda la documentación necesaria relacionada con los protocolos de enrutamiento para redes; analizar y resumir los elementos más importantes del tema, lo cual permitió elaborar el fundamento teórico de acuerdo con lo contenido hasta el momento por las ciencias informáticas en relación a los sistemas de redes.

Para ello se realizó:

Consulta bibliográfica sobre aspectos de redes y protocolos (Internet).

Modelación con el objetivo de elaborar teóricamente el funcionamiento, a partir de sus componentes, del tráfico de información mediante un nuevo protocolo con topología de malla.

Capítulo 1. Marco teórico conceptual

1.1 Algunos fundamentos de redes y conexión entre estas.

Las redes de computadoras, hoy por hoy, son una herramienta indispensable en las empresas que manejan grandes volúmenes de información. En este nuevo milenio, se hace indispensable entender que el futuro de las comunicaciones en el mundo, están lideradas por las redes.

Las redes en general, consisten en compartir recursos, información y servicios, y uno de sus principales objetivos es hacer que todos los programas, datos y equipos estén disponibles para cualquiera de la red que así lo solicite, conectados por enlaces de un medio físico (medios guiados) ó inalámbricos (medios no guiados), sin importar la localización física del recurso y del usuario. Es decir, es un sistema de comunicaciones que conecta a varias unidades y que permite intercambiar información.

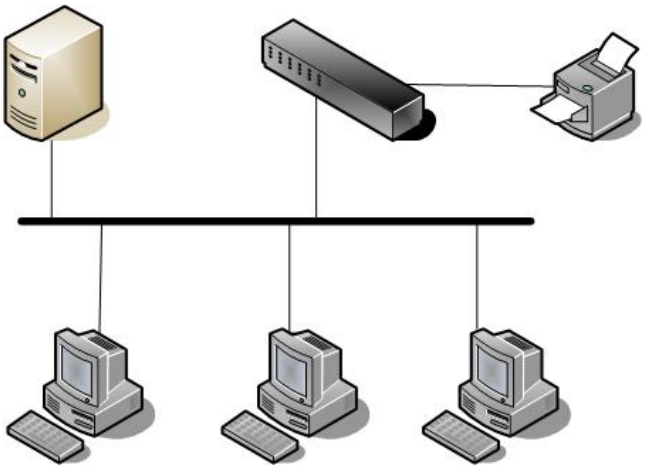


Fig.1.1 Red Real

1.1.1 Interconexión entre redes

- **Principios de la interconexión entre redes**

  – **Requisitos**

1. Proporcionar un enlace entre redes.
2. Proporcionar enrutamiento y entrega de datos entre procesos de diferentes redes.
3. Mantener un mecanismo de contabilidad y estado de redes y enrutamientos.
4. Proporcionar estos servicios sin tener que cambiar la arquitectura de la red.

Para esto, los sistemas se tienen que acomodar a las diferencias entre las redes con:

a) Diferentes esquemas de direccionamiento.
b) Diferente tamaño máximo de bloque.
c) Diferentes mecanismos de acceso a la red.
d) Diferentes valores de expiración de los temporizadores.
e) Recuperación de errores.
f) Informes de estado.
g) Técnicas de enrutamiento.
h) Control de acceso al usuario.
i) Conexión, sin conexión.

- **Enfoques sobre la arquitectura**

El modo de funcionamiento determina la arquitectura de la red.

a) **Modo de funcionamiento con conexión:** cuando se emplea este tipo de funcionamiento cada sistema intermedio conecta dos subredes. Para pasar información desde un emisor hasta un receptor, ambos sistemas establecen un circuito lógico a través de una serie de sistemas intermedios. Estos sistemas intermedios son los mismos y únicos para cada conexión de los dos equipos conectados.

Para los usuarios emisor y receptor, parece que la conexión es punto a punto. Para hacer esto posible, la capa de red del emisor, receptor y sistemas intermedios deben de proporcionar funciones similares.

b) **Modo de funcionamiento sin conexión:** en funcionamiento sin conexión el emisor envía un bloque a la red y cada sistema intermedio repite el bloque para enrutarlo al sistema

final. De esta forma, es posible que el mismo bloque llegue al destino varias veces y por distintos caminos.

En cada unidad de enrutamiento se decide el mejor camino a seguir por cada bloque, independientemente de que pertenezca al mismo emisor y al mismo destino. Para esto, es necesario que todos los sistemas emisor, receptor e intermedios tengan un protocolo similar de red (IP, Internet Protocol).

c) **Enfoque utilizando puentes:** mediante los puentes, es la capa MAC (Control de acceso al medio, debajo de la de red) la encargada de la retransmisión de los bloques. Para esto, los sistemas inicial y final deben compartir la capa de red y transporte. Además, todas las redes deben usar el mismo protocolo en la capa de enlace.

- **Interconexión entre redes sin conexión**

  - **Operación de un esquema de interconexión sin conexión**

IP proporciona un servicio sin conexión (con datagramas) con las siguientes ventajas:

- Es un sistema flexible ya que permite trabajar con muchos tipos de redes, algunas incluso con conexión.
- Es un sistema muy robusto.
- Es el mejor sistema para un protocolo de transporte sin conexión.

Ejemplo: sean dos sistemas (**A** y **B**) que pertenecen a dos redes distintas conectadas por medio de otra red WAN (Redes de Área Metropolitana). La red WAN es de conmutación de paquetes. Los sistemas **A** y **B** deben de tener el mismo protocolo IP de red e idénticos protocolos superiores (de transporte y de aplicación). Los dispositivos de enrutamiento sólo deben de implementar las capas de red e inferiores. El protocolo IP de **A** recibe bloques de datos y les añade una cabecera de dirección global de red (dirección de red de la estación **B**). De esta forma, se construye un datagrama. Este datagrama se pasa a la red y es recibido por el primer sistema de enrutamiento que lee la cabecera IP y pone la cabecera necesaria para poder ser leído por la WAN. La WAN lo recibe y lo pasa al sistema de enrutamiento que lo va a guiar a la estación final. Este sistema de enrutamiento quita la cabecera de la WAN y pone la

de IP para enviarlo al sistema final donde llegará a su protocolo IP (y será pasado sin cabecera IP a su capa superior). El sistema final hace lo mismo. Cuando un dispositivo de enrutamiento lee la cabecera IP del datagrama que tiene que enrutar y no sabe dónde enviarlo, devuelve un datagrama con la información del error.

Cada nueva unidad de datos se pone en cola de su capa inferior hasta que le llega el turno de ser enviada. Si hay dos redes conectadas por un sistema de enrutamiento, éste puede desechar datagramas de su cola para así no perjudicar la red más rápida esperando datagramas de la más lenta.

IP no garantiza que los datos lleguen a su destino y en orden, es TCP la que se encarga de esto.

IP, al no garantizar el orden y llegada de datos, funcionará con cualquier tipo de red ya que los datos pueden seguir caminos múltiples antes de llegar a su destino. Esto le permite además, cambiar de rutas cuando hay congestión o algún tipo de compatibilidad.

- **Cuestiones de diseño**

La arquitectura de interconexión de redes es similar, en su ámbito, a la arquitectura de red de conmutación de paquetes. Los dispositivos de enrutamiento son similares en su funcionamiento a los nodos de conmutación de paquetes y usan las redes intermedias de una forma semejante a los enlaces de transmisión.

d) **Enrutamiento:** se implementa mediante una tabla en cada sistema de enrutamiento y en cada sistema final. Por cada red de destino, el siguiente dispositivo de enrutamiento al que hay que enviar el datagrama. Las tablas pueden ser estáticas o dinámicas, siendo las dinámicas mejores porque se pueden actualizar cuando hay congestión o sistemas intermedios en mal funcionamiento. En las tablas se pueden incluir sistemas para manejar la seguridad (se le puede impedir el acceso a ciertas redes o a ciertas estaciones no acreditadas). Puede hacerse enrutamiento en la fuente, indicando ésta en el datagrama el camino a seguir. En los propios datagramas, los sistemas de enrutamiento pueden adjuntar información de su dirección para difundirla en la red.

e) **Tiempo de vida de los datagramas:** para evitar que un datagrama circule indefinidamente por la red, se puede adjuntar un contador de saltos (que va decreciendo cada vez que salta a un dispositivo de enrutamiento) o un contador de tiempo que haga que pasado un cierto tiempo, el datagrama sea destruido por un dispositivo de enrutamiento.

f) **Segmentación y ensamblado:** puede ser necesario que los paquetes, al pasar de unas redes a otras, deban de ser troceados por necesidades propias de dichas redes. Se puede dejar que el sistema final los vuelva a ensamblar, pero esto hace que haya demasiado trabajo para él y además, puede que haya subredes intermedias que puedan trabajar con bloques más grandes que los suministrados por la red anterior, de forma que se pierde eficiencia. Pero las ventajas de este sistema de ensamblado al final es que los dispositivos de enrutamiento no tienen que mantener en memoria los sucesivos trozos del datagrama y además se permite enrutamiento dinámico (ya que los sucesivos trozos no tienen por qué tomar el mismo enrutamiento). En IP se hace el ensamblado final. El sistema final debe de tener la suficiente memoria para ir guardando los trozos para ensamblarlos cuando lleguen todos. Como IP no garantiza la llegada de todos los datos, se debe utilizar un sistema de temporización (usando un tiempo propio desde la llegada del primer trozo del datagrama o usando los datos de temporización incluidos en la cabecera del datagrama).

g) **Control de errores:** IP no garantiza la llegada de un datagrama, pero debe de informar a la estación o dispositivo de enrutamiento del error.

h) **Control de flujo:** el control de flujo en servicios sin conexión se realiza enviando tramas de retención a los dispositivos anteriores para que éstos paren de enviar datos.

1.2 Algunos fundamentos de enrutamiento y los protocolos que se usan

Teniendo en cuenta las necesidades y los avances producidos en una sociedad sumamente compleja, resulta de gran importancia destacar tanto la transmisión de información, como la necesidad de que ésta llegue a su destino en el momento preciso mediante el uso de las redes.

Es a través de la Internet que queda probado, y todos los días se muestra con mejor y mayor detalle, que ha sido y será revolucionaria en las áreas de los servicios financieros, de entretenimiento, salud, educación, etc.

El proceso de digitalización de todas las técnicas de comunicación, transmisión (cable, satélite) y recepción, produce nuevas convergencias entre diferentes sectores (cultura, comunicación, lengua, educación, telecomunicaciones, etc.), pero muy especialmente lo que produce es la transformación de los "espacios de comunicación", los límites y las fronteras y, como consecuencia, la trasformación de los espacios de intercambios culturales.

Los principales cambios estructurales de la sociedad se producen ahora entorno al tratamiento y a la transmisión de la información.

La capa de red, dentro de una arquitectura de red de datos, es la que se encarga de llevar los paquetes de datos desde el origen (estación transmisora) hasta el destino (estación receptora). Llegar al destino, en tiempo y forma, puede requerir que el algoritmo de ruteo, que es el encargado de escoger las rutas y las estructuras de datos, cumpla con ciertas propiedades que aseguren la eficiencia de su trabajo.

Estas propiedades son: corrección, estabilidad, robustez, equitatividad, sencillez, imparcialidad y optimalidad.

La corrección y la sencillez casi no requieren comentarios; no así la necesidad de robustez, la cual se refiere a que el algoritmo debe ser diseñado para que funcione dentro de la red por años, sin fallas generales. El algoritmo deberá estar preparado para manejar cambios de topología y tráfico sin requerir el aborto de las actividades o el re arranque de la red.

La estabilidad, ya que es posible que si un sistema es muy robusto, se convierta en inestable al reaccionar demasiado brusco ante situaciones concretas.

La imparcialidad, porque hay sistemas que premian, en aras de optimalidad, las conexiones cercanas frente a las más lejanas, con lo que la comunicación entre estaciones alejadas se dificulta.

La equitatividad y la optimalidad resultan con frecuencia contradictorias, ya que muchas veces se requiere una concesión entre la eficacia global (optimización) y la equitatividad; es decir, antes de intentar encontrar un justo medio entre estas dos, se debe decidir qué es lo que se busca optimizar.

Minimizar el retardo de los paquetes (disminuyendo escalas y ancho de banda) y maximizar el rendimiento total de la red sería la combinación más apropiada para un algoritmo de ruteo.

El enrutamiento es el proceso usado por el ruteador para enviar paquetes a la red de destino, es así como un ruteador toma decisiones en función de la dirección IP destino de los paquetes de datos. Cuando los ruteadores usan enrutamiento dinámico, esta información se obtiene de otros ruteadores, y cuando se usa enrutamiento estático, el administrador de la red configura manualmente la información acerca de las redes remotas.

- **Criterios sobre prestaciones**

Hay dos formas de elegir un enrutamiento eficiente: una es elegir el camino más corto (que la distancia entre la estación emisora y la receptora sea la mínima) y otra es elegir el menor número de saltos (que entre la estación emisora y la receptora haya el menor número de nodos). En aplicaciones reales se suele elegir la del camino más corto.

- **Lugar e instante de decisión**

El instante en que se decide hacia dónde se enviará un paquete en un nodo es muy importante. Hay dos lugares donde se puede decidir hacia dónde debe enviarse un paquete desde un nodo: una es en el propio nodo (enrutamiento distribuido) y otra en un nodo señalado para esta tarea (enrutamiento centralizado).

Esta última forma tiene el inconveniente de que si este nodo se estropea, el enrutamiento de todos los nodos que dependen de este nodo de enrutamiento es imposible, y todos los nodos serán inservibles. Hay otra forma de controlar el enrutamiento, y es en la propia estación de origen.

1.2.1 Estrategias de enrutamiento

1. Enrutamiento estático. Cada nodo enrutará sus datos a otro nodo adyacente y no cambiará dicho enrutamiento nunca (mientras dure la topología de la red). Existe un nodo de control que mantiene la información centralizada.

Como cada nodo enrutará sus datos sólo a un nodo adyacente para cada nodo destino posible, sólo es necesario almacenar estos contactos entre nodos adyacentes y no todos los caminos entre todos los nodos de la red.

En el nodo central se almacenan todas las tablas de enrutamiento, pero en cada nodo sólo hay que almacenar las filas que conectan ese nodo con el siguiente para conseguir el enrutamiento a cada nodo posible destino de la red.

Este sistema es muy eficiente y sencillo pero poco tolerante a fallos en nodos adyacentes, ya que sólo puede enrutar a uno.

2. Inundaciones. Consiste en que cada nodo envía una copia del paquete a todos sus vecinos y éstos los reenvían a todos sus vecinos excepto al nodo del cuál lo habían recibido. De esta forma se asegura que el paquete llegará a su destino en el mínimo tiempo posible. Para evitar que a un nodo llegue un paquete repetido, el nodo debe guardar una información que le haga descartar un paquete ya recibido.

Esta técnica, al ser muy robusta y de coste mínimo, se puede usar para mensajes de alta prioridad o muy importantes. El problema es la gran cantidad de tráfico que se genera en la red. Esta técnica libera de los grandes cálculos para seleccionar un enrutamiento.

3. Enrutamiento aleatorio. Consiste en que en cada nodo, se elegirá de forma aleatoria el nodo al cuál se va a reenviar el paquete. De esta forma, se puede asegurar que el paquete llegará al destino pero en un mayor tiempo que en el de inundaciones. Pero el tránsito en la red es mucho menor. Esta técnica también libera de cálculos para seleccionar el enrutamiento.

4. **Enrutamiento adaptable o dinámico.** Consiste en que la red va cambiando su sistema de enrutamiento conforme se cambian las condiciones de tráfico de la red. Para conseguir esto, los nodos deben de intercambiar información sobre congestión de tráfico y otros datos.

En estas técnicas de intercambio de información entre nodos, pueden hacerse intercambios entre nodos adyacentes, todos los nodos, o incluso que haya un nodo central que coordine todas las informaciones.

Los inconvenientes principales son:

- El costo de procesamiento en cada nodo aumenta.
- Al intercambiar información de nodo en nodo, aumenta el tráfico.
- Es una técnica muy inestable.

Las ventajas:

- El usuario cree que aumentan las prestaciones.
- Se puede ayudar en el control de la congestión.

1.2.2 Funciones de un Enrutador

- Determinar las trayectorias óptimas a través de una red.
  - Menor retardo.
  - Mayor fiabilidad.

- Transportar paquetes a través de la red.
  - Examina la dirección de destino del paquete.
  - Decide a través de que puerto enviar el siguiente paquete.
  - Basa su decisión en la tabla de rutas.

- Los ruteadores interconectados intercambian sus tablas de rutas para mantener una visión clara de la red.

- En una red grande, los intercambios de tablas pueden consumir mucho ancho de banda.
    - Se requiere un protocolo para actualización de rutas.

En una red de gran tamaño, el mantenimiento manual de las tablas de enrutamiento puede requerir de una enorme cantidad de tiempo de administración. En redes pequeñas, con pocos cambios, las rutas estáticas requieren muy poco mantenimiento.

1.2.3 Enrutamiento estático y dinámico

Enrutamiento estático es la solución más simple

Limitaciones

- Laborioso de configurar
- No se adapta a la adición de nuevos enlaces o nodos
- No se adapta a las fallas de los enlaces o los nodos
- No maneja fácilmente trayectorias diferentes hacia el mismo destino
- No permite crecimiento

Características deseables en el enrutamiento dinámico

- Detectar automáticamente los cambios y adaptarse a ellos.
- Proveer siempre trayectorias óptimas.
- Escalabilidad.
- Robustez.
- Simplicidad.
- Convergencia Rápida.
- Algo de control sobre las alternativas de enrutamiento.
    Ej. Qué enlaces se prefiere utilizar.

Qué es convergencia:

- La Convergencia ocurre cuando todos los ruteadores tienen la última información.
- Mientras la red no converge, hay averías
  - Los paquetes no van a donde deben ir.
    - Agujeros negros (Los paquetes “desaparecen”).
    - Bucles (Los paquetes viajan una y otra vez entre los dos mismos nodos).
  - Ocurre cuando un enlace o un ruteador cambia de estado.

Los algoritmos dinámicos son los preferidos en la mayoría de las redes debido a su capacidad de responder a cambios en el estado de la red.

En una red estática y pequeña, las tablas de enrutamiento se pueden crear y mantener manualmente. En redes mayores los ruteadores mantienen sus propias tablas actualizadas intercambiando información unos con otros. Pueden descubrir dinámicamente:

-Si se ha añadido una nueva red.

-Que el camino a un destino ha fallado y que ya no se puede alcanzar dicho destino.

-Se ha añadido un nuevo enrutador a la red. Este enrutador proporciona un camino más corto a ciertos lugares.

No existe una única norma para el intercambio de información entre ruteadores. La libertad de elección del protocolo más apropiado ha estimulado la competencia y ha conseguido una gran mejora en estos protocolos.

Por lo que la solución sería usar enrutamiento dinámico, ya que cuando una red crece, este sería la única manera factible de gestionar la red. Planteándose la necesidad de utilizar protocolos de enrutamiento dinámico en vez de usar rutas estáticas en todos los nodos.

En Informática y Telecomunicaciones, un protocolo es una convención, o estándar, o acuerdo entre partes, que regula la conexión, la comunicación y la transferencia de datos entre dos sistemas. En su forma más simple, un protocolo se puede definir como las reglas que

gobiernan la semántica (significado de lo que se comunica), la sintaxis (forma en que se expresa) y la sincronización (quién y cuándo transmite) de la comunicación. Es el conjunto de reglas que especifican el intercambio de datos u órdenes durante la comunicación entre las entidades que forman parte de una red.

1.2.4 Funciones Principales de los Protocolos de Enrutamiento

- Definición de la asignación de pines en la interfaz física.
- Definición de la disciplina de línea a ser usada (Full dúplex – Half dúplex).
- Definición del medio y las interfaces para acceso al medio.
- Detección y corrección de errores en la transmisión.
- Definición de la señalización y codificación a ser usada.
- Proveer una secuencia para los paquetes de datos transmitidos.
- Establecer una técnica de enrutamiento dentro de la Red.
- Garantía confiable de la transmisión y recepción de los datos.
- Establecer una disciplina de dialogo para determinar quien transmite en un momento dado y por cuanto tiempo.
- Proveer un método para establecer y terminar una conexión.
- Establecer una técnica para compresión o encriptación de los datos.

1.2.5 ¿Cómo opera un protocolo de enrutamiento?

Un proceso recibe un mensaje, lo procesa y envía una respuesta, sin que exista relación entre este evento y otro anterior o posterior.

El proceso origen, conocerá la dirección del proceso destino y la incluirá en el mensaje. Esta dirección, identificará únicamente a un procesador, quién conocerá al proceso destino. El originador cuando despacha un mensaje, entra en un estado de espera de respuesta en una de sus puertas.

El proceso destino ejecuta la función especificada en el mensaje, construye la respuesta (con resultados y dirección del origen) y envía el mensaje respuesta por una puerta de salida,

(quedando libre para aceptar otro mensaje).

La respuesta llega al originador, quien realiza un chequeo para asegurarse que viene del lugar correcto antes de aceptarla, luego, pasa al estado “no espera respuesta” en esa puerta de entrada.

Este es un protocolo muy simple, necesita de la sintaxis para definición de formatos de los mensajes y una semántica muy simple. Debe considerarse el hecho que la red introduce demoras causadas por congestión, enrutamiento, etc., e incluso puede ocurrir pérdida del mensaje.

Para esto, el proceso que realiza la consulta deberá tener un reloj (timer) el que será activado al enviar el mensaje. El reloj enviará una señal al expirar el tiempo indicado en la activación indicando que la respuesta no llegó en el tiempo esperado, por lo que el mensaje deberá ser retransmitido.

Un protocolo de enrutamiento es el esquema de comunicación entre ruteadores. Permite que un ruteador comparta información con otros ruteadores, acerca de las redes que conoce así como de su proximidad a otros ruteadores.

Los protocolos de enrutamiento aprenden todas las rutas disponibles, incluyen las mejores rutas en las tablas de enrutamiento y descartan las rutas que ya no son válidas. El ruteador utiliza la información en la tabla de enrutamiento para enviar los paquetes de datos. El algoritmo de enrutamiento es fundamental para el enrutamiento dinámico. Al haber cambios en la topología de una red, por razones de crecimiento, reconfiguración o falla, la información conocida acerca de la red también debe cambiar.

Las funciones de red bajo el control de una organización se denominan un Sistema Autónomo (Autonomous System, AS). Una organización puede elegir el protocolo de intercambio de información de enrutamiento que desee para su propio AS. Un sistema autónomo o AS será la subred que es administrada por una autoridad común, que tiene un protocolo de ruteo homogéneo mediante el cual intercambia información en toda la subred y que posee una política común para el intercambio de tráfico con otras redes o sistemas autónomos.

Cada AS es operado por una organización diferente y puede usar internamente su propio algoritmo de enrutamiento. Por ejemplo, las redes internas de las compañías X, Y, y Z generalmente se verían como tres AS si las tres estuvieran en Internet. Las tres pueden usar algoritmos de enrutamiento diferentes internamente. No obstante, la existencia de estándares aún para ruteadores internos, simplifica la implementación en las líneas divisorias entre los AS y permite la reutilización de código. El algoritmo de enrutamiento interno de un AS se llama Protocolo de Pasarela Interior (Interior Gateway Protocol, IGP); al algoritmo de enrutamiento entre varios AS se le llama Protocolo de Pasarela Exterior (Exterior Gateway Protocol, EGP).

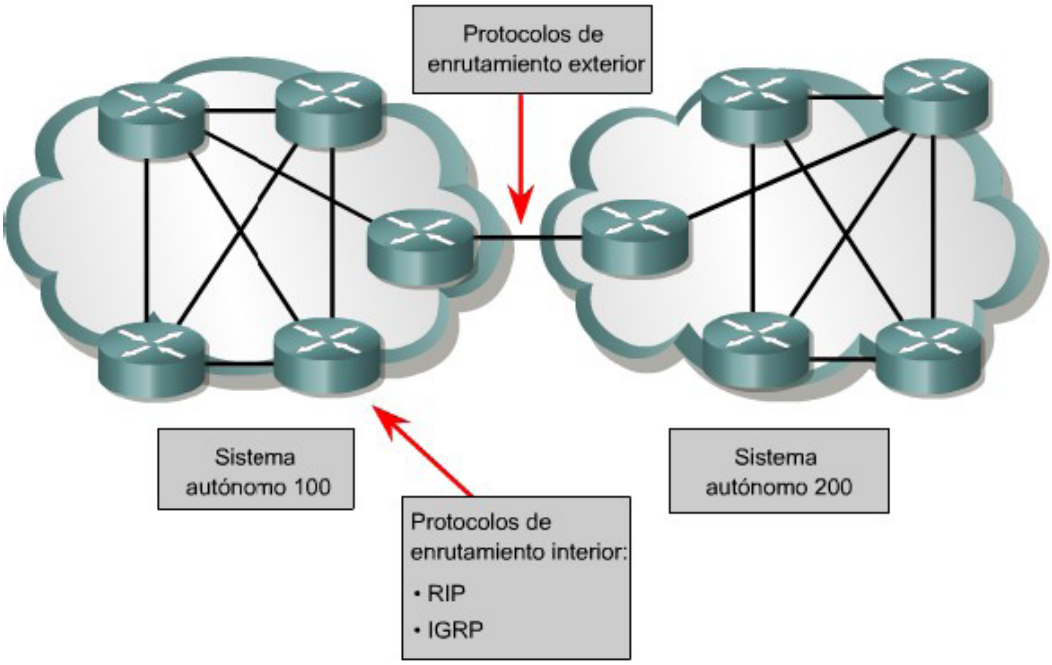


Fig.1.2 Protocolo de Enrutamiento Interior (IGP) y Exterior (EGP).

1.2.6 IGP: está diseñado para ser usado en redes cuyos segmentos se encuentran bajo el control de una sola organización. Los criterios de diseño de este tipo de protocolo requieren que encuentre la mejor ruta a través de la red.

Los IGPs más usados son:

· RIP.

· OSPF.

Algoritmos de enrutamiento usados en IGPs:

· Vector-distancia

· Estado del enlace

- **Vectores de Distancias (Distance Vector)**

Los ruteadores cooperan en un cálculo distribuido de las rutas. El algoritmo en cada ruteador calcula el mejor camino (mínimo costo) a todos los destinos. Cada ruteador informa a sus vecinos de las rutas que ha calculado. Informan de la dirección (vector) y el costo (la distancia) a cada destino. Viendo las rutas anunciadas por los vecinos puede que el ruteador encuentre un mejor camino (menor costo). El algoritmo, tras varias iteraciones, converge a los mejores caminos (se estabilizan las rutas). El cálculo es: simple, asíncrono, incremental y distribuido. La tarea más difícil en uno de estos algoritmos es prevenir la inestabilidad.

Ejemplos: RIP, IPX-RIP, DECnet, IGRP, EIGRP

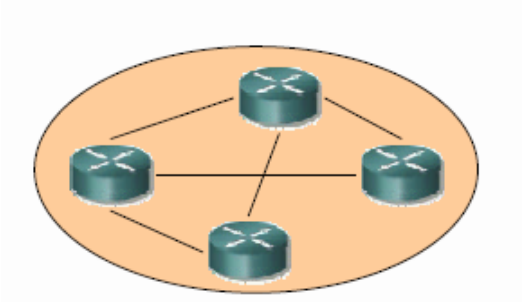


Fig.1.3 Vectores de Distancias.

- **Estado de Enlaces (Link State)**

Aproximación de base de datos distribuida replicada en vez de un cálculo distribuido incremental. Cada ruteador posee información global sobre la red: nodos y enlaces existentes. Cada ruteador envía periódicamente una descripción de su conexión (el estado de su enlace) a sus vecinos (aquellos conectados a la misma red). Todos los ruteadores tienen una imagen (grafo) de la red (todos la misma) y a partir de ahí eligen los caminos. Este tipo de protocolos, a diferencia de los protocolos vector-distancia, envían actualizaciones cuando hay noticias. Lo importante es la información intercambiada en el estado de enlace, no el contenido de la tabla de enrutamiento. Los usuarios consiguen respuesta a los eventos de red más rápido, convergencia más veloz, y acceso a servicios de red más avanzados.

Ejemplos: OSPF, IS-IS, PNNI

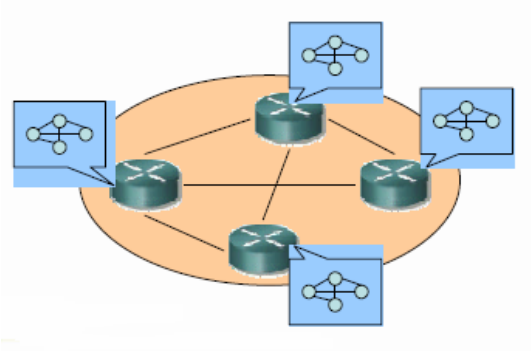


Fig.1.4 Estado de Enlaces.

1.2.7 EGP: está diseñado para ser usado entre dos redes diferentes, las cuales se encuentran bajo el control de dos organizaciones diferentes.

El EGP más usado es:

- El protocolo BGP (Border Gateway Protocol, Protocolo de Pasarela de Borde)

Algoritmos de encaminamiento usado:

- Vectores de Ruta

➢ **Vectores de Ruta (Path Vector)**

Similar al Vector de Distancia**.** Cálculo distribuido**.** Los ruteadores informan a sus vecinos de las rutas calculadas pero incluyen todo el camino (path) hasta el destino de cada ruta.

Ejemplo: BGP

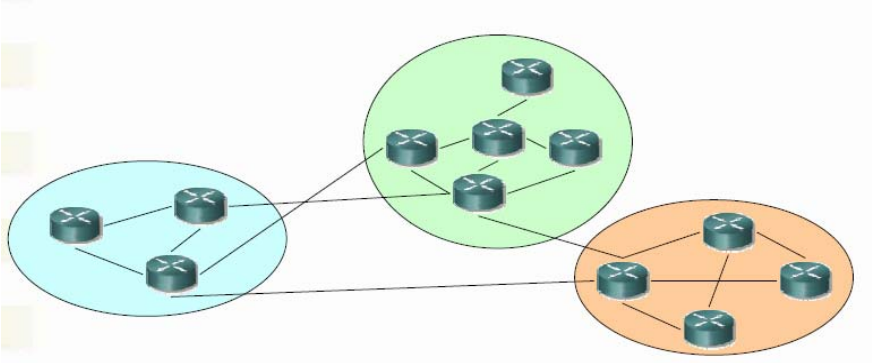


Fig.1.5 Vectores de Ruta.

El protocolo RIP

- Es un protocolo de enrutamiento por vector-distancia.
- Utiliza el número de saltos como métrica para la selección de rutas.
- Si el número de saltos es superior a 15, el paquete es desechado.
- Por defecto, se envía un broadcast de las actualizaciones de enrutamiento cada 30 segundos.

El protocolo OSPF

- Es un protocolo de enrutamiento de estado del enlace.
- Es un protocolo de enrutamiento público.
- Usa el algoritmo SPF para calcular el costo más bajo hasta un destino.
- Las actualizaciones de enrutamiento producen un gran volumen de tráfico al ocurrir cambios en la topología.

El protocolo BGP

- Es un protocolo de enrutamiento exterior por vector-distancia.
- Se usa para enrutar el tráfico de Internet entre sistemas autónomos.

1.3 Bases teóricas de la propuesta de un modelo de enrutamiento para implementar un nuevo protocolo en la universidad.

A finales de la década de los 80's, aparecen progresivamente las limitaciones fundamentales del enrutamiento de vectores de distancia. Un intento, para mejorar la escalabilidad de las redes fue basar las decisiones de enrutamiento en los estados de los enlaces más que en la cantidad de saltos o en otros vectores de distancia. Un enlace es la conexión entre dos ruteadores en una red. El estado de ese enlace puede incluir atributos tales como la velocidad de transmisión y niveles de retardo.

El grupo: Fuerza de Trabajo de Ingenieros de Internet IETF, en respuesta a la necesidad aumentada por construir más y más grandes redes basadas en IP, formó un grupo de trabajo específicamente para desarrollar un protocolo de enrutamiento abierto de estado de enlace que pudiera usarse en grandes y heterogéneas redes IP. Este nuevo protocolo se basó en la serie moderadamente exitosa, en los protocolos de enrutamientos el Camino más Corto (Shortest Path First, SPF) que había proliferado en el mercado. Todos los protocolos de enrutamiento SPF, incluyendo el OSPF de IETF, fueron basados directamente en un algoritmo matemático conocido como el Algoritmo de Dijkstra. Este algoritmo facilita la selección de rutas basadas en estados de enlace a diferencia de los vectores de distancia.

El IETF desarrolló el protocolo de enrutamiento OSPF a finales de la década de los 80's. OSPF fue una versión abierta, de la clase SPF de protocolos de enrutamiento. La primera versión fue especificada en RFC 1131. Esta versión (OSPF Versión 1) fue superada rápidamente por una versión que se mejoró grandemente, la cual se documentó en RFC 1247, y se le llamó OSPF Versión 2 para denotar explícitamente sus mejoras sustanciales en estabilidad y funcionalidad. Numerosas actualizaciones se le han hecho a esta versión, esquematizándose en RFC 1528, 2178, y 2328 (versión actual). A consecuencia de que Internet e IP son altamente dinámicos, es muy probable que OSPF continúe evolucionando a lo largo del tiempo.

En abril de 1990, la NASA cambió al protocolo OSPF y el tráfico de enrutamiento se redujo drásticamente. Tras un cambio e interrupción de la red, las informaciones de enrutamiento global se restablecían rápidamente (a los pocos segundos, en comparación con los minutos de otros protocolos más antiguos).

OSPF tiene dos características fundamentales. La primera es que es un protocolo abierto, es decir, que su especificación está en el domino público. La especificación está

publicada como Request For Comments (RFC) 1247. La segunda característica es que OSPF está basado en el algoritmo SPF, que algunas veces es llamado como el algoritmo de Dijkstra, llamado de esta forma debido a la persona que lo creó.

Este protocolo propone el uso de rutas más cortas y accesibles mediante la construcción de un mapa de la red y mantenimiento de bases de datos con información sobre sistemas locales y vecinos, de esta manera es capaz de calcular la métrica para cada ruta, entonces se eligen las rutas de enrutamiento más cortas. En este proceso se calculan tanto las métricas de estado del enlace como de distancia, en el caso de RIP se calcula sólo la distancia y no el tráfico del enlace, por esta causa OSPF es un protocolo de enrutamiento diseñado para redes con crecimiento constante y capaz de manejar una tabla de enrutamiento distribuida y de rápida propagación. Entre las características más resaltantes de OSPF están:

- Rápida detección de cambios en la topología y restablecimiento muy rápido de rutas sin bucles.
- Poca sobrecarga, usa actualizaciones que informan de los cambios de rutas.
- División de tráfico por varias rutas equivalentes.
- Enrutamiento según el tipo de servicio.
- Uso de multienvío en las redes de área local.
- Máscaras de subred y superred.
- Autentificación.

El protocolo OSPF reconoce tres tipos de conexiones y redes:

1. Líneas punto a punto entre dos dispositivos.
2. Redes multiacceso con difusión (la mayoría de redes LAN).
3. Redes multiacceso sin difusión (la mayoría de redes WAN).

1.3.1 Enrutamiento de área en OSPF

El enrutamiento dentro de un área se basa en un mapa completo de estado de enlace del área. OSPF se diseñó para que admitiera el crecimiento de la red porque un enrutador

necesita conocer la topología detallada e información de métricas solo de un área a la que pertenece.

Todos los ruteadores con OSPF implementado, en un área mantienen una base de datos de enrutamiento idéntica que describe la topología y estado de todos los nodos de esa área. La base de datos se usa para construir el mapa de esa área. Esta base de datos incluye el estado de todos los ruteadores, interfaces útiles de los ruteadores, las redes conectadas y sus ruteadores adyacentes. Siempre que ocurre un cambio, la información se propaga por toda el área. De esta forma los ruteadores siempre estarán en un estado óptimo para cualquier petición. De esta manera si tenemos un área bastante densa y se cae un enlace con un enrutador, en ese momento el enrutador vecino de ese enlace perdido informará a todos los demás que esa ruta será inaccesible, en cuanto se recupere el enlace informará de nuevo que se recuperó la comunicación con ese enrutador.

Un enrutador que esté arrancando obtendrá una copia de la base de datos actual de enrutamiento de su vecino más cercano (vecino se denomina a cualquier enrutador que esté en su área), tras esto, solo se comunicarán los cambios (esto hace óptimo a OSPF, ya que no replica toda la base de datos de nuevo). Los cambios se difunden rápidamente, ya que OSPF utiliza un algoritmo de distribución eficiente para extender la información de actualización por un área.

Como se dijo anteriormente este protocolo utiliza el algoritmo de enrutamiento de estado de enlace.

- Es una alternativa primaria a los esquemas vector-distancia.

- Características principales:
    - Un conjunto de redes físicas se divide en un número de áreas.
    - Todos los ruteadores dentro de un área tiene idénticas bases de datos.
    - La base de datos de cada ruteador describe la topología completa del dominio de encaminamiento (qué ruteador se conectan a qué redes).

- Cada ruteador envía periódicamente una descripción de su conexión (el estado de su enlace) a sus vecinos (aquellos conectados a la misma red).

- Cada ruteador del dominio mantiene una copia idéntica y sincronizada de una base de datos compuesta de la información del estado de enlace.

- Este tipo de protocolo, a diferencia de los protocolos vector-distancia, envía actualizaciones cuando hay noticias.

- Lo importante es la información intercambiada en el estado de enlace, no el contenido de la tabla de enrutamiento.

- Los usuarios consiguen respuesta a los eventos de red más rápido, convergencia más veloz, y acceso a servicios de red más avanzados.

El OSPF funciona haciendo una abstracción del conjunto de redes, ruteadores y líneas en un grafo dirigido en el que a cada arco se le asigna un costo (distancia, retardo, etc.). Entonces se calcula la trayectoria más corta con base en los pesos de los arcos.

En la figura 1.6 (a) se muestra la representación gráfica de la red de la figura 1.6 (b). Lo fundamental que hace el OSPF es representar la red como un grafo de este tipo y luego calcular la trayectoria más corta de un enrutador a todos los demás.

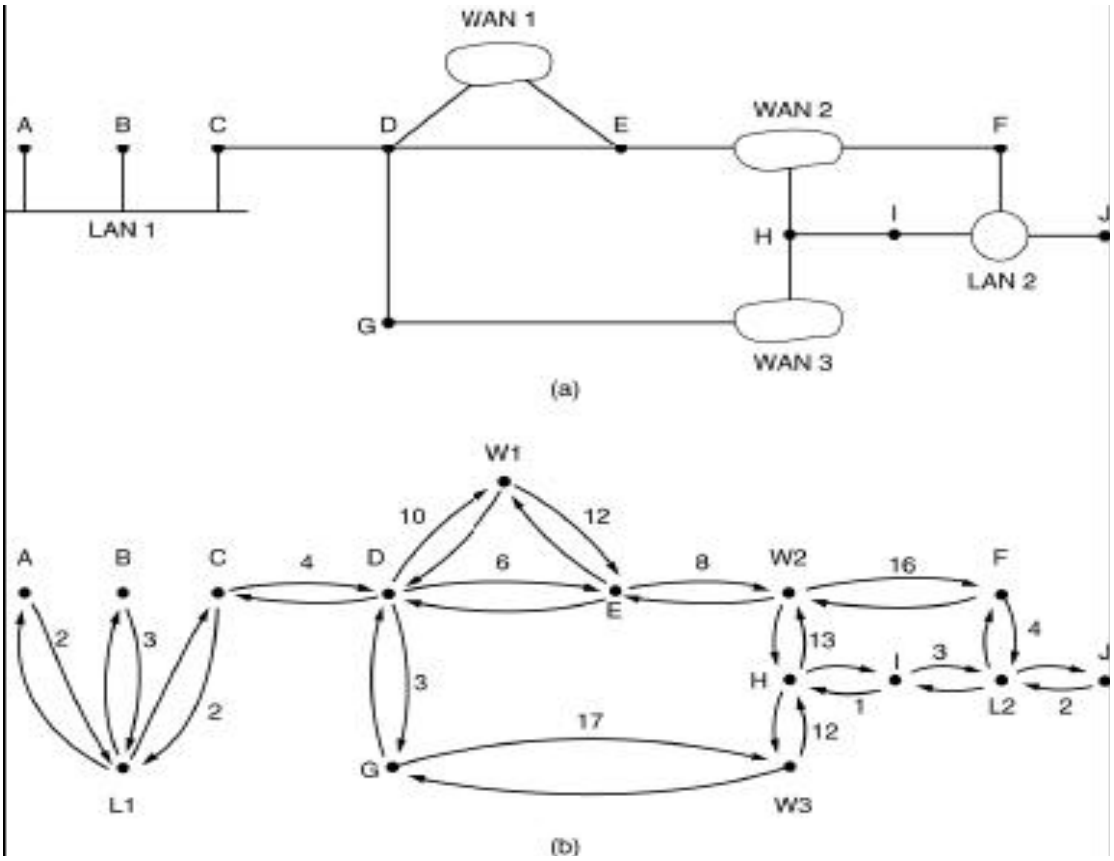


Fig. 1.6. (a) Sistema Autónomo. (b) Representación con grafos de (a).

Muchos de los AS de Internet son grandes y nada fáciles de manejar. OSPF permite su división en áreas numeradas, donde un área es una red o un grupo de redes contiguas. Un área es una generalización de una subred. Fuera de un área, su topología y detalles no son visibles.

Cada AS tiene un área de *backbone*, llamada área 0, con todas las áreas conectadas, posiblemente mediante túneles, por lo que hay posibilidad de ir de cualquier área del AS a cualquier otra a través del *backbone*. Un túnel se representa en el grafo como un arco y tiene un costo. Cada enrutador conectado a dos o más áreas es parte del *backbone,* siendo la topología del mismo no visible desde fuera de este.

Dentro de un área, cada enrutador tiene la misma base de datos de estado de enlace y ejecuta el mismo algoritmo de trayectoria más corta; su tarea principal es calcular la trayectoria más corta de sí mismo a todos los demás ruteadores del área, incluido el ruteador que está conectado al *backbone*.

La manera en que OSPF maneja el enrutamiento de tipo de servicio es teniendo varios grafos, uno etiquetado con los costos cuando la métrica es el retardo, otro etiquetado con los costos cuando la métrica es el rendimiento, y uno más etiquetado con los costos cuando la métrica es la confiabilidad. Aunque esto triplica el cálculo, permite rutas separadas para optimizar el retardo, el rendimiento y la confiabilidad.

Durante una operación normal pueden necesitarse tres tipos de rutas: intra área, inter área y ruta externa. Las rutas intra áreas son las más fáciles, dado que el enrutador de origen ya conoce la trayectoria más corta al enrutador de destino. El enrutamiento inter área siempre procede en tres pasos: va del origen al *backbone*, pasa a través del *backbone*, al área de destino y va al destino. Este algoritmo obliga a una configuración en estrella en el OSPF, siendo el *backbone* el centro y las demás áreas los rayos.

El OSPF distingue cuatro clases de ruteadores:

1. Ruteadores internos que están contenidos en una sola área.
2. Ruteadores de borde de área que conectan dos o más áreas.
3. Ruteadores de *backbone* que están en el *backbone.*
4. Ruteadores de frontera de AS que hablan con los ruteadores de otras áreas AS.

El OSPF funciona intercambiando información entre ruteadores adyacentes, que no es lo mismo que entre vecinos. En particular es ineficiente hacer que todos los ruteadores de una LAN hablen con todos los de otra LAN. Para evitar esta situación, se elige un ruteador como designado, el cual se dice que es adyacente a todos los demás, e intercambia información con ellos. Los que no son vecinos no intercambian información entre ellos, se mantienen actualizados designando un ruteador de respaldo para facilitar la transición en el caso que el designado primario se caiga.

Después de ver las características fundamentales del protocolo OSPF, se hizo una comparación entre el protocolo que se encuentra actualmente en la universidad y el que se quiere implementar.

1.3.2 OSPF vs. RIP

El rápido crecimiento y expansión de las redes hoy en día ha presionado a RIP a sus límites. RIP tiene ciertas limitaciones que puede causar ciertos problemas en algunas redes grandes:

- RIP tiene un límite de 15 saltos. Una red RIP que se expande a más de 15 saltos (15 ruteadores) se considera inalcanzable.

- RIP no puede manejar máscaras de subred de tamaño variable (VLSM). Dado lo corto de las direcciones IP y la flexibilidad, VLSM cede en la asignación de direcciones IP.

- La difusión periódica de todas las tablas de enrutamiento consume un alto ancho de banda. Este es un gran problema con grandes redes especialmente con enlaces lentos en las nubes WAN.

- RIP converge más lento que OSPF. En grandes redes la convergencia viene en el orden de minutos. Los ruteadores RIP van a través de un período de recolección de basura y la información se vence rápidamente. Esto es inapropiado en grandes redes.

- RIP no tiene el concepto de retardo en red y alto costo. Las decisiones de enrutamiento se basan en los saltos. El camino con menos saltos es el que es preferido hasta el destino aunque tenga un menor ancho de banda y alto retardo.

- Las redes RIP son redes delgadas. No existe el concepto de áreas.

Algunos cambios fueron hechos en nuevas versiones de RIP llamadas RIP2. Las direcciones RIP2, VLSM, la autentificación y las actualizaciones de difusión. RIP2 no es una gran mejora sobre RIP (ahora llamado RIP1) porque todavía tiene limitaciones sobre el número de saltos y convergencia muy lenta que es esencial en las redes de hoy en día.

Por otro lado OSPF:

- Con OSPF, no hay limitaciones en el número de saltos.

- El uso inteligente de VLSM es muy útil en la asignación de direcciones IP.

- OSPF utiliza difusión IP para enviar las actualizaciones de los estados de enlaces. Esto asegura menos procesamiento en los ruteadores que no están escuchando los paquetes OSPF. Además, las actualizaciones se envían solamente en caso de que ocurran cambios, en vez de periódicamente. Esto asegura mejor uso del ancho de banda.

- OSPF tiene mejor convergencia que RIP. Esto es porque los cambios de enrutamiento son propagados inmediatamente y no periódicamente.

- OSPF permite mejor balance basado en el costo del enlace. Los retardos del enlace son el mayor factor en la decisión de por donde enviar las actualizaciones de enrutamiento.

- OSPF tiene en cuenta una definición lógica de las redes, las cuales pueden ser divididas en áreas. Esto limita la explosión de los estados de enlaces sobre toda la red. Además provee un mecanismo para agregar rutas y cortar la propagación innecesaria de la información de la subred.

- OSPF permite la autentificación de enrutamiento basado en diferentes métodos de autentificación.

Estado de Enlace vs. Vector Distancia

A continuación se realiza una comparativa entre estos dos algoritmos:

Ancho de banda: Puesto que la métrica de retardo es la longitud de la cola, el vector distancia no considera el ancho de banda usado. Antes de 1979 el máximo ancho de banda era de 56Kb posteriormente se modernizaron las líneas a 230Kbps o incluso a 1,5Mbps lo que hizo necesario el uso de mejores técnicas.

Convergencia: El algoritmo por vector distancia tarda demasiado en converger aún con la técnica del horizonte dividido.

Información de la red: En enrutamiento por vector distancia, cada ruteador envía información sólo a sus vecinos, pero esta es sobre toda la red. Sin embargo el enrutamiento por estado de enlace envía a todos los nodos de la red, pero su información es relativa a sus vecinos. Además el enrutamiento por vector distancia no permite conocer la topología de la red.

Capacidad y uso de memoria: Con algoritmos basados en estado de enlace, el tráfico de la red siempre es el mismo sin depender del tamaño de la red. Con vectores distancia, se transmiten vectores de un tamaño proporcional al número de nodos. El enrutamiento por vector distancia sólo guarda las distancias al resto de nodos. Con estado de enlace se ha de almacenar además la topología de la red.

Sucesos en la red: Al no tener información sobre la topología, el enrutamiento por vector distancia no se adapta tan bien a los cambios en la red como el basado en estado de enlace. Sin embargo, el enrutamiento basado en vector distancia es mucho más sencillo que el de estado de enlace, lo que en ocasiones puede resultar bastante útil.

Observándose así la superioridad del protocolo OSPF en comparación con RIP, se propone implementar aquel en la red de la universidad para una mayor eficiencia en cuanto a la transmisión de datos.

Capítulo 2. OSPF (Open shortest path first)

En el capítulo anterior se habló de algunas características y funcionalidades del protocolo OSPF y de cómo es más ventajoso que el protocolo RIP. En este capítulo se hablará con más profundidad de la terminología de OSPF, el algoritmo y el pos y los contras del protocolo para el diseño de largas y complicadas redes de hoy en día.

OSPF es uno de los protocolos de enrutamiento abierto disponibles más poderosos y ricos en características. Su complejidad es además una fuente de flaqueza, porque diseñar, construir y operar una red OSPF requiere más técnica y esfuerzo que una red similar usando cualquier otro protocolo de enrutamiento.

OSPF fue diseñado específicamente como un protocolo de enrutamiento IP con el objetivo de usarse dentro de un AS. Como tal, no puede transportar datagramas de otros protocolos de red ruteables tales como IPX o AppleTalk. OSPF calcula rutas basadas en la dirección IP destino que se encuentra en la cabecera del datagrama IP; y no está hecho para calcular rutas a los destinos de los cuales no se conoce el IP. Los mensajes OSPF son encapsulados directamente en IP y no se necesita ningún otro protocolo (tal como TCP, UDP, etc.) para la entrega. Este protocolo de enrutamiento ha introducido nuevos conceptos tales como autenticación de actualizaciones de ruteo, VLSM, resumen de rutas, etc.

OSPF fue diseñado también para detectar rápidamente cambios topológicos en un AS y converge en un nuevo consenso de la topología después de detectar un cambio. Las decisiones de enrutamiento se basan en el estado de enlace que interconectan los ruteadores en el AS. Cada uno de esos ruteadores mantiene una base de datos idéntica que rastrea los estados de enlaces en la red. El estado del ruteador está incluido en esta base de datos. Esto incluye sus interfaces utilizables, los vecinos alcanzables conocidos, y la información del estado del enlace.

Se puede pensar en un enlace como una interfaz en el ruteador. El estado del enlace es una descripción de esa interfaz y su relación con los ruteadores vecinos. Una descripción de la interfaz incluiría, por ejemplo, la dirección IP de la interfaz, la máscara, el tipo de red a la que está conectada y los ruteadores conectados a la misma. La colección de todos estos enlaces formaría una base de datos del estado de enlace.

2.1 Algoritmo del Estado de Enlace

OSPF usa el algoritmo del estado del enlace para construir y calcular el camino más corto a todos los destinos conocidos. El algoritmo por sí mismo es bastante complicado. A continuación se muestran algunos pasos del mismo:

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

2. Todos los ruteadores intercambiarán con sus vecinos dentro del área los estados de los enlaces por medio de inundaciones. Cada ruteador que reciba un estado de enlace actualizado debería almacenar una copia en su base de datos de estado de enlaces y luego propagar la actualización a otros ruteadores.

3. Después de que la base de datos de cada ruteador esté completa, esta información se usa para construir una imagen de la red y sus enlaces. Cada imagen del ruteador usa una estructura de árbol, con él mismo como raíz. Este árbol, conocido como el Árbol del Camino más Corto (Shortest Path Tree) rastrea dicho camino a cada destino dentro del AS y se calculará usando el algoritmo de Dijkstra basado en el costo acumulativo para alcanzar dicho destino. Los destinos, el costo asociado y el próximo salto para alcanzar esos destinos formarán la tabla de enrutamiento IP.

4. En caso de que no ocurran cambios en la red OSPF, tales como el costo de un enlace, o la adición o eliminación de una red, OSPF se mantendrá en silencio. Cualquier cambio que ocurra será comunicado a través de Paquetes del Estado del Enlace (LSPs), y el algoritmo Dijkstra se vuelve a calcular para encontrar el camino más corto.

2.2 Paquetes de Estado de Enlace, LSP

Existen diferentes tipos de LSPs, los cuales se encuentran normalmente en una base de datos de OSPF. Estos son:

- Enlaces de ruteadores
- Enlaces de resumen
- Enlaces de red
- Enlaces externos

Los enlaces de ruteadores son una indicación del estado de las interfaces de un ruteador perteneciente a un área determinada. Cada ruteador generará un enlace de ruteador para todas sus interfaces. Los enlaces de resumen son generados por Ruteadores de Borde de Área; así es como la información de la accesibilidad de la red es diseminada entre áreas. Normalmente, toda la información es inyectada en el Backbone (área 0) y a su vez este lo pasará a otras áreas. Los ruteadores de borde de área además tienen la tarea de propagar la accesibilidad de los ruteadores de frontera de sistemas autónomos. De esta forma los ruteadores saben cómo llegar a rutas externas en otros AS.

Los enlaces de redes son generados por un Ruteador Designado en un segmento. Esta información es una indicación de todos los ruteadores conectados a un segmento multiacceso particular tal como Ethernet, Token Ring y FDDI (además NBMA).

Los enlaces externos son una indicación de las redes que están fuera del AS. Estas redes son inyectadas en OSPF a través de la redistribución. El ruteador de sistemas autónomos tiene la tarea de inyectar estas rutas en un AS.

2.3 Áreas de OSPF

Una de las razones claves por la rapidez de la convergencia de OSPF es que usa áreas. Es importante recordar que los dos objetivos principales que IETF trató de lograr con OSPF fueron:

- Escalabilidad de red mejorada.
- Tiempo de convergencia rápido.

La clave de esto consiste en dividir en compartimientos una red en pequeñas regiones. Estas regiones se conocen como áreas. Un área es una colección de sistemas finales

interconectados, ruteadores y facilidades de transmisión. Cada área está definida con un número de área único en cada ruteador. Las interfaces de ruteadores definidos con el mismo número de área formarán parte de la misma área. Idealmente, estas áreas no se definen arbitrariamente. En lugar de eso, los límites de un área deben ser seleccionados para disminuir la cantidad de tráfico entre diferentes áreas. En otras palabras, cada área debe reflejar patrones reales de tráfico en vez de límites geográficos o políticos. Por supuesto, esto es una idea teórica y puede resultar impráctico en un entorno en particular.

El número de áreas en las redes OSPF que se puede soportar está limitado por el tamaño de su campo de Identificador de Área (Área ID). Este campo es un número binario de 32 bit. Por lo tanto, el número máximo de redes en teoría es un número binario de 32 bit con todos sus bits igual a 1. El equivalente decimal de este número es 4,294,967,295. Obviamente, el número máximo de áreas en la práctica que puede soportar es mucho menor que el número teórico. En la práctica, cuan bien diseñada esté la red, determinará el número práctico máximo de áreas que se puede soportar. La figura 2.1 ilustra una red OSPF sencilla de solo tres áreas, enumeradas 0, 1 y 2.

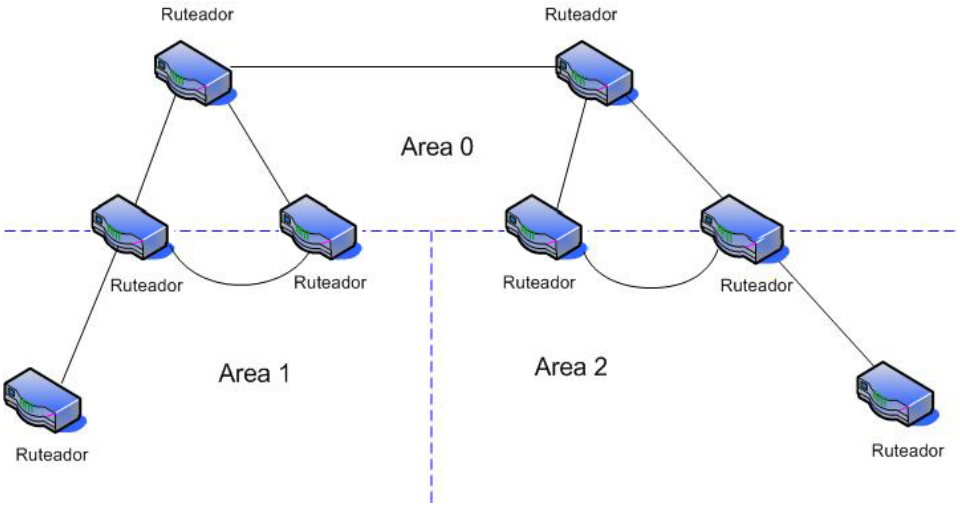


Fig. 2.1. Una red OSPF pequeña con tres áreas.

2.4 El Backbone y Área 0

OSPF tiene restricciones especiales cuando están implicadas múltiples áreas. Si se configuran varias áreas, una de estas áreas tiene que ser el área 0, que también se le conoce

como el Backbone o Dorsal. A la hora de diseñar redes se considera como buena práctica empezar con área 0 y así sucesivamente.

El backbone tiene que estar al centro de todas las otras áreas, y estas estar conectadas físicamente al backbone. Esto es debido a que OSPF espera que todas las áreas inyecten información de enrutamiento hacia el backbone y que desde este se disemine esta información en las otras áreas.

El siguiente diagrama muestra el flujo de información en una red OSPF:

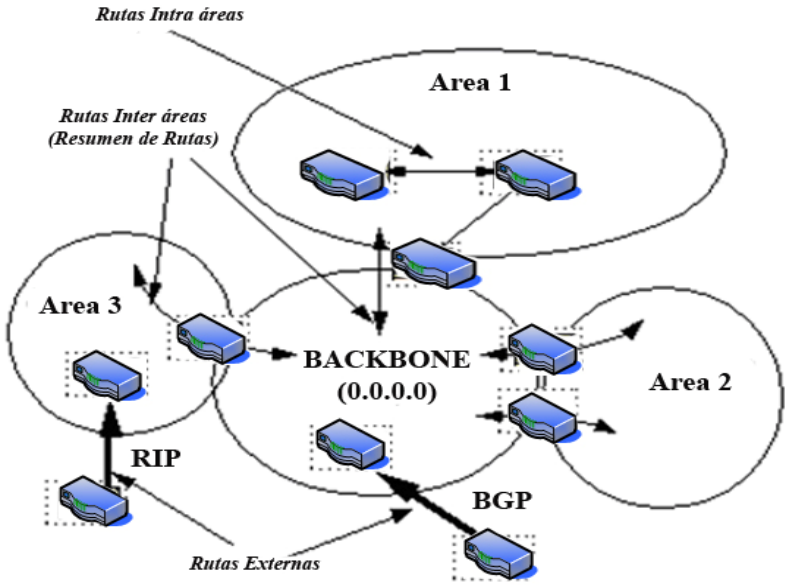


Fig.2.2 Flujo de información en una red OSPF

Las rutas que son generadas dentro de un área (el destino pertenece al área) son llamadas Rutas Intra áreas. Las rutas que se originan desde otras áreas son llamadas Rutas Inter áreas o Resumen de rutas. Las rutas que son originadas desde otros protocolos de enrutamiento (o diferentes procesos de OSPF) y que son inyectadas a OSPF mediante la redistribución se llaman Rutas externas.

Existen raras situaciones donde se introduce una nueva área que no tenga un acceso físico directo al backbone, en este caso se tendrá que configurar un enlace virtual.

2.5 Enlaces Virtuales

Los enlaces virtuales son usados por dos razones:

1. Para enlazar un área que no tenga conexión física con el backbone.
2. Ajustar el backbone en caso que ocurra discontinuidad de área 0.

2.5.1 Áreas que no están físicamente conectadas al Área 0

El enlace virtual proporcionara un camino lógico del área desconectada al backbone. Tiene que establecerse entre dos ruteadores de borde de área que tienen un área común, con uno de ellos conectado al backbone. Esto se ilustra en el siguiente ejemplo:

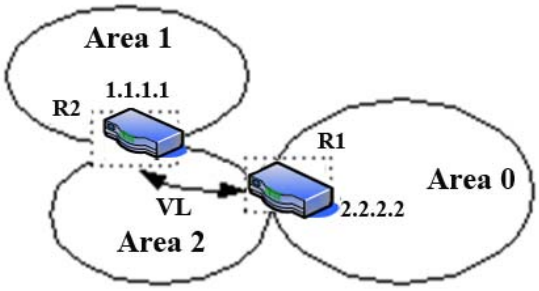


Fig. 2.3 Enlace virtual entre areas

En este ejemplo, el área 1 no tiene una conexión física con el área 0, por lo que tiene que configurarse un enlace virtual entre R2 y R1. El área 2 está para ser usada como área de transito y R1 es el punto de entrada en el área 0. De esta forma R2 y el área 1 tendrán una conexión lógica al backbone.

2.5.2 Continuidad del Backbone

Si el backbone es discontinuo las diferentes áreas no podrán comunicarse. OSPF permite enlazar las partes discontinuas del backbone usando un enlace virtual. En algunos casos, diferentes áreas 0s necesitan ser enlazadas. Esto puede ocurrir si, por ejemplo, una compañía está tratando de combinar dos redes OSPF separadas en una sola red con una área 0 común. Si algún ruteador falla, esto causa que el backbone se separe en dos y entonces los

enlaces virtuales son agregados por redundancia. Cualquiera sea la razón, un enlace virtual puede ser configurado entre separados ABRs que toque el área 0 desde cada lado y teniendo un área común. Esto se ve en el siguiente ejemplo:

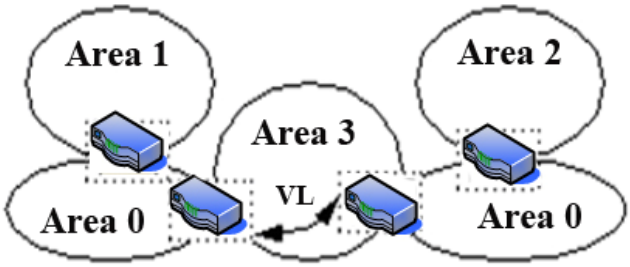


Fig. 2.4 Enlace virtual entre diferentes áreas ceros

Como se ve en el diagrama dos áreas 0 están enlazadas mediante un enlace virtual. En caso de que no estén en una misma área, se adiciona un área, en este caso el área 3, para convertirse como área de tránsito.

2.6 Área Stub

OSPF permite algunas áreas para ser configuradas como áreas stub. Un área stub es aquella que no recibe rutas externas. Las redes externas, tales como las redistribuidas desde otros protocolos en OSPF, no están permitidas para ser inundadas en un área stub. El enrutamiento desde estas áreas hacia el exterior está basado en una ruta por defecto. Configurando un área stub se reduce el tamaño de la base de datos topológica dentro de un área y reduce los requerimientos de memoria de los ruteadores dentro de esa área.

Un área podría ser calificada como stub cuando exista un simple punto de salida desde esa área o si el enrutamiento hacia fuera del área no tiene que tomar un camino óptimo. Esta descripción es una indicación que un área stub que tiene múltiples puntos de salida tendrá uno o más ruteadores de borde de áreas inyectando un ruta por defecto en esa área.

Otra restricción del área stub es que no puede ser usada como un área de tránsito para enlaces virtuales. Además, un ruteador de frontera de AS no puede ser interno a un área stub. Estas restricciones se hacen porque un área stub se configura principalmente para no llevar

rutas externas y cualquiera de esas situaciones causa enlaces externos para ser inyectadas en esa área. El backbone, por supuesto, no puede configurarse como stub.

Todos los ruteadores OSPF dentro de un área tienen que ser configurados como ruteadores stub. Esto es porque si un área se configura como stub, todas las interfaces que pertenezcan a esa área iniciarán intercambiando paquetes de hello con una indicación que muestra que esa interfaz es stub. Todos los ruteadores que tienen un segmento común tienen que ponerse de acuerdo. Si ellos no se ponen de acuerdo, entonces no se convertirán en vecinos y el enrutamiento no toma efecto.

Una extensión a las áreas stub son las llamadas áreas totalmente en trozo (totally stubby áreas). Es un área que bloquea rutas externas y resumidas desde dentro del área. De esta forma las rutas intra áreas y la ruta por defecto de 0.0.0.0 son las únicas rutas inyectadas en esa área.

2.7 Tipos de ruteadores

Es importante recordar que OSPF es un protocolo de enrutamiento de estado de enlace. Por tanto, los enlaces y las interfaces de los ruteadores a la que se unen están definidos como miembros de un área. Basado en la agrupación de un área, pueden definirse los ruteadores dentro de una red OSPF de cuatro tipos diferentes:

- Ruteador Interno (Internal Router, IR)
- Ruteador de Borde de Área (Area Border Router, ABR)
- Ruteador de Dorsal (Backbone Router, BR)
- Ruteador de Frontera de Sistema Autónomo (ASBR)

Un área es una interfaz específica. Un ruteador que tiene todas sus interfaces dentro de la misma área se llama Ruteador Interno, IR. Un ruteador que tiene interfaces en múltiples áreas es llamado Ruteador de Borde de Área, ABR. Los ruteadores que actúan como pasarelas (redistribución) entre OSPF y otros protocolos de enrutamiento (IGRP, EIGRP, IS-IS, RIP, BGP, Estática) u otras interfaces del proceso de enrutamiento de OSPF son llamados Ruteadores de Sistema Autónomo, ASBR. Cualquier ruteador puede ser un ABR o un ASBR. Un Ruteador del

Dorsal, BR es uno que tiene al menos una interfaz definida de manera que pertenezca al Área 0.

2.8 Tipos de enrutamiento

OSPF soporta dos tipos diferentes de enrutamiento:

- Enrutamiento Intra área
- Enrutamiento Inter área

El enrutamiento Intra área es autónomo y limitado solamente a los ruteadores internos a una sola área. La siguiente figura muestra una comunicación intra área en una red OSPF.

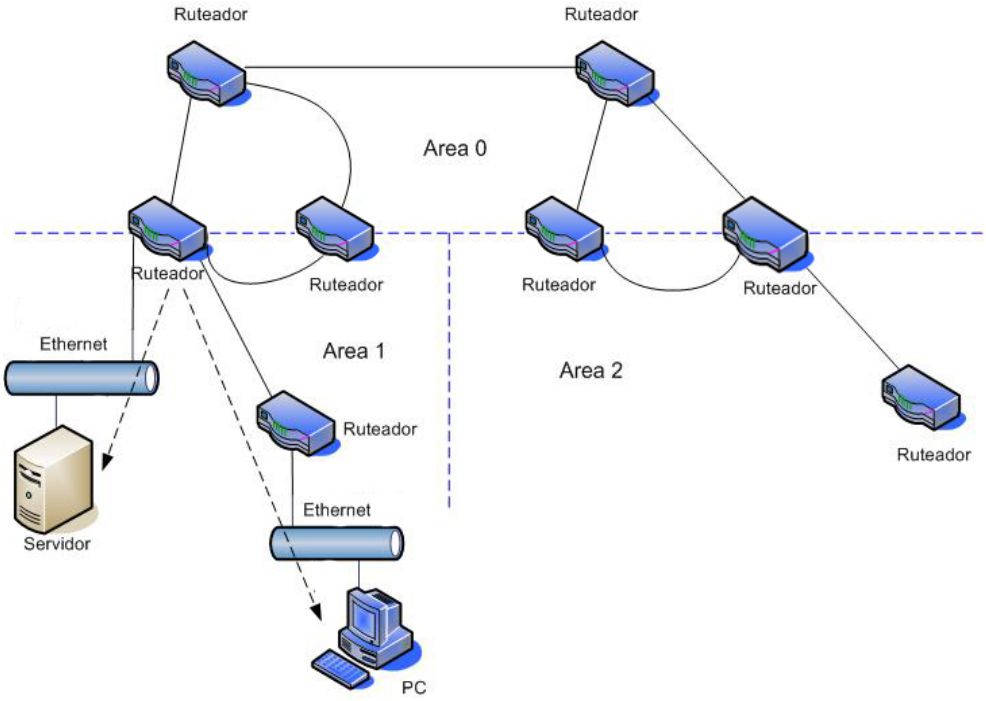


Fig.2.5 Comunicaciones Intra área en una red OSPF

El enrutamiento Inter área requiere el intercambio de datos entre diferentes áreas. Todo enrutamiento inter área tiene que ser conducido a través del Área 0. Los números de áreas distintos de cero no están permitidos para comunicarse directamente con otro. Esta restricción jerárquica asegura que las redes OSPF escalen satisfactoriamente sin convertirse en conjuntos confusos de enlaces y rutas.

La siguiente figura muestra el uso correcto del Área 0 para facilitar una comunicación inter área en una red OSPF.

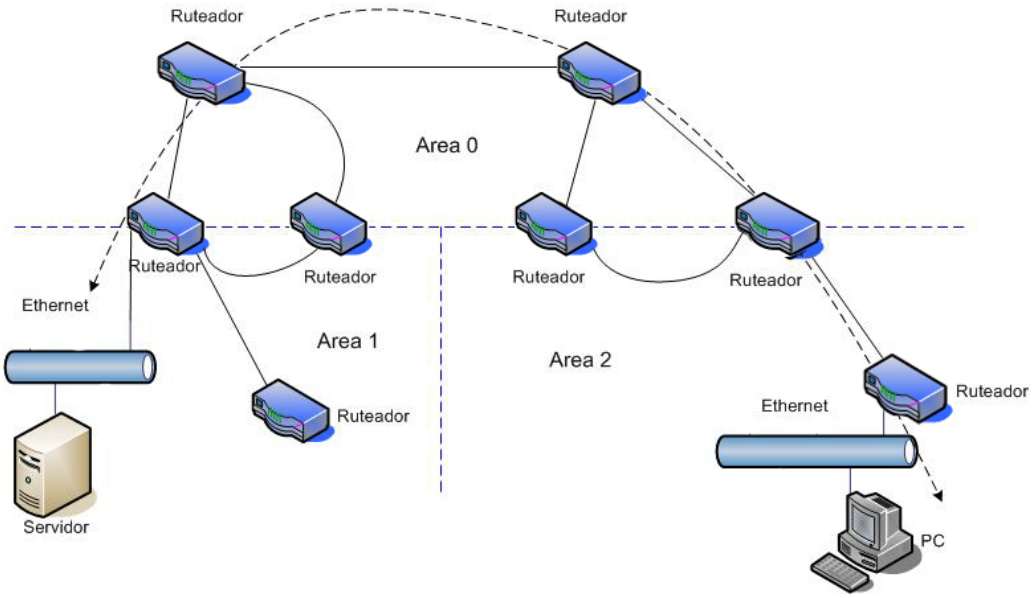


Fig.2.6 Usando Área 0 para facilitar una comunicación inter área en una red OSPF.

2.9 Enrutamiento entre redes

OSPF puede ser usado para interconectar redes separadas. Tales redes pueden ser otra red completa de OSPF o que utiliza un protocolo de enrutamiento completamente diferente. Interconectar una red OSPF con un protocolo de enrutamiento diferente es una tarea complicada y usa una técnica conocida como redistribución de ruta. La información de enrutamiento de las redes que no son OSPF se resume y se distribuye en la red. La red OSPF etiqueta todas las rutas aprendidas en este modo como externas.

Interconectar dos redes diferentes es más fácil, porque no hay necesidad de convertir una información de costo de ruta del protocolo de enrutamiento en un formato que otro protocolo pueda entender. Adicionalmente, OSPF posibilita la creación de AS y usaría un solo protocolo de enrutamiento.

OSPF permite asignar un número de AS a una red. Una red muy larga OSPF podría ser segmentada en dos o más AS. Estos sistemas serían interconectados mediante el ASBR, el cual resume toda la información de enrutamiento para su AS y reenvía ese resumen a su

contraparte de ASBR en el AS vecino. En consideración, funciona mayormente como un ABR. La diferencia, obviamente, es que ellos componen el borde entre los AS separados más que las áreas entre un solo AS o una red. La siguiente figura muestra la interconexión entre AS usando ASBRs:

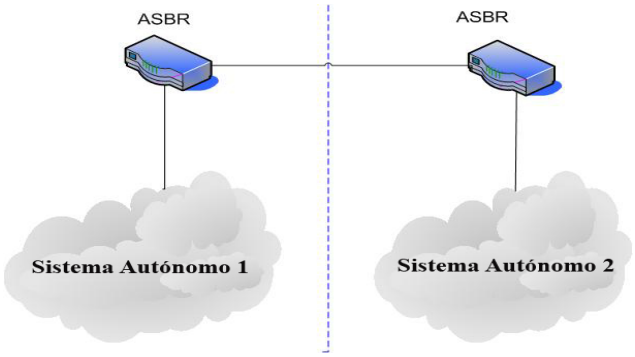


Fig. 2.7 Sistemas Autónomos de OSPF interconectados

2.10 Actualizaciones de Enrutamiento

Una de las razones por las que OSPF es tan escalable es su mecanismo de actualización de enrutamiento. OSPF usa un LSA para compartir información de enrutamiento entre nodos OSPF. Estos anuncios son propagados completamente a lo largo de un área. Por consiguiente, cada ruteador conoce la topología de su área. Sin embargo, la topología de cualquier área dada no se conoce fuera de la misma. Dado que hay cuatro tipos diferentes de ruteadores OSPF: IR, ABR, ASBR y BR, queda claro que cada tipo de ruteador tiene un juego diferente de pares con los cuales los LSAs deben ser intercambiados.

2.10.1 Ruteadores de Áreas Internas

Tienen que intercambiar LSAs directamente con cada uno de los otros ruteadores en su área. Esto incluye cada IR así como cualquier ABR que debe además ser miembro en su área. En la figura 2.8 se muestra el reenvío o inundación de LSAs a través del Área 1 de una red simple de OSPF. Nótese que los ruteadores de la misma área no necesitan ser directamente conectados a cada uno de los otros para compartir información de LSA. Un ruteador OSPF direcciona directamente los paquetes a cada ruteador conocido en su área y reenvía esos paquetes usando enlaces disponibles.

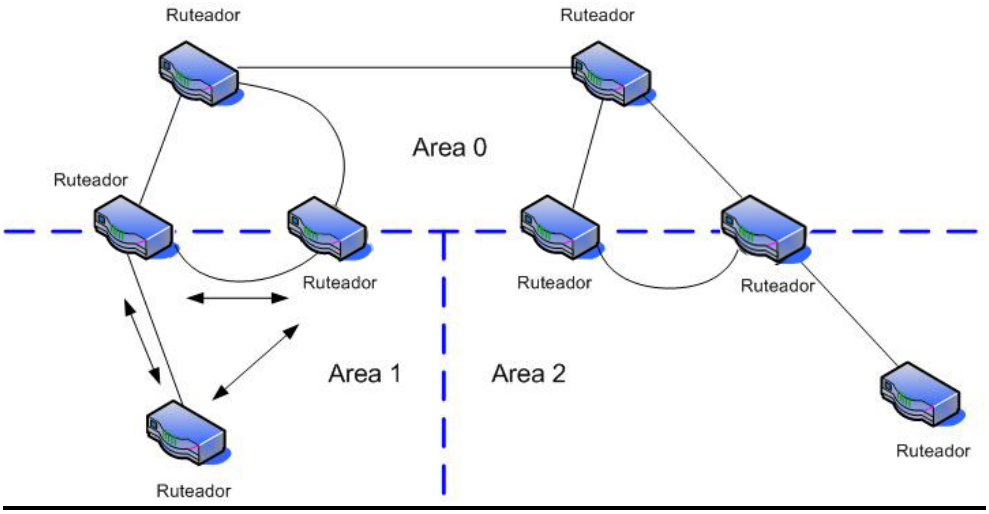


Fig.2.8 Inundación de LSA dentro del Área 1.

Una implicación sutil de esta figura es que la convergencia puede ocurrir bastante rápido. Existen dos razones para esto. La primera es que un ruteador OSPF direcciona y trasmite directamente los LSAs a todos los ruteadores en su área simultáneamente (conocido como inundación). El resultado es una convergencia casi instantánea en una nueva topología dentro de esa área.

La convergencia es además acelerada a través de la definición y uso de áreas. El dato topológico no se propaga fuera de los bordes de áreas. Por consiguiente, la convergencia no necesita ocurrir entre todos los ruteadores en el AS, solamente entre los ruteadores en el área afectada.

2.10.2 Ruteadores de Borde de Área

Son los responsables del mantenimiento de la información topológica en sus bases de datos para cada una de las áreas para las cuales contienen interfaces. Por consiguiente, si un ABR interconecta dos áreas diferentes, tiene que intercambiar los LSAs con pares en ambas redes. Como con los ruteadores de áreas internas, estos LSAs son direccionados y trasmitidos directamente a sus pares en cada área. La siguiente figura muestra esto.

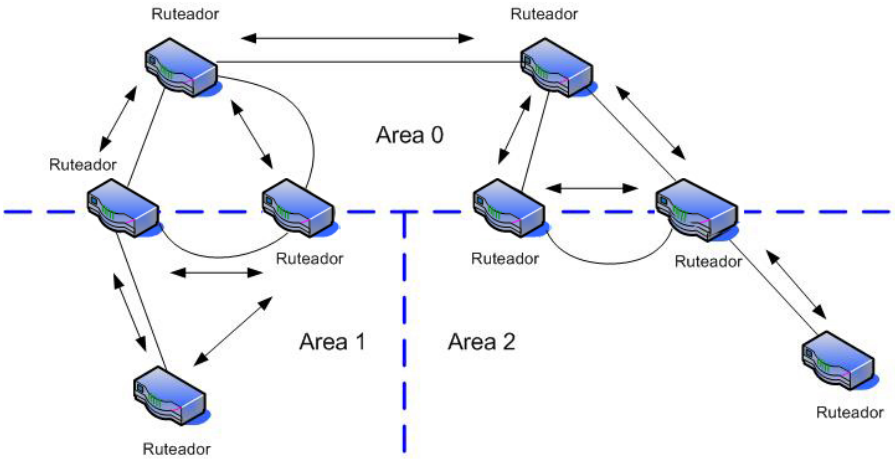


Fig.2.9 Inundación de LSA Intra área en una red OSPF por ABRs.

Otra de las características de realce del cumplimiento de OSPF es el resumen de ruta. La información topológica sobre un área no se comparte con otros ruteadores fuera de esa área. En lugar de eso, el ARB resume todas las direcciones contenidas en las áreas para las cuales está contenida. Este dato de enrutamiento resumido es después compartido, mediante el tipo 3 de LSAs, con ruteadores pares en cada una de las áreas que este interconecta. En la figura, el ABR anuncia este dato resumido directamente a todos los ruteadores en el Área 0.

2.10.3 Ruteadores del Dorsal

Son los responsables del mantenimiento de la información topológica para el backbone así como para la preparación de la información topológica resumida para cada una de las otras áreas dentro del AS. La siguiente figura muestra el intercambio de LSAs por el ruteador backbone.

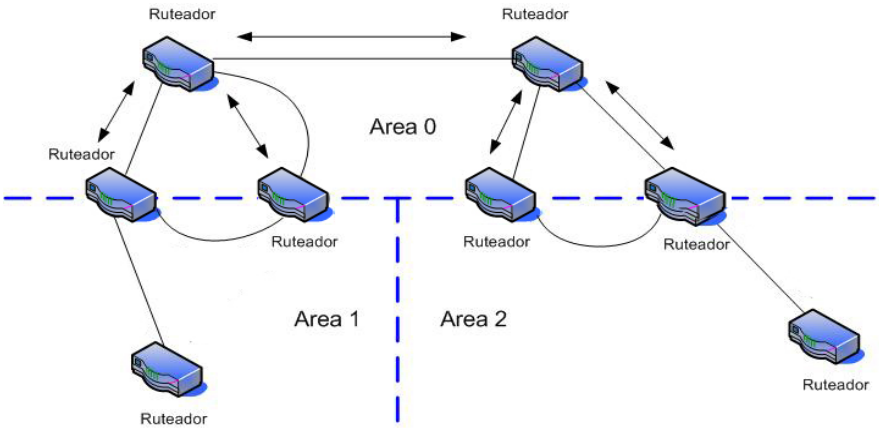


Fig.2.10 Inundación de LSA Intra área en una red OSPF por los ruteadores backbone.

2.11 OSPF y Resumen de Rutas

El resumen es la consolidación de múltiples rutas en un solo anuncio. Esto se hace normalmente en los límites de los ABRs. Aunque el resumen se podría configurar entre dos áreas cualquiera, es mejor resumir en la dirección del backbone. De esta forma el backbone recibe todas las direcciones agregadas y a su vez las inyectará, ya resumidas, en otras áreas. Existen dos tipos de resúmenes:

_ Resumen de ruta Inter área
_ Resumen de ruta Externa

2.11.1 Resumen de Ruta Inter Área

Se hace en los ABRs y se aplica a las rutas dentro del AS. No se aplica a las rutas externas inyectadas en OSPF mediante la redistribución. Para tomar ventaja del resumen, deben ser asignados números de red en áreas de forma continua para ser capaz de aglomerar estas direcciones en un rango. A continuación se muestra un ejemplo de resumen:

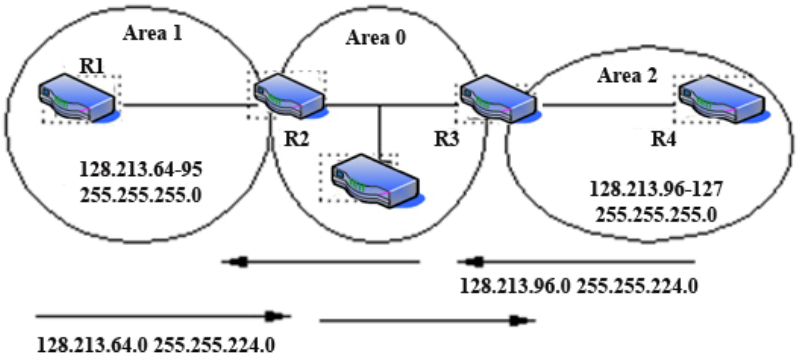


Fig.2.11 Resumen de rutas inter área

En la figura, R2 está resumiendo el rango de subredes desde 128.213.64.0 a 128.213.95.0 en un rango: 128.213.64.0 255.255.224.0. Esto se logra enmascarando los tres primero bits que están a la izquierda de 64 usando una máscara de 255.255.224.0. En la misma forma, R3 está generando la dirección resumen 128.213.96.0 255.255.224.0 en el backbone.

Podría ser difícil resumir si las subredes entre el área 1 y el área 2 están solapadas. El área backbone recibiría rangos de resumen que se solaparían, y los ruteadores en el medio no sabrían a donde enviar el tráfico basado en la dirección resumida.

2.11.2 Resumen de Ruta Externa

Este tipo de resumen es específico para rutas externas que son inyectadas en OSPF mediante la redistribución. Además, asegura que los rangos externos que están siendo resumidos sean contiguos. Los rangos de resumen solapados de dos ruteadores diferentes podrían provocar que los paquetes sean enviados al destino equivocado.

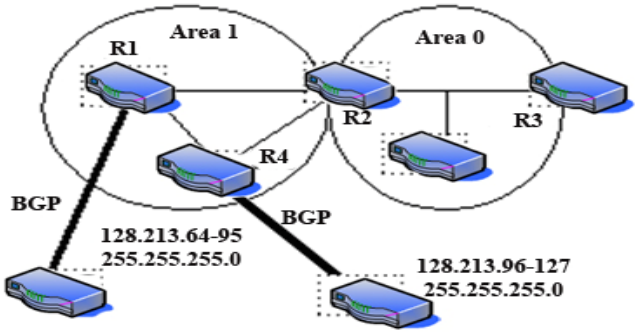


Fig. 2.12 Resumen de Ruta Externa

En el diagrama R1 y R4 son rutas externas inyectadas en OSPF mediante la redistribución. R1 está inyectando subredes en el rango 128.213.64-95 y R4 está inyectando subredes en el rango 128.213.96-127.

2.12 Costo de OSPF

El costo (llamado además métrica) de una interfaz en OSPF es una indicación del gasto requerido para enviar paquetes a través de cierta interfaz. El costo de una interfaz es inversamente proporcional al ancho de banda de esa interfaz, por lo que un mayor ancho de banda indica un menor costo. Existe más gasto (mayor costo) y retraso implicado en cruzar un enlace serie de 56k que en cruzar un tramo Ethernet de 10mb. La fórmula usada para calcular el costo es:

Costo= 10^8/(Ancho de Banda)

Ejemplo

Para cruzar un tramo de 10M Ethernet

Costo= 10^8/10^7 = 10

Para cruzar un enlace serial T1

Costo= 10^8/1544000 = 64

2.13 Calculo de las rutas

OSPF, a pesar de su complejidad, calcula los costos de una ruta de una o dos formas notablemente simples:

- Se puede usar un valor por defecto no sensible al ancho de banda para cada interfaz de OSPF.
- OSPF puede calcular automáticamente el costo de usar interfaces de ruteadores individuales.

Independientemente de cual sea el método que se desarrolle, el costo de cualquier ruta dada se calcula sumando los costos de todas las interfaces encontradas a los largo de esa ruta. Se mantiene un registro de los costos sumados para el destino conocido en el árbol del camino más corto de OSPF.

2.13.1 Auto cálculo

OSPF puede calcular automáticamente el costo de una interfaz. Este algoritmo se basa en la cantidad de ancho de banda que cada tipo de interfaz soporta. La suma de los valores calculados de todas las interfaces en una ruta dada forma la base para las decisiones en enrutamiento OSPF. Estos valores posibilitan a OSPF calcular rutas basadas en el ancho de banda disponible por enlace en rutas redundantes. La siguiente figura muestra una red simple que demuestra este punto.

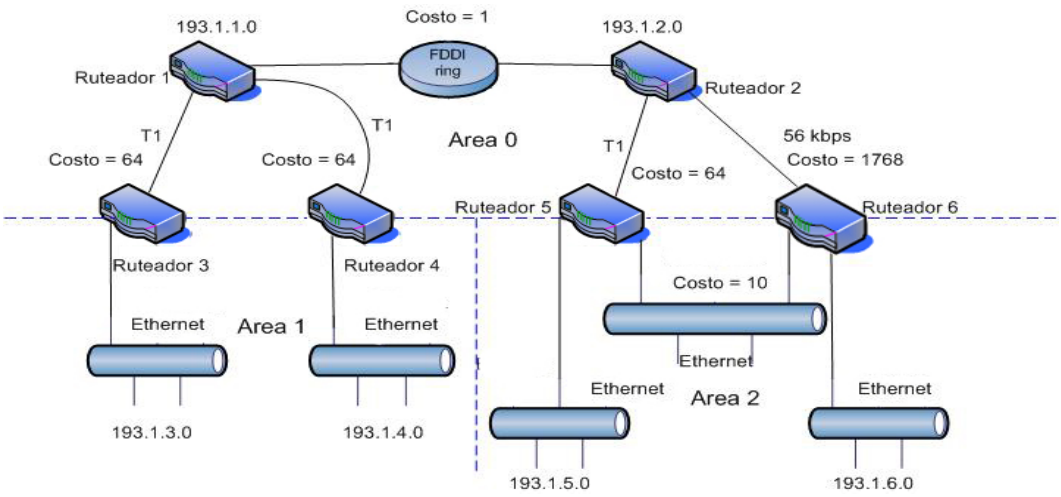


Fig.2.13 Costos auto cálculo de los enlaces.

En la figura, el costo de una ruta WAN entre un host en la red 193.1.3.0 y un sistema final en la red 193.1.4.0 es 138. Este costo es la suma de los dos enlaces T1 entre esas redes, cada cual con un costo de 64, más el costo de las interfaces de Ethernet a la red 193.1.4.0. El costo de las interfaces Ethernet en los puntos de origen y destino no están incluidos en el cálculo del costo de OSPF porque el OSPF calcula solamente los costos de interfaces de ruteadores con rumbo exterior.

La siguiente tabla resume los costos calculados automáticamente para cada una de las interfaces usadas en el diagrama de red de la figura anterior.

Tabla.2.1 Costos calculados por tipo de interfaz

Tipo de Interfaz	Costo Calculado
100-Mbps FDDI	1
10-Mbps Ethernet	10
1.544-Mbps T1 serial link	64
56-kbps serial link	1,768

2.13.2 Costos de Rutas por defecto

Es usual en el mayor interés tener costos de rutas de OSPF calculadas automáticamente, aunque esto no pueda ser posible. Los ruteadores viejos, por ejemplo, no

podrían soportar la característica de auto cálculo. En tales casos, todas las interfaces tendrán el mismo costo de OSPF. Por lo tanto, un T3 tendrá exactamente el mismo costo de una línea arrendada de 56-kbps. Claramente, estas dos facilidades ofrecen niveles de funcionamiento muy diferentes. Esta diferencia debería formar la base de las decisiones de enrutamiento informadas.

Existen, sin embargo, circunstancias que pueden hacer aceptables los costos del uso de las rutas por defecto. Si una red por ejemplo, consiste de facilidades de transmisión relativamente homogéneas, los valores por defecto serían aceptables. Alternativamente, se puede cambiar manualmente las métricas de costo para interfaces específicas. Esto facilitaría modelar los patrones de tráfico en una red de OSPF hasta que se vean ajustados, mientras se estén usando todavía los costos de enrutamiento por defecto predominantemente.

- **Redes homogéneas**

En una red homogénea, todas las facilidades de transmisión son las mismas. Todas las interfaces de una LAN deberían ser por ejemplo, de 10-Mbps Ethernet y todas la interfaces WAN de serial deberían ser T1s. En tal caso, usar los valores por defecto prefijados probablemente no causaría problemas de enrutamiento. Esto sería particularmente cierto si hubiera poca o ninguna redundancia de ruta. Para ilustrar este punto se considera el siguiente diagrama de red.

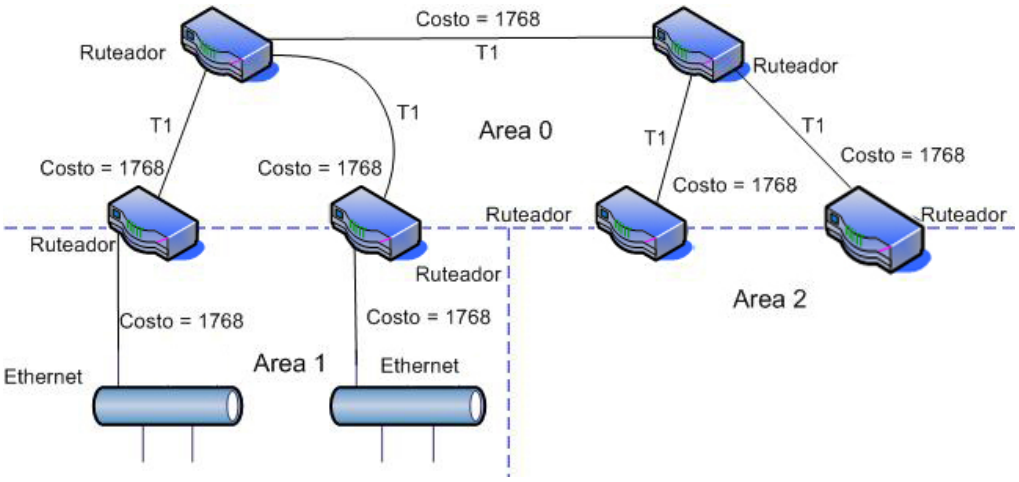


Fig.2.14 Uso aceptable de valores de interfaces predeterminadas de OSPF.

En la figura, un valor predeterminado de 1,768 fue asignado para cada una de las interfaces. Todos los enlaces WAN, sin embargo, son T1s. Dado que son todos los mismos, no importa si el valor asignado a ellos es 1, 128, 1768 o 1000000. Las decisiones de enrutamiento, en una red homogénea, serán un asunto tan simple como contar y comparar saltos (si bien es cierto que esto ocurre en múltiples costos de interfaces).

Obviamente, en una red compleja con redundancia de ruta sustancial y una diferencia en las tecnologías de transmisión usadas, el valor por defecto no posibilitaría la selección de rutas óptimas para cualquier destino dado.

- **Valores manualmente configurables**

En algunas redes, puede ser considerable aceptar costos por defecto de OSPF, y luego restaurar manualmente esos enlaces específicos que difieran de esos costos por defecto. Por ejemplo, un valor de costo por defecto de una red podría ser 1768 (valor calculado para un enlace de serie de 56 kbps). Si todos menos uno o dos de los enlaces en una red presenta el mismo ancho de banda, se podría aceptar los valores por defecto y después restaurar los valores para sus enlaces particulares.

Si se usan costos de enrutamiento calculados automáticamente, costos predeterminados, o costos configurados manualmente es irrelevante para nodos OSPF. Aceptarán completamente tales valores de costos y desarrollarán una perspectiva del árbol del camino más corto de la red.

2.13.3 El Árbol del Camino Más Corto

El propósito de los mecanismos de LSA es habilitar cada ruteador para desarrollar una perspectiva de la topología de la red. Esta topología se puede ver en la forma de un árbol. El ruteador OSPF forma la raíz del árbol. El árbol proporciona el camino completo para todas las direcciones de destino conocidas, ya sea red o host, aun cuando solo el próximo salto es realmente usado para reenviar datagramas. La razón de esto es simple:

El rastreo de los caminos completos hasta los destinos hace posible comparar los caminos redundantes y seleccionar el mejor de cada destino conocido. Si existen múltiples caminos de igual costo, son todos descubiertos y usados por OSPF. El tráfico se balancea dinámicamente de forma aproximadamente igual a través de tales enlaces disponibles.

2.14 Vecinos

Los ruteadores que comparten un segmento común son vecinos en ese segmento. Los vecinos son elegidos mediante el protocolo de Hello. Los paquetes de Hello son enviados periódicamente de cada interfaz usando IP multidifusión. Los ruteadores llegan a ser vecinos en el momento en que ellos se vean listados en el paquete Hello del vecino. De esta forma, una comunicación bidireccional se garantiza. La negociación vecina se aplica a la dirección primaria solamente. Las direcciones secundarias pueden ser configuradas en una interfaz con una restricción que tienen que pertenecer a la misma área que la dirección primaria.

Dos ruteadores no se convertirán en vecinos a menos que cumpla lo siguiente:

- Dos ruteadores teniendo un segmento común**,** sus interfaces tienen que pertenecer a la misma área en ese segmento. Por supuesto, las interfaces deben pertenecer a la misma subred y tener una máscara similar.

- OSPF permite la configuración de la clave para un área específica. Los ruteadores que quieren convertirse en vecinos tienen que intercambiar la misma clave en un segmento particular.

- OSPF intercambia paquetes de Hello en cada segmento. Esto es una forma de que los ruteadores tengan conocimiento de la existencia de un segmento, además de que con este mecanismo eligen el enrutador designado (DR) en segmentos multiacceso. El intervalo Hello especifica el tiempo, en segundos, entre los paquetes de Hello que un ruteador manda en una interfaz de OSPF. El Intervalo muerto es la cantidad de segundos que estos paquetes no se han recibidos antes de que sus vecinos lo declaren ruteador OSPF muerto.

OSPF requiere que estos intervalos sean exactamente los mismos entre dos vecinos. Si cualquiera de ellos es diferente, estos ruteadores no se convertirán en vecinos en un segmento particular.

- A dos ruteadores le deben coincidir las indicaciones del área stub de los paquetes de Hello para llegar a ser vecinos.

2.15 Adyacencias

La adyacencia es el paso siguiente después del proceso de encontrar los vecinos. Los ruteadores adyacentes irán más allá que el simple intercambio de Hello y el proceso de intercambio de la base de datos. Para reducir al mínimo la cantidad de intercambio de información en un segmento particular, OSPF elige un ruteador para ser el Ruteador Designado (Designer Router, DR), y otro para ser el Ruteador Designado de Respaldo (Backup Designated Router, BDR), en cada segmento multiacceso.

El BDR es elegido como un mecanismo de respaldo en caso de que se caiga el DR. La idea de esto es que los ruteadores tienen un punto central de contacto para intercambiar información. En vez de que cada ruteador intercambie actualizaciones con cada uno de los otros en el segmento, intercambia información con el DR y el BDR y estos les trasmiten esa información a todos los demás.

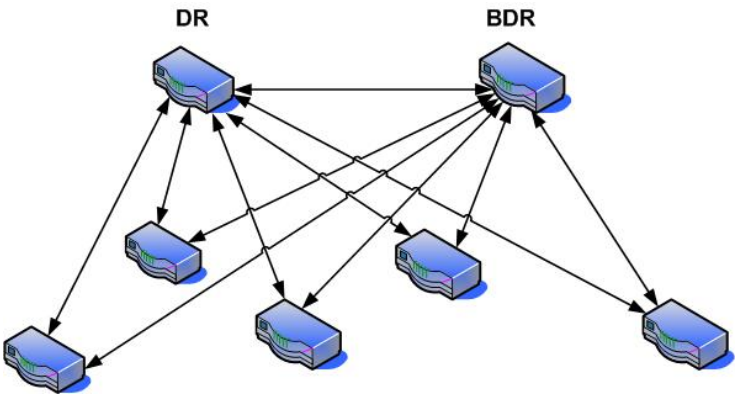


Fig. 2.15 Ruteadores adyacentes con el DR y el BDR

En el diagrama todos los ruteadores comparten un segmento multiacceso. Debido al intercambio de paquetes de Hello, un ruteador es elegido DR y otro es elegido BDR. Cada

ruteador en el segmento (el cual ya se convirtió en vecino) tratará de establecer una adyacencia con el DR y el BDR.

2.15.1 Elección del DR

La elección del DR y del BDR se hace mediante el protocolo Hello. Los paquetes de Hello son intercambiados mediante los paquetes IP multidifusión en cada segmento. El ruteador con la más alta prioridad de OSPF en un segmento se convertirá en el DR para ese segmento, repitiéndose el mismo proceso para la elección del BDR. En caso de un lazo, el ruteador con la más alta dirección IP (RID) ganará. El predeterminado para la prioridad de la interfaz de OSPF es uno. Recordar que los conceptos del DR y el BDR son para segmentos multiacceso. Una prioridad con valor 0 indica una interfaz que no debe ser elegida como DR o BDR. El siguiente diagrama muestra la elección del DR:

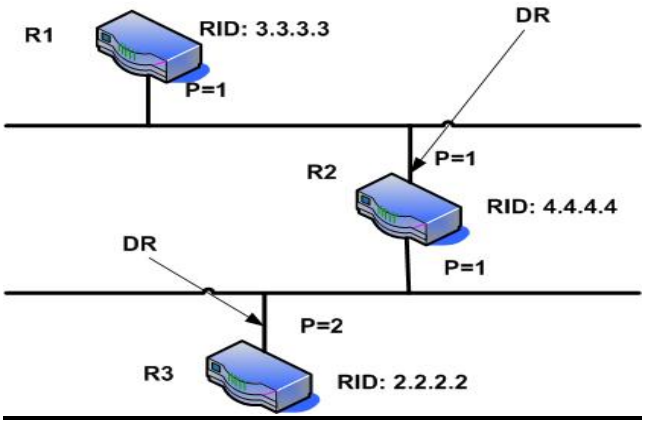


Fig. 2.16 Diagrama de eleccion del DR

En el diagrama R1 y R2 tienen la misma prioridad de interfaz pero R2 tiene más alto RID. R2 deberá ser el DR en ese segmento. R3 tiene una mayor prioridad que R2, por tanto es el DR en ese segmento.

2.15.2 Construyendo la Adyacencia

Los procesos de construir la adyacencia toman efecto después que se han cumplido múltiples etapas. Los ruteadores que se vuelven adyacentes tendrán exactamente la misma

base de datos de estado de enlace. A continuación se muestra un breve resumen de los estados por el que debe pasar un ruteador antes de ser adyacente a otro ruteador:

- Ninguna información ha sido recibida de alguien en el segmento.

- En nubes de acceso múltiple sin broadcast tales como Frame Relay and X.25, indica que ninguna información reciente ha sido recibida desde el vecino. Se debería hacer un esfuerzo para contactar al vecino mediante el envío de paquetes de Hello.

- La interfaz ha detectado un paquete viniendo de un vecino pero la comunicación bidireccional todavía no se ha establecido.

- Existe la comunicación bidireccional con un vecino. El ruteador se ha visto en los paquetes de Hello viniendo desde un vecino. Al final de esta etapa la elección del DR y del BDR habría de estar hecha. Al final de la etapa 2-way, los ruteadores decidirán si proceder con la construcción de la adyacencia o no, basándose en si uno de los ruteadores es un DR o un BDR o el enlace es punto a punto o virtual.

- Los ruteadores están tratando de establecer el número de secuencia inicial que será usado en los paquetes de intercambio de información. El número de secuencia asegura que los ruteadores siempre consigan la información más reciente. Un ruteador se convertirá en primario y el otro será secundario. El ruteador primario encuestará al secundario para información.

- Los ruteadores describirán completamente su base de datos de estado de enlaces enviando paquetes de descripción de base de datos. En este estado, lo paquetes podrían ser inundados a otras interfaces en el ruteador.

- En este estado, los ruteadores están finalizando el intercambio de información. Los ruteadores han construido una lista de la solicitud del estado de enlace y una lista de retransmisión del estado de enlace. Cualquier información que parezca incompleta o anticuada será puesta en la lista de solicitud. Cualquier actualización que se envíe se pondrá en la lista de retransmisión hasta que se reconozca.

- En este estado, la adyacencia está completa. Los ruteadores vecinos están completamente adyacentes. Los ruteadores adyacentes tendrán exactamente la misma base de datos de estado de enlace.

2.15.3 Tipos de adyacencias:

- **Adyacencias en interfaces Punto a Punto:** OSPF siempre formará una adyacencia con el vecino en el otro lado de una interfaz punto-a-punto tales como líneas serial punto a punto.

- **Adyacencias en redes de acceso múltiple sin broadcast (NBMA):** Se debe tener cuidado cuando se configura OSPF sobre medios de acceso múltiple sin broadcast tales como Frame Relay, X.25, ATM. El protocolo considera estos medios como cualquier otro medio de broadcast tales como Ethernet. La selección del DR se vuelve un problema porque el DR y el BDR necesitan tener una conectividad física completa con todos los ruteadores que existen en la nube. Además, debido a la falta de capacidades de difusión, el DR y el BDR necesitan tener una lista estática de todos los demás ruteadores unidos a la nube.

El siguiente diagrama muestra una red donde la selección del DR es muy importante:

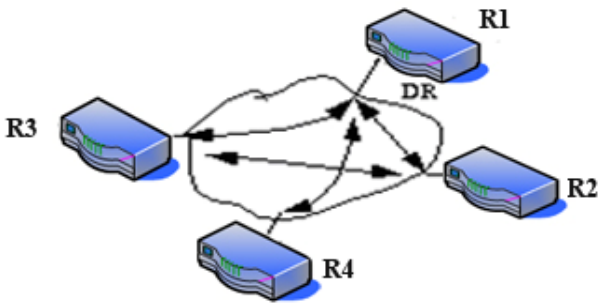


Fig. 2.17 Elección del DR

Es esencial para la interfaz de R1 de la nube ser el DR elegido, porque es el único ruteador que tiene conectividad completa con los otros ruteadores. La elección del DR podría estar influenciada por la configuración de la prioridad de OSPF en las interfaces.

2.16 Redistribución de rutas en OSPF

La redistribución de rutas en OSPF de otros protocolos de enrutamiento o estáticos causará que estas rutas se conviertan en rutas externas.

Ruta externa E1 vs. E2

OSPF soporta dos tipos de métricas externas, tipo externa 1 y tipo externa 2. La diferencia entre los dos es en la forma de costo (métrica) de la ruta que está siendo calculada. El costo del tipo 2 es siempre el costo externo, independiente del costo interior para alcanzar esa ruta. El costo del tipo 1 es la suma del costo externo y del interno usado para alcanzar esa ruta. Una ruta tipo 1 se prefiere siempre sobre una ruta tipo 2 para el mismo destino. Esto se ilustra en el siguiente diagrama:

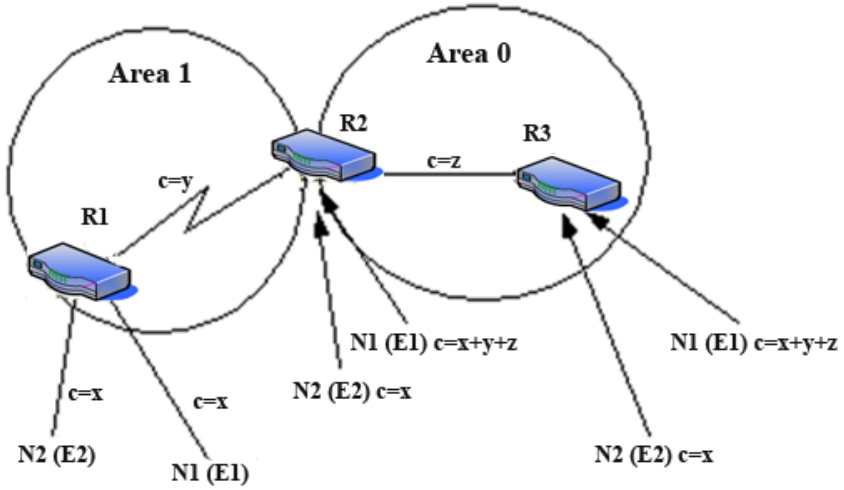


Fig. 2.18 Costo de rutas externas

Como se muestra en el diagrama, R1 está redistribuyendo dos rutas externas en OSPF. N1 y N2 tienen un costo externo de **x**. La única diferencia es que N1 es redistribuido en OSPF con un tipo métrico 1 y N2 se redistribuye con un tipo métrico 2.

Si se muestra el flujo de las rutas desde el Área 1 al Área 0, el costo para alcanzar N2 desde R2 o R3 como se puede ver será siempre **x**. El costo interno no es considerado. Por otra parte el costo para alcanzar N1 es incrementado por el costo interno. El costo es **x+y** como se puede ver desde R2 y **x+y+z** desde R3.

Si las rutas externas son ambas de tipo 2 y los costos externos a la red destino son iguales, entonces el camino con menor costo al ASBR se selecciona como el mejor camino.

Salvo que se especifique lo contrario, el tipo externo dado a las rutas externas por defecto, es el tipo 2.

2.17 Redistribución de OSPF en otros protocolos

➢ Uso de una Métrica Válida

Siempre que se redistribuya OSPF en otros protocolos, se tienen que respetar las reglas de esos protocolos. En particular, la métrica aplicada se debe corresponder a la métrica usada por el protocolo. Por ejemplo, la métrica de RIP es una cantidad de saltos que se extiende entre 1 y 16, donde 1 indica que una red es un salto lejos y 16 que la red es inalcanzable.

➢ Máscara de red de tamaño variable, VLSM

Otra edición a considerar es VLSM. OSPF puede llevar información múltiple de la red hasta la red principal, pero otros protocolos como RIP e IGRP no pueden. Si la red principal cruza la frontera de un dominio OSPF y RIP, la información redistribuida de VLSM en RIP o IGRP se perderán y las rutas estáticas tendrán que ser configuradas en el dominio RIP o IGRP.

➢ Redistribución mutua

La redistribución mutua entre protocolos se debe hacer con mucho cuidado y de manera controlada. Una configuración incorrecta podría conducir a un lazo potencial de información de enrutamiento. Una regla para la redistribución mutua es no permitir que la información aprendida de un protocolo sea inyectada de vuelta dentro del mismo protocolo. Las interfaces pasivas y las listas distribuidas deben ser aplicadas en los ruteadores de redistribución.

2.18 Estructura de datos de OSPF

OSPF es un protocolo de enrutamiento que usa un arreglo extensivo de estructura de datos. Cada estructura, o tipo de mensaje, está definido para realizar una tarea específica. Todos ellos comparten un encabezado común, conocido como el encabezado de OSPF, que tiene 24 octetos de largo y tiene los siguientes campos:

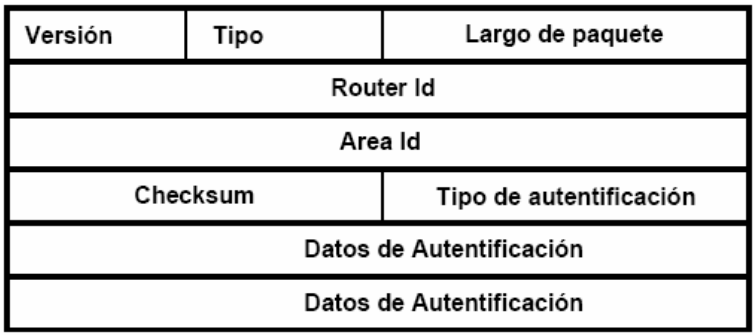


Fig.2.19 Encabezado de OSPF

Versión: El primer octeto de un encabezado de OSPF es para la identificación del número de versión.

Tipo: El segundo octeto identifica cuál de los cinco tipos de paquetes OSPF está anexado a esta estructura de encabezado. Los cinco tipos de paquetes están numéricamente identificados.

Largo del paquete: Los siguientes dos octetos del encabezado de OSPF se usan para informar el nodo que recibe el paquete de su largo total. El largo total incluye la carga útil del paquete así como su encabezado.

Identificador del Ruteador: A cada ruteador en un área se le asigna un número de identificación único de 4 octetos. Un ruteador OSPF ocupa este campo con su número ID antes de transmitir cualquier mensaje de OSPF a otros ruteadores.

Identificador del Área: Cuatro octetos del encabezado son usados para identificar el número de identificación del área.

Checksum: Cada encabezado de OSPF contiene un campo checksum que se puede usar para detectar el daño hecho al mensaje en tránsito. El originador ejecuta un algoritmo matemático para cada mensaje y almacena los resultados en este campo. El nodo receptor ejecuta este mismo algoritmo para el mensaje recibido y compara su resultado con el resultado en el campo checksum. Si el mensaje arribado está intacto, los dos resultados deberán ser idénticos, por lo que una incompatibilidad indica que el paquete OSPF fue dañado en el tránsito. El receptor solamente descarta los paquetes que estén dañados.

Tipo de autentificación: OSPF puede protegerse contra los tipos de ataques que pueden resultar en información de enrutamiento falsa por la autentificación del originador de cada mensaje OSPF. Este es un campo de dos octetos que identifica cuál de todas las formas de autentificación se usa en este mensaje.

Datos de Autentificación: Los últimos nueve octetos del encabezado son usados para llevar cualquier dato de autentificación que puede ser necesitado por el receptor para autentificar el originador del mensaje.

Esta estructura básica contiene toda la información que un nodo OSPF necesita para determinar, ya sea que el paquete debería ser aceptado por un procesamiento superior o descartado. Los paquetes que han sido dañados serán descartados, así como los paquetes que no pueden ser autentificados.

OSPF usa cinco tipos diferentes de paquetes. Cada uno de los cuales está designado para soportar una función específica dentro de la red:

- Paquetes de Hello (Tipo 1)
- Paquetes de descripción de la base de datos (Tipo 2)
- Paquetes de solicitud del estado del enlace (Tipo 3)
- Paquetes de actualización del estado del enlace (Tipo 4)
- Paquetes de reconocimiento del estado del enlace (Tipo 5)

2.18.1 El paquete de Hello

OSPF contiene un protocolo (el protocolo Hello) que es usado para establecer y mantener relaciones entre los nodos vecinos. Estas relaciones son llamadas adyacencias. Las adyacencias son la base para el intercambio de enrutamiento de datos en OSPF.

Es a través del uso de este protocolo y de este tipo de paquete que un nodo OSPF descubre los otros nodos OSPF en su área. Típicamente, los mensajes se envían cada 10 segundos, y se considera que ha ocurrido una falla en un vecino si no se recibe un mensaje de él durante 40 segundos. Se le llama así intencionalmente; el protocolo Hello establece comunicaciones entre ruteadores vecinos potenciales. Usa una estructura de subpaquete especial que es anexado al encabezado OSPF estándar de 24 octetos. Juntas, estas estructuras forman un paquete de Hello.

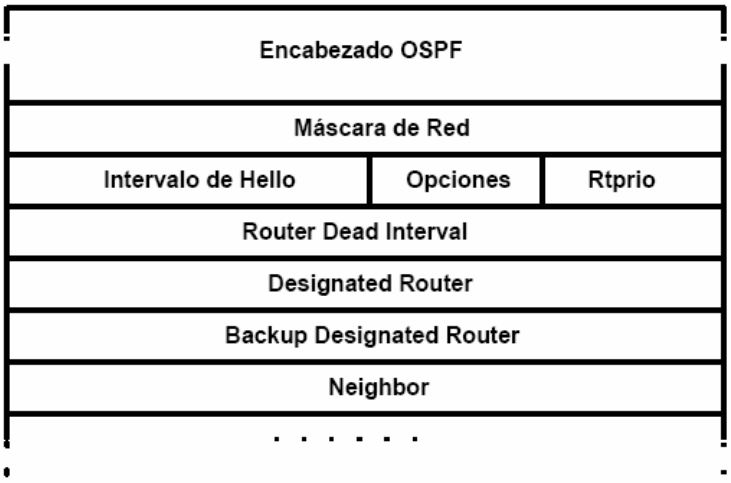


Fig.2.20 Paquete de Hello

Todos los ruteadores en una red OSPF pueden adherirse a ciertas convenciones que puede ser uniformada completamente la red. Estas convenciones implican lo siguiente:

- Máscara de red
- Intervalo de Hello: intervalo en el cual los paquetes de hello serán emitidos.
- Intervalo muerto del ruteador (Router Dead Interval): la cantidad de tiempo que puede transcurrir antes que el ruteador no responda será declarado muerto por los otros ruteadores en la red.

Todos los ruteadores en una red OSPF deben estar de acuerdo para usar el mismo valor de cada uno de estos parámetros; de otra manera, la red podría no funcionar adecuadamente. Estos parámetros son intercambiados usando paquetes de hello. Juntos, incluyen la base para las comunicaciones vecinas. Aseguran que las relaciones vecinas no se formen entre ruteadores en diferentes subredes y que todos los miembros de la red concuerden en cómo se mantienen en contacto con los otros frecuentemente.

El paquete de hello además incluye una lista de otros ruteadores (usando sus identificaciones de ruteador) con los que el ruteador fuente ha estado recientemente en contacto. El campo Vecino (Neighbor) facilita el proceso del descubrimiento del vecino. El paquete de hello además contiene otros campos tales como el Designated Router y Backup Designated Router. Estos campos son útiles en el mantenimiento de adyacencias y soportan la operación de la red OSPF en los periodos de estabilidad y convergencia.

2.18.2 El paquete de descripción de la base de datos

Este paquete se intercambia entre dos ruteadores OSPF cuando inicializan una adyacencia. Este tipo de paquete es usado para describir, pero no transporta realmente, los contenidos de una base de datos de estado de enlaces de un ruteador OSPF. Debido a que esta base de datos puede ser muy larga, múltiples paquetes de descripción de base de datos pueden ser necesitados para describir todo el contenido de una base de datos. De hecho, un campo es reservado para la identificación de la secuencia de los paquetes de descripción de la base de datos. La re secuenciación asegura que el recipiente puede reproducir fácilmente la descripción de la base de datos trasmitida.

La descripción de la base de datos intercambia procesos, además sigue un método de votación/respuesta, en el cual uno de los ruteadores es designado como el maestro. Las otras funciones como el esclavo. El ruteador maestro envía sus contenidos de la tabla de enrutamiento al esclavo. Las responsabilidades del esclavo son solamente el conocimiento de los paquetes de descripción de la base de datos recibidos. Obviamente, la relación entre el esclavo y el maestro varía con cada intercambio de la descripción de la base de datos. Todos los ruteadores dentro de la red, en tiempos diferentes, funcionaran como maestro y esclavo durante este proceso.

2.18.3 El paquete de solicitud del estado del enlace

Este paquete es usado para solicitar pedazos específicos de una base de datos de estado de enlace de un ruteador vecino. Aparentemente, después de recibir una actualización de la descripción de la base de datos, un ruteador OSPF puede descubrir que la información del vecino es o más corriente o más completa que la suya propia. Si es así, el ruteador envía uno o varios paquetes de solicitud de estado de enlace a sus vecinos (el que está con la información más reciente) para solicitar más información específica de enrutamiento del estado de enlace.

La solicitud para más información tiene que ser muy específica, ya que tiene que especificar cuál dato se requiere. Para esto se usan los siguientes criterios:

- El número del tipo de estado de enlace
- El identificador del estado de enlace
- Ruteador de Anuncio

Juntos, estos criterios identifican una subred específica de una base de datos de OSPF, pero no su instancia. Una instancia es la misma subred de información pero con una frontera temporal. Es importante recordar que OSPF es un protocolo de enrutamiento dinámico: se puede esperar una actualización automática de las perspectivas de la red como una reacción a los cambios en el estado de enlace en la red. Por consiguiente, el receptor de un paquete de petición de estado de enlace lo intercepta para ser la iteración más reciente de este pedazo particular de su base de datos de enrutamiento.

2.18.4 El paquete de actualización del estado del enlace

Es usado para transportar LSAs a los nodos vecinos. Estas actualizaciones son generadas en respuesta a una solicitud de LSA. Existen cinco tipos de paquetes de LSA. Estos tipos de paquetes y sus respectivos números de LSA se muestran a continuación:

- *LSA Ruteador (Tipo 1): D*escribe el estado y el costo de los enlaces del ruteador al área. Todos los enlaces semejantes tienen que estar descritos en un solo paquete LSA.

Además, un ruteador tiene que originar un ruteador LSA para cada área a la que pertenece. Por consiguiente, un ABR generaría múltiples LSAs ruteadores, considerando que un IR necesita generar solamente una actualización.

- **LSA Red (Tipo 2):** Un LSA red es similar al LSA ruteador en que además describe la información del estado de enlace y del costo para todos los ruteadores unidos en la red. La diferencia entre ellos es que un LSA red es una agregación de toda la información del estado de enlace y del costo en la red. Solamente el DR de la red rastrea esta información y puede generar un LSA red.

- **LSA-IPred Resumen (Tipo 3)**: Solamente los ABRs en una red OSPF pueden generar este tipo de LSA. Se usa para comunicar la información de enrutamiento resumida sobre el área a las áreas vecinas en la red OSPF. Es usualmente preferible resumir rutas por defecto en vez de propagar información de OSPF resumida en otras redes.

- **LSA-ASBR Resumen (Tipo 4)**: Un análogo al LSA tipo 3 es el LSA tipo 4. La diferencia entre ellos es que el LSA tipo 3 describe rutas inter áreas, mientras que el tipo 4 describe rutas que son externas a la red OSPF.

- **LSA AS-externo (Tipo 5):** Como su nombre implica, se usan para describir destinos fuera de la red OSPF. Estos destinos pueden ser direcciones tanto host-especificas como de redes externas. Un nodo OSPF que funciona como el ASBR al sistema autónomo externo es responsable por la propagación de esta información de enrutamiento externo a lo largo de todas las áreas a las cuales pertenece.

Estos LSAs se utilizan para describir diferentes aspectos del dominio de enrutamiento de OSPF. Son directamente direccionados a cada ruteador en el área OSPF y transmitidos simultáneamente. Esta inundación asegura que todos los ruteadores en un área OSPF tengan la misma información sobre los cinco aspectos (tipos de LSA) de su red. Una colección completa de los datos de LSA del ruteador se almacena en una base de datos del estado de enlace. El contenido de esta base de datos, cuando está sujeto al algoritmo de Dijkstra, resulta en la creación de la tabla de enrutamiento de OSPF. La diferencia entre la tabla y la base de datos es que esta última contiene una colección completa de los datos en bruto considerando

que la tabla de enrutamiento contiene una lista del camino más corto para conocer destinos mediante los puertos de interfaz de ruteadores específicos.

En vez de examinar la estructura de cada tipo de LSA, podría ser suficiente examinar solamente sus encabezados.

Encabezado de LSA

Todos los LSAs usan un formato de encabezado común. Este encabezado es de 20 octetos de largo. El encabezado de LSA está designado para identificar cada LSA. Por consiguiente, contiene información sobre el tipo de LSA, el Identificador del estado de enlace y el Identificador del ruteador de anuncio. Los campos del encabezado de LSA son:

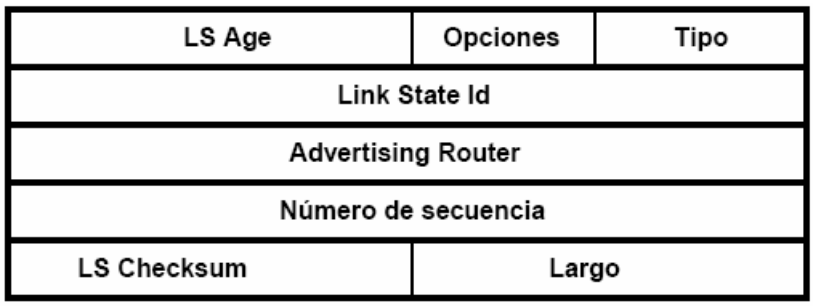


Fig.2.21 Encabezado de un LSA

- LS Edad: Esta edad es el número de segundos que ha trascurrido desde que el LSA fue originado.

- Opciones de OSPF: Consiste de una serie de indicaciones que identifican los servicios opcionales que una red OSPF puede soportar.

- Tipo de LS: Identifica cuál de los cinco tipos de LSA contiene. El formato de cada tipo de LSA es diferente. Por consiguiente, es necesario identificar cuál tipo de dato está anexado a este encabezado.

- Identificador del Estado de Enlace: Identifica la porción específica del entorno de la red que el LSA describe. Este campo está estrechamente relacionado con el campo del Tipo de LS. De hecho, el contenido de este campo depende directamente en el tipo de LS. En un

LSA ruteador, por ejemplo, el Identificador del estado del enlace contiene el Identificador del ruteador OSPF del originador del paquete: el ruteador anunciador.

- Ruteador Anunciador: Es el ruteador que origina este LSA. Por consiguiente, el campo del ruteador anunciador contiene el Identificador del ruteador OSPF del originador de LSA.

- Número de Secuencia del LS: Los ruteadores OSPF incrementan el número de secuencia por cada LSA generado. Por consiguiente, un ruteador recibe dos instancias del mismo LSA y tiene dos opciones para determinar cuál de los dos es el más reciente. Este campo puede ser chequeado para determinar cuánto tiempo el LSA ha estado atravesando la red. Es teóricamente posible para un LSA reciente tener una mayor edad de LSA que un LSA viejo, particularmente en largas y complicadas redes OSPF. Por consiguiente, los ruteadores receptores comparan el número de secuencia del LS y el que tenga el mayor número es el que fue generado más reciente.

- Checksum de LS: Es usado pata detectar daños para los LSAs en rumbo a sus destinos. Los Checksums son algoritmos matemáticos simples. Su salida depende de su entrada. La entrada es altamente consistente. Suministrada la misma entrada, un algoritmo de Checksum retornará siempre a la misma salida. Este campo usa parte del contenido del paquete de LSA (el cual incluye el encabezado, excepto por los campos de la edad del LS y del Checksum) para derivar un valor Checksum. El nodo fuente ejecuta un algoritmo conocido como el algoritmo de Fletcher y almacena los resultados en el campo LS Checksum. El nodo destino ejecuta el mismo ejercicio matemático y compara su resultado con el resultado almacenado en el campo Checksum. Si los valores son diferentes, es relativamente seguro asumir el daño que ha ocurrido en el tránsito. Por lo tanto, se genera una solicitud de retransmisión.

- Longitud del LS: De forma previsible, este campo informa el receptor de la longitud del LSA, en octetos.

El resto del cuerpo del paquete de LSA contiene una lista de LSAs. Cada LSA describe uno de los cinco aspectos distintos de una red OSPF, como se identifica por el número de LSA.

Por consiguiente, un paquete del LSA ruteador debería anunciar información sobre los ruteadores conocidos para existir dentro de un área.

Procesando actualizaciones de LSA

OSPF difiere sustancialmente de otras tablas de enrutamiento en que sus actualizaciones no son directamente utilizables por los nodos receptores. Las actualizaciones recibidas desde otros ruteadores contienen información sobre la red de la perspectiva de ese ruteador. Por consiguiente, el dato del LSA recibido tiene que ser sometido al algoritmo de Dijkstra de un ruteador para convertirlo a su propia perspectiva antes que el dato pueda ser interpretado o usado.

Aparentemente, los LSAs son trasmitidos porque un ruteador detecta un cambio en el/los enlace(s). Por consiguiente, después de recibir un LSA de cualquier tipo, un ruteador OSPF tiene que chequear que el contenido del LSA contra la de su base de datos de enrutamiento. Esto no puede estar hecho hasta después que el ruteador use el nuevo dato para formar una nueva perspectiva de la red, la cual se hace mediante el algoritmo SPF. El resultado de esta salida es la nueva perspectiva de ruteador de la red. Estos resultados se comparan con la base de datos de enrutamiento existente para ver si cualquiera se sus rutas han sido afectadas por el cambio del estado de la red.

Si una o más rutas existentes tienen que cambiar como resultado del cambio de estado, el ruteador construye una nueva base de datos de enrutamiento usando la nueva información.

LSAs duplicados

Dado que los LSAs son inundados a través de un área OSPF, es posible que la múltiple ocurrencia, conocida como instancias, del mismo tipo de LSA exista simultáneamente. La estabilidad de una red OSPF, por consiguiente, requiere que un ruteador sea capaz de identificar la instancia más actual del LSA duplicado. Un ruteador que recibe dos o más instancias del mismo tipo de LSA examina los campos de la edad, número de secuencia y Checksum del LS en los encabezados de LSA. Solamente la información más nueva contenida en el LSA es aceptada y subordinada a los procesos descritos anteriormente.

2.18.5 Paquete de reconocimiento del estado de enlace

OSPF destaca una distribución confiable de los paquetes LSA (recordar que LSA es válido para el anuncio del estado de enlace y no para su reconocimiento). La confidencialidad significa que el recibo del paquete tiene que ser reconocido; de otra forma, el nodo fuente no tendría una forma de conocimiento si el LSA realmente cumplió su destino pretendido. Por lo tanto, algún mecanismo se necesita para reconocer el recibo de LSAs; este mecanismo es el paquete de reconocimiento del estado del enlace.

Este paquete solamente identifica el paquete LSA del cual se reconoce el recibo. Esta identificación se basa en la información del encabezado contenida en el encabezado del LSA. Incluyendo el número de secuencia del LS y del ruteador anunciador. Múltiples LSAs pueden ser reconocidos con un solo paquete de reconocimiento.

Capítulo 3. Características generales de la UCI y propuesta de implementación del protocolo de enrutamiento OSPF.

En el capítulo anterior se abordó la arquitectura del protocolo de enrutamiento OSPF incluyendo tópicos de gran importancia en el mundo de hoy en las redes telemáticas.

En este capítulo se realiza un análisis de lo que constituye el objeto de estudio para la aplicación de un nuevo protocolo de enrutamiento en la UCI garantizando que el tráfico sea lo más eficiente posible, para la implantación de servicios futuros en la universidad. Dando lugar a una propuesta para dar solución a los problemas en la red.

3.1 La red de la UCI.

La Universidad de las Ciencias Informáticas tiene como misión ser una universidad innovadora de excelencia científica, académica y productiva, siendo el soporte de la informatización del país y la competitividad internacional de la industria cubana del software. En aras de cumplir sus objetivos la UCI posee una infraestructura de red de grandes dimensiones sobre la cual se desarrolla el concepto de una “ciudad digital”, en la que existe un elevado tráfico de información.

Cuenta con una infraestructura de red de área local (LAN), donde los switches capa 3 de los nodos nivel 1 como el nodo central, docencia, parque tecnológico y residencia están conectados mediante fibra óptica con una velocidad de 10Gbps. El nodo de parque tecnológico se conecta con sus módulos a una velocidad de 1 Gbps, al igual que el nodo de docencia con los nodos de los docentes 2, 3, 4 y 5. El nodo central con el rectorado, el docente 1 viejo y producción también se conectan a esa velocidad. El nodo de residencia se conecta con el nodo Biblioteca, Edificio 58 y Edificio 123 a una velocidad de 2 Gbps. Las conexiones entre máquinas de los edificios de residencia, laboratorios u oficinas se conectan a un switch capa 2 a una velocidad de 100 Mbps mediante cable UTP. Estos switches se conectan a sus respectivos subnodos a una velocidad de 100 Mbps pero mediante fibra óptica.

En la siguiente figura se muestra lo explicado anteriormente:

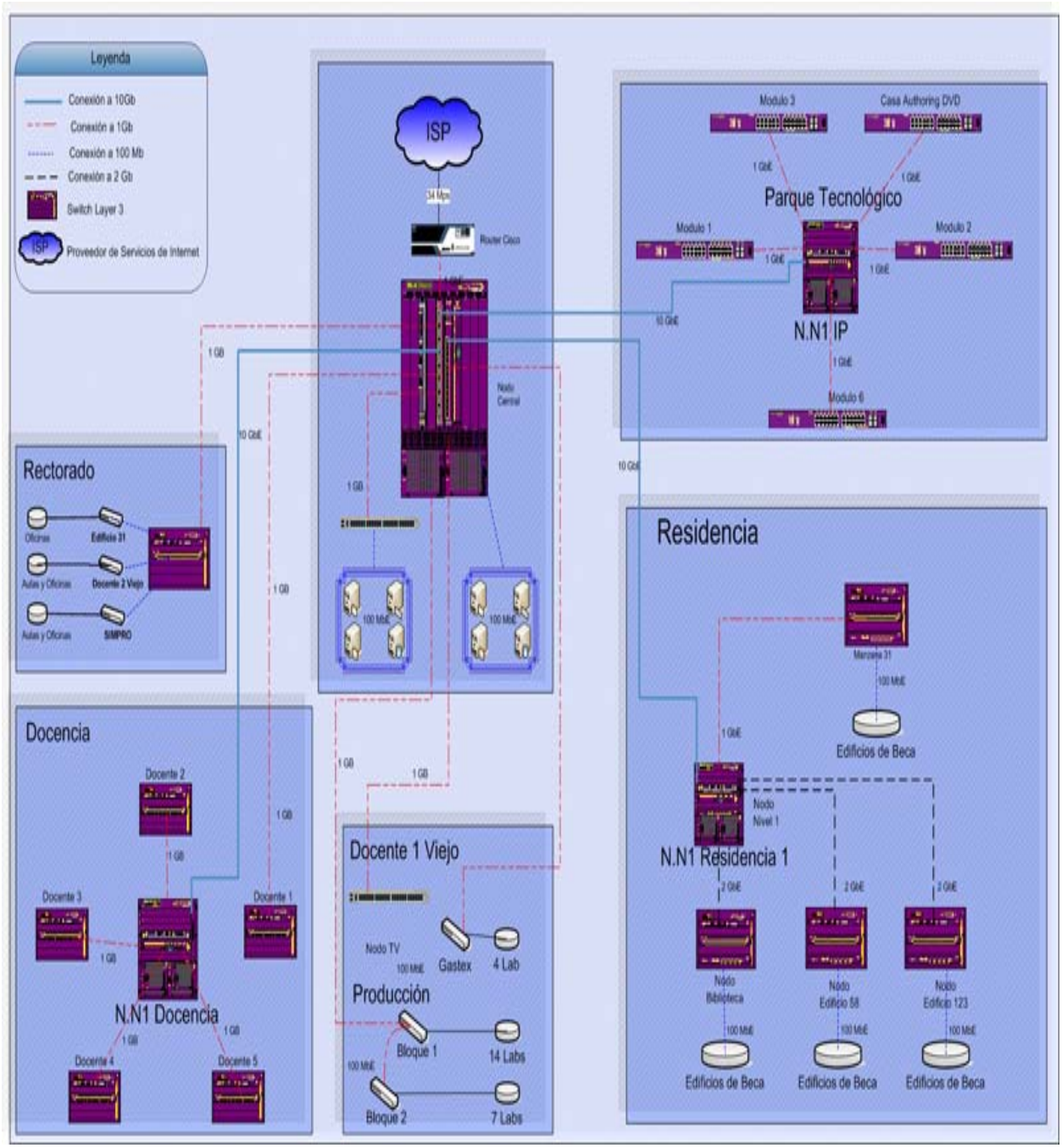


Fig.3.1 Red Actual de la UCI

La universidad empezó con una red relativamente pequeña y cuenta hoy en día con alrededor de 7500 computadoras y poco más de 13 000 usuarios, los cuales tienen acceso a distintos servicios que brinda la red de la universidad, como son correo electrónico, navegación

por Internet, intranet y mensajería instantánea, los cuales son soportados por servidores localizados en el nodo central por un personal capacitado.

Se espera que la red de la UCI siga aumentando, puesto que existen nuevas facultades regionales en Artemisa, Ciego de Ávila y Manzanillo y hay expectativas de que existan en cada provincia del país, por lo que la cantidad de usuarios va a aumentar al igual que el tráfico en la red.

3.1.1 Servicios actuales en la universidad

En la red de la UCI se brindan una gran cantidad de servicios telemáticos, puesto que se quiere lograr digitalizar todos y cada uno de los servicios de la universidad. Estos son:

Correo electrónico: Este servicio garantiza el intercambio de correo electrónico entre todos los usuarios de la universidad y de estos con personas e instituciones fuera de la misma. La mensajería interna se maneja con el Microsoft Exchange Server 2003, mientras que el correo que se recibe y se manda hacia internet con el Qmail de Linux.

Navegación: Esta les da a los usuarios la posibilidad de poder visitar sitio de interés. Esta navegación se realiza de distintas maneras, una es la navegación nacional, la otra es la navegación básica y finalmente la navegación plena. Estás se aplican según los niveles de autorización que tengan los usuarios. La navegación se realiza a través de un servidor Proxy (Squid, de Linux), el cual tiene implementado un sistema para el control de cuotas y realiza la autenticación de usuarios a partir de un servicio LDAP implementado en los controladores del dominio.

Mensajería instantánea: Los usuarios disponen de un servicio de comunicación en tiempo real que brinda un servidor de Jabber.

Acceso remoto: Este servicio habilita a los profesores y algunos trabajadores para acceder remotamente, utilizando la vía telefónica, a la red de la UCI.

Multimedia: En la universidad hay un servidor de media: Inter-nos, que da la posibilidad de acceder a las teleclases y a opciones de entretenimiento como películas, series, etc. Este servicio es un alto consumidor de recursos de red.

Transferencia de ficheros: Brinda la posibilidad de que mediante un servidor FTP que posee gran volumen de documentación y programas de utilidad para los usuarios de la universidad, la descarga de los mismos.

Debido a que se quiere digitalizar la universidad, se propone brindar otros servicios que requieren un mayor ancho de banda. Entre ellos está la telefonía IP, IPTV (variante de la televisión digital) y la videoconferencia. Para esto se quiere implementar un protocolo de enrutamiento que pueda disminuir el constante intercambio de información y que escoja caminos de menor ancho de banda.

3.1.2 Topología y protocolo de enrutamiento actuales en la UCI

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

La topología en una red es la configuración adoptada por las estaciones de trabajo para conectarse entre sí. En la universidad la red se encuentra distribuida en topología en estrella.

Topología en estrella

Reduce la posibilidad de fallo de red conectando todos los nodos a un nodo central. Todos los nodos periféricos se pueden comunicar con los demás transmitiendo o recibiendo del nodo central solamente. Un fallo en la línea de conexión de cualquier nodo con el nodo central provocaría el aislamiento de ese nodo respecto a los demás, pero el resto de sistemas permanecería intacto.

Los datos en estas redes fluyen del emisor hasta el concentrador, este realiza todas las funciones de la red, además actúa como amplificador de los datos.

La red se une en un único punto, normalmente con un panel de control centralizado, como un concentrador de cableado. Los bloques de información son dirigidos a través del panel de control central hacia sus destinos. Este esquema tiene una ventaja al tener un panel de

control que monitorea el tráfico y evita las colisiones y una conexión interrumpida no afecta al resto de la red.

Debido a que la topología estrella utiliza un cable de conexión para cada computadora, es muy fácil de expandir, sólo dependerá del número de puertos disponibles en el hub o switch. La desventaja de esta topología en la centralización de la comunicación, ya que si el hub falla, toda la red se cae.

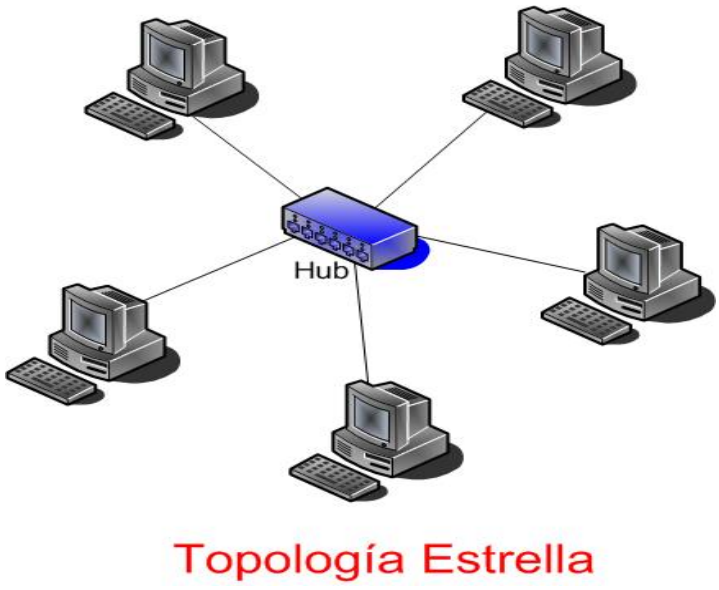


Fig. 3.2 Topología en estrella de una red

Ventajas de la topología Estrella	Desventajas de la topología Estrella
Gran facilidad de instalación	Requiere más cable que la topología de BUS.
Posibilidad de desconectar elementos de red sin causar problemas	Un fallo en el concentrador provoca el aislamiento de todos los nodos a él conectados.
Facilidad para la detección de fallo y su reparación.	Se deben comprar hubs o concentradores.

Protocolo de Información de Enrutamiento, RIP

RIP calcula el camino más corto hacia la red destino usando el algoritmo del vector de distancias. La distancia o métrica está determinada por el número de saltos de ruteador hasta alcanzar la red de destino.

RIP no es capaz de detectar rutas circulares, por lo que necesita limitar el tamaño de la red a 15 saltos. Cuando la métrica de un destino alcanza el valor de 16, se considera como infinito y el destino es eliminado de la tabla (inalcanzable).

La métrica de un destino se calcula como la métrica comunicada por un vecino más la distancia en alcanzar a ese vecino. Teniendo en cuenta el límite de 15 saltos mencionado anteriormente. Las métricas se actualizan sólo en el caso de que la métrica anunciada más el coste en alcanzar sea estrictamente menor a la almacenada. Sólo se actualizará a una métrica mayor si proviene del enrutador que anunció esa ruta.

- **Ventajas y desventajas**

En comparación con otros protocolos de enrutamiento, RIP es más fácil de configurar. Además, es un protocolo abierto, soportado por muchos fabricantes.

Por otra parte, tiene la desventaja que, para determinar la mejor métrica, únicamente toma en cuenta el número de saltos (por cuántos ruteadores o equipos similares pasa la información); no toma en cuenta otros criterios importantes, especialmente el ancho de banda. Esto puede causar ineficiencias, ya que puede preferir una ruta de bajo ancho de banda.

- **Actualizaciones de enrutamiento**

RIP envía mensajes de actualización de enrutamiento en intervalos regulares y cuando ocurren cambios en la topología de la red. Cuando un ruteador recibe una actualización que incluye cambios no registrados, actualiza su tabla de enrutamiento para asentar la nueva ruta.

El valor de la métrica para el mensaje es aumentado por el ruteador en uno, y el origen es indicado como el próximo salto. Los enrutamientos con RIP utilizan solamente la mejor ruta (la ruta con el menor costo de métrica) a un destino. Después de la actualización de su tabla de enrutamiento, el ruteador inmediatamente trasmite las actualizaciones para informar a los ruteadores vecinos. Estas actualizaciones son enviadas independientemente de las actualizaciones programadas que RIP envía. Esto trae como consecuencia que se genere mucho trafico con el envío periódico de estas actualizaciones.

- **Métrica de enrutamiento de RIP**

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

- **Prevención de loops**

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

En la Universidad este protocolo es ineficiente puesto que al enviar copias periódicas de las tablas de enrutamiento de un ruteador a otro, genera mucho tráfico en la red. Escoge el camino más corto, sin tener en cuenta el ancho de banda, ya que puede enviar los paquetes por un camino que tenga bajo ancho de banda. Además, como la red de la universidad está en topología en estrella un paquete para ir de una fuente a su destino tiene que dar muchos saltos

y pudiera llegar a dar 16 saltos y el destino volverse inalcanzable. El algoritmo que utiliza este protocolo acumula información acerca de las distancias de la red, permitiéndole mantener una base de datos de la topología de la red. Sin embargo, los algoritmos de vector-distancia no permiten que un ruteador conozca la topología exacta de una red, ya que solo ven a sus ruteadores vecinos.

3.2 Proyección futura de la red de la UCI

En la UCI se quieren hacer cambios significativos en la red para garantizar mayor eficiencia y rapidez en la transmisión de datos. Para esto es necesario reestructurar la red tanto física como lógica.

3.2.1 Diseño topológico de la red

Se desea reorganizar la red para una estructura de topología malla puesto que utiliza conexiones redundantes entre los dispositivos de la red así como una estrategia de tolerancia a fallas. Utilizando conexiones punto a punto entre todas las terminales de la red, permitiendo que cualquier terminal se comunique con otras terminales de forma paralela si fuera necesario.

La principal ventaja es que este tipo de redes difícilmente falla, pues inclusive, si alguna de estas líneas fallara aún así se podrían encontrar otras rutas para lograr la información.

La desventaja de la topología en malla, es que se requiere demasiado cableado, pero debido a la redundancia, la red puede seguir operando si una conexión se rompe.

Si existen n terminales en la red entonces se requerirían:
No. cables=n(n-1)/2 cables en total.

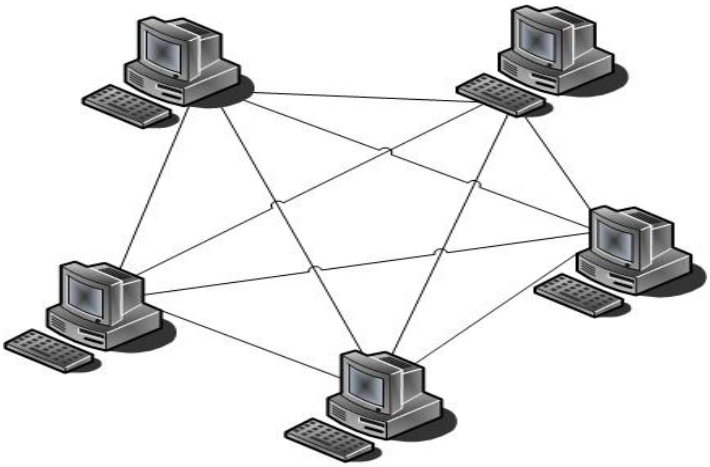


Fig. 3.3 Topología en malla de una red

Debido a los cambios topológicos que se quieren hacer en la red de la UCI, el protocolo RIP no sería eficiente, puesto que no se utilizarían las ventajas que aporta esta nueva topología. RIP solo escoge un camino, mientras que OSPF que es el protocolo que se quiere implementar trabaja en redes que sean redundantes y si se cae la conexión de un destino, puede enviar el paquete por otro camino. OSPF es un protocolo de enrutamiento por excelencia para este tipo de redes, además que de tiene en cuenta el ancho de banda, generando menor tráfico, siendo el ideal para redes LAN de cantidades considerables de clientes.

También que se espera que la UCI siga creciendo y al crecer el tamaño de las redes, crecen proporcionalmente las tablas de enrutamiento del enrutador. Las tablas que siempre crecen no solo consumen memoria del enrutador, sino que también necesitan más tiempo CPU para examinarlas y más ancho de banda para enviar informes de estado entre ruteadores.

En cierto momento, la red puede crecer hasta el punto en que ya no es factible que cada enrutador tenga una entrada para cada uno de los demás ruteadores, por lo que el enrutamiento tendrá que hacerse jerárquicamente, como ocurre en la red telefónica, usando OSPF este tipo de enrutamiento, proporcionando que los ruteadores se dividan en lo que se le conoce como áreas, en donde cada ruteador conoce todos los detalles de la manera de enrutar paquetes a destinos dentro de su propia región, pero no sabe nada de la estructura interna de las otras regiones.

Al interconectar diferentes redes, es natural considerar cada una como región independiente, a fin de liberar a los ruteadores de una red de la necesidad de conocer la estructura topológica de las demás.

En la figura siguiente se muestra la proyección futura de la UCI en topología malla. Donde el nodo central se conectará con los nodos nivel 1 a través de fibra óptica a 10 GbE y todos estos nodos a su vez se conectan a 2 GbE, que son los llamados enlaces redundantes.

La idea es que todos los equipos de conectividad de la red de la UCI, se conecten a su nodo principal y a su vez exista conexión entre ellos, debido a la topología malla.

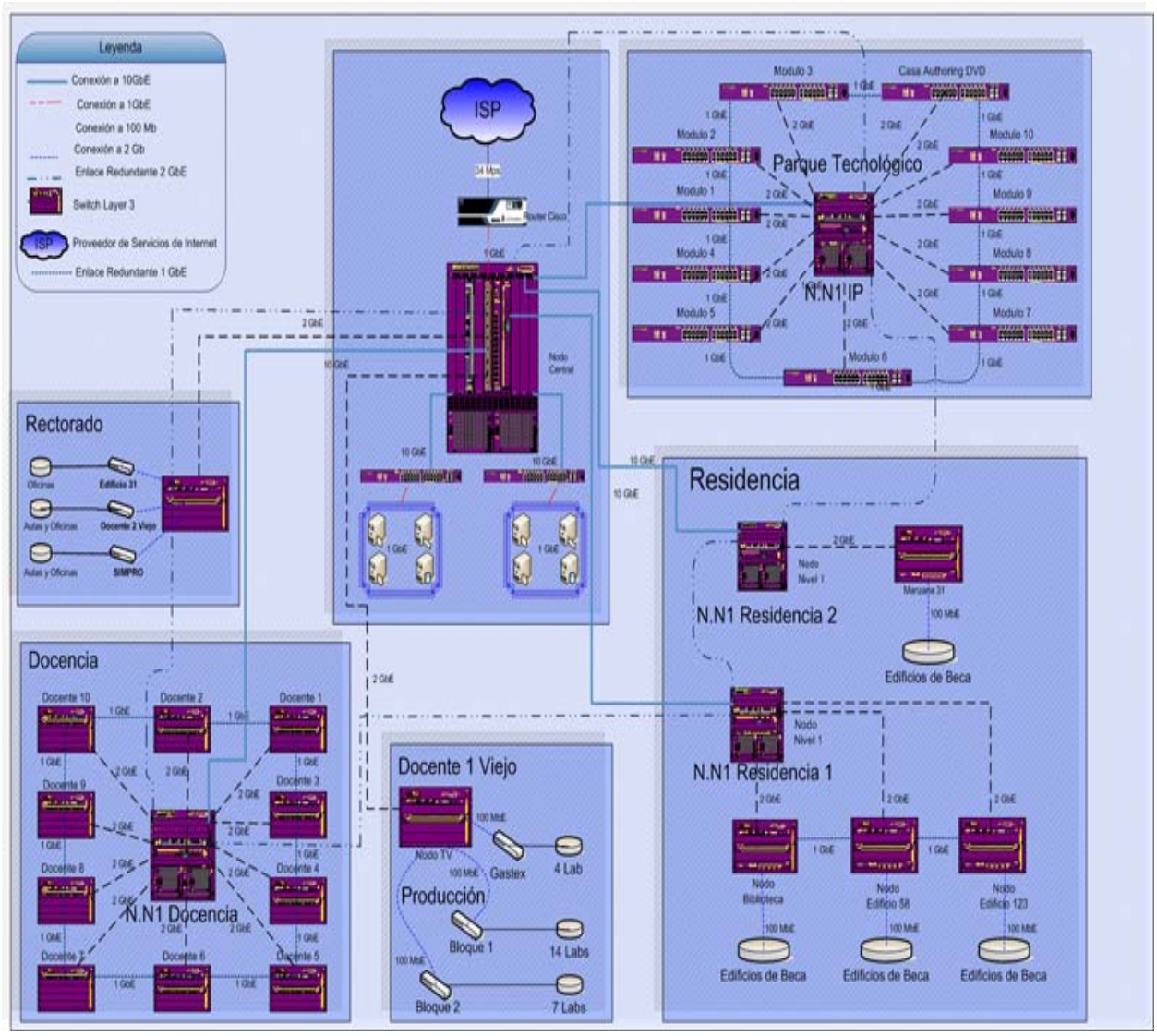


Fig.3.4 Red Futura de la UCI

3.3 El protocolo de enrutamiento OSPF para la red UCI

Después de haber analizado las proyecciones futuras y cambios topológicos en la red de la UCI, así como las características y funcionalidades del protocolo de enrutamiento OSPF, se tomarán en cuenta algunos comandos a utilizarse para la implementación del mismo.

3.3.1 Algunos comando para la configuración de OSPF en el ruteador

Para habilitar el protocolo OSPF se realiza mediante el comando **enable ospf.** Al hacer esto, se debe estimar el número máximo total de rutas externas y el número máximo total de ruteadores OSPF en la red.

Se definen los parámetros OSPF de cada uno de los interfaces del ruteador que participan en el protocolo mediante el comando **set interface**. Entre otros, se debe configurar por cada interfaz:

1. El identificador del área en la que se encuentra.
2. Los valores de los “timer” propios del protocolo (se suelen configurar los valores por defecto)
3. La prioridad del ruteador a la hora de ser elegido “ruteador designado” en una LAN.
4. Los parámetros de autenticación de intercambio de información entre ruteadores.
5. Las rutas exportadas por OSPF (estáticas, directamente conectadas, de subred, etc.)
6. El costo del enlace.

Si se quiere que el ruteador importe rutas aprendidas de otros protocolos de enrutamiento (RIP o rutas configuradas estáticamente) hay que habilitar el enrutamiento de frontera de Sistema Autónomo (SA) mediante el comando **enable AS boundary routing.**

Con el comando **create ospf area <area identifier>** se puede crear un área OSPF. El área 0.0.0.0 no necesita ser creada. Esta existe por defecto.

El comando **configure ospf add vlan [<vlan name> | all] area <area identifier> {passive}** se utiliza para asociar un VLAN (interfaz del ruteador) con un área OSPF. Por defecto, todas las interfaces del ruteador están asociadas al área 0.0.0.0.

A todos los switches configurados para soportar múltiples áreas OSPF se les puede aplicar un filtro a través de perfiles de acceso, en los que se crea una lista de ruteadores OSPF externos que están anunciando sus rutas dentro del área. Esta característica adiciona seguridad a la configuración del OSPF, pues evita los ataques por envenenamiento de rutas, esto se logra con el comando **configure ospf area external-filter**

3.3.2 Propuesta de OSPF

Teniendo en cuenta lo antes expuesto, además de las condiciones reales en la UCI y que en el futuro se quieren brindar gran variedad de servicios que requieren un tráfico óptimo y seguro en la red se considera una propuesta de implementación del protocolo OSPF para la red de la Universidad de las Ciencias Informáticas.

Se deberá diseñar el sistema autónomo, para esto es necesario subdividir la red de la UCI en áreas que puedan resumirse, tal como se muestra en la figura 3.5.

Como se puede observar, todas las áreas están físicamente conectadas, con una infraestructura formada por 3 áreas y 2 ABR.

Con las facilidades que brinda el enrutamiento inter área el cual permite mediante el área 0 que se conduzcan los datos, aprovechando así la estructura cableada y el backbone de alta velocidad implementado en la red de nuestra universidad.

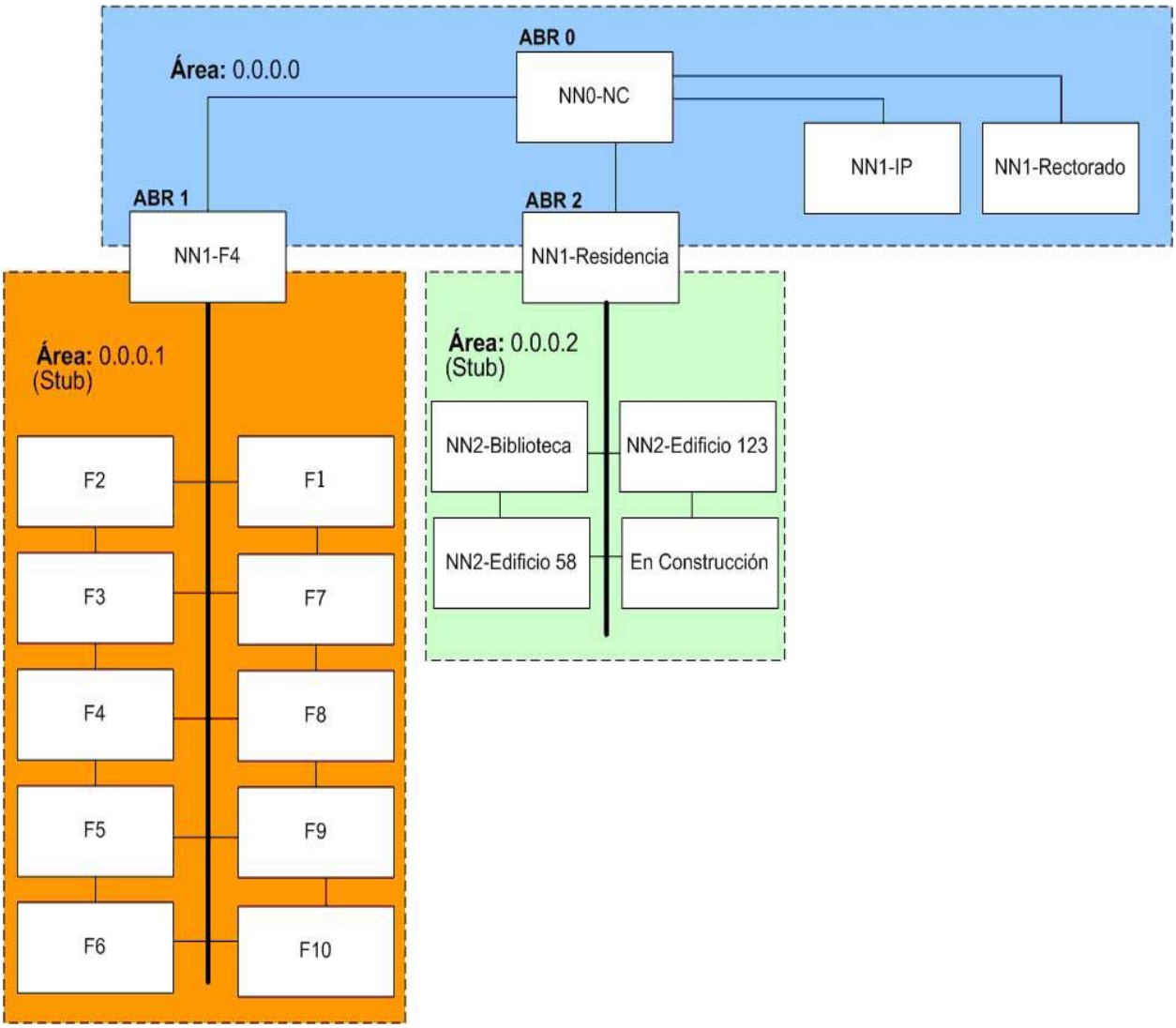


Fig. 3.5 Proyección futura de las áreas de OSPF en la UCI

Conclusiones

- Se realizó un estudio de las redes y de la forma de interconectarse entre ellas mediante los tipos de enrutamiento llegando a la conclusión de que el enrutamiento dinámico es más factible para redes grandes con la utilización protocolos de enrutamiento.

- Se hizo una comparación del protocolo RIP (utilizado actualmente) y el protocolo OSPF (que se quiere implementar), demostrando que este último es mucho más eficiente en redes LAN.

- Se analizaron las funcionalidades y característica del protocolo OSPF.

- Se examino la red de la UCI actual, problemas que tiene, servicios que brinda, mediante la cual no se podría implementar el protocolo, por lo que se analizo un proyección topológica futura.

- Se arribó a una propuesta de implementación del protocolo de enrutamiento OSPF para garantizar un mejor tráfico y menor utilización de ancho de banda.

Recomendaciones

Es necesario destacar que para el futuro deberá crearse una tercera área, que será el Parque Tecnológico (IP). Dicha área también estará conectada con el área 0, lo que mantendrá la filosofía de enrutamiento abordada en esta propuesta.

En el futuro deberá comprarse un módulo nuevo para el backbone para que la comunicación trabaje óptimamente, además por los servicios que se quieren brindar posteriormente.

Bibliografía

CISCO. Internetworking Technologies Handbook [en línea]. Disponible en World Wide Web: http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/index.htm.

CISCO. OSPF Design Guide [en línea]. Actualizado: abril, 2006. Disponible en World Wide Web: http://www.cisco.com/warp/public/104/1.html.

DIAZ ATAUCURI, Daniel. Protocolo de Enrutamiento: RIP y OSPF. En II Jornadas Técnicas: de IPv4 a IPv6. Red Académica Peruana, Lima, Perú: 30 Octubre - 02 Noviembre, 2006.

ECHEBERRIA, Raúl. Introducción a TCP/IP. Direccionamiento y ruteo. [México]: junio, 2000. Disponible en World Wide Web: www.aprendegratis.com

GOITIA, María Julieta. Protocolos de Enrutamiento Para la Capa de Red en Arquitecturas de Redes de Datos. [Corrientes, Argentina]: Dpto. Informática. Universidad Nacional del Nordeste.

GOITIA, María Julieta, LA RED MARTINEZ, David Luis. Protocolos de Enrutamiento Simulador de Tráfico de Redes. [Corrientes, Argentina]: Dpto. Informática. Universidad Nacional del Nordeste. Dpto. Informática; FACENA; UNNE; 9 de Julio.

JIMENEZ CUESTA, Juan Ignacio. Protocolo de encaminamiento OSPF. Madrid, España. Actualizado por: Carlos CAMBRIDGE, diciembre de 2000. Disponible en World Wide Web: http://www.solont.com/z-net/ospf/ospf.htm.

Microsoft Technet. OSPF. España. Actualizado: enero, 2005. Disponible en World Wide Web: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/es/library/ServerHelp/5e40738f-7c26-4b25-aa4b-35f9605c44ea.mspx?mfr=true.

MOY, John. OSPF Version 2. Abril, 1998. Disponible en World Wide Web: http://www.faqs.org/rfcs/rfc2328.html.

SPORTACK, Mark. IP Routing Fundamentals. [USA]: Marzo, 1999. [citado 20 enero de 2007] Disponible en World Wide Web: http://wwwin.cisco.com/cpress/cc/td/cpress/fund/iprf/ip2912.htm

VEGAS, Jesús. Protocolos TCP/IP. [España]: Dpto. Informática Universidad de Valladolid.

Anexos

Anexo 1.

Algoritmo de Dijkstra

- Sea G= (V, A) un grafo dirigido y etiquetado.

- Sean los vértices *a* ∈ V y *z* ∈ V; *a* es el vértice de origen y *z* el vértice de destino.

- Sea un conjunto C ⊂ V, que contiene los vértices de V cuyo camino más corto desde *a* todavía no se conoce.

- Sea un vector D, con tantas dimensiones como elementos tiene V, y que "guarda" las distancias entre *a* y cada uno de los vértices de V.

- Sea, finalmente, otro vector, P, con las mismas dimensiones que D, y que conserva la información sobre qué vértice precede a cada uno de los vértices en el camino.

- El algoritmo para determinar el camino de longitud mínima entre los vértices *a* y *z* es:

1. C ← V

2. Para todo vértice $i \in C$, $i \neq a$, se establece $D_i \leftarrow \infty$; $D_a \leftarrow 0$

3. Para todo vértice $i \in C$ se establece $P_i = a$

4. Se obtiene el vértice $s \in C$ tal que no existe otro vértice $w \in C$ tal que $D_w < D_s$

   - Si $s = z$ entonces se ha terminado el algoritmo.

5. Se elimina de C el vértice s: $C \leftarrow C - \{s\}$

6. Para cada arista $e \in A$ de longitud l, que une el vértice s con algún otro vértice $t \in C$,

   - Si $l + D_s < D_t$, entonces:
     1. Se establece $D_t \leftarrow l + D_s$
     2. Se establece $P_t \leftarrow s$

7. Se regresa al paso 4

Al terminar este algoritmo, en D_z estará guardada la distancia mínima entre a y z. Por otro lado, mediante el vector P se puede obtener el camino mínimo: en P_z estará y, el vértice que precede a z en el camino mínimo; en P_y estará el que precede a y, y así sucesivamente, hasta llegar a a.

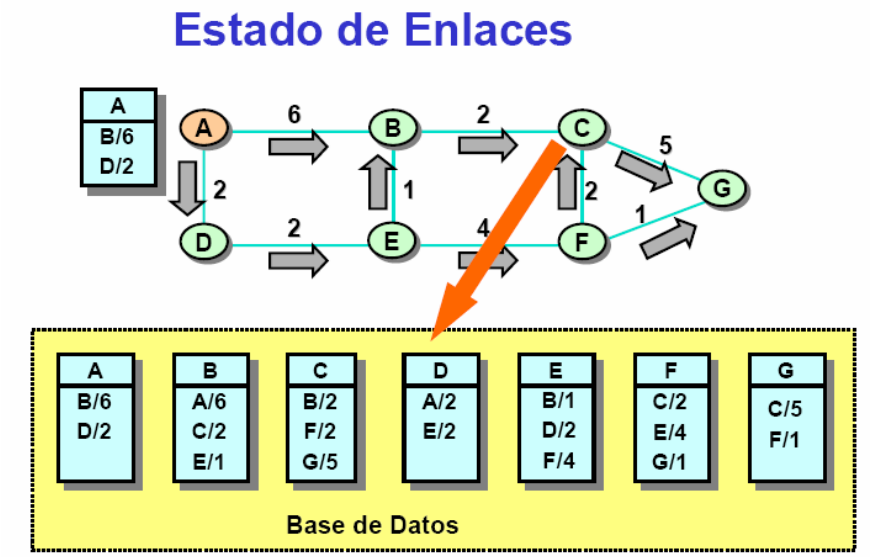
Pseudocódigo del algoritmo

- Estructura de datos auxiliar: Q = Estructura de datos Cola de prioridad

```
DIJKSTRA (Grafo G, nodo_fuente s)
    // inicializamos todos los nodos del grafo. La distancia de cada nodo es infinita
    // y los padres son NULL
    for u ∈ V[G] do
        distancia[u] = INFINITO
        padre[u] = NULL
    distancia[s] = 0
    //encolamos todos los nodos del grafo
    Encolar (cola, V[G])
    mientras cola != 0 do
       // OJO: Se extrae el nodo que tiene distancia mínima y se conserva la condición
       // de Cola de prioridad
        u = extraer_minimo(cola)
        for v ∈ adyacencia[u] do
            if distancia[v] > distancia[u] + peso(u,v) do
                distancia[v] = distancia[u] + peso(u,v)
                padre[v] = u
```

- Complejidad del algoritmo O((V+E)(log V))

Anexo 2



Anexo 2. Ejemplo de Estado de Enlaces.

Glosario de Términos

Algoritmo de Dijkstra: También llamado algoritmo de caminos mínimos, es un algoritmo para la determinación del camino más corto dado un vértice origen al resto de vértices en un grafo dirigido y con pesos en cada arista. Su nombre se refiere a Edsger Dijkstra, quien lo describió por primera vez en 1959.

Algoritmo SPF: El algoritmo de ruteo SPF (Primero la Trayectoria Más Corta) es la base de la operación del OSPF. Cuando un ruteador SPF se enciende, inicializa sus estructuras de datos para el protocolo de ruteo y posteriormente las señales de los protocolos de las capas inferiores que indican que sus interfases están funcionando correctamente.

Ancho de banda: En conexiones a Internet el ancho de banda es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (BPS), kilobits por segundo (kbps), o megabits por segundo (mps).

AppleTalk: Es un conjunto de protocolos desarrollados por Apple Inc. para la conexión de redes. Fue incluido en un Macintosh en 1984 y actualmente está en desuso en los Macintosh en favor de las redes TCP/IP.

ATM: Modo de Transferencia Asincrónico (*Asincronous Transfer Mode*). Es una tecnología de red de conmutación de celdas orientada a conexión basada en circuitos virtuales.

Broadcast: Sistema de entrega de paquetes en el que una copia de un paquete dado se envía a todos los hosts conectados a la red. Ejemplo: Ethernet.

Conmutación: La conmutación es una técnica que sirve para hacer un uso eficiente de los enlaces físicos en una red de computadoras. Si no existiese una técnica de conmutación en la comunicación entre dos nodos, se tendría que enlazar en forma de malla. Una ventaja adicional de la conmutación de paquetes, (además de la seguridad de transmisión de datos) es que como se parte en paquetes el mensaje, éste se está ensamblando de una manera más rápida en el nodo destino.

Datagrama: Es un fragmento de paquete que es enviado con la suficiente información como para que la red pueda simplemente enrutar el fragmento hacia el ordenador receptor, de

manera independiente a los fragmentos restantes. Esto puede provocar una recomposición desordenada o incompleta del paquete en el ordenador destino. La estructura de un datagrama es: cabecera y datos.

Dirección IP: Es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red o nivel 3 del modelo de referencia OSI.

Ethernet: Es el nombre de una tecnología de redes de computadoras de área local (LANs) basada en tramas de datos. Ethernet define las características de cableado y señalización de nivel físico y los formatos de trama del nivel de enlace de datos del modelo OSI. Ethernet se refiere a las redes de área local y dispositivos bajo el estándar IEEE 802.3.

FDDI (Fiber Distributed Data Interface): Es un conjunto de estándares ISO y ANSI para la transmisión de datos en redes de computadoras de área local (LAN) mediante cable de fibra óptica. Se basa en la arquitectura token ring y permite una comunicación tipo Full Duplex. Dado que puede abastecer a miles de usuarios, una LAN FDDI suele ser empleada como backbone para una red de área amplia (WAN).

Frame Relay Frame Relay: es una técnica de comunicación mediante retransmisión de tramas, introducida por la ITU-T a partir de la recomendación I.122 de 1988. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos (“frames”) para datos, perfecto para la transmisión de grandes cantidades de datos.

Full dúplex: Cualidad de los elementos que permiten la entrada y salida de datos de forma simultánea. El concepto está muy relacionado con el campo de las comunicaciones en vivo a través de la red, ya que indica que se puede oír y hablar al mismo tiempo.

Half dúplex: Significa que el método o protocolo de envío de información es bidireccional pero no simultáneo.

Host o terminal: Aparato capaz de realizar operaciones de diálogo con un servidor. También se le llama cliente. Puede ser un ordenador, un servidor de archivos, un dispositivo de almacenamiento por red, una máquina de fax, impresora, etc.

IETF: Internet Engineering Task Force, en español Grupo de Trabajo en Ingeniería de Internet, es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, tales como transporte, encaminamiento, seguridad.

IP: El Protocolo de Internet (IP, Internet Protocol) es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

IPX: Siglas de Internetwork Packet Exchange (Intercambio de paquetes inter red). Protocolo de nivel de red de Netware. Se utiliza para transferir datos entre el servidor y los programas de las estaciones de trabajo. Los datos se transmiten en datagramas. Intercambio de paquetes inter redes.

LAN: Es la abreviatura de Local Area Network (Red de Área Local o simplemente Red Local). Una red local es la interconexión de varios ordenadores y periféricos. Su extensión esta limitada físicamente a un edificio o a un entorno de unos pocos kilómetros.

Multicast (Multidifusión): Una forma especial de broadcast en la que las copias del paquete se entregan sólo a un subconjunto de todos los posibles destinos.

Nodo: Punto de intersección o unión de varios elementos que confluyen en el mismo lugar. En una red de ordenadores cada una de las máquinas es un nodo, y si la red es Internet, cada servidor constituye también un nodo.

Paquete de datos: Un paquete de datos es una unidad fundamental de transporte de información en todas las redes de computadoras modernas. El término datagrama es usado a veces como sinónimo.

Pasarela(gateway) : El término original de Internet para lo que ahora se conoce como ruteador, o más exactamente, ruteador IP. Actualmente, los términos pasarela (gateway) y pasarela de aplicación (application gateway) se refieren a sistemas que efectúan alguna traducción de un formato nativo a otro.

RFC: Petición de comentarios, es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet, que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.

Ruta: Es un par definido de direcciones: una dirección de "destino" y una dirección de "pasarela".

Ruta por defecto: Se utiliza solamente cuando no se puede aplicar ninguna de las otras rutas existentes

Ruteador: Dispositivo de hardware para interconexión de redes de las computadoras que opera en la capa tres (nivel de red) del modelo OSI.

Subred: Es un conjunto de direcciones IP y con ella se pueden hacer dos cosas: asignar direcciones IP a los equipos o dividirlo nuevamente en subredes más pequeñas. En cada división, las subredes primera y última no se usan, cabe aclarar que no se usan para asignar direcciones IP a los equipos pero si se pueden usar para dividirlas en subredes más pequeñas.

Token Ring: Arquitectura de red desarrollada por IBM en los años 70's con topología lógica en anillo y técnica de acceso de paso de testigo. Token Ring se recoge en el estándar IEEE 802.5. En desuso por la popularización de Ethernet; no obstante, determinados escenarios, tales como bancos, siguen empleándolo.

Topología: La topología o forma lógica de una red se define como la forma de tender el cable a estaciones de trabajo individuales; por muros, suelos y techos del edificio.

VLSM: El concepto básico de VLSM es muy simple: Se toma una red y se divide en subredes fijas, luego se toma una de esas subredes y se vuelve a dividir tomando bits "prestados" de la porción de hosts, ajustándose a la cantidad de hosts requeridos por cada segmento de nuestra red.

WAN: Es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, dando el servicio a un país o un continente.

X.25: Es un estándar UIT-T para redes de área amplia de conmutación de paquetes. Establece mecanismos de direccionamiento entre usuarios, negociación de características de comunicación, técnicas de recuperación de errores. Los servicios públicos de conmutación de paquetes admiten numerosos tipos de estaciones de distintos fabricantes. Por lo tanto, es de la mayor importancia definir la interfaz entre el equipo del usuario final y la red.