UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
"ARAGON"

OSPF como Protocolo de Ruteo en el backbone de RedUNAM - Propuesta.

T E S I S

QUE PARA OBTENER EL TITULO DE

INGENIERO EN COMPUTACION

P R E S E N T A N:

EDGAR FLORES CRUZ

ERIC CASTILLO CAMACHO

SAN JUAN DE ARAGON, ESTADO DE MEXICO. 2000

Agradecimientos

A mis padres Margarito y Carolina por haberme brindado su apoyo incondicional, cariño y comprensión, por éstas y muchas razones, este trabajo se los dedico con todo cariño y amor.

A mis hermanas Carolina y Martha por haberme ayudado a alcanzar esta meta, por los consejos y la ayuda que siempre me han brindado, espero que siempre sigamos juntos para compartir nuestros triunfos y nuestros fracasos.

Al Ing. Juan Gastaldi Pérez por su apoyo en la realización de este trabajo.

Al Departamento de Operación de la Red de la DGSCA de la Universidad Nacional Autónoma de México: a Gaby, Alfredo, Octavio, al NIC, TAC, Diseño, Módems, Investigación y Desarrollo y en especial al personal Centro de Operación de la Red NOC-UNAM: Hugo, Leonel, Osvaldo, Mario, Carolina, Estela, Eric.

A mis amigos de generación y de trabajo; Teck, Rene, Eric, Sarai, Raquel, Rocío, Estela gracias por brindarme su amistad.

A mi compañero de tesis Eric, gracias por brindarme tu amistad, espero que sigas adelante y te sigas superando.

Edgar

Agradecimientos

A mi Alma Mater, la Universidad Nacional Autónoma de México, en especial al Campus Aragón y a sus maestros que con su compromiso y dedicación tuve la oportunidad de estar aquí.

A la Subdirección de Redes de la DGSCA-UNAM: a Alfredo, Gaby, Octavio, al personal que está o estuvo en el TAC, NOC, NIC, Diseño, Investigación y desarrollo, modems y a todos los que omito, gracias por compartir su trabajo, ilusiones y entusiasmo.

Al Ing. Juan Gastaldi Pérez por su apoyo en la realización de este trabajo.

Eric

Con especial dedicación

Esta tesis, el trabajo, sacrificio y empeño que significa la dedico a Juan, Elena, Selene y Rebeca que a pesar de los percances en el camino, logramos este objetivo. Gracias por todo su apoyo y cariño. Los amo.

A la persona que aportó la parte cálida de este trabajo, abrió mis horizontes y por el empuje que me imprimió por ser alguien mejor cada día: Maite. Gracias por coincidir.

A Chio, Teck, Rene, Ra, Sarai, Edgar, Estela, a ustedes que saben el significado de este trabajo, gracias mil por su amistad, apoyo y por seguir en mi camino.

Con especial dedicación a mi compañero y amigo Edgar Flores por el esfuerzo, trabajo e insistencia durante este trabajo y toda la carrera; a su familia. Gracias.

Gracias a Edgar Deloera, por todo lo que hemos aprendido juntos con ésta amistad tan añeja.

Eric

ÍNDICE

INTRODUCCIÓN

I. Conceptos básicos 2
I.1. Redes de datos 2
I.1.1. OSI 2
I.1.2. Redes LAN 4
I.1.2.1. Ethernet 4
I.1.2.2. Fast Ethernet 5
I.1.3. ATM 7
I.1.3.1. LANE 10
I.2. TCP/IP 12
I.2.1. Direccionamiento IP 13
I.2.1.1. VLSM 16
I.2.1.2. CIDR 17
I.3. Enrutamiento 19
I.3.1. Características de diseño 20
I.3.2. Clasificación 21
I.3.2.1. Dinámico / Estático 21
I.3.2.2. Single-path / Multi-path 21
I.3.2.3. Plano / Jerárquico 22
I.3.2.4. Algoritmos Interdominio / Intradominio 22
I.3.2.5. Distance Vector / Link State 22
I.3.3. RIP 22
I.3.4. IGRP 25
I.4. Conceptos básicos de diseño de redes de datos 27
I.4.1. Análisis de requerimientos. 28
I.4.2. Desarrollo de la topología de la red. 28
I.4.3. Direccionamiento 29
I.4.4. Provisionamiento de hardware. 29
I.4.5. Implantación, monitoreo y administración de la red. 29

II. Descripción de la estructura actual de RedUNAM 35
II.1. Historia de RedUNAM 35
II.2. Descripción general de RedUNAM 36
II.3. Nivel de transporte 36
II.4. Nivel de enrutamiento 43
II.4.1. Enrutamiento estático 50
II.4.2. Enrutamiento dinámico 52
II.5. Desventajas de la estructura de enrutamiento actual 55

III. OSPF 58
III.1. Historia de OSPF 58
III.2. Descripción preliminar de OSPF 58
III.3. Base de datos topológica o Link-State 59
III.3.1. Shortest Path Tree o árbol de la ruta más corta 64

III.4. Enrutamiento jerárquico 64
III.4.1. Áreas en OSPF 64
III.4.1.1. Área backbone o área cero 65
III.4.1.2. Áreas stub 65
III.4.1.3. Clasificación de enrutadores 66
III.5. Adyacencias 66
III.5.1. Elección del DR y BDR. 67
III.5.2. DR y BDR. 67
III.5.3. Construcción de la adyacencia. 68
III.6. Formato de los paquetes de OSPF y LSA´s 69
III.6.1. Encapsulación de paquetes de OSPF en IP 70
III.6.2. El campo de opciones 71
III.6.3. Formato de los paquetes de OSPF 72
III.6.3.1. OSPF Header 72
III.6.3.2. HELLO Packet 73
III.6.3.3. Database Description Packet 74
III.6.3.4. Link State Request Packet 75
III.6.3.5. Link State Update Packet 76
III.6.3.6. Link State Acknowledgment Packet 76
III.6.4. Formato de los LSA´s 77
III.6.4.1. LSA Header 77
III.6.4.2. Router Links Advertisements 79
III.6.4.3. Network Links Advertisements 80
III.6.4.4. Summary Link Advertisements 81
III.6.4.5. AS External Link Advertisements 82
III.7. Administración 83
III.8. Interacción con otros protocolos 85
III.9. Seguridad y autenticación en OSPF 85
III.10. Ventajas y desventajas de OSPF con respecto a otros protocolos de enrutamiento 85

IV. Propuesta de OSPF en RedUNAM 90
IV.1. Requerimientos 90
IV.2. Direccionamiento IP 92
IV.2.1. Direccionamiento en el backbone 93
IV.2.2. Direccionamiento en enlaces WAN numerados 94
IV.2.3. Direccionamiento en dependencias internas y externas 95
IV.3. Topología de red 100
IV.3.1. Asignación de áreas de OSPF en RedUNAM 101
IV.3.1.1. Área 0.0.0.0 o de backbone. 101
IV.3.1.2. Áreas 1.1.1.1 y 2.2.2.2 102
IV.4. Provisionamiento de hardware y software. 106
IV.5. Implantación, monitoreo y administración de OSPF. 107

CONCLUSIONES 110

Apéndice 1. Formato de paquetes 111

Apéndice 2. Propuesta de direccionamiento IP 114

GLOSARIO DE TÉRMINOS 118

BIBLIOGRAFÍA 122

OTRAS REFERENCIAS 123

INTRODUCCIÓN

En la actualidad el desarrollo de las tecnologías de información y telecomunicaciones en el ámbito mundial conlleva en gran medida la utilización de las redes de computadoras en un sin fin de actividades. De esta manera se pueden compartir recursos de software y hardware, y realizar tareas en forma distribuida para la solución de problemas. El ejemplo mas claro se observa en el desarrollo de Internet; millones de personas la utilizan en la educación, comercio electrónico y recreación. Aplicaciones como correo electrónico, páginas web, voz sobre IP, chats, foros de discusión y videoconferencia sobre IP son servicios cada vez más comunes en nuestros días, a tal grado que la red Internet juega un rol estratégico que afecta la forma en como aprendemos, trabajamos, vivimos, pensamos y nos divertimos.

Sin embargo poco se conoce de su funcionamiento y de las políticas que la rigen. Internet es más que un montón de cables y equipos de cómputo; debemos también considerar a los componentes lógicos que la conforman: los protocolos.

Internet, la red de redes, permite a las diversas redes que la conforman comunicarse entre sí e intercambiar información a través de la técnica de conmutación de paquetes. Conforme la información es empaquetada y se dirige de un origen a un destino, la decisión de por cual ruta deben encaminarse la llevan a cabo las computadoras de aplicación específica llamadas enrutadores (routers en inglés). El mecanismo que siguen los enrutadores para intercambiar información de rutas y así tomar la decisión correcta de por donde enviar cada uno de los paquetes es conocido como "protocolo de enrutamiento". Protocolos como RIP, IGRP, IS-IS, BGP y OSPF son los protocolos más comunes para el enrutamiento en redes TCP/IP, y por tanto, de Internet. Esta tesis versa sobre el análisis de la viabilidad de la implantación del protocolo de enrutamiento OSPF dentro de la red educativa más grande de México y América Latina, RedUNAM.

Por lo anterior, el presente trabajo "OSPF como protocolo de ruteo en el backbone de RedUNAM-Propuesta" se encuentra estructurado de la siguiente forma:

Durante el capítulo I se tomaran en cuenta los conceptos básicos de redes de datos para estar en la posibilidad de analizar la estructura de RedUNAM, además, se incluyen consideraciones y objetivos en el diseño de redes con la finalidad de proveer una metodología en la que se apoyará este trabajo de tesis.

En el transcurso del capítulo II se analiza la estructura, funcionamiento, ventajas y desventajas del enrutamiento actual en el backbone de RedUNAM, por esto se hace necesario describir como se encuentra estructurado a nivel de transporte y enrutamiento. Esta descripción dará la pauta para comprender las desventajas en el enrutamiento actual y con ello, presentar la propuesta que aporte soluciones a ellas.

El capítulo III describe las características, funcionalidad y forma de trabajar del protocolo de enrutamiento OSPF con miras a comprender todo su potencial y propòner un esquema de enrutamiento con todos los beneficios que ofrece. Así mismo se incluye al final un comparativo donde se aprecian las ventajas de OSPF sobre los protocolos en uso en RedUNAM.

A lo largo del capítulo IV se lleva a cabo la propuesta tomando como base los conceptos vistos durante los capítulos anteriores. En especial se toman en cuenta los pasos del diseño de redes de datos dividiendo la propuesta en cinco partes fundamentales: a) requerimientos necesarios; b) direccionamiento IP necesario para aprovechar el protocolo; c) la topología de la red con la asignación de áreas; d) los componentes de hardware y software necesarios; e) la implantación, monitoreo y administración de la red OSPF.

Finalmente, debido a la basta terminología utilizada en el ámbito de las telecomunicaciones, se anexa un glosario de términos, así como también un índice de referencias por si se desea profundizar en los temas vistos durante éste trabajo.

Capítulo I

Conceptos Básicos

I. Conceptos Básicos

Para comprender el tema desarrollado en esta tesis, se considera necesario exponer algunos temas importantes relacionados con redes de datos, ATM, TCP/IP y enrutamiento. Estos serán vistos en el transcurso de este capítulo y se describen de manera escueta debido a que son sólo un repaso necesario para poder comprender el objetivo de esta tesis; profundizar en el estudio del funcionamiento del protocolo de enrutamiento OSPF analizado en el capítulo III.

1.1 Redes de datos

El más importante de los conceptos es el de red de datos. Red de datos es un grupo de equipos interconectados entre sí a través de un medio físico (sea cable, fibra óptica, o el aire inclusive) con la finalidad de compartir recursos e información. La popularidad e importancia que han tomado a últimas fechas radica en que son consideradas como herramientas necesarias de competitividad y auxiliares en la toma de decisiones. Sin embrago, para poder hacer posible la comunicación de equipos con diferentes arquitecturas y marcas, es necesario fijar ciertas reglas o protocolos. Con esto surgen diferentes modelos (TCP/IP, Novel Netware, Apple Talk, etc.), pero para entenderlos se analizará el modelo que sirve como referencia en el análisis y diseño de redes de computadoras y el que ha llegado a considerarse el más importante y relevante en la actualidad: el modelo de referencia OSI.

1.1.1 Modelo de referencia OSI

En el año de 1984 la Organización Internacional para la Estandarización (ISO por sus siglas en inglés), creó el modelo de referencia OSI (Open System Interconnection – Interconexión de Sistemas Abiertos). El modelo de referencia OSI rápidamente se convirtió en un modelo de arquitectura primaria para las comunicaciones.

Este modelo de referencia describe las tareas que los "sistemas abiertos" deben realizar en términos de siete capas y especifica la funcionalidad de cada una. Las dos primeras (física y enlace de datos) están implementadas generalmente con hardware y software —conocidas también como capas bajas — las otras cinco son generalmente implementadas en software. OSI no especifica como deben ser implantadas, debido a que sólo es un modelo de referencia y no una aplicación práctica.

Cabe mencionar que cada capa en el equipo origen, se comunica con su capa adyacente en el equipo destino. Para ello cada capa inserta cierta información, que sólo la va poder interpretar la capa del mismo nivel en la máquina destino.

El modelo OSI tiene la siguiente estructura:

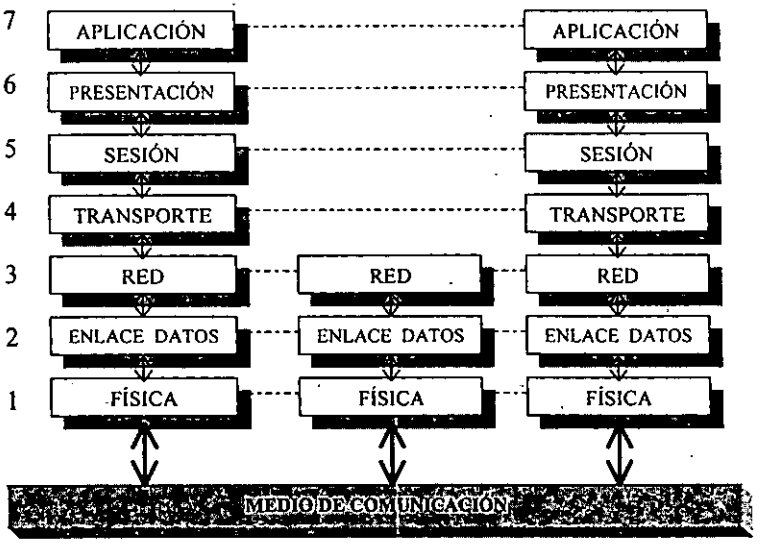


Figura 1.1 Modelo de referencia OSI.

La funcionalidad que presta cada una de las siete capas del modelo OSI se describen a continuación:

- *Aplicación (7):* Interfaz final con el usuario. Tiene la habilidad de sincronizarse con las aplicaciones remotas, establecer acuerdos de procedimiento de recuperación de errores y del control de integridad de datos. Se encuentra definida en los protocolos de aplicación.
- *Presentación (6)*: Se asegura que la información que es enviada por la capa de aplicación de un sistema, pueda ser leída por la capa de aplicación de otro ya que maneja diferentes códigos de presentación estándar (ASCII, Unicode, EBCDIC, Entero complemento a uno y complemento a dos, etc.).
- *Sesión (5):* Encargada de iniciar, mantener y terminar un diálogo entre computadoras. Esta capa sincroniza la conversación entre la capa de presentación y administra el intercambio de datos.
- *Transporte (4):* Esta capa provee de mecanismos para la detección y corrección de errores, e información de control de flujo, con la finalidad de asegurar que la transmisión de punto a punto se lleve a cabo en forma correcta.
- *Red (3):* Encargada de la selección de la mejor ruta entre dos o más sistemas en segmentos lógicos diferentes.
- *Enlace de Datos (2):* Provee de un tránsito confiable de datos a través del medio físico. Esto se logra gracias a que esta capa trabaja con la dirección MAC, topología de la red, notificación de errores, control de flujo, etc.
- *Física (1):* Explica los mecanismos para enviar y recibir los datos (cadenas de ceros y unos lógicos) a través del medio físico. En ésta capa se ve todo lo referente a las interfaces físicas, conectores, tipo de cableado, códigos de línea, etc.

1.1.2 Redes LAN

Existen diferentes tecnologías de redes de área local (redes LAN). De los diferentes estándares de redes: Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, 100VG-AnyLAN, FDDI, CDDI, etc., todos ellos abarcan las dos primeras capas del modelo de referencia OSI. Aunque nos ofrecen funcionalidades semejantes en la capa de enlace de datos (cada estándar lo hacen de una forma distinta), son muy diferentes en la capa física. A continuación se describen las características más importantes de las tecnologías de redes LAN que están en uso actualmente dentro de RedUNAM: Ethernet y Fast Ethernet.

1.1.2.1 Ethernet

Ethernet es el nombre de la tecnología de red de área local más popular hoy en día. Inventada por Xerox Corporation's PARC (Palo Alto Research Center) a principios de los 70's sirvió como base en las especificaciones del estándar IEEE 802.3. La diferencia entre la tecnología Ethernet de los años 70´s y el estándar IEEE 802.3 usado hoy en día, inclusive dentro de la UNAM, radica en el formato de la trama, por lo demás se pueden considerar iguales. Cuando se hable de la tecnología Ethernet, se debe tomar en cuenta que se refiere al estándar IEEE 802.3.

La funcionalidad principal de esta tecnología es permitir comunicar diferentes equipos de cómputo no dispersos geográficamente (por ser una red LAN) a través de un medio físico eléctrico conocido como bus, a una velocidad máxima de 10 Mbps en tipo Half-Duplex y en Full-Duplex usando el método de acceso al medio CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

Las primeras redes Ethernet que se utilizaron se implantaron de acuerdo a las características de los estándares 10Base5 y 10Base2, sin embargo, debido a los problemas que presentan se crearon nuevos estándares 10BaseT y 10BaseFl que son los más usados en la actualidad.

La IEEE asigna a cada estándar un identificador, cada uno de ellos está formado por tres partes. La primera, "10" se refiere a la velocidad del medio, es decir que va a transmitir a 10 Mbps. La segunda parte, "Base" se refiere al tipo de señalización: banda base. Este tipo de señalización se refiere a que solamente existe en el medio una sola portadora. Y la última parte se refiere al tipo de cableado a utilizar.

En la siguiente tabla se presenta las características físicas de los estándares mencionados anteriormente.

ESTANDAR	CABLEADO	LONGITUD MÁXIMA DE SEGMENTO	NODOS / SEGMENTO	CARACTERISTICAS	NUMERO MÁXIMO REPETIDORES	TOPOLOGIA FÍSICA
10Base5	Coaxial Grueso	500 m	100	Uso en Backbone	4	Bus
10Base2	Coaxial Delgado	185 m	30	El más barato	4	Bus
10Base-T	Par Trenzado	100 m	1024	Fácil mantenimiento	4	Estrella
10Base-FL	Fibra Óptica	2000 m	1024	Conexión de campus	4	Punto a Punto

En la capa de Enlace de Datos, los estándares anteriores comparten el mismo método de acceso al medio, conocido como CSMA/CD que se describe a continuación.

CSMA/CD: Cuando una máquina quiere transmitir, censa el estado del bus para determinar si se está transmitiendo información, es decir, si está ocupado el medio. Si detecta al medio libre, la máquina comienza a transmitir; en caso contrario esperará a que éste se libere. Cuando se empieza a transmitir la información en el medio, la señal no llega a cada punto de la red simultáneamente, por lo anterior, es posible que dos máquinas determinen que el medio no está siendo ocupado y comiencen a transmitir al mismo tiempo, provocando que exista una colisión. Una colisión, por lo tanto, es un error consistente en un voltaje mayor al permitido en el medio, es por eso que las máquinas cancelan la transmisión y espera un tiempo aleatorio hasta que la actividad en el medio se normalice antes de volver a intentar transmitir.

Cuando la misma máquina quiere intentar transmitir y vuelve a sufrir una colisión, entonces, existe una política de retención exponencial, que nos indica que el emisor espera un tiempo aleatorio 2 veces más largo que el primer tiempo aleatorio. En caso de que se vuelva a presentar este caso el tiempo de espera será 4 veces más grande, así reducirá al máximo la probabilidad de colisión. A este algoritmo se le conoce con el nombre de Binary Exponential Backoff o disminución exponencial binaria.

1.1.2.1 Fast Ethernet

En la actualidad dentro de la UNAM, como fuera de ella, los usuarios de la red corren aplicaciones que requieren mayores velocidades en redes LAN para tener un desempeño aceptable. Debido a esta necesidad, en julio de 1993 un grupo de compañías de redes (Intel, 3Com, LAN Media, SynOptics, Cabletron, National Semiconductor, SMC, Grand Junction y Sun Microsystems) se juntó para formar la alianza de Fast Ethernet. Este grupo genera las características principales de la especificación 802.3u de la IEEE, y aceleró la aceptación de dicha especificación en el mercado.

Fast Ethernet comparado con las especificaciones de Ethernet a 10 Mbps incrementa su velocidad 10 veces, es decir, los paquetes que son transmitidos en el medio son 10 veces más rápido.

Un aspecto importante que debemos mencionar, es que Fast Ethernet tiene el mismo formato de trama, la misma manera de transportar tramas, soporta esquemas semejantes de cableado del Ethernet tradicional y el mismo mecanismo de control de acceso al medio que Ethernet (CSMA/CD), por lo que su funcionamiento es el mismo. Todo lo anterior se debe a que Fast Ethernet tiene como principal objetivo mantener la compatibilidad con Ethernet, permitir la interacción de ambas tecnologías sin necesidad de cambios totales, además de proveer la posibilidad de una migración paulatina hacia 100 Mbps.

Las especificaciones de Fast Ethernet incluyen mecanismos de auto negociación de velocidad del medio, esto hace posible proveer una velocidad dual, además de tener compatibilidad con equipos Ethernet y poder trabajar a velocidades ya sea a 10 o 100 Mbps automáticamente.

Existen actualmente tres estándares para poder transmitir señales a 100 Mbps: 100BaseT4, 100BaseTx, 100BaseFx. Aquí cabe mencionar la tercera parte del identificador que nos indica el tipo de medio a utilizar. El tipo "T4", es par trenzado (Twisted-Pair) con cuatro pares de cable telefónico categoría 3, 4 y 5[1]; el tipo "TX" utiliza dos pares de cable trenzados sin malla (UTP) categoría 5 o con malla (STP) tipo 1; el medio "FX" es fibra óptica con dos hebras de fibra multimodo de 62.5/125 μm.

Los cambios en el medio generaron especificaciones diferentes en las distancias soportadas por segmento dependiendo del tipo de estándar que se use. Así, tanto 100BaseT4 como 100BaseTx soportan como segmento máximo 100 m en Half o Full Duplex; 100BaseFx soporta como longitud máxima 412 m por segmento en Half Duplex o 2000 m en Full Duplex. También se vio afectado el número máximo de repetidores, mientras en Ethernet era de cuatro, en Fast Ethernet se redujo a sólo dos para todos los estándares (a excepción de 100Base Fx que es para conexiones de punto a punto).

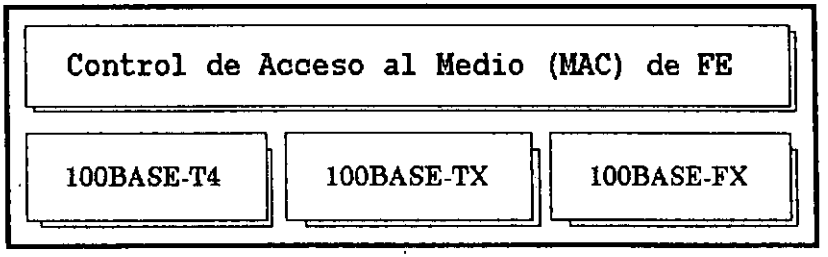


Figura 1.2 Estándares de Fast Ethernet

Los estándares de Fast Ethernet requieren forzosamente una configuración física de estrella utilizando un concentrador o switch central. El concentrador emulará el bus del Ethernet tradicional.

[1] La categoría en un cable par trenzado se refiere a la calidad de éste. Esta está dada por el número de cruces de los cables en un metro lineal. La categoría de un cable UTP va de la 3 a la 5.

1.1.3 ATM

Las exigencias de las redes de comunicaciones modernas:

- Mayor soporte a múltiples tipos de tráfico (voz, datos y vídeo).
- Seguridad y flexibilidad en los enlaces.
- Accesibilidad segura a la capacidad de las redes para equipos existentes y futuros.
- Escalabilidad del ancho de banda de la red en función de los servicios transportados.
- Garantía a la calidad del servicio, etc.

No son soportadas por las redes convencionales. Una evolución de éstas a fin de cumplir todos los objetivos ha originado una nueva tecnología: ATM (Asyncronous Transfer Mode, Modo de Transferencia Asíncrona). ATM parece ser la mejor respuesta a la tan esperada *B-ISDN*, la cual tiene la intención de ofrecer servicios digitales de radiodifusión, telefonía, comercio electrónico (a través de Internet), videoconferencia todos estos integrados sobre una red pública. Este tipo de aplicaciones requiere de tasas de transmisión de Megabits y Gigabits por segundo, diferentes tipos de información bajo un mismo medio, aplicabilidad en *LAN* y *WAN*, etc. Aquí es donde ATM parece ser la mejor respuesta a este tipo de necesidades, además es recomendada por los más importantes organismos de la industria de las telecomunicaciones, tal es el caso de la ITU-T (antes CCITT).

Se puede definir a ATM como una tecnología de conmutación de celdas (paquetes de longitud fija) de alta velocidad, orientada a conexión la cual no sufre de los problemas de retardo como ocurre en las transmisiones basadas en paquetes y medios compartidos; provee ancho de banda dedicado para la conexión, haciéndola ideal para aquellas aplicaciones a retardos en tiempo como voz y vídeo; mantiene la compatibilidad con las redes de datos actuales; garantiza un ancho de banda flexible cuando y donde sea necesario; además es una tecnología de comunicaciones capaz de integrar en ambiente local, campus y de área amplia los diferentes servicios.
El protocolo que define a ATM abarca las capas física y de enlace de datos del modelo de referencia OSI como se observa en la figura 1.3.

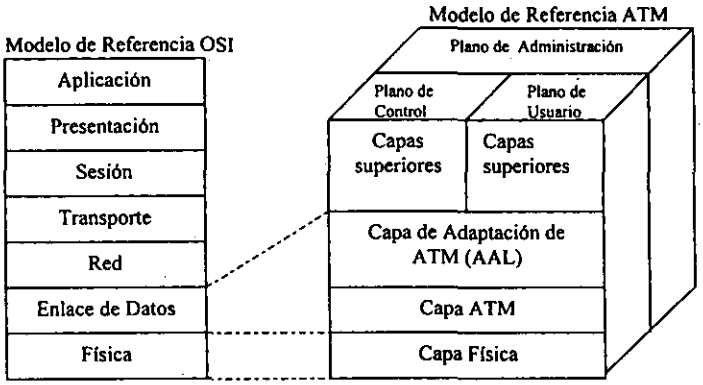


Figura 1.3 ATM vs OSI

A continuación se describe a mayor detalle la estructura de ATM, para lo cual se muestra el modelo de capas que lo define:

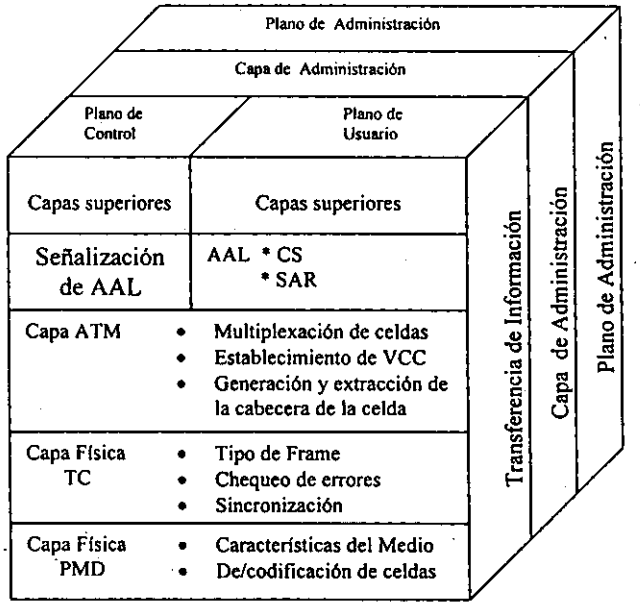


Figura 1.4 Modelo de referencia ATM

Como se puede apreciar, el modelo de ATM es un modelo tridimensional que cubre tres planos:

- *Plano de Usuario:* Provee transferencia de información de usuarios a usuarios y el control que requiere.
- *Plano de Control:* Provee las funciones de establecimiento y control de conexiones.
- *Plano de Administración:* Provee la administración de los tres planos.

Las diferentes capas del modelo de ATM son:

Capa física de ATM

La función de esta capa es similar a la función de las redes tradicionales; además se encarga de controlar el flujo de bits, chequeo de errores, etc. A su vez está dividida en dos subcapas:

- PMD (Physical Medium Dependent): Define las características del medio físico, las interfaces, la codificación y decodificación de las celdas.

- TC (Transmission Convergence): Especifica el tipo de frame a utilizar (SONET, DS-3, SDH), chequeo de errores, extracción de información del medio, inserción de celdas vacías para sincronización, intercambio de información de operación y mantenimiento.

Capa ATM

La capa ATM es responsable de la multiplexación de celdas y establece canales punto a punto multiplexados conocidos como VCC (Virtual Channel Connections). Un VCC está compuesto por un conjunto de saltos entre switches, cada salto está compuesto por un Identificador de Ruta Virtual (VPI) y un Identificador de Canal Virtual (VCI) como se muestra en la figura 1.5:

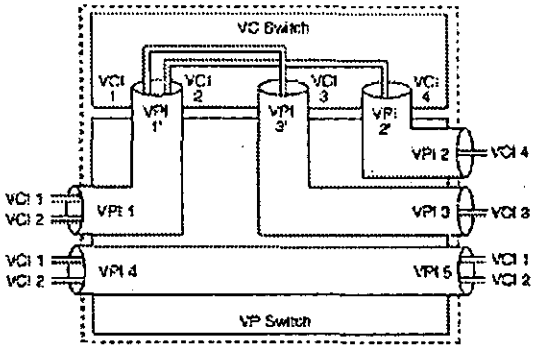
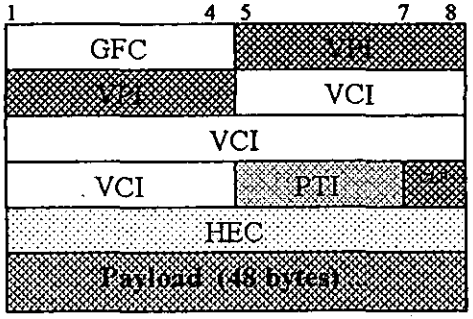


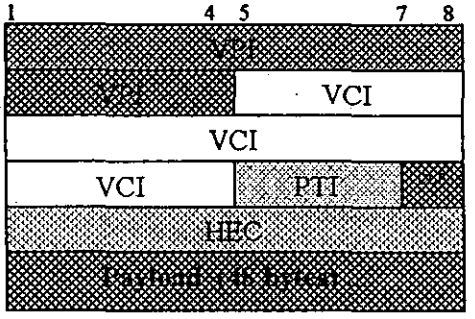
Figura 1.5 VCC =VPI/VCI

Esta capa también define al paquete de información de ATM, conocido como celda ATM. Una celda es un paquete de información de tamaño fijo, con 48 bytes de payload y 5 más de cabecera para un tamaño total de 53 bytes. El campo de payload transmite información de usuario o de control y la cabecera permite establecer las conexiones de punto a punto, control de congestión, administración de tráfico, además del chequeo de errores.

Existen 2 tipos de celdas definidas: la celda que es usada en conexiones de equipos ATM a equipos terminales, tipo UNI (User Network Interface), y las usadas entre equipos ATM, tipo NNI (Network to Network Interface). Existe una pequeña diferencia en la cabecera entre ambos tipos, la celda del tipo UNI contiene el campo de GFC, los demás campos son los mismos.



Celda de ATM tipo UNI



Celda de ATM tipo NNI

Generic Flow Control (GFC). Tiene sólo significado para funciones locales.
VPI: Virtual Path Identifier / VCI: Virtual Channel Identifier. Asocia a la celda con una conexión.
Payload Type Identifier (PTI). Indica si la celda contiene información de usuario o información de administración de conexión.
Cell Lost Priority (CLP). Indica si la celda puede ser descartada (CLP = 1) o no (CLP = 0).
Header Error Control (HEC). Usada por la capa física de ATM para chequeo, corrección de errores en la cabecera de la celda.
Payload. Información a transmitir

El tamaño fijo de la celda ofrece diferentes ventajas:

- Son menos complejas y de fácil manejo, lo que permite que sean procesadas por hardware a mayor velocidad.
- Permiten el envío de información en paralelo, lo que mejora notablemente su velocidad en comparación con la arquitectura tipo broadcast (Ethernet, Token Ring, FDDI, etc.).
- Mejor manejo de retardos, lo que permite establecer control de tráfico y colas para un mejor manejo de congestión.

Capa de adaptación de ATM (ATM Adaptation Layer)

Esta capa es clave para el transporte de múltiples tipos de tráfico (voz, vídeo y datos) sobre ATM a través de dos subcapas:

- Segmentation And Reassembly (SAR); segmentación y re-ensamble.
- Convergence Sublayer (CS); subcapa de convergencia.

La subcapa SAR segmenta la información de las capas superiores —de longitud variable— para que puedan ser transmitidas en celdas de tamaño fijo (payload de 48 bytes), y a la inversa. La subcapa CS realiza las funciones para adaptar los servicios de ATM a aquellos que son requeridos por las capas más altas, por lo tanto depende del tipo de tráfico dependientes del servicio (voz, datos o vídeo).

Debido a que ATM transporta diferentes tipos de tráfico, se definen 5 tipos de AAL:

AAL1: Usado para aplicaciones de tipo voz, vídeo digital.
AAL2: Usado para aplicaciones de voz y vídeo comprimidos.
AAL3/4: Inicialmente pensado para transporte de datos, sin embargo, actualmente tiene poco uso.
AAL5: Usado actualmente para aplicaciones de datos.

1.1.3.1 LAN Emulation

Para mantener la compatibilidad con los protocolos y LAN tradicionales, o "legadas", el ATM Forum decidió emular las redes LAN a nivel MAC (Medium Access Control, parte de la capa 2 de la torre de protocolos OSI) para minimizar los cambios necesarios para la migración y

coexistencia con la tecnología ATM. Por su difusión se decidió entonces que fueran las redes Ethernet 802.3 y Token Ring 802.5 las LAN a emular.

LAN Emulation o la Emulación de redes LAN adoptó una solución de arquitectura cliente/servidor. La emulación de LAN ha sido definida por el ATM Forum[2], en el documento LAN Emulation over ATM.

LAN Emulation es el método para permitir a los dispositivos de redes locales comunicarse sobre ATM sin realizar cambios en protocolos de capaz superiores y software de aplicación. Ya que LANE es implementado en dispositivos terminales, es completamente transparente para la red ATM y para los dispositivos de redes locales, ya que se encarga de mapear las direcciones MAC de redes LAN a direcciones ATM.

LAN Emuladas

Se define este concepto como un grupo de dispositivos unidos por ATM que lógicamente es análogo a un grupo de estaciones de LAN unidas a segmentos Ethernet o Token Ring, es decir, una LAN virtual (VLAN) a través de ATM.

Componentes de LANE

Cada red emulada está compuesta de:

- Un Cliente de LAN Emulation (LEC)
- Un Servicio de LAN Emulation por cada ELAN compuesto por:
  - Un Servidor de LAN Emulation (LES)
  - Un Broadcast and Unknown Server (BUS).
  - Además existe un único Servidor de Configuración de LAN Emulation (LECS) que sirve para todas las Redes Emuladas (ELANs).

LAN Emulation Client (LEC)

Reside en el nodo final desde la perspectiva de la red ATM o en los convertidores de ATM a LAN. Desempeña el reenvío, resolución de direcciones y otras funciones de control. En el se encuentra el software de LANE.

LAN Emulation Service

LECS

Provee información de configuración acerca de redes ATM y LAN. También provee la dirección de LES a los clientes.

LES

Sólo hay uno por LANE y es responsable de registrar y resolver direcciones MAC a ATM.

BUS

Es responsable del manejo de broadcast, multicast y frames unicast iniciales de LECs.

[2] Para mayor información referirse a http://www.atmforum.com

Forma de operar de LANE

- El equipo que provee los servicios de LANE recibe una trama de un equipo de orilla tipo Ethernet. Este equipo origen tiene como destino otro equipo de orilla Ethernet que se encuentra en otro extremo del backbone de ATM. El LEC envía una petición de resolución de dirección de MAC a dirección ATM al LES.
- El LES envía la respuesta de dirección de MAC a ATM a todos los demás LECs.
- El LEC origen reconoce la respuesta, aprende la dirección ATM del destino y establece un circuito virtual switcheado (SVC) para transportar la información en celdas ATM a través de la capa de adaptación AAL5.

A grandes rasgos éste es el funcionamiento para todas las redes Ethernet que trabajan a través de LANE en RedUNAM.

1.2 TCP/IP

Ahora toca mencionar las características más importantes de la familia de protocolos TCP/IP[3]. Es de suma importancia mencionar a TCP/IP debido a la estrecha relación que tienen con el encaminamiento de paquetes que se lleva a cabo en redes de tecnología internet (como es el caso de RedUNAM).

TCP/IP es una familia de protocolos de comunicaciones de datos. Obtiene su nombre de los dos protocolos más importantes Transfer Control Protocol e Internet Protocol. TCP/IP fue adoptado en los 80's como estándar para la red militar ARPANET, antecesora de la muy conocida Internet.

Gracias a la necesidad de establecer una comunicación global entre equipos no importando arquitectura, marcas, etc. fue necesaria la creación de reglas conocidas como protocolos. Muchos protocolos se desarrollaron, sin embargo, el único protocolo que ha hecho esto posible, y bajo el cual está funcionando la red internacional Internet, es TCP/IP.

Algunas de las principales características que hicieron posible que TCP/IP se convirtiera en el estándar de facto para la red de alcance mundial Internet son:

- Es ideal para comunicar diferentes tipos de hardware y software, ya sea a través de Internet o en aplicaciones locales.
- Es independiente del nivel físico. TCP/IP integra diferentes tipos de redes como Ethernet, Token Ring, X-25, etc.

[3] La familia de TCP/IP está compuesta por diferentes protocolos encargados cada uno de una tarea específica. Entre ellos destacan Internet Protocol (IP), Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), User Datagram Protocol (UDP), Transport Control Protocol (TCP), Telnet, Simple Mail Transfer Protocol (SMTP).

- Provee de un esquema de direccionamiento común capaz de identificar y establecer comunicación con cualquier otro dispositivo en la red, inclusive si es una red de nivel mundial.
- Estandariza los protocolos de alto nivel para proveer una interfaz que soporte cualquier tipo de aplicación de usuario.

A diferencia de OSI, que es sólo un modelo de referencia, TCP/IP es una aplicación de cuatro capas donde cada capa, al igual que OSI, realiza funciones especificas. La capa más importante, siguiendo el objetivo de ésta tesis, es la capa de Internet. Esta capa se encarga principalmente de manejar el movimiento de paquetes a través de la red. El enrutamiento de paquetes toma lugar aquí con la interacción de protocolos como IP, ICMP, IGMP y de enrutamiento: RIP, OSPF, IGRP, etc., como se ilustra en la figura 1.6.

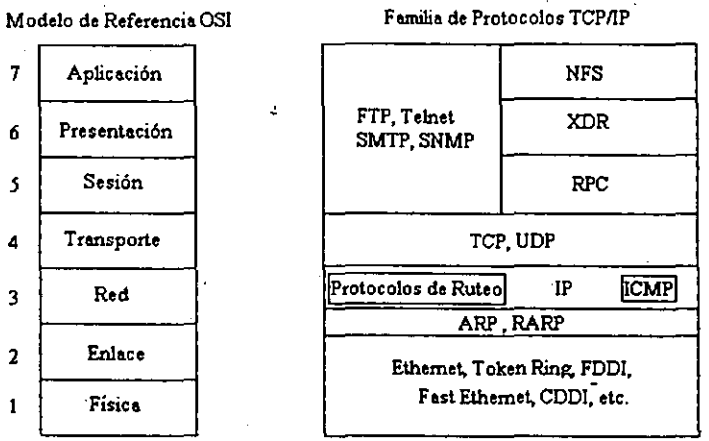


Figura 1.6 OSI vs TCP/IP

1.2.1 Direccionamiento IP

Los equipos conectados a la red internacional con tecnología TCP/IP requieren de identificadores o direcciones únicas, comúnmente llamadas direcciones IP. Sin embargo, cuando se tiene una red local TCP/IP sin conexión a la Internet se puede asignar cualquier dirección IP valida, de lo contrario, si la red está conectada a la red internacional se deberá asignar una dirección de red IP única.

El formato de la dirección IP lo define el protocolo Internet Protocol versión 4 y está compuesta por 32 bits (4 bytes), representada mediante una notación decimal de la siguiente forma: W.X.Y.Z donde W, X, Y. Z pueden tomar el valor de 0 a 255. Un ejemplo: 132.248.10.4.
La dirección IP consiste de dos partes: un identificador de red (NetID) y un identificador de equipo (HostID). Existen diferentes clases de redes IP: A, B, C y D como se observa en la siguiente tabla.

Clase de Dirección	Rango de direcciones		Bit orden mas alto
A	1.0.0.0	126.255.255.255	0
B	128.0.0.0	191.255.255.255	10
C	192.0.0.0	223.255.255.255	110
D	224.0.0.0	239.255.255.255	110
E	240.0.0.0	255.255.255.255	111

La Clase A usa sólo el primer byte para el identificador de red, la Clase B los primeros dos bytes, la Clase C los primeros tres bytes y la clase D utiliza los cuatro bytes como identificador para un grupo de multicast.

Si el tipo de red es una clase A o B, es posible obtener "subredes". Una subred es un rango de direcciones que forman parte de la red original. Por ejemplo, la red clase B que posee la RedUNAM se encuentra "subneteada" o dividida en pequeñas subredes.

Para poder "subnetear" una red, es necesario utilizar una máscara de red la que nos permite distinguir el NetID del HostID. La máscara de red es un conjunto de bits con formato semejante a la de la dirección IP que nos permite interpretar a que red pertenece una dirección IP dada y debe poseer 32 bits; deben de ser unos contiguos (aunque no siempre) a partir de la izquierda para identificar al NetID y los bits restantes deben de ser ceros para identificar al HostID.

Una máscara de red permite dividir la parte del HostID en dos partes por medio de la operación booleana AND bit por bit con lo que se obtiene:

- La primera parte identifica al número de subred.
- La segunda parte identifica al host en esa subred.

	Identificador de Red		Identificador de Equipo	
Mascara de red	11111111	11111111	00000000	00000000
	255.	255.	0.	0

Dirección IP regular

	Identificador de Red		Identificador de Subred	Identificador de Equipo de la Subred
Mascara de subred	11111111	11111111	11111111	00000000
	255.	255.	255.	0

Dirección Subneteada

Para el mejor entendimiento del "subneteo" se ejemplifica un caso dentro de RedUNAM.

La UNAM cuenta, entre otras, con una red clase B con dirección 132.248.0.0 y con 2^{16} (65536) direcciones para asignar a equipos. Debido a las necesidades de asignar direcciones por dependencia se optó por dividir el rango de direcciones en 256 subredes con 256 host cada una, utilizando una máscara de "subred" 255.255.255.0 de la siguiente forma:

Red :	132.248.0.0		
Clase :	B		
Máscara Natural :	255.255.0.0		
Máscara Aplicada :	255.255.255.0	Máscara 24 bits	
No. de subredes :	256	**Utilizables:**	254
No. de hosts por subred :	256	**Utilizables:**	254

100000100 . 11111000 . 00000000 . 00000000 132.248.0.0 de manera binaria
11111111 . 11111111 . 11111111 . 00000000 255.255.255.0 de manera binaria

FORMATO BINARIO	DECIMAL	SIGNIFICADO
Subred 0		
11111111 . 11111111 . 00000000 . 00000000	132.248.0.0	NetID de la subred 0
11111111 . 11111111 . 00000000 . 00000001	132.248.0.1	Primera dirección
11111111 . 11111111 . 00000000 . 00000010	132.248.0.2	Segunda dirección
...	...	...
11111111 . 11111111 . 00000000 . 11111101	132.248.0.253	Penúltima dirección
11111111 . 11111111 . 00000000 . 11111110	132.248.0.254	Última dirección
11111111 . 11111111 . 00000000 . 11111111	132.248.0.255	Dirección broadcast subnet 0
Subred 1		
11111111 . 11111111 . 00000001 . 00000000	132.248.1.0	NetID de la subred 1
11111111 . 11111111 . 00000001 . 00000001	132.248.1.1	Primera dirección
11111111 . 11111111 . 00000001 . 00000010	132.248.1.2	Segunda dirección
...	...	...
11111111 . 11111111 . 00000001 . 11111101	132.248.1.253	Penúltima dirección
11111111 . 11111111 . 00000001 . 11111110	132.248.1.254	Última dirección
11111111 . 11111111 . 00000001 . 11111111	132.248.1.255	Dirección broadcast subnet 1
...	...	...

De lo anterior resulta :

No.	ID RED	BROADCAST	RANGO			UTILIZABLE
1	132.248.0.0	132.248.0.255	132.248.0.1	-	132.248.0.254	NO
2	132.248.1.0	132.248.1.255	132.248.1.1	-	132.248.1.254	SI
3	132.248.2.0	132.248.2.255	132.248.2.1	-	132.248.2.254	SI
4	132.248.3.0	132.248.3.255	132.248.3.1	-	132.248.3.254	SI
5	132.248.4.0	132.248.4.255	132.248.4.1	-	132.248.4.254	SI
...	...	...	...	...	...	...
252	132.248.251.0	132.248.251.255	132.248.251.1	-	132.248.251.254	SI
253	132.248.252.0	132.248.252.255	132.248.252.1	-	132.248.252.254	SI
254	132.248.253.0	132.248.253.255	132.248.253.1	-	132.248.253.254	SI
255	132.248.254.0	132.248.254.255	132.248.254.1	-	132.248.254.254	SI
256	132.248.255.0	132.248.255.255	132.248.255.1	-	132.248.255.254	NO

Existe una fórmula que ayuda a calcular el valor de la máscara y determinar el número de hosts y subredes que más convenga a las necesidades de cada red:

$$N^{o} \text{ de hosts o } N^{o} \text{ de subredes} = 2^{n} - 2, \text{ donde } n = N^{o} \text{ de bits.}$$

Este tipo de arreglos se vienen pensando debido al gran crecimiento de Internet, de hecho uno de los mayores problemas que enfrenta la comunidad de Internet es el agotamiento de direcciones IP; esto nos lleva a la implantación de nuevas estrategias en el manejo de direcciones IP: Variable Length Subnet Masks (VLSM) y Classless Inter-Domain Routing (CIDR), para contrarrestar este problema. A continuación se describen.

1.2.1.1 VLSM (Variable Length Subnet Masks)

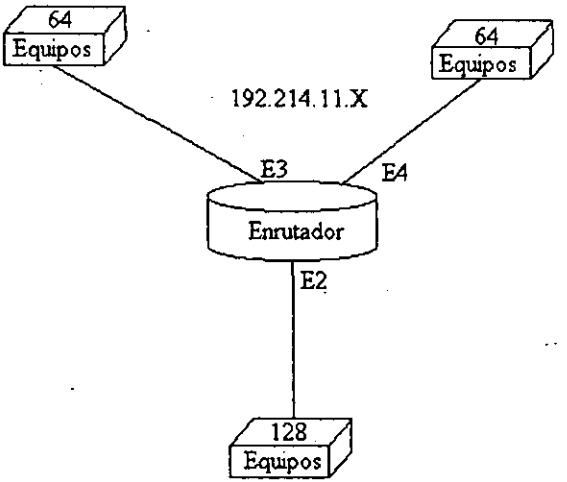
El término VLSM, se refiere a que una red pude ser configurada con diferentes máscaras de red. LSM es una extensión del subneteo básico donde las redes clase A, B y C pueden ser subneteadas utilizando una máscara de longitud variable. La idea de VLSM es ofrecer más flexibilidad para dividir —de acuerdo a las diferentes necesidades— la red en múltiples subredes utilizando diferentes máscaras de red para cada una de ellas y así tener un número adecuado de hosts en cada subred. Sin VLSM, una máscara de subred solamente puede ser utilizada.

Supóngase, por ejemplo, que se tiene la red clase C 192.214.11.0 y se necesita dividir esta red en tres subredes, con 100 hosts en una subred y las dos restantes con 50 hosts. Ignorando las direcciones 0 y 255, teóricamente se tendrían disponibles 256 direcciones, que va de la 192.214.11.0 a la 192.214.11.255. La división que se plantea no puede hacerse sin VLSM.

En VLSM existen máscaras del tipo 255.255.255.***X***, que pueden ayudar a dividir la red clase C 192.214.11.0 en más subredes, donde ***X*** puede tomar cualquier valor de máscara mostrado en la tabla siguiente para segmentar las 256 direcciones disponibles en más subredes.

Máscara	No. de subredes y posibles hosts
252 (1111 1100)	64 subredes con 4 hosts cada una
248 (1111 1000)	32 subredes con 8 hosts cada una
240 (1111 0000)	16 subredes con 16 hosts cada una
224 (1110 0000)	8 subredes con 32 hosts cada una
192 (1100 0000)	4 subredes con 64 hosts cada una
128 (1000 0000)	2 subredes con 128 hosts cada una

Sin VLSM, se tendría que escoger el uso de una máscara 255.255.255.128 y dividir la red en dos subredes de 128 hosts cada una o usar la máscara 255.255.255.192 y dividir a la red en 4 subredes con 64 hosts. Esto no cumple con los requerimientos. Sin embargo, utilizando múltiples máscaras se puede usar la máscara 255.255.255.128 para dividir la red en dos subredes con 128 hosts cada una, y usar la máscara 255.255.255.192 para dividir a una subred de ambas en dos con 64 hosts cada una, como se observa en la figura 1.7.



128 Direcciones (E2) (máscara 255.255.255.128)	
64 Direcciones (E3) (máscara 255.255.255.192)	64 Direcciones (E4) (máscara 255.255.255.192)

Figura 1.7 Varible Length Subnet Mask- VLSM

Sin embargo existen limitaciones, no todos los protocolos de enrutamiento pueden manejar VLSM. Por ejemplo RIP versión 1 e IGRP no pueden utilizar máscaras variables, pero protocolos como OSPF, EIGRP, ISIS y RIP versión 2 si soportan éste esquema. Por lo consiguiente si se quiere aprovechar las bondades que el esquema VLSM provee, se necesita implantar un protocolo cuyas características de diseño haya tomado en cuenta esta propiedad.

1.2.1.2 CIDR (Classless Inter-Domain Routing)

Recientemente, las tablas de enrutamiento IP en los enrutadores de Internet han crecido en gran cantidad, provocando que éstos empiecen a saturarse, tanto en procesamiento como en memoria (dos de los requerimientos más críticos en el enrutamiento). *"Se hicieron estudios de crecimiento los cuales indican que las tablas de enrutamiento se han duplicado en un lapso de 10 meses entre 1988 y 1991. Si no hubiese existido algún plan, las tablas de enrutamiento hubieran crecido aproximadamente a unas 80,000 rutas en 1995, sin embargo, en 1996 el tamaño de las tablas de*

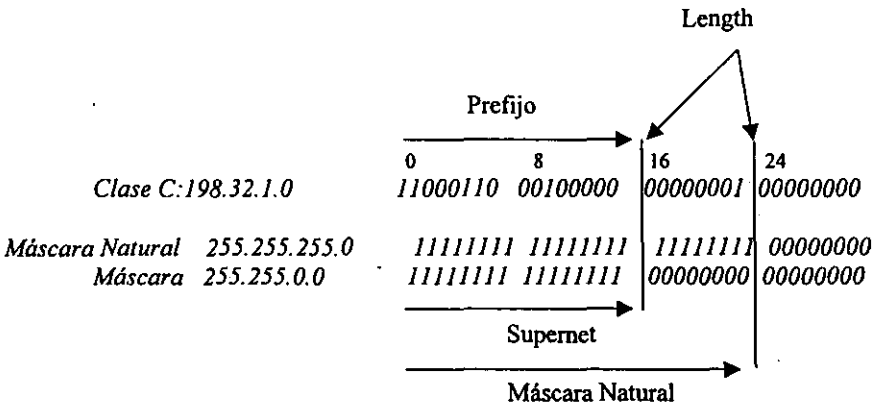
enrutamiento fue de alrededor de 42,000 rutas"[4]. Este decremento en el crecimiento es atribuido a CIDR.

CIDR es un mecanismo que permite anunciar un conjunto de subredes y redes a través de una sola dirección IP y una máscara (lo que se conoce como super-red). CIDR ofrece una solución alternativa que pretende resolver el problema de direccionamiento IPv4. Este problema lleva consigo el incremento en las tablas de enrutamiento y el agotamiento de las direcciones de redes clase B.

En CIDR, una supernet está representada por un prefijo (que es la dirección IP), junto con una "length"[5] (equivalente a la serie de bits unos contiguos más significativos dentro de esta dirección IP). La representación *prefijo/length* se le llamará *agregado*. Por ejemplo la red 198.32.0.0 , solía ser una red clase C ilegal, ahora es valida con la siguiente notación 198.32.0.0/16. La length "/16" indica que estamos utilizando 16 bits de máscara de red, empezando a contar desde la izquierda. La notación anterior es similar a tener 198.32.0.0 255.255.0.0.

También en CIDR, una red es llamada supernet, cuando la máscara que se esté utilizando sea más pequeña a la máscara natural de esa red. Una red clase C 198.32.1.0, por ejemplo, tiene una máscara natural 255.255.255.0. La representación 198.32.0.0 255.255.0.0 puede denotarse como 198.32.0.0/16 (que es una máscara menor a la máscara natural de la clase C), por lo tanto es una supernet.

Este esquema de direccionamiento es ilustrado en la figura 1.8:



198.32.1.0 255.255.255.0 ⇔ 198.32.1.0/24
198.32.1.0 255.255.0.0 ⇔ 198.32.1.0/16

Figura 1.8 Classless Inter-Domain Routing

[4] Dato obtenido del Libro Internet Routing Architectures, de Bassam Halabi.
[5] Notación decimal parecida a una máscara de red

Esta notación, nos permite juntar todas las redes especificas de la red 198.32.0.0 (como son la 198.32.1.0, 198.32.2.0 y así sucesivamente) en un solo anuncio llamado agregado.

Todas las redes que son parte de un bloque CIDR son llamadas prefijos "*más específicos*" porque dan más información a cerca de la localización de la red. Los prefijos más específicos tienen una length más grande que el agregado como se observa:

198.213.0.0/16	Agregado con una length de 16 bits.
198.213.1.0/20	Prefijo más específico con length de 20 bits.

1.3 Enrutamiento

En TCP/IP el enrutamiento se define como el movimiento de información a través de redes interconectadas, determinando la mejor ruta de un origen a un destino. Para esto se utiliza el protocolo enrutable IP y protocolos de enrutamiento como RIP, OSPF, IGRP, BGP, etc. IP es un protocolo enrutable ya que una la dirección IP nos ofrece información que es analizada para identificar a cada host y la red o subred a la que pertenece. La red o subred es analizada por un protocolo de enrutamiento cuya función es decidir la mejor ruta para encaminar cada paquete de información.

La Internet es una serie de Sistemas Autónomos (AS), que definen políticas de administración y de enrutamiento de diferentes organizaciones. Un Sistema Autónomo ocupa Protocolos de Compuerta Interna (IGP's Interior Gateway Protocol), tales como RIP, IGRP, EIGRP, OSPF, e ISIS, para enrutar información del mismo Sistema Autónomo. Estos a su vez se interconectan vía un Protocolo de Compuerta Externa (EGP Exterior Gateway Protocol), tales como EGP y BGP para intercambio de información entre Sistemas Autónomos.

Un enrutador es un dispositivo de red de propósito particular, que a través de protocolos de enrutamiento IGPs y EGPs encamina la información de un lugar origen a un destino por la mejor ruta. Este equipo actúa sobre la capa 3 (Red) del modelo OSI. Los enrutadores construyen tablas de enrutamiento conteniendo información de los mejores caminos (paths), a todos los destinos que conocen.

Existen dos tipos de enrutamiento: El directo y el indirecto.

Directo:

Es la transmisión directa de un paquete de información de una máquina a otra siempre y cuando ambas máquinas pertenezcan al mismo segmento lógico y por lo tanto físico.

Indirecto:

Cuando las máquinas que se quieren comunicar no están en la misma red (lógica y física), lo cual se traduce en la necesidad de utilizar un equipo adicional, que se encargue de comunicar la red origen al destino.

Un enrutador se comunica con otro enrutador con el fin de intercambiar tablas de enrutamiento, información de control y diversos mensajes. Este intercambio de información se da gracias a los algoritmos de enrutamiento.

Los algoritmos de enrutamiento emplean comúnmente una tabla de enrutamiento en la que almacena información referente a los posibles destinos y como llegar a ellos. Las tablas se generan a partir de dos procesos: Iniciación del proceso de enrutamiento e intercambio de tablas con otros enrutadores.

Existen diferentes algoritmos de enrutamiento y cada uno de ellos fue diseñado con un propósito en particular, es por eso que tienen diferente impacto sobre la red y sobre los recursos de los enrutadores. Cada uno de estos algoritmos utilizan una variedad de métricas[6], que afectan directamente en el cálculo de la mejor ruta. Los algoritmos de enrutamiento generalmente tienen una o más de las siguientes características de diseño.

1.3.1 Características de diseño

Robustez.

La robustez nos indica que el algoritmo de enrutamiento debe de soportar una buena cantidad de rutas en las tablas de ruteo, además debe ser tolerante a implantaciones incorrectas y a fallas de hardware.

Estabilidad.

Esta característica de diseño nos indica que los anuncios de enrutamiento que se encuentran en nuestros equipos, deben de ser coherentes con lo que está aconteciendo en la red en todo momento.

Flexibilidad.

Cuando se desee que el enrutador crezca en un mayor número de interfaces, entonces, el equipo como el protocolo de enrutamiento debe ser lo suficientemente flexible para permitir agregar una nueva tarjeta al enrutador y automáticamente debe reconocer la tarjeta y debe permitir configurarla.

Los algoritmos de enrutamiento deben adaptarse rápidamente a la gran variedad de circunstancias que ocurran en la red, es decir, los algoritmos deben de ser programados para adaptarse a los cambios en la red, como son el ancho de banda, tamaño de colas, retardos en la red, y otras variables.

Simplicidad y Bajo Overhead.

El algoritmo de enrutamiento debe de ser lo más simple posible, en otras palabras, debe ofrecer funcionalidad y eficiencia con un mínimo de recursos. La eficiencia es particularmente importante cuando la implantación del algoritmo de enrutamiento debe de

[6] Métricas. Es una medida asignada a un anuncio de enrutamiento. Se calcula por medio de una evaluación de ciertas variables como son: Ancho de Banda, Retardo, Costo, Número de Saltos, confiabilidad y carga. Que intervienen en la determinación de la ruta óptima para poder llegar a un destino y la forma de calcularse depende del algoritmo que se esté utilizando.

correr en un enrutador con recursos físicos limitados. Por ejemplo, el enrutador no debe de utilizar mucho ancho de banda para transportar sus anuncios de enrutamiento.

Rápida Convergencia.

La convergencia es el proceso de conformidad por todos los enrutadores sobre las rutas óptimas, es decir, cuando un anuncio de una red deja de ser anunciada por un enrutador, entonces, se debe de mandar mensajes de actualización de rutas para recalcular rápidamente la ruta óptima para poder llegar a ese destino por otro lado. Si no existiera una convergencia rápida, se provocaría una inconsistencia en los anuncios de las redes.

Optimización.

Si tenemos varias rutas en nuestra tabla de enrutamiento para poder llegar a un destino determinado, el protocolo de enrutamiento debe de ser lo suficientemente inteligente para poder seleccionar la mejor ruta.

1.3.2 Clasificación

Los algoritmos de enrutamiento pueden ser clasificados por varios tipos.

- Estáticos o Dinámicos
- Single-Path o Multipath
- Plano o Jerárquico
- Intradominio o Interdominio
- Link State o Distance Vector

1.3.2.1 Estáticos o Dinámicos.

En los algoritmos de enrutamiento estático el administrador de la red crea una tabla de enrutamiento manualmente. Dicha tabla no cambia a menos que el administrador lo haga. Los algoritmos que usan rutas estáticas son fáciles de diseñar y trabajan bien en ambientes donde el trafico de la red es relativamente predecible y el diseño de la red es relativamente simple.

Actualmente este tipo de algoritmos no son utilizados debido a que éstos no ven los cambios que acontecen en la red.

Los algoritmos de enrutamiento dinámico van ajustando las rutas dinámicamente en tiempo real, gracias a que analizan los mensajes de actualización de rutas. Este tipo de algoritmos permite la implantación de rutas estáticas cuando éstas sean necesarias.

1.3.2.2 Single-Path o Multipath.

Existen protocolos de enrutamiento muy sofisticados que aceptan múltiples rutas para un mismo destino. Estos algoritmos son llamados Multipath, y pueden balancear cargas a través de múltiples líneas. Los algoritmos Single-Path, por el contrario, sólo aceptan una sola ruta por cada red.

1.3.2.3 Plano o Jerárquico.

En sistemas de enrutamiento plano, todos los enrutadores son parejas de todos. En un sistema jerárquico, algunos enrutadores conforman el backbone. Cuando un paquete que provenga de un enrutador que no pertenezca al backbone, lo manda a los enrutadores que si pertenezcan a él para que estos se encarguen de encontrar una ruta para llegar a su destino.

1.3.2.4 Algoritmos Intradominio o Interdominio.

Algunos algoritmos de enrutamiento trabajan sólo dentro de dominios, otros trabajan dentro y entre dominios, es decir, los enrutadores que trabajan con algoritmos Intradominio sólo intercambias tablas de enrutamiento dentro de su sistema autónomo; en cambio, los enrutadores que utilizan algoritmos Interdominio pueden intercambiar sus tablas de enrutamiento dentro y fuera de su sistema autónomo.

1.3.2.5 Distance Vector o Link State.

Los algoritmos Link State (conocidos como algoritmos Shortest Path First), mandan su información de enrutamiento a todos los nodos de la red. Sin embargo, cada enrutador envía sólo una porción de su tabla de enrutamiento que describe el estado de sus enlaces. Los algoritmos Distance Vector (conocidos como algoritmos Bellman-Ford), mandan toda la tabla de enrutamiento, pero sólo a sus vecinos. Los algoritmos de tipo Link State son menos propensos a loops de enrutamiento, porque convergen más rápido que los algoritmos Distance Vector. Una posible desventaja de Link State es que requiere de más CPU y memoria.

1.3.3 RIP

RIP (Routing Information Protocol) está definido en el RFC 1058. Es un protocolo distance-vector y usa el número de saltos como métrica. RIP se utiliza mucho para enrutamiento de tráfico como protocolo de compuerta interna (IGP), lo que significa que trabaja dentro de un solo sistema autónomo. Existen dos versiones de RIP, la primera versión no acepta VLSM y la segunda sí.

Actualizaciones de Enrutamiento.

RIP envía mensajes de actualización de enrutamiento en intervalos de tiempo regulares (30 segundos) y cuando hay algún cambio en la topología de la red. Cuando el enrutador recibe una actualización de enrutamiento con algún cambio de alguna red, actualiza su tabla de enrutamiento para que se vean reflejados los cambios. El valor de la métrica que utiliza es el número de saltos y éste se va incrementando de uno en uno por cada enrutador que pase. Este protocolo sólo guarda en su tabla de enrutamiento la mejor ruta (la ruta con la menor métrica) hacia un destino en particular. Después de actualizar su tabla de enrutamiento, el enrutador inmediatamente empieza a transmitir a los demás enrutadores actualizaciones de enrutamiento, avisándoles que hubo algún cambio en la red. Estas actualizaciones se envían independientemente de las actualizaciones de ruteo que RIP periódicamente envía.

Las actualizaciones en RIP se hacen por medio de un paquete de broadcast como se muestra en la figura 1.9 donde el enrutador más a la izquierda manda un paquete de broadcast que es escuchado por todos los equipos.

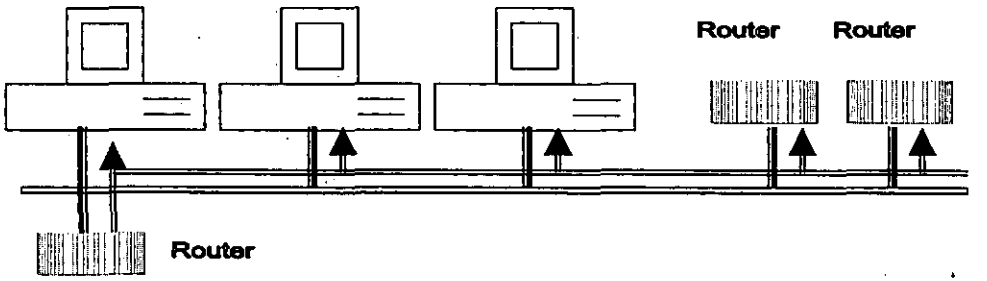


Figura 1.9 Routing Information Protocol v1

Métrica.

RIP usa una métrica muy sencilla "número de saltos" para medir la distancia entre la red origen y la destino. A cada salto en el path del origen al destino se le asigna un valor al número de salto, que por lo regular es 1. RIP prevee loops de enrutamiento implementando un límite de número de saltos alojado en el path, desde el origen al destino. El número máximo de saltos en el path es de 15. Si un enrutador recibe una actualización de enrutamiento y ve que la métrica es 16, entonces la red destino se toma como inalcanzable.

Estabilidad en RIP.

Para que RIP se ajuste a los rápidos cambios en la topología de una red, implementa los mecanismos de split-horizon y el de hold-down para prevenir que información incorrecta sea propagada a los demás enrutadores.

Formato del Paquete.

A continuación se muestra el formato de los paquetes de RIPv1 y RIPv2.

Formato RIP

La longitud de los campos está dada en bytes.

1	1	2	2	2	4	4	4	4
A	B	C	D	C	E	C	C	F

Donde:

A= Comando B= Versión C= Zero

D= Identificador de familia de direcciones E= Dirección F= Métrica

Comando. Indica si el paquete es una petición o una respuesta. La petición consiste en pedirle al enrutador toda o parte de la tabla de enrutamiento al enrutador. La respuesta puede ser una actualización de enrutamiento no solicitada o una respuesta a una petición.

Versión. Especifica la versión de RIP que se esté utilizando.

Zero. No utilizado.

Identificador de familia de direcciones (AFI). Especifica la familia de direcciones utilizada. RIP es designado a encaminar información de enrutamiento por diferentes protocolos. Cada entrada tiene un identificador de familia de direcciones para indicar el tipo de direccionamiento utilizado. El AFI para IP es 2.

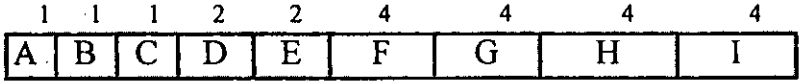
Dirección. Especifica la dirección IP de la entrada.

Métrica. Indica cuantos saltos (enrutadores) ha atravesado en el viaje para llegar al destino. Este valor es entre 1 y 15 para una ruta valida, o 16 para una ruta inalcanzable.

Cuando utilizar RIP.

- Cuando son redes locales muy pequeñas
- Cuando son redes no redundantes.
- Bueno cuando son redes con enlaces muy estables.
- La implementación se hace en unas cuantas horas.

Formato RIPv2.



Donde:

A= Comando B= Versión C= Zero D= AFI
E= Etiqueta de ruta F= Dirección IP G= Máscara de Subred H= Próximo Salto
I= Métrica

Comando. Indica si el paquete es una petición o una respuesta. La petición consiste en pedirle al enrutador toda o parte de la tabla de enrutamiento al enrutador. La respuesta puede ser una actualización de enrutamiento no solicitada o una respuesta a una petición.

Versión. Especifica la versión de RIP que se esté utilizando.

Zero. No se utiliza

AFI. Especifica la familia de direcciones utilizadas. La familia de IP es 2. Si en el campo AFI el primer mensaje es 0xFFFF, el aviso de esta entrada contiene información de autenticación. Actualmente sólo cuenta con autenticación simple en password.

Etiqueta de Ruta. Provee un método para distinguir entre enrutadores internos (Aprendidos por RIP) y enrutadores externos (Ruteadores aprendidos por otros protocolos).

Dirección IP. Especifica la dirección IP de la entrada.

Máscara de subred. Contiene la máscara de la subred de esta entidad. Si este campo está en cero, no existe una máscara de red para esta entrada.

Próximo Salto. Indica la dirección IP del próximo salto al cual el paquete va a ser enviado.

Métrica. Indica cuantos saltos (enrutadores) ha atravesado en el viaje para llegar al destino. Este valor es entre 1 y 15 para una ruta valida, o 16 para una ruta inalcanzable.

Las ventajas de RIPv2 sobre la primera versión son:

- Sumarización de rutas
- Autentica las actualizaciones de enrutamiento utilizando el método de encriptamiento MD5.
- Para las actualizaciones de enrutamiento RIPv2 utiliza multicast como se muestra en la figura 1.10 donde únicamente los enrutadores atienden dicha actualización.

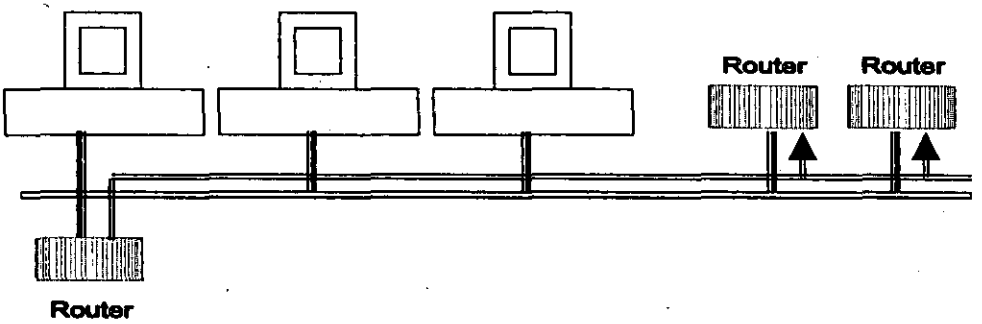


Figura 1.10 Routing Information Protocol v2

1.3.4 IGRP

IGRP (Interior Gateway Routing Protocol) es un protocolo de enrutamiento que fue desarrollado a mitad de la década de los 80s por Cisco System Inc. La idea principal del desarrollo de este protocolo fue proveer un mecanismo robusto para enrutamiento dentro de un mismo AS (IGP).

IGRP vs RIP
IGRP viene a dar solución a las limitantes que presentaba RIP, ya que RIP es un protocolo útil para redes homogéneas de pequeñas a tamaño moderado, cuando las redes comenzaron a crecer RIP empezó a ser obsoleto, principalmente debido al límite de saltos (16) que limita el tamaño de las redes y a la métrica que sólo considera el número de saltos.

- IGRP difiere en tres características de RIP:
- Implementa una métrica compuesta, a comparación de la métrica simple de hop-count.
- Maneja múltiples rutas para distribuir el tráfico.
- Diversas características de estabilidad son introducidas.

Funcionamiento
IGRP es un protocolo IGP de tipo Distance-Vector ya que intercambia parte o toda su tabla de enrutamiento en intervalos de tiempo regulares a cada uno de sus vecinos en mensajes tipo broadcast. Cada enrutador compara la tabla que recibe con la suya propia y si existe una nueva ruta es agregada a su tabla de enrutamiento; si una ruta tiene menor métrica reemplazará a la existente. Conforme las tablas de enrutamiento se dispersan por la red, los enrutadores podrán calcular distancias a todos los nodos dentro del AS.

Estabilidad en IGRP.
En cuanto a las características de estabilidad IGRP incluye los mecanismos de estabilidad: hold-down, split horizons, y poison-reverse (descritas anteriormente).

Métricas en IGRP
IGRP usa una combinación de diferentes factores para el cálculo de la métrica utilizada para las decisiones de enrutamiento:

- Retardo en la red (D)
- Ancho de banda del segmento de la ruta con menor ancho de banda (BW)
- Confiabilidad de la ruta (r)
- Ocupación del canal de la ruta

Todas ellas se usan para calcular una métrica compuesta dada por la siguiente ecuación:

$$[(K1 / B) + (K2 * D)]\, r$$

Donde K1, K2 son constantes que indican el peso a asignarse al ancho de banda y el retardo de acuerdo al "tipo de servicio" que el administrador desee configurar de acuerdo a los diferentes tipos de aplicaciones (voz, datos, etc.). IGRP puede usar las de omisión y las configuradas por el administrador para el cálculo de rutas óptimas.

Los valores de cada una de las métricas pueden tomar rangos extensos. Por ejemplo, la confiabilidad y carga pueden tomar un valor entre 1 y 255; el ancho de banda puede tomar valores desde 1200 bps a 10 Gigabits por segundo; el retardo puede fluctuar entre 1 a 2^{24}. Lo anterior con el objetivo de ser más específicos en cada uno de los casos.

Adicionalmente a las métricas y mecanismos de estabilidad, IGRP implementa "timers" o temporizadores. Son 4 las constantes de que controlan la propagación y expiración de rutas:

- Broadcast Time. Los mensajes son enviados en broadcast por todos los enrutadores en todas sus interfaces. Su valor por default es 90 segundos.
- Invalid Time. Si un mensaje de update de una ruta determinada no ha sido recibido por un periodo de tiempo se considera con tiempo expirado. Este tiempo deberá ser varias veces el valor del Tiempo de Broadcast. Su valor es 3 veces el tiempo Broadcast.
- Hold Time. Cuando una ruta es inalcanzable (o la métrica ha aumentado lo suficiente para causar envenenamiento), la ruta se pone el "holddown". Durante este estado, ninguna ruta será aceptada durante un periodo de tiempo dado. Este valor deberá ser varias veces el Broadcast Time, el valor de omisión es 3 veces el Broadcast Time más 10 segundos.
- Flush Time: Después del Invalid Time, la ruta expira y es removida. Sin embargo la entrada en la base de datos permanece, esto con el objeto de poner la ruta en holddown. Después del Flush Time, la entrada en la base de datos es removida. El valor deberá ser un poco mayor que el valor de Invalid Time más el de holddown. El valor por omisión es 7 veces el Broadcast Time.

Además IGRP permite enrutamiento multi-ruta, lo que significa que IGRP puede enviar información en IGRP en dos líneas con igual ancho de banda por medio de un round-robin y eligiendo alguna de ellas de manera automática en caso de que alguna de ambas falle.

1.4 Conceptos básicos de diseño de redes de datos

Existen cinco puntos básicos que se deben de tomar en cuenta para llevar a cabo un buen diseño de redes de datos, cabe mencionar que estos cinco puntos nos ayudan a tomar ciertas decisiones, pero no garantizan el perfecto funcionamiento de ésta, todo depende de las necesidades particulares de la organización.

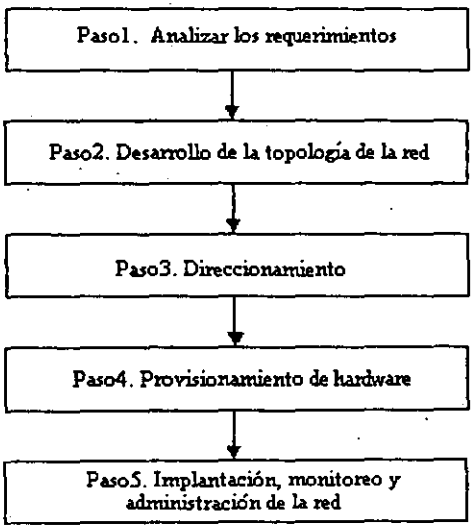


Figura 1.11 Pasos en el diseño de redes

1.4.1 Analizar los requerimientos.

El analizar los requerimientos determinará cuáles son las necesidades reales de la organización y así cubrir todas las expectativas de los usuarios para llevarlas a cabo a la red real. Hay que tomar en cuanta que las necesidades de los usuarios siempre cambian, y algunas veces ni saben lo que quieren pero siempre hay que tomar en cuenta estos requerimientos para su utilización en un futuro.

1.4.2 Desarrollo de la topología de la red.

El desarrollo de la topología de la red consiste en determinar el trazado de la red física, generalmente se ocupan dos diseños de topología, jerárquica o plana.

En la topología plana todos los enrutadores esencialmente realizan las mismas funciones, es decir, no existe una definición clara de las funciones específicas de cada uno de ellos.

En la topología jerárquica la red está organizada en niveles, las cuales tienen definidas claramente sus funciones. En este tipo de redes existen tres niveles:

- Nivel Core (Backbone). En este nivel se encuentran todos los enrutadores que se conectan al backbone. Todos estos enrutadores estarán interconectados y no deberá haber ninguna conexión a un host, esto es, porque el principal propósito de este nivel es proveer de conectividad entre todas las demás áreas.
- Nivel de Distribución. En este nivel es donde van todas las demás áreas, todas éstas conectadas a través de enrutadores de borde de área (ABRs) hacia el área cero. En este nivel se lleva a cabo la implantación de políticas de la red como lo es: la seguridad, DNS, políticas de enrutamiento, etc.
- Nivel de Acceso. Es aquí donde los enrutadores inter-area proveen de conexión a los usuarios finales. Es en esta parte donde la mayor parte de los host y servidores se proveen de servicios de red.

Los beneficios que la topología jerárquica implementada en una red son las siguientes:

- Escalabilidad. Las redes pueden crecer muy fácilmente debido a la funcionalidad de los niveles, por esto si se quiere agregar otro nodo, es muy fácil de realizarlo e implementarlo.
- Predictibilidad. Debido al seccionamiento por niveles de esta topología, hace que la funcionalidad de cada nivel sea más predecible. Esto hace más fácil la planeación de modelado de la red.
- Soporte de Protocolos. Con este tipo de esquema es muy fácil implementar diferentes protocolos de enrutamiento dentro de un mismo sistema autónomo, como puede ser BGP y OSPF.
- Fácil Troubleshooting. Es fácil reconocer donde radica cierto problema debido a la estructura de esta topología

1.4.3 Direccionamiento.

Asignando bloques de direcciones a porciones de la red, trae como beneficios la simplificación del direccionamiento, mejor administración, un buen esquema de enrutamiento y escalabilidad.

El direccionamiento jerárquico permite una sumarización muy eficiente de rutas a través de la red. También hay que determinar si se va a utilizar direccionamiento público o privado en el esquema, ya que hay que tomar en cuenta la escalabilidad de la red debido a que el crecimiento de una red es constante.

Se debe determinar el rango de direcciones IP que se va a emplear para el direccionamiento dentro de la red.

1.4.4 Provisionamiento de hardware.

En esta parte hay que ver la documentación de los fabricantes para determinar el hardware necesario a utilizar para la construcción de la red, tanto para la LAN como la WAN. Para las LANs se debe de tener en cuenta los modelos de los enrutadores, switches, sistemas de cableado y conexiones al backbone. Para la parte WAN se debe de tomar en cuenta enrutadores de mayor capacidad, modems, CSUs/DSUs, y servidores de acceso remoto.

1.4.5 Implantación, monitoreo y administración de la red.

Con respecto a la implantación es necesario leer los manuales de configuración de los equipos que se van a utilizar para implantar cualquier esquema de enrutamiento, ya que los equipos de cada proveedor pueden poseer ciertas características particulares.

La administración de una red, es un conjunto de actividades que se deben de llevar a cabo para lograr un optimo desempeño de una o varias redes de datos. Para llevar a cabo esta tarea se requiere de dos cosas: Operación y planeación.

- La operación es una actividad que involucra funciones tales como: mantenimiento y configuración de dispositivos, monitoreo y atención a fallas.

- La planeación es una actividad que comprende tareas tales como: la obtención de estadísticas de desempeño, análisis y diseño, crecimiento en infraestructura y servicios.

La adecuada administración y operación de la red proporciona varios beneficios:

- *Brinda el soporte necesario a las redes de misión crítica.* Mantener operando la red las 24 horas del día, los 7 días de la semana; es un requisito. Las redes robustas no pueden ser administradas únicamente con el esfuerzo humano, se requiere de mecanismos de administración, control y monitoreo como apoyo.

- *Reduce los tiempos de caída de la red.* Cada minuto que la red esté "caída" equivale a perdidas de dinero que deben ser sufragadas. Aquí es donde el monitoreo cumple su principal función: administración proactiva.

- *Se requiere de menos personal para mantener operativa la red.* Cuando se tiene la red administrada adecuadamente los requerimientos de personal calificado se reducen.

- *Se reducen los costos de administración y operación.* Las labores administrativas se automatizan, permitiendo al personal más tiempo para otras actividades, como diseño y análisis.

- *Mejor documentación de la red.* La automatización del proceso de documentación de la red se automatiza, lo que hace más verídicos y actuales los inventarios, configuraciones, etc.

- *Se hace un mejor uso de la infraestructura de red.* Una buena administración permite un mejor conocimiento de la red que se refleja en una mejor asignación del equipo activo.

- *Permite un mejor análisis de los patrones de tráfico así como en la seguridad.* Esto gracias a las herramientas de monitoreo remoto (SNMP con RMON/RMON2).

La Organización Internacional de Estándares (OSI) define la administración de redes en cinco áreas funcionales:

- Administración de fallas.
- Administración de contabilidad.
- Administración de configuración.
- Administración de desempeño.
- Administración de seguridad.

Administración de fallas.

Esta área permite habilitar la detección, registro y corrección de problemas que se presenten en la red.

Administración de contabilidad.

Habilita los parámetros para medir la utilización de la red, además regula el uso de los recursos a los usuarios.

Administración de configuración.

Control, monitoreo y mantenimiento de la configuración operativa de cada uno de los dispositivos de la red.

Administración de desempeño.

Mide los parámetros de desempeño de una red y sus recursos, además mantiene un nivel aceptable de desempeño.

Administración de seguridad.

Controla el acceso a los recursos de la red de acuerdo con las políticas de la organización.

Cuando se justifican los gastos de la implantación de un esquema de administración de la red, se mejora el desempeño, no solo de la red, sino que se refleja en todos los niveles dentro de la compañía. Existen diversos tipos de software para tales tareas. Su funcionamiento y arquitectura se describe a continuación:

La arquitectura de administración de redes se compone de tres componentes principales que trabajan en arquitectura Cliente/Servidor:

- *Network Management System - NMS* (Sistema de Administración e Red). Conjunto de programas cliente encargados de polear (poll) a los agentes con el objetivo de obtener información de los dispositivos de la red.
- *Agent* (agente). Programa servidor encargado de obtener la información de la base de datos de los dispositivos y entregarla al NMS.
- *Network Management Protocol* (Protocolo de Administración de la Red). Protocolo de comunicación encargado de comunicar al NMS con el Agent (Cliente/Servidor respectivamente).

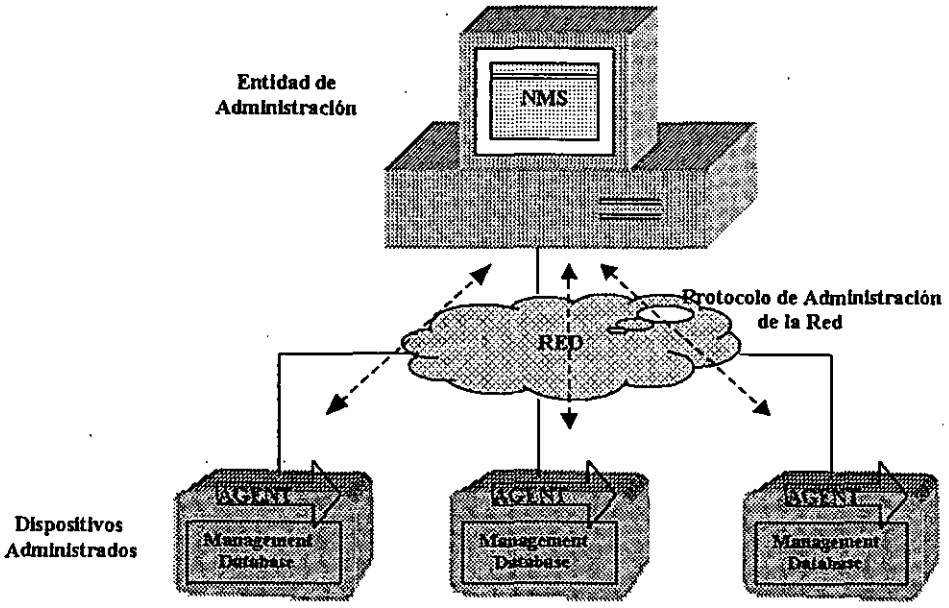


Figura 1.12 Arquitectura de administración de redes

Un Sistema de Administración de Red (NMS) está compuesto por dos partes:

- Una Plataforma de administración de Red
- Una Aplicación de administración de Red

Una Plataforma de Administración de Red es una colección de herramientas de red que hacen uso de SNMP, RMON, etc., para monitorearla y controlarla. Esta suite de herramientas se puede ver como un software que proporciona funcionalidades genéricas de administración para diferentes dispositivos de red. Estas herramientas deben contar con las siguientes características:

- Interfaz gráfica.
- Mapa de red.
- Manejador de base de datos.
- Método estándar de consulta de dispositivos.
- Sistema de menús flexible.
- Bitácora de eventos.

A continuación se muestra gráficamente estos elementos:

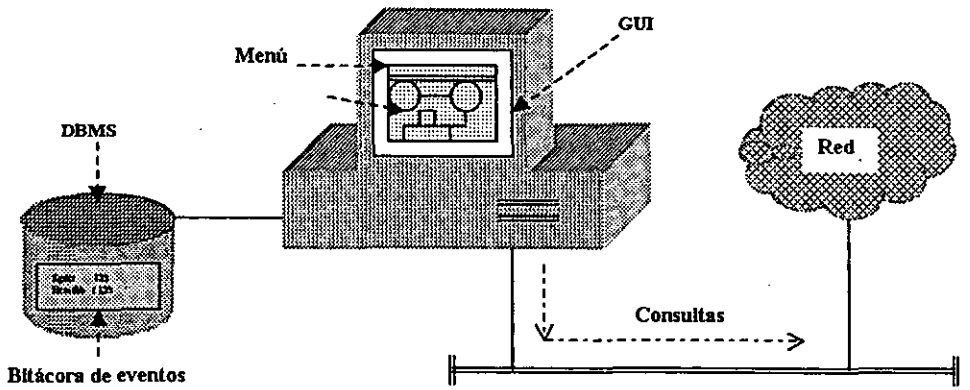


Figura 1.13 Plataforma de administración de redes

Las plataformas más comunes son:

- HP Open View (HP)
- Solstice Enterprice Management (SunSoft)
- Netview (IBM)
- StarSentry (AT&T)

Una Aplicación de Administración de Red es un software propietario que complementa a la Plataforma de Administración de Red y ofrece funcionalidades específicas de acuerdo al equipo activo de red que soporta. Ejemplo de éste software es:

- Transcend de 3Com Corporation.
- Optivity de Nortel Networks
- Spectrum (Cabletron Systems)

Los agentes de red (Agents) son en sí los diversos equipos activos que soporten administración bajo este esquema. Ejemplo de ellos: enrutadores, switches, hubs, workstation, etc.

Finalmente, la parte más importante de la administración de redes se encuentra en el Protocolo de Administración de Red. Este protocolo es el conjunto de reglas y procedimientos que permite que el Agente y el NMS se comuniquen. De los más importantes se encuentra:

- SNMP/SNMPv2

SNMP (Protocolo Simple de Administración de Red) es el método estándar para configurar y monitorear los protocolos TCP/IP y dispositivos de red. SNMP manipula datos de administración dentro de los dispositivos de red, como lo es un enrutador. Estos datos forman la información base de administración de un dispositivo, comúnmente llamado MIB, el cual está organizado en una estructura de árbol. Cada protocolo de Internet que trabaje dentro de un dispositivo requiere que se provea de sus propios datos de administración.

SNMP provee de 3 funciones para accesar a los datos de administración: get, get-next, y set. Cada uno de ellos es un tipo de paquete de SNMP.

La función get de SNMP lee el valor de una instancia en particular de una variable de MIB, por ejemplo:

```
get 1.3.6.1.2.1.14.8.1.4.132.248.254.254.0.0
```

Regresara el tipo de servicio (TOS) con costo igual a 0 de la interfaz OSPF cuya dirección IP sea 132.248.254.254.

La función get-next obtiene un identificador de objeto como argumento, pero regresa una instancia de la variable de la MIB que inmediatamente sigue del identificador de objeto dado, en orden lexicográfico (esto es, el orden de las palabras son listadas en un diccionario). Esto permite a get-next navegar por toda la base de datos repetitivamente. Por ejemplo esta función se puede ocupar para listar los costos de OSPF de todas las interfaces de un enrutador.

```
$ get-next 1.3.6.1.2.1.14.8.1.4
1.3.6.1.2.1.14.8.1.4.132.248.1.2.0.0   100
1.3.6.1.2.1.14.8.1.4.132.248.1.254.0.0 150
1.3.6.1.2.1.14.8.1.4.132.248.5.132.0.0 45
```

En SNMP la función set permite escribir una instancia de variable de la MIB en particular, por ejemplo, para agregar un costo de 150 a una interface OSPF en particular, se realiza con el siguiente comando:

```
set 1.3.6.1.2.1.14.8.1.4.132.248.5.135.0.0 150
```

SNMP también tiene la facilidad de permitir a los dispositivos de Internet enviar notificaciones asíncronas de eventos importantes a estaciones de administración de red, llamados SNMP traps.

Capítulo II

Descripción de la Estructura Actual de RedUNAM

II. Descripción de la estructura actual de RedUNAM

En el transcurso de este capítulo se verá la historia y evolución de RedUNAM así como la estructura actual de la red de datos de manera modular, con la finalidad de dar un enfoque más detallado de su funcionamiento y los problemas que presenta, por lo que éste capítulo se encuentra dividido en cuatro partes:

- Historia y Descripción general de RedUNAM
- Nivel de Transporte: Ethernet, Fast Ethernet, ATM y LANE
- Nivel de Red: switches capa 3, backbone de enrutadores
- Problemática

II.1 Historia de RedUNAM

En el año del 1987, la UNAM establece la primera conexión de la Red Académica de cómputo de aquel entonces con la Red BITENET mediante enlaces telefónicos desde Ciudad Universitaria hasta el Instituto Tecnológico de Estudios Superiores de Monterrey (ITESM) en Monterrey y de ahí hasta San Antonio, Texas en los EUA. Dicha conexión consistía en una computadora IBM 4381 para manejo de correo electrónico.

Para 1989, a través del Instituto de Astronomía se establece un convenio para enlazar a la red académica de la UNAM con la red de la NFS en EUA. El enlace se realizó mediante el satélite mexicano Morelos II que conectaba el Instituto de Astronomía en la UNAM y el UCAR-NCAR con residencia en Boulder Colorado. La finalidad del proyecto estaba enfocada a la investigación de fenómenos astrales. A la par se llevó a cabo el primer enlace para conectar las redes de área local, del Instituto de Astronomía y la Dirección General de Servicios de Cómputo Académico (DGSCA) utilizando enlaces de fibra óptica. A partir de ese momento se inició dentro de la UNAM una revolución en las comunicaciones.

Acciones como la adquisición masiva de computadoras personales, su conexión a red y la intercomunicación de redes de área local (principalmente en las dependencias de investigación científica) permitió desarrollar la infraestructura de comunicaciones de fibra óptica actual de RedUNAM, establecer más enlaces satelitales hacia Cuernavaca, Morelos, y San Pedro Mártir en Ensenada, Baja California Norte, también el primer enlace de microondas de alta velocidad sobre la Ciudad de México entre la Torre II de Humanidades y la Dirección General de Servicios de Cómputo Académico, DGSCA.

Para el año de 1990 la UNAM, fue la primera institución en Latinoamérica que se incorpora a la red mundial Internet, que enlaza a millones de máquinas y decenas de millones de usuarios en todo el mundo. Su ininterrumpido desarrollo contempla como elemento fundamental, el diseño de una arquitectura que permita la comunicación de redes de diferentes arquitecturas trabajando bajo el protocolo TCP/IP, mismo que se mantiene como estándar en la actualidad, dado su funcionalidad y posibilidad de adaptación a los requerimientos que se van presentando.

La operación de la Red Integral de Telecomunicaciones con una plataforma de backbone basada en la tecnología ATM dio inicio en la primera semana del mes de agosto de 1997. En esa fecha solo se enviaba tráfico de datos. Para la segunda quincena del mes de octubre se incorpora el tráfico de voz y videoconferencia. Este mismo esquema basado en ATM se encuentra en funcionamiento hoy en día y es el que se explica a lo largo de este capítulo.

Uno de los aspectos relevantes de la Red Integral de Telecomunicaciones de la UNAM es la interoperabilidad; ya que la plataforma de RedUNAM está formada por equipos de diferentes fabricantes. Sin embargo, aunque los productos cumplen con los estándares, se tuvieron en un principio algunas incompatibilidades entre ellos. Éstas incompatibilidades fueron resueltas con actualizaciones en las versiones del software y a la fecha están interoperando adecuadamente. Desde entonces, se han hecho muchas mejoras a las versiones de software, lo que permite optimizar el funcionamiento de los equipos entre las que destaca mejorar el esquema de enrutamiento estático.

II.2 Descripción general de RedUNAM

RedUNAM es el proyecto que se desarrolló para la transmisión de información entre las facultades, institutos, centros de difusión, coordinaciones y demás dependencias que conforman a la UNAM. Actualmente cuenta con más de 25,000 computadoras conectadas a la red de datos, más de 424 líneas del sistema telefónico digital que atienden a cerca de 12,000 cuentas de Dial-Up y 11 enlaces internacionales sumando, una capacidad de transmisión de más de 21 Mbps a EE.UU. para la conexión a Internet.

RedUNAM es una red de computadoras LAN dentro de las dependencias e institutos; MAN con las conexiones a las ENEPs, FESes, Preparatorias, CCHs y demás centros dentro del área metropolitana; WAN en las conexiones con instituciones externas (instituciones públicas y privadas) y enlaces internacionales. Utiliza tecnología Ethernet, Fast Ethernet, ATM y TDM que sirven como infraestructura para comunicarse principalmente por medio de la suite de protocolos TCP/IP.

Debido a la complejidad y tamaño de la red, se describe únicamente la parte que concierne a la tesis, es decir, las conexiones de los equipos que conforman el backbone y la forma en cómo interactúan para posteriormente poder entender el comportamiento que presentan en el enrutamiento de datos. El objetivo que se pretende alcanzar en este capítulo, está más enfocado a la parte del enrutamiento de datos; por lo que la parte referente a enlace de datos se mencionará de manera somera.

II.3 Nivel de transporte

A grandes rasgos, la capa encargada del transporte de información de la red UNAM cuenta con un core, una capa de distribución y una de acceso.

Core

Se maneja un backbone de ATM debido a que posee las siguientes ventajas: integración de servicios (voz, datos y video), mayor ancho de banda (155 Mbps), posibilidades de escalabilidad, redundancia en enlaces, etc. Sin embargo, la tecnología ATM no es completamente compatible con las tecnologías de redes LAN, por lo que se hace necesario usar un mecanismo que permita la interacción de ambas, es decir, emular redes LAN o LANEmmulation. LANE es el método para permitir a los dispositivos de redes locales comunicarse sobre ATM sin realizar cambios en protocolos de capaz superiores y software de aplicación (LANE se explica más a detalle en el capítulo anterior).

Distribución

Debido a que la tecnología ATM es muy costosa para hacerla llegar a las dependencias, y además de que las dependencias de la UNAM en su mayoría cuenta con redes Ethernet, se optó por seleccionar la tecnología Fast Ethernet como medio para conectar las dependencias hacia el core (capa de distribución). Fast Ethernet ofrece las ventajas de costos aceptables, compatibilidad con las redes LAN y debido a que es una tecnología switcheada, nos permite mejorar el manejo de trafico de broadcast.

Acceso

Casi todos los equipos de cómputo de las dependencias de la UNAM poseen tarjetas de red con tecnología Ethernet, de modo que éstos al conectarse a RedUNAM hacen uso de esta tecnología (capa de acceso). La capa de acceso se refiere a la interfaz final hacia el usuario.

De lo anterior, la estructura global de RedUNAM se observa en la figura 2.1.

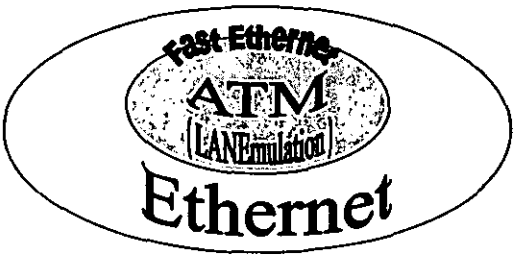


Figura 2.1 Esquema del funcionamiento global en capa 2 de RedUNAM

Ahora que se ha dado la idea general de la estructura de transporte, se procede a describir el funcionamiento de RedUNAM de acuerdo a los equipos que la integran y a las funciones que realizan dentro de cada una de las capas (core, distribución, acceso). Los principales equipos son: Passport 160 (core), CELLplex 7000 (core, distribución, acceso), CoreBuilder 2500 (distribución y acceso).

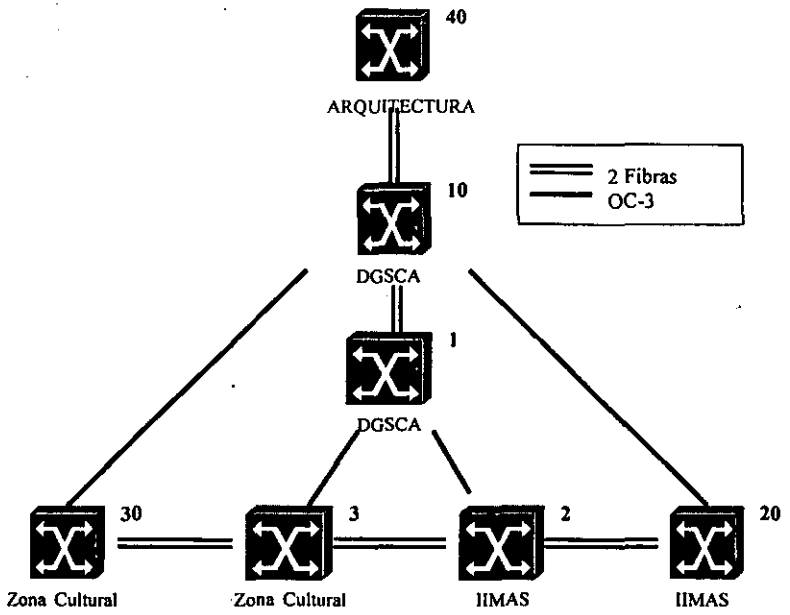


Figura 2.2 Backbone ATM de RedUNAM

Switches ATM Passport 160

Los equipos 1, 2, 3 son switches ATM del modelo Passport 160 marca Nortel con interfaces de OC-3 ATM para datos, E1s para voz y video, y Frame Relay para la interfaz de administración del equipo. Este equipo conforman el backbone o core de servicios integrados de RedUNAM. Como únicamente nos concierne la parte de datos, sólo se tomarán a los equipos Passport como equipos de transporte de celdas ATM y no se profundizará en ellos.

Switches ATM/LAN CELLplex 7000

Por el contrario, los equipos representados con los números 10, 20, 30, 40 de la figura 2.2 dedicados a datos, son switches ATM/LAN CELLplex 7000 de la marca 3Com que provee servicios de las tres capas por medio de las interfaces:

- OC-3 de ATM que proveen el transporte de información en celdas ATM (core).
- Fast Ethernet para la conexión hacia los switches CoreBuilder 2500 (capa de distribución).
- Ethernet para 22 redes LAN de las diferentes facultades, dependencias e institutos internos de la UNAM (capa de acceso).

Las características de los equipos CoreBuilder 2500 se explicaran más adelante.

Como se observa el CELLplex 7000 tiene funciones en el core, en la distribución y en el acceso. Por lo anterior, también provee los servicios de LANE ya que provee la interacción de las redes LAN de la UNAM con el core ATM.

Funcionamiento de LANE en el CELLplex 7000

En RedUNAM, la emulación de redes LAN (LANE) funciona de la siguiente manera:

- Dentro de la nube ATM existen dispositivos con interfaces tanto de ATM como Ethernet o Fast Ethernet (CELLplex 7000), que implementan los servicios de LANE (LECS, LES, BUS, LEC vistos en el capítulo I).
- Estos equipos permiten crear redes virtuales dispersas geográficamente, llamadas ELANs.
- Cada ELAN actúa de manera análoga a un dominio de broadcast. [1]
- Todo equipo conectado a una interfaz Ethernet o Fast Ethernet del CELLplex tiene configurado una ELAN.
- RedUNAM soporta 64 ELANs; cada uno de los cuatro CELLplex aloja 16 ELANs.
- De las 64 ELANs, actualmente sólo operan 23 de ellas.
- 22 de ellas están asignadas a 22 dependencias internas de RedUNAM.
- La restante, es la ELAN de administración.
- La ELAN de administración funge como backbone o core para todas las redes de las dependencias de la UNAM, ya que conecta a todos los equipos LAN (switches LAN, switches capa 3 y enrutadores) necesarios para brindar el funcionamiento sobre TCP/IP de RedUNAM.
- Dicha ELAN es el punto donde toda la información de los diferentes segmentos debe de circular para alcanzar algún segmento diferente e inclusive la salida hacia Internet (a excepción de las dependencias que se conectan dentro de un mismo CoreBuilder 2500). Estos equipos se explican más adelante.

Las ventajas que provee esta configuración a través de LANE dentro de la UNAM son:

- Mayor velocidad de transmisión (155 Mbps).
- Reducción en los costos debidos a cambios y movimientos de dependencias, ya que con la creación de redes emuladas, si alguna dependencia se cambia de edificio o crece su red a un nuevo edificio, los cambios sólo se llevan a cabo en la configuración de los CELLplex 7000 sin realizar ningún cambio físico.
- Mayor rapidez en el caso de tener la red de determinada dependencia segmentada y separada geográficamente, ya que se elimina el uso de equipos de capa 3: enrutadores "switchear es más rápido y barato que enrutar".
- Creación de grupos de trabajo dispersos, tal es el caso de la ELAN de administración, ya que tiene configurados equipos en diferentes partes geográficas del campus universitario.
- De lo anterior tenemos una operación y administración centralizada de todos los equipos de backbone en una sola ELAN.
- Capacidad de escalamiento en la velocidad de transmisión, ya que ATM nos provee la característica de incrementar en ancho de banda a diferencia de las redes LAN.

[1] Un dominio de broadcast es un conjunto de máquinas que reciben un paquete tipo broadcast enviado por cualquiera de las máquinas. Un dominio de broadcast generalmente corresponde a una subred.

Como se ha venido explicando, la ELAN de administración permite la interconexión de todos los equipos que intervienen en el enrutamiento en un sólo segmento de broadcast, lo que permite que la comunicación entre todos ellos sea una comunicación de punto a punto para ofrecer un mejor servicio de distribución y por consiguiente un mejor enrutamiento.

Como se mencionó anteriormente, existen 22 dependencias, representadas por las nubes en la figura 2.3, conectadas a uno de los puertos del CELLplex 7000 y configuradas a una ELAN diferente de la de administración. Estas dependencias representan la capa de acceso dentro del CELLplex.

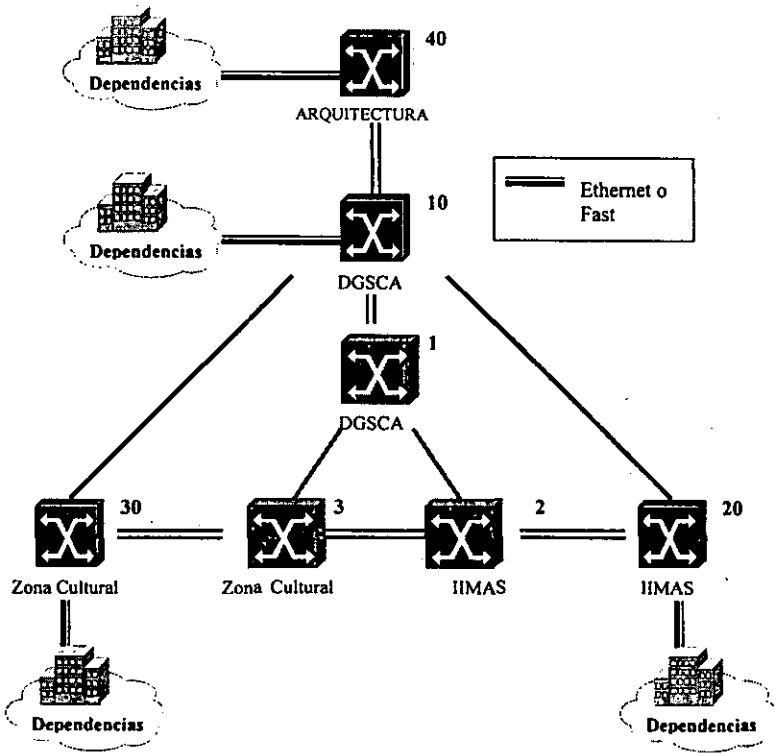


Figura 2.3 Dependencias internas en el CELLplex 7000

Switches LAN CoreBuilder2500.

En la capa de acceso a RedUNAM, la mayor parte de los institutos, facultades y dependencias de la UNAM se conectan a través de uno o varios segmentos de red Ethernet, dependiendo del número de equipos DTEs que posea dicha dependencia. Estos segmentos de red se encuentran conectados a través de un switch LAN con capacidades de enrutamiento modelo CoreBuilder2500 de la marca 3Com (aunque su nombre comercial anterior era LANplex 2500). Dicho equipo cuenta con una interfaz de Fast Ethernet para llevar a cabo la capa de distribución de las dependencias y comunicarlas hacia el core.

Para dar un ejemplo de la capa de acceso, en la siguiente figura se observa que toda dependencia se conecta a través de un hub o switch a un puerto Ethernet en el CoreBuilder2500. Éste puerto puede ser de fibra óptica o UTP dependiendo de la distancia geográfica entre el CoreBuilder 2500 y la dependencia. Por otra parte, la capa de distribución al core se realiza a través de un puerto Fast Ethernet configurado en la ELAN de administración.

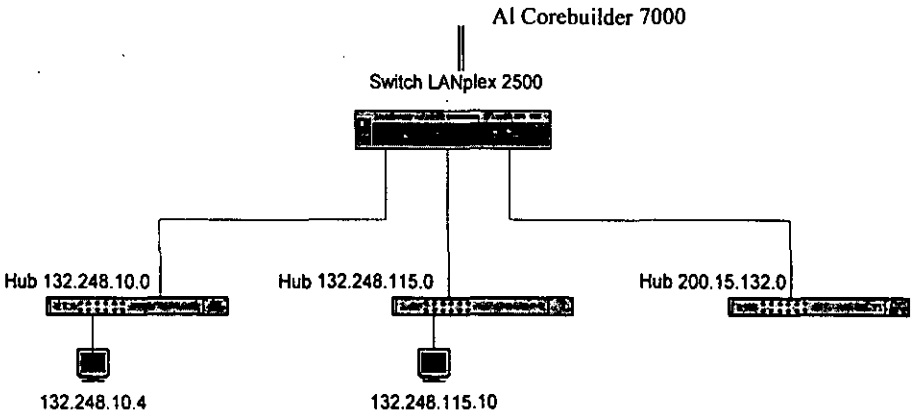


Figura 2.4 Dependencias dentro del CoreBuilder 2500

En conjunto, los 26 CoreBuilder 2500 con que cuenta la Universidad (conectados de los equipos representados con los números 10, 20, 30, y 40 en la figura 2.3), cada uno de ellos cuenta en promedio con 5 segmentos de red Ethernet (5 dependencias) para dar servicio a un total de 99 dependencias. Estos equipos están repartidos dentro de los cuatro nodos de telecomunicaciones de la UNAM como sigue:

- Nodo DGSCA con 7 CoreBuilder 2500.
- Nodo Zona Cultural con 4 CoreBuilder 2500.
- Nodo IIMAS con 8 CoreBuilder 2500.
- Nodo Arquitectura con 6 CoreBuilder 2500.

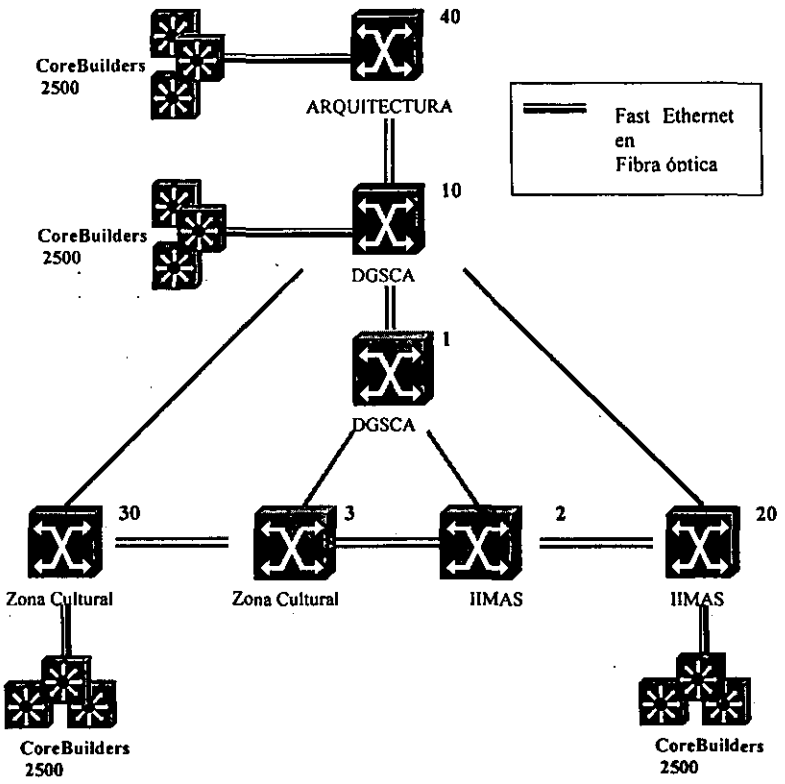


Figura 2.5 CoreBuilder 2500 en el Backbone

Las interfaces de conexión entre los CoreBuilder 2500 y los CELLplex son a través de tecnología Fast Ethernet con la finalidad de brindar una distribución de la información de todas las dependencias conectadas al CoreBuilder 2500 con un ancho de banda adecuado. La interfaz Fast Ethernet que conecta al CoreBuilder 2500 con el CELLplex se configura a la ELAN de administración, por lo que todos los CoreBuilder 2500 pertenecen a la misma red emulada, o lo que es lo mismo, la comunicación que establecen entre ellos es de punto a punto con la finalidad de lograr un óptimo enrutamiento de información entre las dependencias.

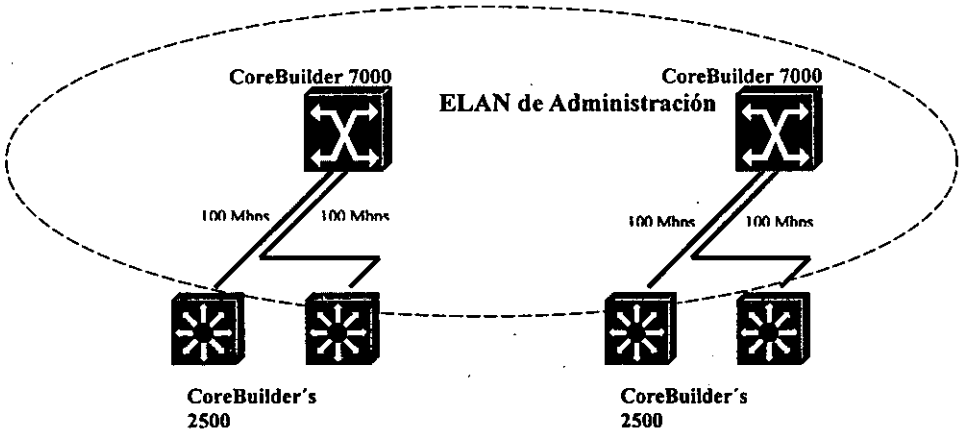


Figura 2.5 Conexión entre equipos CPX y CoreBuilder 2500

Sin embargo, todas éstas dependencias requieren establecer comunicación con las demás e inclusive con el resto de Internet, por lo que es necesario implantar servicios de enrutamiento de datos a través de TCP/IP.

II.4 Nivel de enrutamiento

En el ámbito de enrutamiento, la RedUNAM cuenta con un conjunto de redes de instituciones externas e internas[2], además de las conexiones a Internet. Actualmente la UNAM cuenta con 84 enlaces hacia instituciones externas y 71 a instituciones internas, además de 11 enlaces internacionales (9 enlaces E1s y 2 T1s) para brindar un ancho de banda de 21 Mbps aproximadamente de salida a Internet. Todo esto se explica con mayor detalle a lo largo de éste capítulo. Pero antes de profundizar en el tema de enrutamiento, y recordando que RedUNAM trabaja con protocolos de enrutamiento que hacen uso de la tecnología TCP/IP, es necesario hablar acerca de la asignación de las subredes IP dentro de la UNAM.

Todas las ELANs y las redes Ethernet de las diferentes dependencias tienen asignado un segmento de red para proveer el enrutamiento de información de TCP/IP entre ellas. Como se menciono en el Capítulo I, la RedUNAM cuenta con dos redes clase B la 132.248.0.0 y la 132.247.0.0, además del bloque de direcciones clase C de la 200.15.1.0 a la 200.15.254.0 asignada por la Universidad de Rice para ser administrada por la UNAM, es decir, en calidad de préstamo.

La red 200.15.0.0 está asignada a redes de instituciones externas, cuando hablamos de instituciones externas nos referimos a las redes ajenas a la UNAM como pueden ser hospitales,

[2] Para mayor información de las dependencias conectadas a RedUNAM consultar los URLs http://www.dtd.unam.mx/REDUNAM/inst-externas.html y http://www.dtd.unam.mx/REDUNAM/nodos.html.

escuelas particulares, instituciones gubernamentales, etc. La red 132.247.0.0 no está asignada actualmente, y para el caso de la red 132.248.0.0, para hacer mejor uso de ésta red clase B se hace necesario subnetearla; para lo cual se utiliza la mascara de red 255.255.255.0 o mascara de 24 bits. La mascara de 24 bits nos genera 255 subredes (ver capítulo I para mayor detalle) de la 132.248.0.0 a la 132.248.255.255. Con excepción de la 132.248.0.0 usada como identificador de la red clase B y la 132.248.255.255 dirección de broadcast de la red clase B, las demás subredes están asignadas a dependencias internas de la UNAM; por dependencias internas nos referimos a todas las redes de instituciones que dependen directamente de la UNAM como lo son facultades, institutos de investigación, CCHs, preparatorias, FESs.

Sin embargo, el subnetear la red implica separar la red en segmentos completamente independientes en el nivel de enrutamiento. Así, aunque se mejoró el direccionamiento IP para la red clase B 132.248.0.0 ahora se tiene el problema de comunicar diferentes subredes. Para resolver lo anterior, se hace necesario implantar enrutamiento entre los diferentes segmentos de dependencias a través de equipos enrutadores. A éstos equipos se les asigna la última dirección de cada subred, la 254 (ejemplo 132.248.*.254, donde * puede ser de la 1 a la 254). Dentro de las redes internet (redes que hacen uso del protocolo TCP/IP), a este equipo se le conoce como Default Gateway, ya que permite la comunicación entre varias sudredes independientes.

Por lo anterior, hay tres cosas importantes que recordar en el enrutamiento de información en IP para todos los equipos:

Dirección de Subred:
Cualquier dirección que termine en cero, 132.248.[1-254].**0**.
Dirección IP:
Puede ir de la 132.248. **[1-254]**.**[1-253]**.
Default Gateway:
Dirección asignada a un enrutador con terminación 254, 132.248.[1-254].**254**.
Mascara de red:
Para subtenear la clase B en RedUNAM se utiliza **255.255.255.0** o mascara de 24 bits.

La RedUNAM para fines de administración y de enrutamiento tiene asignada toda la subred 132.248.254.0 a la ELAN de administración y dentro de ella se encuentran todos los equipos encargados del enrutamiento.

La estructura general de enrutamiento de la RedUNAM es un sistema plano o lineal. Como se mencionó en el capítulo anterior, en este enrutamiento todos los equipos con función de enrutamiento son peers o vecinos, es decir, se encuentran en un mismo dominio de broadcast como se muestra en la figura 2.6.

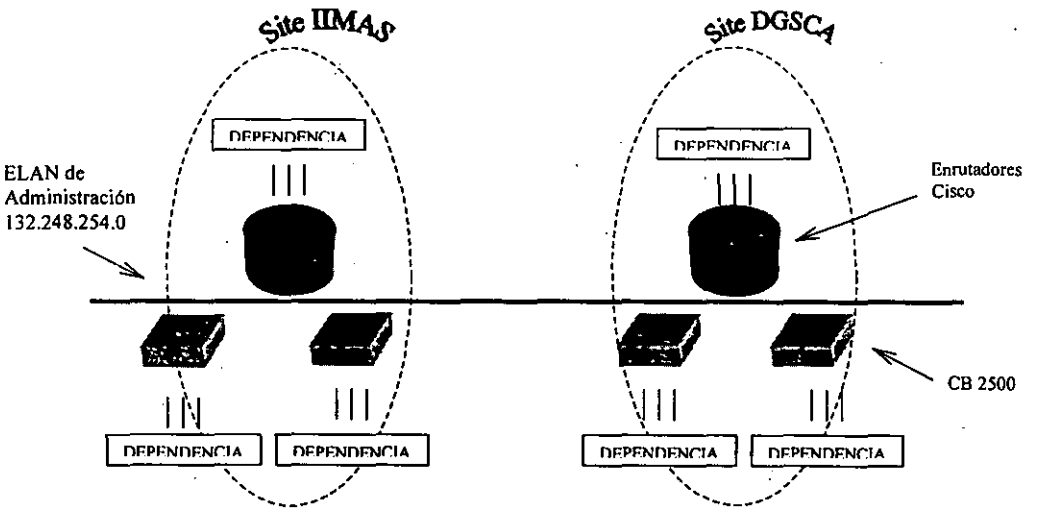


Figura 2.6 Esquema del funcionamiento global de enrutamiento de RedUNAM

Como se puede observar, las dependencias internas se encuentran conectadas en los puertos de los equipos CoreBuilder 2500; las dependencias conectadas al CELLplex y configuradas a una ELAN diferente a la de administración se representan conectadas a los Cisco (que es la forma en como se comportan a nivel de enrutamiento como se verá más adelante). La ELAN de administración está representada por el segmento de red que interconecta a los equipos que poseen capacidades de enrutamiento (Ciscos y CoreBuilder 2500). El enrutamiento de información entre las diferentes dependencias puede ser de distintos tipos:

- Dependencias conectadas en un mismo CoreBuilder 2500.
- Dependencias conectadas en los CELLplex.
- Dependencias conectadas en los Cisco.

Dependencias conectadas dentro del mismo CoreBuilder 2500.

Los CoreBuilder 2500 no llevan a cabo el proceso de enrutamiento de información ya que actualmente no poseen la configuración necesaria (aunque es capaz de hacerlo); por el contrario, cuentan con una configuración de ruta estática hacia un equipo que sí esté ejecutando un proceso de enrutamiento (cualquier equipo Cisco).

A pesar de esto, los equipos de computo (PC's, workstation, etc.) de 99 dependencias de la UNAM poseen configurado como Default Gateway a un CoreBuilder 2500, por poseer características de enrutamiento. Este equipo es capaz de identificar únicamente el tráfico que tenga como destino un segmento de subred dentro del mismo switch y lo enruta por el puerto adecuado.

Por ejemplo, como se observa en la figura 2.7, si la máquina 132.248.10.4 desea comunicarse con la máquina 132.248.115.10, el switch será capaz de encaminar los paquetes por el puerto correspondiente.

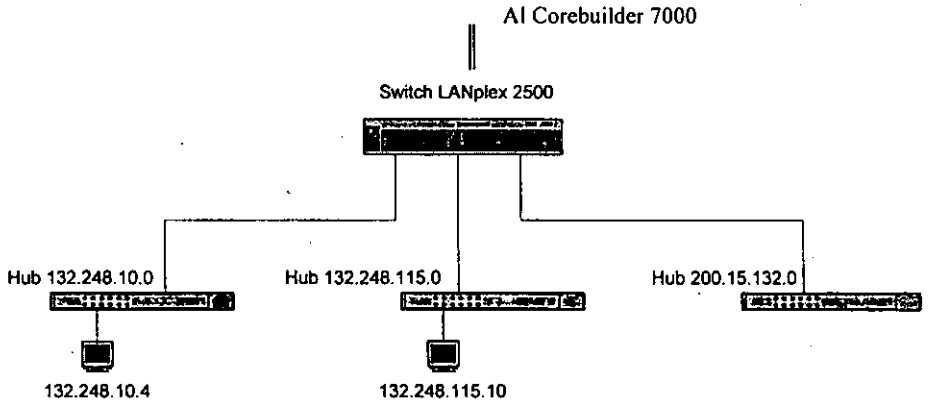


Figura 2.7 Dependencias dentro del CoreBuilder 2500

La forma en como el CoreBuilder 2500 decide hacia donde enviar la información es a través de una tabla de enrutamiento. Esta tabla contiene las redes o subredes que tiene directamente conectadas (para este caso las subredes 132.248.10.0, 132.248.115.0 y la 200.15.132.0), adicionalmente posee una ruta estática hacia su salida o ruta por default (el Cisco) utilizada para enviar la información cuando no tiene directamente conectada la red destino. Por lo tanto todo el enrutamiento de las dependencias que se conectan a un CoreBuilder 2500 y tiene como destino una red fuera del mismo depende totalmente del Cisco, éste es el que se encarga de enrutarlas a cualquier parte de RedUNAM e inclusive de Internet. Un ejemplo de la tabla de enrutamiento dentro de un CoreBuilder 2500 es la siguiente:

Destination	*Subnetmask*	*Metric*	*Gateway*	*Status*
Default Route	--	--	*132.248.254.254*	*Static*
132.248.10.0	*255.255.255.0*	--	--	*Direct*
132.248.115.0	*255.255.255.0*	--	--	*Direct*
132.248.254.0	*255.255.255.0*	--	--	*Direct*
200.15.132.0	*255.255.255.248*	--	--	*Direct*

Tabla de enrutamiento

Dependencias conectadas dentro de los CELLplex

Existen 22 dependencias internas de RedUNAM que se encuentran directamente conectadas a los puertos Ethernet/Fast Ethernet de los equipos CELLplex. Cada uno de los puertos del CELLplex es un Cliente de LANEmmulation (LEC). El Cisco por su parte posee una interfaz ATM, lo que

permite crear múltiples LECs (conocidos como interfaces virtuales ATM). Todo LEC debe ser configurado a una ELAN.

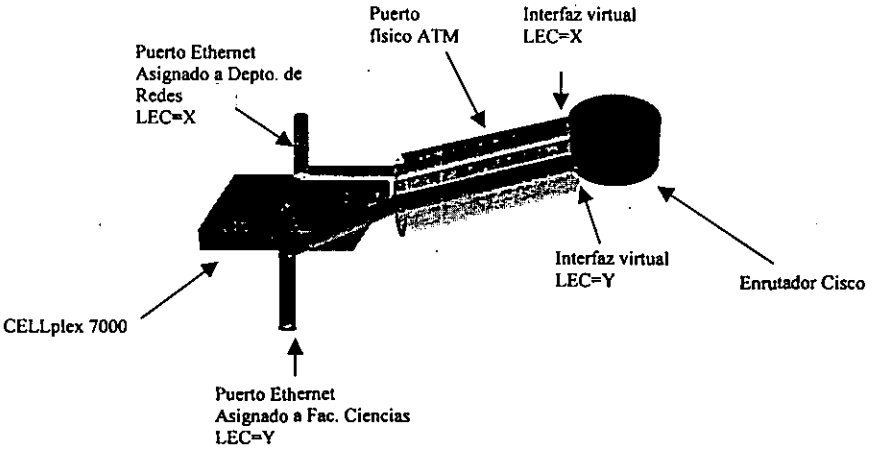


Figura 2.8 Vista física de las diferentes ELANs

Una vez que el/los puertos del CELLplex y una interfaz virtual del Cisco se asocian a una misma ELAN, a ésta se le asigna una subred IP dentro del rango 132.248.1.0 — 132.248.253.0. De lo anterior, la conexión a través de LANE emulando una red 802.3, antes explicada, nos permite una topología lógica muy parecida a la de un segmento físico Ethernet; como se muestra a continuación:

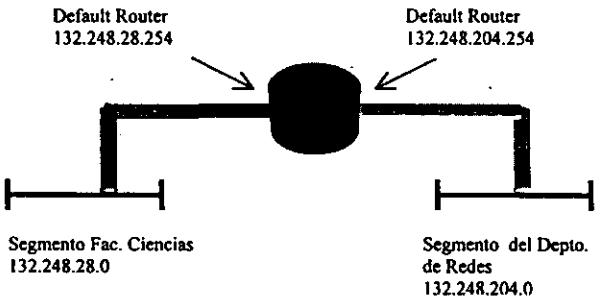


Figura 2.9 Vista lógica de las diferentes ELANs

En la figura 2.9, se muestra que todas las subredes de las dependencias conectadas al CELLplex poseen su Default Gateway en un puerto virtual ATM dentro del Cisco.

Por lo tanto, la forma en como trabajan el enrutamiento en las dependencias conectadas a los CELLplex es muy similar a la que se presenta en un segmento Ethernet, si un equipo que se

conecta en un puerto del CELLplex quiere comunicarse con cualquier equipo en algún otro segmento, a través de LANE buscará el puerto de su Default Router en el Cisco para que este lo encamine a algún otro puerto virtual ATM, un puerto físico Ethernet, FDDI e inclusive a través de un puerto serial hacia alguna red externa a RedUNAM.

Cabe destacar que cuando se forma una ELAN, los clientes de LANE (LEC) pueden estar distribuidos geográficamente, lo que significa que el(los) puerto(s) del CELLplex asignado(s) a la dependencia y la interfaz virtual dentro del puerto ATM del Cisco pueden estar geográficamente separados. Tal es el caso de la ELAN de administración.

La topología lógica y física explicada anteriormente se presenta también en los equipos de la ELAN de administración. Todos los equipos que se conectan a los CELLplex —CoreBuilder 2500, equipos de monitoreo y los equipos de acceso remoto— y algunas interfaces virtuales dentro de los Cisco se configuran a la ELAN de administración. A esta ELAN se le asigna el segmento de red 132.248.254.0, de forma que todos los equipos dentro de la ELAN deben poseer una dirección dentro de dicho segmento como, se muestra a continuación:

EQUIPOS	DGSCA	IIMAS	Zona Cultural	Arquitectura
CELLplex	132.248.254.40	132.248.254.30	132.248.254.20	132.248.254.10
CoreBuilder 2500	132.248.254.240 a 132.248.254.246 (7 CoreBuilder 2500)	132.248.254.230 a 132.248.254.237 (8 CoreBuilder 2500)	132.248.254.220 a 132.248.254.223 (4 CoreBuilder 2500)	132.248.254.210 a 132.248.254.215 (6 CoreBuilder 2500)
Cisco	132.248.254.254	132.248.254.253	132.248.254.252	132.248.254.251

La clasificación anterior es importante por que permite entender el esquema de enrutamiento dentro de RedUNAM. Todos los equipos que se conectan dentro de un CELLplex deben mantener el patrón de direcciones IP de acuerdo a ese CELLplex. Por ejemplo si el CELLplex tiene la dirección 132.248.254.**40**, todos los CoreBuilder 2500 que se conecten a él deben conservar un direccionamiento del 132.248.254.**240** al 132.248.254.**246** y como se mencionó anteriormente, los CoreBuilder 2500 cuentan con una configuración de ruta estática hacia un equipo de enrutamiento, un equipo Cisco, éste tiene la dirección132.248.254.**254.** Como se observa, todas las direcciones de los equipos dentro de un CELLplex (DGSCA en este caso) conservan el patrón de: 40, 240's, 254. Para el caso de Zona Cultural el patrón será: 20. 220's, 252.

Las interfaces virtuales ATM dentro del Cisco, configuradas para las dependencias dentro de un CELLplex, se configuran dentro del equipo de enrutamiento más cercano. Por ejemplo, si la red de la Subdirección de Redes y Comunicaciones (segmento 132.248.204.0) se encuentra conectada en el CELLplex de DGSCA, la interfaz virtual se debe configurar dentro del Cisco conectado en DGSCA, el 132.248.254.254. De esta forma la interfaz virtual dentro del Cisco DGSCA tendrá asignada la dirección 132.248.204.254.

De manera análoga, los CoreBuilder 2500 tendrán configurado como Default Gateway al Cisco que tengan más cercano, así, todos los CoreBuilder 2500 de DGSCA tendrán configurado al

132.248.254.254; para los CoreBuilder 2500 de Zona Cultural su Default Gateway será el 132.248.254.252.

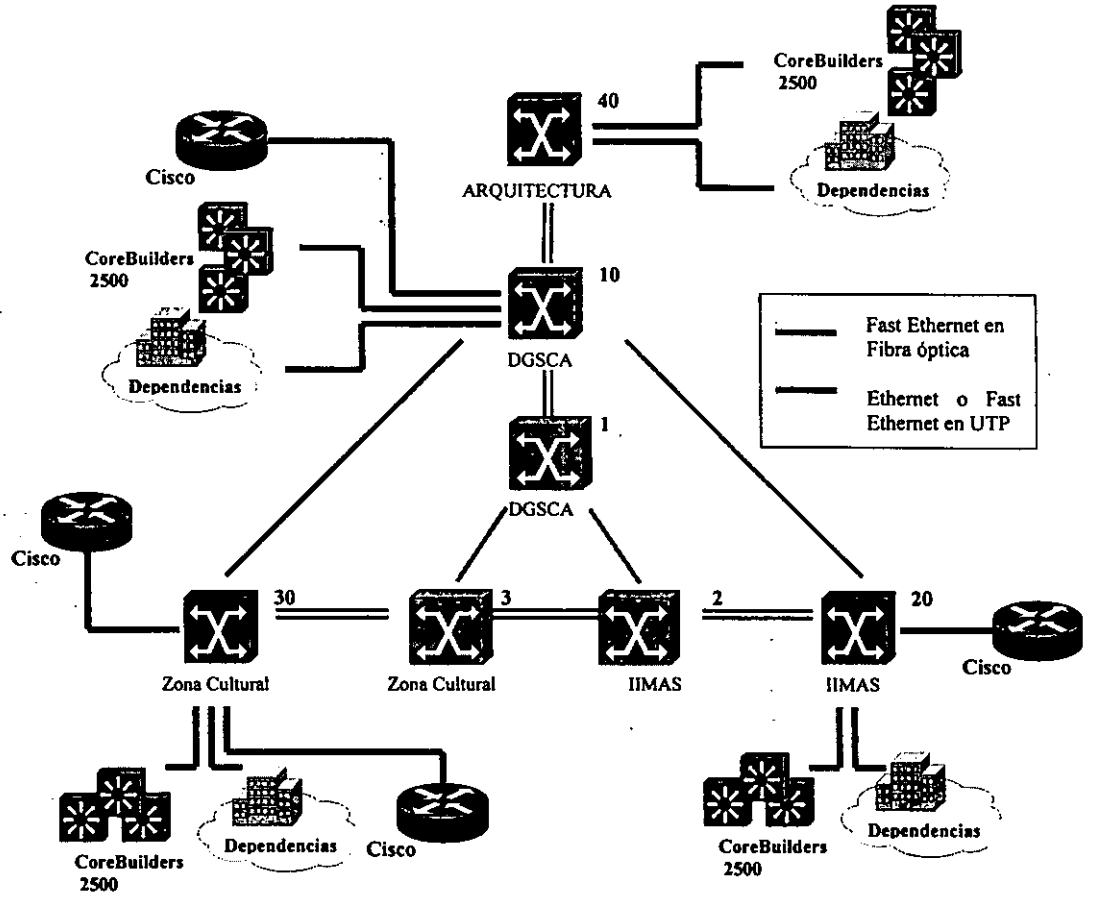


Figura 2.10 Backbone de enrutamiento con equipo cisco

Dependencias conectadas dentro de los Cisco

Dentro de ésta categoría entran las dependencias conectadas al CELLplex y las físicamente conectadas por un puerto Ethernet o serial al Cisco. Todos estos casos presentan el mismo comportamiento.

Ya que los equipos ATM CELLplex, puertos Ethernet y puertos seriales sólo brindan el transporte de la información para las dependencias conectadas a ellos, se hace necesario contar con equipo que brinden la capacidad de enrutamiento de paquetes a través de TCP/IP —este

mismo equipo funge como Default Gateway para los switches CoreBuilder 2500 que, como se mencionó anteriormente, no tienen configurado el proceso de enrutamiento—. Estos son los enrutadores marca Cisco que integran el backbone de enrutamiento de RedUNAM y que se muestra en la figura 2.11.

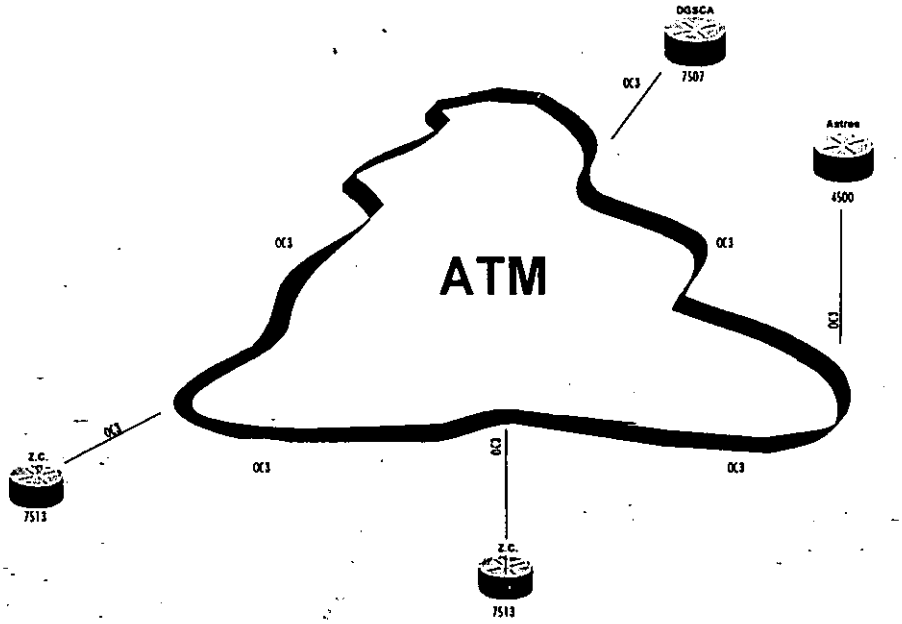


Figura 2.11 Enrutadores principales en RedUNAM

Los enrutadores de RedUNAM permiten comunicar a los segmentos de diferentes dependencias internas y externas e institutos a la UNAM entre sí—es decir, segmentos que se encuentran conectados a los diferentes equipos CELLplex, CoreBuilder 2500 y Cisco— y a su vez con el resto del mundo con conexiones internacionales a Internet. La forma en que estos equipos llevan a cabo el enrutamiento de información es a través del intercambio de información de enrutamiento, con el fin de que todos los enrutadores pertenecientes al Sistema Autónomo de la UNAM tengan las rutas para poder llegar a cualquier otra red, sea dentro o fuera de la UNAM.

Los enrutadores Cisco tienen configurado dos tipos de enrutamiento: estático y dinámico. Esta configuración se debe a las diversas necesidades que se presentan en RedUNAM; la gran extensión geográfica, complejidad y diversidad de equipos que existen dentro de ésta.

II.4.1 Enrutamiento estático

El enrutamiento estático dentro de RedUNAM se establecido configurado entre los Cisco y los CoreBuilder 2500; ya que estos últimos no están configurados para mantener una sesión de enrutamiento con los Cisco, dado que no hablan el mismo lenguaje o protocolo de enrutamiento.

Para que se lleve a cabo este tipo de enrutamiento es necesario configurar rutas estáticas en ambos equipos de todas y cada una de las redes configuradas en un CoreBuilder 2500.

Hay que recordar que un enrutador con rutas estáticas reenvía la información a un equipo predeterminado. Esto se lleva a cabo gracias a que se configura en el cisco, una relación entre la red destino y el puerto o equipo por el cual puede llegar a esa red. Un ejemplo de esta configuración estática en RedUNAM es la siguiente:

ip route 132.248.10.0 255.255.255.0 132.248.254.243
ip route 132.248.11.0 255.255.255.0 132.248.254.237

Dicha configuración se ve reflejada en la tabla de enrutamiento de la siguiente manera:

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

Gateway of last resort is 200.33.209.9 to network 200.33.208.0

B 170.170.37.0 [200/0] via 207.248.130.142, 10:44:02
S 132.248.10.0/24 [1/0] via 132.248.254.243
S 132.248.11.0/24 [1/0] via 132.248.254.237

Donde:
S = Indica que es una ruta estática.

Como se puede observar, la dirección 132.248.254.243 pertenece a un equipo CoreBuilder 2500 en DGSCA y 132.248.254.237 a uno en IIMAS. Debajo de ellos se encuentran la red 132.248.10.0 y la 132.248.11.0 respectivamente, cuando cualquier paquete que sea procesado por un Cisco y tenga como destino cualquier red perteneciente al segmento 10 o al segmento 11, el enrutador ya sabe a que CoreBuilder 2500 reenviarlo.

Este tipo de enrutamiento presenta muchas desventajas, como son:

- Actualización constante por parte del administrador de las tablas de enrutamiento estático.
- Subutilización de las capacidades de enrutamiento de los equipos CoreBuilder 2500.
- Sobrecarga en el procesamiento de los enrutadores principales en horas pico, lo que puede hacer que éstos fallen.
- Si uno de los Cisco falla, los CoreBuilder 2500 que dependen de cada uno de ellos quedan sin servicio de red.
- En el caso de que falle un Cisco con salida a Internet, gran parte del ancho de banda internacional se pierde.

Sin embargo existen beneficios en el uso de éstas:

- Por ejemplo, las rutas programadas estáticamente ayudan a tener una red más segura, ya que existe una ruta única tanto para entrar como para salir de dicha red o subred.

La configuración que se presenta para rutas estáticas en los equipos CoreBuilder 2500, donde todos y cada uno de ellos posee una ruta hacia un Cisco dentro del mismo site, se mencionó anteriormente.

II.4.2 Enrutamiento dinámico

El proceso de enrutamiento dinámico se presenta con las instituciones externas a la UNAM y en los enlaces hacia Internet. El protocolo que se está utilizando para llevar a cabo el enrutamiento de paquetes dentro del backbone de enrutadores de RedUNAM es el protocolo propietario de CISCO: IGRP. *En las dependencias internas no se está trabajando con este proceso de enrutamiento debido a que IGRP es propietario y ningún equipo 3COM puede entenderlo.*

Este proceso de enrutamiento se encuentra trabajando en todos los enrutadores administrados por la UNAM. Como se mencionó anteriormente, los algoritmos de enrutamiento dinámico van ajustando las rutas en tiempo real, gracias a que analizan los mensajes de actualización de rutas. Una ventaja de este tipo de algoritmos, es que permite la implantación de rutas estáticas cuando éstas sean necesarias, como es el caso presentado anteriormente.

Un ejemplo de enrutamiento dinámico en los equipos Cisco se presenta en la siguiente tabla de enrutamiento:

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

Gateway of last resort is 200.33.209.9 to network 200.33.208.0

S 132.248.11.0/24 [1/0] via 132.248.254.237
I 200.15.55.0/24 [100/160358] via 132.248.254.249, 00:00:32, ATM0/0.1
I 200.15.80.0/24 [100/158358] via 200.15.3.108, 00:00:34, ATM0/0.1
[100/158358] via 192.100.199.28, 00:00:34, ATM0/0.1
[100/158358] via 192.100.200.76, 00:00:34, ATM0/0.1
[100/158358] via 132.247.254.252, 00:00:34, ATM0/0.1
I 200.15.20.0/24 [100/158550] via 192.100.199.99, 00:00:00, Ethernet4/3
I 192.100.164.0/24 [100/41162] via 192.100.199.34, 00:00:00, Serial6/3

Donde:

S = Indica que es una ruta estática.
I = Indica que es una ruta aprendida por el algoritmo de enrutamiento IGRP.

Como podemos observar en la tabla anterior, para poder llegar a una máquina perteneciente a la red 200.15.55.0 es necesario reenviar la información a un siguiente enrutador con dirección IP 132.248.254.249 a través de la interfaz virtual ATM0/0.1[3] y el segundo enrutador puede o no tener directamente conectada dicha red, en caso de tenerla conectada directamente lo envía por el puerto adecuado, en caso contrario realiza el mismo proceso de reenvío hacia otro enrutador, para de esta manera llegar al destino.

En el caso de querer llegar a la red 200.15.80.0 como se puede observar existen cuatro opciones en la tabla de enrutamiento por la cual podemos llegar a dicha red, estas son a través de los siguientes enrutadores: 200.15.3.108, 192.100.199.28, 192.100.200.76 y el 132.247.254.252; todas a través de la interfaz virtual ATM0/0.1. Este tipo de configuración se debe gracias a que IGRP es un protocolo de enrutamiento muy sofisticado que acepta múltiples rutas para un mismo destino, a éste tipo de algoritmos se les llama Multipath (ver Capítulo I).

RedUNAM brinda a muchas instituciones externas la salida hacia Internet, por lo que RedUNAM es un ISP (Internet Service Provider), es decir, provee acceso a Internet por medio de convenios a universidades, escuelas y dependencias gubernamentales externas a la UNAM que requieran conectarse a RedUNAM, también provee la asesoría técnica para la adquisición de equipo, medios de enlace y software.

Dos requisitos técnicos que las dependencias deben cubrir son: Contratar con un carrier (Telmex, Avantel, etc.) un enlace TDM dedicado que puede ser desde un DS0 hasta un E1 completo y contar con un equipo que provea los servicios de enrutamiento.

La conexión es muy sencilla, se colocan dos enrutadores en ambos extremos del enlace, por lo general la UNAM provee uno de los puertos dentro de los enrutadores de backbone. Existen algunos casos en los cuales las dependencias externas no cuentan con enrutadores marca Cisco, por lo que es necesario configurar el protocolo de enrutamiento estándar RIP en el enrutador de la dependencia externa así como en el enrutador de la UNAM que reciba la conexión. Sin embargo se requiere de una redistribución de rutas entre protocolos con el fin de anunciar las redes tanto de las dependencias externas hacia RedUNAM como las redes de RedUNAM e Internet hacia las dependencias. Todo este procedimiento tiene como objetivo que las redes de las dependencias sean alcanzables por todo equipo de cómputo en cualquier parte de la Internet y viceversa.

Aunque se tiene configurado lo necesario para llegar a cualquier red conectada directamente a RedUNAM a través de enrutamiento estático y los protocolos RIP e IGRP, se hace necesario configurar en los enrutadores un protocolo de compuerta externa que permita comunicar el Sistema Autónomo de la UNAM con otros para que todas las redes de RedUNAM y las redes de las instituciones que dependen de ella, sean anunciadas al resto del mundo. Esto se hace a través del protocolo estándar BGP (Border Gateway Protocolo).

Existen dos tipos de BGP; iBGP y eBGP. Enrutadores que pertenecen al mismo Sistema Autónomo de la UNAM e intercambian información de BGP, están hablando BGP interno (iBGP). Enrutadores que pertenecen a un diferente Sistema Autónomo de la UNAM e intercambian información de BGP, la hacen a través de BGP externo (eBGP).

[3] Notación que se refiere a la tarjeta en el slot ATM cero, al puerto ATM cero e interfaz virtual 1.

Antes de intercambiar información de enrutamiento con un Sistema Autónomo externo, BGP se asegura que todas las redes dentro de su Sistema Autónomo sean alcanzables, por lo que se hace necesario:

- Tener una configuración full-mesh (conexión en malla de todos contra todos) entre los enrutadores que hablan iBGP dentro del Sistema Autónomo a través de IGPs.

- Redistribuir rutas de IGP a BGP (y viceversa) del Sistema Autónomo, es decir, RIP e IGRP a BGP para el caso de RedUNAM.

Una vez que todas las redes internas de RedUNAM son conocidas por los enrutadores que tienen configurado el proceso de iBGP, se utiliza eBGP para anunciarlas a su(s) vecino(s) externo(s). De esta forma todas las redes que dependen de RedUNAM son anunciadas al resto del mundo. Un proceso similar realizan los demás Sistemas Autónomos de toda Internet.

Es por lo anterior que BGP solamente está configurado en aquellos enrutadores que tienen enlaces con instituciones externas que pertenezcan a un Sistema Autónomo diferente al de la UNAM.

En la figura 2.12 observamos que tres de los enrutadores de backbone tienen conexión hacia Internet, por lo tanto, cada uno de ellos tienen configurado eBGP para con sus vecinos de otros Sistemas Autónomos fuera de la UNAM e iBGP para con sus vecinos internos. En RedUNAM los enrutadores configurados con iBGP y eBGP son tres: dos enrutadores de Zona Cultural (ZC) y uno más en DGSCA.

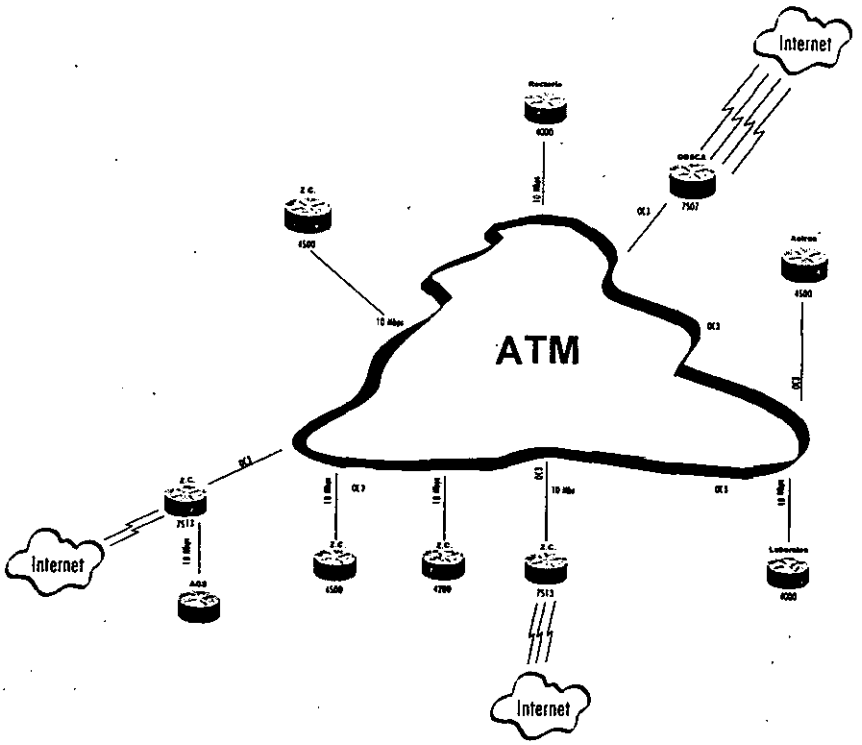


Figura 2.12 Enlaces para salida a Internet

Los enrutadores que tienen conectadas las salidas internacionales de RedUNAM poseen una configuración más robusta, es por ello que estos equipos necesitan ser de mayor capacidad de hardware con respecto a los otros enrutadores del backbone, debido a que manejan información de enrutamiento tanto de protocolos IGPs y EGPs y la redistribución que implica.

II.5 Desventajas de la estructura de enrutamiento actual

Como se ha venido observando en el transcurso de este capítulo, el esquema actual de enrutamiento presenta muchos inconvenientes. Es importante identificar cuales son estos, para tenerlos presentes y posteriormente no arrastrar estos mismos a la propuesta.

A continuación se numeran las desventajas encontradas en el esquema de enrutamiento y sus consecuencias:

- El problema del direccionamiento del bloque 200.15.0.0/16, es un problema operativo - administrativo, debido a que dicho bloque debe ser entregado a la Universidad de RICE ya que es una red no homologada, y por término de contrato, se debe de regresar a dicha Universidad. Actualmente existen muchas dependencias externas que cuentan

con direccionamiento perteneciente a este bloque, como consecuencia del término de contrato, se piensa migrar todas las instituciones involucradas a direccionamiento perteneciente al bloque 132.247.0.0/16.

- El protocolo IGRP se encuentra trabajando en el backbone y debido a las características del mismo, no permite tener una estructura jerárquica, como consecuencia se tiene un esquema de enrutamiento plano, el cual trae consigo todos los problemas que éste presenta como lo son:
  - No permite plantear un esquema de crecimiento estructurado.
  - Por ser una estructura plana es más difícil aislar los problemas que se presenten en algún momento dado.
- Al no tener configurado un protocolo estándar, existen problemas de incompatibilidad con ciertos equipos, ya que IGRP es protocolo propietario y si alguna de las instituciones no cuenta con equipo que entienda este protocolo, se hace necesario hacer una redistribución de protocolos. Esta redistribución se evitaría si se estuviera trabajando con algún protocolo estándar como lo es OSPF.
- Debido a que en el diseño de IGRP no se contempló la utilización de VLSM y CIDR, representa un problema, ya que en la actualidad una de las características para tener una mejor administración del esquema de direccionamiento es el uso de VLSM, y para ayudar a reducir el crecimiento de las tablas de enrutamiento en los equipos que conforman el backbone de Internet es necesaria la sumarización de rutas a través de CIDR. Es por esta razón que es necesario implantar algún protocolo que soporte dichas características.
- Con respecto al enrutamiento estático: En el caso de que la información dentro de un CoreBuilder 2500 tenga como destino un segmento de red conectado fuera de este equipo, el CoreBuilder 2500 no está configurado para enrutarla, debido a que cuenta con una configuración de enrutamiento estático a un gateway por default y aunque es capaz de hacerlo y originalmente estaba pensado de esa forma, no se implantó por lo incompatibilidad de RIP y el protocolo de enrutamiento del backbone, IGRP. Esta configuración trae como consecuencia:
  - Trabajo excesivo para los enrutadores Cisco (gateway por default de los CoreBuilder 2500) en horas pico.
  - Subutilización de la capacidad de enrutamiento de los equipos CoreBuilder 2500.
  - Actualización constante por parte del administrador de las tablas de enrutamiento estático.
  - Si alguno de los Cisco falla, los CoreBuilder 2500 que dependen de cada uno de ellos queda sin servicios de capa 3 de OSI.

Capítulo III

OSPF

III. OSPF

En el siguiente capítulo se presentará los orígenes, para después definir los conceptos más importantes referentes al protocolo de enrutamiento OSPF que permitan entender el funcionamiento y las ventajas que ofrece.

III.1 Historia de OSPF

El protocolo Open Shortest Path First (OSPF) fue desarrollado por el grupo de trabajo OSPF de la Internet Engineering Task Force (IETF) como una respuesta a la necesidad de la comunidad de Internet de introducir un protocolo de compuerta interna (IGP) de alta funcionalidad que no fuese propietario (como es el caso de IGRP actualmente en uso en RedUNAM). Los estudios comenzaron en el año de 1988, pero fue hasta el año de 1991 que se formalizaron las especificaciones de este protocolo.

OSPF es un protocolo de compuerta interna utilizado para distribuir información de enrutamiento dentro de un Sistema Autónomo, está basado en tecnología Link State o SPF (Shortest Path First), que provienen del algoritmo Bellman-Ford ocupado en los protocolos de enrutamiento tradicionales como RIP. OSPF es una alternativa más reciente a RIP entre los protocolos internos, corrigiendo todas las limitaciones que tenía éste.

III.2 Descripción preliminar de OSPF

A continuación se describe el funcionamiento de manera general de OSPF, posteriormente se describirá de manera más específica el funcionamiento de cada una de sus partes.

El protocolo de enrutamiento OSPF analiza para el encaminamiento de paquetes principalmente en la dirección IP destino y en el tipo de servicio (TOS por sus siglas en ingles) se localizan en la cabecera del paquete IP. Es un protocolo de enrutamiento dinámico, ya que detecta de una manera muy rápida cualquier cambio topológico que exista dentro del Sistema Autónomo; tal como una falla en la interfaz de un enrutador, y recalcula nuevas rutas que estén exentas de loops después de un periodo muy corto de convergencia.

OSPF es un protocolo Link State a diferencia de RIP, el cual es un protocolo distance vector. En OSPF cada enrutador mantiene una base de datos, la cual describe la topología del Sistema Autónomo que es idéntica a la de los demás. Estos enrutadores intercambian el estado de cada uno de sus enlaces con los enrutadores vecinos a través de anuncios llamados "Link State" que transportan dicha información, la cual se propaga a través del Sistema Autónomo. Todos los enrutadores dentro del Sistema Autónomo realizan el mismo proceso, y basándose en su base de datos, construyen el "Shortest-Path Tree" o SPT (Árbol con las rutas más cortas) tomándose a él mismo como la raíz o punto de inicio. Este árbol nos indica la ruta para alcanzar cualquier destino.

OSPF puede calcular un conjunto separado de rutas para cada tipo de servicio IP (TOS), es decir, que para un mismo destino pueden existir varias entradas en la tabla de enrutamiento, una por cada tipo de servicio. Cuando existen muchas rutas con un mismo costo hacia un mismo destino, el trafico se distribuye equitativamente entre ellos. En este estudio se omite el uso de TOS y se considera sólo el valor de 0.

OSPF permite agrupar una serie de redes llamadas "áreas". La topología de un área sólo es conocida por los enrutadores dentro de la misma, gracias a esto existe una gran reducción del trafico de enrutamiento, reducción en el procesamiento de los enrutadores, etc.

Cada ruta distribuida por OSPF tiene una dirección IP destino y una mascara de red. Dos subredes diferentes dentro de una misma red pueden tener diferentes tamaños, es decir, diferentes mascaras de subred. Por ejemplo, en el caso de que existan dos rutas para un mismo destino, el paquete se va a enrutar por el mejor camino o, lo que es lo mismo, por la ruta más especifica. Esto es comúnmente llamado "subneteo de longitud variable" (VLSM) mencionado en el Capítulo I.

Todos los intercambios de paquetes Link State dentro del protocolo OSPF son autenticados por medio de passwords, esto significa que sólo los enrutadores autorizados dentro del Sistema Autónomo pueden participar en el enrutamiento de información. Existe una gran variedad de esquemas de autenticación, por esto en algunas áreas pueden configurarse esquemas de autenticación muy simples y en otras áreas se puede tener autenticación más estricta.

III.3 Base de Datos Topológica o Link State

La base de datos topológica (conocida también como base de datos Link State) describe la topología completa de una red (como la que se muestra en la Figura 3.1), esto es: enrutadores (RTx), segmentos de red (Nx)y la forma en que estos se interconectan (las líneas en la imagen).

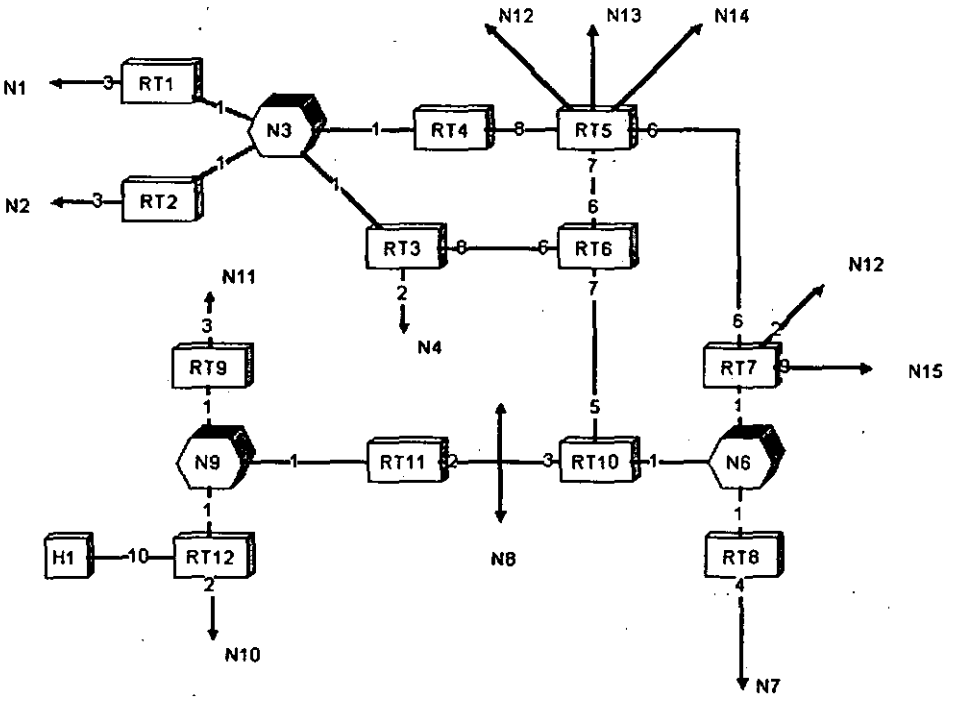


Figura 3.1 Ejemplo de topología de red

La base de datos topológica se representa a través de una tabla donde los vértices son enrutadores y redes.

	ORIGEN															
Destino	**RT1**	**RT2**	**RT3**	**RT4**	**RT5**	**RT6**	**RT7**	**RT8**	**RT9**	**RT10**	**RT11**	**RT12**	**N3**	**N6**	**N8**	**N9**
RT1													0			
RT2													0			
RT3						6							0			
RT4					8								0			
RT5				8		6	6									
RT6			8		7					5						
RT7					6									0		
RT8														0		
RT9																0
RT10						7								0	0	
RT11															0	0
RT12																0
N1	3															
N2		3														
N3	1	1	1	1												
N4			2													
N6							1	1		1						
N7								4								
N8										3	2					
N9									1		1	1				
N10												2				
N11									3							
N12					8		2									
N13					8											
N14					8											
N15							9									
H1												10				

Ejemplo de base de datos topología

Cuando existe una intersección en la tabla entre dos enrutadores indica que estos se conectan a través de una interfaz física de red punto a punto (un enlace serial). Cuando existe una intersección de un enrutador hacia una red, indica que el enrutador tiene una interfaz asociada hacia a esa red. La intersección entre vértices puede tener diferentes tipos de valores de acuerdo a la tarea o función que la red o enrutador tenga.

En el caso de que un enrutador solamente transporte información, más no tenga como destino u origen algunas de sus redes (esto es, que sólo sea un enrutador de tránsito), en la tabla se representará por medio de una intersección en ambos sentidos, es decir, tanto de entrada como de salida.

OSPF soporta los siguientes tipos de redes:

Redes punto a punto (Seriales)

Es una conexión entre dos enrutadores a través de una línea serial.

Redes multiacceso tipo broadcast

Son redes que soporta más de dos conexiones de enrutadores con la capacidad de mandar un mensaje hacia todos los equipos conectados (broadcast). Un ejemplo de este tipo de red es Ethernet.

Redes multiacceso tipo no-broadcast

Son redes que soporta más de dos conexiones de enrutadores pero que no tiene la capacidad de mandar mensajes tipo broadcast, en su lugar utilizan mensajes tipo multicast, como es el caso de Frame Relay y X.25.

Todos los protocolos de enrutamiento proveen una forma para que el enrutador descubra y mantenga relación con sus vecinos (también conocidos como vecindad o *peer*). Los vecinos del enrutador, o peers, son aquellos con los cuales el enrutador va a intercambiar directamente información de enrutamiento.

La vecindad de cada nodo de la red depende si la red tiene capacidad de multiacceso (sea de tipo broadcast o no), si es así, es igual al número de enrutadores teniendo una interfaz dentro de esa red.

Dos enrutadores que se unen a través de una interfaz punto a punto se representa en la tabla con una intersección en cada dirección. Los enlaces punto a punto entre enrutadores no necesitan una dirección IP a cada extremo, a esto se le conoce como redes no numeradas.

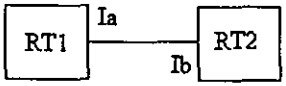


Figura 3.2 Topología de enlace punto a punto

	Origen	
Destino	**RT1**	**RT2**
RT1		X
RT2	X	
Ia		X
Ib	X	

Base de datos topológica de enlace punto a punto

Cuando múltiples enrutadores se conectan a una red multiacceso, en la tabla se representan conectadas al vértice de la red bidireccionalmente.

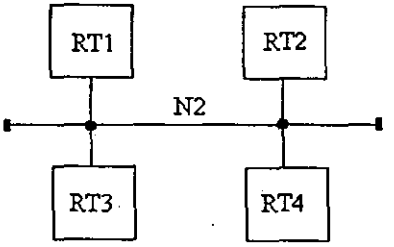


Figura 3.3 Topología de red Multiacceso

	Origen				
Destino	**RT1**	**RT2**	**RT3**	**RT4**	**N2**
RT1					X
RT2					X
RT3					X
RT4					X
N2	X	X	X	X	

Base de datos topológica de red Multiacceso

Si un solo enrutador se conecta a una red multiacceso, la red aparecerá en la tabla como una conexión STUB.

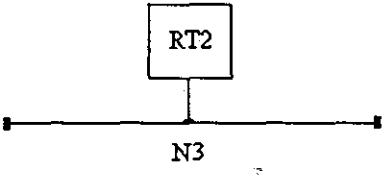


Figura 3.3 Topología de red Multiacceso Stub

	Origen	
Destino	**RT2**	**N3**
RT2		
N3	X	

Base de datos topológica de red Multiacceso Stub

A cada interfaz del enrutador donde se conecta ya sea a un enrutador o hacia una red multiacceso se le asigna un costo. Este es configurado manualmente por el administrador. El costo más bajo es el que se prefiere para enviar la información.

III.3.1 Shortest Path Tree o árbol de la ruta más corta

Dentro de un Sistema Autónomo, cada enrutador dentro del sistema tiene una base de datos idéntica de la cual se forma una representación gráfica llamada Shortest Path Tree. Un enrutador forma su tabla de enrutamiento calculando su árbol de rutas más cortas (SPT) tomándose a él mismo como raíz. El árbol resultante dependerá directamente del enrutador desde el cual se realice el cálculo. Una vez calculado el árbol, la información se enviara por la rama o ruta más corta que conduzca al destino. Después de que el enrutador mande la información al próximo salto serán los siguientes enrutadores los que decidan la ruta a seguir utilizando el mismo proceso.

III.4 Enrutamiento Jerárquico

OSPF nos permite implantar un esquema modular y jerárquico de enrutamiento de información. Estos módulos no ofrecen diferentes ventajas como se explicará a continuación. A éste esquema modular de OSPF se le nombra área.

III.4.1 Áreas en OSPF

Un anuncio Link State, con información de la topología de la red, se envía a todos los enrutadores de toda la red cada vez que se genere un cambio en la información de enrutamiento. Sin embargo, cuando la red es muy grande, es necesario reducir el alcance de los anuncios Link State a través de asignación de áreas. El protocolo OSPF permite agrupar redes y host continuos; a esta asociación, junto con las interfaces de los enrutadores que abarcan a las redes y hosts, se le conoce con el nombre de "*área*".

Por lo tanto, el objetivo principal de un área en OSPF es establecer un límite a los "floodings" (anuncios generados por los anuncios Link State) y calcular el algoritmo "Shortes Path Tree" para generar la tabla de enrutamiento por área, lo que reduce ampliamente su complejidad. El manejo de la información de enrutamiento por áreas ofrece muchas ventajas, entre ellas destacan:

- Se reduce la información de enrutamiento a transferir en la red, por lo que existe menor cantidad de tráfico de enrutamiento en el Sistema Autónomo.
- Las áreas permiten el desarrollo de enrutamiento jerárquico, lo que permite proteger un área de la información de enrutamiento externa generada en otra.
- La información de enrutamiento es ocultada y protegida por los ruteadores hacia fuera del área a la que pertenecen. Este "ocultamiento" de información tiene fines de seguridad, dado que la topología de un área nunca será conocida por ruteadores de un área diferente.
- Dentro de cada área se tiene una misma base de datos topológica.

El enrutamiento de paquetes dentro del Sistema Autónomo se lleva a cabo en dos niveles dependiendo de donde residan el origen y destino. Si ambos se encuentran dentro de la misma área se realiza enrutamiento Intra-área e Inter-área en caso de pertenecer a diferentes áreas.

A continuación se describen las áreas más importantes que define el protocolo OSPF.

III.4.1.1 Área backbone o área cero.

En el caso de existir más de dos áreas, una de las áreas deberá ser área cero —también llamada área de backbone—. Esta área debe ser el centro de las demás, lo que significa que las otras deben estar conectadas físicamente a ella. La razón se debe a que OSPF espera que las diferentes áreas envíen información de enrutamiento al área cero, para que ésta la redistribuya a las demás en turnos. Por lo anterior, el área cero debe ser contigua, sin embargo, aunque físicamente se presente discontinuidad en el área cero, OSPF permite mantener la conectividad del backbone lógicamente configurando "virtual links" (ligas virtuales).

Un virtual link puede ser configurado entre dos enrutadores que posean una de sus interfaces en un área común diferente al área de backbone y uno de ellos con al menos una interfaz al backbone. OSPF maneja a los dos enrutadores conectados por virtual links como conectados en un enlace de punto a punto con métrica de cero (el tráfico entre virtual links usa enrutamiento Intra-área únicamente).

El área cero posee las mismas características que cualquier otra área por lo que su manejo es análogo a cualquiera de ellas. Cabe mencionar que para que OSPF funcione es necesario la existencia del área cero.

En el siguiente ejemplo se muestra el uso del área cero. En el caso del enrutamiento Inter-área, se puede describir el proceso de enrutamiento en tres partes:

- Una ruta Intra-área desde el origen hasta el enrutador de borde de área (ABR)
- Una ruta dentro del área de backbone desde el ABR del área origen a el ABR del área destino
- Finalmente una ruta Intra-área hacia el destino.

Como se aprecia, el enrutamiento Inter-área utiliza una configuración de estrella del Sistema Autónomo donde el área cero actúa como un concentrador o hub para las demás áreas.

III.4.1.2 Área Stub

En algunos Sistemas Autónomos, la mayor parte de la información de la base de datos topológica puede consistir de anuncios de Sistemas Autónomos externos. Un anuncio de Sistema Autónomo externo es normalmente anunciado a todo el Sistema Autónomo. Por lo anterior OSPF permite que ciertas áreas sean configuradas como "áreas stub". En ellas, los anuncios de Sistemas Autónomos externos no le son anunciados, lo que significa que el enrutamiento a destinos externos al Sistema Autónomo se basa en rutas por default, una ruta de default por área. Esto

reduce significativamente el tamaño de la base de datos topológica y por lo tanto los requerimientos de memoria y procesador de los enrutadores del área.

III.4.1.3 Clasificación de enrutadores

En el caso de que el Sistema Autónomo sea dividido en más de dos áreas, también es necesario la clasificación de los enrutadores de acuerdo a sus funciones. Existen cuatro categorías principales:

Enrutador Interno (Internal Router): IR

En este tipo de enrutadores todas las redes que se conectan a él pertenecen a una misma área. Cada uno de estos enrutadores mantiene una base de datos topológica única.

Enrutador de Borde de Área (Area Border Router). ABR.

Enrutador conectado a diferentes áreas. Estos enrutadores mantienen una base de datos topológica por cada área a la que estén conectadas y una más adicional para el área cero. Así mismo, este tipo de enrutadores resume la información de la topología de las áreas que poseen para posteriormente redistribuirla al área cero. El área cero se encargará de distribuirla a las demás áreas.

Enrutador de Backbone (Backbone Router): BR.

Enrutador con una interfaz al backbone. Estos incluyen a los enrutadores que poseen entre sus interfaces más de un área, por ejemplo ABR. Por el contrario, los enrutadores de backbone no tienen que ser ABRs y los enrutadores con todas sus interfaces conectadas al área cero son considerados IR.

Enrutador de frontera de Sistema Autónomo (AS Boundary Router): ASBR.

Enrutador que intercambia información de enrutamiento con otros enrutadores de diferentes Sistemas Autónomos, otros protocolos de enrutamiento u otros procesos de OSPF para después anunciarlo en el proceso de OSPF propio. La ruta para llegar a cada ASBR debe ser conocida por todos los enrutadores del Sistema Autónomo. Esta clasificación es completamente independiente de las anteriores por lo que pueden existir combinaciones.

III.5 Adyacencias

El proceso de adyacencias es el próximo paso después del proceso de creación de vecindad. Los enrutadores adyacentes son aquellos que además del intercambio de paquetes Hello, continúan con el proceso de intercambio de la base de datos. Para llevar a cabo el proceso anterior, OSPF elige a un enrutador para ser Designated Router (DR), y uno más para ser el Backup Designated Router (BDR). El BDR se elige como un mecanismo de respaldo en caso de que el DR falle. La idea anterior es que los enrutadores tengan un punto central de contacto para el intercambio de información, en lugar de que cada uno de ellos intercambie información con los demás en el segmento. Cada enrutador va a intercambiar información con el DR y el BDR, estos a su vez reenviaran la información a los demás enrutadores del segmento a través de las direcciones multicast AllSPFRouters (224.0.0.5) y AllDRouters (224.0.0.6).

III.5.1 Elección del DR y BDR.

La elección del DR y BDR se realiza a través de intercambio de paquetes Hello. Estos paquetes se intercambian vía paquetes IP multicast en cada segmento. El enrutador con la mayor prioridad dentro del segmento en OSPF va a ser el DR para ese segmento. El mismo proceso se repite para la elección del BDR. En caso de que exista un empate el enrutador con el mayor identificador va a ser elegido. Hay que recordar que el concepto de DR y BDR son para segmentos de red multiacceso.

III.5.2 DR y BDR

Designated Router, DR

El DR es elegido por el protocolo Hello. Un paquete Hello de un enrutador contiene la prioridad del mismo, la cual es configurable por interfaz de red. En general, cuando un enrutador se pone en funcionamiento por primera vez, checa si existe un DR para la red. Si lo hay, lo acepta a pesar de la prioridad que este posea. De otra manera, el enrutador se proclama DR si tienen el Router Priority más alto.

El DR es el punto final de muchas adyacencias. Para optimizar el funcionamiento de las redes tipo broadcast, el DR manda mensajes de multicas Link State Update a la dirección AllSPFRouters en vez de usar un mensaje unicast a cada adyacencia.

Este enrutador tiene dos principales funciones dentro de OSPF:

- El DR origina Networks Links Adverisements. Estos anuncios listan el grupo de enrutadores (incluido él mismo) actualmente unidos a la red. El Link State ID para este anuncio es la IP de la interfaz del DR (la dirección de red puede ser obtenida por medio de la máscara).

- El DR logra ser adyacente con todos los demás enrutadores de la red. A partir de que la base de datos Link State se sincroniza a través de las adyacencias (por medio del inicio de adyacencias y después el procedimiento de flooding), el DR juega un papel central en el proceso de sincronización.

Backup Designated Router, BDR

Para hacer más rápida la transición de un DR a otro nuevo, existe un DR de respaldo para cada red de multiacceso. El BDR también es adyacente a todos los demás enrutadores de la red y toma el papel del DR cuando este falla. El periodo de interrupción del tráfico en la red toma sólo el tiempo necesario para que los mensajes LSAs se dispersen por medio del proceso flooding anunciando al nuevo DR.

El BDR también es elegido por el protocolo Hello. Cada mensaje Hello posee un campo que especifica al BDR de la red.

En algunos pasos del proceso de flooding, el BDR juega un papel pasivo, mientras que deja que el DR haga la mayor parte del trabajo.

III.5.3 Construcción de la adyacencia.

Los enrutadores que se vuelven adyacentes con el DR y BDR tendrán exactamente la misma base de datos topológica. A continuación se mencionan los estados que deben de pasar los enrutadores antes de obtener la adyacencia.

1. DOWN
   Ninguna información ha sido recibida por ningún enrutador en ese segmento.

   1'. ATTEMPT
   En redes multiacceso tipo no broadcast como frame relay y X.25, este estado indica que no se ha recibido información reciente de su vecino. Cuando pasa esta situación el enrutador trata de contactar de nuevo con su vecino a través de paquetes Hello.

2. INIT
   La interfaz ha detectado un paquete Hello proveniente de un vecino, pero la comunicación bidireccional no se ha establecido aún.

3. TWO-WAY
   Existe una comunicación bidireccional con el vecino. El enrutador se ha visto a él mismo en los paquete Hello provenientes de su vecino. Al final de esta etapa se ha elegido al DR y BDR, los enrutadores serán capaces de decidir con quien hacer las adyacencias y conque enrutadores no.

4. EXSTART
   Los enrutadores tratan de establecer el Initial Sequence Number que va a ser utilizado para el intercambio de paquetes de información. Este número de secuencia asegura que los enrutadores siempre obtengan la información mas reciente.

5. EXCHANGE
   Los enrutadores describirán su base de datos topológica enviando Database Description Packets. En este punto, los paquetes deben de ser enviados a todas las interfaces del enrutador por medio del proceso flooding.

6. LOADING
   En este paso los enrutadores han finalizado el intercambio de información. Los enrutadores han construido una lista de Link State Request y una lista de Link State Retransmission. Cualquier información incompleta o desactualizada, se pondrá en la lista de peticiones "request". Cualquier actualización que es enviada se pondrá en la lista de "retransmission" hasta que llegue su acuse de recibo (Acknowledge).

7. FULL

La adyacencia está completa. Los enrutadores vecinos están completamente adyacentes unos con otros.

OSPF siempre tendrá una adyacencia con un vecino que se encuentre conectado en una interfaz punto a punto. Aquí no existen los conceptos de DR y BDR.

III.6 Formato de los paquetes de OSPF y LSAs

En este apartado se describe el formato de los paquetes usados en el protocolo OSPF. Los paquetes se muestran a continuación así como una breve descripción de su uso.

Tipo	Nombre del Paquete	Función
1	Hello	Descubre y mantiene vecinos
2	Database Description	Resume el contenido de la base de datos
3	Link State Request	Transfiere la base de datos
4	Link State Update	Actualiza la base de datos
5	Link State Acknowledge	Acuse de recibo del proceso flooding

También se describen los formatos de los paquetes LSAs; se muestran en la siguiente tabla y se describen brevemente.

Tipo	Nombre del Anuncio	Función
1	Router Links Advertisements	Describe el estado de las interfaces de los enrutadores. Originado por todos los enrutadores. Distribuidos por área.
2	Network Links Advertisements	Contiene la lista de enrutadores conectados a una red. Originado por el DR en redes multiacceso. Distribuidos por área.
3, 4	Summary Link Advertisements	Originado por ABRs para anunciar el estado de su área. Describe una ruta de un destino fuera del área pero dentro del Sistema Autónomo. El tipo 3 describe rutas hacia redes y el tipo 4 describe rutas hacia los ASBRs.
5	AS External Link Advertisements	Originado por los ASBRs. Describe la ruta a un destino fuera del Sistema Autónomo. También pueden anunciar rutas por default. Distribuidos en todo el Sistema Autónomo.

Más adelante se describen con mayor detalle cada uno de ellos.

Antes de describir los paquetes es necesario describir la encapsulación de OSPF en IP, posteriormente se describirá el campo de options, ya que está contenido dentro de los paquetes Hello packets, Database Description packets y en los OSPF LSAs.

III.6.1 Encapsulación de paquetes OSPF en IP

OSPF corre directamente sobre la capa de internet de TCP/IP (capa de red en OSI) por lo que los paquetes de OSPF son encapsulados en paquetes IP. OSPF no define la forma para fragmentar sus paquetes y depende de IP para esto, cuando se envían paquetes de mayor tamaño al MTU de la red en cuestión. En el caso de ser necesario, la longitud del paquete de OSPF puede ser mayor a 65,535 bytes (incluyendo el encabezado de IP). El tipo de paquetes que suelen ser mayores (Database Description Packets, Link State Request, Link State Update y Link State Acknowledge Packets) pueden ser usualmente divididos en paquetes separados sin que se pierda su funcionalidad, sin embargo se recomienda que la fragmentación de IP se evite siempre que sea posible. Usando este razonamiento, se deberá hacer un esfuerzo para limitar el tamaño de los paquetes de OSPF que sean enviados sobre virtual liks a 576 bytes.

Las otras características importantes de la encapsulación de OSPF sobre IP son:

- Uso de multicast en IP. Algunos mensajes de OSPF son multicast cuando se envía sobre redes de broadcast. Dos direcciones multicast IP son utilizadas dentro de OSPF, las cuales sólo deben ser reenviadas en un solo salto por lo que es necesario configurar un TTL a 1. Estas direcciones multicast de OSPF son:

  AllSPFRouters

  Esta dirección de multicast tiene el valor asignado de 224.0.0.5. Todos los enrutadores corriendo OSPF deben estar preparados para recibir los paquetes enviados a esta dirección. Los paquetes Hello son siempre enviados a este destino, así como ciertos paquetes de OSPF son enviados a esta dirección durante el proceso de "flooding".

  AllDRouters

  Esta dirección de multicast ha sido asignada al valor de 224.0.0.6. Los enrutadores DR y BDR (ambos) deben estar listos para recibir paquetes de esta dirección.

- OSPF tiene el identificador 89 dentro de IP, este número ha sido registrado ante el Network Information Center (NIC).

- Todos los paquetes de enrutamiento OSPF son enviados usando el valor normal de 0000 binario dentro del campo de TOS.

- Los paquetes de enrutamiento OSPF son enviados con la precedencia puesta a Internetwork Control dentro del campo de TOS en IP. Los paquetes de OSPF deberán tener preferencia sobre los del tráfico normal de IP en ambos casos cuando se envíen o reciban (ver el subcampo de Precedence dentro del campo TOS de la cabecera de IP).

III.6.2 El campo de opciones

El campo de opciones de OSPF se encuentra dentro de los paquetes de Hello packets, Database Description packets y en todos los anuncios Link State. El campo de opciones habilita a los enrutadores en OSPF a soportar (o no) capacidades opcionales para comunicar su nivel de capacidad hacia otros enrutadores. A través de este mecanismo, enrutadores de diferentes capacidades pueden mezclarse dentro de un mismo dominio de enrutamiento.

Cuando se utiliza en paquetes Hello, el campo de options permite al enrutador rechazar la relación de vecindad con otro debido a que no tienen las mismas capacidades. Opcionalmente cuando las capacidades se intercambian en los Database Description packets, un enrutador puede elegir no retransmitir ciertos anuncios Link State a un vecino debido a que reduce su funcionalidad.

Actualmente sólo están definidas dos capacidades. La capacidad depende directamente del tipo de paquete que se esté transmitiendo, por ejemplo, el ExternalRoutingCapability (llamado E-bit) tiene únicamente significado en los paquetes de Hello.

Para el futuro se tiene planeado agregar más capacidades aunque actualmente los enrutadores cuando se encuentran con capacidades que no conocen, ya sea en Hello packets, Database Description packets o anuncios Link State deben de ignorar esa capacidad y procesar el paquete o anuncio normalmente.

El campo de opciones

T-bit

Describe la capacidad de TOS del enrutador. Si el T-bit está en cero, entonces el enrutador solamente soporta el tipo de servicio 0. La ausencia del T-bit en un Summary Link Advertisement o en un AS External Link Advertisement indica que el anuncio está describiendo una ruta TOS = 0.

E-bit

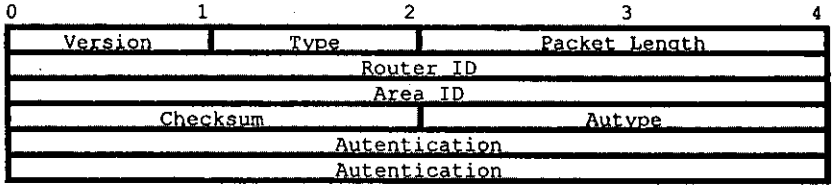
Un anuncio AS External Link Advertisement no es anunciado hacia las áreas stub en OSPF. El E-bit asegura que todos los miembros de un área stub están de acuerdo en la configuración de dicha área. El E-bit solamente tiene significado en los Hello packets de OSPF. Cuando el E-bit se inicializa en el Hello packet enviado a una interfaz en particular, significa que el enrutador no recibirá ni enviará LSAs del tipo AS External Link Advertisement en esa interfaz (es decir, la interfaz está conectada a un área stub). Dos enrutadores nunca podrán ser vecinos a menos que coincida en el valor del E-bit.

III.6.3 Formato de los paquetes de OSPF.

Existen cinco diferentes tipos de paquetes en OSPF. Todos estos paquetes empiezan con una cabecera estándar de 24 bytes. Se describirá la cabecera y a continuación cada tipo de paquete de OSPF. Todos los tipos de paquetes de OSPF se relacionan con anuncios Link State.

III.6.3.1 OSPF Header.

La cabecera contiene toda la información necesaria para determinar si un paquete deberá ser aceptado y procesado o eliminado. A continuación se presenta en forma gráfica los campos que conforman la cabecera en OSPF.



Versión #.

Versión de OSPF que se esté utilizando. La última versión es la 2.

Type.

Los cinco tipos de paquetes en OSPF son los siguientes:

Tipo	Descripción
1	Hello
2	Database Description
3	Link State Request
4	Link State Update
5	Link State Acknowledgment

Packet length.

Longitud del paquete en bytes. Esta longitud incluye a la cabecera de OSPF.

Router ID.

Identificador del enrutador del paquete origen. En OSPF el origen y el destino de un paquete en un protocolo de enrutamiento son las dos puntas de una adyacencia.

Area ID.

Serie de 32 bits que identifica el área a la cual pertenece el paquete. Todos los paquetes están asociados a una sola área. Los paquetes que viajan a través de un "virtual link" son etiquetados con el área ID del backbone 0.0.0.0.

Checksum.

Se utiliza el chequeo de errores estándar de IP comenzando desde la cabecera, pero excluyendo los 64 bits del campo de autenticación.

Autype.

Identifica el esquema de autenticación que va a ser utilizado en el paquete.

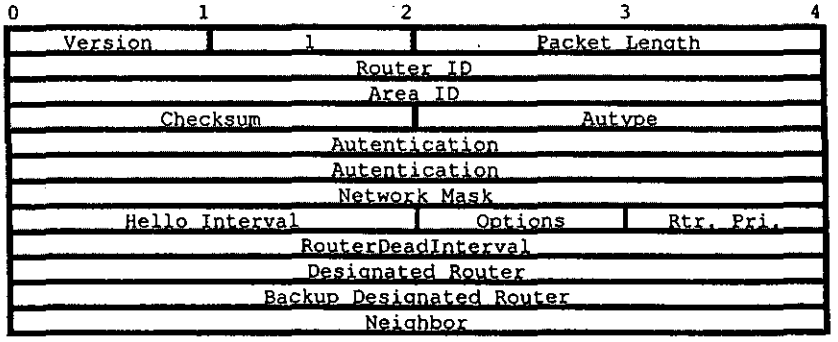
Authentication.

Campo de 64 bits utilizado en el esquema de autenticación.

III.6.3.2 HELLO Packet.

Los paquetes de Hello son de tipo 1 en OSPF. Estos paquetes se envían periódicamente a través de todas las interfaces del enrutador (incluyendo los virtual links) con el fin de establecer y mantener la comunicación con los vecinos. Los paquetes de Hello son multicast en aquellas redes que sean multicast o broadcast habilitando el descubrimiento automático de vecinos.

Todos los enrutadores conectados a una red en común deben estar de acuerdo con ciertos parámetros (Network Mask, Hello Interval, RouterDeadInterval). Estos parámetros vienen dentro del paquete de Hello como se muestra a continuación:



Network mask.

Mascara de red asociada a esta interface. Por ejemplo, si la interface está asociada una red clase B en la cual el tercer byte se utiliza para subnetear, las mascara de red será 255.255.255.0.

Options.

Capacidades opcionales soportadas por el enrutador, como es el rechazo de un vecino.

Hellointerval.

Número en segundos para mandar anuncios de Hello entre enrutadores.

Rtr Pri.

La prioridad de enrutador se utiliza en la elección del (Backup) Designated Router. Si se pone en 0 (cero), el enrutador será inelegible para ser un (Backup) Designated Router.

RouterDeadInterval.

Número en segundos antes de declarar a un enrutador como inalcanzable.

Designated Router.

Identifica al Designated Router con la dirección IP de la interface de esta red. Se pone 0.0.0.0 si no existe un Designated Router.

Backup Designated Router.

Identifica al Backup Designated Router con la dirección IP de la interface de esta red. Se pone 0.0.0.0 si no existe un Backup Designated Router.

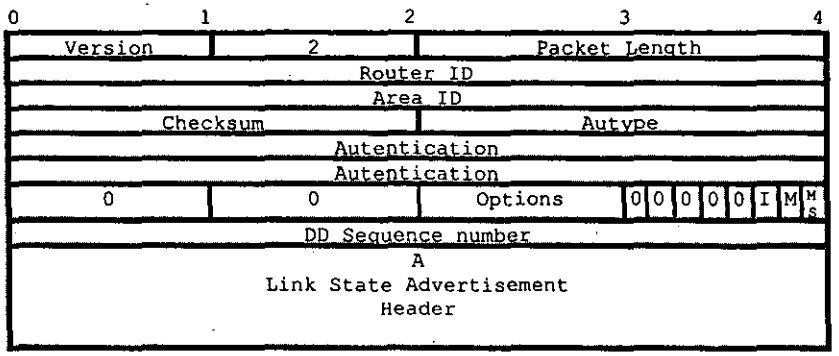
Neighbor.

Los Router IDs de cada enrutador del cual los paquetes de Hello validos se han escuchado recientemente en la red. Recientemente significa en los últimos segundos del periodo de RouterDeadInterval

III.6.3.3 Database Description Packet.

Los paquetes de descripción de la Base de Datos dentro de OSPF son del tipo 2. Estos paquetes se intercambian cuando se trata de establecer una adyacencia. Describen el contenido de la base de datos topológica. Múltiples paquetes se utilizan para poder describir toda la base de datos, para este propósito se utiliza el procedimiento conocido como "poll-response". Uno de los enrutadores es designado como maestro y el otro como esclavo. El maestro envía los paquetes que describen a la base de datos al esclavo (polls), éste acusa de recibido al maestro a través de paquetes Database Description (responses). Los paquetes "response" acusan de recibido a los paquetes "poll" vía un DD Sequence number.

El formato del paquete Database Description es muy similar a los paquetes Link State Request y Acknowledgment. La parte principal de estos tres paquetes radica en una lista de campos que describen una parte de la base de datos topológica.



Los campos marcados con "0" están reservados y deben de ser ceros.

Options.

Describe una serie de opciones como la de no reenviar anuncios Link State a un vecino debido a que reduce funcionalidad.

I-bit.

Cuando el Init bit se pone en 1 significa que es el primer paquete del Database Description.

M-bit.

El More bit se pone en 1 cuando a continuación se esperan más paquetes de Database Description.

MS-bit.

El bit master/slave cuando se pone en 1, indica que este enrutador es el maestro durante el proceso de intercambio, de otra manera el enrutador es esclavo.

DD sequence number.

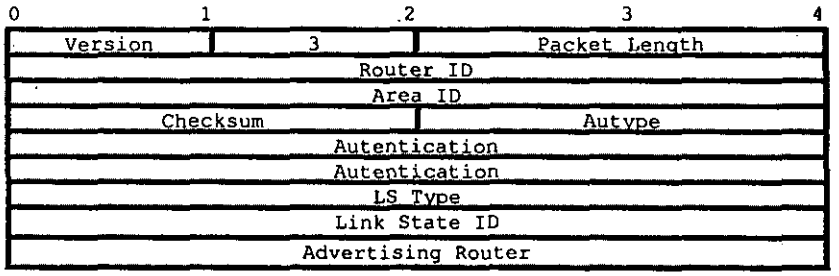
Aquí se pone la secuencia de los paquetes Database Description. El valor inicial debe de ser único y se va incrementando hasta que la descripción de la base de datos sea completada.

El resto del paquete consiste de una lista de partes de la base de datos topológica.

III.6.3.4 Link State Request Packet.

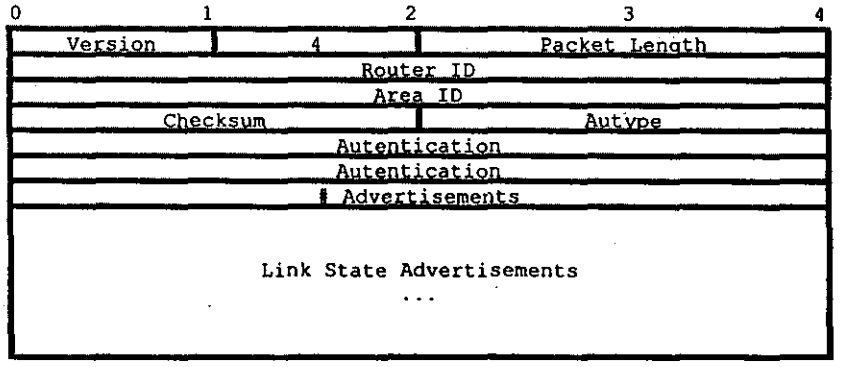
Estos paquetes son del tipo 3 en OSPF. Después de intercambiar los paquetes Database Description con los enrutadores vecinos, un enrutador debe encontrar las partes de la Base de Datos que estén desactualizadas, posteriormente se envían paquetes de peticiones Link State Request a los vecinos para obtener información más actualizada de la base de datos. El envío de paquetes Link State Request es el último paso para obtener la adyacencia.

Un enrutador que envía paquetes Link State Request tiene en memoria el momento preciso de las peticiones que ha hecho a fragmentos de la base de datos, a través de los campos LS sequence number, LS Checksum y LS age, sin embargo estos campos no son especificados en el paquete Link State Request, estos campos pertenecen al LSA header .



III.6.3.5 Link State Update Packet.

Estos paquetes son del tipo 4 en OSPF, implementan el llamado "flooding" de anuncios Link State. Este tipo de paquetes transporta una colección de LSAs. Como su nombre lo indica se utilizan para mantener actualizada su base de datos. Son anuncios tipo multicast en redes tipo multicast y tipo broadcast. Para que el procedimiento de flooding sea seguro, estos anuncios son acusados de recibido en paquetes de Link State. Si se necesita una retransmisión de un anuncio, es retransmitido siempre por un paquete Link State Update unicast.



#Advertisements.

Número de anuncio Link State incluido en esta actualización.

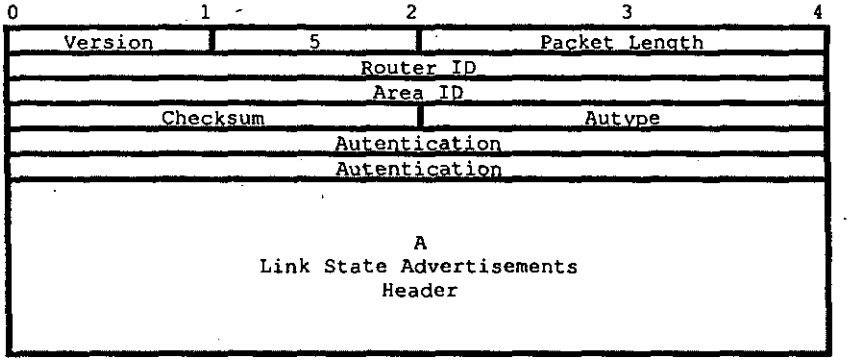
III.6.3.6 Link State Acknowledgment Packet.

Paquete tipo 5 en OSPF. Para hacer más seguro el "flooding" de los anuncios Link State, todos

los anuncios son acusados de recibido. Este acuse finaliza cuando se envía y se recibe paquetes de Link State Acknowledgment. Múltiples anuncios Link State pueden ser acusados por un solo paquete Link State Acknowledgment.

Dependiendo del estado de la interfaz que envía el paquete puede mandarse un paquete Link State Acknowledgment ya sea multicast a todos los enrutadores "DR" o un solo paquete unicast.

El formato de este paquete es muy similar al Data Description Packet. El cuerpo de ambos paquetes es una simple lista de cabeceras de Link State Advertisement.



III.6.4 Formatos de los LSAs

Existen 5 tipos diferentes de LSAs, cada uno de ellos comienzan con una cabecera común de 20 bytes. Esta cabecera se explicará posteriormente para después definir cada tipo de LSA específico.

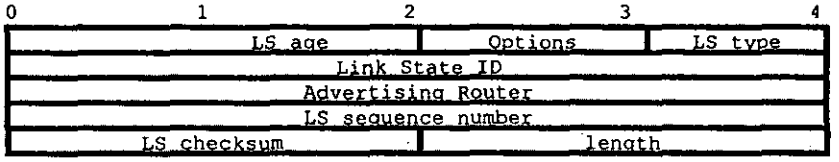
Cada uno de los LSAs describe un fragmento del dominio de enrutamiento OSPF. Por ejemplo, todos los enrutadores originan un Router Link Advertisement; cuando un enrutador es elegido como DR, éste origina un Network Link Advertisement; de manera semejante otros LSAs pueden ser originados. Cabe mencionar que todos los LSAs son "flooded" o enviados a través del dominio de enrutamiento de OSPF. El algoritmo de flooding se asegura que todos los enrutadores tengan la misma colección de LSAs, conocida como base de datos de Link-state o base de datos topológica.

De la base de datos topológica, todos y cada uno de los enrutadores construye un SPT tomándose a él mismo como la raíz para posteriormente construir su tabla de enrutamiento.

III.6.4.1 LSA Header

Todos los LSAs comienzan con una cabecera común de 20 bytes que contiene la información suficiente para identificar el tipo de LSA (LS type, LS ID y Advertising Router). Pueden existir múltiples instancias de un LSA en un tiempo determinado para lo cual es necesario determinar

cual de ellas es la más reciente examinando los campos LS age, LS sequence number y el campo de LS checksum todos ellos incluidos en el LSA Header.



LS age

El tiempo en segundos desde que el LSA fue originado.

Options

Las capacidades opcionales soportadas por la porción del dominio de enrutamiento.

LS type

Tipo de LSA. Cada tipo de LSA tiene un formato diferente. Los diferentes tipos son:

Tipo de LS	Description
1	Router LSAs
2	Network LSAs
3	Summary LSAs (IP network)
4	Summary LSAs (ASBR)
5	AS External LSAs

Link State ID

Este campo identifica únicamente un LSA que fue originado por un enrutador en específico de los demás del mismo tipo. El contenido de este campo depende del LS type. Por ejemplo, en un Network LSA, el Link State ID es la IP de la interfaz del DR de esa red.

Advertising Router

El identificador del enrutador que originó el LSA. Por ejemplo, en un Network LSA, este campo es igual al identificador del enrutador del DR de la red.

LS sequence number

Número usado para detectar LSAs anteriores o duplicados. Instancias sucesivas de un LSA son dadas con sucesivos LS sequence numbers.

LS checksum

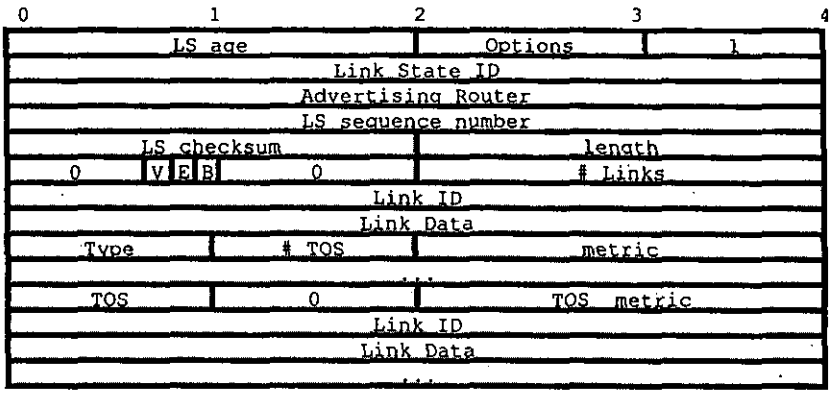
El chequeo de errores de Fletcher aplicado al contenido completo del LSA, incluyendo la cabecera pero excluyendo el campo de LS age.

Length

Longitud en bytes del LSA. Esta incluye los 20 bytes del header.

III.6.4.2 Router Links Advertisements

El paquete Router LSA es del tipo 1. Cada enrutador dentro de un área origina un Router LSA que describe el estado y costo de las interfaces de cada enrutador hacia el área. Todas las interfaces del enrutador hacia el área deben estar descritas en un sólo Router LSA.



En los paquetes Router LSA, el campo de Link State ID es igual al identificador del enrutador de OSPF. Estos anuncios sólo son enviados dentro de un área.

Bit V

Cuando es usado, el enrutador es un punto final de uno o más virtual links completamente adyacentes, lo que significa un área como un Área de Transito (la V proviene de punto Virtual Link de punto final).

Bit E

Cuando está prendido, el enrutador es un ASBR (la E proviene de External).

Bit B

Cuando está prendido, el enrutador es un ABR (la B proviene de Border).

Links

El número de Router-Links descritos en ese LSA. Este número debe ser igual al total de la colección de los Router-Links (por ejemplo, interfaces) hacia el área.

Los siguientes campos (Type, Link ID, Link Data, TOS y TOS 0 metric) son usados para describir cada interfaz del enrutador. A cada interfaz se le asigna el tipo de interfaz de la siguiente tabla. Puede ser una interfaz hacia una red de transito, hacia otro enrutador o hacia una área stub. Los valores de los demás campos que describen la interfaz dependen del campo Type. Por ejemplo, cada interfaz tiene un campo Link Data de 32 bits, para interfaces de áreas stub, el campo especifica la máscara de red IP, para los otros tipos el Links Data especifica la dirección IP de la interfaz del enrutador.

Type

Esta es una descripción rápida de interfaz del enrutador. Las rutas hacia hosts utilizan el tipo 3 (Conexión a áreas stub) con máscara de red de 255.255.255.255.

Tipo	Description
1	Point-to-point connection to another router
2	Connection to a transit network
3	Connection to a stub network
4	Virtual link

Link ID

Identifica al objeto que el enrutador tiene conectado en la interfaz. Este valor depende del campo Type. Los valores que puede tomar son los siguientes:

Tipo	Link ID
1	Neighboring router's Router ID
2	IP address of Designated Router
3	IP network/subnet number
4	Neighboring router's Router ID

Link Data

Depende también del campo Type. Para conexiones a redes stub, el Link Data especifica máscara IP de la red. Para conexiones no numeradas punto a punto, este campo especifica el valor de IfIndex de la interfaz de MIB-II. Para los otros tipos de conexiones, el valor especifica la dirección IP de la interfaz. La información de éste campo será utilizada durante el proceso de construcción de la tabla de enrutamiento para el cálculo de la dirección IP del próximo salto.

TOS

El número de las diferentes métricas de TOS dadas a esta conexión. Si no es proporcionada una métrica de TOS, este campo será puesto en cero.

TOS 0 metric

El costo asignado al uso de esa interfaz con TOS = 0.

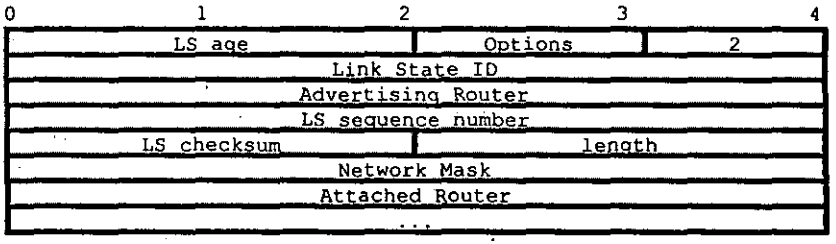
Información adicional del TOS puede ser incluida codificada en los campos de: TOS, TOS IP y TOS Metric (no vistas en este documento y que es innecesario).

III.6.4.3 Network Links Advertisements

Los Network LSAs son del tipo número 2. Estos mensajes son originados por cada red multiacceso dentro de un área que soporte dos o más enrutadores. Los Network LSAs son originados por el DR de la red. Dentro de este paquete se describen todos los enrutadores dentro

de una red, incluyendo al DR. El campo Link State ID de todo LSA lista la dirección IP del DR.

La distancia de la red a todos los enrutadores conectados a ella es cero. Por lo tanto, los campos de métrica no necesitan ser especificados en este tipo de anuncio.



Network Mask

Máscara de red de IP para la red. Por ejemplo, para una red clase A, la máscara de red sería 255.0.0.0 (0xff000000).

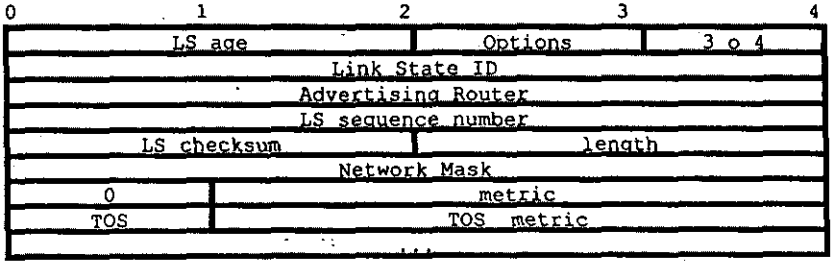
Attached Router

El Router ID de cada uno de los enrutadores de la red. Solamente los enrutadores que son completamente adyacentes al DR son listados (el DR es incluido en la lista). El número de enrutadores puede ser deducido del campo Length de la cabecera del LSA.

III.6.4.4 Summary Link Advertisements

Los paquetes Summary-LSAs son del tipo tres y cuatro de los LSAs. Los paquetes Summary LSAs son originados por los ABRs.

El tipo 3 se utiliza cuando el destino es una red IP. En este caso el campo Link state ID del LSA es la dirección IP de una red. Cuando el destino es un ASBR, el tipo 4 de Summary-LSAs es usado y el campo Link State ID es puesto al identificador del enrutador ASBR de OSPF. En cualquier otro caso el campo Link State ID del tipo 3 y 4 son idénticos.



Para áreas stub, los Summary LSAs de tipo 3 pueden ser usados para describir una ruta por área por default. El resumen de las rutas por default se utiliza en áreas stub en vez del uso del flooding de todas las rutas externas. Cuando el LSA describe una ruta resumida de default, el Link State ID siempre está puesto al DefaultDestination (0.0.0.0) y el campo Network Mask es puesto a 0.0.0.0.

Network Mask

Para el tipo 3 de Summary LSAs, este campo indica la máscara de la dirección IP de la red destino. Por ejemplo, cuando se anuncia una red clase A, el valor deberá ser puesto en 0xff000000 (255.0.0.0). Este campo no tiene significado y deberá ser cero en el tipo 4 de Summary LSAs.

TOS

El tipo de servicio del costo descrito.

Metric

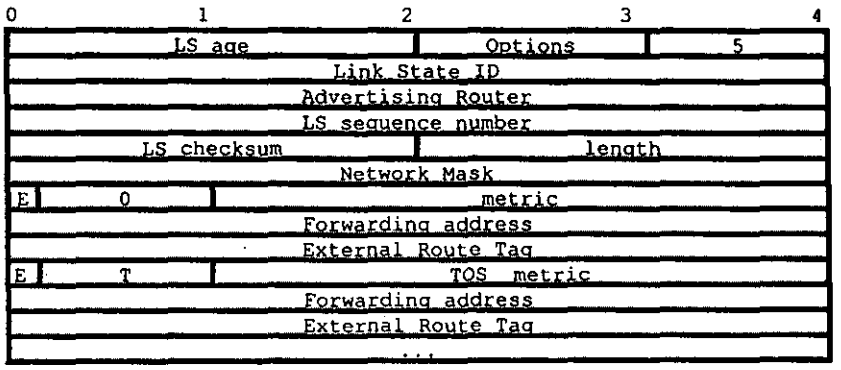
El costo de esta ruta. Expresada en las mismas unidades que en el costo de la interfaz en los Router LSAs.

Adicionalmente información específica de TOS, puede ser incluida para compatibilidad con versiones anteriores de OSPF. La información está codificada en los campos de TOS y TOS metric.

III.6.4.5 AS External Link Advertisements

Los AS External LSAs son el tipo 5. Estos paquetes son originados por el ASBR para describir destinos externos al Sistema Autónomo.

Los AS External LSAs usualmente describen un destino en particular externo. Para estos LSAs, el campo Link State ID especifica un número de IP de red. Los AS External LSAs también son usados para describir una ruta de default. Las rutas de default son usadas cuando no existe una ruta específica hacia un destino. Cada vez que se describan rutas de este tipo, el campo Link State ID siempre es puesto al valor del DefaultDestination (0.0.0.0) y la máscara de red a 0.0.0.0.



Network Mask

La máscara de la dirección IP que se anuncia. Por ejemplo, cuando se anuncia una red clase A, la máscara de red es 0xff000000 (255.0.0.0)

Bit E

Tipo de métrica Externa. Si el bit E está prendido, la métrica especificada es una métrica del tipo 2 externa, lo que significa que es considerada más grande que cualquier otra ruta Link State. Si el bit E es cero, la métrica especificada es una métrica del tipo 1 externa, lo que significa que está expresada en las mismas unidades que la métrica del Link State (ejemplo, las mismas unidades del costo de la interfaz).

Metric

El costo de la ruta. Su interpretación depende del bit E (arriba).

Forwarding address

El tráfico de datos hacia la dirección destino anunciada será reenviada a esta dirección. Si la Forwarding address es puesta a 0.0.0.0, el tráfico de datos será reenviado al que originó el LSA.

External Route Tag

Campo de 32 bits anexado a cada ruta externa. No utilizado por el protocolo OSPF y puede ser utilizado para comunicar ASBRs (información más detallada no es necesaria de especificar dentro de este documento).

Además, información adicional de TOS puede ser incluida para cuestiones de compatibilidad con versiones de OSPF anteriores. Para cada tipo de TOS, la información es codificada con los siguientes campos: TOS, bit E, TOS metric, Forwarding address y External Route Tag.

III.7 Administración

La administración del protocolo OSPF está relacionada con la organización lógica del enrutamiento dentro del AS. Las principales actividades que incluye la administración tienen que ver con aspectos como:

- ¿Cuáles son los límites del AS?
- ¿Qué enlaces deberán ser preferidos sobre otros y bajo que circunstancias?
- ¿ Qué tipo de información deberá ser redistribuida al AS propio y que información deberá ser pasada a los vecinos?
- Número y tamaño de las áreas dentro del AS, así como delimitar, ¿Donde acaba y termina cada una de ellas?
- Establecer el tipo de seguridad necesaria para los enrutadores.

La forma tradicional de administración de cualquier equipo de comunicación —cualquier dispositivo de Internet— es por medio de telnet o por consola, pero actualmente existen herramientas gráficas que el fabricante en específico desarrolla para una mejor administración de

sus equipos. Este tipo de herramientas trabajan con métodos estándar de configuración, monitoreo de protocolos internet y dispositivos a través del protocolo llamado SNMP (Simple Network Management Protocol). SNMP manipula datos de administración dentro de un dispositivo de Internet, tal como un enrutador. Este tipo de administración requiere de información base del dispositivo para poder administrarlo comúnmente llamado MIB. Las MIB´s más comunes dentro de OSPF son:

	OspfGeneralGroup
	Parámetros globales de OSPF
	.ospf.1
	OspfAreaTable
	Parámetros del área específica
	INDEX area ID
	.ospf.2
	OspfStubAreaTable
	Anuncios default dentro de áreas Stub
	INDEX area ID, TOS
	.ospf.3
	OspfLsdbTable
	Accesa a la base de datos Link State de área específica
	INDEX area ID, LS type, Link state ID, Adversising roture
	.ospf.4
	OspfHostTable
	Anuncios de host directamente conectados
	INDEX HostIP address, TOS
	.ospf.6
	OspfIfTable
Ospf MIB (14)	Parámetros específicos de una interfaz OSPF
1.3.6.1.2.1.14	INDEX Interface IP address, MIB-II IfIndex
	.ospf.7
	OspfIfMetricTable
	Costo de la interfaz de OSPF
	INDEX interface IP address, IfIndex, TOS
	.ospf.8
	OspfVirtIfTable
	Parámetros de Virtual Links de una interfaz OSPF
	INDEX area ID, Neighbor Roture ID
	.ospf.9
	OspfNbrTable
	Enrutadore vecinos de OSPF
	INDEX Neighbor IP address, IfIndex
	.ospf.10
	OspfVirtNbrTable
	Parámetros de de Virtual Links de vecinso en OSPF
	INDEX area ID, Neighbor Roture ID
	.ospf.11
	OspfExtLsdbTable
	Acceso a Link State Advertisements globales
	INDEX LS type, Link state ID, Advertising Router
	.ospf.12
	OspfAreaAggregateTable
	Sumarización de direcciones en los límites de área
	INDEX area ID, LS type, net, mask
	.ospf.14

III.8 Interacción con otros protocolos

OSPF debe de ser capaz de interactuar con otros protocolos de enrutamiento como lo son: RIP, IGRP, BGP, etc., debido a que, si dentro del mismo AS por cierta razón, se tiene configurado diferentes protocolos de enrutamiento y cada uno de estos protocolos conoce ciertas redes, las redes que estén configuradas dentro de un protocolo jamás va a ser entendidas o alcanzadas por el otro protocolo, en cambio si interactuan entre sí, todas las redes van a ser conocidas y alcanzadas por cualquier otro protocolo. A esta interacción se le conoce como redistribución.

III.9 Seguridad y Autenticación en OSPF

Los enrutadores que este corriendo el mismo proceso de enrutamiento de OSPF pueden decidir si el enrutador que les esté haciendo una petición puede o no participar en el dominio de enrutamiento basados en un password predefinido. OSPF por omisión utiliza un password nulo lo que significa que no se encuentra habilitada la autenticación, sin embargo OSPF utiliza un método de autenticación por password muy sencillo que se agrega a cada paquete de enrutamiento.

Este método de autenticación permite que un password sea configurado por cada área dentro del AS. Cada enrutador en la misma área que quiera participar en el dominio de enrutamiento tendrá que configurarse. La desventaja de este método es que es vulnerable a ataques pasivos, lo que significa que el password puede obtenerse fácilmente a través de un analizador de protocolos o sniffer. Sin embargo, con las nuevas versiones de los sistemas operativos de los equipos de enrutamiento se incluyen mejoras a través de autenticación criptográfica del password utilizando MD5.

III.10 Ventajas y desventajas de OSPF con respecto a otros protocolos de enrutamiento.

RIP, OSPF, BGP, IGRP e Integrated IS-IS, se pueden clasificar dentro del grupo de IGP's y EGP's. Los protocolos de enrutamiento pueden clasificarse de acuerdo a la tecnología básica de enrutamiento que emplean: Distance Vector o Link-State.

Tipo de Protocolo	Distance Vector	Link-State
IGP's	RIP	OSPF
	IGRP	Integrated IS-IS
EGP's	EGP	
	BGP	

Clasificación de protocolos de enrutamiento

Cada protocolo de enrutamiento tiene que realizar una serie de actividades básicas. Por ejemplo, un enrutador debe de ser capaz de detectar a los enrutadores vecinos. Tiene que tener un método seguro de colección de información de enrutamiento y poner estas entradas en la tabla de enrutamiento. Para entender como los protocolos de enrutamiento trabajan y así poder compararlos, se describirá a los diversos protocolos en términos de las siguientes categorías:

Tipo:

Puede ser un protocolo EGP o un IGP, si emplea tecnología Distance Vector o Link-State.

Encapsulación:

El protocolo de enrutamiento trabaja directamente sobre IP, sobre algún protocolo de transporte de Internet (TCP o UDP), o trabaja directamente sobre la capa de enlace de datos.

Métricas:

¿Cuáles son las métricas que están tomando para elegir la mejor ruta?, Es decir, RIP siempre elige como mejor ruta a aquel que tenga un menor número de saltos para llegar al destino. Otros protocolos pueden seleccionar a la mejor ruta a aquel que tenga un menor retardo, etc.

Mantenimiento y descubrimiento de vecinos:

¿Cómo un enrutador descubre a los enrutadores vecinos (llamados también "peers")?. ¿Con cual intercambia información de enrutamiento? ¿Cómo el enrutador descubre problemas con los enrutadores vecinos? Y ¿Cómo manda información de actualización?.

Eliminación de rutas:

Cuando algún destino se convierte en inalcanzable, ¿Cómo esta información es propagada por el protocolo de enrutamiento?

Cálculo de la tabla de enrutamiento:

¿Cómo el enrutador calcula las entradas de la tabla de enrutamiento de información de enrutamiento proveniente de sus vecinos?

Seguridad:

¿Cómo el protocolo se protege de intrusos que tratan de modificar datos de enrutamiento y/o que tratan de alterar los intercambios de información del protocolo?. Como ejemplo, los equipos de cómputo con sistema operativo Unix, Linux inclusive Windows NT 2000 cuentan con módulo de enrutamiento RIP (en el caso de Unix es nativo), el cual al momento de ejecutar dicho módulo empieza a intercambiar tablas de enrutamiento RIP con el enrutador debido a que no cuenta con un sistema de autenticación entre estos dispositivos. Esto quiere decir que cualquier equipo de cómputo que se conecte al segmento y prenda el módulo de enrutamiento se volverá un peer o vecino del enrutador lo que ocasionará incongruencia en las tablas de enrutamiento de todo el AS. Lo anterior no pasa con OSPF gracias al esquema de autenticación con que cuenta.

A continuación se mencionan las características generales de ciertos protocolos de enrutamiento con el cual se pueden dar una idea de cuales son las ventajas y desventajas que tiene OSPF sobre los demás protocolos.

RIP.

- Es un protocolo de compuerta interna (IGP).
- Es un protocolo estándar.
- Protocolo utilizado por las work station.
- RIP es un protocolo clásico que utiliza tecnología Distance Vector.
- Corre sobre UDP utilizando el puerto 520.
- Manda actualizaciones de tablas cada 30 segundos.
- No soporta CIDR.[1]
- RIP tomo únicamente como métrica para la elección del mejor camino es el número de saltos. El número máximo de saltos soportados por RIP es de 15, un destino que esté a 16 saltos o más es considerado como inalcanzable.
- RIP no cuenta con descubrimiento y mantenimiento de vecinos.
- RIPv1 no cuenta con seguridad.

OSPF.

- Es un protocolo de compuerta interna (IGP).
- Protocolo estándar.
- OPSF trabaja directamente sobre IP, protocolo número 89.
- Protocolo que utiliza tecnología Link-State.
- Originalmente OSPF fue diseñado para remplazar a RIP.
- Diseñado para tener una rápida convergencia.
- El corazón de OSPF consiste en crear y mantener su base de datos topológica.
- Descubre y mantiene a sus vecinos por medio de mensajes multicast (OSPF Hello packets).
- Su métrica está definida en base a un costo.
- Con respecto a la seguridad OSPF, un enrutador puede autenticar paquetes de OSPF que recibe, también puede haber una autenticación más estrecha utilizando firmas digitales en los LSAs de OSPF.
- Soporta VLSM.
- CIDR es soportado por OSPF.
- Soporte de grupos de multicast. MOSPF
- Compatibilidad con IPv6.

IGRP.

- Protocolo propietario por CISCO.
- Utiliza tecnología Distance Vector.
- Protocolo de compuerta interna (IGP).
- Trabaja directamente sobre IP, como protocolo IP 88.
- Para decisión de la mejor ruta toma en cuanta diversas métricas como lo es el retardo, ancho de banda, carga, etc.
- IGRP no tiene implementado el descubrimiento y mantenimiento de vecinos.
- La actualización de sus tablas se lleva a cabo cada 90 segundos.
- No tiene implementado ningún esquema de seguridad.

[1] RIPv2 si soporta CIDR, pero las primeras versiones de este protocolo de enrutamiento no lo soportaban.

Como nota adicional, BGP es un protocolo de compuerta externa y OSPF es un protocolo de compuerta interna, es decir, cada protocolo de enrutamiento tiene propósitos diferentes, es por eso que no pueden ser comparados.

BGP.

- Es un protocolo de compuerta externa (EGP).
- Tecnología Distance Vector.
- BGP trabaja sobre TCP por el puerto 179.
- Se utiliza para intercambiar rutas entre Sistemas Autónomos.
- Solo envía actualizaciones cuando detecta algún cambio en las tablas locales.
- Es un protocolo estándar.
- En BGP se le tiene que configurar cuáles van a ser sus vecinos en vez de que los descubra dinámicamente.
- Con lo referente a la seguridad los primeros 16 bytes de los mensajes de BGP son reservados para la autenticación. Se diseñaron algoritmos de autenticación basados en MD5.

Capítulo IV

PROPUESTA DE OSPF EN REDUNAM

IV. Propuesta de OSPF en RedUNAM

Durante el transcurso de este trabajo de tesis se han venido explicando los conceptos necesarios para exponer a estas alturas la propuesta de OSPF en RedUNAM —el funcionamiento del esquema actual de enrutamiento, su problemática, además del funcionamiento del protocolo OSPF—. Sin embargo, es conveniente antes establecer la forma en cómo se aplican las bases de diseño, vistas en el capítulo I en que se apoya esta propuesta.

Para el desarrollo de la propuesta se tomaran en cuenta los cinco puntos de diseño de redes:

- Requerimientos.
- Direccionamiento IP
- Topología de red.
- Requerimientos de hardware y software
- Implantación, monitoreo y mantenimiento de la red

Cada uno de ellos es un punto visto durante esta propuesta, donde se proponen las modificaciones, configuración, requerimientos y ventajas de manera específica, tomando en cuentas las necesidades y recursos actuales.

IV.1 Requerimientos.

Existen diversos requerimientos generales en la propuesta de diseño de la red OSPF en RedUNAM que deberán ser considerados. Dentro de ellos destacan los siguientes:

- Funcionalidad
- Escalabilidad
- Adaptabilidad
- Administrabilidad
- Costo/Beneficio

Estos requerimientos pretenden cubrir las expectativas que se establecieron en el capítulo I. Adicionalmente en cada punto del diseño general, se agregan requerimientos concernientes al punto en específico, esto es Direccionamiento IP tiene sus propios requerimientos que serán explicados en el punto correspondiente.

Funcionalidad

La red debe de operar en un 99.9 % del tiempo, ésta es definitivamente la principal directiva, ya que las redes de las diferentes dependencias internas o externas, son parte integral para que los usuarios puedan realizar su trabajo, de tal forma que se debe de saber cual es la expectativa de su operación de la red de acuerdo al diseño de la misma.

Escalabilidad

De acuerdo al crecimiento de RedUNAM la red debe de ser capaz de mantener el paso. Ya que una red que no pueda mantener el crecimiento que demanda la organización a la que da servicio es una red mal diseñada y por lo tanto no es utilizable.

La sumarización de rutas es un factor muy importante para el éxito del diseño de la red por esto en la propuesta se tomará en cuenta. Si se quiere asegurar que la red pueda crecer apropiadamente, la sumarización es el principal factor de éxito. Sin sumarización, se tendrá un diseño de direccionamiento plano con información de rutas especificas para cada host. Este tipo de diseño no es práctico para redes de gran tamaño y el crecimiento que puedan presentar.

Adaptabilidad

Se refiere a la capacidad de la red de OSPF de RedUNAM para responder a los cambios que existan en la misma. En muchos de los casos la adaptabilidad se refiere a la capacidad de la red para adaptarse a nuevas tecnologías, capacidades de anchos de banda, etc. de una manera eficiente debido a que el ámbito de las telecomunicaciones cambia de una manera muy rápida.

Administrabilidad

La red debe de contar con las herramientas necesarias para asegurar que siempre se conozca el estado de operación de sus diversos componentes, visto como un solo ente, así como de cada uno de sus componentes de manera individual. La administración del enrutamiento se simplifica gracias a la fácil resolución de problemas y la predecibilidad de OSPF, además posee toda una estructura estándar MIB dentro de la estructura de árbol de SNMP que permite hacer una administración del protocolo automatizada. Por ser estándar todos los fabricantes ofrecen soporte a OSPF y sólo se requiere agregar a la plataforma de administración que se utilice.

Costo/Beneficio

Una vez claras las cualidades que nuestro diseño debe cubrir, existan también algunas limitantes, ya que nuestro diseño deberá considerar también los recursos y presupuestos con que se dispone. Para el caso de OSPF, no se requiere gastos en equipo adicional, tampoco de recursos humanos.

Adicional a los requerimientos anteriores, existen ciertos requerimientos de diseño más prácticos que deben ser considerados:

- Confiabilidad en la red
- Retardo en la comunicación
- Cantidad de tráfico actual y futuro
- Compatibilidad con estándares y redes legadas
- Compatibilidad con estándares y tecnologías futuras
- Simplicidad en el diseño
- Facilidad de configuración

Todo los puntos antes mencionados deberán de ser tomados en cuenta a lo largo de este capítulo para que la propuesta de red real los cubra en manera de lo posible.

IV.2 Direccionamiento IP

A consecuencia de que no se consideró durante el diseño de la red actual el crecimiento que se tiene hoy en día, y aunado a que no se hace uso de direccionamiento estructurado y jerárquico, se carece de una asignación de direcciones funcional y escalable.

El direccionamiento jerárquico y estructurado básicamente se basa en la asignación de bloques de direcciones IP contiguos. Direccionamiento jerárquico y estructurado trae consigo la simplificación y una mejor administración del direccionamiento además de que incrementa la característica de escalabilidad. El direccionamiento jerárquico y estructurado viene de la mano con VLSM y CIDR; la combinación de ambos permiten mejorar el enrutamiento, ya que se reduce la complejidad y tamaño de las tablas de enrutamiento hacia el área cero y hacia los Sistemas Autónomos vecinos, y por consiguiente, las necesidades de procesamiento y memoria de los enrutadores.

Por lo anterior, para el caso de la propuesta de OSPF en RedUNAM se propone un direccionamiento jerárquico "óptimo" que cumpla con los requerimientos de funcional, escalable, adaptabilidad y de fácil administración, esperando que en un futuro se ponga en funcionamiento, si bien no esta propuesta, una similar en su estructura.

Actualmente la UNAM cuenta con dos redes clase B: 132.248.0.0 y 132.247.0.0. El bloque de direcciones de la 200.15.1.0 a la 200.15.254.0 ya no será administrado por la UNAM, esto trae como consecuencia que todas las instituciones conectadas que hacen uso de éstas, deberán de cambiar su direccionamiento a alguna de la red 132.247.0.0[1] ya que se tiene como plazo un año para llevarla a cabo. Respeto al direccionamiento actual de la red 132.248.0.0, cabe mencionar que también es recomendable una reestructuración, aunque este proyecto sea a más largo plazo que el anterior.

De cualquier forma, la reestructuración de ambas redes es necesaria debido a que la red 132.248.0.0 está siendo utilizada hasta este momento en un 90% (debido a que no se llevó a cabo una distribución adecuada) y la red 132.247.0.0, después de la reestructuración, ocupará aproximadamente un 75% de su capacidad; éstos cifras podrían mejorarse con el uso de VLSM. Adicionalmente, por cuestiones de planeación y crecimiento, la UNAM deberá solicitar un bloque de direcciones del tamaño de una red clase B (máscara de 16 bits) ante las autoridades de NIC-México o ARIN[2], dado al tamaño y crecimiento previsto a mediano plazo en la RedUNAM. Sin embargo, las autoridades antes mencionadas requieren de una justificación soportada por los siguientes puntos:

[1] El Centro de Información (NIC-UNAM) ya le está dando seguimiento a dicha reestructuración en conjunto con el Centro de Operación (NOC-UNAM)

[2] Organismo encargado de la asignación de direcciones IP a nivel mundial.

a) 80% como mínimo de utilización de los bloques actuales.
b) Uso detallado que se les da a ambos bloques.
c) Políticas de enrutamiento presuponiendo que se hace uso de características de VLSM.

Utilizando un esquema de direccionamiento estructurado y jerárquico permitirá hacer uso de las características de CIDR y VLSM; con esto se podrá poner en marcha el protocolo de enrutamiento OSPF, lo que dará la pauta para mejorar notablemente el direccionamiento actual, además se tendrán todos los requerimientos que ARIN y NIC-México necesitan para la asignación de un nuevo bloque de direcciones. Finalmente, todo lo anterior permitirá a RedUNAM mejorar los servicios de conexión que la UNAM brinda hacia diversas instituciones externas y a las suyas propias.

Con la perspectiva mostrada en el párrafo anterior se presenta lo que se considera sería el direccionamiento de IP más adecuado para hacer uso de las ventajas mencionadas anteriormente:

Dentro de RedUNAM se tienen diferentes necesidades de direccionamiento, que se pueden separar en tres partes debido a sus características y necesidades:

1. Direccionamiento en el Backbone
2. Direccionamiento numerado para enlaces WAN
3. Direccionamiento en dependencias (internas y externas)

IV.2.1 Direccionamiento en el Backbone

En el backbone se asignará de dos bloques completos de red clase C (/24) para cuestiones administrativas y operativas, aunque no se ocupen en su totalidad (Debido a políticas de RedUNAM). Estos bloques de direcciones se asignarán a los equipos que conformen el core de RedUNAM. El direccionamiento de estos bloques debe de ser lo más sencillo posible debido a cuestiones de administración y monitoreo.

Los bloques propuestos para esta tarea son: el 132.248.254.0/24 y el 132.247.254.0/24, ya que en este momento se están utilizando de esta forma, además de que se facilitaría la migración de IGRP a OSPF. Como característica adicional, los equipos de enrutamiento robustos que posean alguna dirección de este bloque deberán formar parte del área 0 de OSPF.

El bloque de direcciones sería el siguiente:

Redes:	132.248.254.0 132.247.254.0		
Clase :	B		
Máscara Natural:	255.255.0.0		
Máscara Aplicada:	255.255.255.0	Máscara 24 bits	
No. de subredes:	1 c/u	**Utilizables:**	1 c/u
No. De hosts por subred:	256	**Utilizables:**	254

IV.2.2 Direccionamiento en enlaces WAN numerados

Para los enlaces WAN que requieran de direccionamiento IP para su funcionamiento (debido a las características de los equipos, ya que lo más común es configuración de enlaces sin direccionamiento IP), será necesario el uso de varias subredes, cada una de ellas con dos direcciones IP utilizables, que se asignarán para numerar dicho enlace. Actualmente se están utilizando diferentes redes y subredes con diferente enmascaramiento lo cual trae como consecuencia el desperdicio de muchas direcciones IP. Para resolver este tipo de problemas, se propone el rango de redes siguientes: 132.247.0.0 y 132.247.255.0[3] con máscara 255.255.255.252, es decir,

La red 132.247.0.0/30

Red :	132.247.0.0		
Clase :	B		
Máscara Natural:	255.255.0.0		
Máscara Aplicada:	255.255.255.252	Máscara 30 bits	
No. de subredes:	64	**Utilizables:**	62
No. de hosts por subred:	4	**Utilizables:**	2

No.	ID RED	BROADCAST	RANGO
0	*132.247.0.0*	*132.247.0.3*	*132.247.0.1 - 132.247.0.2*[4]
1	132.247.0.4	132.247.0.7	132.247.0.5 - 132.247.0.6
2	132.247.0.8	132.247.0.11	132.247.0.9 - 132.247.0.10
...	...	...	...
...	...	...	...
61	132.247.0.244	132.247.0.247	132.247.0.245 - 132.247.0.246
62	132.247.0.247	132.247.0.251	132.247.0.249 - 132.247.0.250
63	132.247.0.252	132.247.0.255	132.247.0.253 - 132.247.0.254

Y la red *132.247.255.0/30* con el mismo esquema que la anterior.

Para numerar cada enlace se requiere dos direcciones IP, una para cada equipo. En el esquema de direccionamiento anterior se generan 2 direcciones IP por cada subred con su identificador de red y su dirección de broadcast. Actualmente los dos esquemas en uso para un numerar enlaces generan subredes de 254 direcciones o 6 direcciones IP utilizables, mas sus identificadores de red y de broadcast. Esto trae como consecuencia el desperdicio de 252 y 4 direcciones respectivamente, mientras en el caso propuesto no se desperdicia ninguna dirección IP.

[3] Lo mismo puede ser aplicable para las redes 132.248.0.0/30 y 132.248.255.0/30 en caso de ser necesario.

[4] La primera subred del bloque 132.247.0.0/16 con máscara de 30 bits no es utilizable por ser el identificador de toda la clase B.

A continuación se presenta en una tabla la problemática mencionada.

Para numerar el enlace de una abonado externo se está utilizando la siguiente subred, en el cual se desperdician 4 direcciones.

Identificador de Subred	192.100.199.224/29
Dirección IP equipo UNAM	192.100.199.230
Dirección IP equipo abonado	192.100.199.229
Dirección IP broadcast Subred	192.100.199.231
Direcciones desperdiciadas	192.100.199.225- 192.100.199.228

Esquema de direccionamiento anterior

En otros casos para numerar un abonado interno se desperdicia todo un bloque clase C, debido a que en el enrutamiento classful[5] de IGRP una red no puede subnetearse dos veces.

Identificador de Subred	132.248.181.0/29
Dirección IP equipo UNAM	132.248.181.254
Dirección IP equipo abonado	132.248.181.253
Dirección IP broadcast Subred	132.248.181.255
Direcciones desperdiciadas	132.248.181.1- 132.248.181.252

Esquema de direccionamiento anterior

Adicionalmente cuando se hace necesario subnetear, se desperdicia la primera y última subred (ya que identifican a la red, sea la clase que sea, en el caso de la UNAM es una clase B 132.247.0.0/16 y su correspondiente dirección de broadcast 132.247.255.255). Con el tipo de enmascaramiento anteriormente mencionado, solamente se desaprovecharían 4 direcciones IP de la primera y última subred, mientras en el direccionamiento con el cual contamos en la actualidad se desperdicia todo un bloque clase C o 256 direcciones IP y en el mejor de los casos se desperdician únicamente 8 direcciones IP de la primera y última subred.

IV.2.3 Direccionamiento en dependencias internas y externas

Debido a las diversas actividades que se desarrollan en cada una de las dependencias de la UNAM e instituciones externas, cada una de ellas requiere de diferentes servicios de red, y por tanto de direccionamiento. Algunas requerirán conexión a las supercomputadoras, mientras algunas otras únicamente requerirán de servicios de su red local; pero en su gran mayoría requerirán acceso a Internet, lo que hace necesario su conexión a RedUNAM. Debido a ello, se hace necesario el

[5] Direccionamiento típico que no soporta VLSM y CIDR.

enrutamiento de dicha dependencia para que tenga acceso a cualquier parte de Internet. Este es el punto que concierne a esta tesis, resolver los problemas de direccionamiento y enrutamiento para cada una de las dependencias de acuerdo a sus necesidades muy particulares.

Por lo anterior para resolver el direccionamiento y enrutamiento particular de cada una de las redes LAN de las diferentes dependencias conectadas a la RedUNAM se propone una asignación de direcciones formada por uno o varios bloques consecutivos de direcciones IP —bloques de múltiplos de 2, 8,16, 32, etc., esto en base al formato binario para hacer un mejor subneteo— como se ejemplifica a continuación:

132.247.1.0 /28

00000001.00000000	132.247.1.0
00000001.00000001	132.247.1.1
00000001.00000010	132.247.1.2
00000001.00000011	132.247.1.3
00000001.00000100	132.247.1.4
00000001.00000101	132.247.1.5
00000001.00000110	132.247.1.6
00000001.00000111	132.247.1.7
00000001.00001000	132.247.1.8
00000001.00001001	132.247.1.9
00000001.00001010	132.247.1.10
00000001.00001011	132.247.1.11
00000001.00001100	132.247.1.12
00000001.00001101	132.247.1.13
00000001.00001110	132.247.1.14
00000001.00001111	132.247.1.15

132.247.1.16 /28

00000001.00010000	132.247.1.16
00000001.00010001	132.247.1.17
00000001.00010010	132.247.1.18
00000001.00010011	132.247.1.19
00000001.00010100	132.247.1.20
00000001.00010101	132.247.1.21
00000001.00010110	132.247.1.22
00000001.00010111	132.247.1.23
00000001.00011000	132.247.1.24
00000001.00011001	132.247.1.25
00000001.00011010	132.247.1.26
00000001.00011011	132.247.1.27
00000001.00011100	132.247.1.28
00000001.00011101	132.247.1.29
00000001.00011110	132.247.1.30
00000001.00011111	132.247.1.31

132.247.1.32 /28

00000001.00100000	132.247.1.32
00000001.00100001	132.247.1.33
00000001.00100010	132.247.1.34
00000001.00100011	132.247.1.35
00000001.00100100	132.247.1.36
00000001.00100101	132.247.1.37
00000001.00100110	132.247.1.38
00000001.00100111	132.247.1.39
00000001.00101000	132.247.1.40
00000001.00101001	132.247.1.41
00000001.00101010	132.247.1.42
00000001.00101011	132.247.1.43
00000001.00101100	132.247.1.44
00000001.00101101	132.247.1.45
00000001.00101110	132.247.1.46
00000001.00101111	132.247.1.47

132.247.1.48 /28

00000001.00110000	132.247.1.48
00000001.00110001	132.247.1.49
00000001.00110010	132.247.1.50
00000001.00110011	132.247.1.51
00000001.00110100	132.247.1.52
00000001.00110101	132.247.1.53
00000001.00110110	132.247.1.54
00000001.00110111	132.247.1.55
00000001.00111000	132.247.1.56
00000001.00111001	132.247.1.57
00000001.00111010	132.247.1.58
00000001.00111011	132.247.1.59
00000001.00111100	132.247.1.60
00000001.00111101	132.247.1.61
00000001.00111110	132.247.1.62
00000001.00111111	132.247.1.63

132.247.1.64 /28

00000001. 01000000	132.247.1.64
00000001. 01000001	132.247.1.65
00000001. 01000010	132.247.1.66
00000001. 01000011	132.247.1.67
00000001. 01000100	132.247.1.68
00000001. 01000101	132.247.1.69
00000001. 01000110	132.247.1.70
00000001. 01000111	132.247.1.71
00000001. 01001000	132.247.1.72
00000001. 01001001	132.247.1.73
00000001. 01001010	132.247.1.74
00000001. 01001011	132.247.1.75
00000001. 01001100	132.247.1.76
00000001. 01001101	132.247.1.77
00000001. 01001110	132.247.1.78
00000001. 01001111	132.247.1.79

132.247.1.80 /28

00000001. 01010000	132.247.1.80
00000001. 01010001	132.247.1.81
00000001. 01010010	132.247.1.82
00000001. 01010011	132.247.1.83
00000001. 01010100	132.247.1.84
00000001. 01010101	132.247.1.85
00000001. 01010110	132.247.1.86
00000001. 01010111	132.247.1.87
00000001. 01011000	132.247.1.88
00000001. 01011001	132.247.1.89
00000001. 01011010	132.247.1.90
00000001. 01011011	132.247.1.91
00000001. 01011100	132.247.1.92
00000001. 01011101	132.247.1.93
00000001. 01011110	132.247.1.94
00000001. 01011111	132.247.1.95

132.247.1.96 /28

00000001. 01100000	132.247.1.96
00000001. 01100001	132.247.1.97
00000001. 01100010	132.247.1.98
00000001. 01100011	132.247.1.99
00000001. 01100100	132.247.1.100
00000001. 01100101	132.247.1.101
00000001. 01100110	132.247.1.102
00000001. 01100111	132.247.1.103
00000001. 01101000	132.247.1.104
00000001. 01101001	132.247.1.105
00000001. 01101010	132.247.1.106
00000001. 01101011	132.247.1.107
00000001. 01101100	132.247.1.108
00000001. 01101101	132.247.1.109
00000001. 01101110	132.247.1.110
00000001. 01101111	132.247.1.111

132.247.1.112 /28

00000001. 01110000	132.247.1.112
00000001. 01110001	132.247.1.113
00000001. 01110010	132.247.1.114
00000001. 01110011	132.247.1.115
00000001. 01110100	132.247.1.116
00000001. 01110101	132.247.1.117
00000001. 01110110	132.247.1.118
00000001. 01110111	132.247.1.119
00000001. 01111000	132.247.1.120
00000001. 01111001	132.247.1.121
00000001. 01111010	132.247.1.122
00000001. 01111011	132.247.1.123
00000001. 01111100	132.247.1.124
00000001. 01111101	132.247.1.125
00000001. 01111110	132.247.1.126
00000001. 01111111	132.247.1.127

Habrá dependencias que requieran en promedio de 10 hosts mientras habrá otras que requieran aproximadamente de un ciento de direcciones para hosts. Para el primer caso se asignaría un bloque de 16 direcciones, mientras para la segunda dependencia se asignarían un bloque 96 direcciones: esto equivale a tener 6 bloques de 16 direcciones, con el cual se tiene un rango de 94 direcciones válidas manejando VLSM *(Enmascaramiento de Longitud Variable)*.

Observando el cuadro anterior la primer dependencia podría utilizar la red:

132.247.1.16 /28

Red :	132.247.1.16		
Clase :	B		
Máscara Natural:	255.255.0.0		
Máscara Aplicada:	255.255.255.240	Máscara 28 bits	
No. De subredes:	1	**Utilizables:**	1
No. De hosts por subred:	16	**Utilizables:**	14

No.	ID RED	BROADCAST	RANGO
0	*132.247.1.16*	*132.247.1.31*	*132.247.1.17 - 132.247.1.30*

Mientras la segunda podría utilizar el bloque siguiente con una máscara menos específica:

132.247.1.32/25

Red :	132.247.1.32		
Clase :	B		
Máscara Natural:	255.255.0.0		
Máscara Aplicada:	255.255.255.128	Máscara 25 bits	
No. De subredes:	1	**Utilizables:**	1
No. De hosts por subred:	96	**Utilizables:**	94

No.	ID RED	BROADCAST	RANGO
0	*132.247.1.32*	*132.247.1.127*	*132.247.1.33 - 132.247.1.126*

Con el esquema de direccionamiento anterior se pretende una asignación de direcciones IP contigua para cada uno de los nodos que conforman la RedUNAM, es decir, se asignará un rango de direcciones IP para DGSCA, IIMAS, Zona Cultural y Arquitectura. La asignación de rangos se realizará de acuerdo a un análisis de utilización y crecimiento que ha venido presentando cada uno de ellos en los últimos años[1].

Además del rango asignado a cada nodo para cubrir las necesidades actuales, es necesario considerar posibles crecimientos en cada uno de ellos debido a que constantemente hay nuevas

[1] Dato obtenido de un estudio realizado por el Departamento de Proyectos Especiales (UNAM).

dependencias que requieren del servicio brindado por RedUNAM. A continuación presentamos la propuesta considerando los puntos antes mencionados:

Nodo	Rango en Uso (No. de Direcciones IP)	Crecimiento (No. de Direcciones IP)	Primera IP	Última IP
DGSCA	*11268*	*2502*	*132.247.1.0*	*132.247.54.255*
Arquitectura	6604	*1778*	*132.247.55.0*	*132.247.87.255*
IIMAS	13736	*4044*	*132.248.1.0*	*132.248.70.255*
Zona Cultural	41025	*5711*	*132.248.71.0*	*132.248.254.255*

Como se observa en la tabla anterior, el crecimiento estipulado en cada uno de estos nodos es variable —a consecuencia de la infraestructura instalada en cada uno de ellos— y es por esta razón que el rango de bloques de direcciones IP también lo es. Sin embargo, cabe mencionar que aunque este bloque de direcciones sea asignado, esto no significa que todo el bloque se encuentre configurado y/u operando en los equipos de enrutamiento.

A continuación se desglosa como ejemplo el esquema de direccionamiento propuesto para el nodo DGSCA y de donde se obtuvieron los datos para la propuesta de la tabla anterior:

Equipo	Rango En Uso	Rango Propuesto		Crecimiento Proyectado	
		Primera IP	Última IP	Primera IP	Última IP
Lpx Jardín Botánico	*1016*	*132.247.1.0*	*132.247.4.255*	*132.247.5.0*	*132.247.5.255*
Lpx Química E	*508*	*132.247.6.0*	*132.247.7.255*	*132.247.8.0*	*132.247.8.127*
Lpx Antropológica	*1016*	*132.247.8.128*	*132.247.11.127*	*132.247.11.128*	*132.247.12.127*
Lpx DGSCA Servidores	*508*	*132.247.12.128*	*132.247.13.127*	*132.247.13.128*	*132.247.13.255*
Lpx Anexo Ingeniería	*254*	*132.247.14.0*	*132.247.14.255*	*132.247.15.0*	*132.247.15.63*
Lpx Supercomputo	*254*	*132.247.15.64*	*132.247.16.63*	*132.247.16.64*	*132.247.16.127*
Lpx DGSCA_190	*508*	*132.247.16.128*	*132.247.18.127*	*132.247.18.128*	*132.247.18.255*
Lpx JuriquillasI	*254*	*132.247.19.0*	*132.247.19.255*	*132.247.20.0*	*132.247.20.63*
Lpx JuriquillasII	*254*	*132.247.20.64*	*132.247.21.63*	*132.247.21.64*	*132.247.21.127*
Cisco DGSCA	*6696*	*132.247.21.128*	*132.247.47.255*	*132.247.48.0*	*132.247.54.255*

NOTA:

1) La columna de "Rango en Uso" es únicamente una aproximación obtenida de acuerdo a las subredes configuradas a cada uno de los equipos mencionado, lo que no significa que todas estén en uso. Las

cifras de direcciones en uso reales requieren de un estudio más a fondo que actualmente se está llevando a cabo por parte del grupo de trabajo NICunam.

2) El direccionamiento especificado en el Cisco DGSCA con 6696 direcciones contempla las diversas redes LAN internas a la UNAM, así como también las redes LAN de las dependencias que se conectan a través de un enlace WAN.

Hasta este momento ya se cuenta con la asignación de direccionamiento IP y su posible crecimiento para cada uno de los nodos de telecomunicaciones.

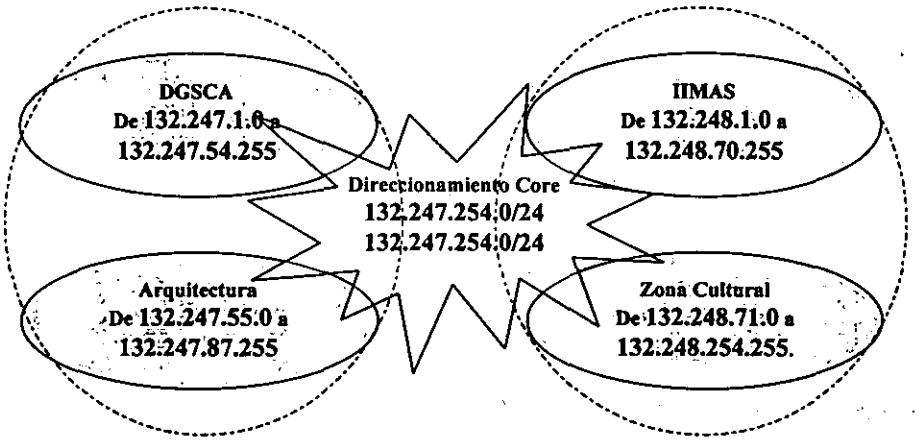


Figura 4.1 Direccionamiento en RedUNAM

Esta asignación da la pauta para proseguir al siguiente punto: Proponer las áreas de OSPF en RedUNAM

IV.3 Topología de red.

La topología que se propone utilizar en RedUNAM, es una topología jerárquica. En la topología jerárquica, la red se encuentra organizada en niveles, cada uno con funciones perfectamente distinguibles. Típicamente se divide en tres partes: core, distribución y acceso. La topología de capa de enlace y física de la red (referencia del modelo OSI) ya está implantada, como se estudió en el capitulo II (capa core, distribución y de acceso). Lo que queda por definir es la topología de nivel de red de OSI distinguiendo también los tres niveles y su correspondencia con la asignación de áreas: el core comprende el área cero compuesta por los enrutadores más robustos, la distribución compuesta por los enrutadores designados como ABR y la de acceso a los equipos enrutadores que proveen servicios a usuarios.

La técnica de asignación de áreas se utiliza comúnmente para construir redes de gran escala, tal es el caso de RedUNAM. A continuación se definen las áreas propuestas tomando en cuenta las características particulares de RedUNAM

IV.3.1 Asignación de áreas de OSPF en RedUNAM

IV.3.1.1 Área 0.0.0.0 o de Backbone

La implantación de áreas trae consigo ciertos requisitos: si un dominio de enrutamiento de OSPF se divide en más de una área, todas las demás áreas requieren conectarse físicamente al área 0.0.0.0 (aunque puede haber casos que no este físicamente conectados sino lógicamente a través de virtual links). La ventaja de que todas las áreas se conecten al área 0.0.0.0 es que limita la topología para el intercambio de enrutamiento inter-área a una simple topología de estrella lo que hace más fácil la redistribución de rutas entre las diferentes áreas y más aun si los anuncios de rutas son sumarizados.

Para el caso de RedUNAM, los equipos enrutadores robustos que conforman el backbone comparten dos subredes: la 132.248.254.x y 132.247.254.x. ambas subredes se encuentran configuradas dentro de la ELAN de administración (esta ELAN conforma el backbone de capa de enlace de RedUNAM) por lo que todos los equipos que pertenezcan a cualquiera de las dos subredes tienen una comunicación de punto a punto lo que beneficia a las tareas de enrutamiento a través de la formación de adyacencias entre los diferentes enrutadores. Se propone que todos los enrutadores con la robustez necesaria que tengan configurada en alguna de sus interfaces una dirección perteneciente a cualquiera de las subredes anteriores, esa misma interfaz pertenezcan al área 0.0.0.0. Dichos equipos cuentan con más recursos en memoria, capacidad de puertos y recursos físicos en general para soportar las tareas que conlleva el área 0.0.0.0.

Estos equipos son:

- 1 enrutador cisco 7507 en DGSCA
- 1 enrutador cisco 7200 en ZC
- 2 enrutadores cisco 7513 en ZC
- 1 enrutador cisco 4000 en Arquitectura
- 1 enrutador cisco 4700 en Astronomía
- 1 enrutador cisco AGS en Laborales

Todos los equipos anteriores deben tener configurado:

- El mismo proceso de enrutamiento OSPF 278.
- Un password establecido de antemano.
- La elección del DR debiera ser forzada al enrutador 7513 de ZC.
- El enrutador cisco 7507 en DGSCA debiera ser configurado como BDR.
- Configuración de los enrutadores 7513 de ZC y 7507 en DGSCA como ASBR ya que son los equipos que poseen los enlaces hacia las salidas internacionales.

La ELAN de administración, como cualquier otra LAN, tiene un DR y un BDR que construyen su adyacencia con todos los demás enrutadores. La elección del DR debiera ser forzada al enrutador 7513 de ZC y el enrutador cisco 7507 en DGSCA como BDR ya que el enrutador con

la mayor prioridad dentro del segmento en OSPF será elegido DR y la segunda prioridad más alta como BDR.

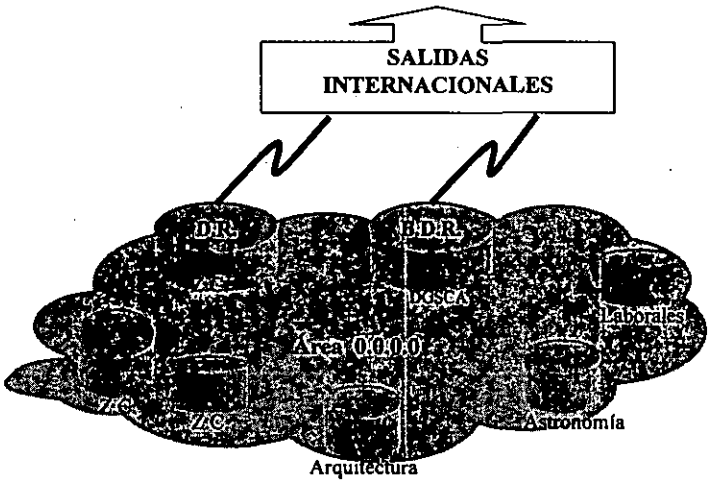


Figura 4. 2 Estructura del área 0.0.0.0 de RedUNAM

Ahora que se tiene perfectamente delimitada las funciones y componentes del área 0.0.0.0, se agregan dos áreas más por las ventajas que se especifican al final.

IV.3.1.2 Áreas 1.1.1.1 y 2.2.2.2

Adicional al área 0.0.0.0 configurada en la ELAN de Administración, se deben generar dos ELANs más en la que se configurarán diversos equipos de enrutamiento. A cada una de estas ELAN se configurará un área y para comunicarse cada una de ellas con el área 0.0.0.0 se deberá configurar dos de los enrutadores más robustos como enrutadores de borde de área (ABR). Las áreas 1.1.1.1 y 2.2.2.2 convienen sean configuradas como stub. Lo anterior explicado se ejemplifica en la figura 4.1:

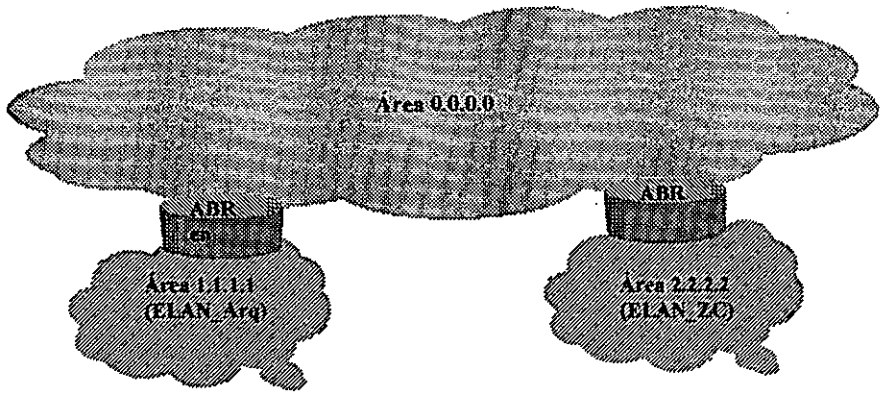


Figura 4.3 Relación del área 0.0.0.0 con las áreas 1.1.1.1 y 2.2.2.2

Para el área 1.1.1.1

- Configurar una ELAN dentro del Corebuilder 7000 del nodo de Arquitectura, llamada ELAN_Arq que fungirá como core del área.
  - Configurar los puertos correspondientes a los 7 Corebuilder 2500 del nodo DGSCA y los 6 Corebuilder 2500 del nodo Arquitectura a la ELAN_Arq antes mencionada.

- Hacer corresponder la ELAN_Arq al área 1.1.1.1 y configurar los puertos de Fast Ethernet (puertos de acceso) de los Corebuilder 2500 del nodo DGSCA y los Corebuilder 2500 del nodo Arquitectura como parte del área 1.1.1.1 configurados como área stub ya que el enrutador de ABR será su única salida para cualquier red no perteneciente a la misma área.

- Configurar los puertos ethernet que dependan del enrutador DGSCA (de manera física y por medio de LANE) al área 1.1.1.1 con stub.

- Configurar el enrutador de DGSCA más robustos como ABR, para lo cual es necesario:
  - Configurar dos interfaces virtuales, una de ellas correspondiente a la ELAN_Admin y la otra a la ELAN_Arq.
  - Configurar cada una de estas interfaces pertenecientes al área 0.0.0.0 y 1.1.1.1 respectivamente.

- Configurar los enlaces WAN que dependan del enrutador DGSCA, en donde sea posible, pertenecientes al área 1.1.1.1, así como configurar el protocolo OSPF 278 dentro del enrutador de la dependencia asignada al área 1.1.1.1

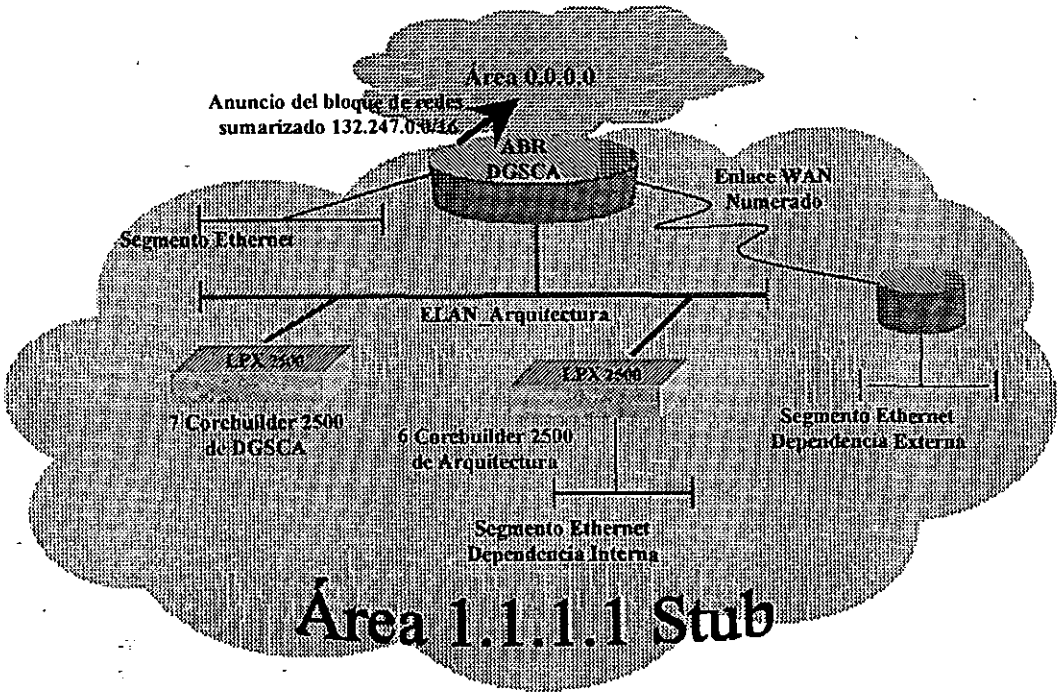


Figura 4.4 Configuración área 1.1.1.1

Para el área 2.2.2.2

- Configurar una ELAN dentro del Corebuilder 7000 del nodo de Zona Cultural, llamada ELAN_ZC que fungirá como core del área.
  - Configurar los puertos correspondientes a los 4 Corebuilder 2500 del nodo Zona Cultural y los 8 Corebuilder 2500 del nodo IIMAS a la ELAN_Arq antes mencionada.

- Hacer corresponder la ELAN_ZC al área 2.2.2.2 y configurar los puertos de Fast Ethernet (puertos de acceso) de los Corebuilder 2500 del nodo IIMAS y los Corebuilder 2500 del nodo Zona Cultural como parte del área 2.2.2.2 configurados como área stub ya que el enrutador de ABR será su única salida para cualquier red no perteneciente a la misma área.

- Configurar los puertos ethernet que dependan del enrutador de Zona Cultural (de manera física y por medio de LANE) al área 2.2.2.2 como stub.

- Configurar el enrutador de Zona Cultural más robustos como ABR, para lo cual es necesario:
  - Configurar dos interfaces virtuales, una de ellas correspondiente a la ELAN_Admin y la otra a la ELAN_ZC.
  - Configurar cada una de estas interfaces pertenecientes al área 0.0.0.0 y 2.2.2.2 respectivamente.

- Configurar los enlaces WAN que dependan del enrutador de Zona Cultural, en donde sea posible, pertenecientes al área 1.1.1.1, así como configurar el protocolo OSPF 278 dentro del enrutador de la dependencia asignada al área 2.2.2.2

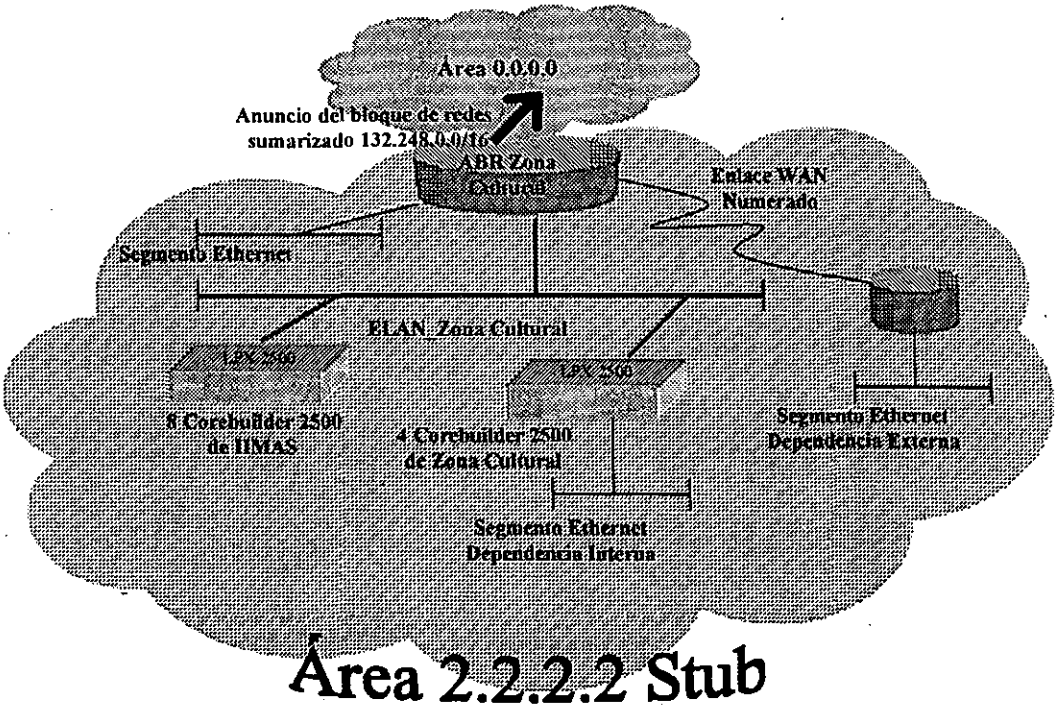


Figura 4.5 Configuración área 2.2.2.2

Para ambas áreas, los puertos Ethernet de los Corebuilder 2500 (capa de acceso hacia los usuarios) no requieren ser configurados con OSPF ya que no existe enrutador con el cual intercambiar información de enrutamiento lo que genera tráfico innecesarios e dichas interfaces.

De las ventajas de la topología antes propuesta se encuentran:

- Debido a que los Corebuilder 2500 del área 1.1.1.1 tienen configuradas direcciones IP contiguas, el direccionamiento que inyectan los ABR es de una sola ruta sumarizada hacia el área 0.0.0.0, lo que reduce la cantidad de entradas en las tablas de enrutamiento de los enrutadores del área 0.0.0.0

- La cantidad de rutas de cada IR de las áreas 1.1.1.1 y 2.2.2.2 se reduce a aproximadamente a la mitad del tamaño actual.
- La configuración de áreas stub trae como consecuencia que los enrutadores ABR no distribuyen el direccionamiento de otras áreas ni de otros Sistemas Autónomos hacia el interior de las áreas 1.1.1.1 y 2.2.2.2.
- En el caso de que la comunicación sea de una dirección dentro de un IR del área 1.1.1.1 a una dirección dentro de otro IR del área 2.2.2.2, el número de saltos son tres: de IR a ABR, de ABR a ABR y de ABR a IR.
- Con este tipo de configuración, se pueden realizar cambios en la estructura de enrutamiento acoplando las necesidades futuras de forma fácil ya que todo es por software.
- Cada una de las ELAN tiene un DR y un BDR que construyen su adyacencia con todos los enrutadores de la misma. Entre menos vecinos existan dentro de una red, se construyen menos adyacencias hacia el DR y BDR.
- La configuración de DR y BDR puede ser manipulada configurando diversos valores en RouterID.
- Se reduce los requerimientos de memoria y procesamiento de todos los equipos.
- La generación de áreas de manera jerárquica (a pesar de que la topología física en una estrella ATM) es una de las ventajas que nos ofrece LANE a través de cambios por software de los Corebuilder 7000 permitiéndonos adaptar la topología de la red de acuerdo a las necesidades. Esta ventaja también nos permite realizar cambios de topología en caso de que nuestras necesidades futuras cambien.

IV.4 Provisionamiento de hardware y software.

El equipamiento actual de RedUNAM, descrito a detalle en el capitulo II, permite la implantación de OSPF como se pudo comprobar en las pruebas realizadas con los Corebuilder 2500 y los enrutadores Cisco con que cuenta RedUNAM, por lo que en éste rubro no se presenta ningún problema. Unicamente se deben cuidar las siguientes características en los equipos, ya que durante las pruebas realizadas fue necesario adecuar algunos aspectos que se resumen en lo siguiente:

Corebuilder 2500

CoreBuilder 2500 (rev 8.6) - System ID 24fd9c
Extended Switching Software
Version 8.3.1 - Built 07/21/98 01:20:54 PM

Cisco

Todos los enrutadores Cisco soportan OSPF, desde el modelo 1005 (el enrutador más pequeño con que cuenta RedUNAM), hasta los 7513 (el equipo más robusto de Cisco y de RedUNAM). Sin embargo únicamente para el modelo de enrutador 1005 es necesario considerar las siguientes características.

Cisco 1005:

Versión ISO: IP/OPSF/PIM

Requiere de hardware: DRAM: 8Mb y Flash memory: 4MB

IV.5 Implantación, monitoreo y administración de la red OSPF

Este último paso dentro del diseño de redes de datos es también el primero ya que es un ciclo constante para el mejoramiento de la red y a medida que se monitorea y administra y se familiariza con los problemas y puntos débiles, la implantación de nuevas características pueden ser requeridas.

Empecemos con la implantación del protocolo OSPF:

Todos los equipos anteriores deben tener configurado:

- El mismo proceso de enrutamiento OSPF 278.
- Configurar la interfaz correspondiente su pertenencia a un área (0.0.0.0, 1.1.1.1 o 2.2.2.2).
- Un password establecido de antemano.
- La elección del DR y BDR puede ser forzada, configurando en un par de enrutadores mayor prioridad dentro del segmento.

Las diversas ELANs, como cualquier otra LAN, tiene un DR y un BDR que construyen su adyacencia con todos los demás enrutadores. La elección del DR puede ser forzada, ya que el enrutador con la mayor prioridad dentro del segmento en OSPF será elegido DR y lo mismo para la elección del BDR y en caso de empate el routerID más alto gana.

Como resumen, se presenta la siguiente tabla con los pasos necesarios para la configuración de OSPF en los Corebuilder 2500 y los diferentes modelos de Cisco (todos los enrutadores Cisco comparten el mismo sistema operativo y por tanto los mismo comandos). La configuración es como sigue:

Configuración	Equipo Cisco	Equipo Corebuilder 2500
Interfaz en área 0.0.0.0	***DGSCA1# router ospf 278*** ***DGSCA1#network 132.248.254.0 0.0.0.255 area 0.0.0.0***	
Interfaz en área 1.1.1.1 (2.2.2.2)	***DGSCA1# router ospf 278*** ***DGSCA1#network 132.248.254.0 0.0.0.255 area 0.0.0.0*** ***DGSCA1#area 1.1.1.1 stub***	***Select menu option (ip/ospf/areas): defineArea*** ***Enter Area ID: 1.1.1.1*** ***Is this a stub area (yes,no) [no]: yes*** ***Select menu option (ip/ospf/interface): areaID*** ***Select interface(s) (1-5|all): 2*** ***Enter Area ID [0.0.0.0]: 1.1.1.1***
OSPF 278	***DGSCA1# config terminal*** ***DGSCA1# router ospf 278***	***Select menu option (ip/ospf/interface): mode*** ***Select interface [1]:*** ***Enter OSPF mode {off,active} [off]: active***
Password	***DGSCA1# config terminal*** ***DGSCA1# interface eth 0*** ***DGSCA1#ip ospf authentication-key N0Cunam*** ***DGSCA1#router ospf 278*** ***DGSCA1# area 0.0.0.0 authentication***	***Select menu option (ip/ospf/interface): password*** ***Select interface [1]:*** ***Enter interface password [none]: N0Cunam***
Elección de DR	***DGSCA1# config terminal*** ***DGSCA1# interface eth 0*** ***DGSCA1# ip ospf priority 250***	***Select menu option (ip/ospf/interface): priority*** ***Select interface [1]:*** ***Enter priority [1]: 250***
Elección de BDR	***DGSCA1# config terminal*** ***DGSCA1# interface eth 0*** ***DGSCA1# ip ospf priority 240***	***Select menu option (ip/ospf/interface): priority*** ***Select interface [1]:*** ***Enter priority [1]: 240***
Sumarización en ABR	***DGSCA1# config terminal*** ***DGSCA1#132.247.0.0 [prefix mask] [not advertise] [tag tag]***	

En cuanto a la administración y monitoreo de OSPF:

La administración de OSPF de los equipos de enrutamiento de RedUNAM es cada día más sencilla; la mayor parte de los equipos actuales incluyen administración por consola, por sesión remota telnet, una interfaz gráfica de administración (en algunos casos propietaria) o través de un

navegador de Web con soporte a Java. Sin embargo, un punto en común para todos ellos y que sin duda nos proporciona un buen punto de partida es SNMP y el conjunto de MIB para OSPF.

OSPF posee muchas ventajas con respecto a los demás protocolos de enrutamiento ya que provee toda una estructura dentro de SNMP que permite hacer una administración del protocolo automatizada (como se vio en el capítulo III) y por ser estándar, todos los fabricantes de plataformas de administración ofrecen soporte a OSPF. Adicionalmente las diversas aplicaciones de administración propietarias de redes agregan MIBs diferentes a las estándar como valor agregado al software de monitoreo que venden, tal es el caso de Spectrum de Cabletron Systems y Transcend Networks de 3Com Corporate que también son aplicaciones de administración en uso en la actualidad en RedUNAM.

El Centro de Operación de RedUNAM (NOCunam) y el Centro de Asistencia Técnica (TACunam) se encarga actualmente del monitoreo y administración de los enrutadores Cisco y switches capa 3 Corebuilder 2500 de RedUNAM y cuenta con los elementos necesarios para establecer una administración y monitoreo del protocolo OSPF con las herramientas que se listan a continuación:

- Administración de fallas.
  Atención oportuna de problemas en la red gracias al monitoreo constante de equipos a través de plataformas de monitoreo como Domain Manager de Sun Microsystems y aplicaciones de administración como Spectrum de Cabletron Systems y Transcend Networks de 3Com Corporate que identifican alarmas críticas y permiten su notificación a los administradores por medio de servicio de *pagers*.

- Administración de contabilidad.
  Se posee un inventario con todos los equipos que conforman la red (operacionales y no operacionales) de manera manual, además las herramientas de monitoreo muestran en pantalla los diversos componentes de la red por medio de iconos lo que permite generar inventarios del equipamiento operativo de la red.

- Administración de configuración.
  Se respalda la configuración de los diversos equipos de enrutamiento por medio de programas shell generados en Unix que interactuan con los diversos equipos y respaldan la configuración por periodos de tiempo continuos de manera que se tienen configuraciones históricas. Adicionalmente se registra una bitácora con los cambios en configuración conteniendo la persona, fecha y hora de modificación.

- Administración de desempeño.
  El software de administración de redes posee herramientas gráficas que permiten saber el estado en tiempo real del desempeño de determinado componente de la red.

- Administración de seguridad.
  Se cuentan con herramientas que nos permiten bloquear y permitir el acceso desde ciertos puntos de la red a los equipos de comunicaciones, y solo se pueden accesar autenticando con un login y un password a servidores remotos y locales.

CONCLUSIONES

Después del exhaustivo estudio teórico realizado a lo largo del trabajo de tesis y las pruebas realizadas siguiendo el objetivo inicial de este trabajo "*Analizar la viabilidad de la implantación del protocolo de ruteo OSPF en el backbone de la red universitaria de datos, RedUNAM*", se puede observar que las características y ventajas de OSPF sobre cualquier otro protocolo de enrutamiento TCP/IP es evidentemente superior. Inclusive OSPF se perfila como la única opción de enrutamiento para redes complejas de gran tamaño en el caso que se desee conservar un enrutamiento con protocolos estándar.

Los inconvenientes que presenta la estructura de enrutamiento actual en RedUNAM; la dependencia de un protocolo propietario, grandes retardos, la subutilización de las capacidades de enrutamiento de diversos equipos, la incapacidad de utilización de VLSM y CIDR, etc. hace necesario la migración hacia otros esquemas que nos permitan superar estos inconvenientes, uno de ellos es el uso de OSPF.

La implantación del protocolo OSPF en la red universitaria ofrecerá las siguientes ventajas:

Establecimiento de una red jerárquica más fácil de operar y mantener, mejor administración del direccionamiento IP, utilización de CIDR y VLSM, tiempo de convergencia más rápido y debido a que es un protocolo estándar, es soportado por cualquier fabricante de computo.

Adicional a los cambios del protocolo de enrutamiento, para aprovechar todas las ventajas que ofrece OSPF, es necesario un cambio en el esquema de asignación de direcciones IP e inclusive es recomendable una reasignación de direcciones completamente diferente que permita: a) soportar el crecimiento actual y futuro, b) reducir el tamaño y complejidad de las tablas de enrutamiento y por tanto la complejidad del enrutamiento, c) que ofrezca opciones de planeación y mejor uso de direcciones IP. Esta reestructuración se debe de llevar en cooperación con el Centro de información de la Red (NICunam), y aunque es un trabajo laborioso, es recomendable llevarlo a cabo paulatinamente, dependencia por dependencia lo antes posible ya que estos cambios involucran costos que pueden incrementar con el paso del tiempo y la complejidad de la red por lo que creemos que también es recomendable un análisis costo/beneficio de estos cambios que tarde o temprano se tendrán que realizar.

Con la reestructuración del direccionamiento IP y la implantación de OSPF en el backbone de la RedUNAM, la red de la UNAM se consolidará como la red educativa más grande a nivel Latinoamérica con mejor desempeño, estructura y servicio que se verá reflejado en todas y cada una de las actividades que realiza esta casa de estudios.

APÉNDICE 1

Formato de paquetes

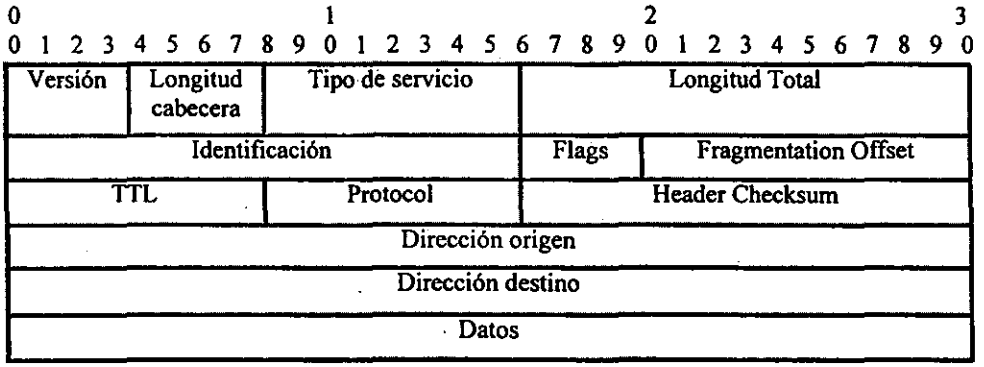
Trama IEEE 802.3

Destino	Origen	Longitud	Datos
6 bytes	6 bytes	2 bytes	46 a1500 bytes

Trama Ethernet II

Destino	Origen	Tipo	Datos
6 bytes	6 bytes	2 bytes	46 a1500 bytes

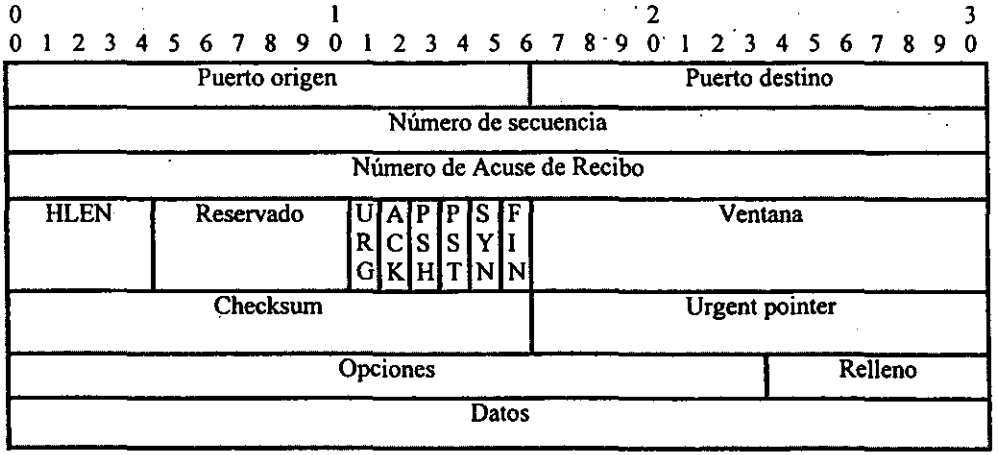
IP Headers



- Versión: Versión de IP (4), longitud de 4 bits.
- Longitud cabecera: Proporciona el encabezado del datagrama con una longitud medida en palabras de 32 bits.
- Tipo de servicio: Usualmente es cero, pero se puede ocupar cuando se requiera calidad de servicio
- Longitud Total: Proporciona la longitud del datagrama IP medido en octetos, incluyendo los del encabezado y los datos.
- Identificación: Contiene un entero único que identifica al datagrama. Permite que el destino tenga información acerca de qué fragmentos pertenecen a qué datagramas.

- Flags: utilizado para indicar si el paquete se puede fragmentar o no.
- Fragmentation Offset: Especifica el desplazamiento en el datagrama original de los datos que se están acarreando en el fragmento. Para reensamblar el datagrama, el destino debe de tener todos los fragmentos comenzando con el fragmento que tiene asignado el desplazamiento igual a 0 hasta el fragmento con el desplazamiento de mayor valor.
- Time To Live: Tiempo de vida del paquete, se utiliza para evitar congestionamiento en la red.
- Protocolo: Número que identifica al protocolo de alto nivel que se utilizó para crear el mensaje.
- Header Checksum: Complemento a dos para verificar que los datos lleguen correctos.
- Dirección origen: Dirección IP de la máquina origen.
- Dirección destino: Dirección IP de la máquina destino.

TCP Headers



- Puerto origen: Campo de 16 bits, contiene los números de puerto TCP que identifican a los programas de aplicación en los extremos de conexión.
- Puerto destino: Campo de 16 bits.
- Número de secuencia: 32 bits, El número de secuencia del primer octeto de datos en este segmento o conexión (excepto cuando el bit SYN esta encendido).
- Número de Acuse de Recibo: 32 bits, Si el campo ACK esta encendido, éste campo contiene el próximo número de secuencia que la maquina origen espera recibir.

- HLEN: Número entero que especifica la longitud del encabezado del segmento, medida en múltiplos de 32 bits.
- Reservado: 6 bits, Reservado para el futuro, deben de ser cero.
- URG: Indica si el puntero de urgente es válido o no.
- ACK: Indica si el campo de acuse de recibo es válido o no.
- PSH: Campo Push.
- RST: Reset o inicio de la conexión.
- SYN: Sincronizar números de secuencia.
- FIN: No mas datos del originador.
- Ventana: Tamaño de la ventana.
- Checksum: 16 bits, detección de errores.
- Urgent Pointer: Mecanismo utilizado para marcar los datos urgentes cuando se transmiten en un segmento, 16 bits
- Opciones: variable.
- Relleno: variable.

APÉNDICE 2

Propuesta de direccionamiento IP

Obtención del direccionamiento actual por cada uno de los site de RedUNAM en que se basa la propuesta de direccionamiento presentada en el capítulo IV.

Site DGSCA

Equipo	Rango en Uso	Rango Propuesto		Crecimiento Proyectado	
		Primera IP	Ultima IP	Primera IP	Ultima IP
Lpx Jardín Botánico	*1016*	*132.247.1.0*	*132.247.4.255*	*132.247.5.0*	*132.247.5.255*
Lpx Química E	*508*	*132.247.6.0*	*132.247.7.255*	*132.247.8.0*	*132.247.8.127*
Lpx Antropológica	*1016*	*132.247.8.128*	*132.247.11.127*	*132.247.11.128*	*132.247.12.127*
Lpx DGSCA Servidores	*508*	*132.247.12.128*	*132.247.13.127*	*132.247.13.128*	*132.247.13.255*
Lpx Anexo Ingeniería	*254*	*132.247.14.0*	*132.247.14.255*	*132.247.15.0*	*132.247.15.63*
Lpx Supercomputo	*254*	*132.247.15.64*	*132.247.16.63*	*132.247.16.64*	*132.247.16.127*
Lpx DGSCA_190	*508*	*132.247.16.128*	*132.247.18.127*	*132.247.18.128*	*132.247.18.255*
Lpx JuriquillasI	*254*	*132.247.19.0*	*132.247.19.255*	*132.247.20.0*	*132.247.20.63*
Lpx JuriquillasII	*254*	*132.247.20.64*	*132.247.21.63*	*132.247.21.64*	*132.247.21.127*
Cisco DGSCA	*6696*	*132.247.21.128*	*132.247.47.255*	*132.247.48.0*	*132.247.54.255*

Número total de direcciones para el site DGSCA: 11268

Rango total de direcciones para el site DGSCA: *132.247.1.0 - 132.248.54.255*

Site Arquitectura

Equipo	Rango en Uso	Rango Propuesto		Crecimiento Proyectado	
		Primera IP	Ultima IP	Primera IP	Ultima IP
Lpx Jardín D.G. Obras	*762*	*132.247.55.0*	*132.247.57.255*	*132.247.58.0*	*132.247.58.191*
Lpx D.G. Presupuestos	*254*	*132.247.58.192*	*132.247.59.191*	*132.247.59.192*	*132.247.59.255*
Lpx Local Arquitectura	*3048*	*132.247.60.0*	*132.247.71.255*	*132.247.72.0*	*132.247.74.255*
Lpx Facultad Arquitectura	*254*	*132.247.75.0*	*132.247.75.255*	*132.247.76.0*	*132.247.76.63*
Lpx Facultad Economía	*508*	*132.247.76.64*	*132.247.78.63*	*132.247.78.64*	*132.247.78.191*
Lpx Facultad Derecho	*254*	*132.247.78.192*	*132.247.79.191*	*132.247.79.192*	*132.247.79.255*
Lpx Facultad Filosofía	*254*	*132.247.80.0*	*132.247.80.255*	*132.247.81.0*	*132.247.81.63*
Cisco Arquitectura	*1270*	*132.247.81.64*	*132.247.86.63*	*132.247.86.64*	*132.247.87.255*

Número total de direcciones para el site Arquitectura: 6604

Rango total de direcciones para el site Arquitectura: *132.247.55.0 - 132.247.87.255*

Site IIMAS

Equipo	Rango en Uso	Rango Propuesto		Crecimiento Proyectado	
		Primera IP	Ultima IP	Primera IP	Ultima IP
Lpx Inst. Geografía	*1016*	*132.248.1.0*	*132.248.4.255*	*132.248.5.0*	*132.248.5.255*
Lpx Facultad Veterinaria	*508*	*132.248.6.0*	*132.248.7.255*	*132.248.8.0*	*132.248.8.127*
Lpx Local IIMAS	*762*	*132.248.8.128*	*132.248.11.127*	*132.248.11.128*	*132.248.12.63*
Lpx Facultad Quimica	*762*	*132.248.12.64*	*132.248.15.63*	*132.248.15.64*	*132.248.15.255*
Lpx Inst. Astronomía	*254*	*132.248.16.0*	*132.248.16.255*	*132.248.17.0*	*132.248.17.63*
Lpx Laborales	*3048*	*132.248.17.64*	*132.248.29.63*	*132.248.29.64*	*132.248.32.63*
Lpx Astronomía	*2286*	*132.248.32.64*	*132.248.41.63*	*132.248.41.64*	*132.248.43.127*
Lpx IIMAS-DGAE	*2540*	*132.248.43.128*	*132.248.53.127*	*132.248.53.128*	*132.248.55.255*
Cisco IIMAS	*2560*	*132.248.56.0*	*132.248.66.255*	*132.248.67.0*	*132.248.70.255*

Número total de direcciones para el site IIMAS: 13736

Rango total de direcciones para el site IIMAS: *132.248.1.0 - 132.248.70.255*

Site Zona Cultural

Equipo	Rango en Uso	Rango Propuesto		Crecimiento Proyectado	
		Primera IP	Ultima IP	Primera IP	Ultima IP
Lpx Centro Cultural	*762*	*132.248.71.0*	*132.248.73.255*	*132.248.74.0*	*132.248.74.191*
Lpx Coord. Humanidades	*1270*	*132.248.74.192*	*132.248.79.191*	*132.248.79.192*	*132.248.80.255*
Lpx Patronato	*1016*	*132.248.81.0*	*132.248.84.255*	*132.248.85.0*	*132.248.85.255*
Cisco Zona Cultural	*37977*	*132.248.12.128*	*132.248.235.127*	*132.248.235.128*	*132.248.254.255*

Número total de direcciones para el site Zona Cultural: 41025

Rango total de direcciones para el site Zona Cultural: *132.248.71.0 - 132.248.254.255*

GLOSARIO DE TÉRMINOS

ABR Area Border Router, Enrutador de borde de área, enrutador conectado a diversas áreas dentro de OSPF.

AS Autonomous System o Sistema Autónomo. Entidad que administra bajo sus propias políticas a un conjunto de redes y enrutadores.

ASBR Autonomous System Boundary Router, Enrutador de borde de sistema autónomo(intercambia información de enrutamiento con enrutadores de diferentes Sistemas Autónomos).

ATM Forum El Foro ATM es una organización internacional no lucrativa, creada con el objetivo de acelerar la utilización de productos y servicios ATM. Además de promover conocimiento y cooperación por parte de la Industria.

BDR Backup Designated Router, Enrutador designado de respaldo.

BGP Border Gateway Protocol (Protocolo de Compuerta Externa).

B-ISDN Broadband Integrated Services Digital Network, es una red adaptable que permite integrar a redes ya existentes. B-ISDN fue conceptualizada para utilizar infraestructura de telecomunicaciones digitales que proveerá gran desempeño para voz, datos, vídeo y servicios de multimedia. El transporte de la información de B-ISDN es vía ATM.

BR Backbone Router, Enrutador de backbone (se encuentra conectado en al menos una interfaz al área cero en OSPF).

Broadcast Mensaje enviado de una máquina a todas.

CCITT El Comité Consultativo Internacional Telefónico y Telegráfico es una organización que determina los estándares de comunicación internacional.

CIDR Classless Inter-Domain Routing (CIDR), es un mecanismo que permite anunciar un conjunto de subredes y redes a través de una sola dirección IP y una máscara (lo que se conoce como super-red).

Corebuilder 2500 Switch modular de alta funcionalidad con capacidades de enrutamiento. Dispositivo de red capas de soportar redes ethernet y fast ethernet de alto desempeño (Ver LANplex 2500).

DHCP Dynamic Host Configuration Protocol (DHCP) es una técnica de broadcast que se utiliza para obtener una dirección IP para una estación o un host en forma dinámica.

DR Designated Router, Enrutador designado.

DS-0 DS-0 Denominación americana con velocidad de 64 kbps.

DS-3	DS-3 (T3) Denominación americana que soporta 672 canales de voz, la velocidad actual es de 44.736 Mbits/seg.
DTE	Data Terminal Equipment. Equipo Terminal de Datos, provee una interfaz entre el usuario terminal y el equipo de comunicación de datos (DCE).
E1	Canal de comunicación en formato europeo (T1 formato americano). El E1 tiene capacidad para 32 canales de 64 kbps, en total 2.048 Mbps.
EGP	Exterior Gateway Protocol (Protocolo de Compuerta Externa).
EIGRP	Enhanced IGRP (Protocolo de Compuerta Interna).
Frame Relay	Protocolo de switcheo de paquetes, generalmente se utiliza para conectar redes tipo WAN.
Full-Mesh	La topología full-mesh se presenta cuando un nodo (enrutador) perteneciente a un AS se conecta con todos los demás nodos del mismo sistema. Para el caso de BGP el full-mesh se realiza en forma lógica.
Half-Duplex	Comunicación que es capaz de transmitir información (sea Tx o Rx) en una sola dirección durante un mismo tiempo.
IETF	El IETF (Internet Engineering Task Force) es una comunidad internacional de diseñadores de red, operadores, proveedores e investigadores preocupados en la evolución de la arquitectura de Internet y el refinamiento de la operación de la misma. Esta organización esta abierta para cualquier empresa o persona que este interesado en ayudar a estos propósitos.
IfIndex	El IfIndex se utiliza en MIB-II para conexiones punto a punto no numeradas Esta información se utiliza durante el proceso de construcción de tablas de enrutamiento cuando se calcula la dirección IP del próximo salto.
IGRP	Interior Gateway Routing Protocol (Protocolo de Compuerta Interna).
IPv6	Internet Protocol versión 6 también conocida como Ipng, es una nueva versión de IP actualmente investigada y revisada por la IETF.
IR	Internal Router, Enrutador interno (sólo se encuentra dentro de un área en OSPF).
ISIS	Integrated Intermediate System to Intermediate System Protocol (Protocolo de Compuerta Interna).
ITU-T	La ITU-T (Sector Telecomunicaciones) cumple con los propósitos de la ITU (International Telecommunication Union), la estandarización de las telecomunicaciones derivado de estudios técnicos, operativos, etc.
LAN	Local Area Network. Red de Área Local.

LANplex 2500	Switch modular de alta funcionalidad con capacidades de enrutamiento. Dispositivo de red capas de soportar redes ethernet y fast ethernet de alto desempeño (Ver CoreBuilder 2500).
LSA	Link State Advertisement, Anuncio link-state.
MAN	Metropolitan Area Network, Red de Área Metropolitana.
MD5	Message Digest 5. Algoritmo creado en 1991, utilizado para crear firmas digitales.
MIB	Management Information Base, base de datos de objetos que pueden ser monitoreados por un sistema de administración de red. SNMP y RMON utilizan el formato estandarizado MIB que permite a cualquier herramienta SNMP o RMON monitorear un dispositivo específico.
MIB-II	Management Information Base, version 2.
Multicast	Mensaje enviado de un origen a muchos destinos (pero no a todos).
NIC	Network Information Center, Centro de información de la Red se encarga de proporcionar servicios de: Asignación de Direcciones IP, Asignación de Dominios y Servicio de Nombres.
OC-3	Optical Carrier (OC), utilizado para especificar la velocidad de la red de fibra óptica conformada por el estándar SONET. Un OC-3 es igual a 155.52 Mbps.
OSPF	Open Shortest Path First (Protocolo de Compuerta Interna).
RIP	Routing Information Protocol. (Protocolo de Compuerta Interna).
SNMP	Conjunto de protocolos para la administración de redes complejas. Trabaja enviando diferentes mensajes PDU's (Protocolo Data Unit) a los equipos activos de red llamados agentes SNMP preguntando por valores específicos almacenados en bases de datos llamados MIB's.
SONET	SONET (Synchronous Optical Network) es el estándar en Estados Unidos para la transmisión de datos síncronos sobre medios ópticos. El equivalente a SONET internacional es SDH (Synchronous Digital Hierarchy). ATM trabaja sobre SONET.
SPT	Shortest-Path Tree, Árbol de rutas más cortas, algoritmo utilizado para calcular la ruta más corta hacia algún destino en particular, por medio de anuncios link-state.
T1	Un T1 consiste de 24 canales de 64 kbps cada uno. Cada canal puede ser utilizado para transportar voz o datos.

TDM Time Division Multiplexing, Multiplexación por División de Tiempo. Tipo de multiplexación, en el cual varias señales pueden ser transmitidas por un mismo medio, asignando a cada una de estas señales un instante de tiempo para ser enviadas a través del medio.

VLSM VLSM (Variable Length Subnet Masks), se refiere a que una red puede ser configurada con diferentes máscaras de red. VLSM es una extensión del subneteo básico donde las redes clase A, B y C pueden ser subneteadas utilizando una máscara de longitud variable.

WAN Wide Area Network. Red de Área Amplia.

BIBLIOGRAFÍA

3Com Corporation [1999], Network Administration Guide (Transcend), 3com, Santa Clara, California.

BAKER, F, COLTUN, R. [1991], RFC1252: OSPF version 2 Management Information Base, Network Working Group.

BASSAM, HALABI [1997], Internet Routing Architectures, Cisco Press, Indianapolis, IN.

E. COMER, DOUGLAS [1998], Redes Globales de información con Intenet y TCP/IP, Prentice-Hall, 3a. Edición, Purdue University, USA.

MOY, J [1994], RFC1583: OSPF version 2, Network Working Group.

QUINN-ANDRY, TERRY, HALLER, KITTY [1998], Designing Campus Networks, Cisco Press, Indianapolis, IN.

STALLINGS, WILLIAM [1997], SNMP, SNMPv2 and RMON, Addison Wesley, 2a Edición, USA.

T. MOY, JOHN [1998], OSPF Anatomy of an Internet Routing Protocol, Addison Wesley,USA.

OTRAS REFERENCIAS

http://192.100.196.1/diseno/pagsweb/red/basicos.htm
http://cgict.uat.mx/comunicaciones/doctec/ligas/routeo.html
http://cisco.com/warp/public/730/General/
http://home.sprynet.com/sprynet/hafeez/ECEN5050.htm
http://jaring.nmhu.edu/NetMan/labs-435.htm
http://pr.erau.edu/~whetten/classes/references/web-ref.html
http://support.baynetworks.com/library/tpubs/html/switches/bstream/115401A/L_125.HTM
http://tiny.uasnet.mx/prof/cln/ccu/mario/COMDAT/apuntes.html
http://www.3com.com/technology/tech_net/white_papers/index.html
http://www.cis.ohio-state.edu/htbin/rfc/rfc2178.html
http://www.cisco.com/cpress/cc/td/cpress/design/ospf/on0407.htm
http://www.cisco.com/spanish/warp/public/779/smbiz/events/
http://www.cisco.com/univercd/cc/td/doc/cisintwk/idg4/nd2002.htm
http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/index.htm
http://www.cisco.com/univercd/cc/td/doc/product/software/ssr90/rpc_r/54043.htm
http://www.disc.ua.es/asignaturas/rc/trabajos/atm/Atm.html
http://www.disc.ua.es/asignaturas/rc/trabajos/atm/Atm.html
http://www.farmington.k12.mo.us/CIE/RFC/791/index.htm
http://www.ietf.org/html.charters/ospf-charter.html
http://www.infotech.tu-chemnitz.de/~paetz/atm/
http://www.mctnow.com/ntwrktxt.htm
http://www.merit.edu/~nanog/mtg-9806/ppt/berkowitz/index.htm
http://www.techfest.com/networking/netmgmt.htm
http://www.teltrend.co.nz/documentation/rel72/html/osp001.htm
http://www.uni-osnabrueck.de/vorlesungen/informatik/networking-programming/RFCs/1247.txt