01130
21

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERÍA

ANÁLISIS PARA LA IMPLEMENTACIÓN DE CALIDAD DE SERVICIO EN EL BACKBONE DE REDUNAM.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN TELECOMUNICACIONES
P R E S E N T A N :
LANDIN ROBLES ALEJANDRO CÉSAR
NIETO HIDALGO MARCO ANTONIO

DIRECTOR DE TESIS: DR. MIGUEL MOCTEZUMA FLORES

CUIDAD UNIVERSITARIA 2003.

A

AGRADECIMIENTOS.

A Dios.
Por tu presencia continua en mi vida, por hacerme sentir que soy especial, por tu protección y por las bendiciones que de una u otra forma has prodigado a mi familia. Por haberme dado el tiempo, el espacio y la voluntad para superar esta barrera, ahora te pido sabiduría para aprovechar lo aprendido a favor de una superación profesional y personal que me haga ser la persona que tu quieres que sea.

A mis Padres:
Nunca podré expresar en toda su dimensión el inmenso agradecimiento que siento, lo único que puedo decir es que sin ustedes no estaría aquí, con las expectativas e indefiniciones de toda una vida por delante pero con las herramientas que su sentido común me brindaron y que he aprendido a valorar con el paso del tiempo. Gracias papá, gracias mamá por todo lo que pudieron darme, ya ven no ha sido en vano y aún cuando la vida sea difícil y complicada, tengo el orgullo de llevar grabadas sus enseñanzas en mi mente y en mi corazón, con ellas todo será más fácil. Los amo mucho más de lo que se imaginan, con todo respeto y admiración les dedico este trabajo, que Dios los bendiga siempre.

A Chelín:
Por tu gran amor y dedicación, y por ser lo más especial en mi vida, pero sobretodo, por el milagro que estamos a punto de recibir. "Te amo".

A mi familia:
Mis hermanos Gina, Lety, Mario y Emma, por las experiencias vividas, por su apoyo incondicional durante mi formación profesional y por ser esa gran familia que es.

Anilu, Nelly y Arturo, por todo el apoyo brindado, por ser cómplices de nuestros grandes sucesos, pero sobretodo por la gran amistad que nos une.

A mis amigos:
Estela, Marco y Teck por hacer que esta experiencia reafirmará el propósito de ser mejores.

A todos aquellos que forman parte en mi vida.

A la UNAM.
Por las herramientas brindadas en mi formación profesional.

Gracias.

Alex.

"Al oír que dice el bruto: <Yo solo me he hecho a mi mismo >, pensamos en lo mal escultor que ha sido."
Ramón Gómez de la Serna

- **A mis papas.**

Gracias a su infinito amor y a su guía he podido llegar a ser lo que soy actualmente. Este trabajo es para ustedes.

- **A Erika y Luis Antonio.**

Ya que el amor que me tienen me ayudó a salir en los peores momentos.

- **A Laura.**

Por ser y estar incondicionalmente siempre en las buenas en las malas y en las peores. Mi gran amiga.

- **A Carlos, Nancy, Juan Carlos, Marissa, Ceci, Guille, Karla, Tela y Teck.** Mis amigos.

Por brindarme su amistad incondicional ya sea de años o reciente. Por muchos de los mejores momentos.

- **A Claudia y Alejandro.**

- **A Teck.**

Sin él este trabajo no hubiera sido posible llevarlo a su fin.

- **A Marisela.**

Por ser la mujer de mi vida. La que me acompañó incondicionalmente en este arduo camino. Por ser quien me enseñó lo que es amar realmente. Por ser ese motor que mueve en fase tanto el corazón como la cabeza. Por ser ese motivo para seguir adelante dando lo mejor de uno mismo. Te amo.

Además:

- **A la UNAM.**

Por se la forjadora de los mejores Ingenieros del país.

- **A DGSCA.**

Por el apoyo a los estudiantes y enseñarles lo que es trabajar con verdadero profesionalismo.

- **Al Ing. Antonio González Velázquez, al Ing. Francisco Becerril Caballero, y en especial, a la Ing. Gabriela Medina Galindo.**

Porque siempre confiaron en mi, en mi trabajo y en mi potencial, ayudandome siempre a explotarlo de la mejor manera.

- **A Dios.**

Por haberme permitido llegar hasta aquí.

Gracias.
Marco

Este trabajo fue elaborado en colaboración con el C. Teck Aguilar Chiu, la C. Estela Serrato Ramírez., y con la Subdirección de Redes y Comunicaciones de la DGSCA-UNAM.

"Permítanme que me explique.
Reconozco que el hombre es un animal creador,
condenado a perseguir conscientemente un fin
y dedicarse al arte de la Ingeniería, es decir,
a abrirse camino de manera constante e ininterrumpida
hacia donde quiera que sea."

Memorias del Subsuelo
Fedor Dostoyevsky

E

ÍNDICE.

INTRODUCCIÓN.....I

CAPITULO I. TECNOLOGÍAS DE REDES..... 1
1.1. Redes de Comunicaciones..... 1
1.1.1. Modelo de Referencia OSI..... 2
1.2. Ethernet..... 3
1.2.1. Características..... 4
1.3. Fast Ethernet (IEEE 802.3u)..... 4
1.4. Gigabit Ethernet (1Gb Ethernet)..... 5
1.5. Modo de Transmisión Asíncrona(ATM)..... 7
1.6. VLANs. Redes de área Local Virtuales..... 9
1.6.1. Como trabajan las VLAN's..... 11
1.6.2. Tipos de VLAN's..... 11
1.7. VTP Virtual Trunk Protocol..... 13

CAPITULO II. MoDelo de referencia TCP/IP **15**
2.1. TCP/IP 15
2.1.1. Modelo TCP IP 16
2.1.2. Protocolos de Internet: IP e ICMP 18
2.1.2.1. Protocolo IP 18
2.1.2.2. Protocolo ICMP 19
2.1.3. Protocolos de Capa de transporte: TCP y UDP 19
2.1.3.1. Protocolo TCP 19
2.1.3.2. Protocolo UDP 20
2.1.3.3. Protocolos de seguridad en IP: IPSec 21
2.1.4. Direccionamiento IP 22
2.1.4.1. Subredes 23
2.1.5. Enrutamiento entre Dominios sin Clase. CIDR 25
2.1.5.1. Super-redes 25
2.1.6. VLSM (Variable Length Subnet Mask) 25
2.2. Enrutamiento IP 26
2.2.1. Arquitectura de Enrutamiento 26
2.2.2. Clasificación 27
2.2.2.1. Estáticos o Dinámicos 27
2.2.2.2. De trayectoria sencilla o de Multitrayectoria 27
2.2.2.3. Plano o Jerárquico 27
2.2.2.4. Extradominio o Intradominio 27
2.2.2.5. Estado del Enlace o Vector de Distancia 27
2.3. Protocolos de Enrutamiento 27
2.4. Servicios 28
2.4.1. Voz sobre IP (VoIP) 28
2.4.1.1. Direccionamiento 29
2.4.1.2. Señalización 29
2.4.1.3. Compresión de Voz 29
2.4.1.4. Transmisión de Voz 29
2.4.1.5. Control de la Transmisión 29
2.4.1.6. Ventajas de la Tecnología de Voz sobre IP 30
2.4.2. H.323 Video 30
2.4.2.1. Arquitectura H.323 31
2.4.2.2. Componentes definidos en H.323 32
2.4.3.2.1. Terminales 32
2.4.3.2.2. Enrutador 32
2.4.3.2.3. Gatekeeper 33
2.4.3.2.4. Unidad de Control Multipunto, MCU 33
2.4.3.3. Protocolo de Inicialización de Sesión (SIP) 33
2.4.4. IP Multicast 34

CAPITULO III. MODELOS DE CALIDAD DE SERVICIO. **37**
Arquitecturas de Calidad de Servicio 37
3.1. Parámetros de Calidad de Servicios en el Tráfico 37
3.1.1. Retraso o latencia 38
3.1.2. Variabilidad del retraso (jitter) 38
3.1.3. Capacidad 40
3.1.4. Pérdida de tráfico 40
3.2. Tipos y características del tráfico 40
3.2.1. Voz 40
3.2.2. Video 41
3.2.3. Datos 41
3.3. Calidad de Servicio en IP 41
3.3.1. Servicios Integrados INT-SERV 42
3.3.1.1. Protocolo de reserva de recursos (RSVP) 43
3.3.1.1.1. Funcionamiento básico 45

3.3.1.1.2. Encabezado RSVP 46
3.3.2. Servicios Diferenciados. (DIFF-SERV) 48
3.3.2.1. Definición del campo DS. 48
3.3.2.2. Comportamiento por salto (PHB). 49
3.3.2.3. Dominios QoS. 51
3.3.3. Conmutación por Etiquetamiento de Multiprotocolos (MPLS) 51
3.3.3.1. Configuración de túneles LSP's 53
3.3.3.2. Distribución de etiquetas. 55
3.3.3.2.1. Protocolo de Distribución de Etiquetas LDP. 56
3.3.3.2.2. Protocolo de Distribución de Etiquetas basado en restricciones de Ruteo.(CBR-LDP). 57
3.3.3.2.3. Extensiones para túneles LSP (RSVP). 58
3.3.4. Ingeniería de tráfico. 59
3.3.5. Administración de Ancho de Banda en subredes SBM. 61
3.3.6. IEEE 802.1 Q/D/p. 62
3.3.7. Acuerdos de Nivel de Servicio (SLA) y Definición de Políticas. 64
3.3.8. Soporte QoS para servicios Multicast. 66
3.3.8.1. Soporte RSVP para Multicast. 67
3.3.8.2. Soporte DiffServ para Multicast. 67

CAPITULO IV. DESCRIPCIÓN Y NECESIDADES DE CALIDAD DE SERVICIO EN EL BACKBONE DE REDUNAM. 68
4.1 Historia de RedUNAM. 68
4.2. Descripción del backbone actual de RedUNAM. 70
4.2.1. Capa de Backbone o Core. 71
4.2.2. Capa de Distribución. 71
4.2.3. Capa de Acceso. 71
4.2.4. Migración al tecnología Gigabit-Ethernet. 72
4.2.4.1. Capa de backbone ó core. 73
4.2.4.2. Capa de distribución. 74
4.3. Servicios de comunicación ofrecidos. 75
4.4. Configuración de enrutamiento en el backbone. 78
4.5. Características principales y necesidades de los diferentes tipos de tráfico. 78
4.6. Necesidad del establecimiento de calidad de servicio en la RedUNAM. 79

CAPITULO V. ESTUDIO PARA LA IMPLEMENTACION DE CALIDAD DE SERVICIO EN EL BACKBONE DE REDUNAM. 81
5.1. Proceso de diseño. 81
5.1.1. Determinación de las prioridades del usuario, políticas de QoS y nivel de servicio requerido. 81
5.1.1.1. Implementación de arquitecturas de calidad de servicio. 82
5.1.1.1.1. INT-SERV y DIFF-SERV. 83
5.1.1.1.2. DIFF-SERV Y MPLS. 89
5.1.2. Caracterización del tráfico de la Red. 96
5.1.3. Monitoreo de Red. 96
5.1.3.1. Administración y monitoreo de la RedUNAM con QoS. 96
5.1.3.2. MRTG. (Multi router Traffic Grapher) 97
5.1.3.3. Spectrum. 101
5.1.3.4. Transcend Enterprise Manager. 103

CONCLUSIONES. 105

ANEXO A. **109**
1.) OSPF (Open Shortest Path First) 109
a.) Enrutamiento Jerárquico 111
b.) Áreas en OSPF 112
i) Área Backbone o Área Cero. 112
ii) Área Stub. 113
2.) Clasificación de Enrutadores. 113
a.) Enrutador Interno (Internal Router): IR 113
b) Enrutador de Borde de Área (Area Border Router) ABR. 113
c) Enrutador de Backbone (Backbone Router)BR. 114
d) Enrutador de Frontera de Sistema Autónomo (AS Boundary Router)ASBR. 114
e) Adyacencias. 114
i) Elección del DR y BDR. 114
ii.) DR y BDR. 114
f) Enrutador Designado de Respaldo, Bakup Designated Router, BDR. 115
g) Construcción de la adyacencia. 113
h) Encapsulación de paquetes OSPF en IP. 116

ANEXO B. **117**
1. Herramientas de QoS. 117
a) Regulación de tráfico. (QoS Policy and Shaping) 117
i) Token Bucket. 118
b) Administración de Congestión. (QoS Congestion management) 119
i) Cola FIFO. 119
ii) Cola de prioridad. 120
iii) Cola personalizada. 121
iv) Encolamiento Ponderado Fair (WFQ). 122
v) Encolamiento Ponderado Fair Basado en Clases (CB-WFQ). 122
vi) Prioridad IP RTP. 123
c) Técnicas para evitar la congestión (QoS Congestion Avoidance). 124
i) Liberación de la cola. (Tail Drop) 124
ii) Técnica de Detección Anticipada Aleatoria 124

ANEXO C. **126**
1) La necesidad de cambio de tecnología de protocolos. IPv6. 126
a) Dirección IPv6. 127
b) Datagrama Ipv6. 128
c) Encabezados adicionales. 130
d) Opciones de salto por salto (hop-by-hop) 131
i) Encabezado de Ruteo. 132
ii) Encabezado de fragmentación. 134
e) Seguridad en Ipv6. 134
i) Autenticación. 135
ii) Confidencialidad. 135

ACRÓNIMOS. **137**

BIBLIOGRAFÍA **144**

INTRODUCCIÓN.

CONCEPTOS BÁSICOS Y LA NECESIDAD DE UNA ARQUITECTURA DE CALIDAD DE SERVICIO.

A) CALIDAD DE SERVICIO.

Siempre que contratamos o requerimos de un servicio sea cual sea, esperamos que cumpla las expectativas que tenemos de él, ya sea rapidez, calidad, etc., de manera que se comporte en forma predecible ante casi cualquier situación. En las redes de datos sucede algo similar. El día de hoy, éstas están basadas en un modelo de "mejor esfuerzo" (*best effort*) para los servicios que proporciona. Este modelo, que es inherente a la red, se basa en que todos lo datos se manejan de forma indistinta y, si existe congestión en la red, se descartarán paquetes de la misma forma, independientemente del servicio o a quién se le esté otorgando. Este tipo de esquemas, para las necesidades actuales de los usuarios, se está convirtiendo en obsoleto, ya que en las redes actuales se mezclan servicios en los que se requiere un tratamiento especial para cada uno de ellos, como puede ser el manejo en tiempo real de algunos (caso de voz, video y aplicaciones interactivas) como de aquellos servicios en donde no se requiere.

Por esto, si no se utiliza el mismo tipo de servicio en la red, es necesario que ésta tenga alguna forma de diferenciar a cada uno, así como darle ciertos privilegios a algunos, dejando un poco de lado a aquellos servicios que por sus características no sea necesario darles algún trato especial.

La red de hoy debe poder hacer una asignación apropiada de la capacidad del manejo de tráfico dentro de esta dependiendo de la aplicación y del usuario. Esto es, debe soportar una tasa de

transmisión de datos, un retraso y los cambios en éstos de manera que la información enviada no se vea comprometida, así como adaptarse a las características de la red. Además debe soportar el manejo de identificadores tanto de aplicación como de usuario, permitiendo discriminar entre éstos, brindando así servicios basados en privilegios o bien en necesidades del servicio.

La Calidad de Servicio (QoS) se basa en una serie de reglas y procedimientos que permiten al usuario final obtener del servicio que está requiriendo lo que espera de él.

La elaboración del presente trabajo es motivada por la necesidad de que se establezcan estas reglas, y se definan y sigan los procedimientos dentro de un caso particular como lo es Red UNAM.

B) VENTAJAS DE UN SISTEMA DONDE SE ADMINISTRE EL ANCHO DE BANDA.

Existen muchas razones por las cuales contar con un sistema que tenga capacidades para manejar QoS, ahorrar dinero es una de las más importantes. Por ejemplo, si tuviéramos una política de administración de ancho de banda sobre Internet, la Voz sobre IP (VoIP) podría ahorrarnos grandes cantidades de dinero de servicio telefónico de larga distancia (si este se encuentra debidamente regulado), o bien, ahorrar en enlaces cuando queremos tener un servicio de videoconferencia entre otros. Hoy en día ya existen algunas aplicaciones de este tipo dentro de Internet, sin embargo apenas empiezan a ser conocidas y en realidad son muy aisladas.

Para el caso particular de Red UNAM, donde las líneas telefónicas están, en su mayoría, aunadas con un equipo de cómputo, sería bastante provechoso eliminar cierta infraestructura redundante para la comunicación por voz.

Otra motivación es la de proteger y asegurar que los datos que tienen importancia crítica se envíen de forma correcta. Esto nos da una pauta para cuando no solo el tipo de servicio nos es importante, si no también la información que se transporta en determinado momento.

Sin embargo, para tener un sistema así, se necesita tomar en cuenta algunas cosas, una de ellas es que no siempre se tiene, sobre todo en redes WAN, dispositivos capaces de manejar y de diferenciar cierto tipo de tráfico. Estos cuestan más dinero del que se tenía proyectado, además que el diseñar una correcta definición de reglas en las que se contemplen todas las posibilidades que nuestra red sea capaz de manejar, no es un gasto que siempre se esté dispuesto a costear, aunque no debería de visualizarse como tal, sino como una inversión que a mediano plazo comenzaría a dar frutos. Hasta el día de hoy, los sistemas con este tipo de implementaciones generalmente se tienen en lo que llamamos *última milla* en donde las tecnologías como *ISDN* y *xDSL* muestran una forma más sencilla y barata de tener esquemas de calidad de servicio, además que es mucho más barato el ancho de banda a nivel LAN que enlaces a nivel WAN, o bien, siempre hay que tomar en cuenta si el gasto del incremento del ancho de banda es más costeable que la implementación de políticas y equipo capaz de soportar QoS y administración de tráfico.

Cabe señalar que uno de los objetivos principales de este trabajo, es el de establecer las políticas y procedimientos dentro de una red LAN como lo es la red interna del *campus* universitario, pero de manera paralela se tendrían que incluir los enlaces externos (WAN) que se tienen tanto con otras instituciones como propios (pero fuera del *campus*).

Tenemos que tomar en cuenta algo adicional. Estamos en un momento en el que para ciertas aplicaciones es más barato la adquisición de ancho de banda adicional, y de esta manera no

tener que invertir tiempo y dinero en la administración de este mismo, que además, como veremos posteriormente, no es una tarea sencilla. Un esquema real de Calidad de Servicio de punto a punto, con todas las implicaciones necesarias a operar en el backbone no existe en este momento. Sin embargo, el traer ancho de banda adicional es una solución a corto plazo, ya que las demandas de este en las aplicaciones que lleguen en los próximos años, harán imposible él seguir adicionándolo, y de esta manera la red se congestionará y no se tendrá un control de las aplicaciones o de los datos que necesiten un manejo crítico, y se empezaran a descartar en la red de la misma manera que los datos comunes.

De hecho, como veremos más adelante, esta fue una de las primeras respuestas de la UNAM, ya que al cambiar su tecnología de ATM a una 1Gb Ethernet, estamos incluyendo ancho de banda, pero sin una correcta administración, cosa que podría comenzarse a plantear con el presente trabajo.

Además, este manejo de ancho de banda también nos puede ayudar a una de las tareas más importantes dentro de la red: "la seguridad de la información". Teniendo una clasificación de tipos de tráfico así como de usuarios críticos, se tiene ya el inicio de una buena infraestructura de QoS, sobre todo en redes LAN y WAN de tipo corporativo o donde se tienen muy bien definidos los alcances de los usuarios hacia la red, como por ejemplo la red de una institución educativa, como Red UNAM.

C) DIFERENTES FORMAS PARA MEJORAR EL APROVECHAMIENTO DEL ANCHO DE BANDA Y EL MANEJO DE TRÁFICO DENTRO DE UNA RED MULTI-SERVICIOS.

Una red convergente (enfocada a soportar las clases de servicios multimedia), debe satisfacer los requerimientos de retraso, variabilidad en el retraso (*jitter*), capacidad y rentabilidad (conceptos que se explicarán más adelante) de todos los servicios que va a soportar. Esta deberá de cumplir con ciertas características.

Enlaces físicos comunes.

Se debe de compartir la misma infraestructura física para todas las aplicaciones y tipos de tráfico. Esto se puede hacer teniendo desde cables UTP categoría 5, o bien el caso óptimo de tener fibra óptica multimodo para permitir Jerarquías Digitales, ya sea Pleosiocrona (*PDH*) o bien Síncrona (*SDH*).

También se debe tener una topología de red común, así como tecnologías de capa 2 que soporten dichos servicios, ya sea en un backbone de alta capacidad, como ATM, o en redes LAN con tecnología Ethernet a 10, 100 o 1000 Mbps, como se tiene actualmente en la UNAM.

Protocolos comunes en capas bajas.

El hecho de tener distintos tipos de tráfico requiere una cantidad de protocolos comunes que sirvan como punto de partida sobre los cuales las aplicaciones y los servicios se puedan desarrollar. Debido a las características y a su capacidad de adaptación a servicios, la tendencia indica que podría ser IP, que con la actual versión 4 soporta ya alguna clase de convergencia de servicios o en un futuro próximo la versión 6, con características especiales para este tipo de arquitecturas multiservicios que serán estudiadas más adelante.

Tecnologías de Conmutación (Switching) en las orillas del backbone.

Los equipos de conmutación reducen los efectos de congestión en los retrasos al medio de acceso, haciendo esto muy benéficioso para aplicaciones que son muy sensibles al retraso como lo es la voz. Además, desde la perspectiva de QoS, una arquitectura de red conmutada hasta el escritorio permite simulación de circuitos punto a punto.

Un backbone (core) de alta velocidad.

Para poder llegar a tener un *core* de alta velocidad con capacidad de administrar una gran cantidad de dominios, se deben tener esquemas de direccionamiento y enrutamiento públicos capaces de mapear a mecanismos de direccionamiento privados. Este debe tener tanto reglas de enrutamiento como de conmutación, como lo tienen sistemas del tipo *Tag Switching* de Cisco, que se ven reflejadas directamente en esquemas como lo es MPLS. El *core* debe manejar relativamente pocos clasificadores (valores del estándar 802.1p, encabezados de MPLS, características de ATM QoS o bien clases, de servicio en IP - TOS).

Lo más importante de tener todas estas características dentro de la misma red, es tener aplicaciones híbridas y hacer interactuar todos estos tipos de tráfico en medida que el usuario final tenga la posibilidad de tener herramientas transparentes para satisfacer sus necesidades.

Un manejo correcto de tráfico podría ser la solución para llegar a este fin. Esto se refiere a una correcta selección de reglas para su clasificación, y de acuerdo a esto, manejar políticas para que éste sea liberado a su destino sin que se pierda alguna de las características básicas, como en algunos casos es el manejo en tiempo real.

Un sistema que pueda manejar Calidad de Servicio puede ser creado de diversas formas:

Se pueden tener tablas y políticas configuradas localmente, logrando de esta manera hacer una mejor distribución de la carga que cada dispositivo tiene que hacer al realizar la clasificación y el manejo del tráfico. Un punto crucial en este aspecto es el tener una consistencia en el desarrollo de las políticas en todos y cada uno de los puntos. Todas estas políticas también pueden ser desarrolladas ya sea en el *core* de la red ó en los enrutadores de acceso, haciendo una clasificación local de los paquetes que le lleguen y marcándolos de alguna manera preferencial para su entrega al siguiente punto, como lo hace IP TOS y el estándar 802.1p. Al igual que en el manejo local, los dispositivos que intervienen en la liberación de los paquetes, deben inferir la forma de clasificar y manejar los diferentes tipos de tráfico de la misma manera.

Otra forma de hacer esto, es que el *host* que envía la información, solicite las características necesarias para el tráfico que va a generar, creando circuitos virtuales dedicados para éste, de manera que todos los dispositivos intermedios, dependiendo del nivel del usuario, hagan las decisiones pertinentes. Esto puede ser muy provechoso para un sistema basado en niveles de usuario, pero hacen totalmente impredecible en comportamiento de la red.

Para llevar a cabo todo esto, se debe tener, en primera instancia, una arquitectura general de políticas, para llevar requerimientos muy específicos a reglas más generales. Estas reglas deben ser susceptibles de cambios dependiendo de diversos factores como lo son la hora del día, el nivel de congestión de la red o bien la intervención del operador.

D) CARACTERÍSTICAS DEL DESEMPEÑO DE TRÁFICO.

Clasificación de tráfico.

Todos los tipos de tráfico tienen ciertas propiedades identificables dentro de cada una de las capas del modelo de protocolos que se esté trabajando. Esto se puede hacer mediante el *mapeo* o asociación de alguna clase de tráfico con algún mecanismo de manejo de este. Éste mapeo trabaja de manera correcta si los mecanismos de prioridad son configurados en todos los dispositivos que intervienen en la liberación del tráfico. Sin embargo, también se pueden manejar listas de acceso, que funcionan bien en dispositivos de frontera (como un *firewall* o bien interfaces LAN o WAN).

Definición de Políticas de Clasificación.

Las políticas de clasificación son definidas por el administrador de los recursos de la red para evitar abusos por parte de los usuarios. Además de la definición de políticas de uso de la red, el administrador debe verificar que estas sean acatadas por todos los usuarios sin excepción, así como la definición de niveles de privilegios de uso de red tanto por servicio como por usuario. Una política debe definir las reglas para que se determinen las especificaciones de cómo, cuándo y dónde la QoS será aplicada a los diferentes tipos de tráfico que atraviesan la red. Las políticas pueden ser definidas desde la estación del usuario, que aunque ayuda a la descentralización del procesamiento de las mismas, no son del todo confiables, debido a que pueden ser cambiadas por el usuario final si no se tiene un control de las actividades de dicho usuario.

Los llamados Acuerdos de Nivel de Servicio (*Service Level Agreements, SLAs*), son los que definen las garantías y responsabilidades entre los abonados y los proveedores de servicio. Estos definen especificaciones de aplicaciones punto a punto de la red que debe cumplir el proveedor de servicios de red, con base en acuerdos celebrados entre este y los usuarios finales. Estos consisten en la disponibilidad de la red, los servicios ofrecidos y las garantías que existen para su liberación, las responsabilidades que tiene tanto el que ofrece como el que usa estos servicios, etc.

Manejo de tráfico.

El sistema debe de manejar una correcta diferenciación de los distintos tipos de tráfico sin que esta afecte al desempeño de la red, como puede ser introducir algún tipo de retraso. Este retraso puede ser muy subjetivo, ya que por ejemplo, el retraso que no puede ser muy costoso en un enlace E1 (2.048 Mbps) para una red WAN, sería demasiado grande en un enlace Gigabit Ethernet (1000 Mbps). En distintos ambientes, las formas de manejar el tráfico debe de ser diferente, dependiendo del tipo de Hardware utilizado, así como las capacidades del Software instalado en éste.

Con los procesadores de alta velocidad actuales, se puede evitar los cuellos de botella en enlaces de baja velocidad simulando sistemas de "encolamiento" (*queuing*) en Software, o bien en Hardware para enlaces de alta velocidad. Es en estos enlaces en donde se agradece una buena administración del manejo de tráfico. El manejo de tráfico vía software puede ser suficiente en interfaces LAN-WAN, ya que se envía el tráfico a una velocidad relativamente baja, sin embargo, en puntos de intercambio de información entre proveedores se pueden generar retrasos en el envío de información, contra el cual no se puede hacer mucho al respecto.

Adicionales.

Además de la definición e implementación de políticas dentro de la red, los equipos componentes de esta (*switches* y *enrutadores*) deben dar la confiabilidad al administrador de la red para llevar a cabo éstas.

Existen varios componentes que una red debe tener para cumplir estas metas:

- Separación de tráfico por medio de "colas" (*queues*) de clasificación, así como una correcta administración de estas.
- Un administrador para llevar a cabo las políticas de QoS y SLA's, así como la configuración y mantenimiento de los *switches* y *enrutadores* de la red.
- Filtrado de tráfico de salida para asegurar una mayor seguridad en la red así como tener un mayor control de congestión.
- Algoritmos avanzados para la descartación de paquetes.
- Monitoreo del comportamiento de tráfico en cada interfase de salida de la red.
- Políticas para asegurar la liberación del tráfico que sea privilegiado.
- Hacer uso correcto de las tecnologías de red actuales enfocadas a QoS.

E) OBJETIVOS Y ALCANCES DEL TRABAJO.

El objetivo del presente trabajo es, que con todos los elementos descritos anteriormente, se acoplen a los recursos (tanto tecnológicos como humanos) con los cuales cuenta Red UNAM, para analizar y elaborar una propuesta de implementación del esquema de Calidad de Servicio punto a punto que este más acorde con las necesidades propias de lo que es esta red, la más grande en el ámbito educativo en América Latina.

La composición del trabajo está dividido en 5 capítulos y 3 anexos.

En el capítulo 1, se describen las tecnologías de redes de capa 2 que se utilizan más frecuentemente en el mercado. Hacemos especial énfasis a las tecnologías que se utilizan en red UNAM, como lo es Ethernet (en todas sus modalidades), ó bien ATM que era la tecnología que se utilizaba anteriormente. También describiremos brevemente el estándar 802.3p/Q que nos brinda un cierto nivel de calidad de servicio en esta capa.

En el capítulo 2, se describen los protocolos que le dan nombre al modelo de referencia TCP/IP. Se describirán las características de cada uno de ellos (tanto en la capa de red como en la capa de transporte). Se revisarán los principios de lo que es el enrutamiento IP y cómo nos ayuda a definir las rutas por dónde la información viajará. Adicionalmente explicaremos algunos de los tipos de servicios en tiempo real que IP puede soportar como lo es la Voz y la Videoconferencia.

En el capítulo 3, se describen los dos modelos definidos por la IETF para QoS: Servicios Diferenciados y Servicios Integrados. Los protocolos que se refieren a cada uno de los modelos, así como técnicas de apoyo a éstos (como el encolamiento y el uso de MPLS). También se definen las bases para la elaboración de un sistema de políticas que se pueda adecuar a las características de la red con respecto a las necesidades de los usuarios.

En el capítulo 4, se describen las características de la red en la cual se está enfocando nuestro estudio: Red UNAM. Se da un poco de historia de las tecnologías que han soportado ésta red desde el anillo de FDDI hasta el actual *"full mesh"* de 1Gb Ethernet. También se describen los

tipos de servicio que actualmente soporta la UNAM, que es lo que impulsa a buscar una arquitectura de Calidad de Servicio.

En el capítulo 5, con los conceptos revisados en el capítulo 3 y las necesidades descritas en el capítulo 4, se presentan dos arquitecturas de calidad de servicio. De estas, se describen sus características así como el cómo se implementarían dentro de la arquitectura de red UNAM, así como varios esquemas de monitoreo para estas arquitecturas.

Los anexos que contiene este trabajo es información adicional que aunque no es utilizada de forma directa en el planteamiento y solución del problema, se utilizan de referencia sobre todo en los capítulos 2, 3 y 5. El anexo A describe de forma más detallada las características del proceso de enrutamiento de paquetes IP, así como los protocolos que se utilizan para ésto en la Red UNAM. El anexo B describe técnicas de QoS que son adicionales a los modelos descritos en el capítulo 3. El anexo C dá las características básicas del protocolo IP en su versión 6, que es la base para la implementación de la red Internet 2.

El alcance del presente trabajo es el de analizar los modelos descritos de calidad de servicio, hacer una composición de estos y definir varias arquitecturas de QoS. De estas, proponer una que sea la más acorde tanto a las características como necesidades de Red UNAM y describir las ventajas y desventajas con aquella que no se eligió. Se darán los requerimientos para que este modelo sea implementado, tanto en cambio de configuraciones en los equipos existentes así como proponer cambios de equipamiento de aquellos que presenten obsolescencia para soportar los protocolos y técnicas mencionadas. Finalmente, definir etapas de implementación de acuerdo a las necesidades de Red UNAM, ya que del modelo descrito se tiene pensado obtener beneficios en la red a mediano plazo, debido a que las configuraciones y movimientos de equipo no se pueden realizar de forma inmediata.

PAGINACIÓN DISCONTINUA

I. TECNOLOGÍAS DE REDES.

1.1. REDES DE COMUNICACIONES.

Las redes de comunicaciones son, como su nombre nos indica, una infraestructura que nos permite el intercambio de información, que mientras más rápida sea, incrementa nuestras posibilidades dentro de nuestro entorno. Hoy en día lo que antes se transmitía en su estado natural analógico como es el audio y el video ya se puede transmitir de manera digital, y por tanto pueden considerarse como datos. Estos permiten que nuestra comunicación sea de manera integral al no sólo transportar texto e imágenes, sino que también puede transmitir información que implique movimientos realizados en ese momento ó bien, hablando, comunicando algo de suma importancia que puede llegar a ser en tiempo real solo con un retraso de algunos segundos debido a la distancia ó al tipo de infraestructura que estemos utilizando, todo esto bajo una sola interfaz.

Estos servicios están catalogados básicamente en dos clases, los que están orientados a conexión (*Connection-oriented services*) y los que no (*Connectionless-oriented services*).

Los primeros son análogos a un sistema telefónico, es decir, se necesita establecer la comunicación entre las partes para poder comenzar la transmisión de información. Los paquetes de información se envían al destinatario llegando en el mismo orden en que fueron enviados, sin permitir retraso, ó bien, que éste sea constante.

Los servicios orientados no-conexión son análogos al sistema postal, esto es, se envía la información sin estar seguro de que el destinatario recibió o no el mensaje, y si se envía más de un mensaje, puede que los que se enviaron primero lleguen antes o bien lleguen después, debido a posibles retardos por la línea.

1.1.1. Modelo de Referencia OSI.

Cualquier red de telecomunicaciones está compuesta por diferentes capas que permiten la correcta implementación de servicios punto a punto dentro de esta. Éstas abarcan todas las partes de las cuales es compuesta, desde la normatividad en cables hasta las aplicaciones que llegan directamente al usuario final. Algunos modelos, dependiendo de la tecnología que se esté utilizando se componen de más o menos capas, aunque siempre se utilizan los mismos elementos de red. Existe un modelo que siempre se utiliza como referencia para la definición de capas en las diferentes tecnologías. Este modelo fue propuesto por la Organización Internacional de Estándares (*ISO, International Standards Organization*), y es llamado modelo de referencia OSI (*Open System Interconnection*), y prácticamente todos los sistemas de comunicaciones se basan en él para definir el suyo.

Éste modelo consta de siete capas, las primeras dos pueden ser implementadas por hardware y definen a éste dentro del sistema de transmisión, las otras cinco se implementan por software y definen desde como se enviará la información, su formato, que rutas tomará, los métodos de seguridad hasta el cómo se presentará al usuario final. Cada una de éstas se comunica con sus dos capas vecinas (tanto hacia arriba como hacia abajo vistas de forma vertical), de manera que se recibe cierta información por una capa y se prepara para ser liberada a la siguiente. Cada una de las capas coloca ó retira cierta información para que pueda ser comprendida por la capa siguiente. Esta información es colocada en un la parte inicial de la información útil llamado encabezado. Al proceso de colocar ó remover esta información se le denomina *encapsulamiento y desencapsulamiento* respectivamente.

A continuación se menciona brevemente cada una de las capas que conforman éste modelo de referencia.

Capa Física. Es la que se encarga de definir el medio de transmisión. Se definen los tipos de cableado, interfaces de comunicación inalámbrica, códigos de línea, etc. Acepta y transmite únicamente tramas de bits, sin darles algún tratamiento especial.

Capa de Enlace. Verifica que el tránsito sobre el medio físico sea confiable, revisa el control de flujo, y verifica algunos errores que hayan acontecido en la capa física. Los equipos que trabajan a este nivel (generalmente los conmutadores) se encargan de revisar si el medio es ruidoso y de retransmitir las tramas que se necesiten, aunque con ésto existe la posibilidad de la duplicidad de información. Aquí también se le puede dar un control de flujo para estabilizar las tasas de transmisión.

Capa de Red. Se encarga del proceso del direccionamiento y enrutamiento de la información, es decir de dónde a dónde viajará determinando los saltos que tomará por los equipos intermedios. Éstas rutas pueden ser definidas por tablas estáticas de enrutamiento en los equipos, ó bien, asignadas dinámicamente dependiendo del desempeño y características de la red.

Capa de Transporte. Se encarga de dividir la información en paquetes más pequeños, y asegurar su llegada con el receptor. Hace las veces de puente entre capas, con desarrollo de protocolos de detección y corrección de errores así como de verificación de la llegada de paquetes, también define el tipo de servicio que proveerá la capa de sesión para los usuarios finales de la red. Además provee un control de flujo entre usuarios finales (no entre equipos intermedios), que hace más seguro el transporte de información.

Capa de Sesión. Permite entablar ó terminar sesiones de trabajo entre usuarios finales. Así, además de permitir el transporte de información como lo provee la capa anterior, también permite el uso de servicios adicionales que ayudan a muchas aplicaciones. Éstos servicios pueden

ser el control de dialogo (permitiendo transmisión *full duplex, simplex*), sincronización de relojes, etc.

Capa de Presentación. Esta capa está referida a la semántica y sintaxis de la información que se está transmitiendo. Le da un formato especial (como el formato ASCII) para que pueda ser entendida por las aplicaciones de la siguiente capa.

Capa de Aplicación. Es la capa que interactúa directamente con el usuario. Tiene la habilidad de establecer terminales remotas para poder hacer uso de aplicaciones de uso específico, como la transferencia de archivos.

1.2. ETHERNET.

Entre las tecnologías de redes más simples encontramos las redes de área local (LAN, *Local Area Network*) que son construidas para enlazar un conjunto de terminales (computadoras, impresoras, servidores, etc.) en una oficina. Las LAN están formadas principalmente por tres componentes: tarjetas de interfaz de red, las cuales se encargan de establecer la comunicación; conmutador ó concentrador, que se encarga de intercomunicar los diferentes elementos de la red; y el cableado. A su vez, las redes de área local adquieren diversas tecnologías que definen el comportamiento de la información, la más común es conocida como *ETHERNET*, la cual se divide en tres principales categorías dependiendo de su velocidad de transmisión, que son:

- Ethernet y IEEE 802.3 que opera a 10Mbps
- 100-Mbps Ethernet también conocida como *Fast Ethernet*, que opera a 100Mbps.
- 1000 Mbps Ethernet también conocida como *Gigabit Ethernet* que opera a 1Gbps.

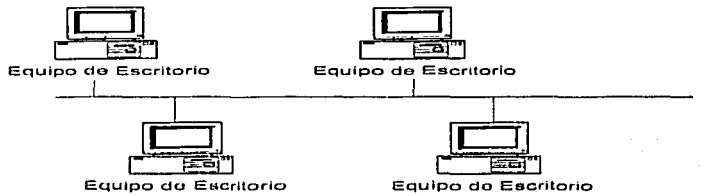


Fig. 1.1. Red LAN (Local Area Network)

1.2.1. Características.

Ethernet ha subsistido como medio esencial de casi cualquier red debido a su gran flexibilidad y facilidad de implementación y entendimiento.

Ethernet fue desarrollado a principios de los setentas para operar a una velocidad de 10Mbps sobre cable coaxial. En 1980 fue desarrollado el estándar por el Instituto de Ingenieros Eléctricos y Electrónicos (*IEEE*) denominado IEEE 802.3 basado en la idea original de Ethernet pero con una mayor variedad de aplicaciones.

Su operación está basada en un ambiente de broadcast en donde cada terminal ve toda la información que es puesta en la red y examina cada trama para determinar su destino. Cuando la terminal identifica su información que fue enviada para ella, la recibe y la reenvía a un protocolo de capa superior. El método de accesar al medio de transmisión es conocido como CSMA/CD (*Carrier Sense Multiple Access / Collision Detection*) en donde cada terminal puede enviar información en cualquier momento verificando si no existe tráfico en la línea; si esta ocupada espera hasta que encuentra el medio libre y vuelve a intentar la transmisión. En caso de que dos terminales envíen información simultáneamente ocurre una colisión, obligando a éstas a retransmitir posteriormente.

Ethernet opera en las capas 1 y 2 del modelo de referencia OSI definiendo un solo medio físico de transmisión, mientras que el estándar IEEE 802.3 define varios medios físicos los cuales permiten mayor flexibilidad y alcance.

La tabla 1.1. muestra las especificaciones de la capa física entre Ethernet y IEEE 802.3.

	Ethernet	**IEEE 802.3**				
Características	Valor	10base5	10base2	10baseT	10baseFL	100baseT
Tasa de transmisión	10 Mbps	10 Mbps	10 Mbps	10 Mbps	10 Mbps	100 Mbps
Longitud máxima del segmento	500 m	500 m	185 m	100 m	2 km	100 m
Medio	Coaxial grueso	Coaxial grueso	Coaxial delgado	UTP	Fibra Óptica	UTP
Topología	Bus	Bus	Bus	Estrella	Punto a Punto	Bus

Tabla1.1. Especificaciones de la capa física entre Ethernet y IEEE 802.3

1.3. FAST ETHERNET (IEEE 802.3u)

Fast Ethernet es un estándar (IEEE 802.3u) para LANs de alta velocidad con las mismas características que Ethernet, pero ofreciendo un incremento en el ancho de banda al usuario final con un mínimo de cambios en su estructura.

100BaseT es la especificación de la IEEE para la implementación de Ethernet a 100Mbps para un medio de tipo cable UTP (*Unshielded Twister-Pair*) ó bien STP (*Shielded Twister-Pair*). El control de acceso al medio (MAC) es igual al estándar IEEE 802.3 Ethernet al igual que el formato y tamaño de la trama y el mecanismo de detección de errores, soporta todas las aplicaciones y software utilizados en IEEE 802.3 y puede operar con ambas tasas de transmisión, 10 y 100Mbps.

100BaseT utiliza principalmente 3 medios físicos en la capa 1 del modelo OSI que son:

- 100BaseTX
- 100BaseFX
- 100BaseT4
- 100BaseT2

Estos medios físicos interactúan con IEEE 802.3 Ethernet MAC de la misma forma que 10baseT.

PROTOCOLOS DE CAPA SUPERIOR		
802.3 MAC		
100BaseTX	100BaseFX	100BaseT4

Tabla 1.2 Medios Físicos de 100BaseT

100BaseTX está basado en la especificación ANSI TP-PMD (*American National Standards Institutes Twisted Pairs-Physical Medium Dependent*). 100Base FX esta basado en la especificación ANSI TP-PMD X3T9.5 y 100BaseT4 esta basado en la especificación IEEE 802.3u.

Existe una tecnología adicional denominada 100VG-AnyLAN. Desarrollado, entre otros fabricantes, por Hewlett Packard y después modificado por el comité IEEE 802.12, fue diseñado como una alternativa para aplicaciones tales como multimedia, utilizando los siguientes medios físicos:

- UTP categorías 3, 4 ó 5.
- STP
- Fibra Óptica

100VG-AnyLAN utiliza un método de manejo de prioridades en la demanda del usuario que elimina colisiones y puede enviar una mayor carga de información que en 100BaseT.

1.4. GIGABIT ETHERNET (1GB ETHERNET).

La aparición de aplicaciones de tipo intranet pronostican una migración a nuevos tipos de datos, incluso video y voz. Antes se pensaba que el video podría requerir una tecnología de gestión de redes diferente, diseñada específicamente para datos de tipo multimedia. Pero hoy es posible mezclar datos y video sobre Ethernet a través de una combinación de:

- Aumentos del ancho de banda proporcionados por Fast Ethernet y 1Gb Ethernet, reforzados por LAN's conmutadas.
- La aparición de nuevos protocolos, como RSVP, que proporciona reserva del ancho de banda
- La aparición de nuevas normas como 802.1Q y/o 802.1p qué proporcionará VLAN's y la información de prioridad explícita para los paquetes en la red.
- El uso extendido de compresión de video avanzado.

Estas tecnologías y protocolos se combinan para hacer a 1Gb Ethernet una solución sumamente atractiva para la entrega de video y tráfico multimedia.

1Gb Ethernet es una extensión a las normas de 10-Mbps y 100-Mbps IEEE 802.3. Ofreciendo un ancho de banda de 1000 Mbps, 1Gb Ethernet mantiene compatibilidad completa con la base instalada de nodos Ethernet.

Soporta nuevos modos de operación *Full-Duplex* para conexiones conmutador-conmutador y conexiones conmutador-estación, y modos de operación *Half-Duplex* para conexiones compartidas que usan repetidores y los métodos de acceso CSMA/CD. Inicialmente operando sobre fibra óptica, 1Gb Ethernet también puede usar cableados de par trenzado (UTP).

Las implementaciones iniciales de 1Gb Ethernet emplean cableados de fibra óptica monomodo o multimodo, los componentes ópticos para la señalización sobre la fibra óptica serán de 780 nm.

1Gb Ethernet opera también sobre par trenzado tanto cableado de tipo UTP así como de tipo STP. Para acomodar ésto, se especifica una interfaz lógica entre las capas de enlace y física.

La tendencia indica que para finales de este año ya se tenga la especificación completa de Ethernet a velocidades de 10 Gbps (10Gb Ethernet), funcionando en principio sobre los mismos medios físicos que 1Gb Ethernet.

Los objetivos más importantes para desarrollar una norma 1Gb Ethernet fueron que:

- Permita Half y Full Duplex a velocidades de 1000 Mbps.
- Use el formato de trama del 802.3/Ethernet.
- Usar el método de acceso CSMA/CD.
- Mantener total compatibilidad con las tecnologías 10BaseT, 100BaseT, 10BaseFx, etc.

Interfaz Física.

La especificación de 1Gb Ethernet describe varios medios de transmisión:

Onda larga (LW) láser en modo simple y fibra multimodo (conocido como 1000 Base LX) y onda corta (SW) láser en fibra multimodo (1000 Base SX). El comité IEEE está estudiando el uso de UTP para la transmisión de Gigabit Ethernet (1000 BaseT).

Nivel de enlace lógico.

1Gb Ethernet ha sido diseñado para adherirse al formato de trama estándar de Ethernet, manteniendo compatibilidad con los productos base instalados de Ethernet y Fast Ethernet, no requiriendo traducción de tramas.

El nivel LLC define servicios de acceso para protocolos que se adhieren al Modelo de Referencia OSI.

Escalando cableados.

1Gb Ethernet se usa para aumentar el tráfico desde múltiples conmutadores pudiendo ser de baja velocidad al enrutador. Los conmutadores de baja velocidad pueden ser conectados tanto vía Fast Ethernet como por 1Gb Ethernet mientras que los conmutadores proveen conmutaciones dedicadas de 10Mbps o grupos de conmutación para usuarios individuales. Por ejemplo los servidores de archivos son conectados vía 1Gb Ethernet para mejorar su desempeño.

1.5. MODO DE TRANSMISIÓN ASÍNCRONA. (ATM)

El modo de transferencia asíncrono fue creado con la finalidad de transportar datos con un gran ancho de banda. El Modo de Transferencia Asíncrona (*ATM*) es una tecnología de red basada en la idea de mantener fija la longitud de la trama que se envía.

ATM es una tecnología para transmitir información que se basa en el principio de conmutación de paquetes. ATM transfiere información en paquetes de tamaño fijo llamados celdas. Cada celda consiste de 53 octetos o bytes. Los primeros 5 bytes contienen la información del encabezado y los 48 restantes contienen la información del usuario.

En ATM el término "asíncrono" no está referido a la forma de transmisión física, la cual de hecho es síncrona. Asíncrono se refiere a la forma en la cuál el ancho de banda es distribuido entre las conexiones de los usuarios. El término "Modo de Transmisión", nos indica que ésta es una técnica de multiplexión y conmutación.

El ancho de banda es dividido en ranuras de tiempo con longitud fija, las cuales son utilizados por la información del usuario sólo cuando este lo requiera, por lo cual éstos no tienen una posición temporal predeterminada; para identificar la conexión, las ranuras de tiempo cuentan con una etiqueta como prefijo, en la cual se tiene la información necesaria para identificar el destino de cada ranura.

El hecho de que ATM sea una tecnología de enlace implica que es, entonces, una tecnología de conmutación y transmisión de paquetes a muy alta velocidad que permite el envío de diversos tipos de información de acuerdo a prioridades, previendo entonces servicios de transferencia de voz, video y datos sobre la misma red, a velocidades que varían de 25 Mbps hasta 1 Gbps o más. Aunque los defensores de ATM indiquen que se podrían reducir de manera significativa, esto en general no es así, ya que una interfaz ATM a la misma velocidad que una Ethernet, es significativamente más cara.

De manera histórica, los servicios de voz y datos siempre han sido manejados de forma totalmente aislada a la red de datos. Esto debido a que la voz no puede esperar mucho para ser procesada ni tampoco permitir retrasos por repetición o pérdida de información, es decir, es un servicio que se debe manejar en tiempo real; mientras que los datos en general, permiten éste tipo de demoras. De ésta manera, ATM debe distinguir entre servicios que requerirán una tasa de bits constante (*CBR, Constant Bit Rate*) como la voz, o bien una tasa de bits variable (*VBR, Variable Bit Rate*).

En los sistemas de conmutación de paquetes, una aplicación puede utilizar todo el ancho de banda cuando se requiera y no solamente una fracción del mismo, como el caso de la tecnología TDM o multiplexión por división de tiempo. Sin embargo, en las tecnologías de conmutación de paquetes tradicionales existe una limitación, si la red es X.25 ó *Frame Relay*, ésta permite que algunos usuarios transmitan grandes volúmenes de información conformados en tramas de gran extensión sobre la red, mientras otros serán forzados a esperar para transmitir aún por periodos muy cortos, lo que trae como resultado retrasos variables que son inaceptables en aplicaciones como voz y video.

ATM ofrece a los usuarios las ventajas de ambas tecnologías: TDM que asigna ancho de banda permanentemente a una aplicación; y la de conmutación de paquetes, en la que una aplicación puede utilizar todo el ancho de banda cuando se requiera, lo cual sucede ante la presencia de *ráfagas de información*, comportamiento típico del correo electrónico, por ejemplo, en la que únicamente durante un pequeño lapso de tiempo se están transmitiendo datos, fuera de lo cual

el canal, en cuanto a esa aplicación concierne, se encuentra desocupado o en estado de espera. A esto se le llama conmutación de celdas.

Además ATM, como en telefonía, es un sistema de telecomunicaciones orientado a conexión. Esto es, que la conexión entre las dos estaciones emisora y receptora se establece antes de que los datos comiencen a fluir entre ellas. Una conexión ATM especifica el camino de transmisión, permitiendo a las celdas encaminarse por sí mismas en una red ATM. Además de ésto, también permite especificar una garantía de QoS para cada conexión, dependiendo que esté viajando sobre ésta.

Debido a que ATM trabaja orientado a conexión, el ancho de banda para alguna conexión es únicamente colocado cuando el usuario hace uso de ésta, permitiendo soportar eficientemente una red bajo demanda, colocando el ancho de banda bajo demanda dependiendo de las necesidades del usuario, concepto que le da el nombre de *asíncrono.*

Otra ventaja de ATMS, es que tiende a ser aceptada como el modo de transferencia predilecto por redes digitales de servicios integrados de banda ancha (*B-ISDN*), debido a que las especificaciones de estas últimas, reunidas en las recomendaciones I.400 de la UIT–T, no detallan la forma en la que BISDN debe llevarse a cabo, entonces ATM es la realización física de tal concepto.

Podemos definir el concepto de ATM con los siguientes principios:

- Toda la información es llevada en forma de unidades de datos de longitud fija llamadas celdas, las cuales consisten en un encabezado y un campo de información.
- ATM es orientado a conexión, y las celdas en la misma conexión virtual mantienen su orden secuencial.
- Las fuentes de tráfico pueden generar celdas tanto como sea necesario sin que tengan una posición temporal predeterminada, por lo cual las celdas contienen un campo en el encabezado para identificar la conexión.
- La función principal del encabezado es la identificación de las celdas pertenecientes a una conexión virtual.
- Las etiquetas de identificación sólo tienen significado local (éstas no son direcciones explícitas) y son cambiadas en cada conmutador.
- El campo de información es llevado transparentemente, por lo tanto no se lleva a cabo un control de errores en éste.

Con ésto se puede determinar que ATM especifica el método de intercambio de información a través de una interfaz red-usuario, y un modo de multiplexión y conmutación dentro de la red. Algunas de las finalidades de las redes ATM pueden resumirse en:

- Soportar e integrar todas las aplicaciones de redes existentes, y aún las desconocidas que pudieran emerger en el futuro.
- Minimizar la complejidad de conmutación.
- Minimizar el procesamiento de la carga en los nodos intermedios para soportar altas velocidades de transmisión.
- Proveer las bases para garantizar la aplicación de los requerimientos de calidad de servicio en la red.
- Permitir la integración de todos los tipos de tráfico dentro de una sola arquitectura de red: voz, video, datos, etc.

1.6. REDES DE ÁREA LOCAL VIRTUALES (VLANs).

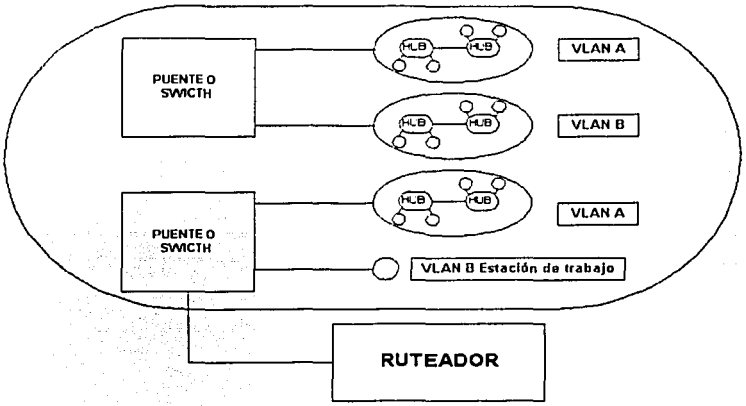
Una LAN fue originalmente definida como una red de computadoras localizadas dentro de la misma área. Éstas son definidas para enviar información entre las mismas computadoras, por lo que si un usuario envía información dentro de su LAN, ésta estará disponible por todos los usuarios de la red, definiendo así un dominio de *broadcast*.

Para que ésta información pueda salir hacia otras LANs, es necesario el uso de un enrutador, la desventaja de éste método es que los enrutadores toman mas tiempo para procesar los datos de entrada y enviarlos hacia los dispositivos como puentes ó conmutadores que entregarán la información a su destino final.

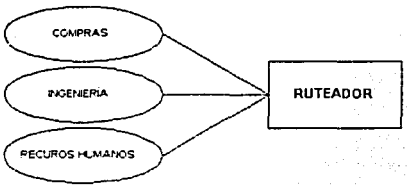
Las redes de área local virtuales, denominadas VLANs, fueron desarrolladas como una alternativa de solución para usarse como enrutadores, que contengan la información de todos los usuarios en las diferentes redes LAN y evitar tiempos adicionales de procesamiento.

En una red LAN tradicional todos los dispositivos (estaciones de trabajo, estaciones de escritorio, impresoras, etc.) están conectados uno con otro por medio de concentradores ó repetidores, dispositivos que propagarán la información a través de la red. El uso de dispositivos como puentes ó conmutadores permite enviar la información a cada uno de los usuarios (servicios de broadcast) ó a un grupo especifico de usuarios (servicios de multicast).

Las VLANs permiten al administrador de la red segmentar lógicamente una LAN en diferentes dominios de broadcast, es decir, en diferentes LANs. Dado que ésta segmentación es lógica mas no física, los dispositivos componentes de la red no tiene que estar físicamente juntos. Por ejemplo, los usuarios en diferentes pisos de un edificio o inclusive en diferentes edificios pueden ahora pertenecer a la misma LAN. Los enrutadores ahora sólo serán utilizados para comunicar dos o más VLAN´s.



Vista Física



Vista Lógica

Fig.1.2. Vista física y lógica de una VLAN.

Las ventajas de las VLANs sobre las LAN tradicionales se enlistan a continuación.

1. Eficiencia:
   En redes donde el tráfico consiste en un alto porcentaje de broadcast y multicast, las VLANs pueden reducir la necesidad de enviar tal tráfico a destinos innecesarios.

2. Formación de Grupos de Trabajo Virtuales:
   Comúnmente es necesario separar los grupos de trabajo dentro de una empresa por departamentos o tipo de actividades; por ejemplo, el área de ventas, ingeniería, mercadotecnia, etc. Por lo que no importa la ubicación física de los componentes del grupo, estos compartirán los servicios de la LAN.

3. Administración Simplificada.
   En la mayoría de las redes convencionales los costos por administración son muy elevados y toman demasiado tiempo llevarlos a cabo. Agregar, mover ó cambiar usuarios implica hacer nuevos cableados, direccionar nuevas estaciones de trabajo y reconfigurar concentradores y enrutadores. Todas éstas tareas pueden ser simplificadas con el uso de VLANs, de ésta manera si un usuario es movido de lugar físico, la reconfiguración de enrutadores es innecesaria.

4. Reducción de costos.
   Las VLANs pueden ser usadas para crear dominios de *broadcast*, lo cual evita la necesidad de adquirir enrutadores lo que implica reducir gastos.

5. Seguridad.
   Las VLANs pueden ser usadas para controlar la información en los dominios de *broadcast*, instalar firewalls, restringir accesos e informar al administrador de la red sobre intrusos que hayan accesado.

1.6.1. Como trabajan las VLAN´s.

Cuando un puente de una LAN recibe datos de una estación de trabajo, éste los marca con un identificador indicando la VLAN de la cual provienen. Éste proceso es llamado marcación explícita. También es posible determinar a cual VLAN pertenecen estos datos usando marcación implícita. En la marcación implícita los datos no son marcados pero es posible determinar de cual VLAN provienen, mediante información como el puerto al cual llegan éstos. La marcación puede ser basada en el puerto del cual provienen los datos, el campo de la dirección MAC (*Media Access Control*), la dirección de la red, otros campos o la combinación de estos.

Las VLANs son clasificadas por el método de marcación utilizado, es decir por el tipo de marca. Para poder realizar la marcación por los diferentes métodos, el puente tendrá que conservar una base de datos actualizada que contenga un mapeo de las VLANs y cualesquiera que sea el campo usado para su marcación. Por ejemplo, si la marcación es por puerto, la base de datos deberá indicar cuales puertos pertenecen a cada VLAN. Los puentes deberán ser capaces de mantener ésta base de datos y también asegurarse de que todos lo puentes en la LAN contengan ésta misma información.

Los puentes determinan el destino de la información basándose en la operación normal de la LAN. Una vez que el puente determina donde deberán ir los datos, éste ahora necesita determinar si el identificador de la VLAN debe ser agregado a los datos y ser enviados a su destino. El identificador es agregado si los datos van a ser enviados a un dispositivo que conoce la implementación de la VLAN, de lo contrario, el puente envía esta información sin el identificador de la VLAN.

1.6.2. Tipos de VLANs.

Los miembros de una VLAN pueden ser clasificados por el puerto, la dirección MAC y el tipo de protocolo.

1. VLAN Capa 1: Miembro por puerto.

La membresía en una VLAN puede estar definida en base a los puertos que pertenezcan a la VLAN; por ejemplo, como se puede observar en la tabla 1.3 en un puente con 4 puertos, los puertos 1,2, y 4 pertenecen a la VLAN 1 y el puerto 3 pertenece a la VLAN 2.

PUERTO	VLAN
1	1
2	1
3	2
4	1

Tabla 1.3. VLAN por puerto.

La principal desventaja de este método es que este no permite la movilidad del usuario, es decir, si un usuario se mueve lejos del puente asignado, el administrador de la red tendrá que reconfigurar la VLAN.

2. VLAN Capa 2: Miembro por dirección MAC.

La membresía en una VLAN está basada en la dirección MAC de la estación de trabajo del usuario. El conmutador rastrea la dirección MAC y determina la VLAN a la que pertenece. Debido a que la dirección MAC forma parte de la interfaz de red de la estación de trabajo, cuando ésta es movida, no es necesario reconfigurar a VLAN para que el usuario permanezca en ella. Observar la tabla 1.4.

MAC	VLAN
1212354145121	1
8729387125623	1
9802761492763	2
1673826374917	1

Tabla 1.4. VLAN por MAC Address.

La desventaja de este método es que la membresía en la VLAN debe ser asignada inicialmente, lo cual dificulta su elaboración para redes con cientos de usuarios.

3. VLAN Capa 2: Miembro por tipo de protocolo.

La membresía en una VLAN para capa 2 también puede estar basada en el tipo de protocolo encontrado en el encabezado de la capa 2, como se muestra en la tabla 1.5.

PROTOCOLO	VLAN
IP	1
IPX	2

Tabla 1.5. VLAN por protocolo.

4. VLAN Capa 3: Miembro por mascara de subred IP.

Ésta membresía está basada en el encabezado de la capa 3. La dirección de la máscara de subred de la red IP puede ser utilizada para clasificar la VLAN. Como ejemplo se muestra la tabla 1.6.

SUBRED IP	VLAN
23.2.24	1
26.21.35	2

Tabla 1.6. VLAN por Subred.

Aunque la membresía está basada en información de capa 3, ésta no tiene nada que ver con el enrutamiento de la red y no debe ser confundida con éste tipo de funciones. En éste método, las direcciones IP son usadas únicamente como un mapeo para determinar a los miembros de una VLAN. No se hace ningún otro proceso con las direcciones IP.

En capa 3 los usuarios pueden mover sus estaciones de trabajo sin reconfigurar las direcciones de la red, el único problema es que generalmente toma más tiempo enviar los paquetes utilizando información de capa 3 en lugar de direcciones MAC.

5. VLAN Capas superiores:

También es posible definir la membresía en una VLAN basándose en aplicaciones y servicios ó la combinación de ambos, por ejemplo las aplicaciones de transferencia de archivos (*FTP*) que pueden ser ejecutadas en una VLAN y las aplicaciones de Telnet en otras.

Como se puede observar existen ventajas significativas con la implementación de VLANs en la tecnología de redes, las cuales permiten la formación de grupos virtuales de trabajo, mejor seguridad y funcionamiento, administración simplificada y reducción de costos. Las VLANs son formadas mediante una segmentación lógica de la red y pueden ser clasificadas en base a las capas 1, 2, 3 y capas superiores del modelo OSI. Lo correspondiente con las capas 1 y 2 es especificado en el estándar 802.1Q. La marcación y las bases de datos permiten a los dispositivos determinar la VLAN fuente y destino de los datos recibidos. Si las VLANs son implementadas efectivamente serán una promesa considerable en el futuro de las soluciones para las redes de datos.

1.7. Protocolo de Troncales Virtuales (VTP).

Como ya mencionamos, la IEEE define una VLAN como una red de área local virtual que define dominios de *broadcast*. VTP es un protocolo desarrollado por Cisco que permite disminuir esfuerzos en la administración de la red en el establecimiento, mantenimiento, cancelación y renombramiento de VLANs.

Para que VTP pueda manejar las VLANs a través de la red, se debe crear un servidor de VTP. Todos los servidores que requieran compartir información de VLANs deberán utilizar el mismo nombre del dominio y el conmutador deberá estar únicamente en un dominio al mismo tiempo.

Un dominio de VTP puede ser usado si existe mas de un conmutador conectado en la red. Si todos los conmutadores están solamente en una VLAN, no es necesario utilizar VTP.

Modos de operación en VTP.

- Servidor: Es necesario establecer al menos un servidor en el dominio de VTP. EL conmutador debe estar en modo de servidor para agregar, cambiar ó borrar VLANs en el dominio de VTP. Todos los cambios hechos son informados a todo el dominio.

- Cliente: Recibe información de los servidores de VTP, recibe y envía actualizaciones, pero no realiza ningún cambio.

- Transparente: No participa en el dominio de VTP pero seguirá enviando los avisos a través de los enlaces troncales configurados. Los conmutadores en modo transparente pueden agregar y borrar VLANs, mientras que el conmutador conserve su propia base de datos, pero este no comparte su información con otros conmutadores.

Para utilizar VTP, cada conmutador deberá tener un nombre de dominio de VTP. La información permanecerá únicamente en el mismo dominio de la VLAN. Las condiciones para los dominios de VTP son las siguientes:

- A cada conmutador en un dominio se le debe asignar el mismo nombre del dominio.
- Los conmutadores deben ser adyacentes.
- Deben ser establecidas troncales entre conmutadores.

II. MODELO DE REFERENCIA TCP/IP

2.1. TCP/IP.

Un gran número de aplicaciones de red están basadas en lo que se conoce como *TCP/IP (Transmission Control Protocol/Internet Protocol)*. TCP/IP no es un protocolo único, sino un conjunto de éstos que cubren los distintos niveles del modelo OSI. Los dos protocolos más importantes son el TCP (*Transmission Control Protocol*) y el IP (*Internet Protocol*), que son los que dan nombre al conjunto.

TCP/IP fue originalmente desarrollado por el Departamento de Defensa (*DoD*) de los Estados Unidos en los inicios de los años 70s, en un proyecto denominado *ARPANET (Advanced Research Project Agency's Network*).

Arpanet inicialmente se diseñó para que fuera una red experimental de tipo WAN para la comunicación de paquetes, dando como resultado el conjunto de protocolos *TCP/IP*, que posteriormente fueron expandidos y refinados.

En los años 80's, *TCP/IP* fue incluido como parte integral de la versión 4.2 de UNIX de la Universidad de Berkeley. En 1983 *TCP/IP* se convirtió en el conjunto de protocolos militares estándar para el diseño de redes.

En los últimos años *TCP/IP* ha adquirido una enorme popularidad debido a lo siguiente:

- Independencia sobre la gran variedad de fabricantes.
- Independencia del tipo de tecnología utilizada en capa 2.
- Soporta todo tipo de plataformas y arquitecturas de computadoras (PC's Worstations, mainframes, etc.)
- Soporta tecnologías de enrutamiento dinámico.

2.1.1. Modelo TCP/IP.

La arquitectura de éste conjunto de protocolos está dividida en cuatro o cinco capas, según diversos autores consultados, cada una de ellas es relacionada con las capas correspondientes al modelo de referencia OSI de la tabla 2.1.

OSI		TCP/IP
Aplicación		Aplicación
Presentación		
Sesión		Transporte
Transporte		
Red		Internet
Enlace		Interfaz de Red
Físico		Físico

Tabla 2.1.Relación Modelo OSI con Modelo TCP/IP.

Cada una de las capas de la modelo *TCP/IP* son brevemente descritas a continuación:

Capa Física. Especifica los requerimientos eléctricos, mecánicos, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre los sistemas terminales; especifica niveles de voltajes, tasas de transmisión, conectores y distancias máximas de transmisión.

Capa de Interfaz de Red. Es equivalente a una parte de la capa física y a la capa de enlace de datos del modelo OSI, éste determina el cómo un *host* accesa a la red.

Para el caso de la resolución de direcciones, se realiza cuando se transforma una dirección lógica en una dirección física ó viceversa. El protocolo que se encarga de esta tarea es el Protocolo de Resolución de Direcciones (ARP, *Address Resolution Protocol*) y sus diferentes versiones.

Capa de Internet. La capa de Internet provee el servicio básico de entrega de paquetes a su destino final a través de múltiples redes. También se encarga de la resolución de direcciones lógicas, y de la formación y mantenimiento de las tablas de enrutamiento.

Para la parte de enrutamiento, existe un dispositivo llamado *enrutador* el que se encarga de transmitir los paquetes en forma independiente a través de la red y determinar el mejor camino para alcanzar su destino.

También se determinan funciones de control para la transmisión de los datos como son el TTL (*Time to Live*), ToS (*Type of Service*), multicanalización y la fragmentación, al igual que el empleo de ICMP (*Internet Control Message Protocol*) para proveer mensajes de error. Toda ésta información viene almacenada en el encabezado del protocolo IP.

Capa de Transporte. Provee servicios de comunicación confiables necesarios para la capa de aplicación. Para lograr esto se compone de dos protocolos que ofrecen diferentes tipos de servicios:

- UDP (*User Datagram Protocol*)
- TCP (*Transfer Control Protocol*)

UDP maneja servicios ó aplicaciones que no requieren que el flujo de datos sea confiable y es un servicio orientado a no conexión. Crea mecanismos para distinguir entre múltiples destinos dentro de un mismo sistema terminal, es decir, que en un sistema terminal o estación de trabajo, se identifica a estos múltiples destinos mediante puertos, esto significa que para cada diferente aplicación a este nivel se le asigna una dirección IP y un puerto diferente. Bajo éste principio, UDP demulticanaliza los datos de una aplicación basado en el puerto destino.

Los diferentes servicios que provee son:

- Servicio de asignación de Nombres de Dominio (DNS, *Domain Name Server*)
- Transferencia de Archivos Triviales (TFTP, *Trivial File Transfer Protocol*)
- Sistemas de Archivos en Red (NFS, *Network File System*)
- Sistemas de Administración de Red (SNMP, *Simple Network Management Protocol*)

Por otro lado, TCP provee servicio a aplicaciones que requieran un flujo de datos confiable y es orientado a conexión. TCP garantiza la entrega de los paquetes, mientras que UDP no; TCP garantiza su confiabilidad utilizando la verificación de mensajes recibidos (*Acknowledgments*) por medio de una técnica llamada ventaneo (*Windowing*).

TCP provee servicios para:

- Transferencia de Archivos (FTP, *File Transfer Protocol*).
- Sesiones Remotas (*Telnet*).
- Manejo de Correo electrónico (SMTP, *Simple Mail Transfer Protocol*).

Capa de Aplicación. La capa de Aplicación es equivalente a las capas de Presentación y Aplicación del modelo de referencia OSI. Las aplicaciones más comunes son:

- Telnet. Es un protocolo que permite el acceso a una terminal remota.
- FTP. Permite el envío de archivos de una estación a otra.
- SMTP. Permite el intercambio de correo electrónico hacia diferentes terminales.
- DNS. Es utilizado para asignar y consultar los nombres de las direcciones IP.

En la tabla 2.2. se muestran los protocolos que se aplican entre las capas de *TCP/IP*.

TCP/IP	PROTOCOLOS
Aplicación	Telnet, DNS, SMTP, SNMP, WWW, TFTP, etc.
Transporte	TCP y UDP
Internet	IP, ICMP, IGMP
Interfaz de Red	Ethernet, Token Ring, FDDI, WAN, ARP
Físico	TOKEN PASSING, CSMA/CD, SLIP, PPP

Tabla 2.2. Protocolos involucrados en el modelo TCP/IP

Para el presente trabajo sólo se mencionarán las funciones principales de 4 de éstos protocolos, que son considerados de gran utilidad para el desarrollo y mejor comprensión de la temática tratada en el mismo, dichos protocolos son: IP, ICMP, TCP y UDP.

2.1.2. Protocolos de la capa Internet: IP e ICMP.

2.1.2.1. Protocolo IP.

El principal protocolo que opera en la Capa de Internet es el protocolo IP. Es el encargado de identificar cada uno de los paquetes y nos puede ayudar a definir la ruta que los éstos deben seguir ya que nos indica las direcciones fuente y destino.

IP proporciona un servicio de distribución de paquetes caracterizado por:

- Transmisión de datos en datagramas (paquetes con encabezado IP).
- No está orientado a conexión, por lo que los paquetes que circulan entre los host son tratados de forma independiente, lo que origina que cada uno pueda seguir una trayectoria diferente en su viaje hasta el host destino.
- No es confiable, ya que no implementa mecanismos de verificación de entrega de paquetes, por lo que no garantiza la entrega de los mismos, tampoco la entrega en secuencia, ni la entrega única. Esto queda en manos del protocolo TCP de la capa superior.
- No implementa corrección de errores ni control de congestión.
- Puede fragmentar los paquetes, si es necesario.
- Direcciona los paquetes mediante direcciones lógicas IP de 32 bits (IPv4) y de 128 bits (IPv6).
- Sólo verifica la integridad de la cabecera del paquete en sí, no los datos que contiene.

Sus misiones más importantes son el direccionamiento de los paquetes así como la administración del proceso de fragmentación y defragmentación de los mismos. Para el direccionamiento de los paquetes, el protocolo IP examina la topología de la red para determinar la mejor ruta de envío.

Pareciera que IP es un protocolo poco confiable, pero éste es fundamental para poder intercomunicar diferentes redes, hasta el punto de formar el pilar sobre el que se ha construido Internet. Para dar confiabilidad al sistema se usan tanto los protocolos de las capas superiores como los de la Capa de Enlace de Datos, encargándose IP tan sólo de dar los datos necesarios para el enrutamiento entre los hosts que se comunican.

El papel de la capa de Internet es averiguar cómo encaminar paquetes o datagramas a su destino final, lo que consigue mediante el protocolo IP. Para hacerlo posible, cada interfaz en la red necesita una dirección IP, que identifica tanto al host como a la red a la que éste pertenece, ya que el sistema de direcciones IP es un sistema jerárquico. Se trata de una dirección única en el ámbito mundial y la concede el Centro de Información de la Red Internet (InterNIC).

2.1.2.2. Protocolo ICMP.

Otro protocolo que también funciona en la capa de Internet dentro del modelo TCP/IP, es el Protocolo de Mensajes de Control de Errores de Internet (ICMP). La utilidad de este protocolo no está en el transporte de datos de usuario, sino en controlar si un paquete no puede alcanzar su destino, si su vida ha expirado, si el encabezado lleva un valor no permitido, si es un paquete de eco ó respuesta, etc.; es decir, se usa para manejar mensajes de error y de control necesarios para los sistemas de red, informando con ellos a la fuente original para que evite o corrija el problema detectado. ICMP proporciona así una comunicación entre el software IP de una máquina y el mismo software en otra.

El protocolo ICMP solamente informa de incidencias en la entrega de paquetes ó de errores en la red en general, pero no toma decisión alguna al respecto, ésto es tarea de las capas superiores.

2.1.3. Protocolos de Capa de transporte: TCP y UDP.

2.1.3.1. Protocolo TCP.

Las funciones principales de la capa de transporte son transportar y regular el flujo de información, garantizando la conectividad de extremo a extremo entre aplicaciones de los hosts que se están comunicando en la red, de manera confiable, eficiente y precisa. Para esto, se utilizan los servicios de la Capa de Red.

Los protocolos de transporte tienen la función de actuar de interfaz entre los niveles orientados a la aplicación y los niveles orientados a la red dentro de la jerarquía de protocolos TCP/IP.

En la Capa de Transporte aparece un protocolo muy importante para una correcta transmisión de datos entre redes, el Protocolo de Control de Transmisión (TCP). Éste ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un bajo nivel de errores.

TCP mantiene un diálogo entre el origen y el destino mientras fragmenta y empaqueta la información de la capa de aplicación en unidades de tamaño adecuado, denominadas segmentos, debiendo ocuparse de los datos independientemente del hardware y del software que componga la red con la que se esté trabajando.

Sus principales características son:

- Es un protocolo orientado conexión, lo que significa que se establece una conexión entre el emisor y el receptor antes de que se transfieran los datos entre ambos.

- Es un protocolo fiable, ya que implementa mecanismos para conseguir que la información enviada por el emisor llegue de forma correcta al receptor. Para ello, cada paquete se trata de forma independiente, asignándole el emisor un número identificador único, lo que permite un posterior control de los paquetes enviados y recibidos.

- Es un protocolo de flujo no estructurado, con posibilidad de enviar información de control junto a datos.

- Es un protocolo con transferencia de memoria intermedia, sistema mediante el cual, y con objeto de hacer eficiente la transferencia y minimizar el tráfico de red, se van almacenando datos suficientes del flujo de transmisión hasta completar un paquete lo suficientemente largo como para ser enviado. En el lado receptor ocurre un proceso similar, almacenándose los datos en una memoria intermedia denominada *buffer*.

- Usa conexiones *full-duplex*, en las que se permite la transferencia de datos concurrente en ambas direcciones, sin ninguna interacción aparente desde el punto de vista de las aplicaciones emisora y destinataria.

- Usa conexiones punto a punto, en las que cada conexión tiene exactamente dos puntos terminales.

2.1.3.2. Protocolo UDP.

El protocolo TCP tiene la robustez, la confiabilidad y las funcionalidades propias de un protocolo de transporte orientado a conexión, pero a veces resulta demasiado complejo. Por ejemplo, cualquier transmisión de información TCP requiere como mínimo el intercambio de seis mensajes para establecer la comunicación y terminarla; además mientras una conexión existe ocupa una serie de recursos en el host.

Para casos en los que no es necesario tanto control de los datos enviados, la Capa de Transporte implementa también el Protocolo de Datagrama de Usuario (UDP). Este es un protocolo no confiable y no orientado a conexión para la entrega de mensajes. En este caso los paquetes enviados mediante el protocolo IP reciben el nombre específico de *datagramas*, no se realiza una conexión definida entre los hosts, ni un control de los paquetes enviados y recibidos. Los datagramas se enrutan independientemente, por lo que deben llevar la dirección completa de destino, como en TCP.

Es simple, eficiente e ideal para aplicaciones como TFTP y DNS. Una dirección IP sirve para dirigir el datagrama hacia una máquina en particular; el número de puerto de destino en la cabecera UDP se utiliza para dirigir el datagrama a un proceso específico en dicha máquina. La cabecera UDP también contiene un número de puerto origen que permite al proceso recibido responder al datagrama.

UDP no admite numeración de los datagramas, factor que, sumado a que tampoco utiliza señales de confirmación de entrega, hace que la garantía de que un paquete llegue a su destino sea mucho menor que si se usa TCP. Esto también origina que los datagramas pueden llegar duplicados y/o desordenados a su destino. Por estos motivos el control de envío de datagramas, si existe, debe ser implementado por las aplicaciones que usan UDP como medio de transporte, al igual que el reensamble de los mensajes entrantes.

Es por ello un protocolo del tipo máximo esfuerzo (*best-effort*), porque hace lo que puede para transmitir los datagramas hacia la aplicación, pero no puede garantizar que la aplicación los

reciba. Tampoco utiliza mecanismos de detección de errores. Cuando se detecta un error en un datagrama, en lugar de entregarlo a la aplicación destino, se descarta dentro de la red.

Cuando una aplicación envía datos a través de UDP, éstos llegan al otro extremo como una unidad. Por ejemplo, si una aplicación escribe 5 veces en el puerto UDP, la aplicación al otro extremo hará 5 lecturas del puerto UDP. Además, el tamaño de cada escritura será igual que el tamaño de las lecturas.

Entre los protocolos superiores que usan UDP se incluyen TFTP, DNS, SNMP, NTP, NFS, etc.

2.1.3.3. Protocolos de seguridad en IP: IPSec.

IPSec es un estándar que proporciona servicios de seguridad a la capa IP y a todos los protocolos superiores basados en IP (TCP, UDP, etc.)

Este protocolo se destaca por ser un conjunto de estándares de la IETF (*Internet Engineering Task Force*). Proporciona un nivel de seguridad común y homogéneo para todas las aplicaciones, además de ser independiente de la tecnología física empleada. IPSec se integra en la versión actual de IP (v4) y lo que es mejor, se incluye por defecto en IPv6.

Dentro de IPSec se distinguen los siguientes componentes:

- Dos protocolos de seguridad: Encabezado de autenticación (*IP Authentication Header,* AH – RFC 2402) y Encapsulamiento Seguro de la carga útil IP (*IP Encapsulating Security Payload,* ESP – RFC 2406), los cuales proporcionan mecanismos de seguridad para proteger el tráfico IP.

- Un protocolo de gestión de claves de Intercambio de llaves de Internet (*Internet Key Exchange,* IKE – RFC 2409) que permite a dos nodos negociar las claves y todos los parámetros necesarios para establecer una conexión AH o ESP.

El protocolo AH es el procedimiento previsto dentro de IPSec para garantizar la integridad y autenticación de los datagramas IP. Proporciona un medio al receptor de los paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no hayan sido alterados durante tránsito por la red. Sin embargo no proporciona garantía de confidencialidad, es decir, los datos transmitidos pueden ser vistos por terceros. AH es realmente un protocolo IP nuevo, y como tal la IANA le ha asignado el número decimal 51.

El protocolo ESP proporciona confidencialidad, para ello especifica el modo de cifrar los datos que se desean enviar y este cifrado se incluye en un datagrama IP. Adicionalmente, puede ofrecer los servicios de integridad y autenticación del origen de los datos incorporando un mecanismo similar al de AH. La IANA le ha asignado a este protocolo el número decimal 50.

Un concepto esencial en IPSec es el de Asociación de Seguridad (SA), el cual es un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente por los nodos que intervendrán en la comunicación. Debido a que únicamente se identifica un canal unidireccional, una conexión IPSec se compone de dos SAs, una por cada sentido de la comunicación. Ambos extremos de una asociación de seguridad deben tener conocimiento de las claves, así como del resto de la información que necesitan para enviar y recibir datagramas AH ó ESP.

Adicionalmente existe un protocolo híbrido cuyo propósito es negociar y proveer material de claves autenticado para SA de una manera protegida, dicho protocolo es IKE.

IKE define tres elementos fundamentales:

- OAKLEY. Especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente.
- SKEME. Mecanismo de intercambio de llave segura para Internet, (*Secure Key Exchange Mechanism for Internet*), describe una forma de intercambio de claves muy versátil que provee anonimato, rechazo y rápida actualización de llaves.
- ISAKMP. Protocolo de administración de llaves y asociación segura en Internet (*Internet Security Association and Key Management Protocol*). Define de forma genérica del protocolo de comunicación y la sintaxis de los mensajes que se utilizan en el IKE, es decir, provee un entorno para autenticación e intercambio de claves, pero no los define, sólo se limita a establecer las fases a seguir.

El protocolo IPSec es ya uno de los componentes básicos de la seguridad en las redes IP y es considerado como una tecnología suficientemente madura como para ser implantada en todos aquellos escenarios en que se requiera seguridad.

2.1.4. Direccionamiento IP.

Todos los destinos en una red poseen un único identificador que permite a otras máquinas enviar información. Este identificador es llamado usualmente *dirección*. En algunas tecnologías, una dirección identifica una máquina en particular, mientras que en otras, como en el protocolo IP, identifica un punto de unión a la red, es decir, una *interfaz*. Una máquina puede tener múltiples interfaces, teniendo una dirección IP por cada una de ellas. Las interfaces son por lo general conexiones físicas distintas, pero también pueden ser conexiones lógicas compartiendo una misma interfaz.

Las direcciones IP son etiquetas que identifican a cada sistema terminal y están compuestas de la siguiente forma:

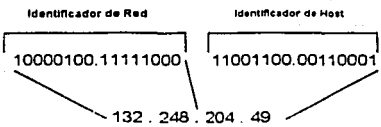


Figura 2.1. Dirección IP.

En su versión 4, la dirección IP consta de 32 bits divididos en dos partes:

Un identificador de red y un identificador de *host*. Es representada por 4 números decimales separados por puntos. Cada interfaz de red contará con una sola y única dirección IP, y los host en la misma red tendrán el mismo identificador de red. Todas las direcciones IP son asignadas por el Centro de Información de la Red (NIC, *Network Information Center*)

Existen 5 diferentes clases de direcciones IP, estas se muestran en la figura 2.2:

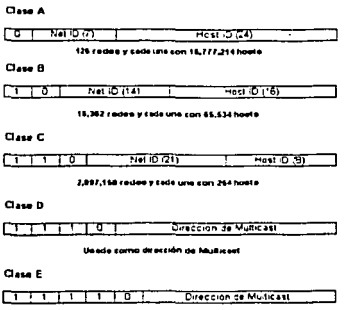


Figura 2.2. Clases de direcciones IP.

Las direcciones validas para cada clase en numeración decimal son:

- Clase A: 1.x.x.x a 126.x.x.x
- Clase B: 128.x.x.x a 191.x.x.x
- Clase D: 192.0.1.x a 191.254.x.x
- Clase D: 224.0.0.0 a 239.255.255.254
- Clase E: 224.0.0.0 a 255.255.255.254

Cada red deberá contar con un *interNIC* que registrará las direcciones IP de tal Red, y con un Centro de Monitoreo de la Operación de la Red (NOC, *Network Operation Center*). Existen direcciones IP especiales, como la dirección de *LOOPBACK*, que es la red de clase A número 127. Esta red es asignada a una función que es usada por determinado software dentro del host, es decir, que no sale de la interfaz física. Ésta dirección fue diseñada para permitir que un cliente y un servidor en el mismo host se comuniquen usando *TCP/IP*. Al igual que la dirección 255.255.255.255 que significa todos los host dentro de la red, llamada dirección de *broadcast*.

2.1.4.1. Subredes.

Los diseñadores de IP obtuvieron experiencia con la definición de clases, descubriendo que las clases originales deberían ser menos amplias, para ser más útiles a las nuevas tecnologías de LAN. Por ejemplo, era innecesario asignar una clase tipo C con posibles 65000 máquinas a una red con solo 1200 conexiones. La solución que desarrollaron fue llamada *subred* y fue el primer uso explícito de las máscaras.

La estructura de direcciones IP puede ser localmente modificada usando los bits del *hostid* como bits adicionales para el *netid*. Esencialmente, la línea de división entre el *hostid* y el *netid* es desplazada, creando redes adicionales pero reduciendo el número de máquinas que pueden

existir en cada red de clase. Es decir, la asignación de nuevos bits al *netid* para una red más grande se le denomina *subred*.

El concepto de subredes surge como una solución al crecimiento del número de usuarios y para solucionar otros problemas presentados por la naturaleza de las direcciones IP. Resumiendo en las siguientes características tenemos:

Ventajas:

- Tiene dos niveles de jerarquía: red y *host*.
- Las tablas de enrutamiento contienen rutas a cada red y no a cada *host*.
- Las direcciones de *host* son asignadas por el administrador local.

Desventajas:

- Crecimiento excesivo de las tablas de enrutamiento en redes muy grandes, sin embargo para la cantidad de nodos de la red UNAM no es tan grave.
- Debe obtenerse un número de red cada vez que una nueva red sea instalada.

De esta manera es posible subdividir nuevamente la dirección IP en número de red, número de subred y número de *host* en la subred, teniendo así una jerarquía de tres niveles. Una ventaja adicional es que la estructura de las subredes no es vista por las redes externas garantizando otro nivel de seguridad para las redes internas, de la misma forma que permite que la administración de la red sea más flexible.

Fig. 2.3. Estructura de subredes.

Para definir ésta división es necesaria una máscara de subred, que consta de 32 bits. La máscara de subred es la encargada de delimitar el número de subredes y el número de hosts para cada división dependiendo de las necesidades de la organización.

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° de hosts o N°. de subredes = $2^n - 2$, donde n = N° de bits.

2.1.5. Enrutamiento entre Dominios sin Clase. CIDR.

2.1.5.1. Super-redes.

Con el crecimiento de Internet, se hizo claro que los identificadores de red clase B se acabarían muy pronto. Para la mayoría de las organizaciones, un identificador clase C no contiene suficientes identificadores de *host*, en cambio, un identificador de red clase B contiene suficientes bits para proporcionar un esquema de subredes flexibles dentro de la organización.

Las autoridades de Internet diseñaron un nuevo método para asignar identificadores de red para prevenir la duplicidad de identificadores de red clase B.

En lugar de asignar un identificador de red clase B, el InterNIC asignó un rango de identificadores de clase C que contenía suficientes identificadores de red y de servidores para las necesidades de la organización. Esto se conoce como creación de superredes (*supernetting*).

Con la creación de subredes y superredes, los algoritmos de enrutamiento deberían conocer las redes a través de su dirección IP y su máscara. En el caso de las subredes resulta en tener que agregar más información para cada subred. Gracias a las superredes se logró agrupar a un conjunto de subredes, facilitando el enrutamiento. Así al asignar varias direcciones tipo C en lugar de una sola tipo B se conservan los números tipo B y se resuelve el problema inmediato de la terminación del espacio para las direcciones de éste. Sin embargo, ésto da origen a un nuevo problema: la información que los enrutadores almacenan e intercambian aumenta dramáticamente. La técnica conocida como CIDR resuelve el problema.

Conceptualmente CIDR condensa un grupo de direcciones tipo B y C contiguas en un solo registro representados por dos datos: direcciones de red y conteo del número de bits, en donde la dirección de red es la más pequeña del grupo y el conteo especifica el número total de direcciones en el grupo.

Aunque esta técnica ayuda a conservar identificadores de red clase B, crea un nuevo problema. Usando las técnicas de enrutamiento convencional, los enrutadores ahora deben tener 8 identificadores de red clase C en sus tablas de enrutamiento para enrutar los paquetes IP. Para evitar que los enrutadores se sobrecarguen con rutas, se utiliza la *CIDR*, para colapsar múltiples identificadores de red en un único elemento correspondiente a todos los identificadores de red clase C asignados a esa organización.

2.1.6. VLSM (Variable Length Subnet Mask).

El término VLSM, se refiere a que una red puede ser configurada con diferentes máscaras de red. Éste 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 la red, de acuerdo a las diferentes necesidades, 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, sólo puede ser utilizada una máscara de subred.

Los beneficios de VLSM incluyen lo siguiente:

- Uso más eficiente de las direcciones IP.
- Uso de diferentes máscaras de red.

Aún y con las ventajas ya mencionadas de VLSM existen limitaciones. Una de las más grandes es que no todos los protocolos de enrutamiento pueden manejar VLSM. Por ejemplo, RIP v1 e IGRP no pueden utilizar máscaras variables, sin embargo protocolos como OSPF, EIGRP, ISIS y RIP versión 2 si soportan este esquema. Por consiguiente, si se quiere aprovechar las bondades que el esquema VLSM provee, se necesita implantar un protocolo cuyas características de diseño lo haya tomado en cuenta.

2.2. ENRUTAMIENTO IP.

2.2.1. Arquitectura de Enrutamiento.

Una arquitectura de enrutamiento engloba el esquema de comunicación entre las diversas redes alrededor del mundo, considerando que cada red interna tiene su propio esquema de comunicación, su propia topología, tecnología de backbone y protocolos de comunicación.

Existen dos tipos de enrutamiento: directo e indirecto.

- En el directo, existe un dispositivo transmitiendo de manera directa un paquete de información a otro, siempre y cuando ambos pertenezcan al mismo segmento lógico.
- En el indirecto, los dos dispositivos que se requiere comunicar no están en la misma red ni lógica ni física, lo cual nos genera la necesidad de equipo adicional que interconecte ambas redes.

Los enrutadores trabajan con tablas de enrutamiento en las que se almacena información referente a posibles destinos y como llegar a ellos. Estas pueden ser generadas, o bien intercambiadas con otros enrutadores. Tanto este intercambio de tablas, como información de control ó de calidad de servicio, se realizan mediante algoritmos de enrutamiento, que fueron diseñados para propósitos particulares dependiendo del impacto que se requiera dar a la red.

Estos tienen las siguientes características:

- Robustez. Nos indica si un algoritmo puede soportar una gran cantidad de rutas en las tablas de enrutamiento, de forma que sea hasta cierto punto, fácil de implementar.
- Estabilidad. Nos indica que los anuncios de enrutamiento (el agregar nuevas rutas debido a la integración de nuevos dispositivos, por ejemplo) que se dan en el ruteador deben de ser coherentes con lo que acontece en la red, de manera que no se presenten oscilaciones ó *loops* en las rutas tomadas.
- Flexibilidad. Esta característica va más enfocada hacia la expansión de los equipos de enrutamiento en cuanto a tarjetas para nuevos enlaces, y que se permita una reconfiguración sencilla.
- Simplicidad. El algoritmo debe ofrecer eficiencia en su funcionalidad, operación y mantenimiento con un mínimo de recursos.
- Optimización. El algoritmo debe de ser capaz de converger a todas las rutas óptimas independientemente de la posición del enrutador en la red.
- Convergencia. El algoritmo debe de ser capaz de llegar a un mismo valor dentro de las rutas que se analizan, esto es que, a través de la interacciones, este llegará a la ruta óptima.

2.2.2. Clasificación.

Los algoritmos de enrutamiento pueden tener varias clasificaciones:

- Estáticos y Dinámicos.
- De trayectoria sencilla ó de Multitrayectoria.
- Plano ó Jerárquico.
- Extradominio ó Intradominio.
- Estado del Enlace ó Vector de Distancia.

2.2.2.1. Estáticos ó Dinámicos.

Los algoritmos estáticos son en los que se tiene, por medio del administrador, rutas predefinidas para llegar de un punto a otro de la red. En cambio en los dinámicos, el enrutador decide cual es la mejor ruta.

2.2.2.2. De trayectoria sencilla ó de Multitrayectoria.

Los algoritmos de Multitrayectoria permiten varias rutas para llegar a un mismo destino. En cambio, los de trayectoria sencilla, solo aceptan una sola ruta.

2.2.2.3. Plano ó Jerárquico.

En los sistemas planos, todos los equipos de enrutadores tienen el mismo nivel y cualquiera puede hacer la operación de enrutamiento. En cambio, en el jerárquico, existen equipos que dan forma a la red y son estos los que pueden realizar las operaciones de enrutamiento.

2.2.2.4. Extradominio ó Intradominio.

En los primeros, los equipos de enrutamiento pueden intercambiar información como tablas de ruteo con equipos de sistemas autónomos diferentes. En cambio, los segundos solo pueden hacer este intercambio con su mismo sistema autónomo.

Un sistema autónomo (AS) es un grupo de redes IP que son gestionadas por uno o más operadores de red que poseen una clara y sola política de rutas. Cada AS tiene un número que es utilizado como un identificador para el intercambio de rutas con otros sistemas externos.

2.2.2.5. Estado del Enlace ó Vector de Distancia.

Los primeros, también conocidos como de Camino Más Corto (*Shortest Path First*), envían información de enrutamiento a todos los equipos de la red; sin embargo, cada enrutador solo envía una porción de su tabla de enrutamiento en la que describe el estado de sus enlaces. En los segundos, también conocidos como Bellman-Ford, los equipos de enrutamiento envían toda la tabla pero solo a sus vecinos.

2.3. Protocolos de Enrutamiento.

Para entender con mayor claridad estos conceptos, es importante ejemplificar con algunos protocolos la utilidad de los puntos antes mencionados, para ello cabe destacar la presencia de Protocolos de Compuerta Interna (IGP), los cuales son usados para intercambiar información de enrutamiento entre enrutadores dentro de un sistema autónomo. Entre ellos se encuentran: RIP, IGRP, HELLO y OSPF, entre otros. Todos los IGPs cumplen la misma función, determinar la ruta optima de destino.

También existen aquellos Protocolos de Compuerta Externa (EGP), los cuales son utilizados para intercambiar información de enrutamiento entre diferentes sistemas autónomos, en donde cada enrutador es responsable de la información de su propio sistema. Como ejemplo podemos citar a BGP (Border Gateway Protocol) y a EGP.

Debido a que el presente trabajo tiene la intención de dar a conocer las necesidades del estado actual de la RedUNAM en cuanto a enrutamiento se refiere, es necesario mencionar dos protocolos de tipo IGP y EGP, los cuales son OSPF y BGP respectivamente, sin embargo no está dentro de los puntos medulares para la arquitectura de QoS a implementar, pero estos se describen brevemente en el anexo B del presente trabajo.

2.4. SERVICIOS.

2.4.1. Voz sobre IP (VoIP).

A finales de 1997, el Foro de Voz sobre IP (*VoIP forum*) del IMTC llegó a un acuerdo que permite la interoperabilidad de los distintos elementos que pueden integrarse en una red VoIP. Debido a la ya existencia del estándar H.323 del ITU-T, que cubría la mayor parte de las necesidades para la integración de la voz, se decidió que el H.323 fuera la base de VoIP. De este modo, VoIP debe considerarse como una clarificación del H.323, de tal forma que en caso de conflicto, y a fin de evitar divergencias entre los estándares, se decidió que H.323 tendría prioridad sobre VoIP.

VoIP tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes para la transmisión de voz sobre la infraestructura de red IP, fijando aspectos tales como la supresión de silencios, codificación de la voz y direccionamiento, así como el establecimiento de nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional. Estos elementos se refieren básicamente a los servicios de directorio y a la transmisión de señalización por tonos multifrecuencia (DTMF)

El concepto de Voz sobre IP, trata de transformar la voz en "paquetes de información" manejables por una red IP. Gracias a otros protocolos de comunicación, como el RSVP (Protocolo de administración de recursos que será descrito en el siguiente capítulo), es posible reservar cierto ancho de banda dentro de la red que garantice la calidad de la comunicación.

La voz puede ser obtenida desde un micrófono conectado a la tarjeta de sonido de la PC, o bien desde un teléfono común: existen *gateways* (dispositivos de interconexión) que permiten intercomunicar las redes de telefonía tradicional con las redes de datos.

De hecho, el sistema telefónico podría desviar sus llamadas a Internet para que, una vez alcanzado el servidor más próximo al destino, la llamada vuelva a ser traducida como información analógica y sea transmitida hacia un teléfono común por la red telefónica tradicional.

Los paquetes VoIP se componen de una o más muestras de *codec* de voz o tramas encapsuladas en cabeceras IP/UDP/RTP (*Real-Time Transport Protocol*, Protocolo de Transporte en Tiempo Real). VoIP usa UDP como protocolo de capa de transporte, ya que no se necesitan los servicios de retransmisión de TCP. Cabe recordar que para las aplicaciones en tiempo real, los paquetes retransmitidos llegan demasiado tarde para que el receptor los pueda usar. UDP proporciona los servicios de entramado y multiplexión de la aplicación para VoIP (a través de los números de puerto UDP), y RTP proporciona los servicios adicionales que se necesitan para el transporte de datos en tiempo real.

VoIP/H.323 comprende a su vez una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación:

- Direccionamiento.
- Señalización.
- Compresión y Transmisión de Voz.

2.4.1.1. Direccionamiento.

- RAS (Registration, Admission and Status). Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través del Gatekeeper.

- DNS (Domain Name Service). Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS.

2.4.1.2. Señalización.

- **Q.931.** Señalización inicial de llamada.

- **H.225.** Control de llamada: señalización, registro y admisión, y paquetización / sincronización del *stream* (flujo) de voz.

- **H.245.** Protocolo de control para especificar mensajes de apertura y cierre de canales para streams de voz.

2.4.1.3. Compresión de Voz.

- Requeridos: G.711 y G.723.

- Opcionales: G.728, G.729 y G.722

2.4.1.4. Transmisión de Voz.

- **UDP.** La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.

- **RTP.** Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

2.4.1.5. Control de la Transmisión.

RTCP (Real Time Transport Control Protocol). Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctivas.

Los elementos que permiten construir las aplicaciones VoIP

- Teléfonos IP.
- Adaptadores para PC.
- Hubs Telefónicos.
- *Gateways.*
- *Gatekeeper.*
- Unidades de audio conferencia múltiple.
- Servicios de Directorio.

Nota. Los conceptos de algunos equipos como *Gateway*, *Gatekeeper* y Unidad de Audio para Conferencia Múltiple, serán definidos en el tema de H.323.

Un aspecto importante a señalar es el de los retardos en la transmisión de la voz. Se debe tomar en cuenta que la voz no es muy tolerante con estos. De hecho, si el retardo introducido por la red es de mas de 300 ms, resulta casi imposible tener una conversación fluida. Debido a que las redes de área local no están preparadas en principio para este tipo de tráfico, el problema puede parecer grave. Hay que tener en cuenta que los paquetes IP son de longitud variable y el tráfico de datos suele ser en ráfagas. Para intentar obviar situaciones en las que la voz se pierde porque tenemos una ráfaga de datos en la red, se ha ideado la implementación del protocolo de señalización RSVP. Éste, en una de sus funciones principales es cortar los paquetes de datos grandes y dar prioridad a los paquetes de voz cuando hay una congestión en un enrutador. Si bien éste protocolo ayudará considerablemente al tráfico multimedia por la red, hay que tener en cuenta que RSVP no garantiza una calidad de servicio como ocurre en redes avanzadas tales como ATM que proporcionan QoS de forma estándar.

2.4.1.6. Ventajas de la Tecnología de Voz sobre IP.

- Integración sobre una Intranet de la voz como un servicio más de red, tal como otros servicios informáticos.
- Las redes IP son la red estándar universal para la Internet, Intranets y Extranets.
- Estándares efectivos (H.323).
- Interoperabilidad de diversos proveedores.
- Uso de las redes de datos existentes.
- Independencia de tecnologías de transporte (capa 2), asegurando la inversión.
- Menores costos que tecnologías alternativas (voz sobre TDM, ATM, Frame Relay), si es que ya está reglamentado por la competencia gubernamental correspondiente, ya que no se paga SLM ni Larga Distancia en sus llamadas sobre IP.

Los protocolos de señalización que son utilizados en VoIP tales como H.323 y SIP, que serán definidos a continuación.

2.4.2. H.323 Video.

El estándar H.323 proporciona la base para la transmisión de voz, datos y video sobre redes no orientadas a conexión y que no ofrecen un grado de calidad del servicio, como son las basadas en IP (incluida Internet), de manera tal que las aplicaciones y productos conforme a ella puedan interoperar, permitiendo la comunicación entre los usuarios sin necesidad de que éstos se preocupen por la compatibilidad de sus sistemas. La LAN sobre la que las terminales H.323 se comunican puede ser un simple segmento ó anillo, o bien, múltiples segmentos (es el caso de Internet) con una topología compleja, lo que puede resultar en un grado variable de rendimiento.

H.323 es la especificación, establecida por la UIT en 1996, que fija los estándares para la comunicación de voz y video sobre redes de área local, con cualquier protocolo, que por su propia naturaleza presentan una gran latencia y no garantizan una determinada calidad del servicio. Para la conferencia de datos se apoya en la norma T.120, con lo que en conjunto soporta las aplicaciones multimedia. Las terminales y equipos conforme a H.323 pueden tratar voz en tiempo real, datos y video, incluida videotelefonía.

El estándar contempla el control de la llamada, gestión de la información y ancho de banda para una comunicación punto a punto y punto a multipunto, dentro de la LAN. Así también define interfaces entre la LAN y otras redes externas, como puede ser una RDSI. Es una parte de una

serie de especificaciones para videoconferencia sobre distintos tipos de redes, que incluyen desde la H.320 a la H.324, éstas dos válidas para RDSI y RTPC, respectivamente.

H.323 establece los estándares para la compresión y descompresión de audio y video, asegurando que los equipos de distintos fabricantes se entiendan. Así, los usuarios no se tienen que preocupar de cómo el equipo receptor actúe, siempre y cuando cumpla este estándar. La administración del ancho de banda disponible para evitar que la LAN se colapse con la comunicación de audio y video, por ejemplo, limitando el número de conexiones simultáneas, también está contemplada en el estándar.

La norma H.323 hace uso de los procedimientos de señalización de los canales lógicos contenidos en la norma H.245, en los que el contenido de cada uno de éstos canales se define cuando se abre. Estos procedimientos se proporcionan para fijar las prestaciones del emisor y receptor, el establecimiento de la llamada, intercambio de información, terminación de la llamada y cómo se codifica y decodifica. Por ejemplo, cuando se origina una llamada telefónica sobre Internet, las dos terminales deben negociar cual de las dos ejerce el control, de manera tal que sólo uno de ellos origine los mensajes especiales de control. Una cuestión importante es, como se ha dicho, es determinar las capacidades de los sistemas, de forma que no se permita la transmisión de datos si no pueden ser gestionados por el receptor.

2.4.2.1. Arquitectura H.323

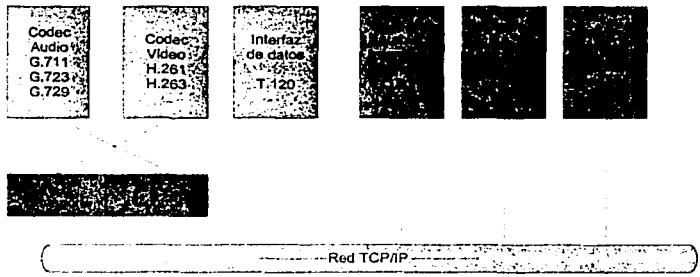


Fig. 2.4. Arquitectura H.323

Una característica de la telefonía sobre una LAN ó Internet es que se permite la información de video sobre la de audio (videoconferencia), que se le da formato de acuerdo con el estándar H.261 ó H.263, formando parte de la carga útil del paquete RTP. Dado que se envían sólo los cambios entre cuadros resulta muy sensible a la pérdida de paquetes, lo que da origen a la distorsión de la imagen recibida.

2.4.2.2. Componentes definidos en H.323.

La especificación define cuatro componentes principales para un sistema de comunicaciones en red: Terminales, Enrutadores, *Gatekeepers* y MCUs.

2.4.3.2.1. Terminales.

Son los clientes finales en la LAN. Proporcionan una comunicación bidireccional en tiempo real. Todos los componentes terminales deben soportar la comunicación de voz, mientras que la de video y datos son opcionales.

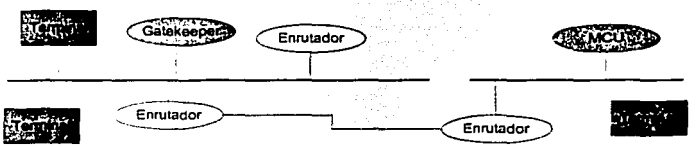


Fig. 2.5 Terminales H.323

Además, deben soportar:

- La norma H.245 la cual se emplea para la negociación del uso del canal y sus prestaciones.
- Q.931 para el establecimiento de la llamada y la señalización.
- RAS (*Registration-Admission-Status*), el cual es un protocolo utilizado para la comunicación con el *Gatekeeper* y sólo si éste está presente en la red.
- Soporte para RTP/RTCP que fija la secuencia de los paquetes de audio y video.
- Opcionalmente las terminales pueden incorporar un codec para video, conferencia de datos según T.120 y la Unidad de Control Multipunto (*MCU, Multipoint Control Unit*).
- Otro protocolo del IETF, aunque no es parte del H.323, el RSVP.

El protocolo TCP/IP utilizado en múltiples comunicaciones es un protocolo de transferencia seguro, gracias a TCP, lo que asegura la transmisión libre de errores. Sin embargo, no hay garantía de que los paquetes lleguen ordenados a su destino en tiempo real, lo que causa problemas para la voz o el video. Para evitar este efecto, el IETF ha propuesto el protocolo RTP que facilita las comunicaciones multimedia.

2.4.3.2.2. Enrutador.

El Enrutador es un elemento opcional en una conferencia H.323, que proporciona muchos servicios incluida la adaptación con otras normas del ITU, es decir, proporciona interoperabilidad con tecnologías que no son H.323, como videoconferencias RDSI ó redes telefónicas tradicionales. En general, su misión es establecer un enlace con otras terminales ubicados en la RTB o RDSI.

Los enrutadores administran:

1) la conversión de señalización de llamada,
2) la conversión de señalización de medios y
3) la conversión de medios cuando se conecta una red H.323 a otra de distinto tipo.

2.4.3.2.3. Gatekeeper.

El *Gatekeeper* realiza dos funciones de control de llamadas que preservan la integridad de la red de datos. La primera es la traducción de direcciones de las terminales de la LAN a las correspondientes IP o IPX, tal y como se describe en la especificación RAS. La segunda es la administración del ancho de banda, fijando el número de conferencias que pueden estar dándose simultáneamente en la LAN y rechazando las nuevas peticiones por encima del nivel establecido, de manera tal que se garantice ancho de banda suficiente para las aplicaciones de datos sobre la LAN.

El *Gatekeeper* proporciona todas las funciones anteriores para las terminales, enrutadores y MCUs, que están registrados dentro de la denominada Zona de control H.323.

2.4.3.2.4. Unidad de Control Multipunto, (MCU)

La Unidad de Control Multipunto está diseñada para soportar la conferencia entre tres o más puntos, bajo el estándar H.323, llevando la negociación entre terminales para determinar las capacidades comunes para el proceso de audio y video, así como controlar la multidifusión.

La comunicación bajo H.323 contempla las señales de audio y video. La señal de audio se digitaliza y se comprime bajo uno de los algoritmos soportados, tales como el G.711 ó G.723, y la señal de video (opcional) se trata con la norma H.261 ó H.263. Los datos se manejan de forma opcional bajo el estándar T.120 que permite compartir aplicaciones en conferencias punto a punto y punto a multipunto.

2.4.3.3. Protocolo de Inicialización de Sesión (*SIP*)

Es un protocolo de control de aplicación de capas para crear, modificar y cerrar sesiones con uno o más participantes. Estas sesiones incluyen conferencias multimedia, llamadas de teléfono, distribución multimedia por Internet, etc.

SIP es uno de los protocolos que forman la arquitectura IETF para una comunicación multimedia escalables, en tiempo real y multiparte. Algunos de los protocolos más destacados de esta arquitectura son:

- RTP y RTCP, que se especifican en la RFC 1889, proporcionan una entrega en tiempo real de los medios.
- El Protocolo de flujo en tiempo real (RSTP, *Real-Time Streaming Protocol*), que se especifica en la RFC 2326, proporciona una entrega bajo demanda de datos en tiempo real.
- El protocolo de descripción de sesión (SDP, *Session Description Protocol*), que sé especifica en el RFC 2327, proporciona un formato de descripción estándar para el intercambio de capacidad de los medios (como los codecs de voz para VoIP). El protocolo SAP, proporciona un método de publicación destinado a las sesiones multidifusión (como un Directorio de sesión (SDR, *Session Directory*).

SIP se diseñó como una solución a largo plazo para las conferencias multimedia y la telefonía en Internet. Se han tenido en cuenta muchas consideraciones con el desarrollo del protocolo para asegurarse de que es una plataforma viable para futuras comunicaciones que se basen en Internet:

- Simplicidad. SIP emplea mensajes de texto plano que se pueden leer. Seguidos, además, de formatos estándares como HTTP 1.1 y *mailto*. Esto hace que el protocolo sea relativamente sencillo para resolver problemas e integrarse con otras aplicaciones.

- Eficiencia. El protocolo superior de SIP tiene poco impacto en la eficiencia de la comunicación, puesto que las funciones de señalización consumen poco ancho de banda en relación con el flujo de medios. SIP es muy eficaz en términos de tiempo de conexión de llamada, ya que toda la información que se pide para el establecimiento de ésta se incluye en el mensaje inicial.

- Escalabilidad. Los servidores no mantienen la información del estado de las sesiones basadas en UDP en el SIP que procesan, por lo que un solo servidor puede manipular eficientemente muchos clientes. SIP detecta y previene los bucles de enrutamiento de mensajes, lo que aumenta el rendimiento de las redes extensas.

- Flexibilidad. Dado que SIP usa SDP para negociar los *codecs*, se puede utilizar cualquiera registrado por la IANA.

- Soporte de movilidad. El modelo de comunicación SIP se dirige a los usuarios que se pueden mover de terminal a terminal (por ejemplo, teléfonos y computadoras), lo contrario a los terminales en sí mismos. El protocolo proporciona soporte para *proxying* y redirección, por lo que los usuarios tienen la opción de proporcionar u ocultar su verdadera ubicación.

- Programación del usuario. Además del soporte nativo para las funciones de telefonía tradicional, SIP puede aprovecharse del Lenguaje de Procesamiento de Llamada (CPL, *Call Processing Language*). Éste permite a los usuarios proporcionar reglas complejas a un servidor, sin importar quién pueda localizarlas, cuándo, dónde y con qué tipo de medios. Las herramientas como *servlets* y las extensiones de la Interfaz de Gateway Común (CGI) de SIP se encuentran en estandarización actualmente, lo que facilita el desarrollo de las aplicaciones que éste permite.

- Extensión. Los creadores del protocolo reconocieron que no podían prever todas las peticiones del mismo, por lo que crearon una arquitectura que fuese modular y flexible.

2.4.4. IP Multicast.

Multicast (mensajes punto a multipunto) es un modelo de comunicación que consiste en que un nodo origen envía un mensaje a un grupo de nodos destino. Aunque, esto podría realizarse enviando mensajes unicast (mensajes punto a punto) a cada nodo destino, es mucho más conveniente utilizar los mensajes multicast que disminuyen la carga de la red, es decir, la utilización del ancho de banda para estas aplicaciones sería el mínimo.

En multicast el nodo origen transmite un solo paquete y solamente es replicado si es necesario. La utilización de grupos es esencial en esta tecnología. Por definición un mensaje multicast es enviado de un origen a un grupo de nodos destino. Estos grupos tienen un identificador de grupo (*GroupID*). Cuando un mensaje multicast es enviado, el grupo destino está especificado por el identificador de grupo. Estos identificadores son esencialmente un conjunto de direcciones IP pertenecientes a la clase D de direcciones IP. Por lo tanto si un nodo (un proceso en éste) quiere recibir mensajes multicast enviados a cierto grupo en particular, de alguna manera tiene que escuchar los mensajes dirigidos a ese grupo. Si las direcciones origen y destino multicast comparten el mismo *bus* (por ejemplo, *ethernet*), cada nodo sólo necesita saber a que grupos pertenecen el ó los procesos multicast en ese nodo. Sin embargo, si las direcciones origen y

destino no pertenecen a la misma LAN, el direccionamiento de los mensajes entre éstos se vuelve más complicado. Para resolver el problema de direccionamiento de los mensajes en Internet, los nodos necesitan unirse a un grupo informándole al ruteador multicast de su subred. El protocolo de Administración de Grupos en Internet (*Internet Group Management Protocol, IGMP*) es usado con este propósito. Éste protocolo también se hace cargo cuando un nodo deja de formar parte del grupo. De esta manera los enrutadores multicast conocen a los miembros de grupos multicast en su red y pueden decidir si direccionan o no un mensaje a su red.

Cuando un enrutador multicast recibe un mensaje de este tipo, verifica el identificador de grupo del mensaje y direcciona el paquete sólo si hay un miembro de ese grupo en las redes directamente conectadas. Sin embargo cuando se tiene que entregar un paquete del nodo origen al destino en otras redes, los enrutadores multicast necesitan intercambiar la información que ellos han reunido a partir de las membresías de los nodos que tienen directamente conectados. Hay varios algoritmos y protocolos utilizados para realizar el intercambio de información de enrutamiento, los cuales no los describiremos porque están fuera del alcance de la investigación.

Basados en la información de enrutamiento obtenida por algún protocolo, cuando un paquete multicast es enviado a algún grupo, los enrutadores decidirán si direccionan ó no el paquete a sus redes. Finalmente el último enrutador verificará por medio de la información IGMP si hay algún miembro de ese grupo en sus redes directamente conectadas y decidirá si direcciona el paquete o no.

Hay aplicaciones que pueden tomar ventaja de esta tecnología como videoconferencias, aprendizaje a distancia, distribución de software, distribución de noticias.

En la figura 2.6. se demuestra como los datos son entregados de un origen a varios destinos usando IP multicast.

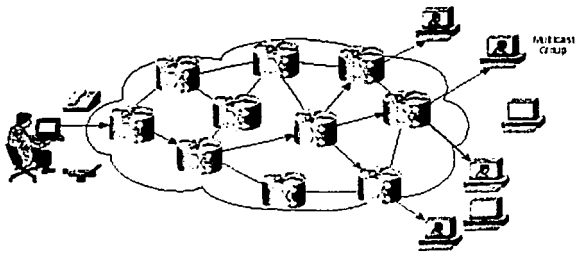


Fig. 2.6. Multicast, de uno a muchos.

Hay tres tipos de direcciones IP en IPv4: *unicast, broadcast* y *multicast*. Las direcciones unicast se usan para transmitir un mensaje a un único nodo. Las direcciones broadcast son utilizadas cuando quiere ser transmitido a todos los nodos de la subred. Y las direcciones multicast son utilizadas cuando se entrega un mensaje a un grupo de nodos destinos, los cuales no están necesariamente en la misma subred, este grupo no tiene fronteras físicas o geográficas (los nodos pueden estar localizados en cualquier parte de Internet). Mientras las clases de direcciones IP A, B, y C son usadas en mensajes unicast, las direcciones de la clase D son usadas para mensajes multicast, lo que significa que el rango de los mensajes multicast oscila entre: 224.0.0.0 – 239.255.255.255. Este rango de direcciones fue asignado por la IANA

Una dirección multicast es asignada a un grupo de nodos definiendo así a un grupo multicast. Los cuatro bits más significativos de las direcciones clase D son: 1110. Los siguientes 28 bits son lo que conocemos como "identificador de grupo multicast". Algunas direcciones clase D están reservadas para propósitos especiales por la IANA. El bloque de direcciones entre 224.0.0.1 a 224.0.0.255 está reservado para los protocolos de enrutamiento en los segmentos de red locales. Los paquetes con éstas direcciones nunca deben ser direccionados por el enrutador. Ellos permanecen locales en un segmento de red en particular. Los protocolos de red usan éstas direcciones para descubrimientos automáticos y para comunicar información de enrutamiento importante. Por ejemplo, OSPF utiliza 224.0.0.5 y 224.0.0.6 para intercambiar información estado de enlace. El bloque de direcciones entre los rangos 239.0.0.0 y 239.255.255.255 está definido en el RFC 2365, y está reservado para los grupos locales u organizaciones y no para aplicaciones propias de Internet. Hay otras direcciones clase D que están reservadas también y que son llamadas las direcciones bien conocidas:

Direcciones	Uso
224.0.0.1	Todos los sistemas en esta red
224.0.0.2	Todos los enrutadores en esta red
224.0.0.5	Enrutadores OSPF
224.0.0.6	Enrutadores OSPF designados
224.0.0.12	Servidor DHCP

Tabla 2.3. Direcciones bien conocidas clase D.

El formato de una dirección IP clase D se muestra en la figura 2.7:

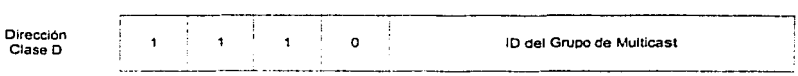


Fig. 2.7. Dirección IP clase D.

Un datagrama multicast es entregado a los miembros del grupo con la misma fiabilidad que un paquete unicast. También es posible la pérdida de paquetes y la entrega fuera de orden. Como en las direcciones unicast debe haber un mapeo de direcciones IP a direcciones MAC. La IANA reservó un conjunto de dirección MAC para los paquetes multicast, a partir de 01:00:5E:00:00:00 hasta 01:00:5E:7F:FF:FF. Una dirección IP multicast puede ser mapeada colocando los 23 bits menos significativos de la dirección IP multicast en los 23 bits menos significativos de la dirección MAC. El mapeo de una dirección IP multicast a una dirección MAC se muestra en la siguiente figura:

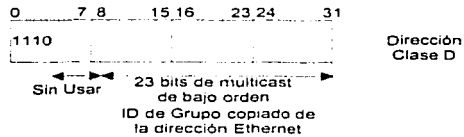


Fig. 2.8. Mapeo de una dirección IP multicast a una dirección MAC

III. MODELOS DE CALIDAD DE SERVICIO

ARQUITECTURAS DE CALIDAD DE SERVICIO.

La definición de una arquitectura depende sobre todo, de las necesidades específicas de cada red, así como el uso de las herramientas disponibles apropiadas para ello. En este capítulo definiremos éstas herramientas, las cuales nos ayudarán a la definición de una arquitectura apropiada para nuestra red en estudio (Red UNAM). Describiremos tanto los modelos de calidad de servicio que se tienen actualmente definidos por la IETF, así como los protocolos que se asocian a cada uno de ellos, además de los que no son directamente asociados a un modelo en especial, como lo es MPLS, pero que es fundamental en la cadena que nos permitirá definir calidad de servicio punto a punto.

3.1. PARÁMETROS DE CALIDAD DE SERVICIOS EN EL TRÁFICO.

En términos cualitativos y cuantitativos la calidad de servicios está directamente relacionada con la respuesta percibida por los usuarios finales cuando acceden a la red y por el grado de satisfacción de los mismos. Si la respuesta de la red no es buena es porque hay deficiencias que impiden acomodar elevadas cargas de tráfico, puntuales o permanentes.

La calidad de servicios se refleja, como se ha indicado, en una serie de parámetros o factores que se pueden medir y ajustar convenientemente para proporcionar un grado de servicio satisfactorio. En las redes IP, los factores que determinan e impactan el desempeño de las aplicaciones son:

3.1.1. Retraso o latencia.

Esta es una característica del manejo de los datos dentro de la red. Es cuando la información no llega en el tiempo esperado de acuerdo a la ruta que se trazó para su información. Existen tres componentes causantes de este retraso:

a) El retraso debido a los componentes de la red (*internetwork*)

Está directamente relacionado con la capacidad que tengan los dispositivos y los enlaces. Una vez que el tráfico supera esta capacidad, este retraso es constante. Una red bien diseñada, debe tener una capacidad mayor (pero no demasiado) a la que sería necesaria para manejar una tasa de transmisión promedio dependiendo de las aplicaciones que se manejen, sin embargo, siempre habrá picos de tráfico en donde la congestión sea inherente y por tanto, existan retrasos en la información.

b) El retraso debido a los protocolos involucrados.

Depende de las características de cada protocolo y de su forma de trabajar. La encripción, compresión, corrección de errores en capas altas y los algoritmos para acceso a la red como CSMA/CD en capas bajas, son algunas de las causas por las cuales un protocolo causa retraso. Este será inherente de acuerdo a la aplicación.

c) El retraso producido por el reenvío de la información.

Existen aplicaciones que antes de enviar su información requieren una confirmación de que la comunicación entre ambos nodos de la red se ha establecido, produciendo un retraso en el envío. Así también, el tiempo de procesamiento de los dispositivos intermedios que intervienen ya sea para la conmutación o enrutamiento de los datos agrega un retraso adicional.

El retraso total dentro de la red será entonces una función del retraso en hardware, el retraso en acceso, el retraso en transmisión y el retraso en el tiempo de procesamiento dentro de los dispositivos.

De estos, el que más influye es el retraso en la transmisión. A medida que el tráfico viaja en la red, este atraviesa por sus nodos intermedios. El retraso que el nodo produce se puede deber a la carga del procesador de este nodo, los niveles de búferes de memoria o bien algunos filtros de paquetes y listas de acceso que este nodo tenga programados.

3.1.2. Variabilidad del retraso ó *jitter*

Aunque en muchas ocasiones el retraso es inevitable, en la mayoría de éstas no perjudica si éste es constante, aún en las aplicaciones que son en tiempo real, a menos que estas sean interactivas. El factor que realmente afecta es la variabilidad de este retraso dentro de la red conocido como *jitter*.

Esta variación, así como el retraso en sí mismo como ya vimos, se debe a diversas causas como lo son físicas, de acceso, de red y de establecimiento de sesión:

a) Variación en el retraso por hardware. La mayoría de los sistemas de hardware actuales proveen un nivel de retraso constante. Sin embargo, sistemas más viejos varían sus velocidades de transmisión si se tienen enlaces de longitudes muy grandes.

b) Variación en el retraso de acceso. Éste es el cambio con el cual la aplicación es capaz de tomar su derecho a transmitir dentro de la red.

c) Variación en el retraso de red. Éste se debe al congestionamiento de la red. En este caso, el encolamiento de la información así como el descartamiento de paquetes, ocasionan retransmisiones que son las causantes del retraso. La variación se debe a que el descartamiento de información sucede de forma aleatoria.

d) Variación en el establecimiento de sesiones. Cuando se establece una sesión, se deben establecer una serie confirmaciones. Dependiendo de factores como la carga de los procesadores, esta secuencia de pasos experimenta retrasos impredecibles para comenzar el servicio de red.

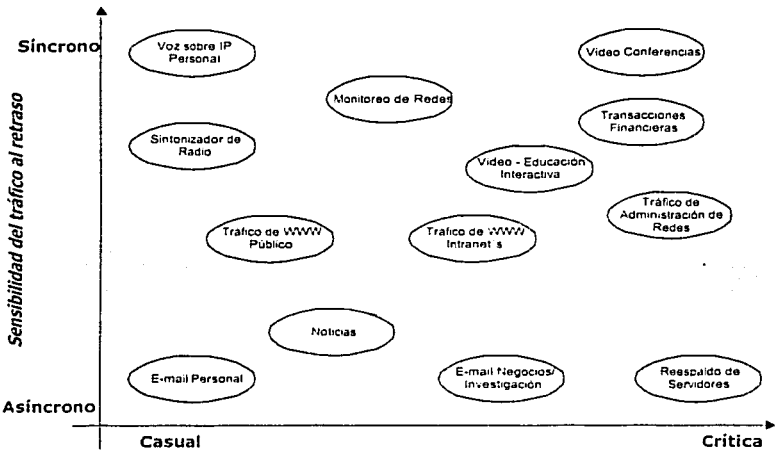


Fig. 3.1. Sensibilidad del tráfico al retraso.

3.1.3. Capacidad.

Para poder entender tanto la capacidad de la red para manejar información así como la rapidez para entregarla, tenemos que saber como se mide ésta. La medida de transmisión de información dentro de una red son bits o paquetes por segundo.

Sin embargo, nunca se puede transmitir a una capacidad mayor a la que tiene nuestro enlace físico. Por ejemplo, en un enlace E1, nunca podremos rebasar los 2.048 Mbps, que es la capacidad de éste.

Además de éstos puntos, existen otros adicionales como lo es el exceso de usuarios dentro de la red así como la tasa de errores. Con las nuevas tecnologías que vienen a dar una mayor seguridad en los enlaces de transmisión, la tasa de errores tiende a ser mínima, mientras que se está presentando un exceso de usuarios cada vez mayor, siendo esto una de las razones más importantes por las cuales se necesita una administración del ancho de banda de la red.

La reservación de ancho de banda para una aplicación permite que la red tenga la suficiente capacidad para soportar las necesidades de transporte de cada aplicación.

3.1.4. Pérdida de tráfico.

La pérdida de paquetes en una red se da cuando ésta se encuentra congestionada, entonces la red comienza a descartar paquetes de información.

Esta pérdida es muy importante en servicios como los son voz y video, debido a que se afecta al proceso de decodificación de éstos en el receptor, lo que es percibido por el usuario final. También afecta a aplicaciones de transmisión de datos, debido a las retransmisiones que se generan por estas pérdidas.

3.2. Tipos y características del tráfico.

Cada uno de los servicios tiene ciertas características propias que se deben de tomar en cuenta para un correcto manejo de este tipo de tráfico.

El tipo de aplicaciones que son realmente críticas en su desempeño son aquellas que necesitan ser recibidas en tiempo real, como lo son las aplicaciones de voz y video interactivo.

3.2.1. Voz.

El tráfico de voz requiere un ancho de banda relativamente pequeño. Una línea telefónica digital normal tiene una tasa de transmisión de 64 kbps (norma UIT-G.711), o bien, comprimiéndolos y teniendo 2 circuitos de 32 kbps dentro de este enlace (norma UIT-G.726).

Éste tráfico es sensible a pérdidas, sin embargo no puede soportar retrasos para corregirlas, por tanto, se puede aceptar un pequeño porcentaje de éstas, debido a la capacidad del oído humano de aceptarlas.

El tráfico de voz debe tener una tasa de transmisión constante pero puede ser pequeña. Consecuentemente, los tamaños de los mensajes son cortos (entre 44 y 200 bytes), permitiendo una transmisión rápida de cadenas de tráfico de baja velocidad.

Es importante señalar, que en una transmisión de voz, aproximadamente el 60% del tiempo son silencios o sonidos reconocidos como ruido de fondo, por lo que resulta intrascendente el envío de esta información sobre el canal, ya que solo lo ocupa de forma ociosa. Por esto se utiliza una red que permita la paquetización de la información para tener una optimización del ancho de banda al compartir el canal enviando información útil durante estos silencios.

3.2.2. Video.

El tráfico de video puede ser clasificado en dos grupos: video interactivo (conversacional) y video dirigido en una sola dirección (reproducción). Las sesiones de video son frecuentemente entregadas sobre enlaces WAN empleando conexiones múltiples. Con la finalidad de ampliar el mercado se han generado productos con diferentes tasas de transmisión que pueden ir desde un simple módem a 56 kbps hasta enlaces E1 a 2.048 Mbps.

Una aplicación típica de video puede estar compuesta por 128 kbps, por tal motivo los dispositivos deberán reconocer la relación entre el canal de control y los canales de datos.

3.2.3. Datos.

En el tipo de redes convergentes de las que estamos hablando, todo lo que corre sobre ellas son datos, lo que los diferencia son sus necesidades dependiendo de la aplicación, sobre todo si estas tienen requerimientos en tiempo real ó no. Las que entrarían en esta categoría serían las segundas, en donde se diferencian los que son datos críticos o no críticos. Considerando aplicaciones como correo electrónico, www, transferencias de archivos, etc.

3.3. Calidad de Servicio en IP.

Las tecnologías de red basadas en protocolos IP se están estableciendo como una plataforma fundamental para los actuales servicios de red a gran escala, y se puede decir que, con su próxima migración a versión 6, jugará un papel dominante en la evolución tanto de las redes públicas así como de las privadas.

La Calidad de Servicio sobre IP (*IP QoS*) se refiere a la forma en que la red diferencia al tráfico de éste tipo para dar prioridad a las aplicaciones que así lo requieran. Entre sus características principales, como fueron vistas al principio del capítulo, están la disponibilidad de recursos, el retraso, el *jitter*, la tasa de transmisión de carga útil y la tasa de paquetes perdidos.

Ésta calidad de servicio se puede obtener ya sea con el aumento del ancho de banda de la red, o bien, con la implementación de protocolos y políticas especiales para llegar a obtener estas funcionalidades en la red. Las aplicaciones multimedia se han convertido en una parte integral de las actuales arquitecturas computacionales, generando a su vez una gran cantidad de tráfico mixto que debe circular a través de la misma interfaz.

Existen dos arquitecturas de IP QoS definidas actualmente por la IETF (*Internet Engineering Task Force*), que son las de Servicios Integrados (*Int-Serv*) y la de Servicios Diferenciados (*Diff-Serv*). La arquitectura *Int-Serv* se enfoca básicamente hacia la reservación de recursos y se desarrolla en general en el borde de la red, en donde el flujo de tráfico puede ser manejado por el usuario. En cambio, *Diff-Serv* es más escalable y juega un papel fundamental en el desarrollo de la red debido a su habilidad para priorizar y clasificar flujos de tráfico, de acuerdo a políticas de administración del ancho de banda disponible.

Los flujos de datos de aplicaciones específicas, la topología de la red ó bien, un sistema de políticas de administración de ancho de banda dictan el tipo de QoS que será el más apropiado para cada flujo de datos. Para solventar esta necesidad, existen algunos protocolos y algoritmos como son:

- Protocolo de Reservación de Recursos (*ReSerVation Protocol, RSVP*).
- Comportamientos dependiendo de Dominios o bien de saltos intermedios: PHBs y PDBs.
- Conmutación por etiquetamiento de Multi protocolos (*MultiProtocol Label Switching, MPLS*).
- Administración de ancho de banda de subredes (Subnet Bandwidth Management, SBM) y los agregados del estándar 802.3p/Q.

Nivel de QoS	Red	Aplicación	Descripción.
Mayor	X		Aumento del ancho de banda de la red.
	X	X	RSVP. Servicios Integrados garantizados (Int-Serv)
	X	X	RSVP. Servicios Integrados Controlados (Int-Serv)
	X		MPLS.
	X	X	Diff-Serv.
			SBM a nivel LAN.
	X		Técnicas normales de encolamiento.
Menor			Mejor esfuerzo. Best-effort.

Tabla 3.1. Nivel de QoS.

3.3.1. Servicios Integrados. INT-SERV.

El modelo de servicios integrados definido en el RFC 2210, está formado por 4 componentes: la programación de paquetes, la rutina de control de admisión, la clasificación y el protocolo establecimiento de reservas. Los primeros 3 componentes forman el llamado control de tráfico. A continuación describiremos brevemente a los componentes.

- Programación de paquetes. Permite el manejo de paquetes utilizando colas y tal vez otros tipos de mecanismos como los temporizadores. Éste componente debe estar implementado en el punto donde los paquetes son encolados.
- Control de admisión. Implementa el algoritmo de decisión que un *host* ó enrutador utiliza para determinar si puede admitirse un nuevo flujo de datos, sin impactar a los otros. El control de admisión se lleva a cabo en cada nodo, lugar en el que se toma la decisión de aceptar ó denegar en el momento en que un *host* pide un servicio de tiempo real en Internet.
- Clasificación. Éste componente toma todos los paquetes de entrada y los mapea a alguna clase de tráfico. Todos los paquetes de una clase son tratados de la misma manera, ésta clasificación se basa en el contenido de los encabezados de los paquetes.
- Protocolo de establecimiento de reservaciones. Éste es necesario para crear y mantener el estado de los flujos en los *hosts* y enrutadores a lo largo de su camino.

El protocolo de establecimiento de reservación de recursos, juega un papel importante en los servicios integrados, por eso describiremos a continuación al protocolo RSVP en Int-Serv.

3.3.1.1. Protocolo de reserva de recursos (RSVP)

Los servicios integrados están basados en el protocolo RSVP (RFC 1633). Éste realiza una reserva de recursos en la red para cada flujo de información del usuario, también conocido como estado de reservación. Así, durante el mantenimiento del núcleo de la red, se hace un mantenimiento de la "reservación de recursos" (tablas de estados de reserva). Esto conduce a un considerable tráfico de señalización y ocupación de recursos en cada enrutador para cada flujo, con la consiguiente complejidad en el hardware, al margen del aporte que ésta señalización hace a la congestión de la red. No es una solución escalable, ni una solución adecuada para grandes entornos como Internet, aunque si lo es para entornos más limitados y también para redes de acceso al backbone.

RSVP es un protocolo señalización de QoS, y posibilita:

- Dar a las aplicaciones un modo uniforme para solicitar determinando nivel de QoS.
- Encontrar una forma de garantizar cierto nivel de QoS.
- Proveer autentificación.

RSVP es un protocolo que realiza sus funciones entre los usuarios y la red, y entre los diferentes nodos (enrutadores) que soportan éste protocolo. Consiste en hacer reservas de recursos en dichos nodos para cada flujo de información de usuario, con la consecuente ocupación de los mismos. Esto requiere, lógicamente, intercambio de mensajes RSVP entre dichos entes funcionales, así como administrar estados de reserva en cada nodo RSVP. De manera que tanto la solicitud de las reservas, como el mantenimiento de éstas durante la comunicación, y su posterior cancelación implica el intercambio de mensajes de señalización, lo que representa un tráfico considerable en entornos como Internet.

RSVP asume que existen recursos reservados para cada flujo de tráfico con ciertos requerimientos de QoS en cada uno de los dispositivos intermedios de la red, estableciendo una señalización punto a punto.

Se definen dos tipos de niveles de calidad, además del mejor esfuerzo en los servicios diferenciados:

- *Garantizado.* (RFC 2212), que asegura a las aplicaciones un tiempo máximo garantizado de transmisión de extremo a extremo y que no se producirán pérdidas por congestión, mientras el tráfico se mantenga dentro de las especificaciones, es decir, se basa en solicitar determinado ancho de banda y cierto retardo máximo para la transmisión.

- *Carga Controlada.* (RFC 2211), un poco más allá del "mejor esfuerzo", pero en una red con poca congestión. Aunque no está muy bien definido, se entiende en general que la pérdida de paquetes debe ser muy baja o nula.

De los dos tipos de servicios que RSVP soporta, el más adecuado para aplicaciones con requerimientos de tiempo real es el servicio garantizado, aunque es más complejo de implementar.

RSVP define dos sentidos para la transferencia de sus mensajes de señalización: *downstream y upstream.* El flujo *downstream* se efectúa desde la fuente al receptor o receptores, y el flujo *upstream* en sentido contrario.

Existen dos mensajes básicos del protocolo RSVP, son: *PATH y RESV.* Son en definitiva los mensajes a través de los cuales se lleva a cabo la reserva de recursos en la red previa la transmisión de información.

Los mensajes *PATH* son generados por la fuente de mensajes de usuario que necesitan la garantía de QoS, e indican las características de los recursos que necesita. La ruta que deben seguir éstos mensajes es la misma que siguen los datos de usuario, para lo cual se requiere previamente un diálogo entre el proceso RSVP y el proceso de enrutamiento, dicha ruta es determinada por el protocolo de enrutamiento, de lo contrario de nada serviría RSVP.

En su paso por cada enrutador RSVP, los mensajes *PATH* se actualizan y se retransmiten, esto consiste en poner la dirección IP del enrutador que lo actualiza y retransmitir el mensaje. Cada enrutador RSVP también almacena la dirección del enrutador anterior. Así, con los mensajes *PATH,* es posible indicar al receptor ó receptores, no sólo las características del tráfico de usuario, sino también la ruta por donde debe solicitar las correspondientes reservas de recursos. Los enrutadores que no soporten RSVP transfieren transparentemente los mensajes *PATH.*

Los mensajes *RESV* son producidos por el receptor ó receptores de los flujos de información de usuario, como respuesta a los mensajes *PATH,* y solicitan a la red (a los enrutadores RSVP) la correspondiente reservación de recursos para soportar la comunicación con cierta QoS, viajando hasta la fuente de datos del usuario, en sentido upstream. Con la información de ruta que suministran previamente los mensajes *PATH,* los mensajes *RESV* dirigen las solicitudes de reservas a los enrutadores RSVP apropiados, esto es, por dónde fluirán los datos.

Los mensajes *RESV* especifican el ancho de banda mínimo que se requiere para obtener determinada demora en un flujo de datos específico. Además, es posible efectuar reservaciones compartidas, esto es, una misma reservación aplicable a varios flujos de datos de usuario. Éstas reservaciones de recursos en los enrutadores RSVP de la red se materializan mediante *soft-states* en dichos enrutadores, estos son estados que se requieren para abastecerse de actualizaciones periódicas, por lo que durante toda la comunicación se necesita la señalización para mantener las reservaciones previamente efectuadas. Esto conlleva, en consecuencia, a cierta señalización permanente durante la fase de transferencia de información, con la consiguiente carga de tráfico.

Vale la pena decir también que la reservación de recursos extremo a extremo que posibilita RSVP será válida sólo si la congestión y demora que introduzcan los enrutadores que no usan RSVP no sea significativa.

Otros mensajes del protocolo RSVP son:

PATHTEAR: son mensajes generados por la fuente de datos de usuario para eliminar la información de los mensajes PATH los enrutadores RSVP. Siguen la misma ruta que los mensajes PATH´s. También pueden ser originados por cualquier nodo cuando se agota el tiempo de vida de un mensaje PATH.

RESVTEAR: son generados por los receptores para borrar los estados de reserva en los enrutadores RSVP, por tanto viajan en el sentido *upstream.* Pueden ser también originados por nodos RSVP al agotarse el tiempo de vida del estado de reserva de los mismos.

PATHERR: viajan en sentido *upstream* hacia el emisor siguiendo la misma ruta que los mensajes PATH´s, y notifican errores en el procesamiento de estos mensajes, pero no modifican el estado del nodo por donde ellos pasan hacia la aplicación emisora.

RESVERR: notifican errores en el procesamiento de mensajes RESV o la interrupción de una reserva. Se transfieren en dirección *downstream* hacia el receptor o receptores apropiados.

3.3.1.1.1. Funcionamiento básico.

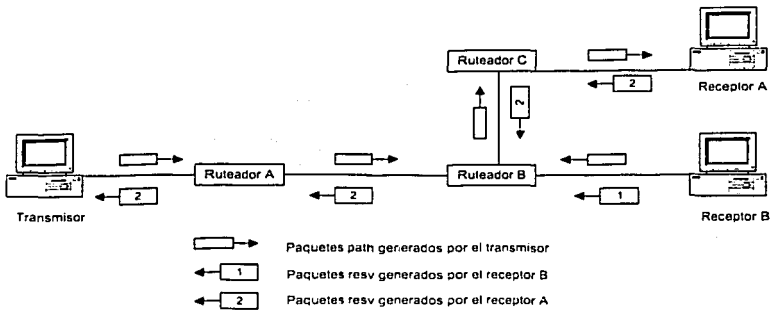


Fig. 3.2. Funcionamiento de RSVP

En la figura 3.2 se muestra de forma simplificada el intercambio de mensajes RSVP, específicamente mensajes PATH y RESV entre un transmisor y dos receptores (A y B), indicándose que la reservación representada por el mensaje RESV2 prevalece sobre la reservación representada por el mensaje RESV1, de manera que esto sugiere que la reservación solicitada por el receptor A es mayor que la solicitada por el receptor B. Esto es, la reservación "mayor" prevalece sobre la "menor", así el enrutador B sólo solicita al A la mayor de las dos solicitudes de reservación a él llegadas desde el enrutador C (originada por A) y desde el receptor B. Esto es una característica de RSVP.

Éstas solicitudes de reservación conducen a que en cada enrutador RSVP se establezca un estado *Soft-state*, es decir, una reserva en cada enrutador con un determinado tiempo de vida, que debe ser actualizada periódicamente por los receptores, de lo contrario vence el tiempo de vida y se deshace la correspondiente reservación, con la consecuente generación de un mensaje RESVTEAR.

La liberación de reservas mediante RSVP se puede llevar a cabo de diferentes maneras, así la solicitud para dar baja a determinada reserva puede ser originada:

- Por el emisor
- Por el receptor
- Por un nodo de red

Cuando la solicitud de liberación es del emisor ó receptor es porque la aplicación así lo decide, en cuyo caso se produce un mensaje PATHTEAR ó RESVTEAR respectivamente. Por parte de un nodo se lleva a cabo cuando vence el tiempo de vida correspondiente del estado PATH o del estado de reserva, lo que origina la emisión de un mensaje PATHTEAR o un mensaje RESVTEAR.

Para poder llevar a cabo la tarea de priorizar los recursos para un servicio y/o usuario en específico, la red debe saber qué cantidad de ancho de banda está disponible para cada uno de ellos. Una vez conociendo esto, para los enrutadores no es problema el reservar dichos recursos. Para esto la aplicación en si debe notificar desde el principio de la transmisión los recursos que va a consumir. También se deben notificar los espacios de tiempo en la cual los recursos reservados no van a ser utilizados por dicha aplicación.

Por otro lado, como ya lo hemos mencionado, una arquitectura de Calidad de Servicio es tan fuerte como su punto más débil. De lo anterior, si la aplicación notifica a la red los recursos necesarios para llevar a cabo la transmisión, y algún punto de la red no es capaz de soportar dicha carga, entonces el requerimiento es denegado y no se pierde tiempo en intentos infructuosos.

En resumen, RSVP se basa en dos conceptos básicos: los flujos de tráfico y las reservaciones. El primer concepto es importante ya que los recursos son reservados para determinado tipo de tráfico. Estos son identificados por RSVP en la red por la dirección IP destino.

3.3.1.1.2. Encabezado RSVP.

Para IPv6, RSVP es un protocolo de control como ICMP, de tal manera que coloca sus mensajes en el relleno de los datagramas IP, utilizando el campo: *próximo encabezado (next header)* con el valor de 46 que corresponde a RSVP. En cambio en IPv4 los encabezados son transportados en datagramas UDP, ya que IPv4 no puede transportar éste protocolo directamente en los datagramas IP. Cada mensaje RSVP comienza con un encabezado común. Como muestra la figura 3.3.

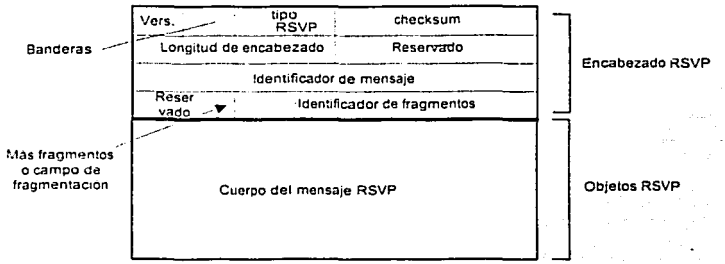


Fig. 3.3. Encabezado RSVP

El encabezado contiene ocho campos definidos, más dos áreas reservadas. A continuación describimos los campos:

- Versión. Campo de 4 bits que indica la versión del protocolo RSVP (actualmente es la versión 2).
- Banderas. Campo de 4 bits. No existen banderas definidas actualmente.

- Tipo. Campo de 8 bits, identifica el tipo de mensaje RSVP con 6 posibles valores, los mensajes PATH y RESV. RSVP define mensajes de error en respuesta a los dos anteriores, y también mensajes para terminar de manera explícita un camino o reservación. La tabla 3.3. nos muestra los tipos de mensajes:

Valor	Tipo de mensaje
1	Mensaje PATH
2	Mensaje de RESV (petición)
3	Respuesta de error a PATH
4	Mensaje de error a RESV
5	Finalización de camino
6	Finalización de reserva

Tabla 3.3. Tipo de mensajes.

- Checksum. Campo de 16 bits, contiene el cálculo que se realiza para proteger al mensaje, es decir, evitar que el mensaje RSVP sea dañado durante su transmisión.

- Longitud de encabezado. Campo de 16 bits, que contiene la longitud del paquete RSVP en bytes.

- Mas fragmentos ó campo de fragmentación, si este campo está activo o el identificador de fragmentos contiene un valor diferente de cero, entonces la longitud será solamente la del fragmento. Esto sucede cuando el paquete es sólo un fragmento de un mensaje completo.

- Identificación del mensaje. Campo de 32 bits, es una etiqueta compartida entre los fragmentos que forman un mensaje, permitiendo que pueda determinarse que fragmentos pertenecen a un mismo mensaje para unirlos apropiadamente.

- Identificador de fragmentos. Campo de 24 bits, que indica al receptor a que parte del mensaje original pertenece el fragmento.

El resto de los mensajes RSVP consiste en una serie de objetos. Estos objetos son el cuerpo del mensaje como observamos en la figura 3.3. Cada objeto tiene el mismo formato básico:

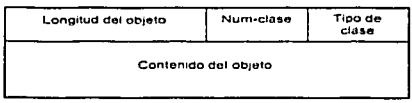


Fig. 3.4. Formato de los objetos RSVP

- Longitud del objeto. Campo de 16 bits que indica el tamaño del objeto.

- Num-clase. Campo de 8 bits, identifica al objeto.

- Tipo de clase. Campo de 8 bits, identifica el tipo de objeto. En combinación el Num-clase y tipo de clase pueden ser usados como un número único para cada objeto.

3.3.2. Servicios Diferenciados. (*DIFF–SERV)*

La arquitectura de Servicios Diferenciados definida en el RFC 2475, está basada en un modelo simple donde el tráfico entra a la red, es clasificado y posiblemente condicionado en los bordes de la red, después es asignado a diferentes conjuntos de comportamientos. Cada conjunto es identificado por un código DS único definido en el encabezado del datagrama. Dentro del *núcleo* de la red, los paquetes son direccionados de acuerdo al comportamiento (PHB, *per-hop behavior*) asociado con el código DS.

El funcionamiento de la arquitectura *Diff-serv* se basa en poner una marca en los paquetes IP, la cual determinará el trato que se les dará a estos en la red, esto es, se aplicando un trato diferente en los enrutadores. Se definen y utilizan diferentes tipos de enrutadores. La diferencia que hace *Diff-Serv* no es la misma en todos los nodos, sino depende de si se trata de un nodo interior ó un nodo frontera. A diferencia de *Int-Serv* basada en RSVP, la red con nodos *Diff-Serv* no establece ni mantiene estados de las conexiones por flujos de paquetes. Es una solución escalable, más apropiada para grandes entornos como Internet. Puede ser fácilmente implementada en las redes IPv4 existentes.

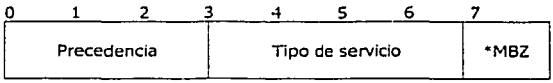
En Ipv6 se contempla este marcado de paquetes, mediante el campo DS, de ocho bits que aparece en el encabezado IP. En la figura 3.5. se muestra el formato del paquete IPV6.

Bit versión 6	Byte Servicio Diferenciado	Etiqueta de flujo 20 bits
Longitud total payload 16 bits	Próximo salto 8 bits	Encabezado salto 8 bits
Dirección IP origen 128 bits		
Dirección IP destino 128 bits		
Próximos encabezados (si hay) longitud variable		
Datos longitud variable		

Fig. 3.5. Formato del paquete Ipv6

3.3.2.1. Definición del campo DS.

Se ha definido al campo DS que reemplaza al campo ToS del encabezado de IPv4 y al TCO. Los bits del campo ToS según el RFC 1349 están definidos en la figura 3.6:



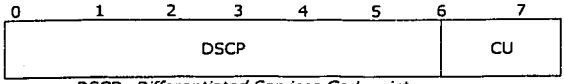
Precedencia	ToS
111 Control de red	1000 Minimizar retardo
110 Control de enrutamiento	0100 Maximizar caudal
101 Crítico	0010 Maximizar fiabilidad
100 Muy urgente	0001 Minimizar coste
011 Urgente	0000 Servicio normal
010 Inmediato	
001 Prioridad	
000 Rutina	

* MBZ. Bit que debe ser cero.

Fig. 3.6. Formato del paquete campo ToS.

Los bits del campo DS están definidos de la siguiente manera:

- Seis bits del campo DS son usados como códigos denominados DSCP (DS *Codepoint*), para seleccionar el comportamiento que tendrán los paquetes en cada nodo (PHB).
- Dos bits del campo DS que actualmente no se utilizan, llamados CU (*Currently Unused*) están reservados para usos futuros. El valor del subcampo es ignorado por los nodos que manejan Servicios Diferenciados cuando se determina el PHB a aplicar en el paquete recibido.



DSCP: *Differentiated Services Codepoint*
CU: *Currently Unused*
Fig. 3.7. Campo DS.

Como sé mencionó en líneas anteriores también en IPv4 se permite dicho marcado de paquetes, a través del campo TOS, y se utilizará como DS.

3.3.2.2. Comportamiento por salto (PHB).

Básicamente, un PHB es una descripción del comportamiento de un conjunto de paquetes denominado Agregado de Comportamiento (*Behavior Agregate, BA*). Los BAs son conjuntos de paquetes marcados con un mismo DSCP y enviados en la misma dirección, pudiendo pertenecer a un mismo agregado de paquetes procedentes de múltiples fuentes o aplicaciones.

Se han estandarizado 4 tipos de PHBs.

- Por defecto (RFC 2472), es equivalente al mejor esfuerzo, y debe estar disponible en todos los nodos DS.
- Selector de clase (RFC 2474), comportamiento compatible con los bits del campo ToS de IPv4. En este tipo de servicio se agregan y clasifican en clases a los que se proporciona una garantía de transmisión relativa. Cuando aumenta el nivel de congestión, el tráfico de una cierta clase experimenta unas pérdidas menores que el tráfico de una clase inferior. Además, el tráfico de prioridad más alta experimenta menos retardos por encolamiento que el tráfico de menor prioridad.
- Reenvío expedito (*Expedited Forwarding*, EF, RFC 2598): Equivale a un circuito dedicado virtual, por lo que se garantiza cierto ancho de banda y servicios con pérdidas, latencia y variación de retardo de valores bajos; cuando el tráfico excede el perfil establecido (por políticas locales), éste es descartado. Tiene un solo valor de DS.
- Reenvío asegurado (*Assured Forwarding*, AF, RFC2597): Los paquetes se etiquetan con "alta prioridad", aunque no se garantiza el ancho de banda. Brinda una Calidad de Servicio superior a la ofrecida tradicional best-effort de Internet. Brinda cuatro clases de servicios, cada una con tres niveles diferentes de descartación de paquetes. En total se manejan doce códigos.

Un nodo DS es, en principio, una combinación de cuatro módulos funcionales, aunque no todo enrutador DS contiene la totalidad de éstos:

1. Clasificador de tráfico: distingue los paquetes en base a uno ó varios campos de su encabezado: dirección fuente, dirección destino, campo DS.
2. Medidor de tráfico (*Traffic Meter*): valora las propiedades temporales de un flujo de tráfico, seleccionado por el clasificador.
3. Marcador de paquetes (*Packet Marker*): establece el código del campo DS, es decir, el DSCP para los paquetes enviados.
4. Conformadores y descartadores (*shapers and droppers*): Al conformar se establece cierta demora para uno ó más paquetes de un flujo para que estén conforme al perfil de tráfico. Algunos paquetes pueden descartarse, para mantener el perfil de tráfico.

La figura 3.8. muestra la representación lógica de los módulos en un nodo DS:

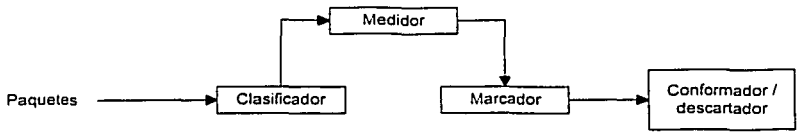


Fig. 3.8 Representación lógica de los módulos en un nodo DS.

En la versión IPv4 se marcan dentro del campo ToS cuatro tipos de servicios:

- Costo mínimo (ancho de banda).
- Máxima confiabilidad.
- Máxima eficiencia del canal.
- Mínimo retardo.

Sin embargo, este campo prácticamente no ha sido utilizado, pues los enrutadores no procesaban esa información; además, se empleaban con igual resultado los bits de prioridad. No obstante, es una posibilidad de tener diferentes grados de QoS en IPv4, y puede emplearse como campo DS en redes *Diff-Serv*.

Int-Serv como *Diff-serv* están basados en modelos complementarios, en *Diff-Serv* la QoS es controlada por el emisor y en *Int-Serv* la QoS se controla por el receptor.

La arquitectura *Diff-Serv* minimiza la señalización agregando información, en general a los encabezados, definiendo una serie de clases de tráfico.

Antes de poder hacer la implementación, existen una serie de requerimientos que se necesitan cumplir dentro de la red.

1. Se debe de tener un conjunto de códigos para el campo DS que cumplan con los estándares establecidos.
2. Descripciones cuantitativas de los atributos para el funcionamiento de las clases de servicios.
3. Mecanismos para agregar de forma eficiente todas las fuentes generadoras de tráfico privilegiado que converjan dentro de los dispositivos internos de la red.
4. Contar con una solución viable a la liberación de tráfico definido en los acuerdos de nivel de servicios, SLAs.
5. Encontrar las mejores herramientas de administración para facilitar los posibles desarrollos y su operación.

Los primeros dos puntos pueden parecer no tan críticos, ya que pueden ser definidos de acuerdo a las características propias de cada red, de manera que se optimice el funcionamiento de acuerdo a la cantidad de tipos de tráfico que se manejen.

Sin embargo, el esquema que parece más prometedor, tanto en términos de estandarización como de escalabilidad, es el que ofrece MPLS.

3.3.2.3. Dominios de QoS.

Un dominio de QoS es aquella red que tiene un intervalo de direcciones válidas de Internet la cual tiene la capacidad de manejar calidad de servicio entre sus nodos y tiene definido un plan de políticas de QoS basado en la diferenciación de tráfico o servicios. Además tiene la capacidad de comunicarse y llevar acuerdos de QoS con otros dominios, como se expresa en la figura 3.9.

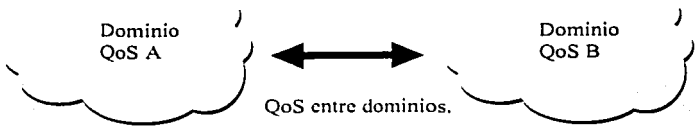


Fig. 3.9 Dominios de Calidad de Servicios

3.3.3. Conmutación por Etiquetamiento de Multiprotocolos. (MPLS)

MPLS es una técnica que utilizan los enrutadores para realizar el enrutamiento de una forma más dinámica y rápida con respecto a la de un enrutamiento IP tradicional. Sin embargo, MPLS no es una técnica para reemplazar a los de enrutamiento operantes, sino que trabajarán de forma complementaria.

MPLS trabaja de forma similar a *Diff-Serv* en el aspecto de que también etiqueta al tráfico que ingresa a la red, así como lo des-etiqueta cuando sale. Sin embargo, las etiquetas de MPLS (20 bits) se asignan para referenciar el siguiente salto dentro de la red. MPLS no es controlado a nivel aplicación, sino que reside únicamente en los enrutadores, además de trabajar independientemente de protocolos ya sea de ruteo o bien de otras capas de aplicación, ya que puede trabajar tanto con IP o IPX, o bien con PPP, ATM o Frame Relay. Por esto, más que ser una técnica para QoS, es una técnica para manejo y distribución de tráfico, mejor conocidas como Ingeniería de Tráfico.

El tipo de ruteo que realiza MPLS es parecido a los circuitos virtuales que utiliza ATM, estableciendo túneles con ancho de banda específico, denominados túneles LSP (*Labeled Switches Path*); sin embargo, a esto se le puede agregar la capacidad de servicios que se puede obtener mediante la estandarización de políticas bien establecidas.

Los dispositivos que manejan el ruteo de datos mediante esta técnica se les denomina LSR (Enrutador de Conmutación de Etiquetas, *Label Switching Router*). Cuando los datos salen del

host emisor al enrutador de ingreso dentro de una red MPLS, éste toma la decisión de hacia dónde serán dirigidos los datos en el próximo salto, esto basado en la dirección destino. Es entonces cuando se determina algún valor apropiado para la etiqueta (en la que se identifica la Clase Equivalente de Direccionamiento, *FEC*). Una FEC es un grupo de paquetes IP que son direccionados en una misma forma. Ésta etiqueta es agregada al paquete y es direccionada al siguiente LSR. Éste enrutador utiliza la etiqueta como un índice que especifica el siguiente salto y, por ende, el valor de la nueva etiqueta. Ésta es una enorme ventaja, ya que si la ruta es determinada por etiquetas, se baja la carga del procesador en el enrutador, sirviendo éste como un *switch*, no teniendo que revisar los encabezados completos evitando procesar tantas direcciones. La cuestión importante aquí es entonces, el establecimiento de reglas y políticas para la elaboración y asignación de las etiquetas.

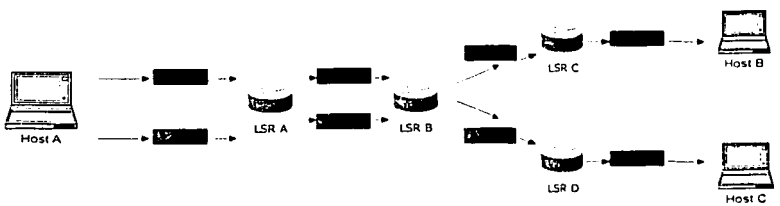


Fig. 3.10. Conmutación por etiquetamiento de protocolos.

Debido a que la pareja conformada entre una etiqueta y el LSR correspondiente es fija, la ruta que toma el paquete etiquetado sobre la red, una LSP, es configurada desde que el enrutador de ingreso etiqueta el primer salto, es por eso que desde ese momento se sabe el túnel LSP que se va a utilizar.

El encabezado de encapsulamiento del protocolo MPLS consta de 32 bits distribuidos de la siguiente forma:

0 .....19 20.....22 23 24 31

Etiqueta MPLS (20 bits)	*EXP.* (3 bits)	S b	Tiempo de vida (8 bits)

Fig. 3.11. Encabezado de encapsulamiento donde se encuentra la etiqueta MPLS en la que se encuentra el encabezado IP.

Como se ve el formato de la figura 3.11. , existen 2 campos además de la etiqueta que juegan un papel importante dentro de este proceso. El campo EXP de 3 bits nos determina el tipo de comportamiento que tendrá el flujo de paquetes de acuerdo a la clase de servicio (8 diferentes combinaciones) que definen los PHBs. Existe un bit S (*Stack*) el cual nos dice si esta entidad de encapsulamiento es la única, o bien, está apilada dentro de varias entidades. Esto nos sirve para definir rutas alternas dentro de las rutas originales.

Además, como en IP, existe un campo que enmarca el tiempo de vida, el cual es un contador que se irá decrementando en cada salto dentro de la ruta tomada, permitiendo que nuestro paquete no caiga en *loops* y viaje para siempre dentro de la red.

Una vez que la etiqueta ha definido cual es el siguiente salto, se define lo que se conoce como el NHLFE (*Next Hop Label Forwarding Entry*) que nos define dónde se llevará a cabo el siguiente salto.

3.3.3.1. Configuración de túneles LSP's.

La conmutación de paquetes consiste de dos componentes:

- Protocolos de enrutamiento convencionales:
  - Se mapea de FECs a NHLFEs, lo que se conoce como un mapeo FTN.
- Encadenamiento y distribución de etiquetas.
  - Se mapea de etiquetas a NHLFEs, lo que se conoce como mapeo ILM.

De esto podemos decir que el FTN direcciona paquetes sin etiquetas y el ILM direcciona paquetes etiquetados. Estos son configurados en cada LSR por el administrador antes de la distribución de etiquetas y de la configuración de LSPs.

Una de las características de MPLS es que una vez que las etiquetas necesarias para llevar a cabo una LSP ya se intercambiaron entre los LSRs de los extremos (LER, *Label Edge Router)*, los LSRs intermedios del LSP no tienen que examinar el contenido de los paquetes sino únicamente la etiqueta correspondiente a cada salto. De esta manera se construyen *túneles* que permiten el flujo de tráfico de un extremo al otro de la ruta, sin que la información pierda en su integridad.

Existen varias opciones para controlar como se van configurando las diferentes LSP's:

- En la asignación de etiquetas salto a salto (*Hop by Hop*) la configuración de la LSP se va realizando de acuerdo al siguiente salto, conforme al sistema de ruteo que se esté utilizando. La configuración de la LSP puede ser inicializada con las actualizaciones de la tabla de ruteo o bien, dinámicamente en respuesta al flujo de tráfico determinado.

- En la asignación de etiquetas no solicitadas en el envío (*Downstream Unsolicited*), el LSR de salida distribuye las etiquetas a ser utilizadas para llegar a un host en particular. El detonante de esto será la información nueva de ruteo recibida en el LSR de salida.

- Una vez que las LSPs han sido establecidas sobre la red, éstas pueden ser usadas para configurar nuevas rutas que vayan siendo disponibles. Así, como los protocolos de ruteo distribuyen actualizaciones de información de ruteo, también pueden indicar que etiqueta puede ser utilizada para alcanzar ciertas rutas establecidas.

- Si un LSR de ingreso quiere configurar una LSP que no corresponde con el siguiente salto de la ruta, este debe usar un protocolo de distribución que permita la especificación de Rutas Explícitas (*Explicit Routes, ER*), el cual requiere distribución de etiquetas bajo demanda.

- Si además un LSR de ingreso requiere configurar una LSP que dé cierto grado de servicio de manera que se reserven recursos en los LSRs intermedios de la LSP. Para esto, la LSP estará restringida a la disponibilidad de recursos de la LSP y a la habilidad que tengan los dispositivos intermedios para llenar los requerimientos de calidad de servicio.

Una Ruta Explícita, ER, es una secuencia precisa de pasos a llevar desde el ingreso hasta la salida de la información dentro de la red. Sin embargo, ésta puede ser restrictiva completamente dando los saltos específicos para llenar una LSP completa, o bien, puede ser más libre y dar estos

mismos saltos específicos y agregar saltos adicionales para completar cierta ruta. Sin embargo, una ER restrictiva nos puede ayudar a definir la LSP que satisfaga nuestros requerimientos de calidad de servicio y realizar así una reservación de recursos apropiada.

Para que MPLS pueda ayudar al enrutamiento de paquetes dentro de la red, todos los LSR deben tener las misma políticas dependiendo de las interfaces de las cuales llegan ó a las cuales van, asignándoles una etiqueta a cada una de ellas. Al proceso de tener las mismas políticas que relacionen las interfaces de entrada/salida con cada etiqueta en cada LSR se le denomina Distribución de Etiquetas. La manera en que estas se distribuyen varía dependiendo de la combinación de hardware que se tenga, así como los alcances necesarios dependiendo de la orientación de servicios a dar. Con esto, se pueden elegir de varias opciones de protocolos para realizar esta tarea, de los cuales existen 2 protocolos que sobresalen de los demás. Estos son el RSVP y el CBR-LDP (*Constraint-based Routed Label Distribution Protocol*), que es una extensión del LDP original.

CBR-LDP fue diseñado específicamente para facilitar el manejo de las LSP´s basadas en ER restrictivo. Utiliza sesiones de TCP entre LSR's y envía mensajes de distribución de etiquetas durante éstas.

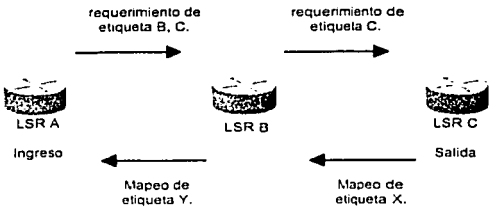


Fig. 3.12. Flujo de configuración de una LSP por medio CBR-LDP

De la figura 3.12, se tiene al LSR de ingreso que determina si se necesita una nueva LSP para llegar al LSR de salida. Los parámetros de tráfico y las políticas establecidas determinan los LSRs intermedios para completar la LSP, que podrían no ser necesariamente los LSR establecidos en un salto a salto (*H by H*). Entonces, el LSR A construye un mensaje de requerimiento de etiqueta en donde incluye la ER a ser utilizada (LSR B y C) y detalles del tráfico a ser cursado para reservar recursos por medio de una sesión TCP. El LSR B recibe éste mensaje, determina que él mismo no es un LSR de salida para esta LSP, y reenvía el requerimiento por la ruta señalada, reservando antes los recursos requeridos en la LSP, y modificando la ER eliminándose de la misma (quedando LSR C únicamente). Al llegar el mensaje al LSR C, éste determina que es el LSR de salida de la LSP, realiza las negociaciones finales de recursos y hace las reservaciones de estos para la LSP. El LSR C envía un mensaje de mapeo de etiqueta de regreso con una etiqueta agregada para la nueva LSP que contiene los detalles de parámetros de tráfico reservados para la misma. Este nuevo mensaje llega al LSR B que confirma que es la respuesta al requerimiento enviado anteriormente con el LSP ID que está contenido en ambos mensajes. Éste finaliza su reservación de recursos, agrega una etiqueta para la LSP y reenvía el mensaje de mapeo al LSR A. Al llegar a este, se hace la reservación final de recursos y la LSP termina de ser configurada.

Por otro lado, RSVP genérico utiliza un intercambio de mensajes para reservar recursos en la red a través de los flujos de información IP. Las extensiones de RSVP para túneles LSP aumenta las propiedades del RSVP genérico para ser utilizado como distribuidor de etiquetas. Este utiliza los

datagramas IP para comunicarse entre LSRs, y no requiere mantener sesiones de TCP, pero esto lo obliga a manejar las pérdidas de mensajes de control.

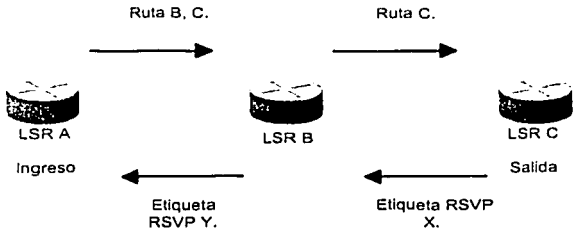


Fig. 3.13. Flujo de configuración de una LSP por medio de RSVP.

Al igual que en el caso anterior, en la figura 3.13, el LSR de ingreso determina la necesidad de una LSP hacía un LSR de salida. Determina los LSR's intermedios que no son necesariamente los mismos utilizados en un HbH. Entonces el LSR A construye un mensaje de requerimiento de ruta con una ER (para los LSR's B y C) y los detalles de tráfico. Este mensaje se envía al LSR B en un datagrama IP. El LSR B lo recibe, determina que él mismo no es un LSR de salida de ésta LSP, reenvía entonces el mensaje al LSR C modificando solamente la ER. Al llegar al LSR C, éste verifica que es el LSR de salida de esta LSP, determina por medio de los parámetros de tráfico en el mensaje el ancho de banda que se requiere reservar y los recursos requeridos. Selecciona una etiqueta para la nueva LSP y la distribuye al LSR B en un mensaje *RESV*, que además contiene los detalles de las reservaciones de recursos requeridas para dicha LSP. El LSR B recibe este mensaje y comprueba la LSP ID contenida en ambos mensajes. Determina los recursos necesarios a reservar y agrega una etiqueta al mensaje, reenviándolo al LSR A en un nuevo mensaje *RESV*. Este llega al LSR de ingreso, se determina la reservación de recursos final y la LSP ha sido configurada.

3.3.3.2. Distribución de etiquetas.

Como ya lo hemos mencionado, una de las características básicas de una red MPLS es el que todos los LSR's involucrados sepan qué etiquetas utilizar en cada interfaz para la configuración de las LSP en el envío de paquetes.

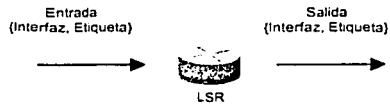


Fig. 3.14 LSR de Intercambio de Etiquetas

Esto se hace si todos los LSR's comparten las mismas tablas de etiquetas referenciadas a alguna interfaz. Esto es realizado mediante la distribución de etiquetas que se tengan del primer LSR que se haya configurado o bien de alguna modificación en algún LSR. Existen varios protocolos

para la distribución de etiquetas, sin embargo son dos los que hasta ahora han tenido mayor aceptación son el Protocolo de Distribución de Etiquetas (*LDP, Label Distribution Protocol*) con su variante de ruteo basado en restricciones (*CBR-LDP, Constraint-Based Routing LDP*) y el ya mencionado RSVP. Cabe mencionar que las etiquetas son siempre asignadas en el sentido destino - fuente (*downstream*).

3.3.3.2.1. Protocolo de Distribución de Etiquetas LDP.

En el capítulo de MPLS elaborado por la IETF se especifica como solución para la distribución de etiquetas el protocolo LDP, pero como hemos mencionado, no es de uso obligatorio ni estandarizado.

Se han definido cuatro categorías de mensajes LDP:

- **Descubrimiento.** Son los utilizados para anunciar y mantener la presencia de los LSRs en la red.
- **Sesión.** Son utilizados para establecer, mantener y terminar las sesiones LDP.
- **Anuncio.** Se utilizan para crear, modificar y borrar las asignaciones de etiquetas a los FEC. Son los que se utilizan para las operaciones relacionadas con la gestión de etiquetas entre LSRs.
- **Notificación.** Transportan información correspondiente a señales de error y suministran información de aviso.

El intercambio de mensajes entre dos LSRs se hace mediante el envío de PDUs (*Protocol Data Unit*) de tipo LDP, basándose en la utilización de sesiones LDP sobre conexiones TCP. Cada PDU de LDP puede transportar más de un mensaje LDP independientes entre sí.

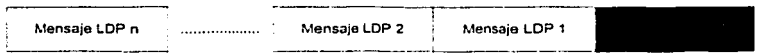


Fig. 3.15 Formato de los PDU de LDP

La cabecera de los PDU contiene la siguiente información.

- **Versión.** Dos octetos con la versión del protocolo.
- **Longitud de la PDU.** Dos octetos con la longitud total.
- **Identificador de LDP.** Seis octetos. Los primeros cuatro identifican al LSR, y los otros dos definen el espacio de direccionamiento del LSR.

El protocolo LDP utiliza el esquema de codificación TLV (Tipo-Longitud-Valor). Esto nos da la siguiente estructura del mensaje LDP:

- **U.** Un bit que le indica al LSR que recibe el mensaje, que hacer en caso de que éste le sea desconocido. Si está en cero, se le responde al LSR de origen, si es uno se sigue procesando la PDU.
- **F.** Campo de un bit que se utiliza si U=1. Si se recibe un mensaje desconocido que tenga que progresarse y F=0, este mensaje no se progresa al siguiente LSR. Si F=1 , si se hace.

- **Tipo.** Catorce bits que definen el tipo de mensaje y, por tanto, indica como debe ser interpretado el campo valor.

Los tipos de mensajes manejados son los siguientes:

- **LABEL REQUEST**
- **LABEL MAPPING**
- **LABEL ABORT REQUEST**
- **LABEL RELEASE**
- **LABEL WITHDRAW**
- **NOTIFICATION**

El tipo NOTIFICATION puede contener la siguiente información:

- **LABEL REQUEST ABORTED**
- **NO LABEL RESOURCES**
- **NO ROUTE**
- **LOOP DETECTED**
- **LABEL RESOURCES AVAILABLE**

- **Longitud.** Campo de dos octetos que especifica la longitud en octetos del campo *valor.*

- **Valor.** Campo de longitud variable que contiene la información del mensaje. La interpretación de la cadena de octetos de este campo depende del contenido del campo *tipo.*

3.3.3.2.2. Protocolo de Distribución de Etiquetas basado en restricciones de Ruteo. (CBR-LDP)

El enrutamiento basado en restricciones se basa en el cálculo de trayectorias sujetas a ciertas restricciones, como pueden ser en ancho de banda, requerimientos de QoS (retardo, *jitter,* etc.), etc. que sean definidos por el administrador de la red.

Debido a esto, el capítulo de MPLS de IETF ha elaborado extensiones necesarias para que el protocolo LDP pueda soportar el enrutamiento, llamado CBR-LDP, que ha sido definido para soportar el establecimiento y mantenimiento de LSP enrutados de forma explícita.

Estas extensiones incluyen los elementos de información necesarios para soportar el enrutamiento explícito y la modificación de los LSPs, pero no incluyen los algoritmos necesarios para computar los trayectos según criterios definidos por el administrador de la red. Por lo que las principales limitaciones que se tienen son las siguientes:

- Sólo se soportan LSP's punto a punto. El soporte punto a multipunto y multipunto a punto está en proceso.
- Sólo se soportan LSP's unidireccionales. El soporte bidireccional está en proceso.
- Sólo se soporta una etiqueta por LSP. El soporte a múltiples etiquetas por LSP está en proceso.

3.3.3.2.3. Extensiones para túneles LSP (RSVP).

Otra de las opciones actualmente consideradas para la distribución de etiquetas es el protocolo RSVP, pero la utilización de éste para la nueva función de distribución de etiquetas *MPLS* ha implicado la adición de nuevas capacidades a dicho protocolo.

Estas nuevas capacidades se refieren a los objetos, formato de los paquetes y procedimientos necesarios para establecer los túneles LSP. Se define como *Túnel LSP* a aquel LSP que es utilizado para transmitir por un túnel (*tunelizar*), el flujo de datos por debajo de los procedimientos normales de enrutamiento y/o filtrado *IP*.

Para el establecimiento de los túneles LSP, el protocolo de señalización usa el modelo conocido como *downstream on demand* para la distribución de etiquetas en un dominio MPLS. Esto significa que la petición de asociación entre un FEC y una etiqueta para crear un túnel LSP es iniciada por el LER de entrada. Para conseguir este objetivo es necesario añadir un nuevo objeto (*LABEL_REQUEST*) al mensaje de PATH, propio de RSVP antes mencionado.

Un requisito adicional para el protocolo RSVP, es que en un dominio MPLS se debe soportar el enrutamiento explícito (*explicit routing*) para facilitar la gestión del tráfico en un dominio MPLS. Para satisfacer esta exigencia es necesario añadir un objeto (*EXPLICIT_ROUTE*) en los mensajes de PATH. Este nuevo objeto encapsula el conjunto de nodos ordenados que constituyen la ruta explícita que debe seguir los datos.

Como la asignación de etiquetas se realiza desde el destino hacia el origen, en sentido contrario al flujo de datos, es necesario incrementar el mensaje RESV con un objeto adicional (*LABEL*) capaz de transportar la nueva información requerida para este uso del protocolo.

Ahora se está en condiciones de describir el funcionamiento del protocolo RSVP para el establecimiento de túneles LSP en un dominio con ayuda de la figura 3.16. En ésta, se observa un dominio MPLS con los distintos elementos que los componen (LER entrada, LSR's intermedios y LER de salida).

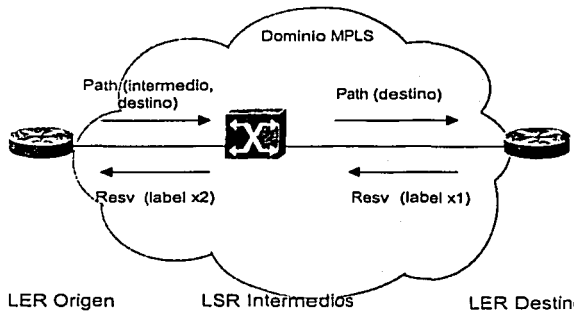


Fig. 3.16 Utilización de RSVP para túneles LSP

- Cuando un LER (que actúa como punto de entrada al *MPLS*) decide que necesita establecer un LSP hasta un determinado LER de salida del dominio, debe iniciar el procedimiento para establecerlo, mediante un mensaje PATH. La ruta que debe seguir el LSP puede ser una ruta explícita determinada por el administrador de la red (esta ruta puede no coincidir con la calculada por los algoritmos de enrutamiento de la capa de red, como ya vimos).

- Cuando los LSR intermedios reciben el mensaje de PATH, lo procesan de acuerdo con las especificaciones del protocolo, y una vez reconocido que no son el extremo del FEC, transmiten el mensaje hacia el siguiente nodo de la ruta.

- Cuando el mensaje de PATH finalmente alcanza el LER destino, éste procede a reservar los recursos internos necesarios, selecciona la etiqueta a utilizar para este túnel LSP y procede a propagarla hacia el anterior LSR mediante un mensaje de reserva (*RESV*).

- Cuando los LSRs intermedios reciben la asignación de la etiqueta con el mensaje *RESV* proceden a reservar los recursos internos necesarios y determinar la etiqueta a utilizar para el flujo. Una vez calculada, la propagan hacia el *LSR* anterior de nuevo con ayuda del mensaje *RESV*. Este proceso se repite hasta alcanzar el LER origen donde también se realiza el proceso de reservar los recursos internos, pero en éste caso no es necesario asignar etiqueta y propagarla ya que se ha alcanzado el origen del FEC.

3.3.4. Ingeniería de tráfico.

La ingeniería de tráfico se puede definir como el proceso de controlar los flujos de datos a través de la red. Es decir, el proceso de optimizar la utilización de los recursos disponibles por parte de los distintos flujos y por tanto, optimizar el uso global de los recursos y las prestaciones de la red.

Otra definición clarificadora de este mismo concepto es la que establece que la ingeniería de tráfico como "un proceso iterativo de planificación y optimización de red con el propósito de optimizar el uso de los recursos y las prestaciones de la red".

En un entorno de redes que utilizan IP como protocolo de capa de red, el enrutamiento de los paquetes se basa en los resultados de los algoritmos de enrutamiento (por ejemplo, *IGP*) y éstos suelen utilizar el criterio de escoger el camino más corto para decidir el camino que deben seguir los paquetes.

Este tipo de algoritmos, diseñados hace unos años, trataba de minimizar el uso de recursos de red escogiendo el camino más corto, pero éste criterio de selección puede producir congestión en algunos enlaces de la red (tradicionalmente este problema se resolvía aumentando la capacidad de los enlaces congestionados), mientras que otros enlaces pueden estar subutilizados.

Aunque en la literatura pueden encontrarse abundantes opiniones sobre la disminución del costo del ancho de banda (si el costo del ancho de banda tiende a cero, los operadores de red pueden ofrecer un ancho de banda muy superior a un costo muy bajo, lo que eliminaría, al menos en teoría, los problemas antes mencionados), la situación actual es que la gestión del tráfico sobre los recursos existentes sigue siendo una realidad para los administradores de red.

Esta realidad demuestra que, en una red IP de mediano a gran tamaño que utilice IGP, la gestión del tráfico es complicada por las siguientes razones:

- Teóricamente, desde una fuente todos los caminos con igual costo (*Equal Cost Multi-Path, ECMPs*) deben cursar el mismo tráfico. Debido a que la tasa de transmisión no puede ser cambiada, algunos caminos terminan cursando significativamente más tráfico que otros, debido a que transportan tráfico originado por otras fuentes (este tráfico adicional no ha sido considerado a la hora de estimar el costo del camino).

- El balanceo de carga no puede hacerse sobre caminos con costos diferentes.

- La modificación de las métricas utilizadas para calcular los caminos con IGP puede tener efectos colaterales indeseados sobre el resto del tráfico, y estos efectos no siempre son fácilmente previsibles.

Un ejemplo de los problemas anteriormente expuestos se muestra gráficamente en la figura 3.15.

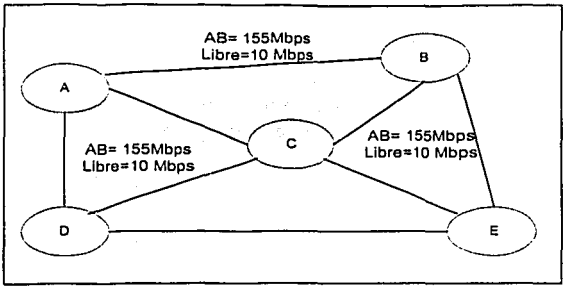


Figura 3.15. Enrutamiento tradicional y enrutamiento restringido

Se observa que el camino más corto entre A y B según la métrica normal IGP es el que tiene sólo un salto, pero puede que el exceso de tráfico sobre los enlaces ó la carga de los enrutadores hagan aconsejable la utilización de un camino alternativo (A-C-B) con dos saltos. Para resolver este tipo de problemas, MPLS es una herramienta efectiva para esta aplicación en grandes redes troncales, ya que:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.
- Permite realizar un enrutamiento restringido (*Constraint-Based Routing, CBR*), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales con distintos niveles de calidad (por ejemplo, garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.).
- El *Enrutamiento Basado en Restricciones (CBR)* puede computar las rutas sujetas a restricciones (ancho de banda disponible, restricciones administrativas, etc.); es decir, que éste tipo de soluciones consideran más datos que la estricta topología de la red para calcular el camino más conveniente.

En el ejemplo de la figura 3.15, aunque la ruta más corta es el camino directo entre A y B si, por ejemplo, el ancho de la banda disponible es de 10 Mbps y se quiere buscar un camino para cursar un tráfico de 20 Mbps, con el enrutamiento *CBR* existe la posibilidad de escoger la ruta A-C-B si en ella existe suficiente ancho de banda.

Como resumen puede afirmarse que para poder hacer la Ingeniería de Tráfico de forma efectiva en una red IP, el administrador de la misma debe disponer de mecanismos para controlar el camino que siguen los paquetes; es decir, debe ser capaz de establecer algún tipo de conexión o circuito en una red sin conexión.

3.3.5. Administración de Ancho de Banda en subredes (SBM).

Algunas tecnologías de capa 2 han sido diseñadas con capacidades para manejar QoS por si mismas como lo es ATM, sin embargo otras tecnologías LAN más comunes, como lo es Ethernet, no fueron diseñadas para hacer esto. La IEEE ha solucionado este problema en Ethernet y otras tecnologías de Capa 2 permitiendo el manejo de QoS mediante mecanismos de diferenciación de tráfico.

Los estándares IEEE 802.1p, 802.1Q y 802.1D definen como los switches Ethernet pueden clasificar las tramas a fin de apresurar la entrega de información. El grupo de trabajo Servicios Integrados sobre Capas de Enlaces Específicos, (*Integrated Services over Specific Link Layers ISSLL*) de la *IETF;* esta encargado de definir el mapeo entre los protocolos de QoS de las capas superiores y los servicios con estas tecnologías de Capa 2 como Ethernet. Entre otras cosas, esto ha resultado en el desarrollo de Administración de ancho de banda en subredes SBM para LAN´s tales como Ethernet, FDDI, Token Ring, etc.

SBM es un protocolo de señalización que permite la comunicación y la coordinación entre los nodos y los switches de la red en su marco de trabajo (SBM Framework) y permite el mapeo de los protocolos de QoS de las capas superiores (SBM Mapping).

Un requerimiento fundamental en el marco de trabajo de SBM es que todo el tráfico debe pasar a través de al menos un switch con SBM activo. Los principales componentes del sistema SBM son:

- Bandwidth Allocator (BA): Mantienen el estado acerca de la ubicación de los recursos de la subred y realiza el control de admisión de acuerdo a los recursos disponibles y otros criterios o políticas establecidas por el administrador.

- Requestor Module (RM): Éste reside en cada estación terminal y no en los switches. El RM hace un mapeo entre los niveles prioritarios de la Capa 2 y los parámetros del protocolo de QoS de las capas superiores de acuerdo con las políticas definidas por el administrador.

Como se ilustra en la figura 3.16 la localización del BA determina el tipo de la arquitectura de SBM en uso: Centralizada ó Distribuida. Si es solamente uno ó más BAs por segmento de red, solamente uno es el SBM Designado (DSBM Designed SBM).

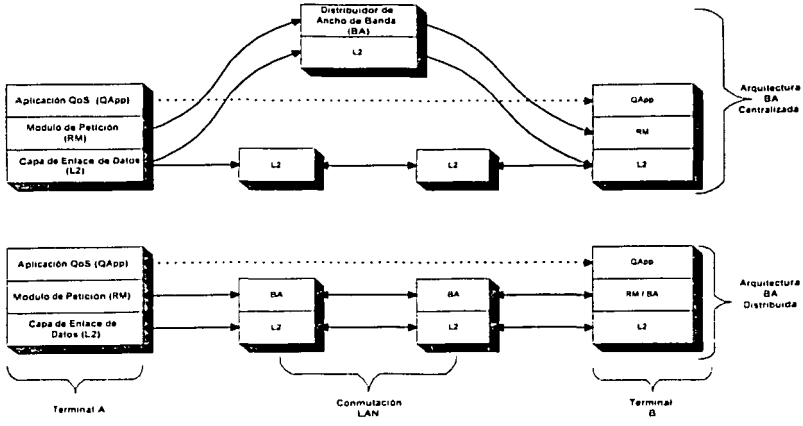


Fig. 3.16 Arquitectura SBM.

El protocolo SBM provee un mecanismo de señalización de RM a BA y de BA a BA para iniciar las reservaciones, encolando el BA en base a los recursos disponibles y cambiando o borrando las reservaciones. El protocolo SBM es también usado entre las aplicaciones de QoS activas y el RM, pero esto involucra el uso de una interfaz de programación mas que del protocolo. Aunque el protocolo SBM está diseñado para ser un protocolo de QoS independiente, este está designado a trabajar con otros protocolos de QoS.

3.3.6. IEEE 802.1Q/D/p.

El tema de la administración de redes de telecomunicaciones es bastante amplio e incluye temas relevantes como la Administración de Políticas, Ancho de Banda, la Calidad de Servicio o del Desempeño, todos ellos entrelazados e interdependientes; sin embargo, en este tema intentaremos concentrarnos en la Administración del Ancho de Banda y algunas de las técnicas o conceptos más comunes para introducirnos en el complejo mundo de la transmisión de datos optimizada.

Con las compuertas totalmente abiertas, oleadas de empleados y usuarios que accesan libremente a Internet, viendo conciertos, escuchando música en línea, "chateando", revisando los resultados deportivos ó simplemente analizando el comportamiento de sus acciones en la bolsa, tanto las empresas como los proveedores de servicios están haciendo uso de tiempo y ancho de banda apreciable. Y, ahora que la economía digital corre sobre el ancho de banda, tiene sentido pensar que los administradores se preocupen cada vez más de tener el control, y los fabricantes salgan al mercado con nuevas formas de permitir esa administración.

Los fabricantes de equipo generalmente ya ofrecen en sus productos alguna combinación de priorización, reservación de ancho de banda, encolamiento (*queueing*) por flujo o administración basada en políticas. Estos nuevos productos incluyen herramientas más precisas para dar

prioridad y optimizar la utilización de la red, así como controles que pueden residir del lado del Proveedor de Servicios ó del lado de la conexión a Internet, y que prometen al administrador mucho más control de su red para entregar múltiples niveles de calidad de servicio en las diversas aplicaciones.

La frase "ancho de banda administrado" hace referencia a la aplicación de técnicas de calidad de servicio de tal manera que diferentes tipos de tráfico obtengan un tratamiento diferenciado por la red. La calidad de servicio diferenciado puede ser provista en muchas formas:

- Técnicas de priorización tales como 802.1p, IP - ToS, encolamiento por "clase de servicio", y encolamiento por flujo.
- Adecuación de Tasa y control de flujo.
- ATM QoS
- FR QoS
- Otro componente del ancho de banda administrado son los mecanismos de control. Estos incluyen señalización RSVP, administración de políticas de red reforzadas por servidores de políticas y mantenidas en servidores de directorios LDAP entre otras.

La propuesta de la IEEE 802.1p es una extensión del estándar 802.1D que dicta como debe hacerse la priorización en la capa MAC de un puente independientemente del medio. Por otro lado, el 802.1Q, estándar para VLANs, añade priorización a los servicios Ethernet en particular. Con el uso de equipo con características 802.1p/Q es posible implementar servicios de priorización completos. La funcionalidad 802.1p se logra a través del uso de 3 bits para prioridad de usuario independientemente de la topología utilizada. Las tramas entrantes pueden ser examinadas buscando un valor de prioridad preexistente, que es *mapeado* al valor específico del 802.1p. Este valor puede ser asignado a una trama saliente u otro medio.

Éstos bits proveen 8 diferentes niveles de prioridad (0 al 7). Sin embargo, Ethernet nunca había tenido el servicio de priorización de forma nativa, por lo que la propuesta 802.1Q complementa perfectamente esta carencia. La implementación de la 802.1Q se hace con cuatro bytes adicionales insertados en el encabezado de la trama. Éstos 4 bytes contienen una variedad de campos, la mayoría de los cuales son específicos de la VLAN, pero uno de ellos provee una bandera de 3 bits. Estos 3 bits proveen 8 valores posibles, los mismos usados en el esquema de mapeo de prioridad del 802.1p.

En redes Ethernet, los campos del encabezado 802.1Q son insertados en las tramas inmediatamente después de los campos de direcciones fuente y destino, y antes del campo de longitud de trama. Con la supremacía a últimas fechas de las redes Ethernet, Fast Ethernet y 1Gb Ethernet, y la llegada de nuevas y complejas aplicaciones en línea, es casi imprescindible que el equipo seleccionado para la red local cuente con estas características para poder tener un mejor control del ancho de banda.

Hablando de Calidad de Servicio (QoS), el estándar IEEE 802.1p define los siguientes parámetros como esenciales para proveer ésta:

1) Disponibilidad del servicio.
2) Pérdida de tramas.
3) Desorden de tramas.
4) Duplicación de tramas.
5) Retraso de tramas.
6) Tiempo de vida de una trama.
7) Tasa de error de tramas no detectado.
8) Tamaño de trama máximo soportado.

9) Prioridad de usuarios.
10) Throughput.

El estándar IEEE 802.1Q define la arquitectura y los servicios provistos por las VLAN´s y los protocolos y algoritmos involucrados para proveer estos servicios.

Ningún mecanismo de QoS está definido en este estándar pero si un importante requerimiento para proveerlo como lo es la prioridad del usuario para recibir la información.

El estándar IEEE 802.1D cubre todas las partes de las clases de tráfico y la filtración dinámica de multicast descritos en el estándar IEEE 802.1p.

El estándar IEEE 802.1p, las clases de tráfico y la filtración dinámica de multicast describe importantes métodos para proveer QoS a nivel MAC.

3.3.7. Acuerdos de Nivel de Servicio (*SLA*) y Definición de Políticas.

Para implementar un esquema de Calidad de Servicio eficiente, además de los protocolos involucrados, se necesita una serie de reglas, políticas que forcen el cumplimiento de las reglas y jueces que decidan en que casos aplican. Todo esto es parte de lo que se llama un Sistema de Políticas Integral. Una política es una o más reglas que describen una acción a realizar cuando ocurre una ó más condiciones específicas. A su vez, una política puede contener políticas en sí misma.

El requerimiento fundamental para una red que permita un sistema de Políticas basadas en QoS, sobre todo en el tipo de red no determinística que se está manejando, es que estas no presenten ambigüedad en algún momento y que sean verificables, habiendo solo una que sea correcta para cada serie específica de condiciones. Además, el proceso de decisión sobre que condición está activa y que acciones resultarán de ésta, debe ser basado en un algún algoritmo global de evaluación de criterios que no cambie entre diferentes dominios de políticas, asegurando así la interoperabilidad de diferentes sistemas de políticas.

Existe un esquema desarrollado por el Grupo de Trabajo para Políticas de Admisión en RSVP (*RAP*), que establece un modelo de control escalable para trabajar con este protocolo de señalización de QoS. El trabajo realizado fue reconocido como un modelo que no solamente es aplicable a éste protocolo y esquema de QoS, sino como de uso general que necesiten el soporte de políticas como la seguridad en red.

En él se identifican dos componentes primarios: Un Punto para Forzar las Políticas (*Policy Enforcement Point, PEP*) y un Punto de Decisión de Políticas (*Policy Decision Point, PDP*), que serían la parte de policía y juez respectivamente. El PEP, como su nombre lo indica, obliga a llevar a cabo las políticas dictadas por el PDP, y este, a su vez toma las decisiones de entablar o no una política determinada dependiendo de los servidores residentes en él, como el servidor de políticas, el servidor de autenticación, entre otros.

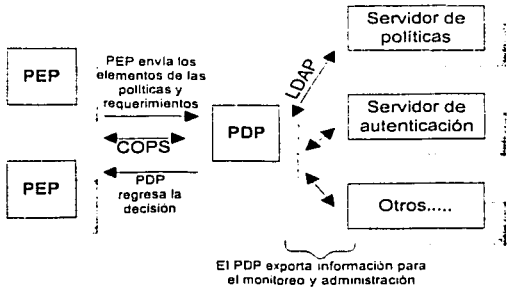


Fig. 3.17. El sistema de Política identifica los elementos funcionales y protocolos requeridos para la red con QoS.

La diferencia entre PEP y PDP es más bien lógica que física, y bien pueden residir en el mismo dispositivo. En general, en una red con Sistema de Políticas QoS, solamente se necesita de unos cuantos PDP's y muchos más PEP's.

Las funciones del PDP son las de recobrar políticas, interpretarlas, detectar si hay conflictos entre dos o más de ellas; además de recibir del PEP las características de la interfaz, requerimientos para decisiones y condiciones de políticas, determinando cuál es la relevante en cada caso, aplicarla y regresar los resultados. El mensaje del Cliente de Aprovisionamiento de Políticas, COPS, fue creado con el propósito de enviar elementos de políticas de manera asíncrona al PEP basadas en actualizaciones o requerimientos de entidades externas.

El PEP, como ya mencionamos, se encarga de aplicar acciones específicas de acuerdo a las decisiones del PDP, basadas en las políticas relevantes para cada caso y de las condiciones actuales de la red.

Ambas entidades, además de estas actividades, realizan mediciones que examinan de manera tanto activa como pasiva la red y sus dispositivos, revisando así las condiciones de la misma, si las políticas están siendo satisfechas o si los usuarios están haciendo uso incorrecto de los recursos de la red.

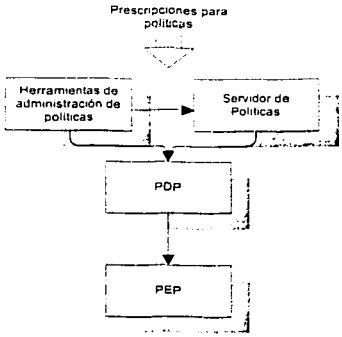


Fig. 3.18. Sistema de administración de Políticas.

Las políticas de uso representan metas y objetivos sobre algún plan de negocios. Debe existir una traducción entre estas y su realización en la red. Esta traducción está representada en los Acuerdos de Nivel de Servicio (SLAs), y sus objetivos y mediciones (Objetivos de Nivel de Servicio, SLOs), que son utilizados para especificar los servicios que la red dará a cada cliente. Las SLAs y en consecuencia, los SLOs, deben ser definidos independientemente de los fabricantes y tipos de dispositivos de los cuales está constituida la red.

Para esto, se definen Clases para la condición de cada política. Estas ayudan a categorizar los criterios que un administrador de red tendrá que manejar para controlar el acceso a los recursos y servicios de la red. Estas se pueden dividir en 5 rubros básicos:

- Por Host. Que define el o los rangos de direcciones fuente o destino.
- Por Usuario. Definiendo tipos de identificadores de usuarios y valores para transmisores y/o receptores.
- Por Aplicación. Se definen el rango de puertos fuente y destino, los protocolos de transporte y/o los valores del IP ToS recibido.
- Por interface de Enrutamiento. Definiendo las interfaces (direcciones IPv4 o IPv6 o ID de interfaces) y la dirección del flujo de tráfico.
- Por dirección de Capa 2. Se definen el rango de direcciones MAC fuente o destino, el Ethertype, el identificador 802.1Q de Vlan, el valor del encabezado SNAP y los valores DSAP y SSAP.

3.3.8. Soporte QoS para servicios *Multicast*.

Los servicios IP bajo un ambiente multicast es una opción bastante viable para redes escalables de éste tipo. El soporte de los protocolos QoS para servicios uno a muchos de audio y video sobre Internet, ha sido uno de los puntos fundamentales a cumplir, por lo que siempre se ha tomado en cuenta en el diseño de este tipo de protocolos. Sin embargo, no se tiene un soporte completo debido a que no se ha estandarizado.

3.3.8.1. Soporte RSVP para Multicast.

El diseño inicial de RSVP y en general de la arquitectura IntServ tomó el soporte de servicios multicast en IP para realizar las reservaciones de recursos basadas en mediciones del receptor. Un aspecto que hace que el soporte de multicast sea un reto, es que los receptores que componen a un grupo de multicast varían ampliamente en las capacidades de ancho de banda para recibir dicha información. Lo que conlleva a tener una gran cantidad de requerimientos de reservación de recursos, y de esta forma, los receptores tendrán que ser capaces de especificar la reservación que vaya de acuerdo a sus posibilidades.

Además, otra característica de RSVP que ayudaría al soporte de multicast, es la capacidad de configurar especificaciones de filtros para receptores heterogéneos, permitiendo de esta forma, la jerarquización de los datos; estos, codificados jerárquicamente son diseñados de forma que, cuando haya menos ancho de banda disponible, los receptores podrán captar todavía una señal útil, pero de menor fidelidad. Las especificaciones de los filtros podrán entonces reservar ancho de banda para la porción de datos que cada receptor sea capaz de recibir dependiendo de sus recursos disponibles.

3.3.8.2. Soporte DiffServ para Multicast

La relativa simplicidad de DS lo hace que sea de las mejores opciones para el soporte de servicios multicast. Sin embargo, existen retos a sobrepasar, como la estimación del tráfico, la naturaleza dinámica de los miembros de cada grupo de multicast, así como que el árbol de distribución tenga un solo punto de ingreso y varios puntos de salida variables dependiendo de los cambios en los grupos de multicast.

IV. DESCRIPCIÓN Y NECESIDADES DE CALIDAD DE SERVICIO EN EL BACKBONE DE REDUNAM.

En el transcurso de este capítulo se describirá 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. Por lo que este capítulo se encuentra dividido en tres partes:

- Historia y descripción general de RedUNAM.
- Descripción del backbone actual de RedUNAM.
- Servicios de comunicaciones ofrecidos.

4.1 HISTORIA DE REDUNAM.

En el año de 1987, la UNAM establece la primera conexión de su Red Académica de Cómputo de aquel entonces con la red BITNET 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 Estados Unidos. Dicha conexión contaba con una computadora IBM 4381 para manejo del correo electrónico.

En 1989, a través del Instituto de Astronomía se establece un convenio para enlazar a la Red Académica de Cómputo de la UNAM con la red de la National Science Foundation, NFS en Estados Unidos. El enlace se realizó mediante el Satélite Mexicano Morelos II que conectaba al Instituto antes mencionado y el UCAR-NCAR con residencia en Boulder, Colorado. La finalidad del proyecto estaba orientada a la investigación de fenómenos astrales. A la par se llevo 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.

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 enlaces satelitales hacia Cuernavaca, Morelos y San Pedro Mártir en Ensenada, Baja California Norte; también su primer enlace de microondas en la Ciudad de México entre la Torre II de Humanidades y la DGSCA.

En 1990, la UNAM fue la primera Institución Educativa en Latinoamérica que se incorpora a Internet, alcanzando así millones de máquinas y usuarios en todo el mundo. Su ininterrumpido desarrollo contempla como elemento fundamental, la implementación de un esquema que permita la comunicación de redes de diferentes arquitecturas, trabajando bajo el protocolo TCP/IP, mismo que se mantiene como estándar en la actualidad dada su funcionalidad y posibilidad de adaptación a los requerimientos que se van presentando.

La estructura de RedUNAM en esos momentos era un anillo doble FDDI, a los cuales estaban conectadas las redes de área local de cada dependencia, facultad, etc. La figura 4.1. nos muestra como se encontraban conectados los enrutadores, en su mayoría del fabricante Cisco Sytems al backbone FDDI:

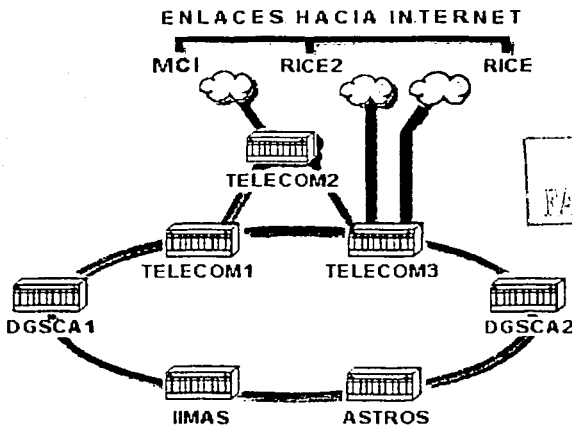


Figura 4.1 Backbone FDDI

En la primera semana del mes de agosto de 1997, se puso en operación la llamada Red Integral de Telecomunicaciones con una plataforma de backbone basada en la tecnología ATM. Este se encontraba formado por equipos de diferentes fabricantes, como son:

Switches.

- Corebuilder 7000 de 3Com, uno a cada extremo de la delta.
- Magellan Passport 170 de Nortel Networks, también uno a cada extremo de la delta.
- Corebuilder 2500 de 3Com, equipos periféricos que conectan las redes de área local con los Corebuilder 7000.
- Enrutadores Cisco, de la serie 75xx en su mayoría.
- Corebuilder 3500 de 3Com.

La figura 4.2. nos presenta la interconexión de los equipos en el backbone ATM:

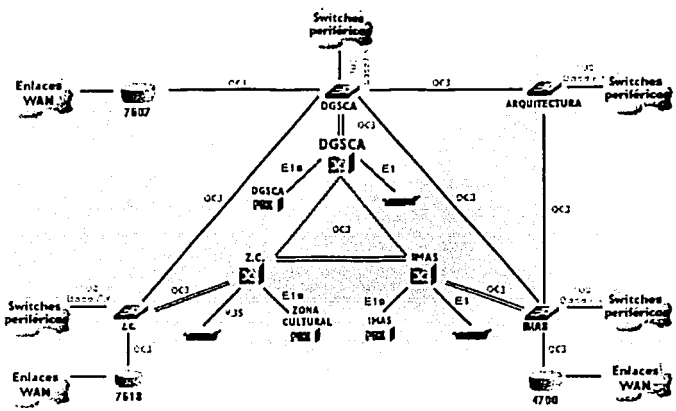


Figura 4.2 Backbone ATM

4.2. DESCRIPCIÓN DEL BACKBONE ACTUAL DE REDUNAM.

Al igual que en otras disciplinas, en las telecomunicaciones resulta conveniente dividir un problema en módulos ó factores con el fin de facilitar su análisis. En el diseño de redes, éste concepto de modularidad nos permite contar con una planeación por capas, que nos facilita el aislamiento de fallas y una fácil identificación de los puntos de mayor tráfico en la red. Explicaremos en que consiste el diseño jerárquico de redes para facilitar la descripción del backbone y su interacción con dispositivos de otras capas.

Las redes pueden ser analizadas por partes o dominios interrelacionados, siendo éstos:

- Capa de Core ó Núcleo.
- Capa de Acceso.
- Capa de Distribución.

4.2.1. Capa de Core ó Núcleo.

Proporciona una estructura de transporte óptima y confiable. Los servicios que brinda son:

- Optimización de rutas.
- Prioridad de tráfico.
- Balanceo de cargas.
- Manejo de rutas alternas.
- Encapsulado de servicios.

4.2.2. Capa de Distribución.

Proporciona el acceso a todos los puntos de la red, así como a los servicios, que son:

- Seguridad
- Administración del ancho de banda
- Filtrado y adaptación de funciones y servicios
- Políticas de intercambio de información
- Soporte multiprotocolo
- Manejo de diferentes tecnologías

4.2.3. Capa de Acceso.

Proporciona acceso a los usuarios y/o grupos de trabajo. Los servicios que brinda son:

- Realiza el filtrado específico de funciones y servicios
- Ancho de banda compartido y/o switcheado
- Segmentación de redes
- Manejo de broadcast y/o multicast
- Seguridad

Como en toda clasificación de redes, la descripción anterior no debe tomarse en forma estricta, el diseño jerárquico permite diseñar redes por capas, lo que reduce las tareas de interconexión.

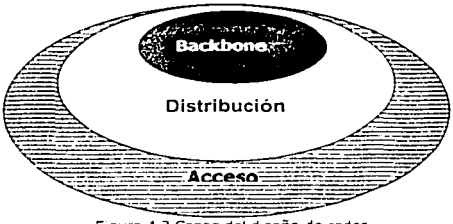


Figura 4.3 Capas del diseño de redes

Cada capa realiza funciones específicas; esto simplifica la elección e implantación de dispositivos, sistemas y políticas para cada una de ellas, además de facilitar los cambios. En la práctica, las barreras entre cada una de las capas se pueden desplazar o traslaparse y en algunos casos hasta disolverse.

4.2.4. Migración a tecnología Gigabit-Ethernet.

En el primer semestre del año 2002, el backbone de la RedUNAM es migrado a la tecnología de Gigabit Ethernet. El objetivo de este proyecto fue, implementar un backbone capaz de soportar de forma óptima los servicios de voz, datos y video sobre IP, y aplicaciones emergentes. Además de permitir el crecimiento de tráfico cuando se requiera.

Uno de los aspectos más relevantes de la red Integral de Telecomunicaciones de la UNAM es la interoperabilidad, es decir, en ella intervienen equipos de diferentes fabricantes manejando los mismos estándares de red. En la siguiente sección veremos a detalle la estructura del actual backbone en Gigabit Ethernet.

RedUNAM, es un proyecto que se desarrolla para la transmisión de información entre las facultades, institutos, escuelas nacionales y demás dependencias que forman la UNAM. Con tres funciones fundamentales:

- Impartir educación superior para formar profesionales, investigadores, profesores universitarios y técnicos útiles a la sociedad.
- Organizar y realizar investigaciones, que den soluciones a problemáticas de ámbitos nacionales e inclusive internacionales.
- Extender con la mayor amplitud posible la cultura.

Actualmente RedUNAM es la red académica más grande de América Latina, con más de 30,000 computadoras conectadas a la red de datos, distribuidas en aproximadamente 600 redes de área local, 90 instituciones externas con acceso a Internet, alrededor de 500 líneas del sistema telefónico que atiende a cerca de 12,000 cuentas de acceso remoto, más de 100 Mbps de salida a Internet a través de enlaces E3, y E1 y 34 Mbps de salida a Internet 2.

Red UNAM es una red que interconecta varias LANs en dependencias e institutos de Ciudad Universitaria; MAN con las conexiones a las ENEP, FES, Preparatorias, CCH y demás centros dentro del área metropolitana; WAN con las conexiones de instituciones externas (públicas y privadas) que se encuentran en el interior de la república y los enlaces internacionales. Utilizando diversas tecnologías como, Ethernet, Fast Ethernet, enlaces dedicados; que sirven como infraestructura para comunicarse principalmente por la suite de protocolos TCP/IP.

Debido a la complejidad y tamaño de la red, se describirá a continuación únicamente la parte que concierne a esta investigación, es decir, las conexiones de los equipos que forman el backbone y la forma como interactúan para posteriormente entender el comportamiento que presentan en el enrutamiento de datos. El objetivo que pretende alcanzar este capítulo está más enfocado a la parte del enrutamiento de datos, por lo que la parte referente a enlaces de datos se mencionará de manera somera.

La figura 4.4. muestra la configuración actual de la red de datos de la UNAM donde se muestra la parte de Core y de distribución, las cuales se describirán a continuación.

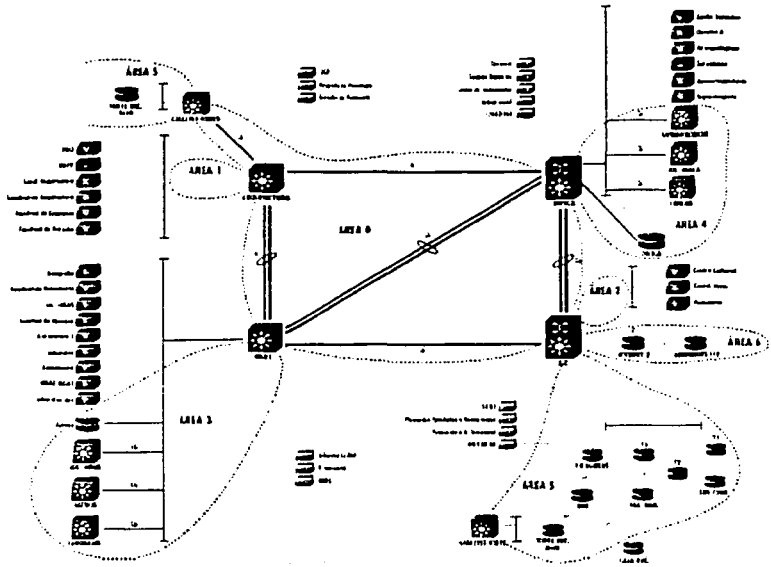


Figura 4.4 Backbone actual

4.2.4.1. Capa de backbone ó core.

La filosofía del core actual a diferencia del anterior, radica en que todos sus equipos manejan sus funciones a nivel de Capa 3 del modelo OSI, es decir, se encarga del direccionamiento entre las diferentes subredes de RedUNAM.

Esta constituida por equipos del fabricante Foundry Networks: *NetIron 800* y *BigIron 8000*, los cuales se encuentran conectados de la siguiente manera: los nodos denominados Arquitectura, IIMAS, DGSCA y Zona Cultural, los cuales manejan dos enlaces bidireccionales denominados Trunking lo que nos permite tener un enlace lógico único con el doble de capacidad. Por otra parte los nodos Arquitectura-DGSCA presentan un enlace sencillo Gigabit Ethernet.

Las características principales del equipo NetIron 800 son:

- Maneja hasta 120 puertos de Gigabit Ethernet.
- Maneja hasta 7 puertos de 10Gigabit Ethernet.
- 333 puertos 10-100 Mbps.

- Soporta MPLS (sólo como LER, requiere de actualización de SW para soportar administración y distribución de etiquetas).
- Soporta RSVP y servicios diferenciados.
- Maneja los protocolos de ruteo BGP Ver. 4, OSPF Ver. 2.
- Maneja el estándar 802.3 para control de flujo.
- Maneja el estándar 802.1p.
- Ruteo basado en políticas (PBR)
- Maneja el estándar 802.1Q para manejo de VLAN´s.
- Protocolos Multicast: DVMRP, MSDP, PIM-SM Y PIM-DM.
- Métodos de encolamiento: SP ó WFQ.

BigIron 8000.

- Tiene la capacidad de hasta 120 puertos de GibaBit Ethernet.
- 333 Puertos 10-100 Mbps.
- Hasta 7 puertos de 10Gigabit Ethernet.
- Maneja el estándar 802.3 para control de flujo.
- Maneja el estándar 802.1Q para manejo de VLAN´s.
- Maneja los protocolos de ruteo BGP ver.4, OSPF ver. 2 y RIP ver. 1 y ver. 2.
- Soporta servicios de IP Multicast.
- Ruteo basado en políticas (PBR)
- Aprovisionamiento del ancho de banda dinámico.
- Funciones de QoS avanzadas, como son:
    - Prioridad de tráfico basada en: Puertos Tcp, VLAN´s, direcciones MAC fuente, 802.1p y ToS ó servicios diferenciados para priorización de flujos.

4.2.4.2. Capa de distribución.

En la capa de distribución existen 2 tipos de equipos, los que están incluidos en el dominio de OSPF y los que no son lo suficientemente robustos para soportarlo o que por consideraciones de diseño sus tareas son diferentes para pertenecer a la capa core. En estos últimos se encuentran switches 3com modelos Lanplex 2500 y Corebuilder 3500 que pertenecían a la anterior capa de distribución de la red ATM. También se encuentran enrutadores Cisco de la serie 7500, los cuales reciben las conexiones WAN de las Instituciones externas. La tarea principal de los Lanplex es trabajar como punto de unión entre los equipos de la capa core y las redes locales donde se encuentran los usuarios finales. La figura 4.5. nos ejemplifica el papel de estos dispositivos:

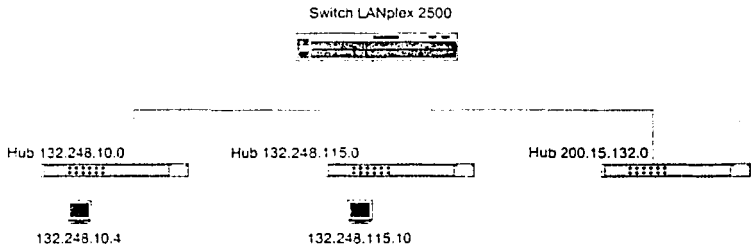


Figura 4.5 Dependencias en el Lanplex 2500.

En los equipos Lanplex existen configuradas VLANs, la asociación de éstas es por puertos o subred, como vemos en la tabla 4.1. la subred 132.248.126.0 se encuentra agrupada en el puerto 5 del switch, también podemos tener casos donde dos VLANs pueden estar configuradas en un mismo puerto, como las VLANs 4 y 6.

CONFIGURACIÓN DE LANPLEX 2500 JARDÍN BOTÁNICO Ethernet 5/1 (Foundry)

VLAN	NOMBRE VLAN	PUERTO	RED IP/IPX	EDIFICIOS
2	IPX.ATM	1	0x2540	JARDIN BOTANICO BODEGA
3	US_II	2, 5-8	132.248.126.254	SEMINARIOS,I-BIOL, COLECCIONES, I.INGENIERIA(M.VIBRADORA)
4	CCH_SUR	3	132.248.86.254	LOCAL CCH SUR
5	IPX.CCH-SUR	3	0X860	LOCAL CCH SUR
6	COORD_ASESORES	3	132.248.208.254	CALLE DE FUEGO (Temporal)
7	IE	4	132.248.49.254	CENTRO DE ECOLOGIA
8	IPX.IE	4	0X490	CENTRO DE ECOLOGIA
9	Instituto de Biología	9	132.248.13.254	
10	AREA4	1	132.248.255.97	

Tabla 4.1. Configuración de Lanplex2500 Jardín Botánico.

Los equipos que están en el dominio OSPF son los switches BigIron 8000 de Foundry Networks, los cuales tienen las mismas características que los que pertenecen a la capa core, sin embargo su tarea es interconectar un mayor número de subredes configuradas en equipos Lanplex con los equipos del backbone. La figura 4.6. nos ejemplifica esta conexión:

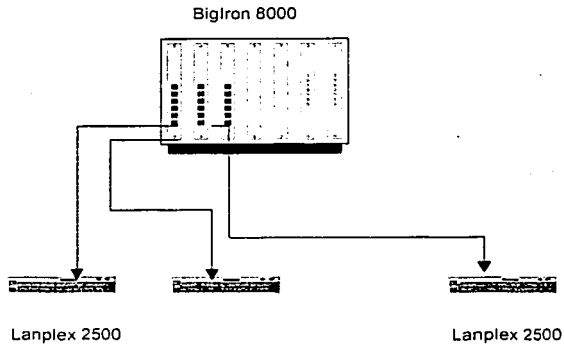


Figura 4.6 Conexión entre Lanplex 2500 y BigIron 8000.

4.3. SERVICIOS DE COMUNICACIÓN OFRECIDOS.

Dentro de la RedUNAM existen 3 tipos principales de servicios: los de datos, voz y video. Los de datos pueden ser catalogados desde alta hasta baja prioridad, pasando por tráfico de Web, correo electrónico y transferencia de archivos básicamente. Los servicios de voz son provistos por la red interna de telefonía formada por cinco nodos principales y pueden ser digitales o analógicos, como se muestra en la figura 4.7.

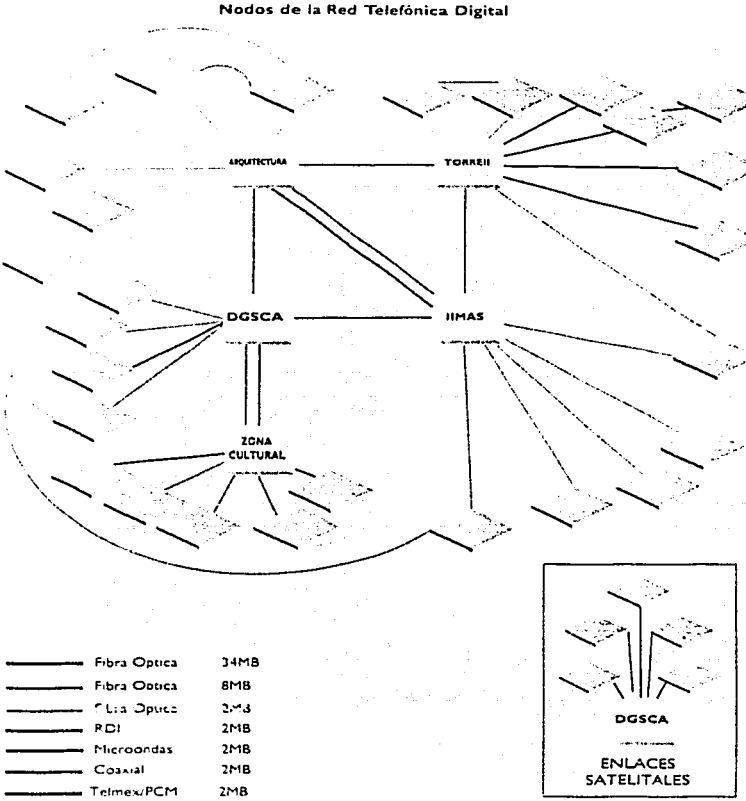


Figura 4.7 Sistema de telefonía digital

El servicio de videoconferencias (VC) se basa en un nodo principal localizado en DGSCA que realiza la tarea de interconectar las entidades que requieren del mismo. Para realizar videoconferencias con algún punto que no forma parte de la red de videoconferencias se utiliza ISDN. Se han realizado videoconferencias con el protocolo H.323, pero con ninguna implementación de calidad de servicio. Esto se logra mediante la configuración de un puerto en una VLAN exclusiva en un Lanplex 2500 que se encuentra conectado a los equipos del *core*, en el otro extremo de la conexión existe un nodo VC que hace la traducción de protocolos de H.323 a H.320. El uso del ancho de banda en los enlaces no se impacta con este servicio, pero han existido problemas con los equipos 3Com, ya que estos se reinicializan al no soportar la carga.

A continuación presentamos un listado donde se muestran las dependencias o institutos que ofrecen el servicio, las que están en pruebas y las que están en proyecto .

Operativos:

- Centro de Enseñanza para Extranjeros
- Facultad de Filosofía y Letras
- Facultad de Economía
- Facultad de Odontología
- Torre de Rectoría
- Facultad de Medicina Veterinaria y Zootecnia
- Instituto de Investigaciones en Matemáticas Aplicadas y Sistemas
- Coordinación de la Investigación Científica
- Facultad de Ciencias
- Facultad de Contaduría y Administración
- Dirección General de Servicios de Cómputo Académico. Auditorio
- Dirección General de Servicios de Cómputo Académico. Aula
- Facultad de Ciencias Políticas y Sociales
- Instituto de Investigaciones Filológicas
- Instituto de Investigaciones Jurídicas

Pruebas:

- Facultad de Derecho
- Facultad de Medicina
- Instituto de Astronomía
- Instituto de Ecología
- Coordinación del Sistema de Universidad Abierta y Educación a Distancia
- Unidad de Seminarios
- Dirección General de Divulgación de la Ciencia

Proyecto:

- Coordinación de Humanidades.
- Coordinación de Humanidades. Torre II
- Dirección General de Personal.
- Instituto de Ciencias del Mar y Limnología.
- Instituto de Física.
- Instituto de Fisiología Celular.
- Instituto de Geofísica.
- Instituto de Investigaciones Biomédicas.
- Instituto de Matemáticas.
- Instituto de Química.
- Posgrado de Ingeniería.
- Torre de Ingeniería.
- Dirección General de Televisión Universitaria.

- Escuela Nacional de Trabajo Social.
- Facultad de Psicología.
- Facultad de Química.

4.4. CONFIGURACIÓN DE ENRUTAMIENTO EN EL BACKBONE.

El protocolo de enrutamiento IGP utilizado es OSPF. En OSPF, la red necesita ser dividida en diferentes áreas. Inicialmente, se configuraron seis áreas. Las cuatro primeras están destinadas para agrupar a los equipos que brindan servicio para LANs dentro del campus universitario; y los dos restantes para los equipos que brinden servicio a dependencias de la UNAM fuera del campus universitario, así como a instituciones externas. Podemos visualizar las áreas OSPF en la figura 4.4 de este mismo capítulo.

Donde:

- El Área 0 está asignada para los equipos del Backbone en Gigabit Ethernet.
- El Área 1 está reservada para los equipos del nodo principal Arquitectura.
- El Área 2 está reservada para los equipos del nodo principal Zona Cultural.
- El Área 3 está asignada a los equipos del nodo principal IIMAS.
- El Área 4 está asignada a los equipos del nodo principal DGSCA.
- El Área 5 está asignada a los enrutadores con enlaces WAN hacía los ISP's de la UNAM, dependencias fuera del campus, instituciones externas y la red de Rectoría.
- El Área 6 está asignada a los enrutadores que conforman la red de Internet 2 (I2) de la UNAM así como los enrutadores que se conectan a I2 a través de la UNAM.

En el backbone, ningún equipo 3Com (Lanplex 2500 ó Corebuilder 3500) está incluido en el dominio OSPF ya que o no lo soportan o bien no son lo suficientemente robustos para ello, sin embargo dichos equipos están configurados en una misma LAN junto con los equipos Foundry de distribución y/o de core de su respectivo nodo. Esto con el fin de facilitar su inclusión al dominio de OSPF en sus respectivas áreas cuando dichos equipos sean cambiados por otros que cumplan con las especificaciones de OSPF.

Durante este estudio, nos hemos percatado que la tendencia en el mercado es que el manejo de los servicios sea la integración de los mismos en una sola infraestructura física y lógica, es decir, una red convergente basada en el modelo TCP/IP.

Dentro de esta convergencia, existen casos aislados de utilización de videoconferencia en H.323 y voz sobre IP, sin llegar a tener todos los servicios que la telefonía puede ofrecer. Con el incremento en la utilización de estos servicios sobre IP provocará que los enlaces compartidos, no cumplan con los requerimientos de manejo de ancho de banda para cada uno de ellos, con la subsecuente saturación de los enlaces en horas pico.

Para llamadas telefónicas, la calidad de la voz puede ser pobre, partes de la conversación se pueden perder, la voz puede ser poco entendible y pueden existir ecos en la línea.

Para videoconferencias la imagen puede ser de mala calidad, retraso en la recepción de la imagen y la transmisión del sonido puede no estar coordinada con la transmisión visual. Para otros tipos de aplicaciones la transmisión puede presentar retrasos o pérdidas de paquetes cuando la red llega a su máxima capacidad.

4.5. Características principales y necesidades de los diferentes tipos de tráfico.

Como lo hemos mencionado, las perspectivas actuales son hacia modelos de redes del tipo convergente, en donde confluyan tanto voz, video y datos dentro de la misma infraestructura física. Para esto se necesita saber como se comportan los servicios que la RedUNAM llevará, así como los requerimientos que pedirán a la red para un buen desempeño.

Sin embargo, con lo que realmente se estará tratando son las aplicaciones que cada usuario final tendrá para cada servicio. Existen dos tipos principales de estas:

i. Aplicaciones de *tráfico elástico*, son las que pueden esperar para la recepción de los paquetes de información, es decir, el orden en que llegan los paquetes no causa pérdidas considerables en la información o bien no modifica las características propias de esta.
ii. Aplicaciones de *tráfico rígido*, son en las que su importancia recae en el hecho de que su flujo de tráfico llegue a tiempo (sin retrasos) y tal como se envió (que es su característica más importante), pudiéndose permitir pequeñas pérdidas en el proceso.

Básicamente, los tipos de tráfico pueden clasificarse de la siguiente forma:

	Ancho de Banda Requerido	Tiempo promedio de duración de la sesión	Capacidad de envió de paquetes	Sensibilidad al retraso (latency)	Sensibilidad a la variación en el retraso (jitter)
Voz	Bajo	Corto	Bajo	Alto	Medio
Video	Alto	Largo	Bajo	Bajo	Alto
Video interactivo	Alto	Largo	Medio	Alto	Alto
Aplicaciones compartidas	Bajo – Medio	Medio	Alto	Medio	Bajo
Datos	Bajo – Medio	Corto – Medio	Alto	Bajo	Bajo

Tabla 4.2. Clasificación de los tipos de tráfico.

4.6. Necesidad del establecimiento de calidad de servicio en la RedUNAM.

Actualmente los servicios de voz, datos y video se proporcionan utilizando redes separadas, es decir, existe una infraestructura de red por servicio: una para datos, una para voz y una para videoconferencias. La tendencia en la actualidad es la integración de servicio en una sola red que permita una administración y operación menos compleja.

Pensamos que para proveer los tres tipos de servicios en una sola infraestructura de red, es necesario tener implementado un modelo de calidad de servicio, ya que cada aplicación demanda diferentes recursos de la red.

La RedUNAM, en los últimos años ha presentado un incremento en la utilización de aplicaciones de misión crítica, como sistemas de bases de datos, las cuales en ciertos períodos de tiempo presentan

lentitud, debido a la sobrecarga en la red, que obliga que las aplicaciones realicen la retransmisión de paquetes a causa de la pérdida de los mismos.

Existen también facultades e institutos de investigación con altos niveles de saturación tanto internos como de en el enlace hacia la RedUNAM, debido a la alta tasa de transmisión y recepción de datos, esto evita la ejecución optima de nuevas aplicaciones multimedia y las tradicionales.

Se presenta también la creciente demanda de ancho de banda debido al crecimiento presentado en las redes de área local universitarias, la aparición de nuevas aplicaciones como transmisión de audio en tiempo real, video en streaming, videoconferencias, comunicaciones interactivas.

La RedUNAM, así como todas las redes IP existentes, realiza la entrega de datos con la filosofía del mejor esfuerzo. La red ha escalado en los últimos años, cada vez hay más hosts que forman parte de ella, aparecen mayores demandas de servicios en la red. El fenómeno que sucede no es la negación del servicio, sino la degradación en el mismo. De alguna manera las aplicaciones típicas de Internet se adaptan a esta situación, como son el correo electrónico, transferencia de archivos y aplicaciones Web. Pero las nuevas aplicaciones no pueden adaptarse a estos niveles de servicios inconsistentes, los retardos en las entregas provocan problemas en la transmisión de aplicaciones en tiempo real, como las que transmiten tráfico multimedia y aun mucho menos la transmisión de telefonía en IP.

Una solución a corto plazo sería aumentar el ancho de banda en la conexión entre las redes de área local y el acceso al backbone, pero la tendencia en la RedUNAM así como las redes que forman parte de Internet, es utilizar el ancho de banda disponible al máximo, es decir, si los usuarios tienen disponible más ancho de banda, éste será consumido y el problema de funcionamiento en las aplicaciones multimedia y de video, y la degradación del servicio se presentaría de nuevo. El aumento del ancho de banda no resuelve el problema de la degradación de los servicios.

Para que la RedUNAM provea el nivel de servicio adecuado, es necesario que se implementen mecanismos para tratar al tráfico de acuerdo a sus características y requerimientos. Pensamos pues que es necesario que la RedUNAM presente un esquema de calidad de servicio en la red, que tenga el objetivo de dar niveles cualitativos y cuantitativos al usuario universitario, así como un control en el comportamiento de la red. La implentación de este esquema de calidad de servicio no ofrece el incremento del ancho de banda, que aclaramos no se descarta como paso previo hacia una red con calidad en casos específicos en los que las redes locales presentan un pobre diseño y administración, sino que se propone administrar el que existe.

V. ESTUDIO PARA LA IMPLEMENTACION DE CALIDAD DE SERVICIO EN EL BACKBONE DE REDUNAM.

5.1. PROCESO DE DISEÑO.

Para presentar la propuesta de implementación de calidad de servicio en el Backbone de RedUNAM, nos basamos en el siguiente proceso de diseño.

5.1.1. Determinación de las prioridades del usuario, políticas de QoS y nivel de servicio requerido.

Hemos definido diferentes tipos de usuarios, como son:

USUARIO	DESCRIPCION
Usuario A	Rector, Secretarios Generales, Directores de Escuelas e institutos de investigación
Usuarios B	Investigadores
Usuarios C	Profesores
Usuarios D	Alumnos y usuarios en general.

Tabla 5.1. Tipo de usuarios.

Donde los usuarios que pertenecen al tipo A tienen mayor prioridad de servicio que los usuarios que pertenecen al tipo B; los del tipo B tiene mayor prioridad que los del tipo C y así sucesivamente.

Así también se tienen las subredes de las dependencias ó institutos que proporcionan el servicio de videoconferencia, los cuales tendrán la mayor prioridad de transferencia aun cuando el usuario que utilice este servicio no pertenezca al tipo de usuario A, ya que como se expresa en la siguiente tabla, el tráfico de videoconferencia es clasificado como el más importante. La lista de dependencias operativas, en prueba y en proyecto de construcción en Ciudad Universitaria que ofrecen el servicio antes mencionado se encuentran listadas en el capítulo 4.

Hemos definido 4 clases de tráfico dentro de las cuales se organizarán las aplicaciones utilizadas, en la tabla 5.2 solo se muestran algunas de ellas, pero se requiere que todas las aplicaciones pertenezcan a una clase.

CLASE DE TRÁFICO	APLICACIONES
Platino	Voz sobre IP, videoconferencias
Oro	Sesiones interactivas, aplicaciones críticas, video en streaming
Plata	HTTP, TELNET
Bronce	FTP, SMTP

Tabla 5.2. Clases de tráfico.

Los usuarios arriba definidos pueden utilizar cualquier tipo de aplicación, la cual tendrá una prioridad asignada dependiendo el tipo de usuario. Esta asignación es parte fundamental de las políticas de tráfico. En la tabla 5.3. presentamos la asignación de prioridades de los usuarios en los tipos de tráfico.

CLASE DE TRÁFICO	USUARIO A	USUARIO B	USUARIO C	USUARIO D
Platino	U_{11}	U_{11}	U_{11}	U_{11}
Oro	U_{21}	U_{22}	U_{23}	U_{24}
Plata	U_{31}	U_{32}	U_{33}	U_{34}
Bronce	U_{41}	U_{42}	U_{43}	U_{44}

Tabla 5.3. Asignación de prioridades.

En "U_{xy}", "X" representa la importancia por clase de tráfico y "Y" representa el nivel de prioridad de un usuario en la misma clase de tráfico. Es decir, los usuarios U_{x3} tienen menos prioridad en la utilización del mismo servicio que el usuario U_{x2} y ésta a su vez tiene menos prioridad que el usuario U_{x1}.

La implementación de las políticas de tráfico será llevada a cabo con la instalación de un servidor que lleve a cabo la función de verificar las prioridades de los usuarios y redes.

5.1.1.1. Implementación de arquitecturas de calidad de servicio.

La implementación de Calidad de Servicios en redes IP ha llevado a dos enfoques principalmente:

La arquitectura de servicios integrados (Int-Serv) con su protocolo de señalización RSVP y la de servicios diferenciados (Diff-Serv). Además se cuenta con MPLS. A todos ellos se les ha presentado de manera independiente de extremo a extremo, es decir, entre emisor y receptor. En la práctica es poco probable que estos modelos sean utilizados de manera independiente, y de hecho están diseñados para utilizarse con otras tecnologías de calidad de servicios para lograr cubrir todas las necesidades de extremo a extremo.

5.1.1.1.1. INT-SERV Y DIFF-SERV.

En éste modelo, Diff-Serv es utilizado por redes en tránsito en él core de la red mientras que hosts y redes de extremo utilizan RSVP/Int-Serv. En contraste a la orientación por flujo de Int-Serv y RSVP, las redes Diff-Serv clasifican los paquetes en un agregado agregado de flujos o clases, basándose en los bits del campo ToS de cada paquete Ipv4.

Para nuestro caso en estudio, la red de tránsito está formada por los equipos de la capa *core*: NetIron 800 y BigIron 8000. La red de *stub* está formada por lo equipos de la capa de distribución: equipos Lanplex 2500, Corebuilder 3500, BigIron 800 que no forman parte del core, algunos enrutadores Cisco.

Podemos ver a los servicios Int-Serv y Diff-Serv como herramientas que se complementan para conseguir calidad de servicio. Para muchas aplicaciones, la QoS de Diff-Serv puede ser adecuada. Sin embargo, algunas aplicaciones necesitarán una calidad de servicios cuantitativa y asegurada. Esta es proporcionada por Int-Serv y RSVP. Por ejemplo: telefonía IP, video sobre demanda y aplicaciones de misión crítica no multimedia.

La figura 5.1 muestra de manera representativa la constitución del enfoque Diff-serv con Int-serv para la RedUNAM.

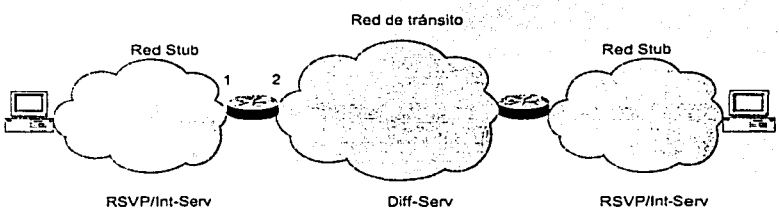


Fig. 5.1. RSVP/Int-Serv y Diff-Serv.

Componentes principales del modelo.

- Host.

Los hosts (emisor y transmisor) usarán RSVP para dar a conocer sus requerimientos de calidad de servicios que demandan las aplicaciones que se encuentran en las redes locales de la RedUNAM, Ver la figura 5.2.

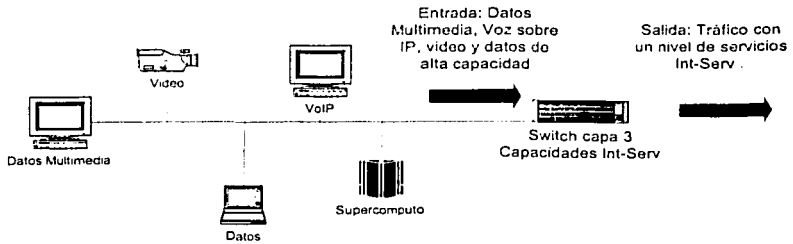


Fig. 5.2 Proceso de transmisión de las redes locales a los equipos de la capa de distribución con capacidades de QoS Int-Serv en la RedUNAM.

- Señalización RSVP extremo a extremo.

Los mensajes de señalización RSVP viajan de extremo a extremo entre un host y otro. Por tal motivo, se necesita que éstos mensajes viajen a través de túneles transparentes en la red de servicios diferenciados.

- Enrutadores extremos y de frontera.

Es aquí donde se establece la frontera entre las regiones RSVP/Int-Serv y Diff-Serv. Podríamos pensar que un enrutador extremo tiene dos mitades, la primer mitad manejando RSVP, que se une a la red stub y una segunda mitad, que se une a la red de tránsito. Estos equipos deberán pertenecer a la capa core de RedUNAM. Los enrutadores frontera deben de manejar Diff-Serv y no necesariamente RSVP. En el caso de la red universitaria los nodos extremos y frontera serán los mismos, ya que el mismo equipo ejecutará tareas pertenecientes a ambos tipos de nodos, ver figura 5.3.

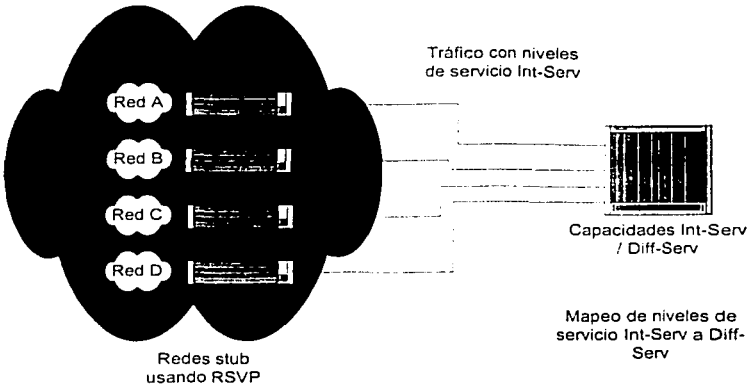


Fig 5.3 Esta imagen muestra el proceso de transmisión entre los equipos de la capa de distribución y los equipos de la capa core, lugar donde se hará el mapeo de servicios de Int-Serv a Diff_Serv en la RedUNAM.

- Red stub.

Consta de hosts y algunos enrutadores que usan Int-Serv. Puede ocurrir que algunos enrutadores no soporten RSVP, si este es el caso no llevarán a cabo tareas de clasificación, señalización o control de admisión y pasarán los mensajes RSVP de manera transparente.

- Red de tránsito.

Esta red, no hace las tareas típicas de clasificación, señalización y control de admisión. Provee dos o más niveles de servicios basándose en el campo DS. Transmite de manera transparente los paquetes RSVP, con un impacto mínimo en el funcionamiento.

Mapeo de servicios.

La señalización RSVP pide un servicio diferenciado y una serie de parámetros, éstos definen los indicadores de calidad de servicio en las regiones Int-Serv. El tipo de servicio Int-serv es mapeado a un nivel de prioridad 802.1p apropiado. Sin embargo, la petición de servicio integral debe ser mapeada al campo DS cuando los paquetes entren a la nube de servicios diferenciados, es decir, la petición debe ser mapeada a un tipo de nivel de servicio Diff-Serv solicitado por la aplicación.

El enrutador de extremo puede realizar el control de admisión a la red Diff-Serv, aceptando o negando las peticiones, basándose en la capacidad del servicio diferenciado demandado, Ver figura 5.4.

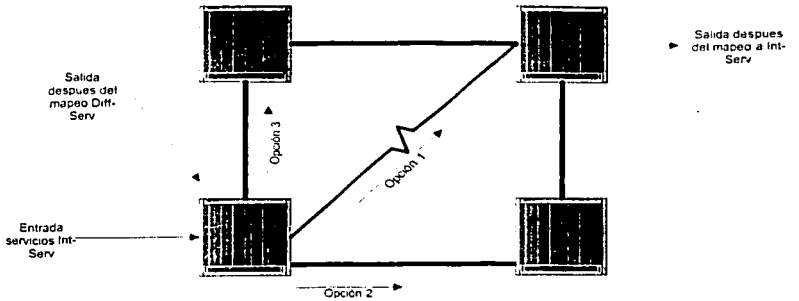


Fig. 5.4 Los equipos del core de RedUNAM, transmiten la información de manera transparente, los equipos de los extremos tendrán la función de mapeo de servicios Int-Serv a Diff-Serv y viceversa.

Existen dos esquemas, que se pueden utilizar para mapear los tipos de servicios Int-Serv a niveles de servicios Diff-Serv.

- *Por Defecto.* Es este esquema, se tienen los mapeos "bien conocidos" de servicios Int-serv a PHB que invocarán al comportamiento adecuado para la red Diff-Serv.
  Para mejorar la calidad del mapeo, es necesario que la petición de calidad de servicio contenga más información. Por ejemplo, si consideramos dos peticiones de QoS para dos flujos diferentes, el primero tráfico de voz interactivo, y el otro tráfico tolerante a retardos. Pueden tener ambos los mismos parámetros Int-Serv (sobretodo cuando se utiliza el servicio de carga controlada), pero probablemente mapearán servicios diferenciados diferentes. Por esta razón se recomienda añadir un "calificador" a Int-Serv indicando su tolerancia relativa al retraso (baja o alta). El calificador deber ser definido como un objeto en los mensajes de señalización Int-Serv.

- *Personalizada.* En éste esquema, los enrutadores de extremo pueden modificar el servicio de mapeo. Los mensajes RESV que se generan en los hosts llevarán ya el tipo de servicio Int-Serv (tal vez con algún calificador). Cuando un mensaje RESV llega al enrutador extremo a partir del cual se entrará a la región de servicios diferenciados, el enrutador determina el código PHB que debe ser usado para obtener el nivel de servicio Diff-Serv correspondiente. Esta información se agrega al mensaje RESV y lo envía al host origen. Cuando el mensaje llega al hosts origen (o un enrutador Int-Serv), éste comienza a marcar los paquetes de salida con su código PHB.

Existen decisiones que pueden sobrescribir al "servicio bien conocido" en un enrutador extremo, basándose en alguna configuración o política. Por ejemplo, cuando una petición de reserva llega al punto de ingreso de una red Int-Serv, y ésta ya ha aceptado reservaciones y alcanzado el límite de capacidad en el nivel de servicio correspondiente, entonces el enrutador de extremo puede decidir el PHB que corresponda a un nivel de servicio basado en una política administrativa.

Retomamos las clases de tráfico para asignarles su respectivo PHB, así también las aplicaciones más comunes, como lo expresamos en la tabla 5.4.

CLASE DE TRÁFICO	APLICACIONES	PHB*
Platino	Voz sobre IP, videoconferencias	EF
Oro	Sesiones interactivas, aplicaciones críticas, video en streaming	AF31
Plata	http Telnet	AF21 AF22
Bronce	SMTP FTP	AF11 AF12

Tabla 5.4. Aplicaciones más comunes.

- Los PHB utilizados están definidos en RFCs, pero existe la posibilidad de crearlos en caso de ser necesario.

Ejemplo: Calidad de servicio de extremo a extremo en RedUNAM.

A continuación describiremos la secuencia del proceso por medio del cual una aplicación obtiene la calidad de servicio punto a punto, para esto nos apoyaremos en la figura 5.5.

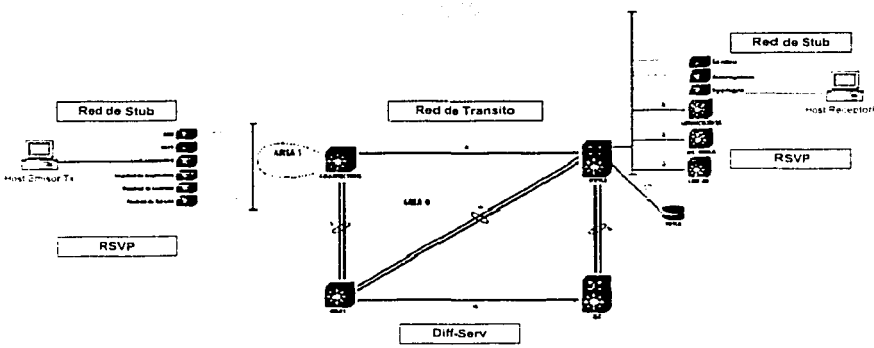


Fig. 5.5. Calidad de servicio punto a punto.

1. El proceso de QoS en el host emisor Tx genera un mensaje PATH de RSVP que describe el tipo de tráfico de la aplicación que se transmitirá.
2. El mensaje PATH es enviado al host receptor Rx. En la red Stub del host origen, se lleva a cabo un proceso RSVP en los nodos que pueden manejarlo.
3. En el enrutador de extremo, el mensaje PATH esta sujeto al proceso RSVP y se crea un estado PATH en el enrutador. El mensaje PATH sigue su camino hacia la red de tránsito.
4. El mensaje PATH es llevado de manera transparente en la red de tránsito, y entonces procesado en el enrutador stub, de acuerdo a las reglas de procesamiento RSVP.
5. Cuando el mensaje PATH llega al host destino Rx, su proceso de QoS genera un mensaje RESV, el cual indica que quiere recibir el tráfico con un cierto nivel de servicio Int-Serv.

6. Se envía el mensaje RESV al host emisor. Cabe señalar que el proceso RSVP puede ser rechazado por cualquier nodo de la red stub receptora si los recursos son insuficientes para transmitir el tipo de tráfico pedido.
7. Si las peticiones no son negadas en la interfaz del enrutador del extremo receptor, el mensaje RESV es transmitido de manera transparente por la red de tránsito hasta llegar al enrutador del extremo receptor.
8. En el enrutador del extremo transmisor, se crea un proceso DSAC. El DSAC compara los recursos solicitados con los recursos disponibles en el correspondiente nivel de servicio Diff-Serv en la red de tránsito. Si el mensaje RESV es aceptado, DSAC actualiza la capacidad disponible para las clases de servicio, es decir hace una substracción de los recursos recién aceptados de la capacidad disponible.
9. Asumiendo que la capacidad disponible es suficiente, el mensaje RESV es admitido y puede continuar su camino hacia el host emisor. Si la capacidad es insuficiente, el mensaje RESV es rechazado y la capacidad disponible permanece sin cambios.
10. El proceso de QoS en el host emisor recibe al mensaje RESV, esto significa que el tráfico ha sido aceptado con el tipo de servicio especificado (en las regiones RSVP de la red) y también con el nivel de servicio Diff-Serv (en las regiones Diff-Serv de la red).
11. El host emisor pone el campo DS en los encabezados de los paquetes que se transmiten con el valor que corresponde al tipo de servicio Int-Serv especificado en el mensaje RESV.

De esta manera se obtiene la calidad de servicio de extremo a extremo, con la combinación de redes que manejan reservaciones RSVP y redes que manejan prioridades Diff-Serv. La llegada de los mensajes RESV al host emisor indica que el control de admisión ha sido exitoso en ambas regiones (RSVP y Diff-Serv).

5.1.1.1.2. DIFF-SERV Y MPLS.

Otro enfoque distinto de establecer un diseño con los protocolos que tenemos de herramientas es utilizar túneles en la red de tránsito con MPLS-TE, y en la red STUB, dependiendo del tráfico solicitado de DiffS-Serv .

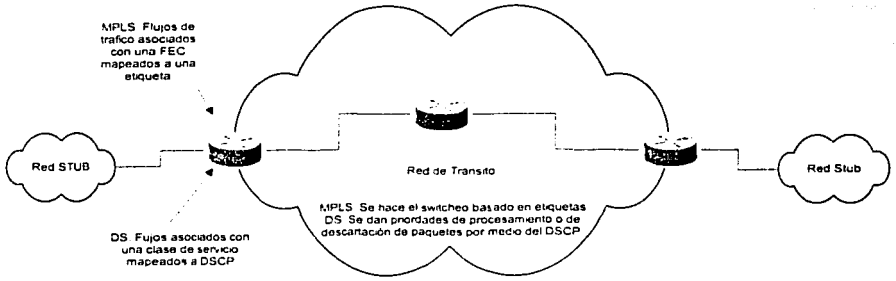


Fig. 5.6 Modelo DiffS-Serv - MPLS

Diff-Serv sobre MPLS describe métodos para configurar túneles de tráfico Diff-serv sobre una red MPLS. Este comportamiento de Ingeniería de Tráfico se puede obtener mapeando alguna de las clases de servicio Diff-Serv (ya sea una por una o a manera de Agregados de Tráfico) en algún LSP, permitiendo utilizar los recursos disponibles para cada PHB mapeado, tomando la ruta más corta ó no, creando el túnel que mejor se comporte de acuerdo a las necesidades de la red. El comportamiento que se espera que la red tendrá con el tráfico de punto a punto en cierto dominio DS se le denomina PDB (*Per Domain Behavior).*

Para la interacción entre redes Diff-Serv y MPLS, se requiere mapear las clases de servicios definidas en el DSCP del campo DS a las LSPs. El DSCP está contenido en el encabezado IP, sin embargo los LSR solo examinan el encabezado de la etiqueta, por lo que tenemos un problema de mapeo, ya que el campo DCSP es de 6 bits definiendo 64 clases de servicio, en cambio el campo EXP es de 3 bit y 8 clases de servicio definidas.

En este tipo de situaciones, se definen lo llamados Agregados de Tráfico (*Traffic Aggregate, TA*), que se denominan a los flujos de tráfico que tienen un DSCP en común que permite que tengan un mismo PHB. Definimos también PSC (*PHB Scheduling Class*) que es un grupo de PHBs para determinar el orden, en que los paquetes de un microflujo deben ser procesado, es decir, los paquetes deben mantener el mismo orden desde el ingreso hasta el egreso de cada LSR, por lo que los paquetes pertenecientes a la misma clase de servicio (PSC) son puestos en la misma cola. Entonces nos referimos a un conjunto de TA's correspondientes a un conjunto de PHB's de una cierta PSC como *{TA}PSC*. Una dada *{TA}PSC* tendrá cierto tratamiento de una PDB asociada con un correspondiente PSC.

Se definen dos tipos de LSP para configurar los túneles que nos ayudan con la Ingeniería de Tráfico, denominados TE-LSP's. Estos son E-LSP (*EXP-inferred LSP*) y L-LSP (*Label-only-inferred LSP*). Los L-LSP son los que pueden cargar un solo tipo de TA por LSP. Los E-LSP permiten múltiples TA's sobre una misma LSP.

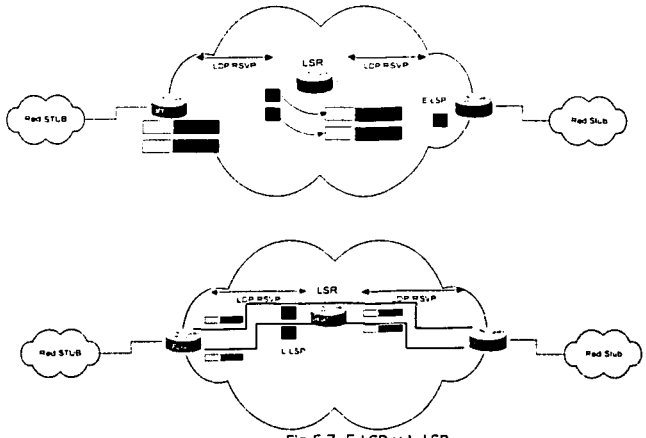


Fig 5.7. E-LSP y L-LSP

Las *EXP-Inferred-PSC LSPs (E-LSP)* tienen las siguientes características:

- La PHB es determinada únicamente por el campo EXP de la etiqueta de MPLS.
- No se requiere señalización adicional.
- Los LSRs mapean los valores EXP a los PHBs
- La liga entre Etiquetas y FEC son las que realizan las decisiones de direccionamiento, que pueden ser realizadas por los protocolos RSVP ó CBR-LDP.
- La relación EXP hacia PHB determina la clase de servicio y la procedencia de desecho de paquetes, todo realizado en cada LSR que son configurados para ello.
- Hasta 8 PHBs por LSP.

Las ventajas de las E-LSPs son:

- Múltiples PHBs (8) por LSP, con lo que se reduce el uso de etiquetas requeridas.
- Fácil de implementar, ya que solo se necesita configurar los LSRs para mapear los valores EXP a los PHBs.

Las desventajas de las E-LSPs son:

- Únicamente se pueden soportar hasta 8 PHB, sin embargo Diff-Serv soporta hasta 64 PHBs.
- No puede ser usado cuando un encabezado de conexión no es utilizado, como ATM.

Las *Label-Only-Inferred-PSC LSPs (L-LSP)* tienen las siguientes características:

- La PHB es determinada tanto por el campo EXP como por el campo donde se define la etiqueta.
- Se utiliza cuando se requieren más de 8 PHBs ó cuando no se requiere un encabezado de encadenamiento (ATM, FR, etc), y por esto el EXP no está habilitado.
- La señalización es por agendarización de grupos de PHB.
  - La liga entre la etiqueta y los TA{PSC}, direcciona hacia el siguiente salto y toma en cuenta el orden del TA.
  - Se realiza la decisión de direccionamiento y determina el PSC.
  - Puede ser realizada por los protocolos RSVP o bien CBR-LDP.
- La relación EXP hacia PHB determina la clase de servicio y la procedencia de desecho de paquetes, todo realizado en cada LSR que son configurados para ello.

Las ventajas de las L-LSPs son:

- Pueden soportar un número muy grande de PHBs (arriba de 64).
- Puede utilizar diferentes rutas para diferentes PHBs. Soporta relaciones de Ingeniería de Tráfico.

Las desventajas de las L-LSPs son:

- Consume una cantidad muy grande de etiquetas.
- Presenta una dificultad más o menos grande para su configuración, ya que se necesita configurar los protocolos de distribución de etiquetas para señalizar PHBs durante la distribución de las etiquetas.

La red puede tener definidos varios TA's a los cuales darles servicio. De esta manera se forman pares de FEC/TA{PSC} para la definición de la LSP correspondiente.

Una forma de hacer esto es no separar los conjuntos FEC/TA{PSC} teniendo así que cada Troncal de Tráfico llevará el tráfico de toda la TA/PSC. Esta opción es usada cuando se requiere instaurar mecanismos de Ingeniería de Tráfico sobre los ya existentes en MPLS. En ese caso, todas las FEC/TA{PSC} de cada FEC son enrutadas colectivamente sobre un conjunto de restricciones y seguirán así la misma ruta. El tipo de LSP que transporta este tipo de Troncal de Tráfico es la E-LSP.

Otra opción es separar los diferentes FEC/TA{PSC} de una determinada FEC en múltiples Troncales de Tráfico basadas en cada TA{PSC}, esto es, que el tráfico de un nodo determinado hacia otro, es separado en múltiples Troncales, basándose en sus clases de servicio, las cuales son transportadas sobre diferentes LSPs que pueden seguir distintas rutas sobre la red. Entonces es como DS-TE toma ventaja de esto, al procesar en la red STUB por separado cada LSP que le llega de la red de tránsito. Al hacer esto, DS-TE puede tomar en cuenta tanto los requerimientos específicos de cada troncal de tráfico transportada en cada LSP (por ejemplo, requerimientos de ancho de banda, prioridades, etc.), como las restricciones específicas que deben ser forzados para cada troncal de tráfico (por ejemplo limitar todas las Troncales de Tráfico transportando un {TA}PSC particular a cierto porcentaje de la capacidad del enlace). Esto nos da un mejor manejo para cada tipo específico de tráfico transportado en cada troncal, además que también sirve para balancear la carga de los enlaces.

En la red en la que estamos haciendo el estudio, se tiene soporte para 4 clases de servicio. Se necesita entonces hacer Ingeniería de Tráfico para balancear la carga de tráfico. Con los

mecanismos existentes de Ingeniería de Tráfico, la proporción de tráfico de un enlace dado variará dependiendo de los siguientes factores:

- El orden en el cual los diferentes TE-LSP's son establecidos.
- La prioridad preestablecida asociada a cada TE-LSP.
- Situaciones de falla del nodo ó enlace.

Esto hace que sea muy difícil configurar los Diff-Serv PHBs para asegurar un trato adecuado a cada clase de servicio. Esto conlleva a los requerimientos que se tienen para DS-TE para que se pueda forzar un determinado ancho de banda para una determinada clase de servicio.

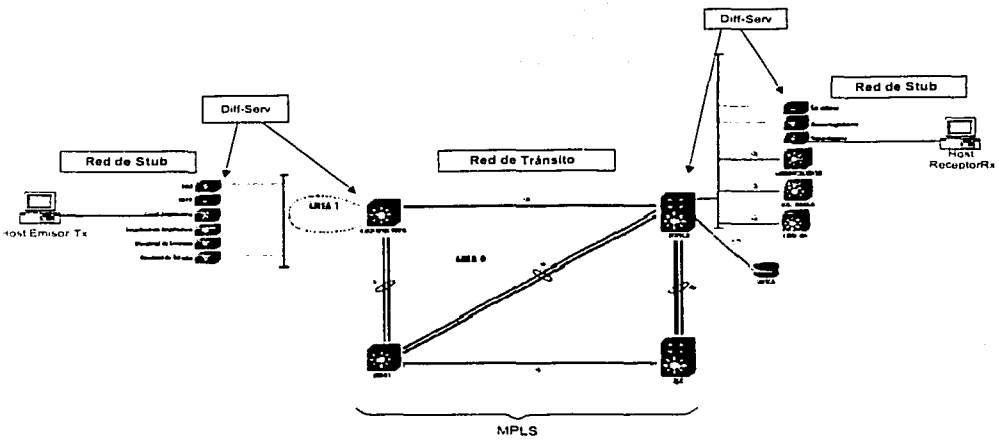


Fig. 5.8 RedUNAM con arquitectura Diff-Serv / MPLS

Entonces, se puede configurar la tasa de servicio de las colas de Diff-Serv para las clases de servicio definidas (Platino, Oro, Plata y Bronce).

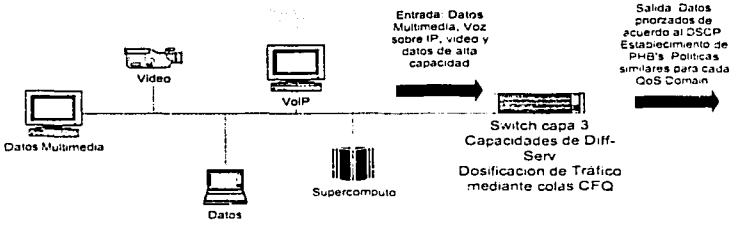


Fig. 5.9. Tráfico de entrada de un switch capa 3 de las redes de Stub dentro de un Dominio QoS.

Por lo tanto, se puede separar el tráfico entrante en diferentes Troncales de tráfico para cada clase de servicio y asociar el ancho de banda necesario para que cada LSP transporte dichas Troncales. También se configurarán, de acuerdo al PHB entrante que configura a cada LSP, prioridades para dar preferencia a las referenciadas con tráfico de clase de servicio Platino y Oro, y una preferencia menor a los de clase de servicio Plata. La clase de servicio bronce se tratará de la misma manera que las trata IP tradicional, dándoles un servicio tipo *mejor esfuerzo.*

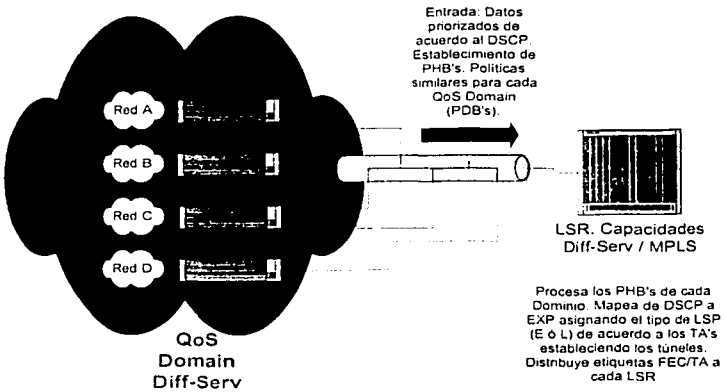


Fig. 5.10. Manejo de datos en la frontera Diff-Serv / MPLS

Entonces DS-TE puede asegurar que después de una falla, el tráfico de las clases de servicio Platino y Oro podrá ser re-enrutado con el principal acceso a la capacidad del enlace, pero sin exceder su tasa de servicio del ancho de banda que le corresponda. El tráfico de la clase de servicio Plata puede ser re-enrutada con el segundo mejor acceso a la capacidad del enlace pero sin exceder su tasa de servicio. Hay que hacer notar que para la clase de servicio Bronce, la de mejor esfuerzo, el requerimiento de DS-TE puede ser asegurar que la cantidad total de tráfico enrutado sobre todas las clases de servicio, no exceda el total de la capacidad del enlace.

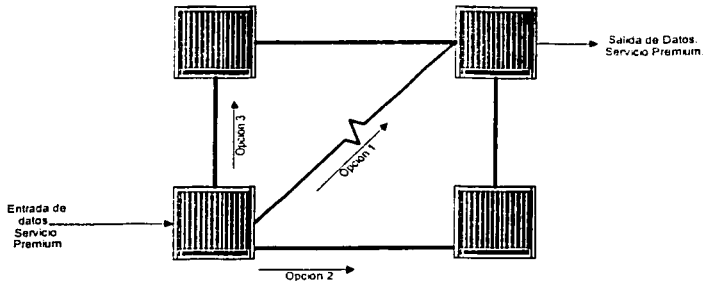


Fig.5.11. Tratamiento de los datos Tipo Premium en caso de falla de enlace.

Además de satisfacer estas clases de servicio, se puede también dar servicio de ancho de banda garantizado punto a punto. Esto conlleva a que se necesita:

- Dedicar un PHB para el tráfico que se necesita garantizar.
- Políticas de tráfico garantizado en el punto de ingreso contra contratos de tráfico y la marcación de los paquetes con el correspondiente valor de DSCP/EXP.

Donde se necesite un alto nivel de PDB para garantizar cierto servicio, puede ser necesario asegurar que la cantidad de tráfico garantizado permanezca por debajo de cierto porcentaje de la capacidad total del enlace. Donde la proporción de tráfico garantizado es alta, el CBR puede ser usado para forzar las restricciones correspondientes, que además de ayudar a dar servicio a este tipo de tráfico, también nos ayuda a darle Ingeniería de Tráfico al tráfico restante.

En el caso de nuestro estudio, la RedUNAM solo definirá un PDB para MPLS, este será definida en el área cero de OSPF, que es donde se encuentra la parte primordial del core, ya que las demás áreas estarán trabajando con Servicios Diferenciados, excepto dos.

El área cinco de OSPF en la red UNAM, en el nodo de Zona Cultural del core, es donde se encuentran definidos los enlaces externos de la red UNAM como lo vimos en el capítulo anterior, es decir, los enlaces WAN. En este caso, como no sabemos realmente que tipo de mensajes de ingeniería de tráfico lleguen por ese punto, se ha definido que también esos equipos sean capaces de manejar las ternas de etiqueta/interfaz y serían definidos como LER's (ya que los equipos definidos en esa área son enrutadores) debido a que conectarían el tráfico MPLS que saliera de Red UNAM (con los PHB's asociados dependiendo de la diferenciación de servicios que se requiriera hacer) con las redes externas de la UNAM o bien de Internet.

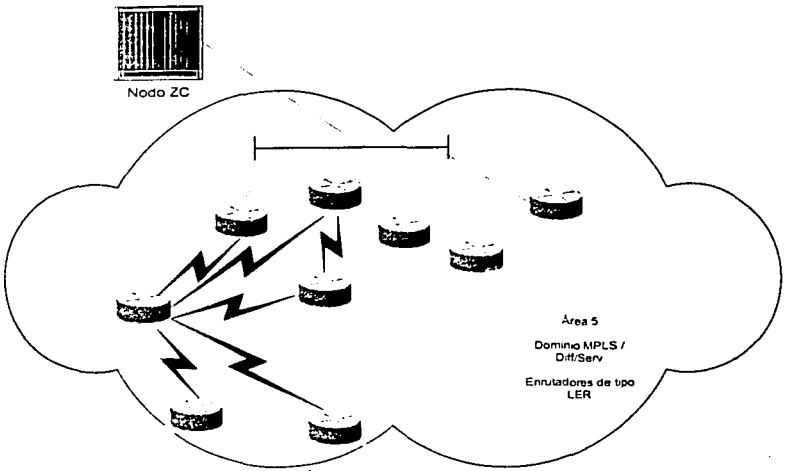


Fig. 5.12. Área 5. Dominio QoS con enlaces WAN.

En el área seis esta definida la parte también utilizará MPLS en ella, ya que se definen equipos de Internet 2 (con IPv6), que como en el área 5 estarán conectados a redes externas con señalización de tipo MPLS. Debido a que IPv6 cuenta con capacidades para soportar RSVP, ésta también es una razón para utilizarlo como protocolo de distribución de etiquetas. Aunque en realidad estos equipos estarán aislados de la red actual IPv4, en un futuro se planea que las redes trabajen de forma paralela, y no solo la parte experimental que trabaja actualmente.

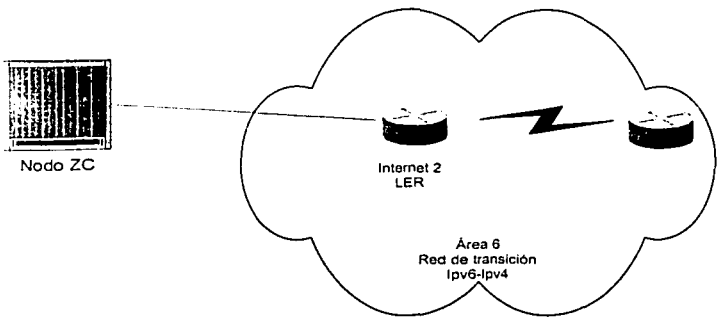


Fig. 5.13. Área 6. Dominio QoS de transición Ipv6-Ipv4

Manejo de colas.

Dado que en los modelos que estamos presentado se utilizan servicios diferenciados, recomendamos utilizar CBQ ó encolamiento basado clases, donde este tipo de mecanismo de colas está basado en las clases de tráfico. El tráfico se clasifica en clases y según estas se asigna a una cola y nos permite también asignar anchos de banda de manera dinámica o estática.

5.1.2. Caracterización del tráfico de la Red.

La caracterización de la red esta desarrollada en el Capitulo *IV. Descripción y necesidades de Calidad de Servicio en el Backbone de RedUNAM.*

5.1.3. Monitoreo de Red.

5.1.3.1. Administración y monitoreo de la RedUNAM con QoS.

Una vez que se tenga en operación la red con calidad de servicios, es muy importante tener mecanismos de administración y monitoreo, los cuales nos proporcionarán información importante: como verificar el buen funcionamiento de la RedUNAM, los problemas presentados durante y después de la implementación, dando pauta para que se hagan los cambios necesarios para corregir los problemas, así también, prever el crecimiento y tendencias de tráfico y nuevas necesidades de los usuarios universitarios. Entre otros posibles eventos están las fallas ocasionales debido a problemas de hardware, fallas de electricidad, cortes de cables, fibras, bugs en el software de los dispositivos y nuevas implantaciones de software.

Actualmente se tiene establecido ya en la RedUNAM un esquema de administración y monitoreo, al cual deberán integrarse los nuevos equipos del backbone QoS. Dicho esquema esta basado en el modelo de administración de redes ISO, el cual está formado por cinco áreas conceptuales:

- Administración del desempeño.

  Se manejan herramientas generalmente gráficas que permiten medir el funcionamiento de la red en tiempo real y con históricos. Con estas herramientas también podemos verificar el funcionamiento de un dispositivo en particular en relación con la red, los tiempos de respuesta y el porcentaje de utilización de un enlace.

- Administración de configuración.

  Se mantiene la información de los equipos que conforman la red, como son: versiones de los sistemas operativos, tipos de interfaces, protocolos de enrutamiento utilizados, etc., que ayuda a detectar posibles problemas en versiones de software ó conflictos entre ellas. Así, cuando ocurre un problema se cuenta con la información disponible para su pronta solución.

  Para configurar los equipos que forman parte de la red, se pueden utilizar varios métodos, entre ellos: la interfaz de comandos en línea (CLI), por medio de interfaces Web, software que maneja el protocolo SNMP ó un software propietario basado en un sistema de ventanas. La configuración se realiza en su mayoría por medio de la línea de comandos.

- Administración de contabilidad.

  Esta área está estrechamente ligada con la administración del desempeño, ya que se obtienen parámetros de utilización de la red. Permitiendo aislar los puntos de mayor tráfico y darles un tratamiento especial.

- Administración de fallas.

  Por medio de bitácoras se detectan los posibles orígenes de las fallas de red y proceder a arreglar los problemas para mantener a la RedUNAM en operación.

- Administración de seguridad.

  En esta área se utilizan herramientas que restringen el acceso a los dispositivos desde ciertos puntos de la red y con autentificación de usuarios por medio de *logins* y *passwords* a los operadores de los mismo. También se guardan los accesos en bitácoras para establecer un control de los accesos a los equipos. La administración de los dispositivos es realizado por el Centro de Asistencia Técnica y el Centro de Operación de la Red.

Para realizar las tareas mencionadas con anterioridad se hace mano de las siguientes herramientas, las cuales deberán ser manejadas por lo nuevos dispositivos de red que formarán parte de la RedUNAM QoS:

5.1.3.2. MRTG. (Multi Router Traffic Grapher)

Por su significado en inglés Multi Router Traffic Grapher, MRTG es una herramienta gratuita que nos permite monitorear la carga de tráfico en la red y sus enlaces. Genera páginas HTML que contienen gráficas creadas en tiempo real e históricas que representan el tráfico.

Algunos de los motivos por los cuales RedUNAM utilizó como una alternativa de solución la implementación y el uso del MRTG fue debido a que en éste encontró las siguientes características:

- Es una aplicación gratuita.
- Es portable. Trabaja sobre la mayoría de las plataformas UNIX y Windows NT.
- Está escrito en *Perl* y viene con la fuente completa, lo cual facilita la configuración de la herramienta para la obtención de mayor información estadística.
- Usa una implementación de SNMP altamente portable escrita completamente en Perl. No es necesario instalar ningún paquete de SNMP externo.
- Cuenta con soporte para SNMPv2c, ya que puede leer los nuevos contadores de 64 bits de SNMPv2c.
- Las interfaces de los enrutadores pueden ser identificadas por su dirección IP, descripción y dirección Ethernet, además del número de interfaz normal.
- Las bitácoras de Logs son de tamaño constante, es decir, NO crecen, ya que el MRTG cuenta con un algoritmo de consolidación de datos.
- Los gráficos mostrados por el MRTG son libres de GIF, ya que son generados directamente en formato PNG.
- Los gráficos son mostrados en páginas Web, las cuales son producidas por el MRTG y son altamente configurables.

El MRTG consiste en un programa en Perl que usa SNMP para leer los contadores de tráfico de sus enrutadores y de un rápido programa de C el cual archiva los datos de tráfico y crea imágenes que representan el tráfico en la conexión de red que es monitoreada. Esos gráficos se insertan en páginas Web que pueden ser vistas desde cualquier *browser.*

Además de una vista diaria detallada, el MRTG crea también representaciones visuales para el tráfico de los últimos siete días, las cuatro últimas semanas y los últimos doce meses. Esto es posible pues el MRTG mantiene un archivo de todos los datos que ha obtenido del enrutador. Este archivo es consolidado automáticamente, así que no crece con el tiempo, pero contiene todos los datos relevantes del tráfico de los últimos dos años. MRTG puede monitorear 200 ó más enlaces de red desde cualquier máquina UNIX .

El MRTG no está limitado al monitoreo de tráfico, es posible monitorear cualquier variable de SNMP que se elija. Se puede usar un programa externo para recolectar datos que serán monitoreados por el MRTG. Por ejemplo se pueden monitorear cosas como Carga del Sistema, Inicio de Sesiones, disponibilidad de módems y más. Además MRTG permite acumular dos o más fuentes de datos en un único gráfico.

La utilización del MRTG en la RedUNAM únicamente es configurado para el monitoreo de enlaces LAN y WAN.

Actualmente se cuenta con un equipo Sun Ultra 10, con Disco Duro de 5 GB y 250 MB de memoria RAM.

Una de sus grandes desventajas es que consume gran cantidad del procesador de la máquina residente.

A continuación presentamos gráficas que ejemplifican su funcionamiento y utilidad:

Gráfica diaria (5 minutos Promedio)

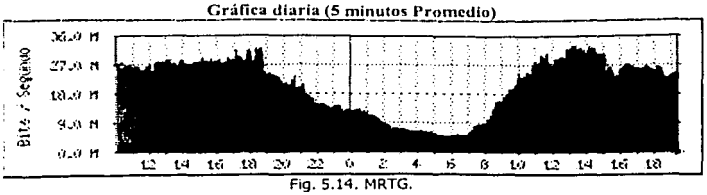


Fig. 5.14. MRTG.

Máx Entrante:	33.2 Mb/s (33.2%)	Promedio Entrante:	20.7 Mb/s (20.7%)	Actual Entrante:	23.3 Mb/s (23.3%)
Máx Saliente:	27.5 Mb/s (27.5%)	Promedio Saliente:	11.6 Mb/s (11.6%)	Actual Saliente:	13.0 Mb/s (13.0%)

Tabla 5.4.

Gráfica semanal (30 minutos Promedio)

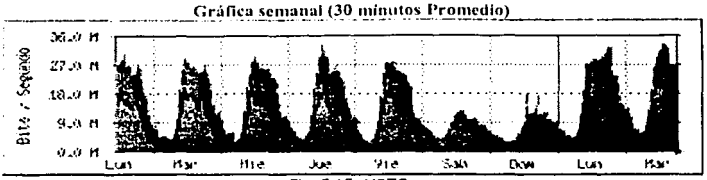


Fig. 5.15. MRTG.

Máx Entrante:	33.4 Mb/s (33.4%)	Promedio Entrante:	14.0 Mb/s (14.0%)	Actual Entrante:	25.7 Mb/s (25.7%)
Máx Saliente:	28.0 Mb/s (28.0%)	Promedio Saliente:	7617.8 kb/s (7.6%)	Actual Saliente:	16.9 Mb/s (16.9%)

Tabla 5.5.

Gráfica mensual (2 horas Promedio)

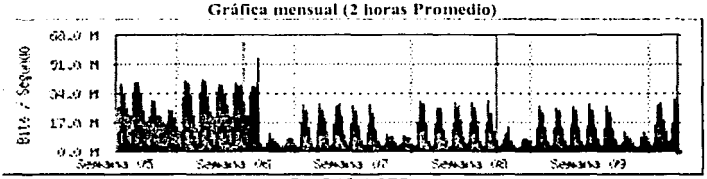


Fig. 5.16. MRTG.

Máx Entrante:	64.4 Mb/s (64.4%)	Promedio Entrante:	17.0 Mb/s (17.0%)	Actual Entrante:	26.1 Mb/s (26.1%)
Máx Saliente:	21.4 Mb/s (21.4%)	Promedio Saliente:	6917.6 kb/s (6.9%)	Actual Saliente:	14.8 Mb/s (14.8%)

Tabla 5.6.

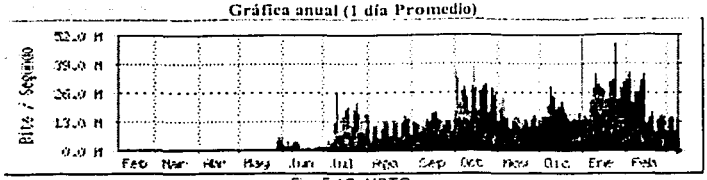


Fig. 5.17. MRTG.

Máx Entrante:	48.2 Mb/s (48.2%)	Promedio Entrante:	10.7 Mb/s (10.7%)	Actual Entrante:	14.5 Mb/s (14.5%)
Máx Saliente:	21.0 Mb/s (21.0%)	Promedio Saliente:	5233.5 kb/s (5.2%)	Actual Saliente:	7756.8 kb/s (7.8%)

Tabla 5.7.

5.1.3.3. Spectrum.

SPECTRUM es una aplicación avanzada de software para la administración de redes, que permite monitorear de forma confiable el estado de los diferentes dispositivos existentes en la red.

Esta poderosa herramienta nos permite establecer un sistema de alarmas mediante un modelo representativo de la red. Éste sistema basa su monitoreo en *poleos* a los dispositivos de red que manejan el protocolo de administración SNMP. Para realizar ésta tarea, Spectrum cuenta con una herramienta llamada *Alarm Mannager*, misma que es utilizada por el personal del Centro de Operación de la Red para administrar y monitorear el core y los enlaces WAN de la RedUNAM, ya que provee una vista dinámica de las alarmas presentes en la red y permite realizar las siguientes operaciones:

- Ver y seleccionar múltiples alarmas.
- Realizar una acción en una alarma o conjunto de alarmas, tal como:
  - Asignar o de-asignar alarmas a troubleshooters, limpiar, realizar acknowledge o Unacknowledged de las alarmas, establecer el estatus de las alarmas, etc.

- Establecer un criterio para filtrar alarmas que serán desplegadas.
- Filtrar alarmas por: *Model Type, Model, Date/Time, Address, Model Class, Severity, Cause, Assignment* y *State*.
- Ordenar las alarmas en base a *Severity, Date/Time, Model Type*, etc.

Cabe mencionar que una alarma es generada cuando una entidad de red que está modelada en la Base de Datos del Spectrum no está funcionando normalmente.

La condición de los modelos se representa mediante un código de colores, que se verá reflejado en el icono del modelo y que éste identificará el estado del mismo.

Los colores asociados con el estado del modelos son:

- Azul. Estado inicial (reconocimiento del dispositivo).
- Verde. Indica que el contacto con el dispositivo ha sido establecido y no existen problemas en el modelo.
- Amarillo. Indica que se ha detectado un problema menor, que no afecta al desempeño en general de la red.
- Naranja. Indica que se ha detectado un problema mayor en la red.
- Rojo. Indica que se ha detectado un problema crítico en la red.
- Gris. Indica que el estado del dispositivo es desconocido.

Otra herramienta de Spectrum muy importante y que es utilizada por el personal del Centro de Operación de la Red, es la llamada *Report*. Con esta herramienta se pueden obtener datos significativos para el desempeño actual y futuro de la red, es decir, se pueden obtener estadísticas tanto preventivas como correctivas de algún problema, aplicando el conocimiento y la experiencia del personal del COR, misma que será apoyada con los datos obtenidos de esta herramienta.

Los reportes pueden proveer información como la que se muestra a continuación:

- Información acerca de alarmas activas en el *Alarm Manager* y una tabla con las posibles causas de cada alarma y las acciones recomendadas para su corrección.

- Información sobre los eventos de actividad de la red recolectados por Spectrum. Estos reportes incluyen un historial del comportamiento de modelos específicos o grupos de modelos del *Event Log*.
- Inventarios que muestran de forma detallada información de tarjetas e interfaces individuales de dispositivos multi-slot. Los reportes de inventarios pueden arrojar información tanto de software como de hardware.
- Información del desempeño de la red y sus dispositivos, mediante datos como: carga, rango de paquetes, rango de errores, paquetes descartados, etc.
- Despliegan información de las veces en las que se perdió contacto con un dispositivo y cuando éste fue reestablecido. El reporte también calcula la cantidad de tiempo en la que el dispositivo estuvo arriba o abajo.

Esta herramienta de monitoreo puede trabajar en plataformas como UNIX y Windows NT. El Centro de Operación de la Red cuenta con un servidor UNIX con Sistema Operativo Solaris versión 2.7 con capacidades en hardware como Procesador a 400 MHz, 2 Discos Duros de 18 GB cada uno y 1 GB en memoria RAM. Actualmente se tiene instalada la plataforma Spectrum en la versión 5.0.1.

La UNAM cuenta con un solo servidor y un cliente gráfico mediante el cual los miembros del COR se comunican a la plataforma y de ésta manera realizar las peticiones pertinentes de lo que se desee obtener de la herramienta.

En las figuras siguientes mostramos la representación de una red con Spectrum:

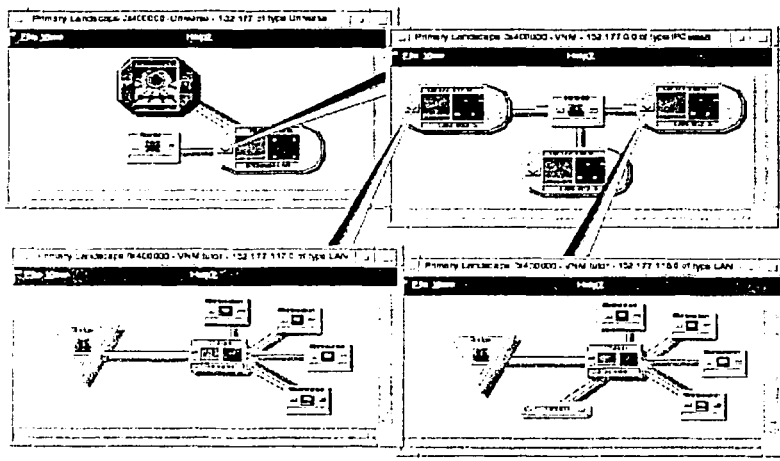


Fig. 5.18 Red con Spectrum.

5.1.3.4. Transcend Enterprise Manager.

Es una herramienta de configuración, administración y monitoreo propietaria de 3Com. Trabaja en sistemas operativos Windows mediante el poleo de dispositivos capaces de manejar protocolo de administración SNMP. Transcend para funcionar utiliza la plataforma HP Openview que nos sirve para modelar nuestra red.

De hecho la herramienta Transcend es un conjunto de módulos que pueden ser utilizados por separado, como son: *Device view*, la cual nos presenta una representación gráfica de las conexiones del equipo; *LANsentry Reporter*, nos permite generar reportes cuando se monitorea algún equipo de red; *upgrade manager*, permite actualizar el sistema operativo de los dispositivos, etc.

Esta herramienta es muy utilizada por el Centro de Asistencia Técnica, área que tiene asignada la tarea de monitoreo, configuración y administración de los equipos 3Com, principalmente los Lanplex 2500 que se encuentran en las capas de distribución y acceso de la RedUNAM y los Cellplex (equipos que fueron eliminados del backbone durante la migración al actual backbone de la RedUNAM).

A continuación presentamos algunas gráficas de esta herramienta de administración y monitoreo:

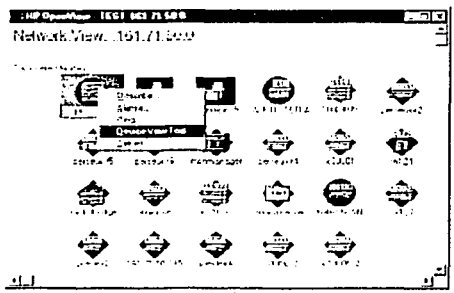


Fig. 5.19. Trancend Enterprise Manager.

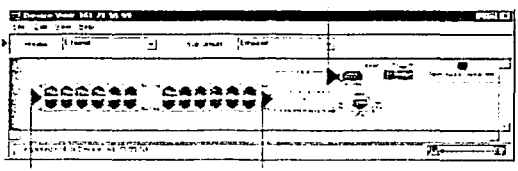


Fig. 5.20. Trancend Enterprise Manager.

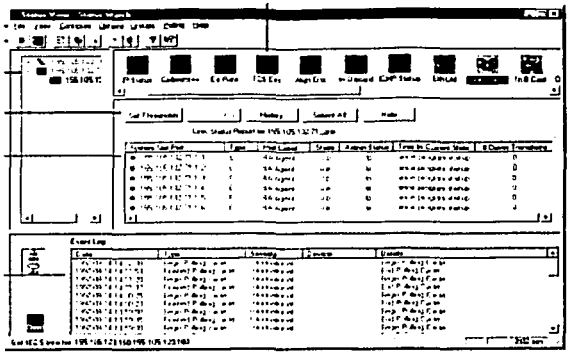


Fig. 5.21. Trancend Enterprise Manager.

CONCLUSIONES.

El aseguramiento del servicio para ciertas aplicaciones y ciertos usuarios dentro de una red educativa tan importante como lo es Red UNAM se vuelve cada vez una tarea con mayor prioridad. A continuación presentamos las conclusiones del presente análisis.

El punto base para la implementación de una arquitectura de Calidad de Servicio es la definición e implementación de las políticas para el aseguramiento del comportamiento del tráfico dentro de la red. Si este trabajo se encuentra bien establecido, el modelo definido que se utilizará para este aseguramiento será mucho más fácil de implementar, ya que las reglas de los protocolos utilizados son basadas en estas políticas tanto para definir medios de trabajo (Diff-Serv), el establecimiento de túneles (MPLS) o bien la reservación de recursos (RSVP)

Las políticas para el caso de RedUNAM que se presentaron en el capítulo 5 son aplicables a cualquiera de los dos modelos indicados y durante la implementación surgirán nuevas políticas, de hecho estas estarán cambiando con cierta regularidad porque dependen de las necesidades y el crecimiento de la red.

La arquitectura de Calidad de Servicio que proponemos, de acuerdo a las necesidades y recursos con los que cuenta Red UNAM, es la de utilizar Diff-Serv en la red de distribución, que es la que se encarga de conectar a los usuarios finales con el core; mientras que en la red de core utilizaremos MPLS. Cabe destacar que en éste momento, solo los equipos Net Iron soportan MPLS y solo como LER, ya que no pueden administrar ni distribuir etiquetas, sin embargo (según el fabricante) solo se requeriría una actualización de software para tener MPLS completamente operativo.

El porqué de utilizar esta arquitectura sobre la otra estudiada en el capítulo pasado (RSVP en la distribución y Diff-Serv en él core), es que presenta las siguientes ventajas de acuerdo a nuestro punto de vista:

- En la red de distribución ó STUB, Diff-Serv presenta una mayor cantidad de opciones para la clasificación de tráfico (64 tipos de acuerdo a los DSCP's) que transita por la red además de darnos la definición de las PHB's correspondientes. Estos PHB's también incluyen la parte de información del usuario y la priorización de acuerdo a este, por lo que permite una mejor interacción con la red de *core* llegando a estas las características de cada uno de los flujos de tráfico entrantes (agregados de tráfico) En cambio, RSVP solo tiene dos tipos diferentes de tráfico (Servicio Garantizado y el Servicio de Carga Controlada), así como también requiere una mayor cantidad de memoria y tiempo de procesamiento dentro de los enrutadores.

- En la red de *core* o TRANSITO, MPLS permite establecer túneles mapeando las clases de servicio definidas en los PHB's de Diff-Serv (DSCP) a los PHB's de MPLS (EXP) pudiendo transportar un solo tipo de TA's (L-LSP's) o bien permitir varios TA's sobre una misma LSP (E-LSP's) de acuerdo a las FEC's definidas. Debido a las características intrínsecas de una red de *core*, donde la cantidad de tráfico en tránsito es muy grande debido a que en ella convergen las redes de distribución asociadas, se requiere el establecimiento de rutas cortas para la interconexión de estas, además de que el tiempo de procesamiento de los equipos intermedios involucrados en los saltos debe ser el menor posible. Esto nos lo proporciona MPLS con el uso de etiquetas y los protocolos de distribución de las mismas (que para nuestro caso, utilizaremos RSVP, aunque CBR-LDP también podría trabajar muy bien de acuerdo a la configuración de esta red, por lo que es indistinto, pero los equipos de core utilizados en la red ya soportan RSVP), estableciendo las LSP's correspondientes dependiendo de los PHB's entrantes de las redes convergentes. MPLS al detectar el tipo de PHB entrante le asigna un TA, después define él o los túneles LSP's tipo L ó E mediante una asociación del tipo de flujo a etiquetas que el LSR asociará al siguiente salto, ahorrando de esta manera una gran cantidad de tiempo de procesamiento. En cambio, Diff-Serv por el variado número de opciones en la clasificación del tráfico así como él tener que ir hasta el encabezado IP para detectar la quíntupla para diferenciar el tráfico (Dirección IP origen, Dirección IP destino, Puerto Origen TCP, Puerto Destino TCP y el protocolo de Transporte) además de los DSCP's definidos en el campo DS, resultando poco práctico a este nivel.

- Por la configuración de Red UNAM, necesitaríamos MPLS en el core, ya que en dos de los dominios QoS definidos (áreas 5 y 6 de OSPF, ambas definidas sobre los equipos de Zona Cultural), se presentan la mayor parte de los enlaces externos (tipo WAN con enlaces de baja velocidad tipo E1, área 5), además de la conexión con la red Internet 2 (área 6), ambas redes con uso masivo de TA's para la definición de LSP's hacia la Red UNAM, por lo que sería necesario mantener equipos con capacidad de manejo de este tipo de tráfico para su correcta distribución dentro del campus. De esta manera lograríamos el primer paso para extender la Calidad de Servicios del backbone RedUNAM a las redes WAN tanto internas como externas. Esto quiere decir que el backbone estará listo para que las redes WAN internas que contengan equipo capaz de manejar servicios diferenciado o que estén en proceso de cambio o actualización del mismo en un primer paso puedan beneficiarse de las ventajas del modelo propuesto.

Se pueden resumir las ventajas y desventajas de las dos arquitecturas en la siguiente tabla:

	RSVP / Diff-Serv	Diff-Serv / MPLS
Variedad de Clasificación de Tráfico	Baja	Alta
Asignación de comportamientos de acuerdo al tipo de usuario en asociación con el tipo de tráfico.	No	Si
Capacidad de envío de tráfico similar sobre la misma ruta	No	Si
Tiempo de procesamiento dentro de los enrutadores	Alto	Bajo
Escalabilidad	No	Si
Métodos de Ingeniería de Tráfico.	No	Si

Si se implementa este modelo dentro de la RedUNAM podría ser bastante benéfico y hacer que el comportamiento de la red actual cambie. Aunque a simple vista se podría decir que sin esta arquitectura no podríamos presentar problemas con los servicios que necesitarán un tratamiento especial de calidad de Servicio, ya que el ancho de banda existente podría ser suficiente, necesitamos pensar a mediano plazo que es cuando esta arquitectura ya podría estar en estado operativo.

En primera instancia, los servicios emergentes cada vez requieren de mayor ancho de banda, por lo que servicios como videoconferencia, video sobre demanda, voz sobre IP (que de hecho, sería uno de los servicios con mayor demanda, ya que se podría decir que de cada 3 extensiones telefónicas, 2 están a lado de una computadora y por tanto podrían ser sustituidas) y otros servicios, por lo que se requiere que se tanga preparada la red para que la calidad de la red en cada servicio no se vea aminorada.

Por otra parte, la red UNAM no solo involucra la red dentro del Campus. Existe una basta cantidad de enlaces de tipo WAN (más de 100, alrededor de 30 internos de la UNAM y más de 80 hacia otras instituciones tanto dentro como fuera del país) que tienen en poca o gran medida interacción con la red del Campus. En estos enlaces el ancho de banda es extremadamente limitado por lo que se necesita que la arquitectura que ya definimos alcancen estos puntos. Las redes externas están confluyendo hacia una arquitectura de Ingeniería de tráfico basada en MPLS o bien en Diff-Serv, por lo que lo más probable es que los datos que vengan del exterior contengan formatos basados en etiquetas o referidas a algún PHB conocido, por lo que el arribo a la red del Campus será como si viniera de una de las redes de distribución, ya sea tráfico MPLS o Diff-Serv, ya que todos los enrutadores conectados a estos enlaces WAN serán capaces de reenviar ambos.

Además, los enlaces que se tienen hacia la red I2 basada en Ipv6 también estarán basada en Diff-Serv, ya que su capacidad para los DCSP es mayor que los de Ipv4. Y todos los enrutadores involucrados podrán definir y reenviar las etiquetas necesarias para la operación de MPLS. La tendencia es que I2 sea una red paralela a la red Ipv4 actual, por lo que todos los enrutadores involucrados deben de ser capaces de utilizar los mismos protocolos.

Debido a las necesidades de software y hardware para establecer esta arquitectura dentro de la Red UNAM, sería necesario el cambio de algunos de los equipos. Aclaramos que la propuesta no forzosamente está ligada al equipamiento suministrado por algún fabricante en especial, por lo que se tendrá varias opciones a elegir según el presupuesto con que cuente la Dirección General de Servicios de Cómputo Académico, la facilidad de manejo y aprendizaje de nuevos comando o en su caso un nuevo sistema operativo para el personal de la subdirección de redes. Sin embargo, el

alcance de este trabajo es definir las características básicas y compatibilidades que el equipo debe de tener (ya sea de los cambios propuestos o bien de los que no se cambiarán).

En lo que respecta al cambio de equipos que se proponen debido a que los instalados actualmente no cumplen los requerimientos básicos, éste se realizará en dos niveles del modelo de redes:

Para la capa de distribución:

- Se requiere el cambio de los switches capa 2 que actualmente trabajan en esta red (Corebuilder's 2500 y 3500) ya que no soportan Diff-Serv ni algún tipo de encolamiento de pueda ayudar a la implantación de Calidad de Servicios para el usuario final.
- Cambiar por equipos que manejen servicios diferenciados, tipos de encolamiento WFQ o por lo menos CBQ, también llamado encolamiento personalizada; algoritmo tipo RED, el cual se encargará de manejar el tráfico en casos de congestión.

Para la capa de core:

- Los equipos Net-Iron actuales (nodos Zona Cultural y DGSCA) soportan tanto MPLS (sin embargo, como ya mencionamos, se requiere una actualización de software) como Diff-Serv.
- Los equipos Big-Iron actuales (nodos Arquitectua e IIMAS) no soportan MPLS, por lo que se recomienda hacer crecer estos equipos ya sea en software o hardware a las mismas características de los Net-Iron.

Además de estos cambios, se necesita instalar una estación de trabajo UNÍX donde resida el servidor de políticas, el PDP y el PEP. Este debe ser capaz de conectarse a cada uno de los equipos componentes de la red, por lo que se recomienda resida en la misma red en la que se tengan los equipos de monitoreo. Uno de estos servidores será el PEP de la red que será el encargado de hacer valer cada una de las políticas de los equipos y un PDP que nos ayudará a verificar y decidir sobre las políticas definidas. Como vimos en el capítulo 3, estos dos servidores pueden residir físicamente en el mismo equipo. Estos tendrán que estar conectados al servidor de políticas y de autenticación (que pueden también estar en el mismo equipo) para la correcta aplicación de las mismas dentro de la red.

Debido a la complejidad del proyecto que involucra a las implementaciones necesarias en los equipos existentes y en el cambio de equipamiento que se está proponiendo porque sus características no cumplen de manera óptima las necesidades de este, se necesita hacer una segmentación del mismo para ser realizado en varias etapas.

La primera etapa sería hacer los cambios necesarios en la red de tránsito (equipos *Foundry*), ya que estos son el corazón por donde todos los datos circulan para intercomunicar los diferentes dominios. En estos se tendrían que habilitar las funciones necesarias para MPLS, el protocolo de distribucion de etiquetas, y las tablas necesarias para el mapeo de PHBs y PDBs de Diff-Serv.

La segunda etapa es integrar las capas 5 y 6 al proyecto, ya que como hemos mencionado contienen tanto los enlaces WAN hacia las instituciones externas y las que se encuentran fuera del campus, así como la red I2. De esta manera se tienen que configurar todos los enrutadores con las listas de Diff-Serv. Además el área 6, también tendrá habilitado MPLS, este tendrá que ser activado y en operación con la red de tránsito.

La tercera etapa es ir habilitando Diff-Serv en los demás dominios, empezando con los que se encuentran conectados al nodo DGSCA, después al nodo IIMAS y al nodo ZC.

ANEXO A.

1. OSPF (OPEN SHORTEST PATH FIRST)

OSPF es un protocolo de estado de enlace y de dominio público, definido en el RFC 2178.

El protocolo de enrutamiento OSPF esta basado solamente en la dirección IP destino que se encuentra en el encabezado del paquete IP. OSPF es un protocolo de enrutamiento dinámico, el cual detecta rápidamente los cambios topológicos en el Sistema Autónomo y recalcula nuevas rutas libres de *loops* después de un periodo de convergencia muy corto. En OSPF cada enrutador mantiene una base de datos, la cual describe la topología del Sistema Autónomo que es idéntica a la de los vecinos a través de anuncios llamados Estado de Enlace ó "Link State" que transportan dicha información, la cual se propaga a través del Sistema Autónomo. Todos los datos, construyen el "Shortest-Path Tree" ó STP (árbol con las rutas más cortas) tomándose a el mismo como raíz ó punto de inicio. El árbol resultante dependerá directamente del enrutador desde el cual se realice el cálculo. Una vez calculado el árbol, la información se enviará 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.

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 tráfico de enrutamiento, reducción en el procesamiento de los enrutadores, etc.

Cada ruta distribuida por OSPF tiene una dirección IP destino y una máscara de red. Dos subredes dentro de una misma red pueden tener diferentes tamaños, es decir, diferentes máscaras de subred. Por ejemplo, en el caso de que existan dos rutas para un mismo destino, el paquete se enrutará por el mejor camino o bien por la ruta más especifica.

Todos los intercambios de paquetes de Estado de Enlace dentro del protocolo OSPF son autenticados por medio de contraseñas, esto significa que sólo los enrutadores autorizados dentro del Sistema Autónomo pueden participar en el enrutamiento de información.

OSPF soporta los siguientes tipos de redes:

- Redes punto a punto. Es una conexión entre dos enrutadores a través de una línea serial.
- Redes Broadcast. Son redes que soportan más de dos conexiones de enrutadores con la capacidad de mandar un mensaje hacia todos los equipos conectados.
- Redes No-Broadcast. Soportan más de dos conexiones de enrutadores, pero este tipo de redes no tiene la capacidad de mandar mensajes tipo broadcast, en su lugar utilizan mensajes de tipo multicast.

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

La vecindad de cada nodo de la red depende si se 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 representan 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.

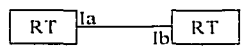


Fig. a.1. Topología de enlace punto a punto.

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

Tabla a.1. Base de Datos Topológica de enlace punto a punto

Cuando múltiples enrutadores se conectan a una red multiacceso, en la tabla se representan conectadas con un vértice en la red bidireccional.

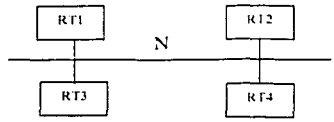


Fig. a.2. Red Multiacceso.

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

Tabla a.2. Topología de Red Multiacceso

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

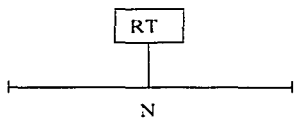


Fig a.3. Topología de red Multiacceso Stub

	Origen	
Destino	RT2	N3
RT2		
N3	X	

Tabla a.3. 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.

a) Enrutamiento Jerárquico.

OSPF permite implantar un esquema modular y jerárquico de enrutamiento de información. A éste esquema modular de OSPF se le nombra área.

b) Áreas en OSPF.

Un anuncio de estado del enlace, 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 del estado de los enlaces 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* (datos generados por los anuncios de estado de enlace) y calcular el algoritmo *Shortest 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 enrutadores hacia fuera del área a la que pertenecen. Esta ocultación de información tiene fines de seguridad dado que la topología de un área nunca será conocida por enrutadores 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 en caso de pertenecer a diferentes áreas se llama inter-área. Podemos encontrar diferentes tipos de áreas, como son:

i) Área Backbone o Área Cero.

En el caso de existir más de dos áreas, una de las áreas deberá ser área cero (también llamada 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 turno. 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 enlaces virtuales.

Un enlace virtual puede ser configurado entre dos enrutadores que posean unas 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 enrutadores conectados por enlaces virtuales como conectados en un enlace de punto a punto con métrica de cero. El tráfico entre enlaces virtuales usa un 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 caso del enrutamiento Intra-área, se puede describir el proceso de enrutamiento en tres partes:

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

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

ii) Área Stub.

En algunos Sistema 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. 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 por área. Esto reduce significativamente el tamaño de las bases de datos topológica y por lo tanto los requerimientos de memoria y procesador de los enrutadores.

2. 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:

a.) 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.

b) 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 conectados 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.

c) Enrutador de Backbone (*Backbone Router*) BR.

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

d) Enrutador de Frontera de Sistema *Autónomo (AS Boundary Router)* ASBR.

Es aquel 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. 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.

e) Adyacencias.

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 su Enrutador Designado (*Designated Router, DR*), y uno más para ser el Enrutador Desigando de Respaldo (*Backup Designated Routerm, BDR*). El BDR se elige como un mecanismo de respaldo en caso de que el DR falle. El objetivo 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 reenviarán la información a los demás enrutadores del segmento a través de las direcciones multicast AllSPFRoutrs (224.0.0.5) y AllDRouters (224.0.0.6).

i) 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. Tanto el DR como BDR se utilizan para segmentos de red multiacceso.

ii.) DR y BDR.

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 anuncia DR si tiene el Prioridad de Enrutador más alta.

El DR es el punto final de muchas adyacencias. Para optimizar el funcionamiento de las redes tipo broadcast, el DR manda mensajes multicast de actualización de estado de enlace 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 Avisos de enlace de redes (*Networks Link Advertisements*) Estos anuncios listan el grupo de enrutadores (incluido él mismo) actualmente unidos a la red. El Identificador de Estado de Enlace (*Link State ID*) para este anuncio es la dirección 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 del Estado de Enlace 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.

f) Enrutador Designado de Respaldo (Bakup Designated Router, BDR)

Para hacer más rápida la transición de un DR a otro nuevo, existe uno 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.

g) 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 pasar los enrutadores antes de obtener la adyacencia.

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

2. 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*.

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

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

5. EXSTART. Los enrutadores tratan de establecer el Número de Inicio de Secuencia que va a ser utilizado para el intercambio de paquetes de información. Este número de secuencia asegura que los enrutadores siempre obtengan la información más reciente.

6. EXCHANGE. Los enrutadores describirán su base de datos topológica enviando los Paquetes de Descripción de la Base de Datos. En este punto, los paquetes deben ser enviados a todas las interfaces del enrutador por medio del proceso *flooding*.

7. LOADING. En este paso los enrutadores han finalizado el intercambio de información. Han construido una lista de Peticiones de Estado de Enlace y una lista de Retransmisión del Estado de Enlace. 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*).

8. FULL. La adyacencia esta 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. Aqui no existen los conceptos de DR y BDR.

h.) Encapsulamiento de paquetes OSPF en IP.

OSPF corre directamente sobre la capa de Internet de TCP/IP 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 (Paquetes de Descripción de la Base de Datos, Petición, Actualización y Verificación del Estado de Enlace)

pueden ser usualmente divididos en paquetes sin que se pierda su funcionalidad, sin embargo se recomienda que la fragmentación de IP se evite siempre que sea posible.

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 el valor de 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 224.0.0.6. Los enrutadores DR y BDR 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 un 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.

ANEXO B

1. HERRAMIENTAS DE QoS.

A continuación describiremos las herramientas que se deben tomar en cuenta durante la implementación de la calidad de servicio en una red.

a) Regulación –normas- y formación –modelado- de tráfico. (QoS Policy and Shaping)

Los mecanismos de regulación y formación tráfico clasifican paquetes e identifican violaciones en el tráfico ambos de la misma manera. Su única diferencia está en el trato que se le da a los paquetes que sobrepasan el límite de velocidad o el ancho de banda. Las normas descartan el tráfico con violaciones, o por lo menos rebajan la precedencia IP. La formación consiste en encolar el tráfico para evitar exceder las velocidades establecidas.

La regulación y formación de tráfico operan independientemente en cada dirección de la transmisión. Es decir, la operación de las normas o de la formación del tráfico en un enrutador o switch no necesita ningún soporte del equipo situado en el otro extremo del enlace. Y podemos clasificarlas de la siguiente forma:

Regulación de tráfico.

- CAR: *Commited Access Rate* (Velocidad de Acceso Suscrita)

Formación de tráfico.

- GTS: *Generic Traffic Shaping* (Formación de tráfico genérico)
- FRTS: *Frame Relay Traffic Shaping* (Formación del tráfico Frame Relay)

La GTS y FRTS utilizan el algoritmo de token bucket, el cual describiremos a continuación:

i) Token Bucket.

El concepto de token bucket que se muestra en la figura B.1. es un método para controlar la tasa de tráfico que pasa por un determinado punto de una red. La idea es que las tramas no pueden ser transmitidas a menos que posean un testigo (token). Los testigos se guardan en un almacén y se suministran de modo inmediato a cualquier trama que se encuentre en espera de ser transmitida.

Si llega un momento en el que se agotan los testigos existentes en el almacén, las tramas no podrán ser transmitidas hasta que vuelva a estar disponible alguno. Los testigos se insertan en el almacén a un ritmo constante, igual a la tasa a la cual se pueden transmitir las tramas. Si, en un momento dado, no existen tramas esperando ser transmitidas, los testigos se empezarán a acumular en el almacén. Cuando el almacén se llena de testigos, los nuevos testigos serán descartados. Este tipo de comportamiento puede ser visto como si fuese un permiso de tipo "o se usa o se pierde" para transmitir tramas. El número de testigos que se pueden guardar en el almacén (en otras palabras, el tamaño del almacén) representa el número máximo de tramas que pueden ser enviadas durante un pico de tráfico. En esta situación, las tramas deberán esperar hasta que vuelvan a existir testigos disponibles.

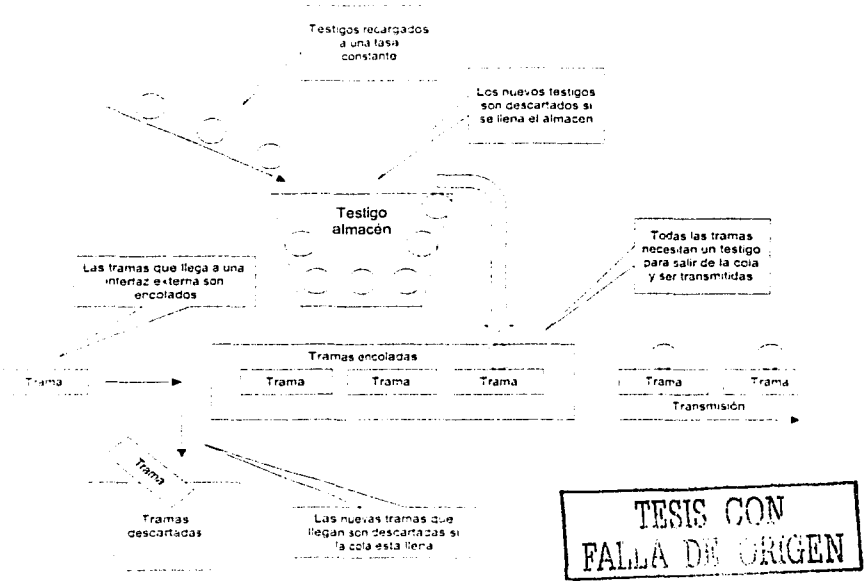


Fig. B.1. Almacén de testigos utilizado para el modelado del tráfico.

El mecanismo de control de tipo almacén de testigos se puede utilizar para las funciones de modelado y control de tráfico. En el caso de las funciones de modelado de tráfico, según se muestra en la figura B.1., las tramas se colocan en una cola cuando el almacén se queda sin testigos. El modelado de tráfico resulta útil en los picos de tráfico, pero atenúa su emisión a ráfagas de datos. El control de tráfico es menos refinado ya que las tramas son descartadas cuando el almacén se queda sin testigos.

CAR asegura que el tráfico identificado no excederá en mucho al promedio de la velocidad. CAR permite ráfagas dentro de un intervalo de tiempo hasta la cantidad definida y ráfagas excesivas en intervalos de tiempo mayores a la cantidad configurada. La función de ráfagas excesivas permite a CAR evitar el descarte en exceso de paquetes antes de que sean clasificados. Al igual que RED, que será descrito más adelante, esta función es una forma de administración del tamaño de la cola.

GTS y FRTS son muy parecidos. La tecnología subyacente es la misma, pero existen implementaciones en diferentes partes de la ruta de tráfico. GTS se implementa en una interfaz o una subinterfaz, mientras que FRTS se implementa en cada PVC.

GTS y FRTS disponen de diferentes opciones de cola. Con FRTS, se puede utilizar la cola de prioridad, personalizada o WFQ para controlar el tráfico que está en la cola. Con GTS, se puede emplear WFQ para controlar el tráfico que está en la cola. Basándose en las diferencias de cola, parece más sensato utilizar GTS para la transmisión de voz en IP.

b) Administración de Congestión. (QoS Congestion management)

La administración de la congestión tiene el objetivo de determinar si un enlace está saturado, es decir, si los usuarios o ciertas aplicaciones están presentando degradación en el servicio y a partir de esto, dar una justa distribución del ancho de banda dando prioridades a los diferentes tipos de tráfico. En resumen la administración de la congestión tiene dos metas principales:

- Proporcionar las solicitudes QoS para aplicaciones identificadas.
- Proporcionar una distribución equitativa de los recursos de ancho de banda.

Normas de Encolamiento

i. Cola FIFO (First Input First Output)

La técnica más básica de cola es FIFO. Una cola FIFO es un búfer sencillo que retiene los paquetes salientes hasta que la interfaz de transmisión pueda enviarlos. Los paquetes se envían fuera de la interfaz en el mismo orden en el que llegaron al búfer, como se muestra en la figura B.2.

COLA FIFO

Fig. B.2. Cola FIFO.

Esta técnica de encolamiento no proporciona algún tipo de QoS para el flujo, ni distribuye un ancho de banda equitativo entre flujos que compartan un enlace. Durante los periodos de congestión, se llena el búfer y los paquetes se descartan sin importar el tipo de paquete o las solicitudes de la aplicación asociada. Las colas FIFO no tratan por igual a la totalidad del flujo de tráfico, aunque descarten paquetes sin importar sus características.

Supongamos que N paquetes se descartan del final de una cola durante un periodo de tiempo. El problema es que algún flujo puede contener sólo N paquetes en esa ventana de tiempo, por lo que el flujo completo se podría destruir. Puede que N paquetes representen solo el 1% de otro flujo durante esa misma ventana de tiempo. Por eso, las colas FIFO están predispuestas contra flujos con pequeñas u ocasionales peticiones de ancho de banda. Este es otro motivo por el que FIFO no es una buena estrategia de encolamiento para interfaces que transmiten tráfico de VoIP.

ii. Cola de prioridad.

La cola de prioridad es un sencillo enfoque para ofrecer un trato preferencial a los paquetes identificados. Este es el método que asegura que los paquetes designados recibirán el mejor tratamiento posible. Los paquetes que llegan a la interfaz para su transmisión se separan en cuatro colas: de baja, normal, mediana y alta prioridad. La salida de estas cuatro colas alimenta un búfer de transmisión de la interfaz, como se muestra en la figura B.3.

Fig. B.3. Cola de Prioridad.

Los paquetes siempre se transmiten desde las colas de alta prioridad. Si los paquetes están esperando en dichas colas, se enviarán al búfer de transmisión. Si la cola de alta prioridad está vacía, se envía al búfer cualquier paquete de prioridad media. Si las colas de alta y media prioridad están vacías, se envían al búfer de transmisión los paquetes de la cola normal, y así sucesivamente.

La cola de prioridad consigue los requisitos QoS de VoIP, pero deja mucho que desear en el campo de la distribución de un ancho de banda equitativo para el resto del tráfico. Con esta técnica de encolamiento, el tráfico de alta prioridad incurre lo menos posible en la latencia y las fluctuaciones de fase, pero no hay provisiones para distribuir un ancho de banda entre el tráfico con las mismas prioridades. Dentro de una misma prioridad, el tráfico es de cola FIFO. La limitación más significativa es que si alguna de las colas tiene un flujo constante de tráfico, las colas de alta prioridad están completamente desprovistas de ancho de banda, como se muestra en la figura B.4.

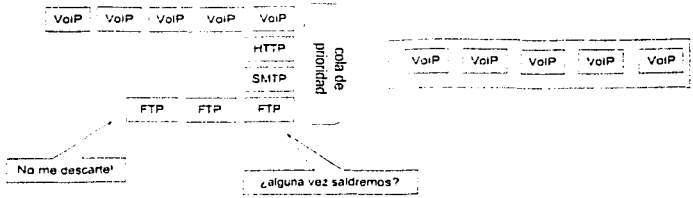


Fig. B.4. Cola de Prioridad.

Normalmente, no se recomienda la cola de prioridad para VoIP, pero es útil cuando debe tratar varios tipos de tráfico de alta prioridad. Si se tiene VoIP y tráfico de arquitectura de redes de sistema (SNA) en el mismo enlace, necesita asegurarse de que los paquetes VoIP estarán siempre colocados en el principio de la cola, pero los paquetes SNA deberían ir justo detrás de los VoIP para encabezar un tráfico de datos normal. LLQ y WFQ con prioridad IP RTP son incapaces de conseguir estos objetivos. La cola de prioridad también puede conseguir las necesidades de encolamiento de VoIP mezclándose con tráfico de video en tiempo real.

Aunque la cola de prioridad es todavía útil cuando están presentes varios tipos de tráfico en tiempo real, no los soporta en combinación con la fragmentación de Frame Relay FRF12. Como resultado, no se pueden mezclar efectivamente varios tipos de tráfico en tiempo real en enlaces Frame Relay de baja velocidad.

iii. Cola personalizada.

La cola personalizada es un algoritmo de encolamiento configurado equitativamente. El tráfico se clasifica en dos colas separadas, y cada cola se sirve al estilo round-robin para asegurarse de que ninguna está desocupada. La figura B.5. muestra la estructura de la cola personalizada.

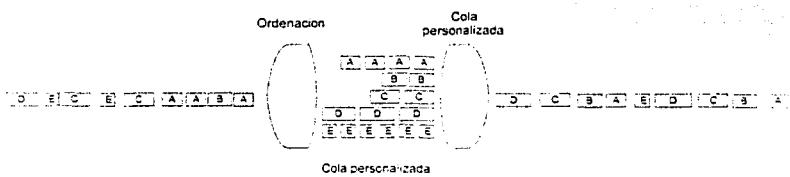


Fig. B.5 Cola Personalizada.

Esta cola debe configurarse manualmente:

- Qué tráfico se asocia con cada una de las colas.
- Cuántos paquetes pueden esperar en cada cola.
- Qué cantidad de ancho de banda se destina a cada cola.

Puede ser difícil configurar la distribución del ancho de banda para cada una de las colas. En lugar de configurar directamente la distribución del ancho de banda, se puede definir el número de bytes que van a ser transmitidos desde cada cola cuando estén en servicio. El mismo número relativo de bytes que se asignan a cada cola identifica el porcentaje de ancho de banda distribuido para ésta.

Aunque la capacidad de transmisión de cada cola se especifica en bytes, la cola transmite paquetes. La cola seguirá transmitiendo paquetes mientras se alcance el límite del contador de bytes, y finalizará con el paquete que esté a la mitad de la transmisión. Esto significa que si el contador de bytes se ajusta a 3050 y hay tras paquetes IP de 1500 bytes cada uno, la cola transmitirá los tres paquetes por un total de 4500 bytes. Se debe tener cuidado cuando se determine los valores del contador de bytes para cada cola, o que la distribución del ancho de banda actual puede ser muy diferente a lo planificado.

La cola personalizada afronta el tema del ancho de banda equitativo, pero no se ajusta bien para proporcionar QoS a flujos de tráfico específico. Como cada una de las colas se sirve al estilo round-robin, no hay una cola que tenga una prioridad mayor que la otra (excepto la cola del sistema para los enrutadores activos). Algunas colas pueden tener un mayor rendimiento que otras, pero ninguna puede ofrecer un tratamiento especial con respecto a la latencia o las fluctuaciones de fase. Esto hace que la cola personalizada sea una mala elección en el caso de VoIP.

iv. Encolamiento Ponderado Fair (WFQ).

El Encolamiento Ponderado Fair trabaja tan bien que a llegado a ser el método de encolamiento predeterminado en las interfaces de algunos enrutadores muy conocidos en el mercado a velocidades de E1/T1 ó menores. Conceptualmente, es muy similar a la cola personalizada, salvo que no necesita ninguna configuración. WFQ crea una cola separada para cada tipo de tráfico (por ejemplo, direcciones IP de fuente-destino y puerto TCP-UDP), y utiliza un valor predeterminado para el tamaño de la cola. Tiene la opción de configurar el tamaño de la cola para cada tipo de flujo.

La parte *weighted* de WFQ entra en juego cuando se utilizan los bits de precedencia IP y RSVP. Con la ausencia de RSVP o de la precedencia IP, WFQ proporciona un ancho de banda equitativo a todos los flujos. Este es un caso especial de la regla por la que WFQ proporciona una cantidad igual de ancho de banda a todos los flujos con la misma precedencia IP o estado RSVP.

WFQ proporciona una distribución equitativa del ancho de banda, permite que el tráfico de alta prioridad tenga una gran asignación de gran ancho de banda, y se configura automáticamente en la mayoría de los casos. WFQ suministra mucho mejor servicio para los flujos en un ancho de banda bajo con respecto a las colas FIFO. Si están presentes muchos flujos, el encolamiento *fair* no sirve a ningúno lo suficientemente rápido para mantener la baja latencia y la fluctuación de fase que pide VoIP. WFQ se debe complementar con la prioridad IP RTP para proporcionar tratamiento de QoS necesario para el tráfico de voz.

v. Encolamiento Ponderado Fair Basado en Clases (CB-WFQ).

El encolamiento CB-WFQ incorpora ideas de las colas personalizadas al formato del encolamiento WFQ. Se han introducido considerables mejoras respecto a las técnicas de encolamiento tradicionales. El número máximo de colas personalizadas (denominadas clases) se ha aumentado de 16 a 64. Sigue existiendo mucha flexibilidad a la hora de asignar el tráfico a cada clase. Cada una de ellas puede usar el método *tail-drop* de administración de tamaño de cola (es decir,

posibilita que las colas se llenen y se sobrecarguen durante la congestión), o bien WRED puede configurarse para cada clase independientemente. Con CB-WFQ, se puede especificar directamente la cantidad de ancho de banda que se quiere destinar a cada clase, y CB-WFQ ajustará los parámetros internos para que esto ocurra.

Con WFQ, es difícil especificar con precisión la cantidad de ancho de banda destinada a cada flujo. El problema es que el ancho de banda actual por flujo depende del número de estos, los cuales cambian constantemente. El parámetro necesario influye en el destino del ancho de banda en WFQ, pero sólo existen seis de éstos que se pueden especificar (precedencia IP de 0 a 5), más uno por flujo RSVP. Dado que WFQ es un algoritmo de encolamiento, cualquier ajuste de los flujos o niveles de precedencia IP afecta a los otros niveles. Esto se suma a la complejidad de la administración del ancho de banda con WFQ.

CB-WFQ se dirige al problema de la asignación del ancho de banda a las clases individuales, usando el concepto de cola personalizada. En una cola personalizada, las colas individuales se configuran con un valor en bytes que controla la cantidad de ancho de banda usada en cada cola. La implementación CB-WFQ es más específica, ya que puede asignar directamente la cantidad de ancho de banda que requiere asignar a cada clase. El algoritmo ajusta el ancho asignado a la clase en función de los requerimientos de cada clase y al total de ancho de banda disponible en el enlace.

Como recomendación global para IP, se debe de utilizar una de las siguientes técnicas de encolamiento para interfaces de ancho de banda bajo, dependiendo de sus necesidades:

- WFQ
- CB-WFQ

Ambas técnicas ofrecen una distribución de ancho de banda equitativa y deben usarse con un mecanismo para priorizar el tráfico de voz. WFQ requiere prioridad IP RTP, y CB-WFQ una clase de tráfico priorizada, denominada LLQ (*Link Layer Queuing*). La decisión de utilizar una técnica se puede basar en los requisitos de asignación de ancho de banda y nivel de complejidad de la configuración. WFQ necesita de una configuración básica a diferencia de CB-WFQ que necesita una más avanzada.

vi. Prioridad IP RTP.

Hasta este momento hemos hablado de técnicas de encolamiento desde la perspectiva de un escenario simple. Enseguida hablaremos de un modelo de cola multietapa.

El modelo de encolamiento multietapa es útil para aunar los requisitos de la QoS de flujos específicos y el ancho de banda equitativo para todos los flujos. Esta técnica de encolamiento identifica el tráfico de prioridad alta que no puede tolerar retrasos y fluctuaciones de fase. El tráfico restante pasa a través de la segunda cola, que proporciona un tratamiento equitativo a los distintos flujos de datos. A este modelo de encolamiento se le conoce como prioridad RTP o *IP priority RTP*. En las figuras B.6 y B.7. se muestra como funciona un modelo de encolamiento sencillo y uno multietapa.

Fig. B.6. Modelo de cola de la interface

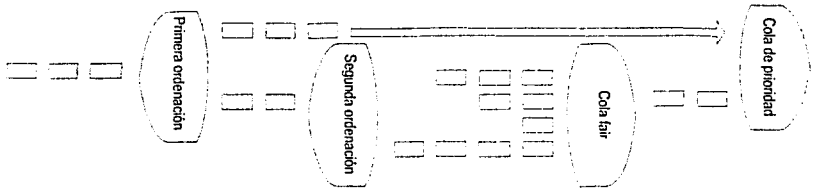


Fig. B.7. Multietapa del modelo de encolamiento suministrando QoS y distribución equitativa de ancho de banda.

c) Técnicas para evitar la congestión (QoS Congestion Avoidance)

A diferencia de las técnicas de encolamiento, las técnicas para evitar congestión tratan de evitarla y para ello se ayudan de los siguientes mecanismos:

i. Liberación de la cola. (*Tail Drop)*

Es el mecanismo que funciona por default cuando WRED no está configurado. Consiste en desechar los paquetes que llegan solo cuando el espacio del búfer está completamente ocupado. Este mecanismo puede provocar que una red no funcione adecuadamente porque genera la sincronización global TCP.

ii. RED, *Random Early Detection* (Detección Anticipada Aleatoria)

El algoritmo de RED monitorea el tráfico y elimina paquetes aleatoriamente si la congestión aumenta. El resultado es que la fuente al darse cuenta, disminuye la velocidad de transmisión. Toma las ventajas de los mecanismos de control de TCP.

RED es una forma de administración activa de la cola. En lugar de esperar pasivamente hasta que los búferes descarten el tráfico, RED descarta progresivamente paquetes en cuanto los búferes comienzan a llenarse. El nombre de detección anticipada refleja que los paquetes de un búfer están basados en un descarte aleatorio para una pronta detección de la congestión. Ningún paquete se descartara por debajo del umbral mínimo del búfer. Sin embargo por encima del umbral máximo, se descartarán todos los paquetes. Entre ambos umbrales, la probabilidad de que un paquete se descarte aumenta linealmente del 0 al 100%.

La detección anticipada aleatoria toma en cuenta el tipo de tráfico. Primero el tráfico es clasificado por el valor del campo de precedencia IP, y después se asigna un umbral mínimo de búfer a cada clase de tráfico. El tráfico con una reservación RSVP es tratado por encima del valor más alto de prioridad IP. El valor predeterminado para el umbral mínimo del búfer aumenta cuando lo hace la prioridad IP, de modo que los paquetes con mayor prioridad no se descartarán con tanta frecuencia como aquellos de menor prioridad.

Existe también WRED (*Weighted Random Early Detection*) basada en el flujo, usa direcciones IP de origen-destino y números de puertos TCP/UDP para diferenciar el tráfico. La idea es de igualar los flujos de forma parecida a WQF. En WRED, los paquetes se descartan independientemente de si provienen o no de una conversación de ancho de banda alto o bajo. Como resultado, un gran porcentaje del tráfico procedente de las estas conversaciones puede ser descartado por WRED. Las colas basadas en WRED proporcionan un tratamiento más equitativo a cada flujo, de modo que los de ancho de banda bajo tienen mayor rendimiento.

ANEXO C.

IPv6.

1) La necesidad de cambio de tecnología de protocolos. IPv6.

La versión del protocolo IP que se utiliza actualmente dentro de las redes que usan el modelo TCP/IP es la de IPv4. Sin embargo, debido al enorme crecimiento que han tenido las redes de este tipo en los últimos 5 años y al avance tecnológico de redes tanto en hardware como en la implementación de protocolos más eficientes, hacen ver sus deficiencias y limitaciones.

La primera, y tal vez la más inmediata es el reducido tamaño de la dirección IP. Actualmente se tiene un espacio de dirección de 32 bits, el cual nos da un rango de direcciones limito, que al ritmo de crecimiento de las redes actuales, no serán suficientes para antes del año 2010. El tamaño de la dirección IP que maneja la versión 6 es de 128 bits, que serán perfectamente aprovechables a largo plazo con un total de 2^{128} direcciones. Con el proceso de globalización y de estándares de redes inalámbricas (3ª generación), se prevé que cada persona tenga su propia dirección IP para manejar ya sea en su computadora o bien en su aparato móvil de datos. Con el tamaño de la nueva dirección IP esto se vislumbra posible.

La segunda de sus limitaciones es que algunas de sus operaciones son realmente ineficientes. La necesidad de este cambio de protocolo nos permitirá perfeccionar este tipo de operaciones. Una de estas sería la migración de un protocolo enfocado directamente a la transmisión de datos a un protocolo multiservicio, es decir, la posibilidad de manejar voz, datos y video sobre una misma interfaz física, con un buen desempeño de operaciones de Calidad de Servicio.

a) Dirección IPv6.

Como mencionamos, una de las partes fundamentales por las cuales se necesita un cambio de protocolo es la parte de las direcciones IP. La convención para escribir la nueva dirección es en enteros de 4 bits, con cada entero representado por un dígito hexadecimal. Entonces, se tienen 8 campos de enteros de 16 bits (4 dígitos hexadecimales), separados por dos puntos.

68DA : 8909 : 3A22 : FA64 : 68DA : 8909 : 3A22 : FACA

Debido a su manejo, es preferible utilizar direcciones jerárquicas, mismas que se manejan en las direcciones IPv6. El formato se tiene con un prefijo, seguido de 5 subcampos jerárquicos que denotan los siguientes datos:

- Prefijo: Denota la dirección basada en el tipo de proveedor.
- Identificador de Registro: Denota a cargo de quien se está registrando.
- Identificador del Proveedor: Denota el ISP (*Internet Service Provider*)
- Identificador de Suscriptor: Denota el ID del suscriptor, que es asignada por el ISP.
- Identificador de la Subred: Denota la subred a la que el suscriptor está asignado.
- Identificador de la Interface: Denota de dirección del host en la subred.

Existen además, como en Ipv4, direcciones que no pueden ser asignadas debido a que tienen un uso especifico. Estas son ejemplificadas en la tabla C.1.

Dirección	*Reservada para*
0000 001	Dirección ISO/ITU-T NSAP
0000 010	Dirección IPX
0000 011	No asignada
0000 1	No asignada
0000 10	No asignada
0001	No asignada
010	Dirección para servicios de unicast basados en el Proveedor
011	No asignada
100	Dirección para servicios de unicast basados en la zona geográfica.
101	No asignada
110	No asignada
1110	No asignada
1111 0	No asignada
1111 10	No asignada
1111 110	No asignada
1111 1110 0	No asignada
1111 1110 10	Dirección para enlace local
1111 1110 11	Dirección para sitios locales
1111 1111	Dirección de multicast

Tabla C.1. Direcciones IP reservadas.

b) Datagrama Ipv6.

Como se vio anteriormente, de acuerdo al modelo TCP/IP, que también aplica a redes de tipo IPv6, los datos en la capa de red se le denominan *Datagramas*. El encabezado de este datagrama consta de 64 bits dedicados al control de este seguidos de los 128 bit de la dirección IP fuente y de los 128 bits de la dirección IP destino. Esta es una de las principales diferencias entre IPv6 y la versión anterior. Los datos y cómo se encuentran distribuidos dentro del encabezado, se describen en la siguiente figura:

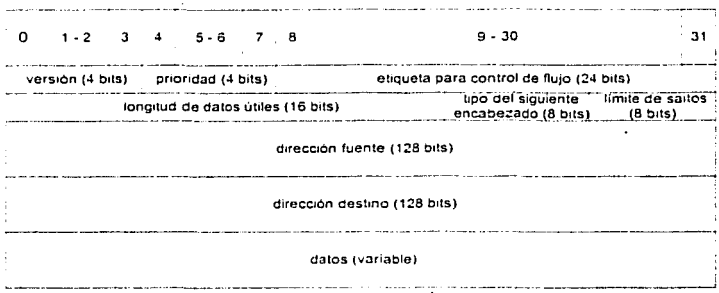


Tabla C.2. Formato del datagrama básico de IP v6.

Algunos de los campos que se observan en este encabezado ya los tenía el de la versión 4, otros fueron modificados, y otros fueron agregados. A continuación se da una descripción de cada uno de ellos.

- *Versión*. Identifica la versión del protocolo IP utilizado. En este caso (versión 6), el código es 0110 para los 4 bits.

- *Prioridad*. Este campo es nuevo dentro de esta versión. Esta diseñado para codificar hasta 16 posibles valores, que nos permite soportar diferentes tipos de tráfico, desde aplicaciones en tiempo real hasta datos.

Valor	*Tipo de tráfico que maneja.*
0	Tráfico no caracterizado.
1	Tráfico de poca prioridad tipo www
2	Transferencias de datos no atendidos (e-mail)
3	Reservado
4	Tráfico de grandes dimensiones (Transferencias de archivos)
5	Reservado
6	Tráfico Interactivo.
7	Control de tráfico (OSPF, SNP)
8	Video de alta definición
9 - 14	Reservado para aplicaciones en tiempo real como voz.
15	Video de baja definición

Tabla C.3. Tipo de trafico.

Estos valores definen la prioridad relativa de cada datagrama en comparación con los demás que viajan sobre la red. Esta distinción depende del tipo de tráfico que estemos manejando (con o sin control de congestión básicamente)

- *Control de Flujo.* Este parámetro del encabezado consta de 24 bits, y está en etapa experimental todavia. Sin embargo, en combinación con la dirección IP destino, se puede identificar un particular flujo de tráfico sobre la red. Este control de flujo ayudaría, por ejemplo, en el tiempo de procesamiento de un enrutador, ya que si este ya ha procesado determinada dirección con un control de flujo determinado, este podrá recordar cuál era su destino sin tener que efectuar el procesamiento de nuevo. Esta bandera nos puede ayudar a la reservación de recursos de la red, ya que si los enrutadores recuerdan las rutas de determinado tipo de tráfico, puede hacer estas reservaciones, sin embargo esta tarea se reserva a protocolos diferentes a IP, como lo es RSVP.

- *Longitud de carga útil.* Este campo indica la longitud total del datagrama IP, sin tomar en cuenta el encabezado. Debido a que este campo consta únicamente de 16 bits, esto limita la carga útil del datagrama a 65,535 bytes como máximo. Sin embargo, es posible enviar datagramas de mayor longitud usando la opción *jumbo payload* en la extensión del encabezado *hop-by-hop.* Si esta opción es utilizada, la longitud de carga útil se establece en cero.

- *Siguiente encabezado.* Este campo identifica que encabezado sigue después del básico de IP dentro del datagrama. Este puede ser un encabezado IP opcional o bien uno de algún otro protocolo de capas más altas. En la tabla C.4. se dan algunos ejemplos de los protocolos que se incluyen dentro de esta opción del datagrama.

Valor	*Protocolo o Encabezado.*
0	Encabezado de las opciones del tipo Hop-by-Hop.
4	Protocolo IP
6	Protocolo TCP.
17	Protocolo UDP.
43	Encabezado de enrutamiento.
44	Encabezado de fragmentación.
45	Protocolo de enrutamiento IRP.
46	Protocolo RSVP.
50	Datos encapsulados de seguridad.
51	Encabezado de autenticación.
58	Protocolo ICMP
59	No habrá encabezado siguiente.
60	Encabezado de opciones de destino.

Tabla C.4. Protocolo o Encabezado.

- *Límite de Saltos.* Este campo determina que tan largo será el viaje del datagrama dentro de la red. El host que envía el datagrama determina algún valor límite de saltos dentro de la red, y a medida que este cruza por algún enrutador, el valor se va decrementando en uno. Cuando este valor llega a cero sin que este haya llegado a su destino, el datagrama es descartado en la red.

- *Direcciones fuente y destino.* Estos dos campos, como su nombre lo indica, nos dan las direcciones IP de los dispositivos fuente y destino. Como ya se vio, estas direcciones son de 128 bits. Al igual que en la versión 4 de IP, las direcciones sirven a los protocolos de ruteo para asignar e identificar el camino a lo largo de la red, tratando de que este sea el óptimo.

c) Encabezados adicionales.

Todos los datagramas IP siempre comienzan con el encabezado básico el cual acabamos de describir, y en la mayoría de las ocasiones, la información contenida en el es suficiente para que el datagrama llegue a su destino.

Sin embargo, existen aplicaciones que necesitan mayor información para su tránsito por la red. Para estas, IP utiliza encabezados extendidos o adicionales. El campo de *siguiente encabezado* dentro del encabezado IP, nos dice que tipo de información seguirá a este dentro del datagrama. Esta estructura nos permite encadenar varios encabezados de distintos protocolos para realizar la tarea de entrega del datagrama de una manera óptima.

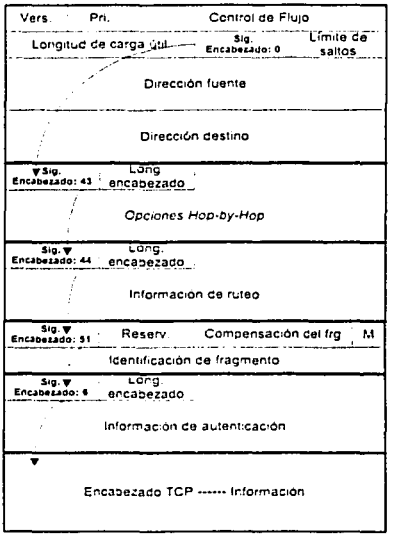


Tabla C.5. Estructura de encabezados concatenados en el datagrama IP

El orden en que se presenten los encabezados de protocolos adicionales es importante, porque permite que los rutedores intermedios permitan procesar los datagramas de forma eficiente. En la mayoría de los casos, estos solo les interesa la información dentro de las opciones *hop-by-hop* o bien los encabezados de ruteo. Así que estos deben de aparecer en primera instancia.

d) Opciones de salto por salto *(hop-by-hop)*

Este encabezado contiene opciones IP para cada sistema dentro de la ruta del datagrama. Cada equipo enrutador intermedio debe examinar y procesar estas opciones.

Tipo	*Opción*	*Tamaño*	*Alineamiento*
0	Pad1	1 byte	Ninguno
1	PanN	2+n bytes	Ninguno
194	Longitud Jumbo de Carga útil.	2+4 bytes	4*n + 2

Tabla C.6. Salto por salto.

La columna que nos indica el tamaño nos da el total de este de cada opción, incluyendo los campos del tipo y longitud de la opción.

El tipo de opción no solo la identifica, sino además dice al enrutador como tratar a ésta cuando es configurada.

En particular, los 2 bits más significativos indican al enrutador que hacer con alguna opción no reconocida. El tercer bit identifica a aquellas opciones que pueden cambiar de valor a medida que el datagrama viaja sobre la red.

Tipo (binario)	*Acción si el tipo no es reconocido.*
00xxxxxx	Ignora la opción y continua procesando el datagrama.
01xxxxxx	Descarta el datagrama y no realiza alguna acción.
10xxxxxx	Descarta el datagrama y regresa un mensaje de error ICMP al host fuente.
11xxxxxx	Descarta el datagrama y regresa un mensaje de error ICMP al host fuente únicamente si el destino no es una dirección multicast.
	Comportamiento del datagrama en transito
xx0xxxxx	El valor de la opción no cambia durante el tránsito en el enrutador intermedio.
xx1xxxxx	El valor de la opción puede cambiar durante el tránsito en los enrutadores intermedios.

Tabla C.7.

1) Opción Pad1.

Consiste en un solo byte, cuyo valor es cero. No tiene un byte explícito de longitud, estando su valor implícito en el único byte de esta opción. Esta opción sirve para saltar posiciones de manera tal que provee a las siguientes opciones sus requerimientos de alineamiento.

Un alineamiento correcto es importante para un eficiente procesamiento de los datagramas. Los microprocesadores actuales, cuyos tamaños de palabra son de 32 o 64 bits, pueden acceder a cantidades multi-bytes con mucha mayor eficiencia si esas cantidades están en sus fronteras naturales de memoria. Para ayudar a lograr este alineamiento, IP define los campos de su encabezado de manera que a medida que el primer byte en el datagrama puede es alineado, los otros campos en el encabezado también pueden ser alineados.

2) Opción PadN.

Esta opción tiene el mismo uso que la anterior, que es la de saltar posiciones para el correcto alineamiento de las siguientes opciones. A diferencia de la anterior, en donde solo se inserta un solo byte de alineamiento, PadN inserta bytes de forma arbitraria, que pueden ir desde 2 bytes.

3) Opción de longitud Jumbo de Carga útil.

Esta opción permite redefinir la longitud de carga útil descrita en el encabezado IP básico. Como ya lo mencionamos, el datagrama tiene como límite una carga útil de hasta 65,535 bytes. Cuando se necesitan un datagrama más grande, el campo de carga útil del encabezado se establece en cero, y es utilizada esta opción. Tiene un límite de 4 bytes, lo que nos da longitudes de hasta 4,294,967,295 bytes de carga útil, que es suficiente para las necesidades propuestas en un futuro a mediano plazo.

i) Encabezado de Ruteo.

En general, el protocolo IP permite a los protocolos de la red (protocolos de ruteo) la entrega de información de un lado a otro de la red. Sin embargo, existen ocasiones en las que el host emisor requiere más control sobre la ruta que los datos tomarán para cruzar la red, tal vez por razones de seguridad, en los que no es deseable atravesar ciertos enrutadores. Con las opciones de este encabezado, se puede obtener cierto control, que combinado con las direcciones IP del encabezado principal, nos puede dar la ruta que el datagrama debe seguir.

Hasta ahora, solo se ha definido un solo tipo de *encabezado de ruteo*, conocido como *tipo 0*, que consiste básicamente en una lista de direcciones IP.

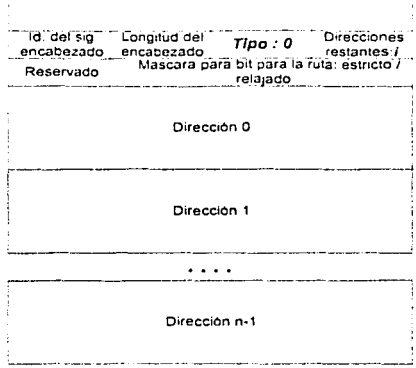


Tabla C.8. Encabezado de Ruteo Tipo 0.

El funcionamiento de este encabezado es como sigue: Al dejar el host fuente el datagrama, la dirección destino del encabezado básico indicará el primer salto dentro de la ruta a seguir. La lista de direcciones del encabezado de ruteo indicará en dónde se efectuarán los siguientes saltos.

El campo de direcciones restantes nos indica en que posición del campo de direcciones estamos, y en cada salto, este número se disminuye en valores de 1, a partir del número *n* que está relacionado con el número total de direcciones.

Además de éste control, existe una característica adicional que permite incrementar la confiabilidad de la designación de la ruta. El campo de la máscara de bits para la determinación del tipo de ruta nos dice como se va a seguir esta ruta salto a salto, ya sea de forma estricta o bien un poco relajada. Cada bit de esta máscara, comenzando por el más significativo, designa a la dirección correspondiente como *estricta* (1) o *relajada* (0). Se tendrá un ruteo estricto cuando el datagrama deba proceder directamente a la dirección que este planteada, sin que intervengan saltos adicionales; si el enrutador no puede satisfacer la ruta de forma estricta, regresará un error ICMP al host fuente. En el ruteo *relajado* permite que el datagrama pase por enrutadores intermedios para llegar a la dirección planteada.

ii) Encabezado de fragmentación.

Con este encabezado podemos fragmentar el datagrama si este es muy grande para pasar por algún tipo de tecnología de capa 2.

Id del sig. encabezado	Reservado	Offset del fragmento	0	bit M
Identificación del fragmento				

Tabla C.9. Encabezado de fragmentación.

En este encabezado, el *offset del fragmento* especifica que tan lejos del datagrama original se encuentra el primer bit del fragmento actual. Este tiene 8 bytes, por lo que únicamente se pueden partir fragmentos, a excepción del último, con un tamaño que sea múltiplo entero de 8 bytes. El bit M se coloca en todos los fragmentos excepto en el último, por lo que nos dice si una pieza es seguida de otra hasta llegar a la última.

La identificación del fragmento, nos indica cuál es el datagrama original al cual pertenece cada pieza, ya que como cada pieza llegará (en la mayoría de las aplicaciones) de forma desordenada, se debe tener cuidado cuando el host receptor este ensamblando las piezas de cada datagrama para no mezclarlas.

c) Seguridad en Ipv6.

Aunque este no es un campo nuevo dentro de los protocolos IP, ya que de hecho estos comenzaron en un área de seguridad nacional, no es hasta esta versión 6 en la que se hace un mayor seguimiento de opciones que aseguren la parte estructural de la información. Ahora, todos los hosts de tipo Ipv6 deben poder ser autenticados además de poder hacerlo con los demás. Además, se tienen bien definidos los procesos de intercambio de mensajes de confidencialidad.

Ambas cuestiones, autenticación y confidencialidad, recaen en asociaciones de seguridad. Estas establecen el contexto para la comunicación, además de definir diversos aspectos de seguridad de la misma. Algunas características de estas asociaciones son:

- Especifican los algoritmos de autenticación y de encripción a utilizar, así como los de sincronización y los vectores de inicialización.
- Especifican la o las llaves de comunicación.
- Sensitividad de los datos protegidos.

i) Autenticación.

Existen dentro de Ipv6 opciones que incrementan la seguridad tanto de la información de control y ruteo, como de la información de carga útil. Una de estas opciones de seguridad es el encabezado de autenticación. Este asegura que el datagrama que se recibió sea autentico, es decir, que la información no haya sido alterada durante su viaje además de que provenga del emisor el cual está configurado.

Id del sig encabezado	Longitud del encabezado	Reservado
Índice de parámetros de Seguridad		
Datos de Autenticación		

Tabla C.10. Encabezado de autenticación.

El algoritmo de autenticación que utiliza Ipv6 es el MD5 (*Message Digest 5,* que es un protocolo de encriptamiento) Este es el asignado por omisión, sin embargo, pueden existir arreglos entre hosts para utilizar uno adicional. Aunque todos los hosts deben de soportar estos algoritmos de autenticación, no están forzados a utilizarlos si ellos así lo requieren.

El campo de índice de parámetros de seguridad (SPI, *Security Parameters Index*), indica el algoritmo de autenticación a seguir, que asociado a la dirección destino del encabezado básico, nos da la asociación de seguridad para la comunicación entre los hosts involucrados.

ii) Confidencialidad.

Aunque la autenticación es importante dentro de la seguridad de los datos ya que nos asegura la información de los hosts destino y fuente, esta no protege a los datos en sí, y estos pueden ser vistos a lo largo de su paso por la red, por ejemplo, con un analizador de protocolos (*sniffers*)

La confidencialidad que nos ofrece IP es dada con el *encapsulamiento* de seguridad para la información (ESP, *Encapsulating Security Payload*) ESP es el estándar para el envío de información encriptada dentro de los datagramas IP.

Todos los sistemas que soporten ESP deben de soportar el algoritmo de encripción. Encadenamiento de Bloques Cifrados (CBC, *Cipher Block Chaining*) del Estándar de Encripción de Datos (DES, *Data Encryption Standard*), que fue especificado por el gobierno de Estados Unidos.

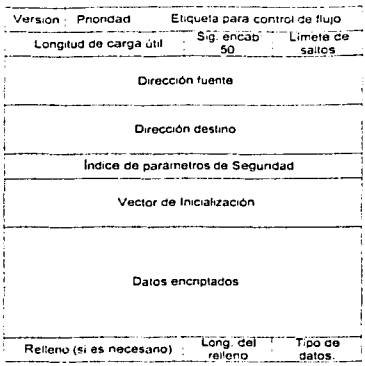


Tabla C.11. Formato del ESP con soporte para el algoritmo DES-CBC.

Un vector de iniciación sigue después del índice de parámetros de seguridad, y su contenido es utilizado en el algoritmo DES-CBC. Después de este vector vienen los datos encriptados. El proceso ESP termina con la introducción de datos de relleno para forzar a que el tamaño de todo el ESP sea de un múltiplo entero de 32 bits así como de la longitud de este. El último campo, el de Tipo de datos, contiene el mismo valor que el campo del siguiente encabezado e indica que protocolo ha sido encriptado.

ACRÓNIMOS

ABR: Area Border Router, *Enrutador de Borde de Área.*

ANSI: American National Standards Institute, *Instituto Nacional de Estándares Americanos.*

AF: Assured Forwarding, *Direccionamiento Asegurado.*

ARP: Address Resolution Protocol, *Protocolo de Resolución de Direcciones.*

ARPANET: Advanced Research Project Agency's Network, *Agencia de Proyectos de Investigación Avanzada de Red.*

ASBR: Autonomous System Boundary Router, *Enrutador de Frontera de Sistema Autónomo.*

ATM: Asynchronous Transfer Mode, *Modo de Transmisión Asíncrona.*

BA: Bandwidth Allocator, *Asignador de Ancho de Banda.*

BDR: Backup Designated Router, *Enrutador Designado de Respaldo.*

BGP: Border Gateway Protocol.

BISDN: Broadband Integrated Services Digital Network, *Red Digital de Servicios Integrados de Banda Ancha.*

BR: Backbone Router, *Enrutador de Backbone.*

CAR: Commited Access Rate, *Velocidad de Acceso Suscrita.*

CBC: Cipher Block Chaining, *Encadenamiento de Bloques Encriptados.*

CBR: Constraint-based Routed, *Ruteo Basado en Restricciones.*

CB-WFQ: Class Based WFQ, *Encolamiento Ponderado Fair Basado en Clases.*

CGI: Common Gateway Interface, Interfaz de Gateway Común.

CIDR: Classless InterDomain Routing, *Enrutamiento Interdominio sin Clase.*

COPS: Cliente de Aprovisionamiento de Políticas.

CoS: Class of Services, *Clases de Servicios.*

CPL: Call Processing Language, *Lenguaje de Procesamiento de Llamada.*

CBR-LDP: Constraint-based Routed Label Distribution Protocol, *Protocolo de Distribución de Etiquetas basado en Ruteo con Restricciones.*

CSMA/CD: Carrier Sense Multiple Access / Collision Detection, *Acceso Múltiple con Detección de Portadora / Detección de colisiones.*

DGSCA: Dirección General de Servicios de Cómputo Académico.

DES: Data Encryption Standard, *Estandar de Encripción de Datos.*

Diff-Serv: Arquitectura da Calidad de Servicio basada en Servicios Diferenciados.

DNS: Domain Name Server, *Servicio de Asignación de Nombres de Dominio.*

DoD: Departament of Defense, *Departamento de Defensa.*

DR: Designated Router, *Enrutador Designado.*

DS: Differentiated Services, *Campo IP de Servicios Diferenciados.*

DSBM: Designed SBM, *SBM Designado.*

DSCP: Differentiated Services Code Point, *Código de Servicios Diferenciados.*

EF: Expedited Forwarding, *Direccionamiento Expedito.*

EGP: External Gateway Protocol, *Protocolo de Compuerta Externa.*

EIGRP: Enhanced Interior Gateway Routing Protocol, *Protocolo de Enrutamiento de Compuerta Interna Mejorado.*

E-LSP: EXP-inferred LSP.

ESP: Encapsulating Security Payload, *Encapsulamiento de Seguridad de la Carga Útil de la Información.*

ER: Explicit Route, *Ruta Explícita.*

FEC: Forwarding Equivalent Class, *Clase Equivalente de Direccionamiento.*

FIFO: First In First Out, *Primero en Entrar Primero en Salir.*

FRTS: Frame Relay Traffic Shaping, *Formación de Tráfico de Frame Relay.*

FTP: File Transfer Protocol, *Protocolo de Transferencia de Archivos*

GTS: Generic Traffic Shaping, *Formación de Tráfico Genérico.*

HbH: Hop by Hop, *Salto a Salto.*

IANA: Internet Assigned Numbers Authority, *Autoridad de Asignación de Números en Internet.*

ICMP: Internet Control Message Protocol, *Protocolo de Mensajes de Control de Errores de Internet.*

IEEE: Institute of Electrical and Electronics Engineers, *Instituto de Ingenieros Eléctricos y Electrónicos.*

IETF: Internet Engineering Task Force, *Grupo de Trabajo en Ingeniería de Internet.*

IGMP: Internet Group Management Protocol, *Protocolo de Administración de Grupos en Internet.*

IGRP: Interior Gateway Routing Protocol, Protocolo de Enrutamiento de Compuerta Interna.

INT-SERV: Arquitectura de Calidad de Servicio basada en Servicios Integrados.

IP: Internet Protocol, *Protocolo de Internet*

Ipv4: Internet Protocol Version 4.

IPv6: Internet Protocol Version 6.

IR: Internal Router, *Enrutador Interno.*

ISAKMP: Internet Security Association and Key Management Protocol, Protocolo de Administración de Llaves y Asociación Segura en Internet.

ISDN: Integrated Services Digital Network, *Red Digital de Servicios Integrados.*

ISO: International Standards Organization, *Organización Internacional de Estándares.*

ISP: Internet Service Provider, *Proveedor de Servicios de Internet.*

ISSLL: Integrated Services over Specific Link Layers, *Servicios Integrados Sobre Capas de Enlaces Específicos.*

ITU-T: International Telecommunications Union-Telecommunications, *Unión Internacional de Telecomunicaciones- Sector de Estandarización de Telecomunicaciones.*

LAN: Local Area Network, *Red de Área Local.*

LDAP: Lightweight Directory Access Protocol, *Protocolo de Servicio de Acceso a Directorios .*

LDP: Label Distribution Protocol, *Protocolo de Distribución de Etiquetas.*

LER: Label Edge Router, *Enrutador de Orilla de Etiquetas.*

LLC: Logical Link Control. *Control de Enlace Lógico.*

LLQ: Link Layer Queuing, *Encolamiento en Capa de Enlace*

L-LSP: Label only inferred LSP.

LSA: Link State Advertisements, *Avisos de Estado de enlace.*

LSP: Label Switched Path tunnel, *Ruta Conmutada por Etiquetas.*

LSR: Label Switched Router, *Enrutador Conmutado por Etiquetas.*

LW: Long Wave, *Onda Larga*

MAC: Media Access Control, *Control de Acceso al Medio.*

MCU: Multipoint Control Unit, *Unidad de Control Multipunto.*

MD5: Message Digest 5.

MPLS: Multiprotocol Label Switching, *Conmutación por Etiquetamiento de Multiprotocolos*

NHLFE: Next Hop Label Forwarding Entry, *Entidad de Definición del Siguiente Salto.*

NIC: Network Information Center, *Centro de Información de la Red.*

NFS: Network File System, *Sistemas de Archivos de Red.*

NNTP: Network News Transport Protocol, *Protocolo de Transporte de Noticias de Red.*

NOC: Network Operation Center, *Centro de Operación de la Red.*

NLA: Networks Link Advertisements, *Avisos de Enlace de Redes.*

OSI: Open System Interconnection, *Sistema Abierto de Interconexión.*

OSPF: Open Shortest Path First.

PBR: Policy Based Routing, *Ruteo Basado en Políticas.*

PDU: Protocol Data Unit, *Unidad de Datos de Protocolo.*

PDB: Per Domain Behavior, *Comportamiento por Dominio QoS.*

PDP: Policy Decision Point, *Punto de Decisión de Políticas.*

PEP: Policy Enforcement Point, *Punto para Forzar las Políticas.*

PHB: Per Hop Behavior, *Comportamiento por Salto.*

PMD: Physical Medium Dependent, *Medio Físico Dependiente.*

PPP: Point to Point Protocol, *Protocolo Punto a Punto.*

PSC: PHB Scheduling Class, *Clase Agendada de PHB*

QoS: Quality of Service, *Calidad de Servicio.*

RAP: RSVP Admision Policy, *Políticas de Admisión para RSVP.*

RED: Random Early Detection, *Detección Anticipada Aleatoria.*

RedUNAM: Red de Datos de la Universidad Nacional Autónoma de México.

RFC: Request For Comments, *Documentos en proceso de Estandarización por parte de la IETF.*

RIP: Routing Information Protocol, Protocolo de Información de Enrutamiento.

RM: Requestor Module, *Modulo de Requerimientos.*

RSVP: Resource reSerVation Protocol, *Protocolo de Reservación de Recursos.*

RTCP: Real Time Transport Control Protocol, *Protocolo para el Control de Transporte en Tiempo Real.*

RSTP: Real-Time Streaming Protocol, *Protocolo de Flujo en Tiempo Real.*

RTP: Real Time Protocol, *Protocolo de Tiempo Real.*

SBM: Subnet Bandwidth Management, *Administración de Ancho de Banda de Subredes.*

SDP: Session Description Protocol, *Protocolo de Descripción de Sesión.*

SDR: Session Directory, *Directorio de Sesión.*

SIP: Session Initiation Protocol, *Protocolo de Iniciación de Sesión.*

SKEME: Secure Key Exchange Mechanism for Internet, *Mecanismo de Intercambio de Llave Segura para Internet.*

SLA: Service Level Agreement, *Acuerdo de Nivel de Servicio.*

SLO: Service Level Objective, *Objetivo de Nivel de Servicio.*

SNMP: Simple Network Management Protocol, *Sistemas de Administración de Red.*

SMTP: Simple Mail Transfer Protocol, *Protocolo Simple de Transferencia de Correo.*

SPI: Security Parameters Index, *Índice de Parámetros de Seguridad.*

STP: Shortest-Path Tree, *Árbol con las Rutas más Cortas.*

STP: Shielded Twister Pair, *Par Trenzado Blindado.*

SW: Short Wave. *Onda Corta.*

TA: Traffic Aggregate, *Agregado de Tráfico.*

TCP: Transmission Control Protocol, *Protocolo para el Control de la Información.*

TDM: Time Division Multiplex, *Multiplexación por División de Tiempo.*

TE: Traffic Engineering, *Ingeniería de Tráfico.*

TFTP: Trivial File Transfer Protocol, *Transferencia de Archivos Triviales.*

TLV: Type, Length and Value, *Tipo, Longitud y Valor.*

ToS: Type of Service, *Tipo de Servicio.*

TTL: Time to Live, *Tiempo de Vida.*

UDP: User Datagram Protocol, Protocolo de Datagrama de Usuario.

UTP: Unshielded Twister Pair, *Par Trenzado no blindado.*

VBR: Variable Bit Rate, *Tasa de Bits Variable.*

VLAN: Virtual Local Area Network, *Red de Área Local Virtual.*

VLSM: Variable-Length Subnet Masks, *Mascara de Subred de Longitud Variable.*

VoIP: Voice Over IP, *Voz sobre IP.*

VTP: Virtual Trunk Protocol, *Protocolo de Troncal Virtual.*

WAN: Wide Area Network, *Red de Área Amplia.*

WFQ: Weighted Fair Queuing, *Encolamiento Ponderado Fair.*

WRED: Weighted Random Early Detection, *Detección Anticipada Aleatoria Ponderada*

XDSL: X-type Digital Subscriber Line, *Línea de Abonado Digital de tipo X.*

BIBLIOGRAFÍA

GARCIA TOMAS, J; RAYA CABRERA, J; [2002]; "Alta velocidad y calidad de servicio en redes IP", Alfaomega, México D.F.

BLACK, U. [2001]; "MPLS and Label Switching Networks"; Prentice Hall.

BLACK, U; [1999]; "Advanced Internet Technologies"; Prentice Hall.

BLACK, U; [1992]; "TCP/IP and related protocols"; McGraw Hill.

ALISTAIR, PACKMAN; [1999]; "Managing Bandwidth: Deploying QoS on Enterprise Networks"; Prentice Hall.

BASSAM, HALABI; [1997]; "Internet Routing Architectures"; McGraw Hill; Indianapolis, IN.

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

QUINN-ANDRY, TERRY, HALLER, KITTY; [1998]; "Designing Campus Networks"; McGraw Hill; Indianápolis, IN.

DOUGLAS COMER; "Intenetworkingwith TCP/IP Vol.1: Principles, Protocols, and Architectures"; McGraw Hill; 4a Edición.

DZIONG, ZBIGNIEW; 1997]; "ATM network resource management"; [McGraw Hill.

DAVIS, RONALD; 1999]; "ATM for public networks"; [McGraw Hill.

AMMANN, PAUL; [2000]; "Managing dynamic IP networks"; McGraw Hill.

TOMSO, PETER; [2002]; "MPLS based VPNs. Designing Advanced Virtual Networks"; Prentice Hall.

BANERJEE, DRAKE, KOMPELLA, REKHTER, et al.; [2001]; IEEE paper; "Generalized Multi-protocol Label Switching: An Overview of Routing and Management Enhancements".

BRADEN, R; ZHANG, L; BERSON, S; HERZONG, S; JAMIN, S; [1997], IETF - RFC 2250: "Resource ReSerVation Protocol (RSVP) --Version 1 Functional Specification"; Network Working Group.

BRFADEN, R; CLARK, D; SHENKER, S; [1994], IETF - RFC 1633: "Integrated Services in the Internet Architecture: an Overview"; Network Working Group.

NIKCHOLS, K; BLAKE, S; BAKER, S; BAKER, F; BLACK, D; [1998], IETF - RFC 2474: "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers"; Network Working Group.

BLAKE, S; BLACK, D; CARLSON, M; DAVIES, E; WANG, Z; WEISS, W; [1998], IETF - RFC 2475: "An Architecture for Differentiated Services"; Network Working Group.

BERNET, Y; YAVATKAR, R; BAKER, F; ZHANG, L; SPEER, M; BRADEN, R; DAVIE,B; WROCLAWSKI, J; [2002], IETF - RFC 2998: "A Framework for Integrated Services Operation over Diffserv Networks"; Network Working Group.

HEINANEN, J; BAKER, F; WEISS, W; WROCLAWSKI, J; [1999], IETF - RFC 2597: "Assurfed Forwarding PHB Group"; Network Working Group.

JACOBSON, V; NICHOLS, K; PODURI, K; [1998], IETF - RFC: 2598: "An Expedited Forwarding PHB"; Network Working Group.

LE FAUCHER, et al.; [2002]; IETF - RFC 3270: "Multi-protocol Label Switching Support of Differentiated Services".

ROSEN, et al.; [1998]; IETF – RFC 2475: "Multiprotocol Label Switrching Arquitecture".

J. MOY; [1997]; IETF - RFC 2178: "OSPF Version 2", Network Working Group.

GANT; SEDDIGH, et al; [2002]; Internet Draft IETF: "MPLS Support of Differentiated Services using E-LSP".

LE FAUCHER, et al.; [2003]; Internet Draft IETF: "Requirements for support of Diff-Serv-aware MPLS Traffic Engineering".

BERNET, Y; YAVATKAR, R; FORD, P; BAKER, F; ZHANG, L; NICHOLS, K; [1999], Internet Draft IETF: "Interoperation of RSVP/Int-Serv and Diff-Serv Networks".

STAURDUST QOS FORUM; [1999]; White Paper "Introduction to QoS Policies".

NORTEL NETWORKS; [1998]; White Paper; "IP QoS – A Bold New Network".

MICROSOFT; [1999]; White Paper; "Quality of Service Technical White Paper".

CISCO SYSTEMS; [2002]; White Paper; "Advanced Topics in MPLS-TE Deployment".

CISCO SYSTEMS; [2001]; White Paper; "Deploying Guaranteed-Bandwidth Services with MPLS".

CISCO SYSTEMS; [2002]; Manual; "Building Scalable Cisco Networks Manual, Volume 1 & 2"

FOUNDRY NETWORKS; [2002]; Hoja de especificaciones; "Datasheet NetIron 400, 800, 1500".

FOUNDRY NETWORKS; [2002]; Hoja de especificaciones. "Datasheet BigIron 4000, 8000, 15000".

3COM CORPORATION; [1999]; Manual; "Network Administration Guide (Transcend)"

Otras referencias:

http://www.cisco.com
http://www.nortel.com
http://www.mbone.org
http://www.qbone.org
http://www.ietf.org