UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

CALIDAD DE SERVICIO MEDIANTE REDES DE SERVICOS DIFERENCIADOS EN INTERNET 2

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

ERNESTO HUMBERTO VENTURI MENA

PROMOCIÓN
1983 - I

LIMA – PERÚ
2006

CALIDAD DE SERVICIO MEDIANTE REDES DE SERVICIOS DIFERENCIADOS EN INTERNET 2

Dedico éste esfuerzo a
Mis padres que nunca dejaron de alentarme,
Mi esposa , por el apoyo incondicional ,
Y a mi hijo para que lo tome como el ejemplo a seguir.

SUMARIO

Las redes basadas en el protocolo IP, por omisión proveen la entrega de datos con el "mejor esfuerzo" (best effort), el cual ofrece el servicio cuando puede y como puede, afectando severamente al retardo, su variabilidad, y la pérdida de los paquetes, parámetros importantes en las aplicaciones de tiempo real. Sin embargo, las redes modernas han aumentado su demanda en ancho de banda, desempeño y flexibilidad, para soportar los servicios de aplicaciones actuales y futuros.

El proyecto de Internet 2, es un esfuerzo de colaboración para desarrollar tecnología y nuevos avances en Internet. Es una red con capacidades avanzadas que utilizan un conjunto de herramientas, una de ellas conocida como la garantía de "Calidad de Servicio" llamada de Servicios Diferenciados (DiffServ), que permite el transporte de nuevas aplicaciones que requieren de mejores características a las que ofrecen la red Internet tradicional.

El desarrollo de la tecnología DiffServ permite el despegue definitivo de determinados servicios con ciertos requisitos de calidad de servicio. Se muestran los mecanismos para adoptar diferentes políticas de calidad de servicio en función de las necesidades de la red. Se muestra la viabilidad de un elemento servidor de políticas como el Bandwith Broker, así como la posibilidad de comunicar los diferentes elementos del escenario mediante un protocolo diseñado para el intercambio de políticas (COPS). Como en la actualidad se está realizando la migración de IPv4 a IPv6, éste trabajo analiza si es posible el modelo DiffServ como proveedor de calidad de servicio y se analiza algunos mecanismos de transición para éste efecto.

INDICE

PROLOGO

La motivación inicial para comenzar a definir la nueva versión del protocolo IP ha sido la limitación impuesta por el campo de direcciones en IPv4, así como la poco eficiente decisión en las clases A, B, C y D. Después, la conveniencia de un formato de PDU optimizado para un proceso más eficiente en los encaminadores, la seguridad y la **calidad de servicio,** contribuyeron a la aparición de una nueva versión de IP, denominada IPv6.

La arquitectura de Servicios Diferenciados (DiffServ) es la mas prometedora de todas las arquitecturas que disminuye la preocupación por la Calidad de Servicio en las redes de nueva generación , debido a que puede ofrecer diferentes niveles de calidad de servicio en forma escalable.

En el Capítulo I se hace una descripción muy resumida de los modelos que brindan calidad de servicio.

En el Capítulo II como se define la Calidad de Servicio en Internet , tipos de flujos de tráfico , mecanismos de control y se describen las diferentes arquitecturas de Calidad de Servicio.

En el Capítulo III , se define el modelo DiffServ que es el protocolo que brinda los servicios diferenciados y algunos requisitos generales para la implementación de una red de Servicios Diferenciados.

En el Capítulo IV , se describe el protocolo COPS que es el que gestiona el control de políticas a protocolos de señalización de calidad de servicio . El modelo no hace referencia sobre los métodos que ejecuta el servidor de poíticas sino se basa en las respuestas del servidor a las peticiones.

En el Capítulo V se describen algunas características de un contrato de prestación de servicios y se da como referencia un ejemplo de un contrato emitido por la NIC de México.

En el Capítulo VI se hace un resumen comparativo entre los modelos IntServ y DiffServ .

En el Capítulo VII se describen algunos mecanismos de transición entre IPv4 al IPv6 analizándose el modelo DiffServ como proveedor de Calidad de Servicio, debido a la coexistencia de IPv4 y IPv6.

En el Capítulo VIII , se analizan las limitaciones del modelo DiffServ.

En el Capítulo IX , se indican algunas aplicaciones y/o Servicios del modelo Diffserv en Internet2.

CAPITULO I

ANTECEDENTES

1.1 Introducción

En las eventuales congestiones de enlaces que son parte del recorrido del tráfico entre dos equipos (host, o terminal) de distintas redes, cada paquete de información compite por un poco de ancho de banda disponible para poder alcanzar su destino.

Típicamente, las redes operan en la base de entrega del mejor esfuerzo (irónicamente llamado WWW: World Wide Wait), donde todo el tráfico tiene igual prioridad de ser entregado a tiempo. Cuando ocurre la congestión, todo este tráfico tiene la misma probabilidad de ser descartado.

En ciertos tipos de datos que circulan por las redes hoy en día, por ejemplo tráficos con requerimientos de tiempo real (voz o video), es deseable que no ocurra pérdida de información, que exista un gran ancho de banda disponible, y que los retrasos en los envíos de estos paquetes de datos sean mínimos. Es por ello que surge la necesidad de aplicar Calidad de Servicio (QoS) en el nivel del transporte de datos, métodos de diferenciación de tráficos particulares con el fin de otorgar preferencia a estos datos sensibles.

Se entiende por "Calidad de Servicio", a la capacidad de una red para sostener un comportamiento adecuado del tráfico que transita por ella, cumpliendo a su vez con los requerimientos de ciertos parámetros relevantes para el usuario final. Esto puede entenderse también, como el cumplimiento de un conjunto de requisitos estipulados en un contrato (SLA: Service Level Agreement) entre un ISP (Internet Service Provider, proveedor de servicios de Internet) y sus clientes.

El protocolo de comunicación IPv4 (Internet Protocol Version 4) contiene especificaciones que permiten ejercer manipulaciones sobre estos paquetes, las cuales deben ser manejadas por los enrutadores al momento de implementar QoS. Sin embargo, en los últimos años, se han estado afinando detalles acerca de un nuevo estándar para el protocolo de Internet (IP), éste es llamado IPv6 (Internet Protocol Version 6), el cual contiene nuevas y reestructuradas especificaciones para ejercer QoS.

Al contar con QoS, es posible asegurar una correcta entrega de la información necesaria o crítica, para ámbitos empresariales o institucionales, dando preferencia a aplicaciones de desempeño crítico, donde se comparten simultáneamente los recursos de red con otras aplicaciones no críticas. QoS hace la diferencia, al prometer un uso eficiente de los recursos ante la situación de congestión, seleccionando un tráfico específico de la red, priorizándolo según su importancia relativa, y utilizando métodos de control y evasión de congestión para darles un tratamiento preferencial. Implementando QoS en una red, hace al rendimiento de la red más predecible, y a la utilización de ancho de banda más eficiente.

Entre los modelos de red retenidos por la IETF para ofrecer QoS, la arquitectura de Diferenciación de Servicios (DiffServ) propone la alternativa de ofrecer distintas clases de servicios basado en el tratamiento agregado de flujos individuales donde cada paquete es etiquetado de acuerdo al tratamiento que desearía recibir al interior de la red.Según el boletín del 9 de Marzo Del 2005 de la Comisión Interamericana de Telecomunicaciones apoyada por la OEA se indica que : *"En cuanto a la calidad de servicio (QoS), el IPv4 y el IPv6 difieren muy poco. Las arquitecturas y aplicaciones de Servicios Diferenciados (DiffServ) y Servicios Integrados (IntServ) son las mismas. El protocolo IPv6 puede alegar algunos campos extras en el encabezado que podrían utilizarse para fines de clasificación pero sin un valor particular. Se dice a menudo, sin embargo, que el IPv6 ofrece mejor QoS y que ello se debe a su "Etiqueta de Flujo". Si bien es cierto que este campo de encabezado puede ser un instrumento muy versátil tanto para la clasificación como para RSVP, su uso todavía tiene que definirse. "*

CAPITULO II

CALIDAD DE SERVICIO EN INTERNET

2.1 Introducción

Los últimos años, han sido testigos del rápido crecimiento de tráfico de redes que permiten en general agregar nuevas ventajas para tratar de responder al ritmo de la demanda creciente; es por eso que se generaron redes de telefonía fija, redes de telefonía móvil, Internet fijo, Internet móvil; es decir, se van creando nuevas necesidades que han evolucionado porque el avance de la tecnología así lo está permitiendo; es por ésta razón que se nota muy claramente que las aplicaciones que aparecen en el ámbito de las redes necesitan cada vez mas recursos . En la Fig.2.1 que sigue se presenta un esquema del comentario anterior.

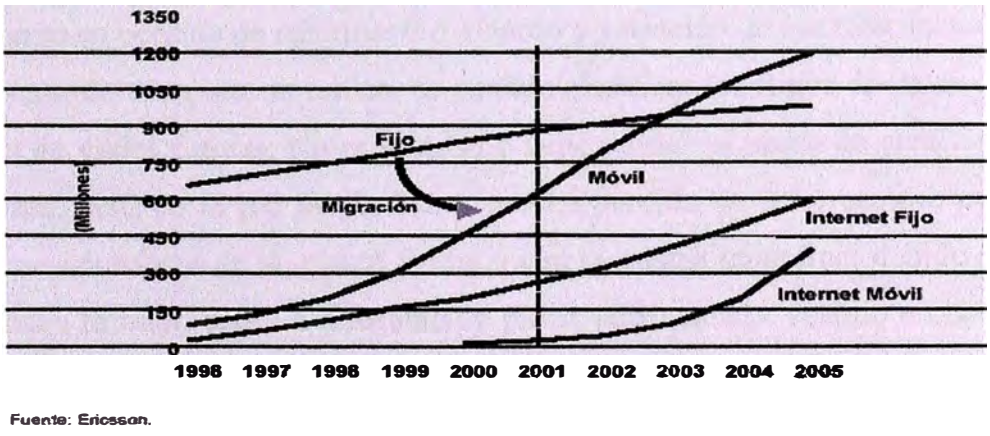


Fig. 2.1 Internet actual

Uno de los problemas mas importantes de los usuarios de la Internet actual, es que pasan gran parte de su tiempo en línea sin hacer otra cosa mas que esperar (esperar para

conectarse a un sitio web, esperar a que se carguen algunas páginas deseadas, esperar para bajar software, etc.) . Como contraste, la nueva generación de Internet (IPv6) nos proporcionará la velocidad que debemos tener.

La calidad de servicio(QoS) consiste en la capacidad que tiene la red de reservar recursos para atender a un tráfico concreto con la intención de proporcionar un determinado servicio. Se debe de tener en cuenta que en la red se pueden utilizar diferentes tecnologías de transporte (ATM, FRAME RELAY, SDH, etc) , de manera que la gestión de QoS implica la interacción de éstas tecnologías con los equipos de conmutación, que son los que finalmente determinarán el nivel de QoS que se va a alcanzar.

En resumen, QoS puede ayudar a mejorar el servicio a los usuarios de la red, al mismo tiempo que reduce los costos de ofrecer dichos servicios.

2.2 Clasificación de Flujos de Datos en Internet

En Internet, cada flujo de datos tiene sus propios requerimientos de calidad de servicio (QoS) . Las aplicaciones son las que fijan estos requisitos, basándose en la calidad que el usuario final espera recibir. Sin importar como, el cliente siempre espera recibir la máxima calidad posible, es decir, el usuario desea que la red no afecte en absoluto a su consumo de información. Ante la ausencia de éste caso ideal, el usuario se adapta a la tecnología disponible y soporta cierta degradación de ésa calidad. Esta degradación se traduce principalmente en pérdida de información, retardo y variación de ése retardo.

Según el punto de vista que se utilice, es posible clasificar los flujos de datos que circulan por Internet de varias formas. No es lo mismo verlos desde el punto de vista de aplicación, que de la red. Así, en la red puede haber mucha pérdida de información, pero desde la aplicación no apreciarse de la misma forma o con la misma magnitud, debido a protocolos que garanticen la fiabilidad. La información puede sufrir mucho retardo en la transmisión, y sin embargo la aplicación ni siquiera percibirlo si no necesita consultarla hasta después de haberla recibido toda (no se percibe la transmisión).Y exactamente lo mismo ocurre con la variación del retardo si la aplicación permite que haya mecanismos de sincronismo y reordenación de la información. Indudablemente, la calidad de servicio no tiene sentido sin un usuario final, por lo que a continuación se planteará la clasificación de los flujos de datos desde el punto de vista del usuario, o lo que viene a ser lo mismo, de la aplicación.

La clasificación se basará en la necesidad de las aplicaciones de utilizar un nivel de servicio mejor que el servicio clásico de *best-effort* . Por otra parte, se analizará lo estricto

que son los requisitos de la aplicación en cuanto a pérdidas y retardos. La variación del retardo no se tendrá en cuenta, ya que en el nivel de aplicación, ésta se puede traducir fácilmente en pérdidas o retardo.

2.2.1 Flujos Elásticos

Se considera que un flujo es elástico cuando no tiene requerimiento estricto en cuanto a pérdidas o retardo, y por lo tanto es suficiente el uso del servicio *best-effort.*

Generalmente, las aplicaciones no pueden aceptar que los datos que reciben lleguen con pérdidas y/o retardos, por lo que utilizan protocolos y mecanismos para reducir en la medida de lo posible uno de los dos casos o ambos. En la Internet actual, en la que se utiliza el servicio *best-effort*, se encuentran habitualmente dos grupos de aplicaciones de este tipo: las tolerantes al retardo (pero estrictas en cuanto a pérdidas) y las tolerantes a pérdidas (pero estrictas en cuanto a retardo). Las primeras utilizan protocolos fiables, tales como TCP (*Transmisión Control Protocol*), que garantizan la integridad de la información mediante la retransmisión de la información que se pierde. Este es el caso, por ejemplo del servicio de correo electrónico o del servicio FTP (*File Transfer Protocol*). Las segundas evitan las retransmisiones que ralentizan la transmisión, por lo que utilizan protocolos como el UDP (*User Datagram Protocol*) y RTP (*Real-Time Transport*). Además pueden utilizar técnicas adaptativas en la que se controla la cantidad de información que se envía en función del estado de la red, con tal de evitar las pérdidas en la medida de lo posible. Este es el caso de las aplicaciones de tipo *streaming.*

En una Internet presente y futura con necesidades de garantías de QoS, las aplicaciones con requerimientos temporales estrictos harán uso de ésas garantías para asegurar que la información llegue a tiempo, aún permitiendo ciertas pérdidas en los datos que se envían. En éste caso, los flujos no se considerarán elásticos, si no como se verá mas adelante, se podrán clasificar como inelásticos o semi-elásticos, ya que el servicio *best-effort* es insuficiente.

En éste escenario, quedarán por tanto como flujos elásticos las aplicaciones tolerantes al retardo (tales como el correo electrónico , el FTP citados anteriormente). En la figura que sigue (Fig. 2.2), se puede observar la relación que existe en éste caso entre el instante que se requiere la información y el instante en que la información llega a su destino. Como se aprecia en la figura, son flujos totalmente tolerantes al retardo, ya que la información no se precisa en un instante concreto de tiempo.

A continuación se examinarán los flujos con requisitos temporales estrictos que se caracterizan por tener un nivel de servicio superior al de *best-effort*.

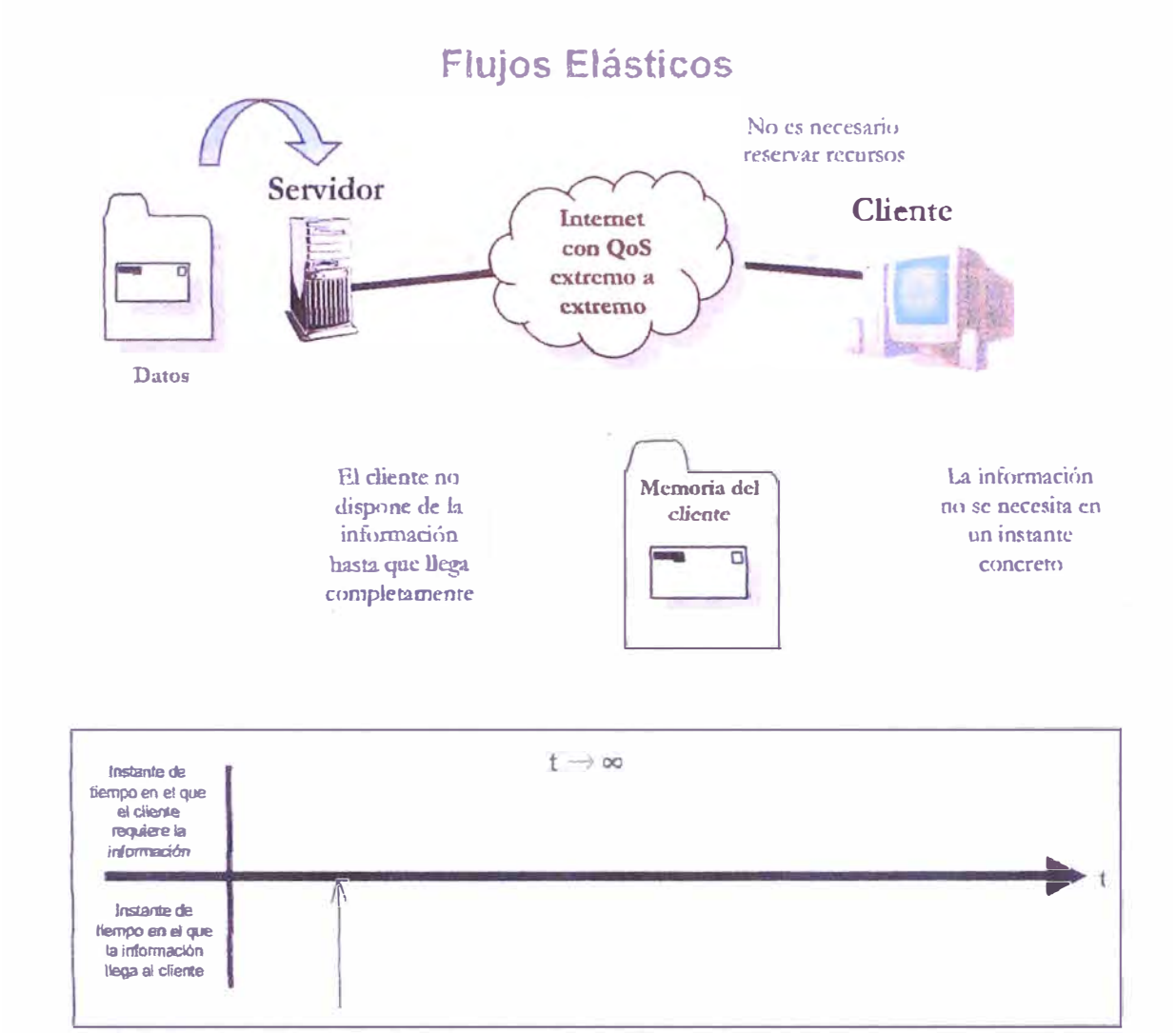


Figura 2.2 Flujos Elásticos

2.2.2 Flujos Inelásticos

Los flujos con requerimientos temporales de QoS muy estricto se definen como flujos inelásticos. En éste caso, la información suele generarse en directo y es esencial la reserva de recursos de la red durante toda la transmisión para poder asegurar su entrega sin degradar la QoS requerida (tal como se muestra en la Fig 2.3). Por otro lado, la información debe de llegar al destino en un instante de tiempo específico (próximo a la generación de la misma) para poder ser consumida. Un ejemplo de aplicaciones que utilizan este tipo de flujo es la transmisión de video en directo (tiempo real). Lógicamente, es posible que la aplicación tenga algún grado de tolerancia a pérdidas de información y

que por tanto, el nivel de QoS requerido sea algo menor. De todas maneras a medida que la oferta de QoS mejora, la tendencia de cualquier usuario es a requerir el nivel máximo de QoS posible por lo que las redes deben orientarse a servir a aplicaciones con requerimientos temporales fuertes.

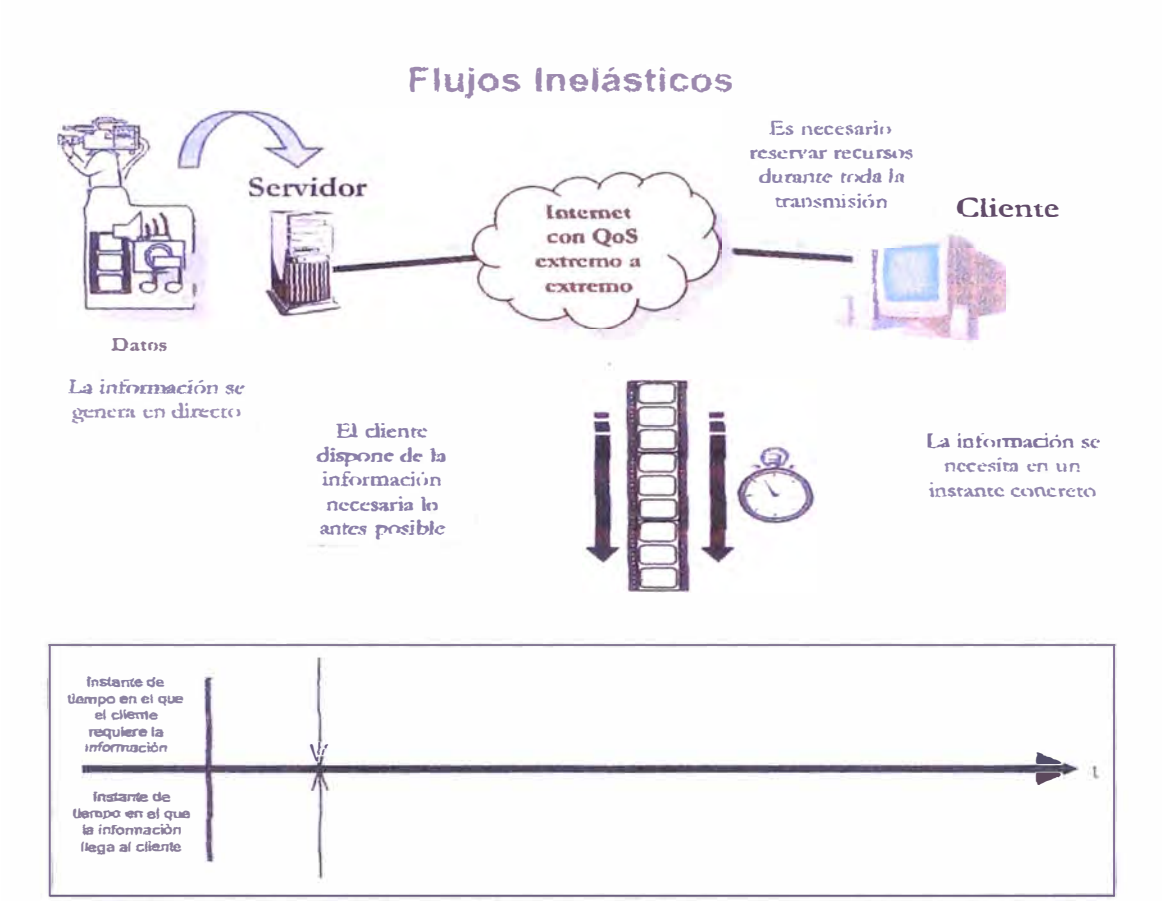


Fig. 2.3 Flujos Inelásticos

2.2.3 Flujos Semi-elásticos

Este flujo requiere un cierto nivel de QoS, pero a menudo no es necesario mantenerlo durante toda la transmisión. En este contexto, la información necesita llegar al cliente en un instante muy específico, como pasa con los flujos inelásticos, pero la red puede entregarla antes (Fig.2.4). Esto es lo que sucede con la información prealmacenada, como es el caso de los servidores denominados *continuous media servers*. Estos flujos, necesitan que la información se almacene en el extremo receptor en una memoria y se consume a una tasa de lectura concreta, por lo que lo único que hay que garantizar es la disponibilidad de suficiente información en esta memoria durante todo el tiempo.

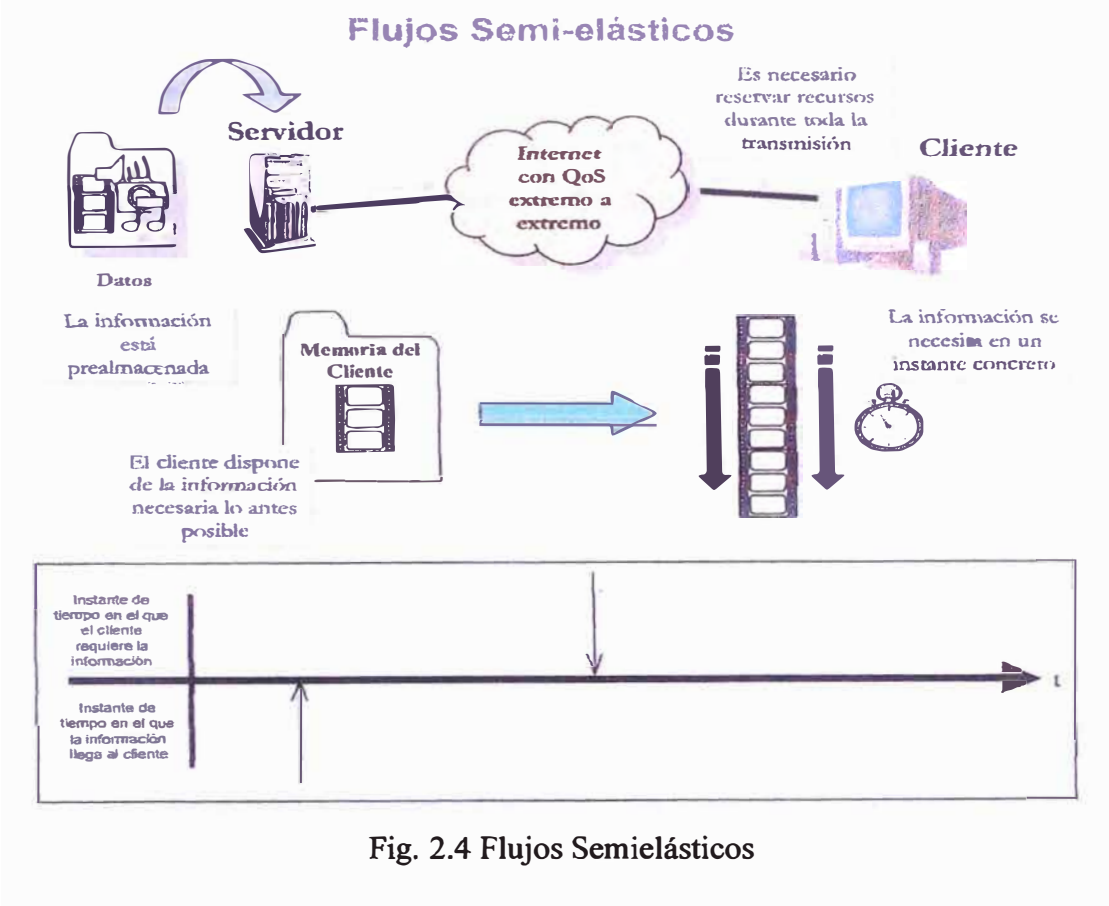


Fig. 2.4 Flujos Semielásticos

Es importante resaltar, que la diferencia entre los flujos inelásticos y semi-elásticos radica en la naturaleza del origen de la información (en directo o prealmacenada), y por lo tanto, en la necesidad de reservar recursos de la red durante toda o parte de la transmisión. Esta cantidad de recursos a reservar para los flujos semi-elásticos dependerá del estado de la red, es decir, de la tasa con que llegue la información utilizando el servicio best-effort, ya que una tasa más alta supondrá una mayor disponibilidad de información.

En cuanto a la tolerancia a pérdidas de este tipo de flujos, cabe destacar que como siempre pueden tener una cierta tolerancia, pero en este caso y debido a la posibilidad de entregar la información antes de que se necesite será habitual el uso de técnicas para garantizar la fiabilidad y evitar al máximo la pérdida de información.

2.3 Como funciona QoS

Toda aplicación genera tráfico a ritmos variables y requieren que la red pueda transportar tráfico al mismo ritmo que las aplicaciones lo han generado. Las aplicaciones son mas o menos tolerantes a diversos retrasos en el tráfico de la red y a la variación de los mismos. Algunas aplicaciones pueden tolerar cierto grado de pérdida de tráfico, mientras que otras

no. Si se contara con recursos de red ilimitados, todo el tráfico de las aplicaciones podrían transportarse al ritmo requerido, sin latencia ni pérdidas de paquetes.

Sin embargo, los recursos de red no son infinitos. Como consecuencia, hay partes de la red en las que los recursos no pueden responder a la demanda. La red está construida mediante la unión de dispositivos de red, tales como modificadores y enrutadores, los cuales se intercambian entre ellos el tráfico mediante interfaces. Si la velocidad en la que el tráfico llega a una interfaz es superior a la velocidad en la interfaz puede enviar el tráfico al siguiente dispositivo, se produce una congestión. De ésta forma la capacidad de una interfaz para enviar tráfico constituye un recurso de red fundamental.

Los mecanismos de QoS funcionan al establecer preferencias en la asignación de éste recurso a favor de cierto tráfico. Para poder realizar ésta acción, es necesario identificar tráficos diferentes. El tráfico que llega a los dispositivos de red se separa en distintos **flujos** mediante el proceso de **clasificación de paquetes**. El tráfico de cada flujo se envía a una **cola** en la interfaz de reenvío. Las colas de cada interfaz se **gestionan** de acuerdo a algunos algoritmos. El algoritmo de la administración de cola determina la velocidad a la que se reenvía el tráfico de cada cola. De éste modo, se determinan los recursos que se asignan a cada cola y a los flujos correspondientes. Para proporcionar QoS en las redes, es necesario configurar y proporcionar a los dispositivos de red lo sgte:

a) Información de clasificación por la que los dispositivos separan el tráfico en flujos.
b) Colas y algoritmos de administración de colas que controlan el tráfico de los diferentes flujos.

Nos referiremos a ambos como mecanismos de control de tráfico. Los mecanismos de control del tráfico por separado no resultan útiles. Deben proporcionarse o configurarse a través de muchos recursos de una forma coordinada que proporcione servicios de un extremo a otro en una red. Para proporcionar servicios útiles, son necesarios tanto los mecanismos de control de tráfico como los mecanismos de provisión y configuración.

2.4 Tecnologías de QoS

En los siguientes apartados, se estudian los principales mecanismos de control del tráfico y de provisión y configuración.

2.4.1 Mecanismos de control de tráfico

Están disponibles varios mecanismos de control del tráfico. Este apartado se centra en varios mecanismos clave: servicios diferenciados(diffserv), 802.1p, servicios integrados(intserv), ATM e ISSLOW. Se debe de tener en cuenta que los mecanismos de control del tráfico se pueden clasificar en mecanismos por conversación o mecanismos por acumulación. Los mecanismos por conversación tratan por separado cada flujo de tráfico para cada conversación. Los mecanismos por acumulación agrupan varios flujos de tráfico en una única clase acumulada. La distinción es parecida al tratamiento de los pasajeros de un avión. Los pasajeros se suelen clasificar en primera clase, clase business y clase turista. Todos los pasajeros de la misma clase tienen el mismo tratamiento. Esto es el tratamiento por acumulación. El tratamiento por conversación es parecido a proporcionar un avión especializado para cada pasajero, resultando evidentemente mas caro.

a) Servicios Diferenciados (Diffserv)

Diffserv es un mecanismo de tratamiento del tráfico por acumulación apropiado para las grandes redes enrutadas. Estas redes pueden transportar varios miles de conversaciones, debido a que no resulta práctico tratar el tráfico por conversación individual. Diffserv define un campo en los encabezados IP de los paquetes, conocido como Diffserv Codepoint (DSCP)[1]. Los host o los enrutadores que envían tráfico a una red Diffserv marcan cada paquete transmitido con el valor DSCP. Los enrutadores de una red Diffserv utilizan DSCP para clasificar paquetes y para aplicar un comportamiento de cola específico basado en los resultados de la clasificación.

El tráfico de varios flujos con requisitos de QoS parecidos se marca con el mismo DSCP, al agregar el flujo a una cola común o al programar el comportamiento.

b) 802.1p

802.1p es un mecanismo de control del tráfico de acumulación apropiado para el uso en muchas redes de área local (LAN).

Define un campo en el encabezado de acceso al medio (MAC) de los paquetes Ethernet, que puede transportar uno de los ocho valores preferentes. Los hosts o los enrutadores que envía tráfico a una LAN marcan cada paquete transmitido con el valor de preferencia adecuado. Los dispositivos LAN, tales como modificadores, puentes o concentradores deben tratar los paquetes de forma adecuada. El ámbito de la marca de preferencia 802.1p

1 DSCP, es un campo de 6 bits que expande los campos antes conocidos de tipo de servicio (TOS) y campos de prioridad IP.

está limitado a la LAN.

c) Servicios Integrados (IntSserv)

Intserv es una estructura para definir servicios. Como tal, incluye un conjunto de mecanismos de control de tráfico subyacentes. Los servicios Intserv se suelen aplicar por conversación individual. Normalmente, aunque no de forma necesaria, Intserv se asocia con el protocolo de señalización RSVP (tratado en el apartado referente a los mecanismos de provisión y configuración).

d) ATM, ISSLOW y otros

ATM es una tecnología de capa de enlace que ofrece un tratamiento del tráfico de alta calidad. ATM divide los paquetes en celdas de capa de enlace y a continuación, se envían a la cola y se controlan con los algoritmos de administración de cola adecuados para uno o varios servicios ATM.

ISSLOW es una técnica para dividir paquetes IP a medida que se transmiten a través de vínculos de velocidad relativamente lenta, tales como las conexiones telefónicas a módems. Cuando se mezclan datos y sonidos en estos vínculos, las latencias de la señal de audio pueden ser considerables y afectan al uso de la aplicación. Se puede utilizar ISSLOW para reducir las latencias de audio en estas aplicaciones.

2.4.2 Mecanismos de provisión y configuración

Para conseguir una provisión efectiva de QoS de red, es necesario desarrollar de forma continua los mecanismos de provisión y configuración del tratamiento del tráfico descritos a través de dispositivos de red múltiples. Se pueden clasificar los mecanismos de provisión y configuración en de arriba a abajo o señalizados.

a) Provisión de arriba a abajo

En la provisión de arriba a abajo, se utiliza un sistema de administración de red para "insertar" la configuración del tratamiento del tráfico en un conjunto de dispositivos de red. Normalmente, los mecanismos de cola están configurados en interfaces de dispositivos. A continuación, se configuran los criterios de clasificación para determinar qué paquetes se envían a cada cola del dispositivo. Los criterios pueden clasificar los paquetes tomando como referencia tupla IP 5 (direcciones y puertos IP de origen y de destino y el protocolo IP) o DSCP y "marcas" de acumulación 802.1p en los encabezados de los paquetes. Se pueden utilizar tuplas 5 con máscara.

Los criterios de clasificación pueden especificar sólo un subconjunto de tuplas 5, por ejemplo, "todos los paquetes con una dirección IP de origen de 2.2.2.X", donde "X" puede ser cualquier valor. Si DSCP o 802.1p se especifican como criterios de clasificación, es necesario "señalar" las marcas DSCP o 802.1p en los paquetes en la parte ascendente del dispositivo de clasificación. Los host o los dispositivos de red que se encuentran cerca del extremo de la red pueden realizar esta acción. En el segundo caso, se configurarían los dispositivos de red de señalización para realizar las marcas tomando como referencia sus propios criterios de clasificación, normalmente, tupla 5 (o algún subconjunto).

a.1) Problemas en la provisión de arriba a abajo

Puede resultar complicado determinar los criterios de clasificación adecuados. Los administradores de redes preferirían utilizar QoS para asignar recursos al tráfico de ciertas aplicaciones o usuarios, en lugar de campos en encabezados de paquetes, tales como direcciones o puertos IP. Los sistemas de provisión de arriba a abajo tratan de ayudar al administrador de la red al crear enlaces entre aplicaciones y puertos IP y entre usuarios y direcciones IP. Desafortunadamente, no se puede confiar plenamente en estos sistemas porque las aplicaciones pueden utilizar puertos transitorios o crear un origen común en un puerto para varios flujos de tráfico (que requieren QoS diferentes). Las direcciones IP de los usuarios pueden variar como resultado de DHCP. Los equipos multiusuario pueden utilizar la misma dirección IP para varios usuarios. El cifrado IPSec puede cifrar puertos IP, lo que los convierte en criterios de clasificación que no se pueden utilizar.

Un problema adicional en la provisión de arriba a abajo es la anticipación de los volúmenes de tráfico en varios nodos de la red. Por ejemplo, se puede utilizar un sistema de administración para configurar una cola de baja latencia en cada dispositivo de red, con una capacidad para tratar diez sesiones simultáneas de telefonía IP con ciertos límites de latencia especificados. A continuación, se configuran los criterios de clasificación en cada dispositivo para transmitir el tráfico de telefonía IP a las colas de baja latencia. Este proceso funciona correctamente siempre y cuando el tráfico de telefonía que llega a cada dispositivo está limitado a diez sesiones. Sin embargo, si se establece una undécima sesión que recorre uno de los dispositivos configurados, se congestionará la cola de baja latencia y se elevará el nivel de latencia por encima del límite especificado. Como consecuencia, el servicio pondrá en peligro la undécima sesión así como las diez sesiones existentes, esto se debe a la naturaleza relativamente estática de la provisión de arriba a abajo y al hecho de

que el sistema de administración no es directamente compatible con los patrones de tráfico actuales.

a.2) Señalización RSVP como mecanismo de reconfiguración

La señalización RSVP se puede utilizar para complementar los mecanismos de provisión de arriba a abajo. En este caso, los hosts generan mensajes de señalización que describen el tráfico de datos relacionado con una conversación en particular. Estos mensajes fluyen por la misma ruta que el tráfico de datos tomaría en la red. Los mensajes RSVP ofrecen la siguiente información a la red:

- Qué soy ? (Por ejemplo, flujo de impresión frente a transacción crítica en el tiempo).
- Quién soy ? (Id. de usuario autorizado).
- Qué deseo hacer ? (tipo de servicio QoS necesario).
- Cuánto deseo ? (ciertas aplicaciones cuantifican los requisitos de recursos de forma precisa).
- Cómo se me puede reconocer ? (criterio de clasificación de tupla 5 por el que se reconoce el tráfico de datos).
- Qué recursos de dispositivos de red se verán afectados por el tráfico de datos asociado?

La señalización basada en host ofrece ventajas importantes a los sistemas de administración de QoS. Como ventaja evidente se puede destacar que la señalización basada en host proporciona enlaces fuertes entre la información de clasificación ,los usuarios y las aplicaciones. Además, este tipo de señalización ofrece control de admisión dinámica compatible con la topología. Esta característica es clave para solucionar "la undécima sesión" descrita anteriormente. La señalización RSVP envía un mensaje relativo a los recursos necesarios hacia los dispositivos en la ruta de los datos. Por tanto, los dispositivos compatibles con RSVP son capaces de evaluar de forma dinámica las repercusiones que tendría el tráfico de datos asociados en los recursos y de notificar a los dispositivos ascendentes cuando no tienen los recursos necesarios para controlar los flujos de tráfico adicionales. En el caso de la "undécima sesión de telefonía", los dispositivos de red rechazarán la admisión del undécimo flujo de tráfico en la cola de baja latencia. De esta forma, se protegen las diez sesiones existentes. Es importante darse cuenta de que la señalización basada en host no impide el control del administrador de la red sobre los

recursos de red, simplemente ofrece información a la red que se puede utilizar para facilitar la administración de los recursos de red.

2.5 Parámetros relevantes de QoS de la red

Los parámetros más importantes de la red, a considerar para las aplicaciones de cara al futuro , son los siguientes:

- Throughput.
- Retardo.
- Variación del retardo.
- Tasa de error.

2.5.1 El Throughput es la velocidad efectiva o ancho de banda efectivo. Se define como la velocidad en la línea menos las cabeceras introducidas por las diferentes tecnologías utilizadas. Además de las cabeceras, hay que considerar las pérdidas de mensajes debidas a la congestión, a errores de transmisión, cuellos de botella, etc.

2.5.2 El retardo es uno de los parámetros más importantes. Hay muchos tipos de retardo, pero nos referiremos al retardo extremo a extremo, que es el tiempo que tarda la red en transmitir un mensaje entre dos sistemas finales.

2.5.3 El jitter o variación del retardo. Cuando se transmite vídeo y el correspondiente audio, normalmente se envían en flujos separados. En una red de conmutación de paquetes, estos flujos son divididos en bloques discretos de datos, siendo cada bloque transmitido en secuencia; si la red es capaz de transmitir todos los bloques con el mismo retardo, entonces cada bloque llegará al destino con un retardo uniforme. Muchas redes no pueden garantizar retardos uniformes por lo que se produce un jitter en la transmisión. El jitter debe tener un límite máximo superior.

2.5.4 La tasa de error puede venir dada de diferentes maneras. Una de ellas es la tasa de error por bit, que se define como el cociente entre el número medio de bits erróneos y el número total de bits transmitidos. Otra forma de medición puede ser la tasa de errores por paquete, que se define de manera análoga pero en relación con los paquetes transmitidos. Algunos ejemplos de tasa de error por bit son para fibra óptica de 10^{-9} a 10^{-12} y para sistemas por satélite de 10^{-7}. Los errores pueden tener poca importancia, como en el caso de audio o vídeo, o ser trascendentales en el caso de estar transmitiendo datos.

En la Fig.2.5 se muestra un esquema de las 4 características mencionadas

EL PROBLEMA DE QoS

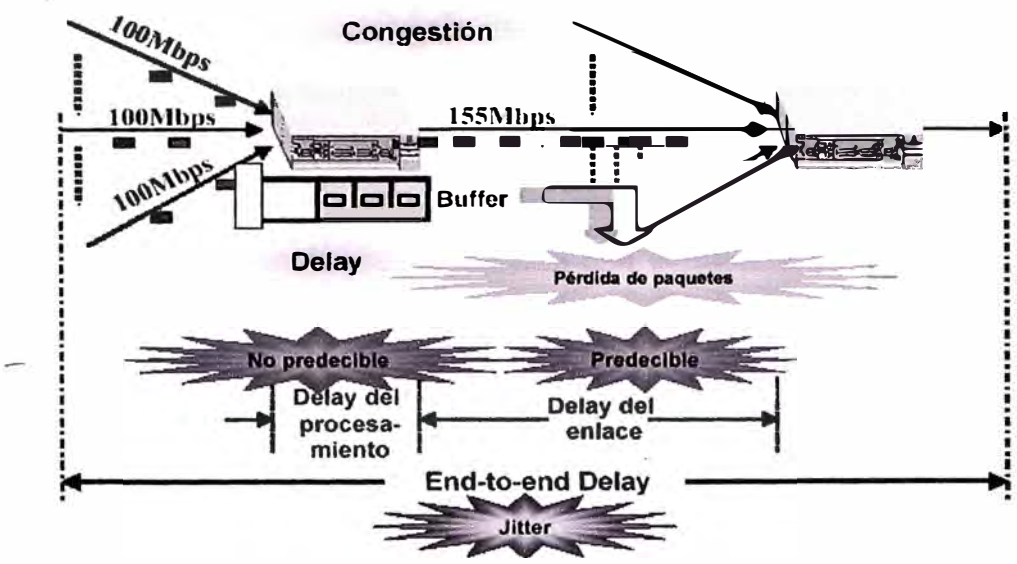


Fig. 2.5 Parámetros de Calidad de Servicio

2.6 Diferentes Arquitecturas con Calidad de Servicio

En Internet hay principalmente dos enfoques para soportar la calidad de servicio:

a) ***Reserva de recursos*** **(Servicios Integrados),** los recursos de la red son reservados en base a los requerimientos de calidad de servicio de las aplicaciones.

b) ***Priorización*** **(Servicios Diferenciados),** el tráfico de red se clasifica y los recursos de la red se asignan de acuerdo a la política de gestión del ancho de banda. La QoS se consigue al dar la red un trato preferencial al tráfico clasificado como de más demanda.

La calidad de servicio se puede aplicar a sesiones individuales o a sesiones agregadas. En las primeras, una sesión se define como un flujo de datos unidireccional entre dos aplicaciones, identificado por las mismas 5 coordenadas de una sesión en Internet (protocolo de transporte, dirección IP origen y destino, puerto origen y destino). En las agregadas hay varias sesiones que tiene alguna identificación en común, puede ser una o varias de las 5 coordenadas, o una etiqueta. Todas las sesiones agregadas reciben la misma QoS.

Para cubrir las diferentes necesidades de calidad de servicio hay varios protocolos y arquitecturas que se enumeran a continuación:

a) ***Servicios Integrados*** **(Protocolo RSVP),** que permite a las aplicaciones solicitar la QoS y puede usarse con sesiones agregadas o individuales.

b) ***Servicios Diferenciados*** **(Differentiated Services,** ***DiffServ*****),** que es una arquitectura que suministra una forma sencilla de clasificar y priorizar el tráfico.

c) ***Conmutación de etiquetas multiprotocolo*** **(Multi Protocol Labeling Switching, MLPS),** inicialmente ideado para acelerar el proceso de transmisión de los datagramas IP en la red, añadiendo una etiqueta a la cabecera y efectuando la conmutación en base a ella, también permite controlar el ancho de banda asignado a una sesión.

d) ***El gestor de ancho de banda de subred (Subnet Bandwidth Manager, SMB)***.Es necesario para mantener la QoS en los enlaces IP sobre Ethernet o Token Ring compartidos o conmutados.

Las tecnologías de QoS anteriores no son excluyentes, sino complementarias

Hay varias arquitecturas, como veremos posteriormente, en las que estos protocolos funcionan juntos para suministrar calidad de servicio. Un problema que se plantea con los protocolos enumerados es que, en muchos casos, los estándares no están lo suficientemente desarrollados.

El encaminamiento IP debe ser cambiado ya que escoge la ruta más corta, no la ruta por donde se puede soportar una determinada QoS.

En los siguientes apartados describimos en detalle las tecnologías anteriores, sus mecanismos y funcionalidades.

2.6.1 Servicios Integrados (IntServ)

En 1994 la comunidad de Internet empezó a definir la Arquitectura de Servicios Integrados (Integrated Services Architecture, IntServ) que pretendía ampliar la arquitectura IP existente para soportar sesiones en tiempo real, manteniendo el servicio best-effort existente [RFC1633].

La arquitectura IntServ define un flujo como una corriente de paquetes con la dirección origen y destino, puerto origen y destino, iguales. IntServ sugiere que para dar QoS a un flujo, la red debe hacer un seguimiento del estado del flujo.

Los componentes básicos de la arquitectura IntServ son los siguientes:

- El control de tráfico, que a su vez incluye a otros tres. El primero es el control de admisión, que comprueba que existen recursos suficientes para soportar el servicio. El segundo es el clasificador de paquetes, el cual analiza los campos de direcciones

y puertos para determinar la clase a la que pertenece el paquete. El tercero es el algoritmo de encolado que gestiona la transmisión de los paquetes por un enlace de salida.

- Las clases de tráfico, que ofrecen dos tipos de servicios: garantizados y de carga controlada, además del best-effort. Los primeros emulan a los circuitos dedicados, garantizando los parámetros de la especificación del tráfico del emisor [RFC2212]. Los segundos son equivalentes al servicio best-effort en condiciones de red descargada [RFC2211] y que suministran mejor servicio que el best-effort, pero no hay garantías como en los primeros.
- Un protocolo, para que una aplicación pida un determinado servicio a la red. El protocolo entrega la petición al control de tráfico de cada enrutador, que comprobará si es viable la petición; éste protocolo es el RSVP, que describimos a continuación.

a. Protocolo de reservas (RSVP)

RSVP es un protocolo de señalización que permite el establecimiento y el control de los denominados Servicios Integrados. RSVP es el más complejo de todas las tecnologías de QoS, tanto para los sistemas finales como para los enrutadores de la red. También representa el mayor cambio con relación al servicio *best-effort* de IP, RSVP tiene el mayor nivel de calidad de servicio en términos de servicios garantizados y también la mayor granularidad de los mismos. RSVP es un protocolo situado a nivel 4 o de transporte. El funcionamiento de RSVP es el siguiente:

- El emisor envía un mensaje denominado PATH, con su especificación de tráfico, hacia el destino o destinos. El propósito del mensaje PATH es el de marcar la ruta entre emisor y receptor además de recolectar información sobre la viabilidad de la solicitud a lo largo del camino. La especificación anterior incluye los valores máximo y mínimo de ancho de banda, retardo y variación del mismo. Cada encaminador va grabando la ruta por la que va circulando el mensaje de PATH, añadiendo la dirección IP de donde viene el mensaje, para que después pueda reconstruirse la ruta de vuelta. Al llegar el mensaje PATH al receptor o receptores, pueden medir que tipo de servicio puede soportar la red.
- Es el receptor o receptores los que realmente hacen la reserva de recursos, al enviar un mensaje RESV. Dicho mensaje incluye además de la especificación

de tráfico recibida del emisor, la especificación requerida por el receptor, que consta del tipo de Servicio Integrado solicitado y un filtro que selecciona los paquetes con una determinada característica (por ejemplo protocolo y número de puerto) a los que se va aplicar la reserva. El identificador de sesión que utilizan los enrutadores está compuesto por el tipo de Servicio Integrado y el filtro.

- Cuando un enrutador recibe un mensaje tipo RESV, usa el control de admisión para aceptar o no la reserva. En caso positivo se hace la reserva y el mensaje RESV progresa hacia el siguiente enrutador en la dirección del emisor. En caso contrario se envía un mensaje de error al receptor.
- Si el enrutador no soporta RSVP retransmite los mensajes RSVP de forma transparente. En estos enlaces no se puede garantizar la calidad de servicio, lo que implica que puede perderse la calidad de servicio extremo a extremo.
- Si el último enrutador efectúa la reserva envía un mensaje de confirmación al receptor.
- Cuando la sesión termina debe indicarse, para liberar los recursos de la reserva.

Se exponen, a continuación, las características más importante de los mecanismos del protocolo RSVP:

- Las reservas no son permanentes y deben ser refrescadas periódicamente con mensajes PATH y RESV.
- Se necesita un interfaz para que las aplicaciones se comuniquen con RSVP. Las aplicaciones suministran la especificación de tráfico, inician el proceso de reserva y reciben la correspondiente notificación acerca de lo que ha ocurrido con la misma. También deben ser informadas de lo que pueda suceder a lo largo de la existencia de la sesión.
- Las reservas las efectúa el receptor, para soportar grandes y heterogéneos grupos receptores de multidifusión.

Como se ha indicado anteriormente, RSVP permite a una aplicación especificar la mayor granularidad y la mejor calidad de servicio posible. El precio que hay que pagar por ello es una mayor complejidad y procesamiento, lo cual no es apropiado para muchas aplicaciones y partes de la red. Por ello se han propuesto métodos más sencillos, como el *DiffServ* que será descrito más adelante. Los servicios ofrecidos por intServ son mostrados en la Tabla 2.1

Tabla 2.1 Tipos de Servicio en InterServ

Servicio	Características	Equivalencia en ATM
Garantizado	▪ Garantiza un caudal mínimo y un retardo máximo. ▪ Cada router del trayecto debe dar garantías.	CBR VBR-t
Carga controlada	▪ Calidad similar a la de una red de datagramas poco cargada ▪ Se supone que el retardo es bajo , pero no se dan garantías.	VBR-nrt
Best Effort	▪ Ninguna garantía(como antes sin QoS	UBR

2.6.2 Servicios Diferenciados (DiffServ)

Los servicios diferenciados (Differenciated Services,*DiffServ*) son una forma sencilla de clasificar los servicios de las aplicaciones,aunque su simplicidad no da idea de su potencia y flexibilidad.Es una tecnología que trabaja en nivel 3.

Varios factores condujeron a su diseño, en primer lugar debía ser escalable, para ello se utiliza la agregación de varias sesiones en una que recibe el mismo tratamiento. También debía poder ser utilizada con todas las aplicaciones y no requerir un protocolo especial de control o un nuevo interfaz de programación como RSVP. Además hay que tener en cuenta, que los grandes avances en las velocidades de transmisión no aconsejan que los enrutadores centrales sean cargados con el seguimiento de cada sesión; es más eficiente y escalable hacer un seguimiento de cada tipo de servicio.

El funcionamiento de *DiffServ* se basa en clasificar las sesiones a la entrada de la red en relación con un determinado servicio y después aplicarle el correspondiente tratamiento dentro de la red.

La clasificación a la entrada en la red está basada en el análisis de uno o varios campos de la cabecera del paquete. Después el paquete se marca, en algún campo de la cabecera como perteneciente a una determinada clase de servicio. Los enrutadores centrales sólo examinan el campo donde se marcó el paquete y le dan el tratamiento correspondiente a esa clase de servicio. Finalmente, antes de salir de la red se suprime la marca. El marcado del tráfico lo

realizan los enrutadores de acceso, aunque también los terminales finales pueden realizarlo [RFC2475].

El protocolo *DiffServ* usa un byte de la cabecera del paquete, denominado campo DS, para marcar el tipo de servicio [RFC2474]. En el caso de IPv4 se redefine el byte de tipo de servicio (Type-of-Service, TOS) [RFC791] como el campo DS. Para IPv6 se utiliza el byte de clase de tráfico (Traffic Class). De los 8 bits del campo DS actualmente se utilizan 6 bits para los puntos denominados de código DS (code points DS, CPDS) [RFC2474], estando los otros 2 bits sin definir todavía.

Al tipo de servicio se le denomina comportamiento del nodo (Per-Hop Behavior, PHB), que será el tratamiento que tenga cada paquete en cada nodo de la red. Un comportamiento agregado (*Behavior Aggregate*) se define para un grupo de paquetes con el mismo CPDS. Un mismo PHB o servicio, es aplicado a cada comportamiento agregado dentro de la red.

Aunque hay más posibilidades, se han definido dos tipos de niveles de servicios:

- ***Reenvío rápido* (Expedited Forwarding, EF),** que tiene minimizado las pérdidas, retardos y variación de los mismos. Es un servicio similar a las líneas alquiladas. El tráfico que exceda el perfil declarado será descartado [RFC2598]. Para ello el tráfico es conformado en los enrutadores de acceso, para no superar la máxima velocidad. Por supuesto esta velocidad debe ser menor que la mínima velocidad de los enlaces de salida de cada enrutador en la red. El EF PHB utiliza un solo bit PDS para indicar que el paquete debe ser colocado en la cola de máxima prioridad.
- ***Reenvío asegurado* (Assured Forwarding, AF),** tiene 4 clases con 3 procedimientos en cada clase que determinan como descartar tráfico. Doce combinaciones CPDS definen las clases AF de precedencia a la hora de tirar los paquetes. Cuando hay congestión en un enrutador los paquetes con mayor precedencia son desechados primero. Las cuatro clases AF no definen un ancho de banda o retardo específico sino que la clase 1 es distinta de la clase 2 y así sucesivamente. El tráfico AF en exceso no es entregado con la misma probabilidad que el tráfico cumplidor, es decir puede ser degradado pero no necesariamente descartado [RFC2597].

DiffServ asume la existencia de un acuerdo entre el usuario y la red, en el nivel de servicio (Service Level Agreement SLA). El SLA establece el perfil del tráfico (ancho de banda, retardo, *jitter* y tasa de pérdidas) y la política (tiempo de disponibilidad, penalizaciones, etc). Se espera que el tráfico sea conformado y espaciado en la entrada

en la red con arreglo al SLA y cualquier tráfico no conforme no tendrá calidad de servicio. *DiffServ* ha sido escogida como la tecnología para soportar la QoS en la Internet2 en la iniciativa conocida como QBone . Las razones que han llevado a esta decisión son las siguientes :

- Flexibilidad, para implementar los diferentes requerimientos de servicios de las aplicaciones avanzadas.
- Escalabilidad, al liberar al núcleo de la red de los procesos más complejos.
- Interoperabilidad, al estandarizar el comportamiento por nodo, más que servicios particulares o algoritmos de encolado.

2.6.3 Etiquetas multiprotocolo (MPLS)

La conmutación por etiquetas multiprotocolo (Multi-Protocol Label Switching, MPLS) es similar a *DiffServ* en algunos aspectos. MPLS también marca el tráfico al entrar en la red, marca que desaparece al salir de la misma. Pero esta marca se utiliza de forma diferente, en *DiffServ* sirve para determinar la prioridad dentro del encaminador. En MPLS la marca simplifica la conmutación al determinar el siguiente encaminador. No está controlado por las aplicaciones, no existen llamadas a MPLS y tampoco existe componente MPLS en los sistemas finales, el protocolo reside sólo en los encaminadores. MPLS es independiente del protocolo superior, de ahí lo de multiprotocolo, por lo que puede usarse con otros protocolos de red o directamente sobre la capa de enlace . MPLS es más un protocolo de ingeniería de tráfico que un protocolo de QoS.

Establece unas conexiones con ancho de banda fijo. Dichas conexiones pueden ser ATM o Frame Relay. La principal ventaja de MPLS es que se simplifica el proceso de encaminamiento, reduciendo el procesamiento y aumentando el rendimiento. Una vez establecida la ruta no se analiza la cabecera IP para hacer el encaminamiento, sólo se analiza la etiqueta, por lo que se conmutan los paquetes en vez de encaminarse .

El funcionamiento de MPLS es el siguiente:

- El encaminador de acceso toma una decisión de retransmisión basada habitualmente en la dirección de destino, después determina el valor de la etiqueta, la adjunta al paquete y lo retransmite.
- El siguiente encaminador utiliza la etiqueta de forma similar a como funciona un encaminador orientado a conexión, con ella busca en una tabla reducida de circuitos virtuales abiertos obteniendo el siguiente encaminador y la nueva etiqueta.

Por último, adjunta la nueva etiqueta y se reexpide. De esta forma se reduce el trabajo que tienen que hacer los encaminadores.

La etiqueta representa la ruta que seguirán y con la política de asignación se puede controlar el tráfico. El aspecto más complejo es la distribución y gestión de las etiquetas entre los encaminadores MLPS, para asegurar el acuerdo en el significado de las distintas etiquetas. Para ello se ha diseñado un protocolo específico, el Protocolo de distribución de Etiquetas (Label Distribution Protocol, LDP) , aunque pueden usarse otros protocolos como RSVP o BGP

2.6.4 Gestión del ancho de banda de subred

No hay que olvidar que la calidad de servicio extremo a extremo, será tan buena como lo sea el peor de los enlaces.

También debe haber QoS en los sistemas finales, de forma que las aplicaciones pueden solicitarla explícitamente o bien los sistemas operativos implícitamente. Cada capa de la torre de protocolos debe soportar calidad de servicio, para dar el tratamiento adecuado a cada tráfico.

Los enlaces LAN que intervengan en la comunicación, también deberán soportar QoS, para que no se pierda la calidad de servicio. Las tecnologías descritas anteriormente eran de nivel 3 (*DiffServ*) o superiores (RSVP) por lo que también es necesaria una tecnología que de QoS a nivel 2. Los estándares IEEE 802.1p, 802.1Q y el 802.1D definen como Ethernet puede soportar calidad de servicio. Existe un grupo de trabajo del IETF el ISSLL (Integrated Services over Specific Link Layers) que tiene por objetivo implementar los Servicios Integrados de Internet dentro de las tecnologías de subred específicas . También trabaja en definir la traducción entre los protocolos de calidad de servicio, de los niveles superiores a las tecnologías de nivel 2. Como resultado de ello se ha desarrollado, recientemente, el gestor de ancho de banda de subred (Subnet Bandwidth Manager, SMB) para redes compartidas o conmutadas, como Ethernet, Token Ring, etc. SMB es un protocolo de señalización , que permite la comunicación y señalización entre los sistemas finales y los conmutadores . Además permite la traslación con los protocolos de QoS de niveles superiores .

El requisito fundamental de SBM es que todo el tráfico pase a través de, al menos, un conmutador SBM. Los componentes de SBM son:

- *El gestor del ancho de banda* (Bandwidth Allocator, BA), que mantiene el estado del los recursos en la subred y realiza el control de admisión. El BA puede estar en el sistema final o en los conmutadores.
- *El módulo de peticiones* (Requestor Module), que está situado sólo en los sistemas finales. La función del módulo es la traducir la calidad de servicio de niveles superiores al nivel 2 de acuerdo con las políticas definidas por el administrador.

El protocolo SBM tiene mecanismos de señalización de módulo de peticiones BA y BA-BA para hacer reservas, preguntar al BA por los recursos disponibles y cambiar o liberar reservas. SBM especifica un interfaz de llamadas con las capas superiores. Es independiente de los protocolos de niveles superiores y debe trabajar con cualquier protocolo de QoS de nivel superior.

IEEE 802.1p utiliza 3 bits (que son parte de la cabecera IEEE 802.1Q) que pueden representar 8 niveles de prioridad. La traducción del tipo de servicio al valor por defecto es la de Tabla 2.2 .

Tabla 2.2: Traslación de tipo de servicio a valor de prioridad en IEEE.802.1p.

Valor	Prioridad	Servicio
0	0	*Best-effort* (por defecto)
1	1	Reservado, menos que el *best-effort*
2	2-3	Reservado
3	4	Sensible al retardo, sin limite
4	5	Sensible al retardo, limite 100 mseg.
5	6	Sensible al retardo, limite 10 mseg.
6	7	Control de red

2.6.5 Combinación de diferentes técnicas de QoS

Las tecnologías de QoS explicadas anteriormente en la práctica no se van a utilizar de forma excluyente y de hecho están diseñadas para ser utilizadas de forma conjunta con otras tecnologías para dar soporte a la QoS extremo a extremo.

La mayoría de las especificaciones de cómo se interrelacionan las diferentes tecnologías de calidad de servicio no están todavía estandarizadas, pero se han previsto varias arquitecturas para soportar calidad de servicio extremo a extremo.

La Fig.2.6 muestra como pueden interacionar las anteriores tecnologías. Podemos observar que para conseguir la calidad de servicio extremo a extremo, hay que realizar una actuación en cada nivel de la torre de protocolos TCP/IP.

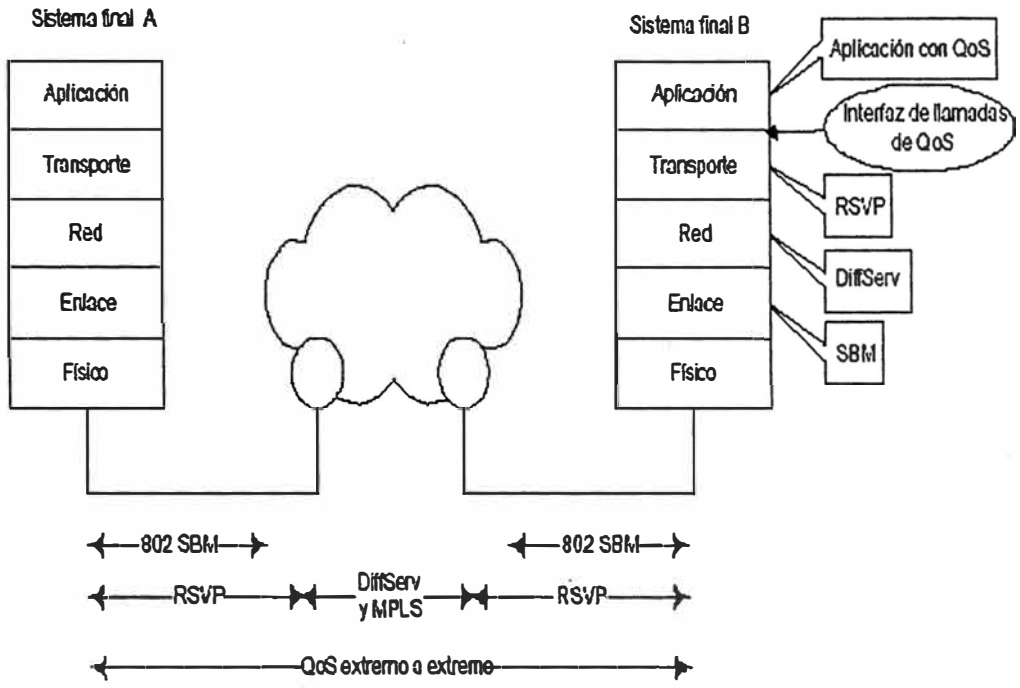


Fig: 2.5 Arquitectura de Calidad de Servicio con diferentes tecnologías

a.) IntServ con DiffServ

IntServ es más complejo y exigente que *DiffServ*, por lo que puede afectar negativamente en los encaminadores internos de la red [RFC2208], así que es mejor utilizar en estos encaminadores *DiffServ*. *IntServ* permite que los usuarios puedan realizar explícitamente peticiones de QoS.

Veamos como se complementan *IntServ* y *DiffServ*. Los sistemas finales pueden utilizar RSVP para solicitar la calidad de servicio con gran granularidad. Los encaminadores de acceso pueden trasladar las reservas de RSVP a la clase de servicio de *DiffServ* en el campo DS, o también puede ser el propio emisor quien haga la citada traslación. Los encaminadores de acceso además hacen el conformado del tráfico de los usuarios para asegurar el SLA.

Otra posibilidad es aplicar *IntServ* en la red de acceso y *DiffServ* en el núcleo de la red. En este caso el encaminador que hace la traslación deben estar entre ambas partes. Esto puede aplicarse beneficiosamente cuando la red de acceso pertenece a un proveedor de acceso a Internet y el núcleo de la red a un operador. Esta

arquitectura presenta además la ventaja de que los encaminadores de acceso, al no soportar grandes velocidades, puede dedicar más tiempo a hacer las tareas más pesadas que conlleva *IntServ*. En cambio, los encaminadores del núcleo al soportar grandes velocidades deben ser sencillos, por lo que pueden soportar *DiffServ* sin problemas. Recientemente se está experimentando con esta arquitectura en el proyecto ELISA subvencionado por la Comisión Europea .

b.) MPLS con IntServ

Existe el propósito de usar un objeto en RSVP para predeterminar el camino a tomar por parte de las sesiones RSVP con etiquetas. Estas sesiones usan las conexiones establecidas por los encaminadores MLPS. Incluso sin este objeto es posible que MPLS asigne etiquetas con arreglo a las especificaciones de RSVP. En cualquier caso, la consecuencia es una simplificación del funcionamiento de *IntServ* en los encaminadores MPLS.

c.) MPLS con DiffServ

Como cabría esperar, dada la similitud entre MPLS y DiffServ, la traslación del tráfico DiffServ a conexiones MPLS es sencilla. El principal problema de MPLS con DiffServ puede hallarse en la incompatibilidad de las múltiples implementaciones, mientras que unos fabricantes anuncian que soportarán 3 ó 4 niveles diferentes de QoS otros prometen miles

CAPITULO III

MODELO DIFFSERV . HARDWARE Y SOFTWARE

3.1 Introducción

La Fig. 3.1 muestra un tráfico sin DiffServ , es decir libre sin calidad de servicio

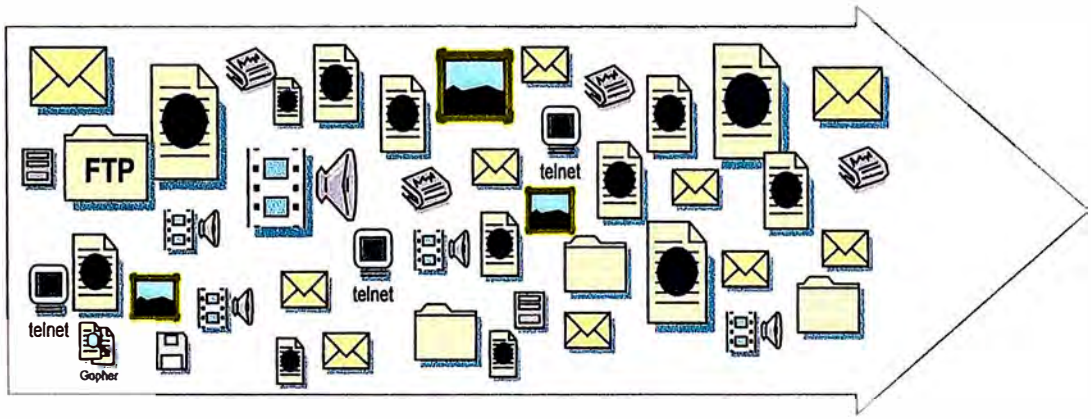


Fig. 3.1 Trafico Libre para todo

Posteriormente , se identifican los flujos , esdecir, se dividen en clases, se filtran los paquetes de cada clase donde cada una tiene un ancho de banda determinado. Esto se muestra en la Fig. 3.2

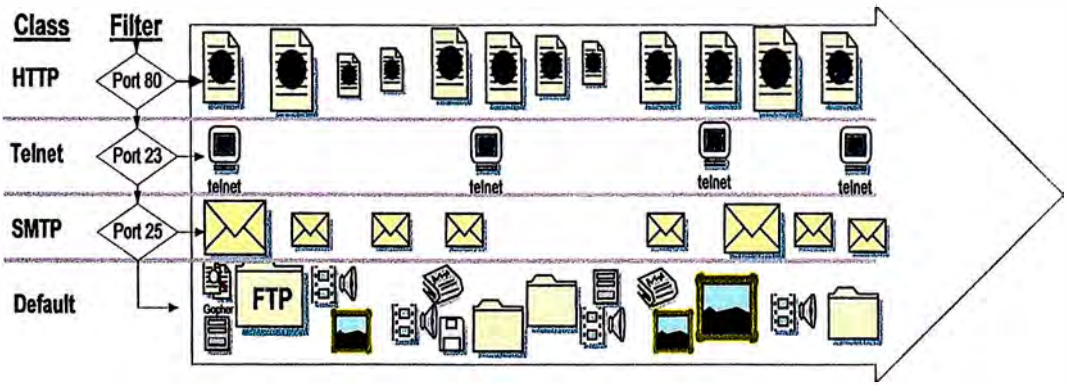


Fig 3.2 Identificación de Flujos

Luego se aplica un contrato (SLA) para garantizar la Calidad de Servicio, tal como se muestra en la Fig. 3.3

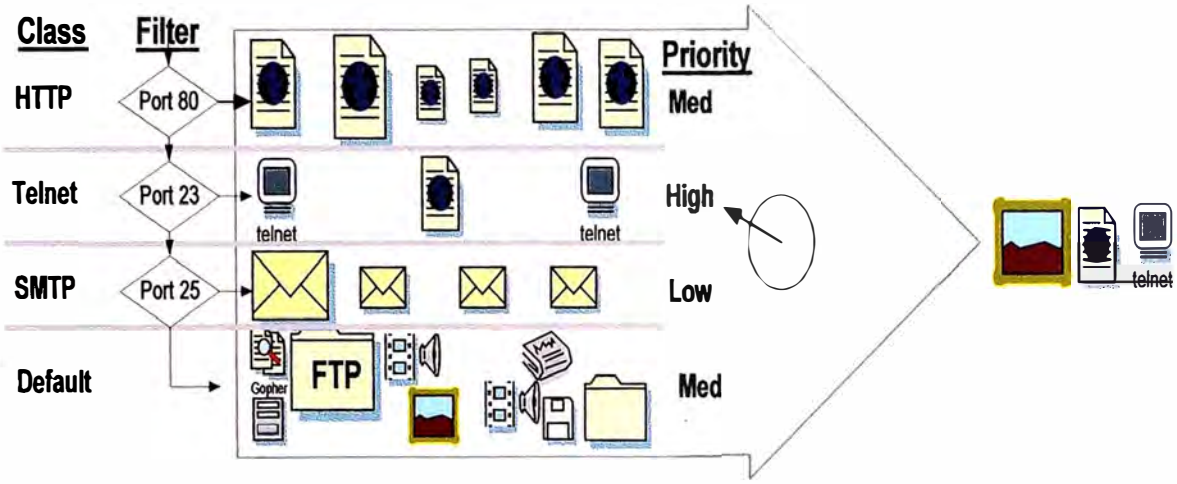


Fig. 3.3 Flujos con SLA

3.2 La Arquitectura de Servicios Diferenciados

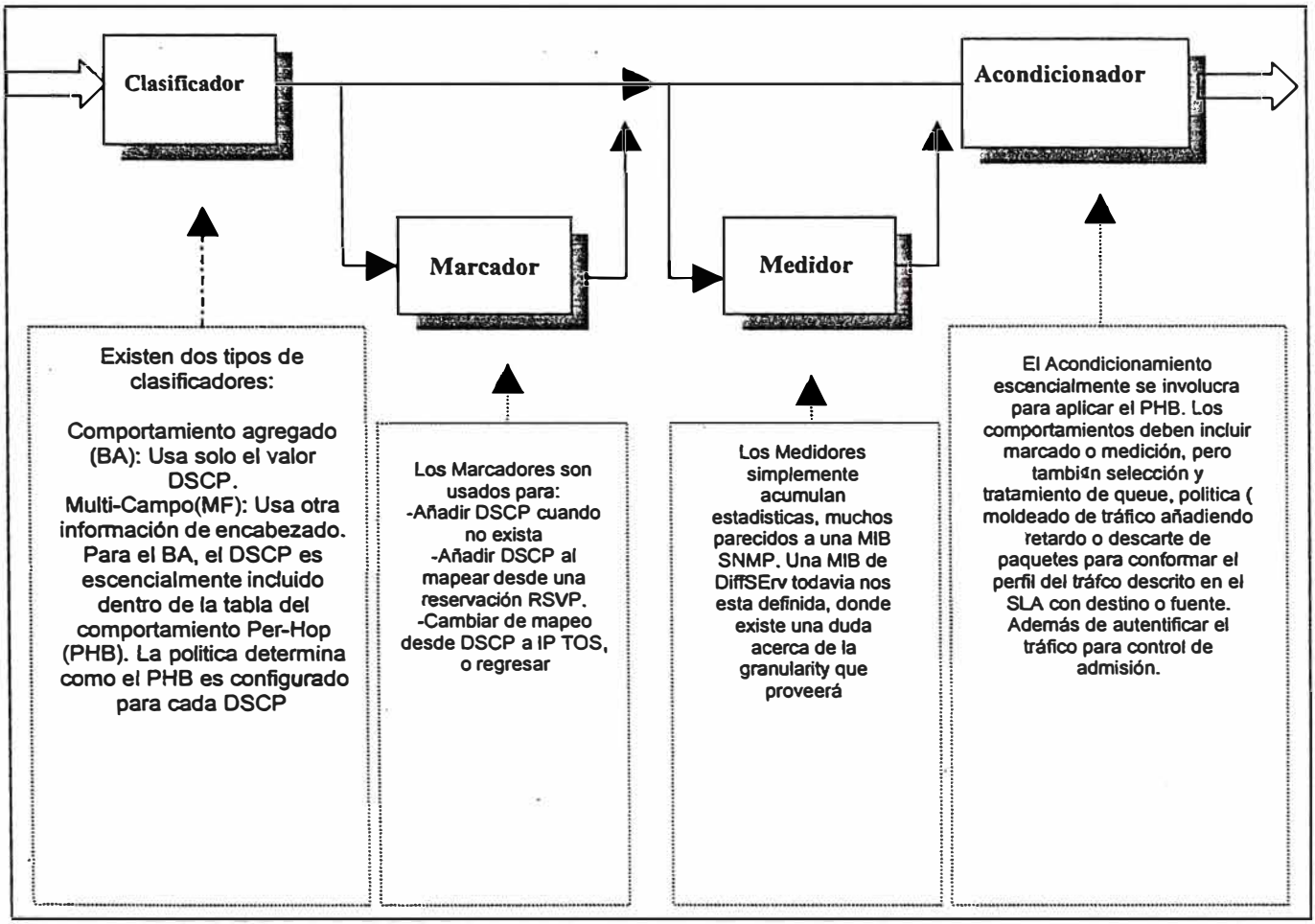


Fig 3.4 Arquitectura de Servicios Diferenciados

La arquitectura de los servicios diferenciados (DiffServ o DS) [4] es la propuesta del IETF para solucionar los problemas asociados a IntServ. La solución DS consiste básicamente en agrupar los flujos de tráfico IP en agregados, dentro de los cuales, los paquetes de un agregado dado serán tratados de la misma forma en cada nodo. Este tratamiento realizado salto a salto se denomina Per-Hop forwarding Behavior (PHB). Por otra parte, el grupo PHB al que pertenece un paquete IP se codifica en un campo de su cabecera llamado DS y su valor determina el tratamiento que se le debe dar a ese paquete en cada nodo o tramo de la red. Asimismo, el valor del campo DS permite tener paquetes con distinta prioridad dentro de un mismo PHB.

El IETF ha definido tres tipos de PHB:

a) **EF (Expedited Forwarding) [7].** Se trata del nivel más alto de prioridad (Premium), en donde los paquetes IP que lleven su cabecera DS marcada con el código EF disfrutarán de prioridad absoluta de servicio frente a los demás. Este

servicio está orientado a dar servicio a flujos de tiempo real o rígidos, que requieren bajos retardos por paquete.

b) **AF (Assured Forwarding) [6].** En realidad, se trata de un grupo de PHBs, entre los cuales es posible ofrecer niveles diferenciados de calidad relativa (por ejemplo, mediante prioridades de descarte). Los paquetes que lleven el octeto DS marcado con alguno de los niveles de Assured tendrán prioridad de servicio más baja que los Premium, pero su prioridad será más alta (bien en cuanto a servicio o a descarte) que la de los paquetes del servicio básico (también denominado Best-Effort). Bajo ciertas condiciones, este PHB podría permitir incluso garantizar un cierto ancho de banda medio (no un retardo por paquete) para los flujos.

c) **Best-Effort.** Corresponde al servicio básico, y en él (como siempre en DS) se encuadran tanto los flujos que no desean contratar niveles de calidad superiores, como los paquetes de flujos Premium y Assured que no son conformes con los perfiles declarados (y vigilados) para sus flujos.

El resumen de lo expuesto se muestra en la Fig. 3.5

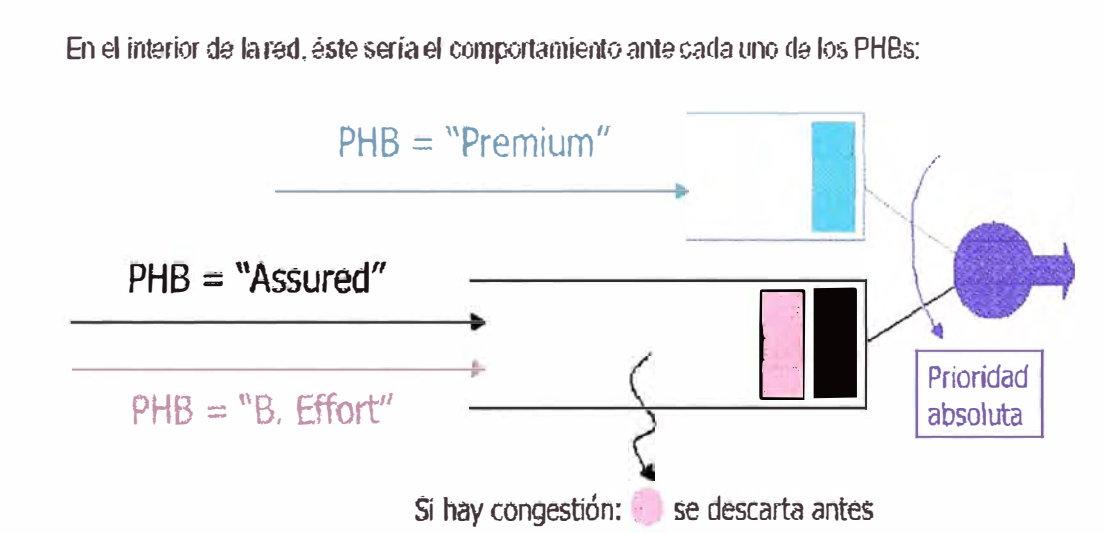


Fig. 3.5 Comportamiento de los Flujos

El fin último de las redes DS es, sin embargo, lograr la interconexión entre dominios en el ámbito de la calidad de servicio. Por esta razón, se han definido los PDBs (Per Domain Behaviours) [10] y BAs (Behaviour Aggregates), en un esfuerzo por pasar del tratamiento salto a salto a servicios que cumplan los requisitos de calidad de servicio extremo a extremo de los clientes.

Los BAs y PDBs unen reglas (éstas son determinados PHBs y configuraciones con características específicas observables) que sirven para configurar los dominios DS y describir sus atributos de calidad de servicio. Hay que diferenciar los PDBs y BAs de los servicios que los ISPs (Proveedores de servicios de Internet) ofrecen a sus clientes, ya que cada proveedor puede elegir un conjunto distinto de herramientas, o incluso desarrollar sus propias soluciones para satisfacer unas métricas particulares observables externamente. Las características que los proveedores exponen a sus clientes en los contratos pueden ser distintas de las características usadas en las definiciones de los BAs y PDBs.

3.3 Provisión de Servicios Diferenciados (DS)

Cada aplicación requiere unas determinadas prestaciones para funcionar correctamente, las cuales pueden dividirse en un conjunto de requisitos explícitos diferentes, de manera que un requisito dado puede ser satisfecho fácilmente. Aunque el problema que se presenta es cómo satisfacer los distintos requisitos a la vez, una primera aproximación podría ser estudiar cómo se puede satisfacer un determinado requisito.

Como muestra de los distintos requisitos se puede distinguir lo siguiente:

- Bajo retardo.
- Baja variación del retardo.
- Bajas pérdidas.
- Ancho de banda mínimo garantizado.

En la Fig. 3.6 se observa cómo están relacionadas las pérdidas y el retardo.

Para una carga dada, el retardo se intercambia por pérdidas modificando el tamaño del buffer: con buffers largos tenemos retardos grandes pero bajas pérdidas, y viceversa. También se puede observar que disminuyendo la carga, las pérdidas y el retardo son menores, por lo cual se deduce que las pérdidas y el retardo están relacionados con la carga y el tamaño del buffer.

El tráfico de tiempo real requiere bajas pérdidas, bajos retardos, así como una baja variación del retardo; es decir, necesita una carga baja y buffers cortos. Por otro lado, el tráfico elástico, aunque también requiere bajas pérdidas, no necesita bajos retardos, por lo que se pueden usar buffers grandes, consiguiendo una mayor ganancia de multiplexación. Sin embargo, hay que tener en cuenta que si la carga es muy alta las prestaciones obtenidas serán muy pobres. Por lo tanto, la manera de obtener unas prestaciones dadas en una red es tener una carga lo suficientemente baja.

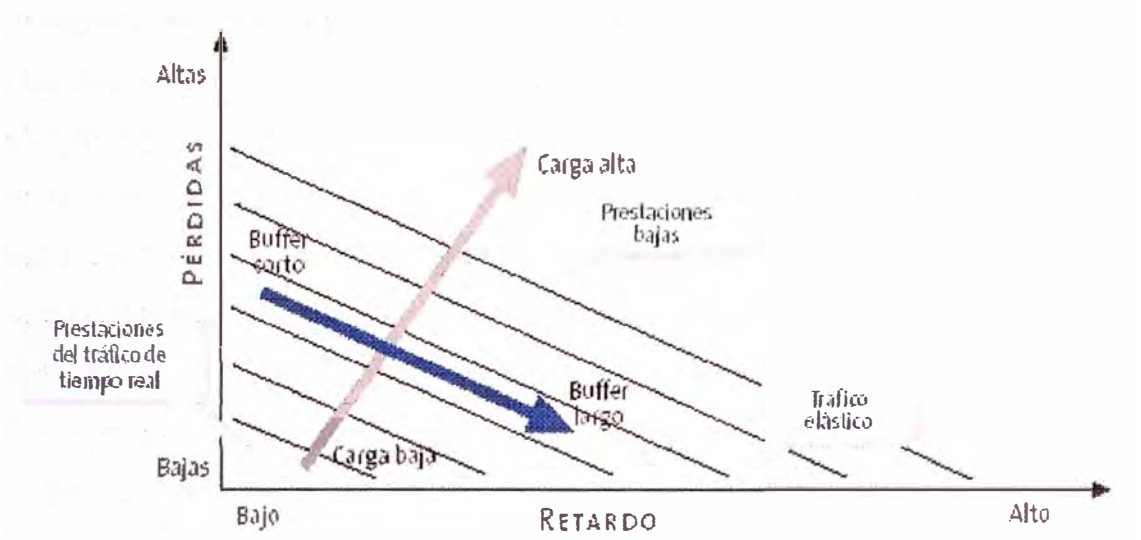


Fig 3.6 Pérdidas versus Retardo

La arquitectura de DS proporciona mecanismos capaces de satisfacer los requisitos que demandan las aplicaciones. Además, la inteligencia de la red de acceso hace posible mantener una carga aceptable, de manera que las prestaciones sean buenas.

Sin embargo, esta provisión de calidad de servicio aunque posible, es difícil de alcanzar. Los mecanismos PHB deben ser estudiados y mejorados, y también tienen que desarrollarse métodos de gestión de tráfico para gestionar y controlar la red de una manera adecuada.

3.4 Modelos de Servicio

El principal criterio de decisión para elegir un modelo de servicio es la clase de garantías de calidad de servicio que se pretende proporcionar.

Los modelos se dividen en:

- **DS absoluto.** Permite ofrecer una calidad de servicio comparable a la que ofrece IntServ [2], pero requiere de controles de admisión. Todavía no está claro si será posible garantizar las prestaciones extremo a extremo, debido a la dificultad de elaborar mecanismos salto a salto que hagan posible ofrecer este tratamiento. Se puede decir que este modelo permite ofrecer garantías explícitas.
- **DS proporcional .** Proporciona garantías predecibles y controlables de calidad de servicio. Así, aunque el nivel de calidad de cada clase varíe con la carga, la relación de calidad entre las clases se mantiene fija, independientemente de la carga de las distintas clases. Es aconsejable introducir controles de admisión para evitar que las prestaciones de las clases más bajas se degraden significativamente.

- **DS relativo.** No ofrece garantías de calidad de servicio predecibles, pero garantiza que las clases más altas obtendrán una calidad de servicio mejor (o por lo menos no peor) que las clases más bajas. Esta solución no sólo es la más sencilla, sino que tiene la ventaja de que si el ancho de banda se hace más barato en un futuro cercano, no será necesario preocuparse de cómo se diferencian los servicios, ya que cada usuario obtendrá todo el ancho de banda que desee. Sin embargo, es muy posible que la demanda de ancho de banda crezca a la vez que lo haga el ancho de banda disponible, por lo cual no está claro que los mecanismos de control de tráfico no sean necesarios en un futuro cercano. Con este modelo sólo se pueden proporcionar expectativas razonables y no garantías.

La solución que se implante puede ser una combinación de estas propuestas, ya que parece difícil vender servicios de tiempo real sin garantías explícitas. Sin embargo para los servicios elásticos las garantías predecibles serían suficientes o incluso expectativas razonables.

3.5 Routers de Servicios Diferenciados (DiffServ)

Se pueden distinguir tres tipos de routers DS:

a) **Los Routers de Entrada (RE),** que se sitúan en los puntos de entrada a la red. En estos nodos se agregan los distintos flujos de los dominios clientes, de los usuarios finales y de los sistemas autónomos.

b) **Los Routers de Salida (RS),** que son los responsables de conformar el tráfico de salida de un ISP, según un SLA (o un SLS) establecido con otro proveedor. Los flujos agregados salen del dominio DS de un proveedor y entran en el dominio de un cliente o de otro proveedor.

c) **Los Routers Interiores (RI).** En las nubes DS, los RI dan un tratamiento diferenciado a los flujos agregados DS.

En la Fig 3.7 se muestra un escenario de dominios DS con todos los tipos de routers DS.

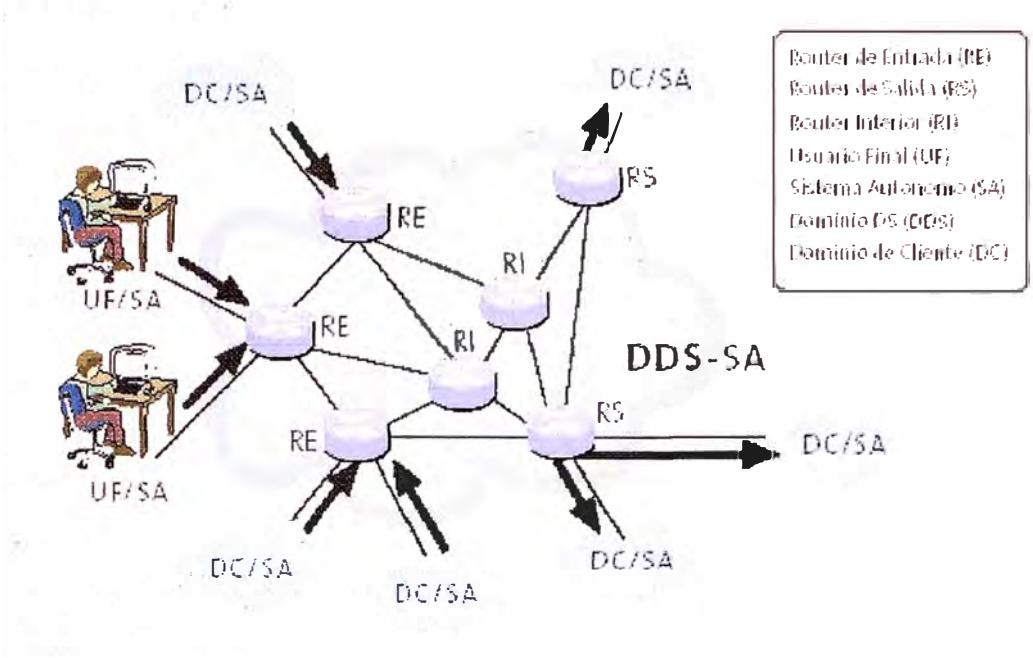


Fig 3.7 Dominio Servicios Diferenciados (DS) con routers DS

3.5.1 Requisitos de los Routers

Los routers DS están compuestos por un conjunto de bloques definidos en [4], pero no todos estos bloques son necesarios en todos los routers.

Dependiendo del número de clientes (usuarios finales o dominios cliente conectados) cada flujo o flujos agregados tienen que ser controlados, limitados y procesados por un acondicionador, que a partir de aquí llamaremos gestor de servicios. El número de gestores crecerá de forma lineal con el número de clientes.

El clasificador y el gestor de servicios necesitan información sobre los clientes, pues en función del perfil del cliente los paquetes serán clasificados y reenviados a uno u otro gestor de servicios.

A partir de ahora asumiremos que las aplicaciones pueden marcar los paquetes; aunque esto no es estrictamente necesario, permitirá la diferenciación de los flujos de distintas aplicaciones de un mismo nodo. Esto no significa que se confíe en el host, ya que el router que se encuentra junto al host tiene el perfil adecuado para controlar el flujo.

La Tabla 3.1 que viene a continuación describe los bloques necesarios para los routers con un PHB EF. La clasificación MF (MutiField) o BA es realizada por un clasificador y cada cliente conectado necesita un acondicionador/gestor de servicios.

Tabla 3.1 Router con un PHB EF

Bloque	*Router* Interior	*Router* de Salida	*Router* de Entrada
Clasificación MF			X
Clasificación BA	X	X	X
Acondicionador / Gestor de servicios			
Medidor		X	X
Marcardor		X	X
Vigilancia/Descarte			X[1]
Conformador		X	X[2]
Facilidades del *Bandwidth Broker*			
Señalización		X	X

1 Para un *router* de entrada conectado a dominios de clientes.
2 Para un *router* de entrada cercano a un usuario final para soportar aplicaciones que produzcan tráfico ligeramente ráfagoso

Asimismo, la Tabla 3.2 muestra los bloques necesarios para un router que soporte el grupo AF. Igualmente, la clasificación BA y MF se realiza en un clasificador, y cada cliente conectado que solicita un tratamiento AF debe ser atendido por un acondicionador/gestor de servicios.

Tabla 3.2 Router con un PHB AF

Bloque	*Router* Interior	*Router* de Salida	*Router* de Entrada
Clasificación MF			X
Clasificación BA	X	X	X
Acondicionador			
Medidor		X	X
Marcardor/Remarcador		X	X
Facilidades del *Bandwidth Broker*			
Señalización		X	X

3.6 Implementación de una red de Servicios Diferenciados (DiffServ)

Un ejemplo de una red mixta de servicios diferenciados es un dominio que tiene implementados los tres PHBs básicos:

1. El PHB Expedited Forwarding [7] como servicio A.
2. Un PHB Assured Forwarding [6] como servicio B.
3. El PHB por defecto (Best-Effort) [5] como servicio C.

Un router DS tendrá implementados los sgtes bloques (ver la Fig 3.8):

- **El clasificador.** Clasificará el tráfico entrante de acuerdo con los perfiles de los clientes y reenviará los flujos al gestor correspondiente (si el tráfico es de clase AF o EF). En el caso del tráfico Best-Effort, los flujos se envían directamente al sistema de colas de salida.
- **Los gestores EF.** Para cada cliente de servicio Premium, se establece un gestor EF. El gestor limitará el tráfico a un ancho de banda, que está definido en el SLA del cliente.
- **El gestor AF.** Se establece una prioridad de descarte para cada cliente, y en el SLA se establecen las tasas de transferencia para las prioridades de descarte baja y media.
- **El sistema de colas de salida.** Cada clase de servicio tendrá una sola cola de salida. Para la clase EF y la clase Best-Effort se puede usar un sistema de encolado FIFO (First In, First Out) o un mecanismo RED . Para la clase AF, en [6] se propone el uso de una cola con mecanismos basados en RED para cada prioridad de descarte.
- **El sistema de desencolado.** Puesto que el tráfico EF tiene la prioridad de servicio más alta, será necesario usar una disciplina de servicio que vacíe la cola EF, siempre que haya un paquete en ésta y la interfaz pueda enviarlo. Para el servicio de AF y Best- Effort puede usarse un mecanismo WFQ (Weighted Fair Queuing). Eligiendo una relación equilibrada entre AF y Best-Effort se garantiza que los flujos Best-Effort no van a dejar de ser bien atendidos.

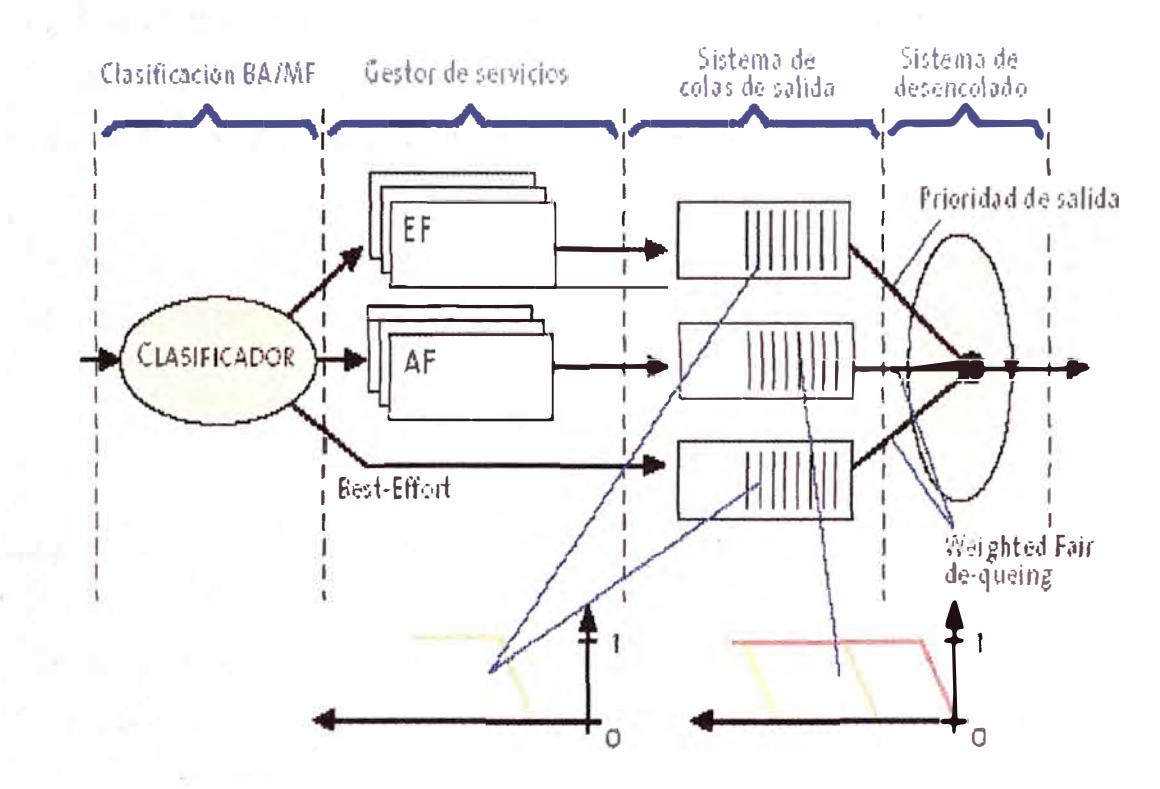


Fig 3.8 Bloques de un router de borde con las tres clases básicas de servicio

Por otra parte, un router de entrada a la red, como el de la Fig 3.5, tendrá el siguiente comportamiento:

- El ancho de banda de salida (C) se divide en cuatro partes:
  a) Ancho de banda de salida EF máximo: $C *. \rho_a$
  b) Ancho de banda de salida AF máximo con baja prioridad de descarte

$$C *. \rho_b \qquad (3.1)$$

  c) Ancho de banda de salida AF máximo, con prioridad de descarte media:

$$C * \rho_c \qquad (3.2)$$

  Este ancho de banda está sobredimensionado en ausencia del tráfico de alta y media prioridad de descarte. El tráfico de prioridad de descarte media define el rango de ancho de banda permitido para las ráfagas.
  d) El ancho de banda restante ($\rho = \rho_a + \rho_b + \rho_c < 1$) es usado por el tráfico Best-Effort y AF con alta prioridad de descarte. El ancho de banda sería: $C*(1 - \rho)$
- El tráfico entrante está definido por los clientes conectados. Éstos son:
  a) Los clientes EF. Hay i gestores EF; esto es, tantos como clientes EF.
  b) Los clientes AF. Hay j gestores AF; esto es, tantos como clientes AF.

c) Los clientes Best-Effort. No están asociados a ningún gestor de servicios; esto es, no hay ningún gestor BE.

En caso de que haya sobrecarga en la entrada, tendremos el siguiente comportamiento de salida:

- El máximo ancho de banda del tráfico EF(B_a) puede ser calculado como la suma del ancho de banda de reenvío de los gestores EF (B_{an}), de lo cual:

$$B_{amax} = \sum_{n=1}^{i} B_{an} \qquad (3.3)$$

El tráfico de un cliente que exceda el ancho de banda acordado será descartado en el gestor de servicio EF.

- El máximo ancho de banda (B_b) del tráfico AF de baja prioridad de descarte se define como la suma del ancho de banda acordado de baja prioridad de descarte (B_{bn}), por tanto:

$$B_{bmax} = \sum_{n=1}^{i} B_{bn} \qquad (3.4)$$

El tráfico de cliente que exceda B_{bn} será remarcado como tráfico de prioridad de descarte media.

- El tráfico AF de prioridad de descarte media se define como el tráfico con tendencia a emitir en ráfagas, pudiendo absorber un abanico de ancho de banda cuyo límite superior es el ancho de banda sobredimensionado. Este ancho de banda puede ser calculado sumando el tráfico agregado de prioridad media o la respectiva información de tasa [8] [9] en el perfil del usuario (B_{cn}), siendo por tanto:

$$B_{cmax} = \sum_{n=1}^{i} B_{cn} \qquad (3.5)$$

En la Fig 3.9 que sigue se muestra el sistema de cola de salida de la clase AF con prioridad de descarte. Si llega más cantidad de tráfico que el ancho de banda sobredimensionado, el excedente será marcado con una alta prioridad de descarte y será descartado relativamente pronto en el sistema de colas de salida, dependiendo de la localización del mecanismo RED de alta prioridad de descarte.

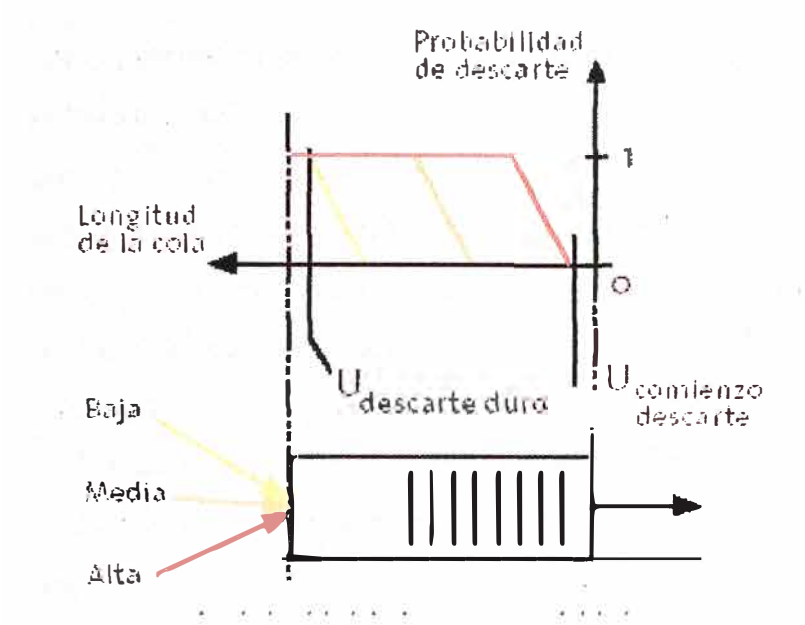


Fig 3.9 Sistema de cola de salida de la clase AF con prioridad de descarte

3.7 Medidas en las Redes DS

Los proveedores de servicios necesitan herramientas de medida para poder gestionar extremo a extremo los recursos de la red. Los parámetros básicos de una conexión IP se definen en la recomendación ITU-T I.380 , pero en la práctica los SLAs especificados por un proveedor de servicios establecen una serie de requisitos para las medidas.

Un desafío adicional es la facturación basada en la cantidad de tráfico, que asume que la matriz de tráfico del usuario se mide continuamente y con la profundidad adecuada; además, la medición por flujo requiere soluciones mucho más complejas que la medición del tráfico agregado. Los parámetros medidos por el proveedor de servicios, responsable sólo de la parte de la conexión que está bajo su control, normalmente son diferentes de los parámetros extremo a extremo. Por lo tanto, los puntos de medida tienen que estar bien definidos e incluidos en los contratos de los clientes para evitar quejas sobre los mismos.

El reto en las redes DS es todavía más complejo debido a la gran variedad existente en las diferentes clases de tráfico.

3.7.1 Métodos de Medida

Las dificultades de los métodos de medida en las redes DS radican en que ni siquiera existen métodos bien desarrollados para las redes IP "simples". Las principales características de un sistema de medida son:

- En servicio o sin servicio.
- Medidas activas o pasivas.
- Medidas centralizadas o descentralizadas.

La eficiencia del método de medida puede mejorarse usando herramientas de medida adicionales con "valor añadido".

3.7.2 Parámetros y Protocolos Medidos

La elección de qué protocolos y parámetros IP de una red IP (DS) se miden depende de la clase de servicio y del proveedor de servicios. Los proveedores de servicio deben seleccionar (en función de las características de su red, de los SLA definidos y de la demanda de los usuarios) el conjunto apropiado de parámetros
y protocolos. Además, hay que tener en cuenta que los resultados de las medidas también se usan de manera frecuente para planificar las redes.

a) Parámetros IP

Los parámetros IP se emplean para especificar y evaluar las características del transporte de los paquetes de una red IP (DS). Estos parámetros generalmente se aplican a servicios IP extremo a extremo y punto a punto, pero en las redes IP actuales los proveedores de servicios sólo garantizan los SLAs en la porción de red que está directamente bajo su control.

Los parámetros IP se definen basándose en los eventos de referencia que pueden ser observados en los puntos de medida asociados, con límites específicos funcionales o jurisdiccionales. Por lo tanto, cada proveedor de servicios tiene que declarar cuidadosamente los puntos de acceso a su red, en el caso de una red DS este punto de acceso al servicio debería ser el sitio de la red donde se realiza el marcado de los paquetes IP (asignación del código DS). Hay que tener en cuenta que en las redes DS los puntos de medida pueden ser los mismos para diferentes clases de tráfico, mientras que los eventos de referencia pueden afectar a una determinada clase DS sólo si el paquete IP pertenece a esa clase.

En una red DS diferentes clases de tráfico pueden tener diferentes características, por lo que la medida de los parámetros IP debería ser realizada (teóricamente) para cada una de las clases DS. Los parámetros IP medidos son:

Retardo de transferencia.

Variación del retardo.

Tasa de pérdidas.

Volumen y distribución del tráfico.

Los parámetros y sus medidas están influidos por los siguientes factores:

- La fragmentación.

- La inestabilidad en el encaminamiento.

b) Protocolos IP

Mientras que los parámetros IP tienen un impacto significativo en las características de las redes DS, los clientes están interesados en las prestaciones de los protocolos de alto nivel. Los protocolos IP "más importantes" (es decir, aquellos que su correcto funcionamiento debe ser vigilado) son diferentes para cada proveedor, dependiendo de los requisitos de sus clientes. Normalmente, los protocolos más importantes son los siguientes: DNS, FTP, HTTP/HTTPS, ICMP, POP3, SMTP, RADIUS, SNMP, RPING, DHCP, NTP, etc.

Los monitores de los protocolos IP emulan las acciones de un usuario real, por ejemplo, un monitor de HTTP intentará regularmente acceder a una página web concreta y medirá cómo de bien se comporta el servicio HTTP. La información almacenada por este monitor permitirá que los operadores de la red puedan conocer el estado del servicio HTTP.

3.7.3 Escenarios de Medida

Hay tres soluciones principales para medir en las redes IP (DS):

a) Los parámetros IP pueden ser medidos basándose en los contadores locales de los routers.

b) Los parámetros IP (excepto el volumen de tráfico y los parámetros de distribución) pueden ser medidos usando paquetes ICMP, ya que ICMP es parte del nivel IP.

c) Los protocolos IP pueden ser monitorizados emulando las acciones de un usuario real.

Independientemente de la solución de medida elegida, se deben estimar cuidadosamente dos características para asegurar la escalabilidad y el correcto funcionamiento del sistema de medida: el volumen de datos que origina la medida y los requisitos de procesado de los datos generados por ésta. En cualquier caso, el volumen de los datos y los requisitos de procesado de éstos pueden disminuirse agregando los datos medidos localmente en los routers.

En el caso de los monitores basados en los contadores incluidos en los routers, los valores de los contadores pueden ser recogidos a través de SNMP en una base de datos centralizada. Los datos recolectados son post-procesados con una aplicación que realiza los informes y son presentados a los clientes mediante una interfaz web.

Se pueden crear contadores locales especiales usando agentes locales que miden las características de los flujos de datos, estos agentes envían los resultados de las medidas

a unos dispositivos especiales (llamados colectores). Este método requiere que los routers dediquen recursos para el procesado de datos (ciclos de CPU).

ICMP es un sistema para informar sobre errores, que es una parte integral de IP, por lo que está incluido en todas las implementaciones de IP. Esto proporciona un sistema de mensajes y señales de error consistente, que entienden todas las diferentes versiones de IP y todos los sistemas operativos. Los mensajes ICMP pueden ser empleados para la medida de parámetros IP, como el retardo de transferencia, la variación del retardo, la tasa de pérdidas y la disponibilidad.

Los protocolos IP pueden ser monitorizados emulando las acciones de los usuarios reales y son medidos por diferentes monitores que activamente generan eventos para monitorizar el estado de los servicios, de manera que cada monitor comprueba regularmente un servicio para determinar si está funcionando adecuadamente.

3.7.4 Cuestiones relacionadas con las medidas

En DS el tráfico IP se separa en clases y estas clases son tratadas de forma diferente dentro de la red. Para controlar que las distintas clases DS reciben su tratamiento correspondiente, se deben medir los distintos protocolos y parámetros de IP. Por lo tanto, los monitores deberían ser capaces de generar tráfico con diferentes DSCPs y también deberían establecerse contadores separados para las diferentes clases de tráfico en los routers.

Generalmente, los monitores actuales son incapaces de generar tráfico con diferentes DSCPs, por lo que habría que situarlos en los límites de la red DS y el primer router debería marcar los paquetes con el código DS correspondiente.

En las redes DS se debe especificar, para cada clase de tráfico, qué parámetros y protocolos deben medirse.

Esto incrementa la complejidad de los sistemas de medida, porque:

- El mismo parámetro/protocolo debe ser medido para cada una de las clases de tráfico DS.
- El volumen de datos de las medidas es grande.
- La agregación de la información de las medidas es más compleja.
- Diferentes SLAs deben ser controlados en diferentes clases de tráfico DS.

3.8 Servicios sobre redes DS :Servicios Basados en EF/AF

3.8.1 Servicios Basados en EF

El BA "Virtual Wire" podría ser usado para proveer servicios de tiempo real. Este servicio basado en EF consistiría en proporcionar una línea virtual alquilada.

Pronosticar y dimensionar este servicio no sería muy complejo siempre que el tráfico de tiempo real se comportara como el tráfico telefónico tradicional. Además, si el tráfico de tiempo real supone una pequeña proporción del tráfico total, la manera más fácil de gestionarlo sería sobredimensionando; por tanto, se puede asegurar que no se desperdiciarían recursos, ya que el ancho de banda sobrante podría ser usado por los tráficos AF y BE. Por otro lado, si se tienen que proporcionar garantías explícitas, sería necesario usar un control de admisión.

3.8.2 SERVICIOS BASADOS EN AF

El servicio de capacidad asignada podría ser un servicio basado en AF que proporcionaría a cada flujo elástico el ancho de banda que requiriera. Este servicio se podría utilizar para tráficos elásticos o de tiempo real adaptativos, proporcionando garantías explícitas si se usa control de admisión o garantías relativas en caso de no usarse. Además, se pueden utilizar cubos de goteo modificados para mejorar las prestaciones de las aplicaciones elásticas, lo que evitaría el uso del control de admisión, proporcionando garantías proporcionales (relativas).

Sin embargo, con los mecanismos actuales no se pueden proporcionar garantías estrictas, ni siquiera proporcionales. Si se tienen que proporcionar las tasas objetivo, se necesitarán nuevas funciones de vigilancia que dependan del RTT.

Sin embargo, usando una modificación del cubo de goteo con tapadera propuesto, que descarta un paquete cada dos RTTs (en lugar de marcarlo como fuera de perfil) una vez que la tasa objetivo ha sido alcanzada, se ayudaría a todos los flujos TCP a conseguir su ancho de banda requerido. Junto a esto, habría que usar una disciplina de servicio GPS, para aislar el tráfico AF del resto del tráfico (especialmente del de mayor prioridad, como el tráfico EF) y evitar así que los flujos TCP sean estorbados, siempre que haya suficientes recursos para todos ellos.

El uso de una disciplina de servicio de tipo GPS sería ventajoso debido a que el pronóstico y dimensionado puede hacerse de forma independiente para tráfico de

tipo corriente y para tráfico elástico. Así, la congestión en una clase más alta no se transmitiría a una clase más baja; siendo la principal desventaja que las clases más bajas pueden obtener unas prestaciones mejores que las clases más altas, cuando éstas estén congestionadas.

Sin embargo, esto no es un obstáculo, es mucho mejor no satisfacer los requisitos de una clase que no satisfacer ningún requisito.

Otra cuestión que se debe tener en cuenta es que el servicio de capacidad asignada ha sido diseñado a nivel de flujo, por lo que un usuario podría tener muchos flujos, cada uno de ellos pidiendo diferentes anchos de banda. Sin embargo, se puede rediseñar este servicio, de una manera u otra, para que un usuario pudiera tener un ancho de banda máximo para sus aplicaciones; de esta manera, el usuario podría asignar a cada flujo el ancho de banda que deseara, siempre que la suma fuera menor que el ancho de banda contratado. Los routers del borde de la red vigilarían cada flujo de cada usuario, comprobando que el ancho de banda total no fuera mayor que el ancho de banda total asignado al usuario.

3.8.3 Facturación/Contabilidad en Redes de Servicios Diferenciados

La oferta comercial de servicios diferenciados IP por parte de los proveedores de servicios depende de la disponibilidad de servicios AAA (Authentication Authorisation Accounting) que permitan el control de acceso a las clases de servicio y, a su vez, permitan una facturación detallada de los servicios consumidos. El grupo de investigación AAAARCH (Arquitectura de Autenticación, Autorización y Contabilidad, Authentication Authorisation Accounting ARCHitecture) [2] del IRTF (Internet Research Task Force) está desarrollando una arquitectura AAA que se ajusta perfectamente a estas necesidades, este grupo propone un modelo de contabilidad basado en políticas que permite la provisión flexible de servicios de contabilidad. Las políticas de contabilidad se aplican para implementar la arquitectura de contabilidad y pueden ser intercambiadas entre entidades AAA para compartir la información de configuración. En [3] se describe el modelo genérico, los bloques de los que está compuesto esta arquitectura y las secuencias de mensajes.

La contabilidad puede ser incluida como parte del proceso de provisión de servicios (contabilidad integrada) o puede ser ofrecida como un servicio independiente (contabilidad discreta). En la contabilidad integrada, la contabilidad está ligada a un

servicio específico; puede estar adaptada para el servicio o puede recoger información de contabilidad directamente, explotando las entidades específicas del servicio. La configuración de la contabilidad se hace como una parte de la configuración del equipo del servicio y las políticas de contabilidad se definen como una parte del acuerdo de provisión.

Un módulo específico de aplicación (Application Specific Module, ASM) común incluye las funcionalidades necesarias para proveer servicios AAA, convirtiendo las instrucciones del servidor AAA en la configuración adecuada del equipo de servicio para establecer las configuraciones de contabilidad. Durante la provisión del servicio los medidores envían datos sobre el consumo de recursos al ASM, donde los datos medidos se convierten en registros de contabilidad que son enviados al servidor AAA, donde se realiza la conversión, agregación y filtrado de dichos datos.

Hay una relación muy estrecha entre la configuración de un servicio DS, en respuesta a una petición de servicio por parte de un usuario, y la configuración requerida en las entidades de contabilidad. A través de una aproximación homogénea, apoyada en la gestión basada en políticas, esta configuración puede ser automatizada, de manera que exista consistencia en todas las configuraciones de todas las entidades involucradas.

La Fig 3.10 muestra los principales componentes incluidos en la configuración de contabilidad integrada, que parece la mejor opción para DS. Con objeto de conseguir el acceso a los servicios, el usuario tiene que enviar una petición de servicio al servidor AAA, que comprueba si el usuario tiene autorización para acceder a ese servicio; en caso afirmativo, la información específica de la aplicación es enviada al módulo específico de la aplicación (ASM), por último éste extrae la información de configuración y la distribuye a los distintos componentes del servicio que tienen que interactuar con la provisión del mismo. En esta etapa se puede realizar la traducción de formatos para permitir la interoperabilidad con los componentes de servicio antiguos que todavía no cumplan con AAA.

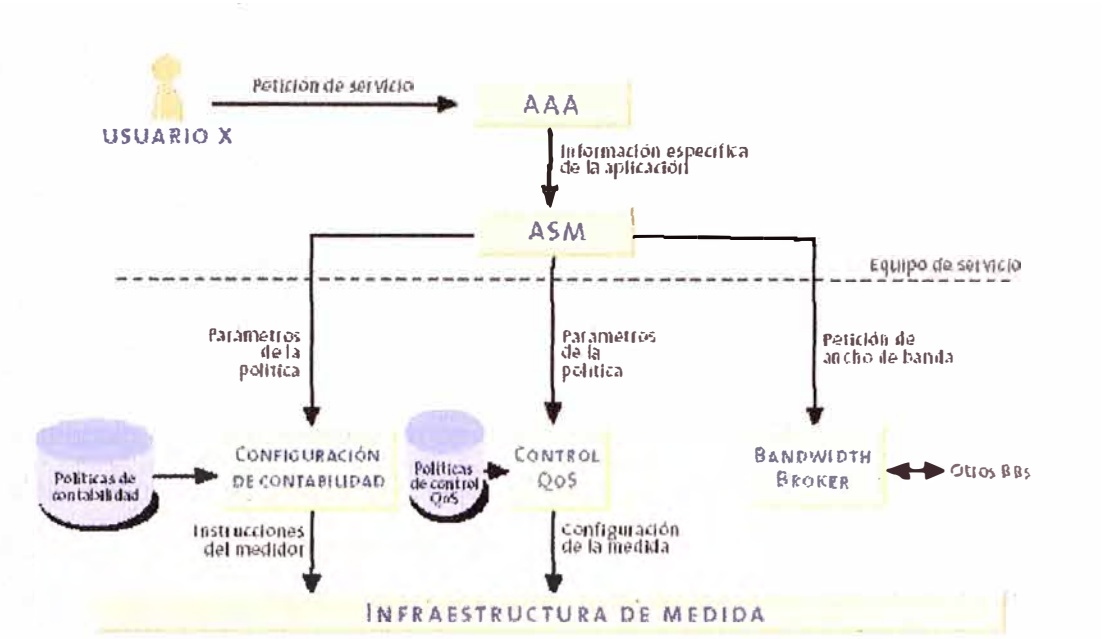


Fig 3.10 Contabilidad integrada basada en políticas para DS

En el caso de DS, lo descrito requiere la configuración de tres componentes: el sistema de contabilidad DS, el control y auditoría de calidad de servicio de DS y el Bandwidth Broker, que es responsable de gestionar Facturación y contabilidad en redes DS tanto en el control de admisión como la gestión de recursos para las peticiones de servicio.

CAPITULO IV
PROTOCOLO GESTOR DE POLITICAS (COPS)

El protocolo COPS (Common Open Policy Service) descrito en la RFC 2748, define un modelo cliente/servidor sencillo para proporcionar control de políticas a protocolos de señalización de calidad de servicio.

El modelo no hace ninguna suposición acerca de los métodos utilizados en el servidor de políticas, sino que se basa en un servidor de políticas (PDP : Policy Decisión Point) que devuelve decisiones a las peticiones realizadas por los clientes (PEP : Policy Enforcement Points). Es el protocolo más apropiado para un intercambio de información entre un servidor de políticas y diversos clientes que instalan perfiles de usuario o aplican métodos de calidad de servicio bajo orden del servidor. El PEP también tiene la capacidad de informar al PDP si ha podido instalar localmente con éxito la decisión recibida, así también el PEP es el encargado de borrar cualquier estado que ya no sea válido debido a eventos en el propio cliente o a decisiones enviadas por el servidor.

Utiliza TCP como protocolo de transporte (puerto 3288) para asegurar así fiabilidad en el intercambio de mensajes entre los clientes y el servidor.

El protocolo necesita información de estados en las máquinas ya que:

a) El estado de una petición/decisión es compartido entre el cliente y el servidor
b) El estado de varios eventos (pares petición/decisión) puede estar interrelacionado.

La definición del protocolo es bastante abierta para que sea extensible y pueda soportar los distintos tipos de clientes que pudieran aparecer en un futuro.

En la Fig 4.1 vemos el modelo del protocolo COPS.

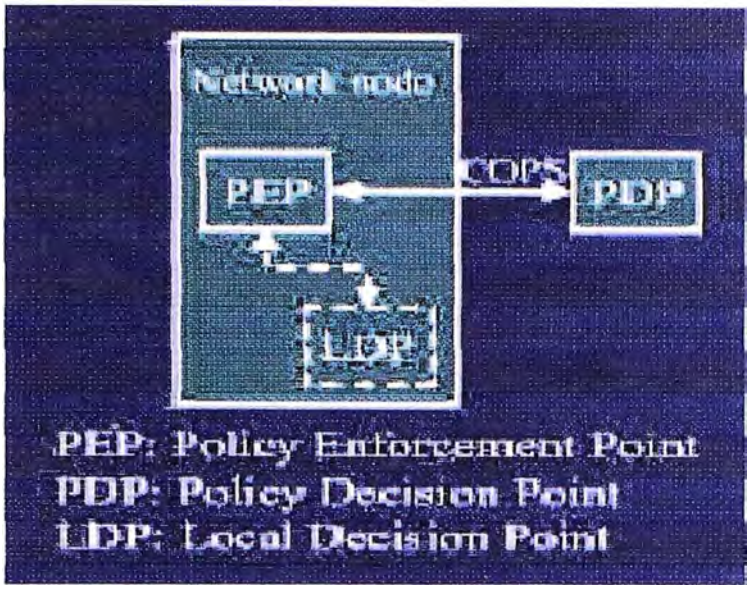


Fig 4.1 Protocolo COPS

Dentro del nodo de red puede existir un PDP local (LPD o LPDP) que puede ser utilizado para tomar decisiones locales en ausencia de un PDP.

Cada mensaje COPS (Tabla 4.1) consta de una cabecera COPS y un conjunto de objetos COPS ya definidos. La cabecera son los 8 primeros bytes y en ella podemos ver, entre otras cosas, el código de operación y el tipo de cliente que manda el mensaje. Aparte, un mensaje se compone de N objetos COPS con el mismo formato y alineados a 32 bits.

Tabla 4.1 Mensaje COPS

	0	1	2	3
<Cabecera común COPS>	Ver	Flags	Cód. Operac.	Tipo cliente
	Longitud total del Mensaje (bytes)			
<Objeto COPS>	Long. Objeto (bytes)		C-Num	C-Type
	... Contenido del objeto ...			

4.1 Características :

El protocolo emplea un modelo de cliente / servidor, donde el PEP envía peticiones actualizaciones y cancelaciones al PDP remoto y las decisiones retornan al PEP.

El protocolo utilizado es el TCP como su protocolo de transporte confiable para el intercambio de mensajes entre los clientes y el servidor de políticas.

Es escalable, es decir, puede apoyar con la especificación de diversos clientes sin requerir modificaciones en el protocolo. Debido a que fue creado para la administración, la configuración, y la aplicación generales de políticas. COPS proporciona seguridad para los mensajes con el fin de autenticarse brindando integridad a los mensajes. COPS puede reutilizar los diferentes protocolos de seguridad como IPSEC, TLS para autenticar y asegurar el canal entre el PEP y el PDP.

Un ejemplo de implementación del protocolo COPS , se nota en el proyecto **MobyDick (Mobility and Differentiated Services in a Future IP Network)** tiene como propósito el diseño, implementación y pruebas de una arquitectura de red móvil de cuarta generación en la que existen aspectos de AAAC (autenticación, autorización, contabilidad y facturación), calidad de servicio (QoS) y movilidad (MIP) todo ello sobre IPv6 y a través de diferentes medios de acceso (Ethernet, WLAN, WCDMA).

4.2 Entorno de QoS para aplicación de COPS

El entorno de aplicación y gestión de calidad de servicio que pasaremos a describir a continuación consta de los siguientes elementos:

4.2.1 Bandwidth Broker (BB)

- Controla el acceso a los servicios de la red por parte de los usuarios. Él es el encargado de hacer cumplir el SLA (Sevice Level Agreement) contratado. Partiendo de los requerimientos que tenga el tráfico de un usuario (BW, prioridad, retardo,...) escoge el DSCP más adecuado y se lo comunica (pasando por el AAAC) al usuario final para que éste marque el tráfico con ese identificador.
- Configura los dispositivos de aplicación de mecanismos de QoS => Routers de acceso. Es el servidor de políticas (PDP).
- Gestiona el uso de la red. Mediante los informes de uso del ancho de banda que le envían periódicamente los routers y conociendo los recurso de la red y los usuarios registrados, su algoritmo de control adaptativo permite reestructurar todos los flujos de usuarios mediante el control de las colas en los routers.

4.2.2 Router de acceso (RA)

- Gestiona y planifica las colas de QoS configuradas por el BB. Es el cliente de políticas (PEP).
- Captura información de los tráficos que lo atraviesan para luego preguntar por ellos al BB.
- Monitoriza las colas de QoS para informar al BB de su uso.
- Clasifica los tráficos salientes hacia las colas según el DSCP del tráfico y bajo orden del BB.

4.2.3 AAAC QoS (Autenticación, Autorización, Contabilidad y Facturación)

- Obtiene el perfil contratado de un usuario de la base de datos de usuarios autorizados, trata de instalarlo en el BB y obtiene los DSCPs de sus servicios de red asociados. Es otro tipo de cliente de políticas (PEP).
- Actualiza o borra dichos perfiles según los permisos de éste.

En la Fig 4.2 podemos ver el proceso completo que se produce al registrase un cliente en la red y mandar tráfico.

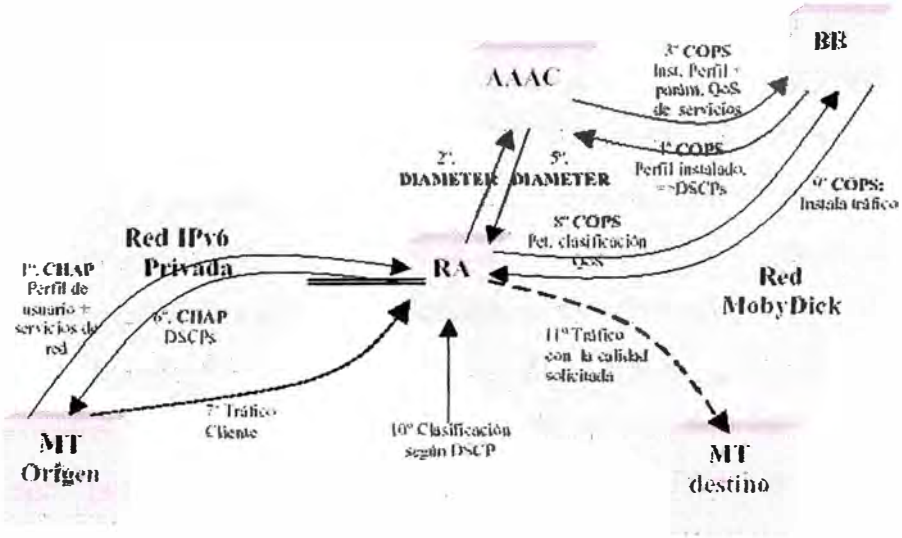


Fig 4.2 Proceso de envío de información en la red

- **1º**: Un cliente (terminal móvil) que desee registrarse en la red MobyDick, debe comunicarse con el AAAC para obtener los DSCPs con los que debe marcar su(s) tráfico(s) de salida según su perfil. El AAAC se encuentra dentro de la red DiffServ al otro lado del router de acceso por lo que debe establecer una serie de conexiones

de señalización seguras para poder acceder a éste. Primeramente el usuario debe comunicarse con su Router de acceso mediante una conexión autenticada mediante el protocolo CHAP (CHAlenge Protocol) para registrarse en el dominio DiffServ MobyDick.

- **2º**: Una vez que la autentificación CHAP se ha realizado con éxito, el router genera un nuevo mensaje de registro hacia el AAAC mediante el protocolo seguro DIAMETER. Este tráfico, al ser de señalización y tener la dirección origen del router, será clasificado a la clase EF (expedited forwarding), la más alta dentro de las calidades de servicio.
- **3º:** el AAAC consulta en sus tablas los permisos y tráficos que al usuario se le permite cursar y avisa al Bandwidth Broker a través del protocolo COPS pasándole toda la información relacionada con el usuario y sus tráficos: dirección origen, dirección de destino, tiempo de vida, ancho de banda, prioridad y máximo retardo permitido.
- **4º:** El Bandwidth Broker busca entonces en su tabla el DSCP más adecuado para cada servicio solicitado, añade estos a una tabla interna con todos los servicios activos y devuelve los DSCPs al AAAC para que éste se los comunique al cliente.
- **5º y 6º:** la información de los DSCPs con los que el cliente debe marcar sus diferentes tráficos viaja hasta él por el camino inverso que siguió el registro. Usando los protocolos de señalización anteriormente expuestos.
- **7º:** El cliente comienza entonces a enviar un tráfico hacia otro terminal. El router captura ese tráfico con su programa capturador y clasifica temporalmente los paquetes como 'por defecto' (clase best-effort), de esta forma se evita tener que retener los paquetes que causaría muchos problemas.
- **8º**: Mediante el protocolo COPS el Router de acceso de nuestra red pide al Bandwidth Broker si tiene o no que encaminar ese tráfico a la cola de QoS asociada a su DSCP. El Router le pasa al Bandwidth Broker la dirección origen y el DSCP del flujo de datos detectado.
- **9º:** El Bandwidth Broker comprueba entonces si ese tráfico está instalado en su tabla. Si el servicio estaba instalado, el Bandwidth Broker le envía al Router una confirmación positiva mediante la conexión COPS. Si no encuentra el tráfico en su tabla la respuesta es negativa y el tráfico seguirá clasificado como 'por defecto'.

La clasificación de QoS en el router tiene un tiempo de vida. Cuando ese tiempo se agota, el router hace una nueva petición para saber si ese flujo de datos debe seguir siendo clasificado hacia la misma cola o hacia la 'por defecto'. De esta forma la asignación de calidad de servicio a los flujos de datos puede actualizarse cada cierto tiempo. También el AAAC actualiza periódicamente el perfil de usuario en el BB o lo borra según los permisos del MT (equipo móvil).

4.3 Configuración y Estadísticas

Continuamos ahora describiendo los mecanismos de configuración y transferencia de estadísticas entre el router y el BB.

Antes de que el entorno opere en su modo normal el router debe haber solicitado al BB una configuración de sus colas. Además durante todo el tiempo que dura su ejecución el router debe encargarse de realizar dos operaciones: obtener estadísticas del uso de las disciplinas de cola instaladas en su interfaz de salida y comprobar si en los mensajes que le manda el BB se le solicita una reconfiguración de sus colas. El intervalo de tiempo entre dos informes de estadísticas está también configurado por el Bandwidth Broker ya que éste se lo indica en el primer mensaje COPS al arrancar.

Para solicitar una (re)configuración se deben seguir los siguientes pasos:

- Mediante un mensaje COPS de "Configuration Request" el router solicita al BB que le mande la configuración de las colas (nuevas o primeras).
- A través de otro mensaje COPS de "Configuration Decision" el BB le manda al router dicha configuración. El mensaje lleva N objetos COPS, tantos como DSCPs se puedan filtrar por el router. Cada objeto lleva los siguientes parámetros: DSCP (con el que se clasifican los tráficos hacia una cola), nº de agregado (permiten unir varios DSCPs en una clase), ancho de banda, f lag de uso de ancho de banda desocupado y parámetros de la cola RIO (Random Input-Output) si procede.
- Con la tabla recibida, el router procede a construir un árbol de calidad de servicio mediante las funciones de control de tráfico del TC API. Ese árbol tiene una forma como el de la parte superior derecha de la Fig 4.2.
- Tanto si todo el proceso de construcción de las colas ha resultado satisfactorio como si no el RA debe informar al BB mediante un mensaje COPS de "Configuration Report". Si la respuesta es negativa se reintentará un número predefinido de veces antes de cerrarse la conexión COPS y el Router.

Además de este proceso, el router periódicamente debe enviar un informe del estado de sus colas al BB. De este modo se cierra el lazo de control de políticas. Esta información va contenida en un mensaje COPS de "Accountig Report" con una línea por cada disciplina de colas creada. Los parámetros que se envían son: identificador de la disciplina, régimen binario, paquetes por segundo, descartes por segundo y sobrecargas por segundo promedio. Las estadísticas que se envían al BB sirven para que éste conozca remotamente la ocupación del router. Si el Bandwidth Broker necesitase cambiar la configuración de calidad de servicio del router se lo comunicaría y éste procedería a repetir una secuencia de configuración de nuevo. Durante el corto tiempo que dura una reconfiguración el implementador puede especificar el ancho de banda que se le proporciona a los tráficos mediante un parámetro en el router.

CAPITULO V
ANALISIS DE UN SLA

Los modelos de red con/sin SLA son los que se muestran en las Fig. 5.1/ 5.2

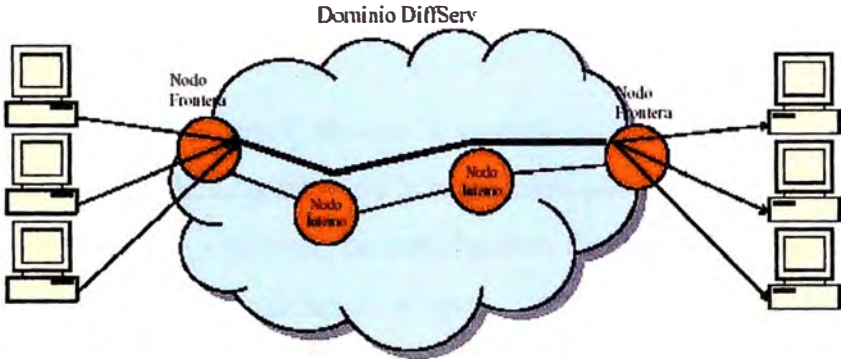


Fig. 5.1 Modelo de red sin SLA

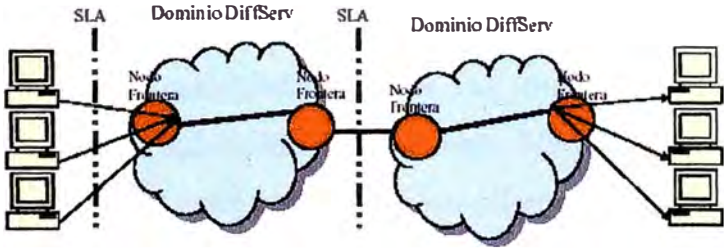


Fig. 5.2 Modelo de red con SLA

5.1 Introducción de SLA

Los SLAs son una herramienta fuerte para las empresas a fin de permitir un uso más eficiente de recursos tercerizados obteniendo un importante beneficio de la inversión. La

clave es encontrar un proveedor de servicios que satisfaga las necesidades de su empresa y, a través de un SLA bien confeccionado y redactado, se convierta en su socio.

5.2 Definición del SLA

El SLA es un convenio entre una empresa y un Proveedor de Servicios el cual establece pautas para la disponibilidad, confiabilidad y seguridad de redes. El proveedor de servicios está a cargo de destilar la complejidad de servicios de telecomunicaciones y convertirla en una serie simple de métricas aceptables y permisibles para la actividad comercial. Si se elige por tercerizar un servicio de red, se tiene que tener en cuenta lo siguiente:

- Confiabilidad, performance, ahorro de gastos.
- Performance mínima aceptable de la aplicación particular o de la conexión de red.
- El costo empresario y el costo de satisfacción de clientes si la red o el servidor que realiza el hosting de su aplicación se cae.
- Garantizar la utilización de las mejores prácticas y pautas abiertas.
- Facilitar la migración de un SP a otro si el SP no satisface las necesidades de su empresa.

Debido a que los ISPs buscan diferenciarse de la competencia, muchos de ellos están ofreciendo SLAs más completos.

5.3 ¿Qué debe cubrir un SLA?

Los SLAs deben cubrir la actividad de todos los routers, switches, vías, y puntos de presencia (POPs) a través de múltiples abastecedores. Un ISP que trunca el SLA basándose en el alcance de su red no les está contando a sus clientes toda la historia del servicio que se está prestando. A los clientes no les importa cómo se brinda el servicio, les importa qué servicio se está prestando.

Un SLA para un servicio de red privada virtual (VPN) puede específicamente determinar las pautas de calidad mínimas cubriendo disponibilidad de red (99,999 a 100 por ciento), umbrales de pérdida de paquetes (0,05 a 1 por ciento), y garantías de latencia para permitir a la empresa retener un cierto nivel de performance en la que puedan confiar las empresas y los clientes.

El SLA por lo general brinda un reembolso económico si el ISP no cumple con el nivel del servicio acordado en el convenio SLA. La forma del reembolso es generalmente a través de una nota de crédito por tiempo de servicios de red o devolución en efectivo (créditos) sobre los honorarios. El SLA puede ser automático o no. Un crédito automático es un

informe común (acordado) que automáticamente emite el crédito cuando fuera apropiado. El crédito automático es común en la industria satelital y se está haciendo estándar con los proveedores de servicios más importantes y estables. Un crédito por solicitud generalmente establece un plazo por el cual la empresa tiene que definir cualquier tiempo inactivo, informarlo, y solicitar el crédito. Algunas compañías audazmente reclaman disponibilidad 100% pero las letras de imprenta en el convenio establecen sólo créditos por solicitud, con un plazo para realizar el reclamo.

Un buen SLA ayuda a su empresa establecer umbrales mínimos sobre latencia y disponibilidad de la red. ¿Ayudan en sí las garantías de latencia y de disponibilidad en la decisión de la compra? La respuesta es: depende. Si se trata de un SLA, entonces la respuesta es probablemente no, pero si se elige un SP más pequeño, se tendría que prestar más atención a estas garantías para garantizar que los recursos son los adecuados para proteger los intereses de su empresa. Hay más temas conexos al SLA que las garantías de latencia y de disponibilidad, y el equipo prudente de redes analizará de cerca las opciones ofrecidas antes de elegir.

¿Qué es lo que uno debe tener en cuenta en un SLA? ¿Cómo se mide la performance? Primero, se debe entender el tipo de tráfico considerado para la tercerización. Existe una importante diferencia entre 60 milisegundos y 120 milisegundos de latencia de retorno si se soporta voz sobre IP (VoIP) o corrientes de video multicast, pero la diferencia en la latencia puede no ser tan importante si se soporta Internet o el correo electrónico de una empresa. Queda en manos del gerente de Tecnología de Información de la compañía decidir en base a los requerimientos comerciales de la empresa.

Como se mencionó anteriormente, los SLAs por lo general ofrecen créditos por no satisfacer las necesidades de acuerdo a lo convenido, pero ¿uno realmente quiere este crédito? El tiempo inactivo y el crédito no devolverán las ganancias perdidas y la desilusión del cliente causada por un error de la red. Si está negociando créditos por servicio y si su modelo comercial soporta VPNs, un escenario que requiere entre 99,999 y 100 por ciento de disponibilidad con menos de una pérdida de paquete del 1% y una latencia por debajo de los 60 milisegundos, entonces es importante asegurarse que el convenio SLA motive al SP para que preste un servicio de alta calidad y que cuenta con la infraestructura y experiencia en el lugar para prestar el servicio.

5.4 Los requisitos mínimos para QBone SLA

De acuerdo con el modelo arquitectónico de DiffServ, todo los SLAs se determinan en forma bilateral entre las redes adyacentes de QBone (dominios DS definidos en [RFC2475]). Sin embargo, para implementar QoS, deben de ser resueltos ciertos requisitos mínimos(SLA) para cualquier QBone . Lo que viene a continuación es una lista de las recomendaciones ("shoulds") y de requisitos ("must") para cualquier QBone SLA que apoya QoS.

La lista asume un SLA bilateral entre un dominio de mas alta jerarquia (Upstream), llamado U de QBone DS y un dominio en sentido descendiente D de QBone DS.

- Dentro del QBone, el octeto Codepoint 101110 del DS se debe utilizar para el PHB EF .
- El dominio D (mas alta jerarquía) D debe de responder a las peticiones de reserva del dominio U. El protocolo por el cual una reserva es establecida especifica cómo D debe responder a las al requerimiento de las peticiones .
- Una parte necesaria e importante de cualquier SLA es un TCA que especifica cómo el tráfico se condiciona en el ingreso. El TCA es un componente dinámico del SLA, que puede necesitar ser ajustado con la creación o el desmontaje de cada reservación . Para poner QoS en ejecución, un TCA debe especificar:
  1. **Acondicionamiento del tráfico**: Primero, el tráfico que ingresa se debe acondicionar en EF y tráfico no EF. Luego el tráfico de EF se puede acondicionar en un solo agregado de comportamiento de EF (BA) o un sistema de EF BAs, cada uno de el cual se podría definir por prefijo de la destinación o por el acoplamiento de la salida en el dominio D.
  2. **Perfiles del tráfico:** Un perfil del tráfico se debe especificar para cada agregado del comportamiento. Dado una tarifa máxima R y "MTU" M del servicio, el perfil del tráfico es definido por un cubo simbólico con un índice simbólico de los octetos de R por segundo y una profundidad del cubo de los octetos de M.
  3. **Disposición de exceso del tráfico:** El tráfico dentro de un BA que exceda el perfil del agregado deba ser desechado.
  4. **El Agrupador:** La generación de los agregados individuales se puede apoyar por los nodos del borde de ingreso / salida del QBone
- El tráfico de ingreso EF del · que se conforma con los perfiles del tráfico del TCA será dado el tratamiento de EF a través del dominio U del DS hacia su destinación.

El EF PHB requiere baja pérdida, baja latencia, aseguramientos en la entrega de los paquetes.

- Los paquetes EF se deben encaminar idénticamente a los paquetes que tienen el PHB con el mejor esfuerzo.
- Cada SLA debe especificar el aseguramiento del jitter hecho al tráfico de EF que se conforma

5.5 Ejemplo : Servicios ofrecidos por la NIC de Mexico

A continuación voy a mostrar el escaneo de algunos originales de los servicios ofrecidos por la NIC México en la actualidad en lo que a IPv6 se refiere:

5.5.1 Registro de bloques de direcciones IPv6

1. Solicitud inicial de un bloque de direcciones IPv6: Para solicitar por primera vez un bloque de direcciones IPv6, debe realizar lo siguiente:
    a) Leer la información relacionada
        - Direcciones

El bloque mínima asignado por NIC México es un /32 y para calificar para la asignación inicial, la organización debe:

1. Ser un LIR (Local Internet Registry), o sea, organización que asigna direcciones para usuarios de los servicios de red que provee. Son, en general, los proveedores de acceso (ISP), cuyos clientes son los usuarios finales u otros proveedores de acceso;
2. No ser un sitio final (usuario final);
3. Documentar un plan detallado sobre los servicios y la conectividad en IPv6 a ofrecer a otras organizaciones (clientes).
4. Anunciar en el sistema de rutas inter-comunio de Internet un único bloque, que agregue todo la asignacion de direcciones IPv6 recibida, en un plazo no mayor de 12 meses;
5. Ofrecer servicios en IPv6 a clientes localizados físicamente en la región del LACNIC en un plazo no mayor de 24 meses.

Antes de hacer la solicitud de un bloque IPv6, le recomendamos leer las

Para solicitar un bloque IPv6 la organización debe llenar el y enviarlo después a la cuenta de correo

Una vez aprobada la solicitud de asignación inicial, un e-mail será enviado con información sobre el Contrato de Prestacion de Servicios (IGA-A) que debe ser firmado y enviado con los siguientes datos (NIC México enviará, a nuestra discreción, su respectiva copia al cliente):

Atn.: Ing. Cristóbal Chapital Tirado
NIC México
Av. Eugenio Garza Sada 427 L4-G
Col. Altavista
Monterrey, Nuevo León
México
C.P. 64840

Después de recibir el contrato firmado NIC México enviará las instrucciones para efectuar el pago correspondiente (para mayor información le sugerimos visitar nuestra página de Tarifas). La asignación solamente será hecha después de la recepción del pago.

- **Políticas IPv6**

Políticas IPv6

A continuación se detallan las políticas que aplican para la asignación de bloques de direcciones IPv6. Sin embargo para la solicitud de este recurso debe dirigirse directamente con LACNIC.

Para mayor información puede revisar la liga (http://lacnic.net sp...html)

Resumen

Este documento define las políticas de registración para la asignación y adjudicación de direcciones IPv6 globalmente únicas a los ISPs y otras organizaciones. Este documento reemplaza el "Provisional IPv6 assignment and allocation policy document".

Este documento fue desarrollado conjuntamente por las comunidades de APNIC, ARIN, y RIPE.

Contenidos

1. Introducción

1.1. Alcance

Este documento describe políticas para la adjudicación y asignación del espacio globalmente único de direcciones IPv6. Actualiza y reemplaza al documento existente, Provisional IPv6 Policies en uso desde 1999 [RIRv6 Policies]. Las políticas descritas en este documento están pensadas para ser adoptadas por cada registro. Sin embargo, la adopción de este documento no excluye variaciones locales en cada región o área.

[RFC2373, RFC2373bis] designan 2000::/3 a ser el espacio global de direcciones unicast que IANA puede adjudicar a los RIRs. De acuerdo con [RFC2928, RFC2373bis, IAB Request], IANA ha adjudicado rangos iniciales del espacio de direcciones globales unicast de IPv6 del bloque de direcciones 2001::/16 a los RIRs existentes. Este documento trata las adjudicaciones iniciales y subsiguientes del espacio de direcciones unicast 2000::/3, para los cuales los RIRs formulan políticas de ajudicación y asignación. Dado que los end sites generalmente recibirán asignaciones de /48 [RFC 3177, RIRs on 48s], el énfasis particular de este documento es sobre las políticas relacionadas con los bits dentro de 2000::/3 a la izquierda del limite /48.

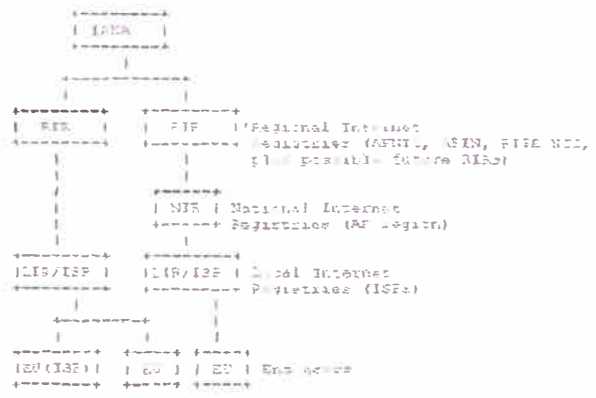
Sin embargo, ya que algunos end sites recibirán asignaciones de /64 y /128, todos los bits a la izquierda del /64 están dentro del alcance.

Esta política es considerada interina. Será revisada en el futuro, cuando se disponga de mayor experiencia en la administración de IPv6.

2. Definiciones

Los siguientes términos y sus definiciones son de gran importancia para la comprensión de los objetivos, contextos y políticas descritas en este documento.

La responsabilidad de la administración del espacio de direcciones de IPv6 está distribuida globalmente de acuerdo con la estructura jerárquica que se muestra debajo.



2.1. Internet Registry (IR)
Un Internet Registry (IR) es una organización responsable de la distribución de espacios de direcciones IP a sus miembros o clientes y del registro de esa distribución. Los IRs están clasificados de acuerdo a su función principal y alcance territorial dentro de la estructura jerárquica delineada en la figura de arriba.

2.2. Regional Internet Registry (RIR)
Los Regional Internet Registries (RIRs) son establecidos y autorizados por las comunidades regionales respectivas, y reconocidos por el IANA para servir y representar grandes regiones geográficas. El rol principal de los RIRs es administrar y distribuir el espacio de direcciones público de Internet dentro de las respectivas regiones.

2.3. National Internet Registry (NIR)
Un National Internet Registry (NIR) adjudica, principalmente, espacios de direcciones a sus miembros o constituyentes, los cuales son generalmente LIRs a un nivel nacional. Los NIRs existen mayormente en la región de Asia Pacífico.

2.4. Local Internet Registry (LIR)
Un Local Intenet Registry (LIR) es un IR que asigna, principalmente, espacios de direcciones a los usuarios de los servicios de red que éste provee. Los LIRs son generalmente ISPs, cuyos clientes son principalmente usuarios finales y posiblemente otros ISPs.

2.5. Adjudicar
Adjudicar significa distribuir el espacio de direcciones a los IRs con el propósito de que ellos realicen la subsiguiente distribución.

2.6. Asignar
Asignar significa delegar espacio de direcciones a un ISP o usuario final, para su uso específico dentro de la infraestructura de Internet que ellos operan. Las asignaciones deben ser realizadas solamente para los propósitos específicos documentados por organizaciones específicas y no para ser sub asignadas a otras partes.

2.7. Utilización
A diferencia de IPv4, IPv6 es generalmete asignado a end sites en cantidades fijas (/48). La utilización real de direcciones dentro de cada asignación será bastante baja comparada con las asigaciones de IPv4. En IPv6, "utilización" es medida en términos de los bits a la izquierda del límite /48. En otras palabras, la utilización se refiere a la asignación de /48s a los end sites, y no al número de direcciones asignadas dentro de /48s individuales en esos end sites.

A lo largo de este documento, el término utilización se refiere a la adjudicación de /48s a los end sites, y no al número de direcciones asignadas dentro de los /48s individuales en esos sites.

2.8. HD Ratio
El HD Ratio es un modo de medir la eficiencia de asignación de direcciones [RFC 3194]. Es una adaptación del H Ratio, originalmente definido en [RFC1715], y es expresado de la siguiente manera:

$$HD = \frac{\text{Log (numero de objetos adjudicados)}}{\text{Log (número máximo de objetos adjudicables)}}$$

donde, en el caso de este documento, los objetos son direcciones IPv6 de sites (/48s) asignadas desde un prefijo IPv6 de un tamaño dado.

2.9. End site
Un end site es definido como un usuario final (suscriptor) que tiene una relación de negocios con un proveedor de servicios que involucra:

- al proveedor de servicios asignando un espacio de direcciones al usuario final
- al proveedor de servicios otorgando un servicio de tránsito para el usuario final hacia otros sites
- al proveedor de servicios transportando el tráfico del usuario final
- al proveedor de servicios anunciando un prefijo de ruta agregado que contiene la asignación del usuario final

3. Objetivos de la administración del espacio de direcciones IPv6

3.1. Objetivos
El espacio de direcciones IPv6 es un recurso público que debe ser administrado de manera prudente teniendo en cuenta los intereses de Internet a largo plazo. Una adminsistración responsable del espacio de direcciones involucra balancear un conjunto de objetivos que a veces compiten entre sí. Los siguientes son los objetivos relevantes para la política de direcciones de IPv6.

3.2. Unicidad
Cada asignación y/o adjudicación del espacio de direcciones debe garantizar la unicidad en todo el mundo. Este es un requerimiento indispensable para asegurar que cada host público en Internet pueda ser identificado univocamente.

3.3. Registro
El espacio de direcciones de Internet debe ser registrado en una base de datos accesible por miembros autorizados dentro la comunidad de Internet. Esto es necesario para asegurar la unicidad de cada dirección de Internet y para proveer información de referencia sobre los problemas de Internet en todos los niveles, desde los RIRs e IRs hasta los usuarios finales.

El objetivo del registro debería ser aplicado dentro del contexto consideraciones de privacidad razonables y leyes aplicables.

3.4. Agrupación
Cuando sea posible, el espacio de direcciones debería ser distribuido de manera jerárquica, de acuerdo a la topología de la infraestructura de la red. Esto es necesario para permitir la agregación de información de ruteo por parte de los ISPs, y para limitar la expansión de las tablas de ruteo en Internet.

Esta meta es particularmente importante en el direccionamiento de IPv6, donde el tamaño del espacio de direcciones total tiene implicaciones significativas tanto para el ruteo interno como externo.

Las políticas de direcciones IPv6 deberían buscar evitar la fragmentación de los rangos de direcciones.

Más aún, los RIRs deberían aplicar prácticas para maximizar el potencial de que las adjudicaciones subsecuentes sean contiguas con las adjudicaciones poseídas actualmente. Sin embargo, no puede haber garantías de adjudicación contigua.

3.5. Conservación
Aunque IPv6 provee un espacio de direcciones extremadamente grande, las políticas de direcciones deberían evitar su desperdicio innecesario. Los pedidos de espacios de direcciones deberían estar avalados por documentación apropiada y debería evitarse la acumulación de direcciones no utilizadas.

3.6. Equidad
Todas las políticas y prácticas relacionadas al uso del espacio de direcciones públicas deberían aplicarse justa y equitativamente a todos los miembros potenciales y existentes de la comunidad de Internet, independientemente de su ubicación, nacionalidad, tamaño o cualquier otro factor.

3.7. Minimización de sobrecarga
Es deseable minimizar la sobrecarga asociada a la obtención de espacio de direcciones. La sobrecarga incluye la necesidad de solicitar espacio adicional a los RIRs muy frecuentemente, la sobrecarga asociada con la administración de espacios de direcciones que crecen vía expansiones sucesivas de pequeños de incrementos en lugar de a través de menos expansiones, más grandes.

3.8. Conflicto entre objetivos
Los objetivos descritos arriba a menudo entrarán en conflicto unos con otros, o con las necesidades individuales de los IRs o usuarios finales. Todos los IRs, al evaluar los pedidos de adjudicación y asignación deben juzgar, buscando balancear las necesidades de los solicitantes con las necesidades de la comunidad de Internet como un todo.

En la política de direcciones de IPv6, el objetivo de agregación es considerado el más importante.

4. Principios de la política IPv6

Para cumplir con los objetivos descritos en la sección anterior, las políticas en este documento discuten y siguen los principios básicos descritos debajo

4.1. Espacio de direcciones no debe ser considerado propietario
Es contrario a los objetivos de este documento y no se encuentra entre los intereses de la comunidad de Internet en su conjunto que los espacios de direcciones sean considerados propietarios.

Las políticas en este documento se basan en el entendimiento de que el espacio globalmente único de direcciones unicast de IPv6 es licenciado para su uso en lugar de adueñado. Específicamente, las direcciones IP serán adjudicadas y asignadas en base a una licencia, con licencias sujetas a renovación periódica. El otorgamiento de una licencia está sujeta a condiciones específicas a aplicarse al comienzo como así también en cada renovación de la misma.

Los RIRs generalmente renovarán las licencias automáticamente, siempre que las organizaciones solicitantes hagan un esfuerzo de buena fe para cumplir con el criterio bajo el cuál calificaron o fueron otorgadas una adjudicación o asignación. Sin embargo, en aquellos casos en que una organización no está utilizando el espacio de direcciones como se espera, o está mostrando mala fe en regirse por las obligaciones asociadas, los RIRs se reservan el derecho de no renovar la licencia.

Notar que cuando una licencia es renovada, la nueva licencia será evaluada y controlada bajo las políticas de direcciones de IPv6 aplicables en el lugar y momento de la renovación, las cuales podrían diferir de las políticas bajo las cuales fue originalmente adjudicada o asignada.

4.2. Ruteabilidad no garantizada
No hay garantías de que la adjudicación o asignación de una dirección será ruteable globalmente.

Sin embargo, los RIRs deben aplicar procedimientos que reduzcan la posibilidad de fragmentación del espacio de direcciones, lo que podría llevar a la pérdida de ruteabilidad.

4.3. Adjudicación Mínima
Los RIRs aplicarán un tamaño mínimo para adjudicaciones de IPv6 para facilitar el filtro basado en el prefijo.

El tamaño mínimo de adjudicación para un espacio de direcciones IPv6 es /32.

4.4. Consideraciones de la infraestructura de IPv4
Cuando un proveedor de servicios de IPv4 pide espacio IPv6 para una transición final de servicios existentes a IPv6, el número de clientes actuales de IPv4 podría ser usado para justificar un pedido más grande del que estaría justificado si el mismo estuviera basado solamente en la infraestructura IPv6.

5. Políticas para adjudicaciones y asignaciones

5.1. Adjudicación inicial

5.1.1. Criterio de adjudicación inicial
Para calificar para la adjudicación inicial de un espacio de direcciones IPv6, una organización debe:

a. ser un LIR;
b. no ser un end site;
c. planear proveer conectividad IPv6 a organizaciones a las cuales asignará /48s, anunciando esa conectividad a través de su única dirección agregada de adjudicación; y
d. tener un plan para realizar al menos 200 asignaciones de /48 a otras organizaciones dentro de un período de 2 años.

5.1.2. Tamaño de adjudicación inicial
Las organizaciones que cumplan con el criterio de adjudicación inicial pueden recibir un mínimo de adjudicaciones de /32.

Las organizaciones podrían calificar para una adjudicación inicial más grande que /32 entregando documentación que justifique razonablemente el pedido. Si así lo hicieran, el tamaño de adjudicación estará basado en el número de usuarios existentes y en la extensión de la infraestructura de la organización.

5.2. Adjudicación subsiguiente
Las organizaciones que ya tengan una adjudicación IPV6 pueden recibir adjudicaciones subsiguientes de acuerdo a las siguientes políticas.

5.2.1. Criterio de alocación subsiguiente
La adjudicación subsiguiente será provista cuando una organización (ISP/LIR) satisfaga el umbral de evaluación de utilización histórica de direcciones en términos del número de sites en unidades de asignaciones de /48. El HD Ratio [RFC 3194] es usado para determinar los umbrales de utilización que justifican la adjudicación de direcciones adicionales como se describe debajo.

5.2.2. HD Ratio aplicado
El valor HD Ratio de 0.8 es adoptado como una aceptable utilización de direcciones para justificar la adjudicación de espacio de dirección adicional. El apéndice A provee una tabla que muestra el número de asignaciones que son necesarias para lograr un valor aceptable de utilización dado el tamaño del bloque de direcciones.

5.2.3. Tamaño de la adjudicación subsiguiente
Cuando una organización ha logrado una aceptable utilización de su espacio de direcciones adjudicado, está inmediatamente calificada para obtener una adjudicación adicional que resulte en una duplicación de su espacio de direcciones adjudicado. Cuando sea posible, la adjudicación será realizada de bloques de direcciones adyacentes, es decir que su adjudicación existente es extendida un bit hacia la izquierda.

Si una organización necesita más espacio de direcciones, debe proveer documentación justificando sus requerimientos para un período de 2 años. La adjudicación se basará en este requerimiento.

5.3. Adjudicación de LIR a ISP

No hay una política específica para la adjudicación de espacio de direcciones de una organización (LIR) a los ISPs subordinados. Cada LIR podría desarrollar su propia política para ISPs subordinados para alentar una utilización óptima del bloque de direcciones total adjudicado al LIR. Sin embargo, todas las asignaciones de /48 a end sites deben ser registradas por el LIR o por sus ISPs subordinados de modo que el RIR/NIR puede evaluar apropiadamente el HD Ratio cuando es necesaria una adjudicación subsiguiente.

5.4. Asignación

Los LIRs deben realizar asignaciones IPV6 de acuerdo con las siguientes provisiones.

5.4.1. Asignación del espacio de direcciones

Las asignaciones deben ser realizadas de acuerdo con las recomendaciones existentes [RFC3177,RIRs on 48], las cuales resumimos aquí como:
/48 en el caso general, excepto para suscriptores muy grandes

/64 cuando se conoce por diseño que una y sólo una subred es necesaria

/128 cuando se conoce absolutamente que uno y sólo un dispositivo se está conectando.

A los RIRs/NIRs no les concierne el tamaño de direcciones que los LIR/ISP realmente asignan. Por lo tanto, los RIRs/NIRs no pedirán información detallada sobre redes de usuarios IPV6 como lo hicieron en Ipv4, excepto para los casos que se describen en la Sección 4.4 y para los propósitos de medir la utilización como se define en este documento.

5.4.2. Asignación de múltiples /48s a un solo site

Cuando un solo end site requiere un bloque de direcciones de /48 adicional, debe pedir la asignación con documentación o materiales que justifiquen el pedido. Los pedidos de bloques múltiples o adicionales de /48s serán procesados y revisados (ej: evaluación de la justificación) al nivel de los RIR/NIR.

Nota: No hay experiencia en el presente con la asignación de múltiples /48s a un mismo end site. Se prevé que la necesidad de que el RIR revise todas estas asignaciones sea una medida temporaria hasta tanto se adquiera algo de experiencia y que se hallan desarrollado algunas políticas comunes. Además, el trabajo adicional de definir políticas en este espacio probablemente será llevado a cabo en un futuro cercano.

5.4.3. Asignación a la infraestructura del operador

Una organización (ISP/LIR) puede asignar un /48 por PoP como un servicio de infraestructura de un operador de servicio IPv6. Cada asignación a un PoP es considerada como una asignación sin tener en cuenta el número de usuarios que usen el PoP. Puede obtenerse una asignación separada para operaciones propias del operador.

5.5. Micro-Asignaciones en IPv6

LACNIC podrá realizar micro-asignaciones en casos de proyectos e infraestructuras de redes claves o críticas para el funcionamiento, y desarrollo de IPv6 en la región como son IXP (Internet Exchange Point), NAP (Network Access Point), RIR, proveedores de DNS ccTLD, entre otros. Dichas asignaciones se realizarán en bloques menores o igual a un /32 pero siempre mayores o iguales a un /48.

En el caso de los IXP o NAP para poder solicitar este tipo de asignaciones las organizaciones deberán cumplir los siguientes requisitos:

1. Documentar adecuadamente los siguientes aspectos:
   - 1.1. Demostrar a través de sus estatutos su calidad de IXP o NAP. Deberá poseer al menos tres miembros y una política abierta para la asociación de nuevos miembros.
   - 1.2.Enviar un diagrama de la estructura de red de la organización.
   - 1.3.Documentar el plan de numeración a instrumentar.
2. Proveer un plan de utilización para los próximos tres y seis meses.

El resto de las solicitudes se estudiarán basados en el análisis de documentación que justifique los aspectos críticos y/o claves del proyecto.

Todas las micro-asignaciones se asignarán de bloques de direcciones específicamente reservados para este tipo de asignaciones. LACNIC hará pública la lista de dichos bloques y las micro-asignaciones realizadas.

La organización que reciba una micro-asignación no podrá realizar subasignaciones con estas direcciones IP.

5.6. Registro

Cuando una organización que posee una adjudicación de espacio IPv6, hace asignaciones

de espacios IPv6, debe registrar la información de asignaciones en una base de datos accesible a los RIRs como corresponde (la información registrada por un RIR/NIR puede ser cambiada en el futuro por una base de datos para registrar manejo de direcciones). La información es registrada en unidades de redes /48 asignados. Cuando a una organización se le asigna más de una /48 la organización que la asigna es responsable de asegurar que el espacio de direcciones esté registrado en una base de datos RIR/NIR.

Los RIR/NIRs usarán los datos registrados para calcular el HD Ratio en el momento de la solicitud, para subsecuentes adjudicaciones y para verificar eventuales cambios en las asignaciones.

Los IRs deben mantener sistemas y prácticas que protejan la seguridad de la información personal y comercial que es usada en la evaluación de solicitudes, pero que no es requerida para registro pública.

5.7. Reverse lookup

Cuando un RIR/NIR delega espacio de direcciones Ipv6 a una organización, también está delegando la responsabilidad de manejar la zona de reverse lookup que corresponde al espacio de direcciones IPv6 asignado. Cada organización debe manejar debidamente su zona de reverse lookup. Cuando una organización hace una asignación de direcciones, debe delegar a la organización asignada, bajo pedido, la responsabilidad de manejar la zona de reverse lookup que corresponde a la dirección asignada.

5.8. Poseedores de IPv6 ya existentes

Las organizaciones que hayan recibido adjudicaciones de IPv6 /35 bajo la política previa de IPv6 [RIRv6 Policies] están inmediatamente autorizadas a expandir su asignación a un bloque de direcciones /32 sin necesidad de justificación, siempre y cuando satisfagan los criterios de la Sección 5.1.1. El bloque de direcciones /32 contendrá el bloque más pequeño ya adjudicado (uno o múltiples /35 bloques en muchos casos) que ya ha sido reservado por el RIR para una subsecuente asignación a la organización. Las solicitudes de espacio adicional más allá del mínimo tamaño /32 serán evaluadas como se discutió en otra parte del documento.

6. Referencias

[RFC1715] "The H Ratio for Address Assignment Efficiency", C. Huitema. November 1994, RFC 1715.
[IAB Request] "Email from IAB to IANA",
http://www.iab.org/documents/docs/2002-04-email.txt
[RFC2373] "IP Version 6 Addressing Architecture", R. Hinden, S. Deering. July 1998, RFC 2373.
[RFC2373bis] http://www.ietf.org/internet-drafts/draft-ietf-ipngwg-addr-arch-v3-07.txt
[RFC2928] "Initial IPv6 Sub TLA ID Assignments", R. Hinden, S. Deering, R. Fink, T. Hain, September 2000, RFC 2928.
[RFC3177] "IAB/IESG Recommendations on IPv6 Address". IAB, IESG. September 2001, RFC 3177.

[RFC3194] "The H Density Ratio for Address Assignment Efficiency An Update on the H ratio", A. Durand, C. Huitema. November 2001, RFC 3194.
[RIRs on 48] http://www.arin.net/policy/ipv6_48assign.html
[RIRv6 Policies]
http://www.arin.net/policy/ipv6.html
http://www.ripe.net/ripe/docs/ripe-196.html
http://www.apnic.net/docs/draft-ap-ipv6-policy.html

7. Apéndice A: HD Ratio

El HD Ratio no tiene el fin de reemplazar las mediciones tradicionales de uso que los ISPs tienen actualmente con IPv4. De hecho, el HD Ratio aún requiere el conteo de objetos asignados. El principal valor del HD Ratio es su utilidad al determinar los rangos razonables de utilización para un espacio de direcciones de un tamaño dado. Este documento utiliza el HD Ratio para determinar los rangos en los cuales una asignación dada ha alcanzado un nivel aceptable de utilización y se justifica la asignación de espacio adicional.

El rango de utilización T, expresado como un número individual de prefijos /48 a ser adjudicados desde un prefijo P de IPv6 puede ser calculado como:

$$T = 2^{((48-P)*HD)}$$

Por consiguiente, el rango de utilización de una organización que solicita subsecuentes asignaciones de bloques de direcciones IPv6 es especificado en función del tamaño del prefijo y el HD ratio. Esta utilización se refiere a la asignación de /48s a los end sites y no a la utilización de esos /48s dentro de los end sites. Es un HD ratio de la utilización de una alocación de direcciones y no de una asignación de direcciones.

De acuerdo a las recomendaciones de [RFC 3194], este documento adopta un HD Ratio de 0.8 como el rango de utilización para alocaciones de espacio de direcciones IPv6.

45	3	8	4	50.0%
44	4	16	9	57.4%
43	5	32	16	50.0%
42	6	64	28	43.5%
41	7	128	49	37.9%
40	8	256	84	33.0%
39	9	512	147	28.7%
38	10	1024	256	25.0%
36	12	4096	776	18.9%
35	13	8192	1351	16.5%
34	14	16384	2353	14.4%
33	15	32768	4096	12.5%
32	16	65536	7132	10.9%
30	18	262144	22417	9.5%
29	19	524288	37641	7.2%
28	20	1048576	65536	6.3%
27	21	2097152	114105	5.4%
26	22	4194304	198668	4.7%
25	23	8388608	345901	4.1%
23	25	33554432	1048576	3.1%
22	26	67108864	1825677	2.7%
21	27	134217728	3178688	2.4%
20	28	268435456	5534417	2.1%
19	29	536870912	9635980	1.8%
18	30	1073741824	16777216	1.6%
16	32	4294967296	50859008	1.2%
15	33	8589934592	88550677	1.0%
14	34	17179869184	154175683	0.9%
13	35	34359738368	268435456	0.8%
12	36	68719476736	467373275	0.7%
10	38	274877906944	1416810831	0.5%
9	39	549755813888	2466810934	0.4%
8	40	1099511627776	4294967296	0.4%
7	41	2199023255552	7477972398	0.3%
6	42	4398046511104	13019906166	0.3%
5	43	8796093022208	22668973294	0.3%

8. Apéndice B: Información sobre antecedentes

8.1. Antecedentes

reunión de APNIC celebrada en Taiwán en agosto de 2001. Discusiones sucesivas se mantuvieron en octubre de 2001 en las reuniones de RIPE y ARIN. Durante éstos una política general que todos los RIRs podrían utilizar, pero dejando detalles de las discusiones individuales que condujeron a las políticas descriptas en el mismo; información detallada acerca de estas puede encontrarse en las minutas de cada uno de los meetings que se encuentran en los siguientes sitios web:

www.apnic.net,
www.arin.net, y
www.ripe.net

8.2. Por qué una política conjunta
Las direcciones Ipv6 son un recurso público que debe ser manejado considerando los intereses a largo plazo de la comunidad de Internet. Aunque los registros regionales adopten políticas de asignación de acuerdo a sus propios procesos internos, las políticas de direcciones deben ser uniformes entre los registros. Tener políticas significativamente variadas en las diferentes regiones no es deseable pues puede conducir a situaciones donde puede ocurrir el "registry shopping" con organizaciones solicitando direcciones a los registros que tengan las políticas más favorables para sus intereses particulares. Esto puede conducir a que las políticas en una región socaven los esfuerzos de registros de otras regiones con respecto a la prudente administración del espacio de direcciones. En los casos en que las variaciones regionales de las políticas sean razonablemente necesarias el abordaje preferido es el de presentar el tema a los otros registros regionales para lograr un acercamiento de consenso que todos los registros apoyen.

8.3. El tamaño de los espacios de direcciones IPv6
Comparado con IPv4, el Ipv6 tiene un aparente interminable espacio de direcciones. Si bien esto es superficialmente cierto, políticas de adjudicación de poca visión y desperdicio pueden resultar en la adopción de prácticas que conduzcan a un prematuro vaciamiento del espacio de direcciones.

Debe notarse que el espacio de direcciones de 128 bit es dividido en tres partes lógicas, con el uso de cada componente administrado en forma diferente. Los 64 bits de más a la derecha, el Interface Identifier [RFC2373], será frecuentemente un globalmente único IEEE identifier (por ej., mac address). Aunque ésta sea una forma "ineficiente" de usar el campo Interface Identifier, desde el punto de vista de maximizar el número de nodos direccionables, el esquema de numeración fue explícitamente elegido para simplificar la Stateless Address Autoconfiguration [RFC2462].

Los 16 bits del medio de una dirección indican el ID de la subred. Por [RFC 3177, RIRs on 48s], este campo será frecuentemente utilizado en forma ineficiente, pero los beneficios operacionales de un ancho de campo de subred regular fueron considerados para compensar las desventajas.

Las decisiones para utilizar en forma ineficiente los bits hacia la derecha de /48 fueron hechas bajo el conocimiento y la presunción de que los bits a la izquierda de /48 serían prudentemente administrados. Si así se hace, esto será conveniente para la esperada duración de IPv6 [RFC3177].

8.4. Reconocimientos
La version inicial de este documento fue producida por el equipo de redacción de políticas JPNIC IPv6 formado por: Akihiro Inomata, Akinori Maemura, Kosuke Ito, Kuniaki Kondo, Takashi Arano, Tomohiro Fujisaki, y Toshiyuki Yamasaki. Van agradecimientos especiales hacia este equipo que trabajó durante un feriado para producir rápidamente el documento inicial.

Un equipo de edición fue luego organizado por representantes de los tres RIRs (Takashi Arano, Chair of APNIC s Policy SIG, Thomas Narten, Chair of ARIN s IPv6 WG, and David Kessens, Chair of RIPE NCC s IPv6 WG).

El equipo de edición desea agradecer las contribuciones a éste documento de Takashi Arano, John Crain, Steve Deering, Gert Doering, Kosuke Ito, Richard Jimmerson, David Kessens, Mirjam Kuehne, Anne Lord, Jun Murai, Paul Mylotte, Thomas Narten, Ray Pizak, Dave Pratt, Stuart Prevost, Barbara Roseman, Gerard Ross, Paul Wilson, Cathy Wittbrodt y Wilfried Woeber.

La edición final de este documento fue hecha por Thomas Narten.

- **Información Contrato de Prestación de Servicios**

Información Contrato de Prestación de Servicios

El Contrato de Prestación de Servicios para clientes de Direcciones IP y ASN ofrece los siguientes beneficios:

Servicios de Direcciones IP y ASN

El cliente obtendrá la descripción detallada de los servicios de Direcciones IP y ASN prestados por NIC México, mismos que podrá solicitar en cuanto lo considere necesario.

El contrato establece un compromiso formal de NIC México hacia sus clientes en lo que respecte a los servicios ofrecidos.

Los servicios de NIC México incluyen de forma enunciativa más no limitativa: el registro, administración, transferencia y revocación de Bloques IP; resolución inversa de los Bloques IP registrados y apoyo en el mantenimiento de los datos de los Bloques de Direcciones IP en el WHOIS de LACNIC.

Certidumbre de los recursos

Tener el reconocimiento ante NIC México, LACNIC y la comunidad de Internet en general, de que los recursos especificados en el contrato están registrados para el uso exclusivo del cliente.

Adicionalmente al registro del cliente y sus recursos en el WHOIS de LACNIC, el cliente contará con un documento con validez jurídica que demuestre que los recursos especificados han sido registrados para su entidad por NIC México.

Membresía

Los miembros de LACNIC son tomados en cuenta en las discusiones y votaciones de propuestas para actualizar las políticas de LACNIC. Como miembro contará con votos de acuerdo a la categoría que tenga, que considera al espacio de direccionamiento que tenga registrado.

Las organizaciones que han registrado bloques de direcciones IP ante NIC México se convertirán automáticamente en miembros o asociados Activos "A" de LACNIC, en caso de que la organización ya cuente con algún tipo de Membresía en LACNIC, se establecerá el tipo de Membresía a otorgar.

Para mayor información respecto a la membresía LACNIC favor de revisar, en el estatuto, los siguientes artículos:
- Categorías de asociados, Artículo 6º.
- Derechos de los asociados, Artículo 7º.
- Obligaciones de los asociados, Artículo 8º
- Régimen disciplinario referente a los asociados, Artículos del 9º. al 11º.
- Respecto a las Asambleas en las que pueden participar los miembros o asociados, Capitulo V, en especial el Artículo 19º. que detalla los votos a que tienen derecho los mismos de acuerdo al espacio de direcciones IP que tienen registrado.

- **Tarifas**

/15	512	131072
/14	1024	262144

Direcciones IPv6*

ISP's

Tamaño	Monto Inicial USD	Monto Renovación USD	Renovación** USD (tarifa aplicable hasta 30 días posteriores a la fecha de aniversario)
/32	$2,500	$2,500	$2,250
>32	$20,000	$20,000	$18,000

En la actualidad y hasta nueva resolución del Directorio de LACNIC, las organizaciones que califiquen para recibir bloques de direcciones IPv6, estarán exoneradas de pagar los dos primeros años, o sea el pago inicial y la primera renovación.
Esta medida se toma como una forma de promoción de la adopción de IPv6 en la región de cobertura de LACNIC y ante la solicitud de varias organizaciones que hicieron este planteo.

Con esta medida, el directorio de LACNIC intenta dar respuesta a las necesidades de la comunidad de Internet de la región.

ASN*

El costo por asignación de un Sistema Autónomo (ASN) es de USD 500. La tasa anual de mantenimiento es de USD 50 y se cobra por adelantado cada año.

Usuarios Finales

Monto Inicial USD	Monto de Mantenimiento USD
$500	$50

Aquellas instituciones en la categoría ISP que poseen Números Autónomos y bloques de dirección IPv4, no pagarán el costo de mantenimiento de los primeros.

Transferencias*

Según lo dispuesto por el Directorio de LACNIC están libres de pago las transferencias de direcciones IP y ASN.

Antes de solicitar una transferencia, debe revisar las políticas de NIC México sobre transferencias de recursos, Punto 3.2.17 del documento Políticas de Direcciones IPv4.

Si un usuario final recibe un ASN, quedará sujeto al pago del mantenimiento de ese ASN según las tasas y condiciones antes expuestas.

Las direcciones IP transferidas a ISP se incluyen en la asignación total del ISP y luego se determina el tamaño del honorario a pagar.

*Los precios mencionados anteriormente pueden variar, siendo responsabilidad del usuario final o ISP verificar esta información al momento de su registro o renovación, según corresponda.

**La tarifa preferencial sólo es aplicable siempre que el cliente (ISP) no solicite factura previa al pago.

- Documentos , Sección de Formularios

5.52 Modelo de Contrato de Prestación de Servicios

Voy a mostrar un contrato de Prestación de Servicios entre NETWORK INFORMATION CENTER MÉXICO y un CLIENTE cualquiera

CONTRATO DE PRESTACIÓN DE SERVICIOS QUE CELEBRAN POR UNA PARTE NETWORK INFORMATION CENTER MÉXICO, S. C., REPRESENTADA EN ESTE ACTO POR EL ING. OSCAR ALEJANDRO ROBLES GARAY, (EN LO SUCESIVO "NIC MÉXICO") Y POR LA OTRA PARTE

REPRESENTADA POR (EN LO SUCESIVO "EL CLIENTE"), AL TENOR DE LAS SIGUIENTES DECLARACIONES Y CLÁUSULAS:

DECLARACIONES

PRIMERA.- Declara EL CLIENTE, por conducto de su representante legal:

a) Que es una organización constituida conforme a la legislación mexicana según lo hace constar con la Escritura Pública No. , de fecha de de , levantada ante la fe del Lic. . Notario Público No. con ejercicio en la ciudad de e inscrita en el Registro Público de la Propiedad y del Comercio de la ciudad de bajo el No. , Vol. , Libro , Sección de fecha de de .

b) Que su representante el , está debidamente facultado para celebrar en su nombre y representación el presente Contrato, como consta en la Escritura Pública No. de fecha de de levantada ante la fe del Lic. , Notario Público No. con ejercicio en la ciudad de e inscrita en el Registro Público de la Propiedad y del Comercio de la ciudad de bajo el No. , Vol. , Libro , Sección de fecha de de y que a la fecha no le han sido revocadas sus facultades.

SEGUNDA.- Declara NIC MÉXICO a través de su representante legal:

a) Que es una sociedad civil legalmente constituida conforme a las leyes mexicanas, cuyo objeto social consta en la Escritura Pública No. 23,730 de fecha el 2 de Octubre de 2002, otorgada ante la fe del Lic. Fernando Méndez Zorrilla, Notario Público 12 con ejercicio en la ciudad de Monterrey, N.L., México e inscrita en el Registro Público de la Propiedad y del Comercio de dicha ciudad bajo el número 1078, Vol. 41, Libro 22, Sección III, el 14 de Octubre de 2002.

b) Que su representante legal el Ing. Oscar Alejandro Robles Garay, se encuentra debidamente facultado para celebrar en su nombre y representación el presente Contrato, como consta en la Escritura Pública No. 23,730 de fecha el 2 de Octubre de 2002, otorgada ante la fe del Lic. Fernando Méndez Zorrilla, Notario Público 12 con ejercicio en la ciudad de Monterrey, N.L., México e inscrita en el Registro Público de la Propiedad y del Comercio de dicha ciudad bajo el número 1078, Vol. 41, Libro 22, Sección III, el 14 de Octubre de 2002, el cual se mantiene vigente a la firma del presente contrato, y que sus facultades no le han sido limitadas ni revocadas de ninguna manera.

DEFINICIONES

Para efectos del presente Contrato y sus ANEXOS y cualquier convenio o contrato derivado o relacionado con el mismo, las partes tendrán como definiciones las siguientes:

a) Internet: Red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación.
b) Internet Corporation for Assigned Names and Numbers (ICANN por sus siglas en inglés): Organización sin fines de lucro que opera a nivel internacional, responsable de asignar

CONTRATO DE PRESTACIÓN DE SERVICIOS QUE CELEBRAN POR UNA PARTE NETWORK INFORMATION CENTER MÉXICO, S. C., REPRESENTADA EN ESTE ACTO POR EL ING. OSCAR ALEJANDRO ROBLES GARAY, (EN LO SUCESIVO "NIC MÉXICO") Y POR LA OTRA PARTE , REPRESENTADA POR (EN LO SUCESIVO "EL CLIENTE"), AL TENOR DE LAS SIGUIENTES DECLARACIONES Y CLÁUSULAS:

DECLARACIONES

PRIMERA.- Declara EL CLIENTE, por conducto de su representante legal:

a) Que es una organización constituida conforme a la legislación mexicana según lo hace constar con la Escritura Pública No. , de fecha de de , levantada ante la fe del Lic. , Notario Público No. con ejercicio en la ciudad de e inscrita en el Registro Público de la Propiedad y del Comercio de la ciudad de bajo el No. , Vol. , Libro , Sección de fecha de de .

b) Que su representante el , está debidamente facultado para celebrar en su nombre y representación el presente Contrato, como consta en la Escritura Pública No. de fecha de de levantada ante la fe del Lic. , Notario Público No. con ejercicio en la ciudad de e inscrita en el Registro Público de la Propiedad y del Comercio de la ciudad de bajo el No. , Vol. , Libro , Sección de fecha de de y que a la fecha no le han sido revocadas sus facultades.

SEGUNDA.- Declara NIC MÉXICO a través de su representante legal:

a) Que es una sociedad civil legalmente constituida conforme a las leyes mexicanas, cuyo objeto social consta en la Escritura Pública No. 23,730 de fecha el 2 de Octubre de 2002, otorgada ante la fe del Lic. Fernando Méndez Zorrilla, Notario Público 12 con ejercicio en la ciudad de Monterrey, N.L., México e inscrita en el Registro Público de la Propiedad y del Comercio de dicha ciudad bajo el número 1078, Vol. 41, Libro 22, Sección III, el 14 de Octubre de 2002.

b) Que su representante legal el Ing. Oscar Alejandro Robles Garay, se encuentra debidamente facultado para celebrar en su nombre y representación el presente Contrato, como consta en la Escritura Pública No. 23,730 de fecha el 2 de Octubre de 2002, otorgada ante la fe del Lic. Fernando Méndez Zorrilla, Notario Público 12 con ejercicio en la ciudad de Monterrey, N.L., México e inscrita en el Registro Público de la Propiedad y del Comercio de dicha ciudad bajo el número 1078, Vol. 41, Libro 22, Sección III, el 14 de Octubre de 2002, el cual se mantiene vigente a la firma del presente contrato, y que sus facultades no le han sido limitadas ni revocadas de ninguna manera.

DEFINICIONES

Para efectos del presente Contrato y sus ANEXOS y cualquier convenio o contrato derivado o relacionado con el mismo, las partes tendrán como definiciones las siguientes:

a) Internet: Red informática mundial, descentralizada, formada por la conexión directa entre computadoras u ordenadores mediante un protocolo especial de comunicación.
b) Internet Corporation for Assigned Names and Numbers (ICANN por sus siglas en inglés): Organización sin fines de lucro que opera a nivel internacional, responsable de asignar

Espacio de Direcciones IP, identificadores de protocolo y de las funciones de gestión [o administración] del sistema de nombres de dominio de primer nivel genéricos (gTLD) y de códigos de países (ccTLD), así como de la administración del sistema de servidores raíz.

c) Internet Assigned Numbers Authority (IANA por sus siglas en ingles): Organización responsable de preservar las funciones de coordinación centrales del Internet global.
d) Country Code Top-Level Domain (ccTLD por sus siglas en inglés): Es el código territorial de dos letras, según la lista ISO-3166-1, dentro del Sistema de Nombres de Dominio supervisado por ICANN e IANA.
e) Días: A menos que se especifique lo contrario, se refiere a dias naturales. En caso de que un plazo termine en día inhábil, el mismo se entenderá prorrogado hasta el siguiente día hábil.
f) IPv4: Protocolo de Internet versión 4.
g) IPv6: Protocolo de Internet versión 6.
h) Bloque IP o Bloques de Direcciones IP o Espacio de Direcciones IP: Conjunto de tamaño variable de direcciones IPv4 o IPv6.
i) Autonomous System Number (Número de Sistema Autónomo, ASN por sus siglas en inglés): Número único que identifica a un conjunto de redes de direcciones IP que son administradas por un grupo de uno o más operadores de red.
j) Servicios de Internet: Son aquellos servicios que permiten al usuario tener cualquier forma de acceso a Internet, se pueden mencionar de forma enunciativa mas no limitativa, los siguientes: proveer a clientes de conexión a Internet a través de cualquier medio de transmisión de datos, alojamiento de sitios de Internet y alojamiento de correo electrónico.
k) Proveedor de Servicios de Internet (ISP por sus siglas en inglés): Un ISP coloca principalmente Espacio de Direcciones IP a los Usuarios Finales de los Servicios de Internet que éste provee. Sus clientes pueden ser otros ISP.
l) Usuario Final (UF): Como Usuarios Finales se considerarán aquellas organizaciones que soliciten direcciones IP para su uso interno en el funcionamiento de sus propias redes. Dichas organizaciones no proporcionarán Servicios de Internet a otras personas físicas o morales.
m) Latinamerican and Caribbean Internet Address Registry (LACNIC por sus siglas en inglés): Organización responsable del Registro Regional de Direcciones IP para América Latina y Caribe.
n) SERVICIO: Todo servicio ofrecido por NIC MÉXICO relacionado con los Recursos de Internet, direcciones y Bloques IP y ASN. Dichos servicios pueden incluir, pero no están limitados a: registro de Espacio de Direcciones IP, registro de Números de Sistemas Autónomos (ASN), Resolución Inversa de los Bloques de Direcciones IP registrados, mantenimiento de la información de los Recursos registrados y la administración del Espacio de Direcciones IP, tal y como se definen en el ANEXO B del presente Contrato.
o) Fecha de aniversario: el dia y mes de cada año que coincide con el día y mes de la fecha de registro del primer Bloque IP o ASN de EL CLIENTE.
p) Recursos y/o Recursos de Internet: Bloques IP y/o ASN.
q) Request for Comments (RFC por sus siglas en inglés): Un RFC es un documento estándar que describe protocolos, sistemas o procedimientos utilizados por la comunidad de Internet. Para consultar un RFC específico, revisar la referencia http://www.ietf.org/rfc.html.
r) HD-Ratio: El HD Ratio es un modo de medir la eficiencia de asignación de direcciones IPv6, según el RFC 3194.
s) Local Internet Registry (LIR por sus siglas en inglés): Un LIR es una organización responsable de la distribución de Espacios de Direcciones IP a sus miembros o clientes y del registro de esa distribución. Un LIR asigna, principalmente, Espacios de Direcciones IP a los usuarios de los servicios de red que éste provee. Los LIR son generalmente ISP, cuyos clientes son principalmente Usuarios Finales y posiblemente otros ISP.
t) Organización single-homed: Una organización que recibe conectividad a Internet a través de un solo Proveedor de Servicios de Internet.
u) Organización multi-homed: Un ISP es multi-homed si recibe conectividad a Internet de tiempo completo a través de más de un Proveedor de Servicios de Internet.

v) Recursos legados: Son considerados Recursos legados aquellos registrados antes del surgimiento de los Registros de Internet Regionales. Cualquier recurso Internet (Bloque IP, ASN) con fecha de asignación anterior al 28 de diciembre de 1997 es considerado legado.
w) Resolución Inversa: Proceso de conversión de la dirección IP registrada para una computadora, al nombre correspondiente registrado para la misma.
x) Transferencia de zona: Transferencia de la información referente a los nombres de las computadoras y sus relaciones con las direcciones IP.
y) Protocolo AXFR: Protocolo que define un mecanismo para replicar o transferir datos relacionados con los nombres de las computadoras y sus direcciones IP asignados.
z) WHOIS: Base de datos en la cual se encuentra registrada la información relacionada con los Recursos en LACNIC de Bloques IP, ASN, entidades que cuentan con registros de Espacio de Direcciones IP, y contactos administrativos para los Recursos antes mencionados.

Los términos definidos en esta sección podrán ser utilizados en el presente Contrato tanto en singular como en plural.

Todos los encabezados utilizados en el presente Contrato se utilizan exclusivamente para facilitar su lectura, mas no se tomarán en cuenta en la interpretación del mismo. Salvo disposición en contrario, todas las referencias en el presente Contrato a CLÁUSULAS o ANEXOS, se hacen a las CLÁUSULAS y ANEXOS de este Contrato.

En virtud de las declaraciones y definiciones anteriores, las partes, de común acuerdo se someten a las disposiciones contenidas en las siguientes:

CLÁUSULAS

CLÁUSULA PRIMERA. OBJETO: Por medio del presente contrato de prestación de servicios (en adelante "Contrato"), sus ANEXOS y los convenios que se deriven del primero, NIC MÉXICO prestará el SERVICIO a los Recursos legados y en su caso adicionalmente a los Recursos mencionados en el ANEXO E, a solicitud de EL CLIENTE conforme a lo establecido en el presente instrumento, según se detalla en el siguiente sitio de Internet http://www.nic.mx/es/IP.Servicios y se menciona en ANEXO B.

CLÁUSULA SEGUNDA. VIGENCIA: Las partes acuerdan que el efecto de este Contrato dará inicio una vez que sea firmado por ambas partes y tendrá una vigencia de dos años a partir de la firma del mismo. Las partes de común acuerdo podrán extender la vigencia del presente Contrato. Esta extensión de la vigencia deberá manifestarse por escrito al menos un mes antes de la terminación del presente Contrato.

CLÁUSULA TERCERA. SERVICIO: Las partes acuerdan que los procedimientos para tener acceso al SERVICIO que proporcionará NIC MÉXICO se regirá por lo establecido en el sitio de Internet de NIC MÉXICO (www.nic.mx) en lo que corresponda al presente Contrato y sus ANEXOS, las Políticas de administración de Recursos de Internet en el área de Latinoamérica y el Caribe publicadas en la siguiente dirección electrónica http://www.nic.mx/es/IP.Politicas y lo establecido en el ANEXO B.

Dichas políticas y procedimientos son publicados por NIC MÉXICO (http://www.nic.mx/es/IP.Politicas), y podrán ser modificados, alterados, eliminados en cualquier tiempo conforme a los procedimientos establecidos por LACNIC y los acuerdos entre éste último con NIC MÉXICO, por lo que EL CLIENTE declara que conoce dichas políticas y procedimientos y que se mantendrá actualizado con relación a los cambios que puedan aplicarse.

CLÁUSULA CUARTA. OBLIGACIONES DE EL CLIENTE: En virtud del objeto del presente Contrato y del desarrollo del mismo, EL CLIENTE se obliga expresamente a:

a) Cubrir las cuotas establecidas por las operaciones realizadas, conforme a las especificaciones establecidas en el ANEXO A.

b) Cumplir con las Políticas, lineamientos sobre los Bloques IP y ASN publicados en el siguiente sitio de Internet (http://www.nic.mx/es/IP.Politicas), el sitio de Internet http://www.nic.mx/es/IP.Servicios y lo mencionado de forma enunciativa mas no limitativa en el ANEXO B del presente.

c) Mantener actualizada la información solicitada por NIC MÉXICO sobre los titulares de los Bloques IP en el WHOIS de LACNIC en el sitio de Internet de LACNIC en la sección de Servicios de Registro.

d) Brindar la información verídica requerida en el llenado de los formularios señalados en el siguiente sitio de Internet: http://www.nic.mx/es/IP.Template_IPs, y mencionados de forma enunciativa mas no limitativa en el ANEXO C del presente instrumento.

e) Cumplir con lo establecido con la Membresía en LACNIC conforme a lo señalado en el ANEXO D;

f) Cumplir con todas y cada una de las obligaciones señaladas en el presente Contrato.

CLÁUSULA QUINTA. OBLIGACIONES DE NIC MÉXICO: En virtud del presente Contrato, **NIC MÉXICO** se obliga expresamente a:

a) Prestar el SERVICIO conforme a lo especificado en el ANEXO B.

b) Mantener actualizada en el sitio de Internet, las Políticas de administración de Recursos de Internet en el área de Latinoamérica y el Caribe (http://www.nic.mx/es/IP.Politicas).

c) Mantener el funcionamiento de los Recursos de Internet registrados ante NIC MÉXICO en la medida de lo posible.

d) Brindar el soporte técnico para el SERVICIO conforme a lo que se señala en el ANEXO B;

e) Cumplir con lo establecido con la Membresía en LACNIC conforme a lo señalado en el ANEXO D.

CLÁUSULA SEXTA. RESPONSABILIDAD PATRONAL.- Las partes acuerdan que este Contrato no podrá interpretarse de manera alguna como constitutivo de cualquier tipo de asociación o vínculo de carácter laboral entre las partes; por lo que las relaciones laborales se mantendrán en todos los casos entre la parte contratante y sus respectivos trabajadores, aun en los casos de los trabajos realizados conjuntamente y que se desarrollen en las instalaciones o con equipo de cualquiera de las partes. En ningún caso podrá considerarse a la otra parte como patrón sustituto, quedando fuera de toda responsabilidad en asuntos relacionados con dicho personal, debiendo la parte que contrató al trabajador de que se trate, liberar de toda responsabilidad a la otra en caso de conflictos laborales provocados por personal de la otra.

CLÁUSULA SÉPTIMA. CONFIDENCIALIDAD.- Ambas partes se obligan a adoptar las medidas necesarias y procedentes a efectos de exigir a su personal la máxima discreción y secreto profesional con respecto a cualquier información propia de EL CLIENTE o de NIC MÉXICO sobre la que lleguen a tener acceso con motivo del presente Contrato. Asimismo, se comprometen a no publicar o divulgar ningún dato salvo que se cuente con el permiso escrito de la contraparte.

Toda información propietaria documental transferida de una de las partes a la otra en consecuencia del Contrato y que se desee amparar bajo la protección de confidencialidad, deberá identificarse por la parte que transmite como tal, por medio de un sello o marca en el documento transferido. La parte receptora mantendrá tal información propietaria en confidencia durante el periodo de la vigencia del contrato y por espacio de cinco años posteriores a la terminación normal, extendida o anticipada. Durante dicho periodo, la parte receptora usará tal información sólo con relación a sus responsabilidades bajo el Contrato y a cualquier otro convenio o contrato que emane en relación al o del Contrato y sólo lo hará

disponible a sus empleados y otro personal que tenga necesidad de saber para efectuar sus funciones respecto a las responsabilidades bajo el Contrato.

Las obligaciones de confidencialidad asumidas por las partes bajo este Contrato se aplicarán, salvo que:

a. La información se haya hecho del dominio público sin que medie culpa o acción de la parte receptora.
b. Se tenía conocimiento de dicha información antes de que le fuera revelada.
c. La información ha sido revelada por algún tercero con posesión legal de dicha información, siempre y cuando dicha revelación no resulte en una violación o incumplimiento a una obligación contractual o legal por parte de dicho tercero.
d. Ha sido requerida por alguna autoridad administrativa o jurisdiccional, en el entendido de que dicha parte estará obligada a notificar por escrito a la otra parte de dicho requerimiento, dentro de lo posible, con anterioridad a la entrega de la información propietaria a dichas autoridades de manera que permita el ejercicio de las acciones o recursos legales que procedan.

CLÁUSULA OCTAVA. RESPONSABILIDAD DE LAS PARTES.- La falta del cumplimiento por alguna de las partes de cualquiera de sus obligaciones en virtud del presente Contrato, no se considerará como violación del mismo cuando dicho incumplimiento se deba a alguna causa imputable a la otra parte.

CLÁUSULA NOVENA.- PROPIEDAD INTELECTUAL.- EL CLIENTE y NIC MÉXICO convienen que el presente Contrato no otorga licencia alguna, o algún tipo de derecho respecto de la "Propiedad Intelectual" de cualquiera de las partes. Para efectos del Contrato, "Propiedad Intelectual" incluye todos los signos distintivos registrados y/o usados en México o en el extranjero por cualquiera de las partes, así como todo derecho sobre información confidencial, nombres comerciales, avisos comerciales, reservas de derechos, nombres de dominio, así como todo tipo de derechos patrimoniales sobre obras y creaciones protegidas por derechos de autor y demás formas de propiedad industrial o intelectual reconocida o que lleguen a reconocer las leyes correspondientes. Las partes se obligan a no usar, comercializar, revelar a terceros, distribuir, regalar, o de cualquier otro modo disponer de de la Propiedad Intelectual de la otra parte, ni de cualquier material que sea resultado de la Propiedad Intelectual de la otra parte, salvo en los términos pactados en el presente Contrato.

Queda estrictamente prohibido para las partes, y para su personal en su caso, reproducir sin autorización previa y por escrito de la otra parte, cualquier tipo de material que éste último le hubiese proporcionado o desarrollado al amparo del presente Contrato, bajo pena de incurrir en alguna de las sanciones establecidas en las leyes aplicables, además de la rescisión al presente Contrato.

CLAUSULA DÉCIMA. TERMINACIÓN.- El presente Contrato podrá darse por terminado anticipadamente por cualquiera de las partes, sin que medie resolución judicial alguna, siempre y cuando se dé aviso por escrito con 30 (treinta) Días de anticipación a la fecha en que dejará de surtir efectos el presente Contrato, procediendo de inmediato a la determinación de las obligaciones pendientes de cumplir por cada una de las partes.

Al finalizar el plazo mencionado **NIC MÉXICO** llevará a cabo la revocación automática de los Recursos legados o Recursos y **EL CLIENTE** se obliga a no utilizar, ni permitir o autorizar a terceros el uso de Recursos Legados o Recursos y dejar de anunciar los Bloques de IP en redes privadas, públicas y base de datos de ruteo, una vez transcurrido el plazo de 30 (treinta) Días señalado en la presente CLÁUSULA y se compromete a liberar los mismos para que se encuentren disponibles.

CLÁUSULA DÉCIMA PRIMERA. LIMITACIÓN DE RESPONSABILIDAD.- EL CLIENTE se obliga a defender, liberar y sacar en paz y a salvo de toda responsabilidad a **NIC MÉXICO**, derivada de cualquier reclamación, demanda, querella, juicio, controversia, o cualquier otro sin importar su naturaleza, que se inicie por cualquier tercero o autoridad competente como consecuencia de las actividades amparadas en el presente Contrato, así como con los

derechos y obligaciones contenidas en el mismo a cargo de EL CLIENTE, incluyendo cualquier investigación o auditoría o controversia que se inicie por alguna autoridad. Así mismo, EL CLIENTE deberá pagar a NIC MÉXICO, todos los gastos, cargos, multas, honorarios de abogados que NIC MÉXICO designe para su defensa o cualquier otro concepto aplicable de acuerdo a lo señalado en la presente CLÁUSULA.

CLAUSULA DÉCIMA SEGUNDA. NOTIFICACIONES. Toda notificación efectuada conforme a este Contrato a las partes se hará por escrito, a las direcciones que se indican enseguida, a menos que el destinatario haya notificado un cambio de dirección por escrito. Toda notificación requerida por este Contrato, se considerará que ha sido debidamente efectuada cuando se envíe físicamente por mensajería certificada y haya acuse de recibo. Lo anterior a excepción de la notificación por pago señalada en la CLÁUSULA DÉCIMO QUINTA, inciso b) la cual podrá realizarse a través de correo electrónico.

Toda notificación se hará única y exclusivamente de acuerdo a la información proporcionada que se menciona a continuación a menos que el destinatario haya notificado el cambio de dirección por escrito.

NIC MÉXICO, dirigida a:

Director General
Atención: Ing. Oscar Alejandro Robles Garay
NETWORK INFORMATION CENTER MÉXICO, S.C.
Av. Eugenio Garza Sada Sur No. 427, Pabellón TEC, Locales 4, 5 y 6
Colonia Alta Vista
Monterrey, Nuevo León, México
C.P. 64840
Teléfono y Fax: +52 (81) 83875346
Correo electrónico orobles@nic.mx

EL CLIENTE, dirigida a:
Puesto:
Atención:
Dirección (Calle y Número):
Colonia:
C. P.:
Ciudad y Estado:
Teléfono y Fax:
Correo electrónico:

CLÁUSULA DÉCIMA TERCERA. COORDINADORES.- Las partes acuerdan que para llevar a cabo el presente Contrato se nombrará un coordinador para cada una de las partes.

Por parte de NIC MÉXICO se nombra a:
Ing. Cristóbal Chapital Tirado
Tel: 01 (81) 83875346 ext. 104
Correo electrónico: chapital@nic.mx

Por parte de EL CLIENTE se nombra a:
Nombre:
Teléfono:
Correo electrónico:

Cualquier cambio en los coordinadores deberá ser notificado por escrito conforme a la CLÁUSULA anterior.

Toda la información, datos o especificaciones amparados bajo el presente Contrato, que no se mencionen en el mismo, deberán ser brindados por los coordinadores según corresponda.

Cualquier dato o información señalada por dichos coordinadores se entenderá que es hecha en nombre de la parte firmante de este Contrato según corresponda.

CLÁUSULA DÉCIMA CUARTA. TOTALIDAD DEL ACUERDO. El presente Contrato (incluyendo sus ANEXOS) constituye la totalidad del acuerdo de las partes del presente, con relación a los asuntos cubiertos por este Contrato y substituye a todos los convenios anteriores, arreglos, negociaciones y discusiones de carácter verbal o escrito, entre las partes y con respecto a dichos asuntos. En caso de conflicto entre las disposiciones del cuerpo de este Contrato y cualquier disposición en los ANEXOS, tendrán precedencia las disposiciones del cuerpo del Contrato.

CLAUSULA DÉCIMA QUINTA. RESCISIÓN. Cualquiera de las partes podrá rescindir el presente Contrato en cualquier tiempo, sin incurrir en responsabilidad ulterior alguna, en cualquiera de los siguientes casos:

a. Por incumplimiento de la otra parte a cualquiera de las disposiciones establecidas en el presente Contrato, las políticas de Bloques IP y Números de Sistema Autónomo (http://www.nic.mx/es/IP.Politicas), las Políticas Generales de Nombres de Dominio, Políticas de Resolución de Controversias, el Reglamento de las Políticas de Resolución de Controversias y/o con lo establecido en el sitio de Internet (www.nic.mx), así como cualquier otra información que sea entregada a **EL CLIENTE** por **NIC MÉXICO**;
b. Cuando **EL CLIENTE** no haya hecho el pago de cualquier cantidad de conformidad con el presente Contrato dentro de los 30 (treinta) Días siguientes a la Fecha de aniversario de los Recursos que tengan registrados;
c. En caso de que cualquiera de las partes sea declarada en concurso mercantil o quiebra o reconozca expresamente su incapacidad general para cumplir con sus obligaciones de pago.
d. **Cuando EL CLIENTE**, no notifique a **NIC MÉXICO** de la transferencia de Recursos, así como la falta de entrega de la documentación que **NIC MÉXICO** solicite a **EL CLIENTE**, la cual compruebe la operación de compra y venta de la organización, fusión, reestructuración, o cambio de razón social de la misma (Copia autenticada del documento que compruebe la transferencia de los bienes entre las organizaciones. Por ejemplo, nota de venta, certificado de fusión, contrato, etcétera; un inventario detallado de los bienes que utilizan los recursos involucrados en la transferencia; una lista de clientes que usan parte de las direcciones IP de la organización que solicita la transferencia; una lista de los bienes adquiridos; una descripción de los bienes adquiridos, incluyendo tipo y cantidad de equipamiento y clientes; una descripción de cómo serán utilizadas las direcciones IP; una topología de la red, incluyendo número de máquinas, máscara de red, diagrama de red y designaciones hechas para clientes; entre otros).

En el caso de que alguna de las partes contratantes notifique la rescisión a la contraparte en los términos del párrafo anterior, esta última cuenta con un plazo de 5 (cinco) días hábiles contados a partir de la fecha en que reciba la notificación, para exponer lo que a su derecho convenga, respecto de la causal que motive la rescisión o el incumplimiento de sus obligaciones; si transcurrido dicho plazo la parte no manifiesta nada en su defensa, o si después de analizar las razones aducidas por ésta, la parte afectada estima que las mismas no son satisfactorias, surtirá sus efectos plenamente la rescisión.

Al finalizar el plazo mencionado **NIC MÉXICO** llevará a cabo la revocación automática de los Recursos legados o Recursos y **EL CLIENTE** se obliga a no utilizar, ni permitir o autorizar a terceros el uso de Recursos Legados o Recursos y dejar de anunciar los Bloques de IP en redes privadas, públicas y base de datos de ruteo, y se compromete a liberar los mismos para que se encuentren disponibles. En caso de que **EL CLIENTE** incumpla con las disposiciones establecidas en la presente CLÁUSULA, las partes acuerdan que el representante legal de **EL CLIENTE** se designara de forma automática como depositario judicial de los Recursos legales y Recursos, asimismo que aplicarán las disposiciones de la CLÁUSULA DÉCIMA SÉPTIMA.

CLAUSULA DÉCIMA SEXTA. MODIFICACIONES. Cualquier modificación, adición o aclaración a los términos del presente Contrato deberá ser realizada por escrito, debidamente firmada de conformidad por el representante legal de cada una de las partes, empezando a surtir efectos a partir de la fecha de su firma, salvo estipulación en contrario.

CLAUSULA DÉCIMA SÉPTIMA. PENA CONVENCIONAL. Las partes acuerdan, y EL CLIENTE se obliga expresamente a pagar a NIC MÉXICO, en los términos de los artículos 1737, 1739,1743, 2012 y demás aplicables del Código Civil para el Estado de Nuevo León, México, por concepto de pena convencional por falta de cumplimiento a cualquiera de las obligaciones a cargo de EL CLIENTE señaladas en el presente Contrato, un monto equivalente al monto total de sumar todas las cuotas pagadas por EL CLIENTE a NIC MÉXICO por la prestación de los SERVICIOS de todos los Recursos legados o Recursos objeto del presente Contrato, más los gastos y costas que se generen para NIC MÉXICO en caso de que esta última se vea obligada a demandar a EL CLIENTE para recuperar dicha pena convencional por cualquier concepto, monto que será pagadero y exigible a más tardar dentro de los 3 (tres) días hábiles siguientes a la fecha en que lleve a cabo la revocación automática de los Recursos legados o Recursos a que se refiere la CLÁUSULA DÉCIMO QUINTA del presente Contrato.

Para efectos de la presente CLÁUSULA DÉCIMA SÉPTIMA, EL CLIENTE conviene en que para la determinación de la pena convencional aquí prevista, equivalente al monto total de sumar todas las cuotas pagadas por EL CLIENTE a NIC MÉXICO por la prestación de los SERVICIOS bajo el presente Contrato, bastará la certificación que para tal efecto realice el contador de NIC MÉXICO.

CLAUSULA DÉCIMA OCTAVA. JURISDICCIÓN Y LEGISLACIÓN APLICABLE. Ambas partes se someten expresamente al fuero de los Tribunales competentes del Primer Distrito Judicial del Estado de Nuevo León, con residencia en la ciudad de Monterrey; y a las leyes, reglamentos y demás disposiciones legales vigentes en dicho Estado, para la solución de cualquier controversia que surja con motivo de la interpretación y/o ejecución de lo convenido en el presente documento, renunciando expresamente a cualquier fuero que por razón de su domicilio presente o futuro, o por cualquier otra causa, pudiera corresponderles.

En señal de conformidad, las partes firman el presente Contrato que consta de 27 hojas útiles sólo por su lado anverso en dos ejemplares de igual tenor, en el lugar y fecha declarados en la comparecencia.

Leído este Contrato por las partes, lo ratifican y firman en la ciudad de Monterrey, N.L., el día de de ; elaborándose este instrumento por duplicado para quedar un tanto con cada una de las partes.

NETWORK INFORMATION CENTER MÉXICO, S. C.

Ing. Oscar Alejandro Robles Garay	Nombre:
Director General	Puesto:
Fecha: de de	Fecha: de de

TESTIGOS

Ing. Cristóbal Chapital Tirado	Nombre:
Ave. Eugenio Garza Sada No. 427 Col Altavista	Dirección:
Monterrey, N. L.	
Tel: (81) 8387-5346	Tel:

ANEXO A

DEL CONTRATO DE PRESTACIÓN DE SERVICIOS CELEBRADO ENTRE NETWORK INFORMATION CENTER MÉXICO, S.C. (en lo sucesivo "NIC MÉXICO") Y

(en lo sucesivo "EL CLIENTE"), EL DIA DE DE EN LA CIUDAD DE MONTERREY, NUEVO LEÓN.

TARIFAS DE RECURSOS.

A continuación se encuentra el detalle de las cuotas y categorías actuales por Recursos legados y Recursos (en adelante Recursos).

Bloques IP.

Las cuotas por el registro o renovación de los Bloques IP se regirán conforme a lo siguiente:

- Para obtener el registro inicial de un Bloque IP, es necesario que la solicitud haya sido previamente aceptada por NIC MÉXICO y haber realizado el pago de la cuota inicial señalada en el presente ANEXO.
- Posteriormente, una vez al año y en la Fecha de aniversario del registro, para mantener el Bloque IP registrado EL CLIENTE deberá cubrir la cuota de renovación señalada en el presente ANEXO.

Al solicitar el registro de Recursos, se entiende que EL CLIENTE, conoce expresamente las cuotas y categorías asociadas con los mismos.
Las cuotas y categorías estarán en vigor desde la fecha de la firma del presente; sin embargo, es obligación y responsabilidad de EL CLIENTE verificar las cuotas y las categorías actualizadas en el sitio de Internet http://www.nic.mx/es/IP.Pagos.

Las cuotas señaladas están relacionadas directamente con lo acordado en la Asamblea de LACNIC, de la cual EL CLIENTE forma parte.

IPv4

ISP			
Categoria	Tamaño	Cuota Inicial (Dólares Americanos)	Cuota de Renovación (Dólares Americanos)
Small/Micro	/24 - /20	$1,000	$1,000
Small	>/20 - /19	$2,000	$2,000
Medium	>/19 - /16	$5,000	$5,000
Large	>/16 - /14	$10,500	$10,500
Extra Large	>/14 - /11	$22,000	$22,000
Mayor	>/11	$33,000	$33,000

Usuarios Finales			
Categoría	Tamaño	Cuota inicial USD, por evento. (Dólares Americanos)	Cuota de Renovación (Dólares Americanos)
Small	/24 - /19	$2,500	$400
Medium	/18	$5,000	$400
Large	/17	$7,500	$400
Extra Large	/16	$10,000 cada /16	$400

El tamaño de los Bloques IPv4 en los cuadros anteriormente mencionados se define por la siguiente tabla de conversiones:

Tabla de equivalencias (prefijos-direcciones IP)

Tamaño del Bloque IPv4 (prefijo)	Número de /24's	Número de direcciones IP
/24	1	256
/23	2	512
/22	4	1024
/21	8	2048
/20	16	4,096
/19	32	8,192
/18	64	16,384
/17	128	32,768
/16	256	65,536
/15	512	131,072
/14	1,024	262,144
/13	2,048	524,288
/12	4,096	1,048,576
/11	8,192	2,097,152

IPv6.

Las organizaciones que califiquen para recibir Bloques de Direcciones IPv6, estarán exoneradas de pagar el pago inicial y la primera renovación.

ISP		
Tamaño	Cuota inicial (Dólares Americanos)	Cuota de Renovación (Dólares Americanos)
/32*	$2,500	$2,500
>/32	$20,000	$20,000

ASN.

Las cuotas por el registro o renovación de los números ASN se regirán conforme a lo siguiente:

- Para obtener el registro de un ASN, es necesario haber realizado el pago a NIC MÉXICO de la cuota inicial señalada en el presente ANEXO.
- Para mantener el ASN registrado EL CLIENTE deberá cubrir la cuota de renovación referente al ASN señalada en el presente ANEXO.

- La cuota inicial de un ASN es de USD $500.00 (quinientos dólares Moneda de los Estados Unidos de Americanos).
- La cuota de renovación es de USD $50.00 (cincuenta dólares, Moneda de los Estados Unidos de América) y se cobra por adelantado cada 3 años.

A continuación se encuentra el detalle de las cuotas por ASN, los cuales estarán en vigor desde la fecha de la firma del presente; sin embargo, es obligación y responsabilidad de EL CLIENTE verificar las cuotas actualizadas en el sitio de Internet http://www.nic.mx/es/IP.Pagos.

Cuota Inicial (Dólares Americanos)	Monto Anual de Mantenimiento (Dólares Americanos)
$500	$50

TRANSFERENCIAS.

Las transferencias de Recursos se regirán conforme a lo siguiente:

- Según lo dispuesto por el Directorio de LACNIC, por el momento están libres de pago las transferencias de direcciones IP y ASN.
- SI un UF recibe un ASN, quedará sujeto al pago del mantenimiento de ese ASN según las tasas y condiciones antes expuestas.
- Los Bloques IP transferidos a ISP se incluyen en el registro total del ISP y luego se determina el tamaño del honorario a pagar.
- EL CLIENTE o el Usuario Final, antes de solicitar una transferencia de cualquier Recurso de Internet, deberá revisar las políticas de LACNIC sobre transferencia de Recursos (Bloque IP y/o ASN). Punto 3.2.17 del documento de Políticas, http://www.nic.mx/es/IP.Politicas.

DEVOLUCIONES.

La devolución de Recursos se regirá conforme a lo siguiente:

- Por el momento están libres de pago las devoluciones de direcciones IP y ASN.
- EL CLIENTE o el Usuario Final, antes de solicitar la devolución de Recursos deberá comunicar solicitar las formas correspondientes y deberá obligarse a no utilizar, ni permitir o autorizar a terceros el uso de Recursos Legados o Recursos y dejar de anunciar los Bloques IP en redes privadas, públicas y base de datos de ruteo, y liberar los mismos para que se encuentren disponibles.

NETWORK INFORMATION CENTER MÉXICO, S. C.

Ing. Oscar Alejandro Robles Garay	Nombre:
Director General	Puesto:
Fecha: de de	Fecha: de de

TESTIGOS

Ing. Cristóbal Chapital Tirado	Nombre:
Ave. Eugenio Garza Sada No. 427 Col Altavista	Dirección:
Monterrey, N. L.	
Tel: (81) 8387-5346	Tel:

ANEXO B

DEL CONTRATO DE PRESTACIÓN DE SERVICIOS CELEBRADO ENTRE NETWORK INFORMATION CENTER MÉXICO, S.C. (en lo sucesivo **"NIC MÉXICO"**) Y

(en lo sucesivo "EL CLIENTE"), EL DIA DE DE EN LA CIUDAD DE MONTERREY, NUEVO LEÓN.

DESCRIPCIÓN DEL SERVICIO.

El presente ANEXO contiene una descripción enunciativa mas no limitativa de los SERVICIOS ofrecidos por NIC MÉXICO a EL CLIENTE, dichos SERVICIOS deberán ser revisados por EL CLIENTE en el siguiente sitio de Internet: http://www.nic.mx/es/IP.Servicios. La descripción es la siguiente:

I. Bloques IP.

a) Políticas de Uso.

1. Administración de Espacio de Direcciones IP (Funciones de NIC MÉXICO y de LACNIC) Los SERVICIOS de NIC MÉXICO incluyen: el registro, administración, transferencia y revocación de Bloques IP y Números de Sistemas Autónomos (ASN); Resolución Inversa de los Bloques IP registrados, mantenimiento de la información proporcionada con los Bloques IP y Número de Sistemas Autónomos.

   Los SERVICIOS de direcciones IP que ofrece NIC MÉXICO se basa en las Políticas de Administración de Recursos de LACNIC señaladas en el siguiente sitio de Internet http://www.nic.mx/es/IP_Politicas.

2. Procedimiento para el registro (requisitos formales y técnicos)

   2.1 Bloques IPv4.

   El procedimiento general para solicitar un Bloque de Direcciones IP es como sigue:

   i. EL CLIENTE debe llenar el formulario indicado y enviarlo después a ipmaster@nic.mx.
   ii. Una vez aprobada la solicitud de registro inicial, un correo electrónico será enviado con información sobre el pago y Contrato a celebrar. El registro solamente será hecho después de la recepción del Contrato firmado por EL CLIENTE y, posteriormente, a la recepción del pago.

   EL CLIENTE se debe comprometer a devolver el Bloque IP anteriormente en uso al Proveedor de Servicios de Internet cuando vaya a recibir un Bloque IP de NIC MÉXICO.

   Al solicitar Bloques IP adicionales, se entiende que EL CLIENTE tiene pleno conocimiento de que existe una tarifa asociada al mantenimiento del registro de los Recursos registrados por NIC MÉXICO conforme al ANEXO A.

   2.1.1. Requisitos para ISP.

   El tamaño mínimo de asignación inicial aplicado a ISP es de un /21 y para calificar para un registro inicial, la organización debe:

   i. Si solicita un Bloque IP /21:
      - Demostrar el uso o la necesidad inmediata de un /23.
      - Entregar un plan detallado de uso de un /22 a un año.

ii. Si solicita un Bloque IP /20 o mayor:
- Organización single-homed: Demostrar la utilización eficiente de un Bloque IP prefijo /21 o más corto registrado por el actual proveedor de acceso a Internet. Ese Bloque IP no precisa ser contiguo.
- Organización multi-homed: Demostrar la utilización eficiente de un prefijo /22 o más corto registrado por el actual proveedor de acceso a Internet y tener más de una conexión independiente a Internet, el Bloque IP no precisa ser contiguo.

2.1.2. Requisitos para UF.

De acuerdo a la actual política de LACNIC el menor prefijo a ser adjudicado por NIC MÉXICO es un /20 (16 Bloques IP/24). En el caso de Usuarios Finales multi-homed el prefijo más pequeño será un /24. Corresponde a NIC MÉXICO determinar el prefijo apropiado en cada proceso de solicitud tomando en consideración la necesidad justificada y la tasa de utilización. EL CLIENTE debe:

i. Demostrar la utilización eficiente de un Bloque IP prefijo /21 o más corto colocado por el actual proveedor de acceso a Internet. Ese Bloque IP no precisa ser contiguo, o
ii. Demostrar la utilización eficiente de un prefijo /25 o más corto (Bloque IP mayor) colocado por el actual proveedor de acceso a Internet y tener más de una conexión independiente a Internet (multi-homed site).

La tasa utilización de las direcciones es utilizada para determinar el tamaño del prefijo que será colocado. Las tasas que serán consideradas:
- Una tasa de 25% de utilización inmediata
- 50% de utilización en un año.

2.2 Bloques IPv6.

Para solicitar un bloque IPv6 EL CLIENTE debe llenar el formulario indicado y enviarlo después para ipmaster@nic.mx.

Una vez aprobada la solicitud de registro inicial, un correo electrónico será enviado con información sobre el pago y sobre el Contrato que debe ser firmado. El registro solamente será hecho después de la recepción del pago y de la firma del Contrato.

Solicitudes de registro adicional solamente serán procesadas o completadas en los casos que no haya pago o documentación pendientes.

El Bloque IP mínimo registrado por NIC MÉXICO es un /32 y para calificar para el registro inicial, EL CLIENTE debe:

i. Ser un LIR (Local Internet Registry), o sea, organización que asigna direcciones para usuarios de los servicios de red que provee. Son, en general, los proveedores de acceso (ISP), cuyos clientes son los Usuarios Finales u otros proveedores de acceso (ISP);
ii. No ser un sitio final Usuario Final o (UF);
iii. Documentar un plan detallado sobre los servicios y la conectividad en IPv6 a ofrecer a otras organizaciones (clientes);

iv. Anunciar en el sistema de rutas inter-dominio de Internet un único Bloque IP, que agregue todo el registro de direcciones IPv6 recibidas, en un plazo no mayor de 12 (doce) meses;
v. Ofrecer servicios en IPv6 a clientes localizados físicamente en la región del LACNIC en un plazo no mayor de 24 (veinticuatro) meses.

3. Registro de Bloques IP Adicionales.

3.1 Solicitud de Bloque IPv4 adicional.

Las organizaciones que deseen solicitar Bloques IPv4 adicionales, deben haber utilizado eficientemente los Bloques IP registrados anteriormente y por lo menos el 80% de Bloques IP registrados más recientemente.

Al solicitar Bloques IP adicionales, se entiende que EL CLIENTE conoce la existencia de una tarifa asociada a la renovación del SERVICIO de registro de los Recursos registrados por NIC MÉXICO.

Solicitudes de registro adicional solamente serán completadas en los casos que no hayan adeudos ni documentación pendientes.

3.2 Solicitud de Bloque IPv6 adicional.

Se concederán adjudicaciones adicionales, cuando EL CLIENTE (ISP/LIR) alcance una alta tasa de utilización del último Bloque IP registrado. La tasa de utilización será calculada en términos de Bloques IP de prefijo /48 registrados a usuarios finales.

Para calcular la tasa de utilización se usara la metodología HD-Ratio RFC3194. Según ésta metodología, una tasa de 0.8 es considerada aceptable en términos de utilización de direccionamiento, lo cual justificará a una adjudicación adicional.

NIC MÉXICO utilizará la información de EL CLIENTE registrada en el WHOIS de LACNIC para calcular el HD-Ratio.

En caso de que EL CLIENTE pruebe una buena utilización del Espacio de Direcciones IP anteriormente registrado, según el criterio mencionado, estará habilitado para recibir un nuevo Espacio de Direcciones IP de tamaño igual al recibido anteriormente.

Siempre que sea posible, el espacio adicional a ser registrado a una organización, será adyacente al último espacio registrado.

EL CLIENTE debe tener claro que existe una tarifa asociada a la renovación del SERVICIO de registro de los Recursos registrados por NIC MÉXICO.

4. Propósito de los Bloques IPv4.

Los Bloques IP deberán utilizarse para fines específicos de acuerdo al tipo de cliente al que le fueron registrados:

i. Bloques registrados a ISP: Los clientes ISP que tengan Bloques de Direcciones IP registrados, los podrán utilizar para proveer de Servicios de Internet a sus propios clientes, siempre y cuando observen las políticas establecidas por LACNIC.
ii. Bloques registrados a Usuarios Finales: Los Usuarios Finales sólo podrán utilizar el espacio registrado de direccionamiento para la infraestructura de redes de la propia empresa, no pudiendo comercializar Servicios de Internet a cualquier persona u organización.

5. Mantenimiento de la información relacionada con los Bloques IP.
   El mantenimiento de la información relacionada con los Bloques de Direcciones IP es ofrecido por NIC MÉXICO de acuerdo al punto I, inciso f) de este mismo ANEXO.

6. Soporte Técnico.
   El soporte técnico para Bloques de Direcciones IP es ofrecido por NIC MÉXICO de acuerdo al punto I, inciso d) de este mismo ANEXO.

7. Transferencias
   Las transferencias de Bloques de Direcciones IP se efectuarán de acuerdo al punto I, inciso c) de este mismo ANEXO que especifica las transferencias de Recursos.

8. Resolución Inversa
   La Resolución Inversa de los Bloques de Direcciones IP se deberá realizar como se indica en el punto I, inciso e) de este mismo ANEXO que especifica las transferencias de Recursos.

9. Revisiones de NIC MÉXICO (auditorías).
   NIC MÉXICO se reserva el derecho de verificar, por medio de la Resolución Inversa de los Bloques IP de EL CLIENTE, la utilización del Bloque IP y la implementación de la Resolución Inversa. Así como solicitar al cliente en cualquier momento documentación que compruebe que EL CLIENTE se ha apegado a las políticas de LACNIC al utilizar el Espacio de Direcciones IP registrado.

   Con el propósito de facilitar la revisión de la Resolución Inversa de los Bloques IP, EL CLIENTE deberá permitir a NIC MÉXICO hacer la transferencia de las zonas de cada uno de los Bloques IP listados en el ANEXO E utilizando el Protocolo AXFR por el puerto 53 de TCP.

10. Revocación de Bloques IP.
    La revocación de Bloques de Direcciones IP se llevará a cabo de acuerdo al punto I, inciso g) de este mismo ANEXO.

b) Vigencia y Renovación.

1. La vigencia de cada Bloque IP registrado será de un año a partir de su fecha de registro.
2. EL CLIENTE realizará un pago por Cuota Inicial que cubrirá por un año el registro del Bloque IP.
3. A partir de la primera Fecha de aniversario del registro, fecha oficial de cobro del Bloque IP, del primer Bloque IP registrado por EL CLIENTE, se cobrará una Cuota de Renovación de todo el Espacio de Direcciones IP registrados para EL CLIENTE.
4. La Cuota de Renovación cubrirá por un año el registro del Espacio de Direcciones IP de EL CLIENTE.

c) Transferencias.

Los Recursos registrados por NIC MÉXICO no están sujetos a transferencias o ventas, una vez que estos Recursos fueran registrados para las organizaciones que cumplieran con los requisitos para registros iniciales. Estos registros son válidos mientras sean válidos los criterios del registro y no haya pagos o documentación pendiente con NIC MÉXICO.

Pero al mismo tiempo, NIC MÉXICO y EL CLIENTE reconoce que hay situaciones donde son necesarias las transferencias de los Recursos de una organización para otra.

Las situaciones en que las transferencias son justificadas son aquellas que resultan de operación de compra y venta de la organización, fusión, reestructuración, o también cambio del nombre.

En los casos en que EL CLIENTE cesara sus actividades, el punto de contacto de los Recursos registrados por LACNIC a EL CLIENTE no tiene permiso para vender, transferir o ceder estos Recursos para otra organización sino que debe devolver los Recursos a NIC MÉXICO.

En los casos de Recursos no registrados directamente por NIC MÉXICO, la transferencia debe ser solicitada al Proveedor de Servicios de Internet correspondiente.

Se podrán transferir los Recursos de Internet primordiales para el funcionamiento de algún servicio adquirido por la organización para la cual están siendo transferidos.

Para solicitar la transferencia de un recurso de Internet registrado por NIC MÉXICO, EL CLIENTE debe llenar el formulario indicado y enviarlo después para ipmaster@nic.mx.

Durante el proceso de análisis de un pedido de transferencia, NIC MÉXICO puede solicitar los siguientes documentos:

- copia certificada del documento que compruebe la transferencia de los bienes entre las organizaciones. Por ejemplo, Escritura Publica, Contrato, etc.;
- un inventario detallado de los bienes que utilizan los Recursos de Internet involucrados en la transferencia;
- una lista de clientes que usan parte de las direcciones IP de la organización que solicita la transferencia.

En caso de ser necesario, podrán también ser solicitados a EL CLIENTE los siguientes documentos:

- una lista de los bienes adquiridos;
- una descripción de los bienes adquiridos, incluyendo tipo y cantidad de equipamiento y clientes;
- una descripción de como serán utilizadas las direcciones IP;
  una topología de la red, incluyendo número de máquinas, máscara de red, diagrama de red y designaciones hechas para clientes.

EL CLIENTE tiene pleno conocimiento de que existe una tarifa asociada a la transferencia de los Recursos registrados por NIC MÉXICO.

El solicitante debe tener claro también que los Recursos legados transferidos de una organización para otra estarán sujetos a tarifas de renovación o mantenimiento para la cuales era exento hasta el momento, según se explica en las siguientes referencias: http://www.nic.mx/es/IP.Transferencias y http://www.nic.mx/es/IP.Recursos_Legados.

d) Soporte Técnico.

El soporte técnico podrá ocurrir de forma personal dentro del horario de 8:30 a 18:00 horas tiempo del centro de México, de lunes a viernes.

Fuera del horario antes mencionado, NIC MÉXICO ofrece a EL CLIENTE atender sus dudas a través de la cuenta de correo electrónico ip-help@nic.mx.

e) Resolución Inversa.

Todo el Espacio de Direcciones IP registrado debe tener un servidor DNS asociado que será responsable por la Resolución Inversa. En el caso de los Bloques direcciones IP registradas en México, esos servidores deben ser registrados en NIC MÉXICO.

NIC MÉXICO podrá utilizar información producto de la Resolución Inversa como indicador de la utilización del Bloque de Direcciones IP registrado.

El registro de los servidores DNS del Espacio de Direcciones IP administrado por NIC MÉXICO, será hecho de forma diferente dependiendo del tamaño del espacio registrado, para mayor información al respecto consulte la página de NIC MÉXICO (http://www.nic.mx/es/IP.Resolucion_Inversa).

En cualquier caso el registro de los servidores de Resolución Inversa deberá ser solicitado a la cuenta ip-sol@nic.mx, incluyendo los datos de los Bloques IP y el nombre y dirección IP de los servidores DNS que se encargarán de la Resolución Inversa. La solicitud debe ser realizada por el contacto para el Bloque IP registrado en la base de datos WHOIS de LACNIC o en su defecto en el de ARIN.

f) Mantenimiento de información de Recursos.

NIC MÉXICO proveerá soporte técnico al cliente siempre que éste solicite, a través de su contacto administrativo quien podrá modificar cualquier tipo de información relacionada con los Recursos registrados directamente por NIC MÉXICO.
Toda solicitud relacionada con el mantenimiento de la información sobre los Recursos registrados a EL CLIENTE, deberá dirigirse a la cuente ip-help@nic.mx.
EL CLIENTE contará con el apoyo de NIC MÉXICO, para resolver cualquier duda al utilizar el sistema de administración de Recursos que ofrece LACNIC en su página de Servicios de Registro.

g) Revocación.

Se entiende por revocación la eliminación del registro de Bloques IP y/o ASN a nombre de EL CLIENTE en las bases de datos del WHOIS de LACNIC, y la colocación de estos Recursos como disponibles para futuros registros de otras organizaciones.

NIC MÉXICO podrá realizar la revocación de Bloques de Direcciones IP o ASN cuando se presenten cualquiera de los siguientes supuestos:

i. Incumplimiento de cualquiera de las obligaciones del presente o de cualquiera de sus ANEXOS.

ii. Incumplimiento de las políticas de LACNIC y/o de NIC MÉXICO.

iii. En caso de terminación anticipada de conformidad con los términos y condiciones del Contrato y sus ANEXOS.

II. Números ASN.

a) Políticas de Uso.

1. Administración de Bloques IP (Funciones de NIC MÉXICO y de LACNIC).
Los SERVICIOS de NIC MÉXICO incluyen de forma enunciativa mas no limitativa: el registro, administración, transferencia y revocación de Bloques IP y Números de Sistemas Autónomos (ASN); Resolución Inversa de los Bloques IP registrados, mantenimiento de la información proporcionada con los Bloques IP y Números de Sistemas Autónomos.

Para los SERVICIOS de Bloques de Direcciones IP que ofrece, NIC MÉXICO se basa en las Políticas de Administración de Recursos de LACNIC (http://www.nic.mx/es/IP.Politicas).

2. Requisitos para el registro (Formales y Técnicos).
Para solicitar un ASN (Autonomous System Number) o Sistema de Número Autónomo, EL CLIENTE debe llenar el formulario indicado y enviarlo después a la cuenta de correo electrónico: ipmaster@nic.mx.

Una vez aprobada la solicitud de ASN, un correo electrónico será enviado con información sobre el pago y sobre el acuerdo que deber ser firmado. El registro del ASN solamente será hecho después de la recepción del pago y del acuerdo firmado. Para calificar para un registro de un ASN, EL CLIENTE debe tener:

i. Una política de enrutamiento única, o sea, una política que difiera de aquéllas practicadas por las redes vecinas con las que EL CLIENTE posee conexión.
ii. Una red con más de una conexión independiente a Internet (multi-homed site).
iii. El solicitante debe tener claro que existe una tarifa de mantenimiento del registro de los Recursos registrados por NIC MÉXICO.

3. Mantenimiento de la información relacionada con los ASN.
   El mantenimiento de la información relacionada con ASN es ofrecido por NIC MÉXICO de acuerdo al punto I, inciso f) de este mismo ANEXO.

4. Soporte Técnico.
   El soporte técnico para el recurso de ASN es ofrecido por NIC MÉXICO de acuerdo al punto I, inciso d) de este mismo ANEXO.

5. Transferencias.
   Las transferencias del recurso de ASN se efectuarán de acuerdo al punto I, inciso c) de este mismo ANEXO que especifica las Transferencias de Recursos.

6. Revocación de ASN.
   La revocación de ASN se llevará a cabo de acuerdo al punto I, inciso g) de este mismo ANEXO.

NETWORK INFORMATION CENTER MÉXICO, S. C.

Ing. Oscar Alejandro Robles Garay	Nombre:
Director General	Puesto:
Fecha: de de	Fecha: de de

TESTIGOS

Ing. Cristóbal Chapital Tirado	Nombre:
Ave. Eugenio Garza Sada No. 427 Col Altavista	Dirección:
Monterrey, N. L.	
Tel: (81) 8387-5346	Tel:

ANEXO C

DEL CONTRATO DE PRESTACIÓN DE SERVICIOS CELEBRADO ENTRE NETWORK INFORMATION CENTER MÉXICO, S.C. (en lo sucesivo **"NIC MÉXICO"**) Y

(en lo sucesivo "EL CLIENTE"), EL DIA DE DE EN LA CIUDAD DE MONTERREY, NUEVO LEÓN.

FORMULARIOS

El presente ANEXO contiene una descripción, enunciativa mas no limitativa, de los formularios que **EL CLIENTE** deberá llenar conforme a lo establecido en el Contrato y en su ANEXO B. EL CLIENTE deberá revisar los formularios en el siguiente sitio de Internet: http://www.nic.mx/es/IP.Template_IPs. La descripción de los formularios es la siguiente:

Solicitudes de Bloques IPv4:

Formulario Direcciones IPv4 ISP.

```
#  No remover el numero de la version
NIC Mexico ISP Template 20041124-1-SP

#  Envie esta solicitud a ip-sol@nic.mx

#  Informacion sobre la organizacion que esta solicitando
#  el bloque IPv4
#  Si la organizacion ya tiene algun recurso registrado con
#  LACNIC, informar solamente su "ownerID".
#  En caso de no saber cual es el "ownerID" consulte algun recurso
#  adjudicado a su organizacion en el servidor WHOIS de LACNIC
#  [whois://whois.lacnic.net]

0a. ID. de la Organizacion (OwnerID):
0b. Nombre de la Organizacion:
0c. Direccion Postal:
0d. Ciudad:
0e. Estado:
0f. Pais: MEXICO
0g. Codigo Postal:

#  Puntos de contacto en la organizacion.
#  Sera necesario informar contacto tecnico, de facturacion y
#  de membresia.
#  Los contactos de facturacion y membresia son internos y por esto
#  no son visibles en las consultas whois.
#  Informar solamente el "userID" de los puntos de contacto.
#  En el caso que no los tenga aun, los debe crear en:
#  http://lacnic.net/cgi-bin/lacnic/idmng?lg=SP

1a. ID contacto tecnico (UserID):
1b. ID contacto facturacion (UserID):
1c. ID contacto membresia (UserID):

#  Conexion hacia Internet.
#  Informar el nombre del proveedor, su direccion postal, su ASN
#  y el estado de la conexion de la organizacion con este proveedor.
#  Copie los campos a continuacion para uno de los proveedores con
#  los cuales la organizacion tiene conexion.

2a. Nombre del Proveedor:
2b. Direccion Postal:
2d. ASN del proveedor:
2e. Estado de la conexion:
```

Conexion con punto se intercambio de paquetes
Reproduzca los campos a continuacion para cada una de las conexiones.

3a. Intercambio con ASN:
3b. Direccion Postal:
3c. Estado de la conexion:

Informacion sobre la utilizacion de las redes.
Informar todos los bloques IP asignados a la organizacion
por LACNIC o por sus proveedores Internet.

4a. Bloques:
4b. Asignados:
4c. Reservados:
4d. Disponibles:
4e. Servicios:

5. Prefijo del bloque CIDR solicitado:

Proyeccion de utilizacion del bloque
Solicitado para los proximos 3 meses

6a. Dial-up:
6b. Cable:
6c. Webhosting:
6d. Conexion Dedicada:
6e. xDSL:
6f. Co-location:
6g. Wireless:
6h. Otros (identificar):

7. Informacion Adicional:

Servidores de resolución inversa.
Copie los campos a continuacion para cada uno de los servidores
de resolucion inversa.

8a. Nombre del servidor:
8b. Dirección IP del servidor:

No remover esta linea
Final del formulario

Formulario Direcciones IPv4 Usuarios finales

No remover el numero de la version
NIC Mexico END-USER Template 20041124-1-SP

Envie esta solicitud a ip-sol@nic.mx

Informacion sobre la organizacion que esta solicitando
el bloque IPv4
Si la organizacion ya tiene algun recurso registrado con
LACNIC, informar solamente su "ownerID".
En caso de no saber cual es el "ownerID" consulte algun recurso
adjudicado a su organizacion en el servidor WHOIS de LACNIC
[whois://whois.lacnic.net]

0a. ID. de la Organizacion (OwnerID):
0b. Nombre de la Organizacion:
0c. Direccion Postal:
0d. Ciudad:
0e. Estado:
0f. Pais: MEXICO

0g. Codigo Postal:

Puntos de contacto en la organizacion.
Sera necesario informar contacto tecnico, de facturacion y
de membresia.
Los contactos de facturacion y membresia son internos y por esto
no son visibles en las consultas whois.
Informar solamente el "userID" de los puntos de contacto.
En el caso que no los tenga aun, los debe crear en:
http://lacnic.net/cgi-bin/lacnic/idmng?lg=SP

1a. ID contacto tecnico (UserID):
1b. ID contacto facturacion (UserID):
1c. ID contacto membresia (UserID):

Conexion hacia Internet.
Informar el nombre del proveedor, su direccion postal, su ASN
y el estado de la conexion de la organizacion con este proveedor.
Reproduzca los campos a continuacion para cada uno de los proveedores con
los cuales la organizacion tiene conexion.

2a. Nombre del Proveedor:
2b. Direccion Postal:
2d. ASN del proveedor:
2e. Estado de la conexion:

Informacion sobre la utilizacion de las redes.
Informar todos los bloques IP asignados a la organizacion
por LACNIC o por sus proveedores Internet.

3a. Direcciones IP asignadas:

Explicar como las direcciones informadas estan siendo
utilizadas en la red de la organizacion.

4a. Numero de hosts:
4b. Numero de subnets:
4c. Mascara de subnet:
4d. Topologia de la red segun el ejemplo:

Numero	Mascara de subnet	Direcc. en uso	Descripcion
0	255.255.255.224	8	Grupo de Red
1	255.255.255.224	17	Ingenieria
2	255.255.255.224	12	Manufactura
3	255.255.255.224	5	Gerencia
4	255.255.255.224	10	Ventas
5	255.255.255.224	7	Finanzas

Informar la funcion de la red en la organizacion

5. Tipo de la red:

6. Numero de direcciones solicitadas:

Brindar con informacion detallada demostrando como la direcciones
solicitadas van a ser utilizadas el los plazos de seis y 12 meses
asi como en el ejemplo:

Numero	Mascara de subnet	Tamano	Hoy	6Meses	12Meses	Descripcion
1.0	255.255.255.224	30	8	16	20	Grupo de Red
1.1	255.255.255.224	30	17	22	30	Ingenieria
1.2	255.255.255.224	30	12	12	20	Manufactura

1.3	255.255.255.224	30	5	9	15	Gerencia
1.4	255.255.255.224	30	10	15	25	Ventas
1.5	255.255.255.224	30	7	8	15	Finanzas
1.6	255.255.255.224	30	0	0		(reserva)
	Totales	210	59	82	125	

7. Informacion Adicional:

Servidores de resolución inversa.
Copie los campos a continuacion para cada uno de los servidores
de resolucion inversa.

8a. Nombre del servidor:
8b. Dirección IP del servidor:

No remover esta linea
Final del formulario

Formulario Direcciones IPv6

No remover el numero de la version
NIC Mexico IPV6 Template 20060101-1-SP

Envie esta solicitud para ip-sol@nic.mx

Informacion sobre la organizacion que esta solicitando
el bloque IPv6.
Si la organizacion ya tiene algun recurso registrado con
LACNIC, informar solamente su "ownerID".
En caso de no saber cual es el "ownerID" consulte algun recurso
adjudicado a su organizacion en el servidor WHOIS de LACNIC
[whois://whois.lacnic.net]

0a. ID. de la Organizacion (OwnerID):
0b. Nombre de la Organizacion:
0c. Direccion Postal:
0d. Ciudad:
0e. Estado:
0f. Pais:
0g. Codigo Postal:

Puntos de contacto en la organizacion.
Sera necesario informar contacto tecnico, de facturacion y
de membresia.
Los contactos de facturacion y membresia son internos y por esto
no son visibles en las consultas whois.
Informar solamente el "userID" de los puntos de contacto.
En el caso que no los tenga aun, los debe crear en:
http://lacnic.net/cgi-bin/lacnic/idmng?lg=SP

1a. ID contacto tecnico (UserID):
1b. ID contacto facturacion (UserID):
1c. ID contacto membresia (UserID):

Brindar informacion sobre la organizacion que solicita el
bloque IPv6.

2a. Informacion de la Organizacion:

Informar el plan para despliegue de la red IPv6 en la
organizacion, el plan de utilizacion de la direcciones IPv6
y plan de sub asignaciones de direcciones IPv6 para los
clientes.

3a. Fecha:
3b. Plan de utilizacion:
3c. Plan de Asignacion:

Brindar informacion sobre la estructura de la red
IPv6 y tipos de servicios que seran ofrecidos para los clientes.
En el caso que se este solicitando un prefijo mas largo que /32
brindar tambien informacion que justifique esta necesidad.

4. Informacion Adicional:

No remover esta linea
Final del formulario

Formulario ASN

No remover el numero de la version
NIC Mexico ASN Template 20060101-1-SP

Envie esta solicitud para ip-sol@nic.mx

Indicar "M" para organizaciones multi-homed, "U" para
organizaciones con politica unica de ruteo

0a. Multihomed (M), Politica Unica (U):

Informacion sobre la organizacion que esta solicitando
el ASN.
Si la organizacion ya tiene algun recurso registrado con
LACNIC, informar solamente su "ownerID".
En caso de no saber cual es el "ownerID" consulte algun recurso
adjudicado a su organizacion en el servidor WHOIS de LACNIC
[whois://whois.lacnic.net]

1a. ID. de la Organizacion (OwnerID):
1b. Nombre de la Organizacion:
1c. Direccion Postal:
1d. Ciudad:
1e. Estado:
1f. Pais:
1g. Codigo Postal:

Puntos de contacto en la organizacion.
Sera necesario informar el contacto tecnico y de facturacion.
El contacto de facturacion es interno y por esto no es
visible en las consultas whois.
Informar solamente el "userID" de los puntos de contacto.
En el caso que no los tenga aun, los debe crear en:
http://lacnic.net/cgi-bin/lacnic/idmng?lg=SP

2a. ID contacto tecnico (UserID):
2b. ID contacto facturacion (UserID):

En el caso de organizacion multi-homed, brindar la
informacion sobre el protocolo de ruteo a ser utilizado,
los bloques IPs que van a ser anunciados con origen en
el ASN solicitado y los ASNs de los proveedores Internet
de la organizacion.

3a. Protocolo de ruteo:
3b. Bloques IPs:
3c. ASN's de los proveedores:

Brindar la informacion sobre los dos o mas proveedores
de Internet de la organizacion, indicando nombre, telefono
y e-mail de la persona de contacto en el proveedor.

3d. Nombre:
3e. Telefono:
3f. E-Mail:

3d. Nombre:
3e. Telefono:
3f. E-Mail:

En el caso de organizacion con politica de ruteo
unica y distinta de la utilizada por el proveedor,
brindar la informacion detallada sobre esta politica
e indicar los proveedores Internet de la organizacion

4a. Politica unica de ruteo:
4b. Conexiones Internet:

5. Informacion Adicional:

No remover esta linea
Final del formulario

Formulario de Transferencia de Recursos

No remover el numero de la version
NIC México Transfer Template 20041124-1-SP

Envie esta solicitud para ip-sol@nic.mx

Informacion sobre la organizacion que actualmente
tiene registrado el Recurso (IP/ASN).
Indique el "OwnerID" de esta organizacion
En caso de no saber cual es el "ownerID" consulte algun recurso
adjudicado a su organizacion en el servidor WHOIS de LACNIC
[whois://whois.lacnic.net]

0a. ID. de la Organizacion (OwnerID):

Recursos siendo transferidos.
Informe todos los recursos registrados para esta
organizacion y que van a ser transferidos.

1a. ASN's:
1b. Bloques IP:

2a. Motivo de la transferencia:

Informacion sobre la organizacion que va a recibir
los recursos Internet indicados en el campo 1a. y/o 1b.

Si la organizacion ya tiene algun recurso registrado con
LACNIC, informar solamente su "ownerID".
Si no tiene ningun recurso registrado, informar los otros
datos de la organizacion

3a. ID. de la Organizacion (OwnerID):
3b. Nombre de la Organizacion:

3g. Código Postal:

Puntos de contacto en la organizacion que va a recibir
los recursos
Sera necesario informar contacto tecnico, de facturacion y
de membresia.
Los contacto de facturacion y membresia son internos y por esto
no son visibles en las consultas whois.
En el caso que los tenga aun, se los debe crear en:
http://lacnic.net/cgi-bin/lacnic/idmng?lg=SP

4a. ID contacto tecnico (UserID):
4b. ID contacto facturacion (UserID):
4c. ID contacto membresia (UserID):
Informar los Recursos Internet que seran transferidos
para la organizacion indicada en el campo 3

5a. ASN's:
5b. Bloques IP:

Final del formulario

NETWORK INFORMATION CENTER MÉXICO, S. C.

Ing. Oscar Alejandro Robles Garay	Nombre:
Director General	Puesto:
Fecha: de de	Fecha: de de

TESTIGOS

Ing. Cristóbal Chapital Tirado	Nombre:
Ave. Eugenio Garza Sada No. 427 Col Altavista	Dirección:
Tel: (81) 8387-5346	Tel:

ANEXO D

DEL CONTRATO DE PRESTACIÓN DE SERVICIOS CELEBRADO ENTRE NETWORK INFORMATION CENTER MÉXICO, S.C. (en lo sucesivo "NIC MÉXICO") Y

(en lo sucesivo "EL CLIENTE"), EL DIA DE DE EN LA CIUDAD DE MONTERREY, NUEVO LEÓN.

MEMBRESIA LACNIC.

La membresía de LACNIC es automática para las organizaciones que reciben Bloques de Direcciones IP directamente de NIC MÉXICO, existiendo diferentes categorías de miembros y niveles establecidos de acuerdo al tamaño del Espacio de Direcciones IP que administra cada organización. La membresía es abierta a cualquier persona u organización interesada en ser parte de LACNIC, por lo que las organizaciones que no reciben direcciones IP de LACNIC o NIC MÉXICO igualmente pueden solicitar su aceptación como miembros.

No es necesario ser miembro de LACNIC para poder solicitar Recursos. El hecho de ser miembro tampoco facilitará el proceso de obtención de los mismos.

Información detallada referente a las categorías de miembros, derechos y obligaciones de los mismos, se encuentra disponible en el Capítulo III del Estatuto: http://lacnic.net/sp/sobre-lacnic/estatuto/iii.html.

De acuerdo al estatuto de LACNIC (http://lacnic.net/sp/sobre-lacnic/estatuto/), los miembros Activos A tienen incluido en su cuota anual de renovación, el costo de la membresía.

Para mayor información sobre otros tipos de membresías LACNIC y cómo conseguirlas, visitar la página de Membresía de LACNIC.

- Nota: Aquellas organizaciones que posean Números de Sistema Autónomos (ASN) no tienen membresía automática, ya que pagan una cuota anual de mantenimiento y no una cuota de renovación. Por lo tanto, si desean ser miembros deberán completar el Formulario de Solicitud de Membresía y pagar la cuota anual de membresía.

El Estatuto LACNIC, el cual contiene información detallada sobre la Membresía A que se otorga a los clientes de NIC MÉXICO con Espacio de Direcciones IP (consultar principalmente Capítulos III y IV) se encuentra en la siguiente dirección electrónica: http://lacnic.net/sp/sobre-lacnic/estatuto/.

NETWORK INFORMATION CENTER MÉXICO, S. C.

Ing. Oscar Alejandro Robles Garay	Nombre:
Director General	Puesto:
Fecha: de de	Fecha: de de

TESTIGOS

Ing. Cristóbal Chapital Tirado	Nombre:
Ave. Eugenio Garza Sada No. 427 Col Altavista	Dirección:
Monterrey, N. L.	
Tel: (81) 8387-5346	Tel:

(en lo sucesivo EL CLIENTE), EL DIA DE DE EN LA CIUDAD DE MONTERREY, NUEVO LEÓN.

De conformidad con las disposiciones establecidas en el Contrato de Prestación de Servicios y sus ANEXOS, se prestara el SERVICIO a los siguientes Recursos:
Recursos legados

Recursos

NETWORK INFORMATION CENTER MÉXICO, S. C.

Ing. Oscar Alejandro Robles Garay
Director General
Fecha: de de

Nombre:
Puesto:
Fecha: de de

Testigos

Ing. Cristóbal Chapital Tirado
Monterrey, N. L.
Tel: (81) 8387-5346

Nombre:
Tel:

a) Completar el formulario y enviarlo a la cuenta de correo ip-sol@nic.mx
b) Al ser aprobada la solicitud, el cliente debe enviar a NIC México dos copias del Contrato de Prestación de Servicios, después de haberlas llenado y firmadas por el representante legal.
c) Posteriormente el cliente recibirá las instrucciones para elaborar el pago correspondiente al monto inicial.
d) El bloque será asignado tan pronto como NIC México compruebe que el pago fue realizado. Solicitud de un bloque adicional de direcciones IPv6: Debe realizar lo siguiente:

a) Leer la información relacionada:

- Direcciones
- Políticas IPv6
- Información Contrato de Prestación de Servicios
- Tarifas
- Documentos , Sección de Formularios

b) Completar el formulario y enviarlo a la cuenta de correo ip-sol@nic.mx
c) Al ser aprobada la solicitud, el cliente debe enviar a NIC México dos copias del Contrato de Prestación de Servicios, después de haberlas llenado y firmadas por el representante legal.
d) Posteriormente el cliente recibirá las instrucciones para elaborar el pago correspondiente al monto inicial.
e) El bloque será asignado tan pronto como NIC México compruebe que el pago fue realizado.

CAPITULO VI
COMPARACION DE LOS MODELOS DIFFSERV vs INTSERV

Como ya se ha visto , el incremento de nuevas aplicaciones que necesitan QoS garantizado ha hecho que aparezcan nuevos modelos que proponen QoS a aplicaciones de tiempo real. Si bien es posible encontrarse con variadas técnicas de implementación de QoS, todas ellas tienen en común la clasificación o diferenciación de flujos de tráfico, en grupos llamados clases.

Es probable que la mayoría de la gente, cuando se les habla de calidad de servicio, piense en clases de servicio diferenciadas, en conjunto quizá con algunos mecanismos para proveer políticas de tráfico o control de admisión. La palabra clave en este tema es la diferenciación, debido a que antes de poder otorgar calidad de servicio a un cliente en particular, aplicación o protocolo, es necesario clasificar el tráfico en clases y determinar la forma en que serán manejadas estas clases de tráfico a medida que circulan por la red.

Durante los últimos años han surgido variados métodos para establecer QoS en equipamientos de redes. Algoritmos avanzados de manejos de cola, modeladores de tráfico (traffic shaping), y mecanismos de filtrado mediante listas de acceso (access-list), han hecho que el proceso de elegir una estrategia de QoS sea más delicado. Cada red puede tomar ventaja de distintos aspectos en implementaciones de QoS para una obtener una mayor eficiencia, ya sea para redes de pequeñas corporaciones, empresas, o proveedores de servicios de Internet. enrutador a lo largo de la ruta, la escalabilidad para cientos de miles de flujos a través de una red central, típicos de una red óptica, se convierte en un problema.

6.1 Servicios Integrados.

El modelo de Servicios Integrados (IntServ: Integrated Services) provee a las aplicaciones de un nivel garantizado de servicio, negociando parámetros de red , de extremo a extremo. La aplicación solicita el nivel de servicio necesario para ella con el fin de operar apropiadamente, y se basa en la QoS para que se reserven los recursos de red necesarios antes de que la aplicación comience a operar. Estas reservaciones se mantienen en pie hasta que la aplicación termina o hasta que el ancho de banda requerido por ésta sobrepase

el límite reservado para dicha aplicación. El modelo IntServ se basa en el Protocolo de Reservación de Recursos (RSVP) para señalizar y reservar la QoS deseada para cada flujo en la red. Debido a que la información de estados para cada reservación necesita ser mantenida por cada enrutador a lo largo de la ruta, la escalabilidad para cientos de miles de flujos a través de una red central, típicos de una red óptica, se convierte en un problema.

6.2 Servicios Diferenciados.

Este modelo incluye un conjunto de herramientas de clasificación y mecanismos de cola que proveen a ciertas aplicaciones o protocolos con determinadas prioridades sobre el resto del tráfico en la red. DiffServ cuenta con los enrutadores de bordes para realizar la clasificación de los distintos tipos de paquetes que circulan por la red. El tráfico de red puede ser clasificado por dirección de red, protocolo, puertos, interfaz de ingreso o cualquier tipo de clasificación que pueda ser alcanzada mediante el uso de listas de acceso, en su variante para la implementación de QoS. Al utilizar el modelo DiffServ se obtienen varias ventajas. Los enrutadores operan más rápido, ya que se limita la complejidad de la clasificación y el encolado. Se minimiza el tráfico de señalización, y el almacenamiento. En DiffServ, se definen clases de servicio, cada flujo particular de datos es agrupado en un tipo de clase, donde son tratados idénticamente. Los enrutadores internos sólo están interesados del comportamiento por saltos (PHB: Per Hop Behavior), marcado en la cabecera del paquete. Esta arquitectura permite a DiffServ rendir mucho mejor en ambientes de bajo ancho de banda, y provee de un mayor potencial que una arquitectura IntServ.

En resumen :

IntServ	**DiffServ**
Reserva	Priorización
Recursos basados en flujos de trafico	Recursos basados en clase de tráfico
Dificultad en escalabilidad	Buena escalabilidad
QoS esta en los routers	QoS está en los datagramas
-------	Implementado en Qbone (Internet2)
Necesita señalización (RSVP)	No hay protocolo de señalización
Garantía de servicio alta	Garantia de servicio menos altas pero suficientes

CAPITULO VII
DIFERENTES MECANISMOS DE TRANSICION IPV4 / IPV6 EN ENTORNO DE QoS

7.1 Introducción

La motivación inicial para comenzar a definir una nueva versión del protocolo IP ha sido la limitación impuesta por el campo de direcciones en IPv4, así como por la poco eficiente división en las clases A, B, C y D. Después, la conveniencia de un formato de PDU optimizado para un proceso más eficiente en los encaminadores, la seguridad, y la calidad del servicio, contribuyeron a la aparición de una nueva versión de IP, denominada IPv6, IPng o IP de nueva generación, que quedó claramente especificado en la RFC 2460.

IPv6 presenta una serie de características mejoradas sobre IPv4, como son:

- Espacio de direcciones ampliado: IPv6 emplea direcciones de 128 bits.
- Mecanismo de opciones mejorado: las opciones de IPv6 se encuentran en cabeceras separadas opcionales situadas entre la cabecera de IPv6 y la cabecera de la capa de transporte. La mayoría de estas cabeceras opcionales no se examinan ni procesan por ningún dispositivo de encaminamiento en la trayectoria del paquete, lo que acelera su procesamiento.
- Direcciones de autoconfiguración: asignación dinámica de direcciones IPv6.
- Aumento de la flexibilidad en el direccionamiento: IPv6 incluye el concepto de anycast, mediante el cual el paquete se entrega solamente a un nodo seleccionado entre un grupo de nodos.
- Facilidad para la asignación de recursos: IPv6 habilita el etiquetado de los paquetes como pertenecientes a un flujo de tráfico particular para el cual el emisor solicita un tratamiento especial.
- Capacidades de seguridad.
- Eliminación de control de errores de cabecera.
- Fragmentación sólo en la fuente.

7.2 Coexistencia con IPv4 y Migración

En una primera fase de despliegue de IPv6, la mayor parte de la red será razonablemente IPv4. Para conectar IPV6 a través de una red IPv4, se pueden utilizar varios sistemas.

7.2.1 ¿Por qué son necesarios los mecanismos de transición?

a) ¿Por qué?

- Hay un gran número de hosts y routers que manejan el protocolo IPv4
- No hay establecido un día en concreto para realizar la transición de IPv4 a IPv6.
- Durante un cierto tiempo, y parece que va ser largo, IPv4 e IPv6 coexistirán Así que ciertos mecanismos de transición deben de ser definidos para permitir a los host con IPv4 y a los que tienen IPv6 comunicarse los unos con los otros.

b) Tres aproximaciones hacia los mecanismos de transición:

Según el punto donde nos encontremos y para conseguir la comunicación, podemos hablar de:

- En el host/router: IPv4/IPv6 Dual Stack
- En la red: tunelización
- En el gateway: traductores IPv4/IPv6

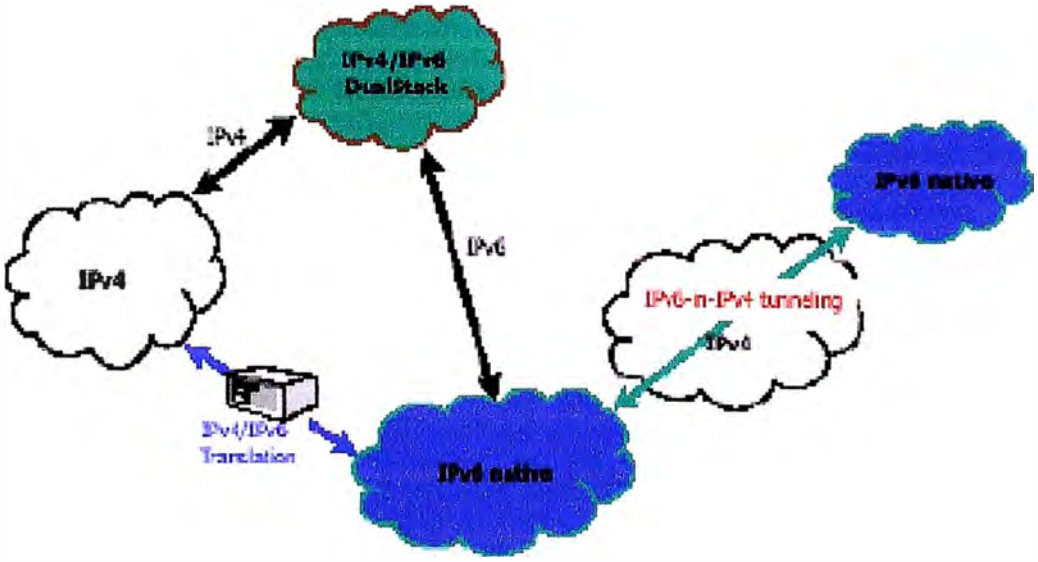


Fig 7.1 Red IPv4 mezclada con red IPv6

7.2.2 Mecanismos básicos para la transición IPv4/IPv6

a) En el host/router

a.1) IPv4/IPv6 Dual Stack

- Este mecanismo provee de soporte completo para ambos protocolos IPv4 e IPv6 en Hosts y Routers.
- Resuelve operaciones con registros A y AAAA(A6) :
- Devuelve sólo direcciones IPv6
- Devuelve sólo direcciones IPv4
- Devolviendo direcciones de ambas versiones del protocolo (IPv4 e IPv6)

Fig 7.2: Resolución de operaciones con IPV4/IPV6 Dual Stack

b) En la red

b.1) Tuneles configurados

- El punto final del túnel esta determinado desde la información de configuración en el nodo de encapsulación.
- La determinación de cuáles paquetes tunelizar se hace mediante la información de encaminamiento del nodo de encapsulación.

b.2) 6to4

Conceptos básicos

- Se utiliza para conectar dominios IPv6 aislados en un entorno IPv4
- Es una especie de tunelización automática que no precisa direcciones compatibles con IPv4
- Los puntos IPv4 finales del túnel se identifican en el prefijo del dominio IPv6

Cómo funciona

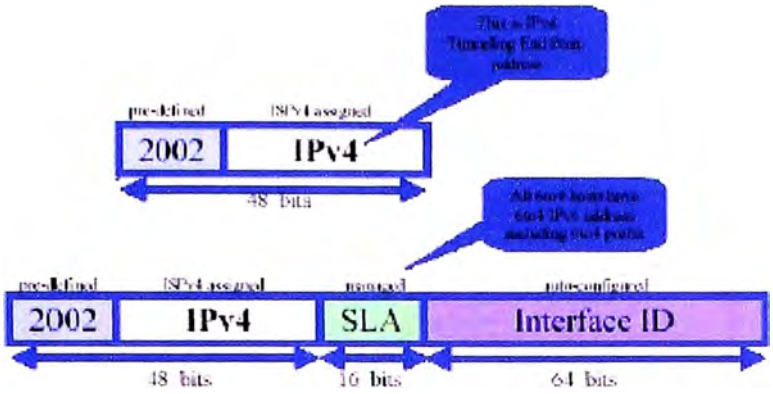


Fig 7.3 Prefijo 6to4 y dirección 6to4

- Router 6to4
  - Router que se encuentra entre un área amplia que trabaja en IPv4 y un sitio IPv6
  - La encapsulación y la desencapsulación se lleva a cabo en el router 6to4
- Host 6to4
  - Host , el cual tiene una dirección 6to4.
- Router de paso
  - Router 6to4 que soporta el encaminamiento de tránsito entre una dirección 6to4 y una dirección IPv6 nativa
  - El router de paso tiene al menos un pseudo interfaz 6to4 lógico y al menos un interfaz IPv6
  - Anuncia el prefijo 6to4 y el prefijo IPv6 nativo
- Escenario de un paquete enviado
  - Un Host A 6to4 obtiene la dirección 6to4 del host B de destino (mediante DNS o algo...)
  - A envía paquetes al router por defecto(router 6to4 A')
  - El router 6to4 A' encapsula el paquete usando la dirección 6to4 del host B de destino y la envía (hace un forwarding) hacia la red IPv4
  - El router frontera B' recibe el paquete de A' y lo desencapsula.
  - B' envía (forward) el paquete a B

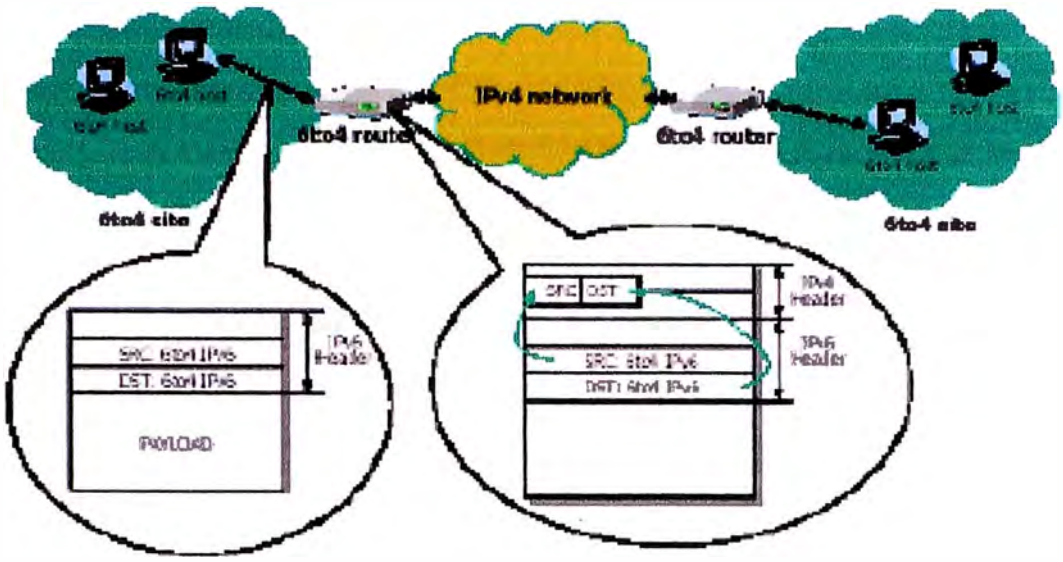


Fig 7.4: Regla de envío y encapsulación

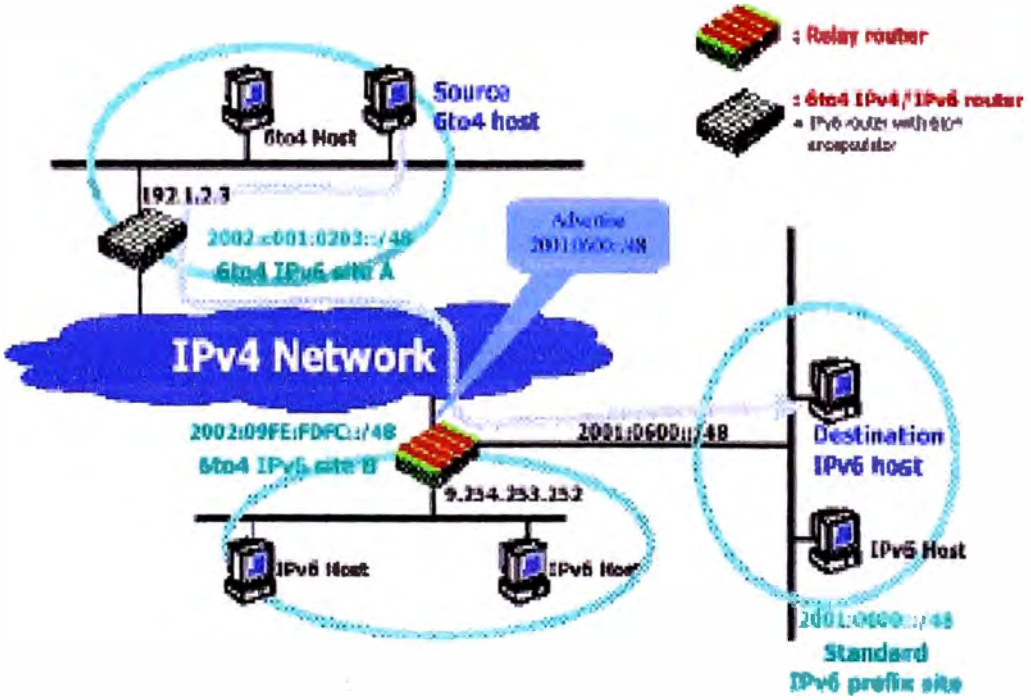


Fig 7.5: Escenario de Retransmisión

c) En el Gateway

c.2) NAT-PT/SIIT

Conceptos básicos

- Se utiliza para comunicaciones entre hosts que son sólo IPv6 e IPv4 respectivamente
- En realidad es NAT (se usa el mecanismo NAT para la asignación de la dirección IPv4) + el Protocolo de Traducción (se usa el mecanismo SIIT).
- Se realiza la traducción IPv4/IPv6 y se mantiene el estado mientras dura la sesión

Como funciona

- Traducción de direcciones
  - Utiliza el fondo de direcciones de IPv4, y mantiene la tabla de mapeado de la dirección IPv4/IPv6
- Protocolo de traducción IPv4 IPv6
  - Se usa SIIT (Stateless IP/ICMP Translation)
  - Provee de una regla de traducción de cabeceras entre IPv4< ---- >IPv6

c.2) Transport Relay (TRT)

Conceptos básicos

- TRT permite a hosts que son sólo IPv6 intercambiar tráfico (TCP, UDP) con hosts que son sólo IPv4
- n TRT localiza entre los hosts sólo IPv6 y los sólo IPv4

Cómo funciona

- Ventajas
  - No realiza modificaciones adicionales en los hosts imitadores de los sólo IPv6.
  - No hay que preocuparse por el problema de la fragmentación
- Desventajas
  - TRT sólo soporta tráfico bidireccional
  - TRT necesita un sistema declarado justo como el NAT
  - Se necesita código especial para retransmitir protocolos no amigables con NAT (como IPSec)

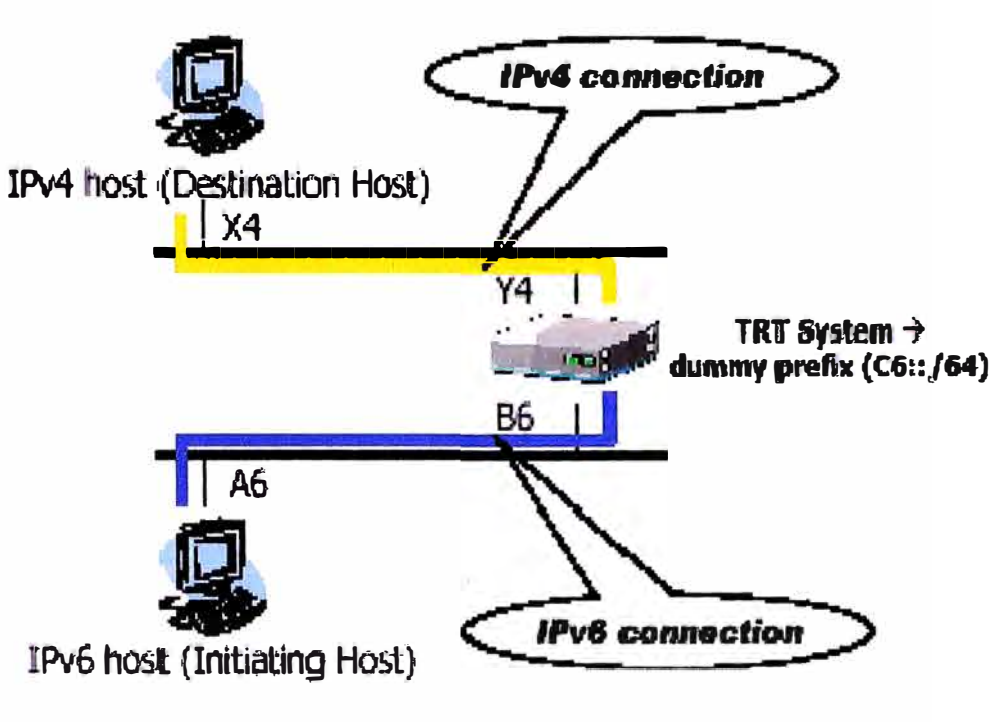


Fig 7.6 Ejemplo de operación con TRT

En el ejemplo descrito en la Figura 7.6 anterior , se realizan los siguientes pasos:

1. Reserva de un prefijo IPv6 el cual permite a los paquetes ser encaminados hacia el sistema TRT (prefijo ficticio)
2. Si la dirección IPv4 del host de destino es A.A.A.A y el prefijo ficticio es C6::/64, la dirección de destino es C6::A.A.A.A. así que, es encaminada a través del sistema TRT.
3. Luego, el sistema TRT investiga lo 32 bits más bajos de la dirección de destino (dirección IPv6 C6::A.A.A.A.) para obtener el destino real IPv4 (dirección IPv4 A.A.A.A). Después hace una conexión TCP/IPv4 de Y4 a X4, y envia el tráfico a través de las dos conexiones TCP.
4. Hay dos conexiones TCP. Una es TCP/IPv6 y la otra es TCP/IPv4, en la figura: De A6 a B6 (como C6::A.A.A.A), y de Y4 a X4.

7.3 Conclusiones

Podemos concluir que, en un entorno en el que convivan los protocolos IPv4 e IPv6, el uso exclusivo de las herramientas de transición presentadas en este capítulo, no es totalmente suficiente en la mayoría de los casos, y en algún caso totalmente imposible (TRT), debido a las características de definición del propio protocolo. Sin embargo, existen herramientas comerciales que pueden lograr la

convivencia en un entorno en el que coexisten IPv4 e IPv6, manteniendo un modelo de Servicios Diferenciados (DiffServ). Un ejemplo de esto, es la herramienta de 6WindGate, que en un entorno controlado, garantiza la obtención de estos servicios diferenciados.

CAPITULO VIII

LIMITACIONES

Directamente relacionado con este acápite, se encuentra el estudio del modelo del negocio que presenta los sgtes problemas de implantación Diffserv :

- Dentro del modelo de Servicios Diferenciados (DiffServ) , se necesita indicar que éste no asegura que los flujos de tráfico consigan determinados parámetros de QoS , como puede hacer ATM a través de circuitos. DiffServ permite agregados de tráfico por lo que nos ofrece cierta **probabalidad de QoS** , por lo que un proveedor puede integrar las conexiones pertenecientes a diferentes VPNs dentro de un mismo agregado , recibiendo todas ellas las mismas prestaciones a nivel de red. De esta manera, el tratamiento que recibirían podría ser diferente del que consiguen los usuarios con acceso gratuito a internet. Por otro lado, conseguir que el modelo DiffServ se ponga en funcionamiento requerirá un gran trabajo de ingeniería de red como un dimensionamiento adecuado para alcanzar determinado parámetros de QoS como puede ser un caudal o retardo asegurados.
- El modelo DiffServ no permite lograr QoS en la red de acceso. Cuando se refiere a QoS de extremo a extremo en DiffServ se hace referencia a QoS entre los routers extremos entre origen y destino. De todas manera la solución no presenta muchas dificultades ya que se supone que el usuario tienen mayor control sobre la red de acceso, quedando una responsabilidad en el dimensionamiento en manos del usuario final.
- Resulta bastante sintomático que en DiffServ , el principal beneficiario de la reserva de QoS será el destino, siendo el origen el que debe de pagar por conseguir el trato diferenciado de su tráfico.De ésta forma surgen conflictos en la descarga de audio streaming, donde el que pagaría será el servidor en lugar del usuario receptor.

- Para alcanzar nuestro destino en internet debemos de atravesar diferentes ISPs. De ésta forma el valor del byte DS puede ser modificado en cualquier equipo intermedio según las políticas de tráfico y diferentes contratos SLAs que tengan entre los diferentes ISPs. De ésta manera , una calidad extremo a extremo solo será alcanzada cuando los elementos involucrados (dominios DiffServ) actúen según las mismas políticas.
- Según el modelo DiffServ parece lógico que para alcanzar un destino más lejano resulte más caro que otro mas cercano donde se necesiten atravesar menos ISPs. Por lo tanto , el costo de enviar un paquete será diferente en función del camino que deba de atravesar, esto es una complicación al momento de ofrecer el servicio y costearlo. Pero éste mismo problema apareció en el nacimiento de Internet, donde también resultaba mas caro enviar un paquete cuanto mas ISPs tuviese que atravesar. Parece lógico pensar que de alguna manera nuestro proveedor de acceso a Internet nos cobrará adecuadamente teniendo en cuenta que los mensajes deberán ser tratados adecuadamente en los diferentes ISPs.
- En el modelo DiffServ , la reserva de QoS es unidireccional los paquetes ACK(aceptación) que viajan en sentido contrario tendrán el tratamiento normal (best-effort) , lo que podría llevar a la QoS final se limitase a la de los paquetes ACK (que limitan el manejo de la ventana de transmisión)
- El modelo DiffServ plantea algnos problemas al momento de decidir quien es el encargado de marcar la QoS en los paquetes. Si el usuario pudiera elegir el tratamiento adecuado, sería entonces necesario de modificar de alguna forma las aplicaciones y/o pila de protocolos.

CAPITULO IX

APLICACIONES Y/O SERVICIOS

En el modelo DiffServ , se pueden distinguir algunas aplicaciones y/o servicios :

9.1 Tele-inmersión:

Permite a usuarios en sitios geográficamente distantes colaborar en tiempo real en ambientes compartidos simulados como si estuvieran presentes en la misma habitación. Es la más completa síntesis de tecnologías mediáticas como reconstrucción de ambientes tridimensionales, tecnologías de proyección, despliegue y seguimiento y audio robótica con redes poderosas.

Los requerimientos de redes para sistemas de tele-inmersión, como gran ancho de banda, baja latencia y poca variación de ésta, la hacen una de las aplicaciones de redes mas complejas, convirtiéndola en la principal aplicación a investigar por la comunidad de Internet 2. ¿Cuales son las aplicaciones potenciales de tele-inmersión? pueden alterar de manera significativa los paradigmas en educación, ciencia y manufactura. Mostrarán su fuerza en los sistemas donde, acoplar objetos tridimensionales reconstruidos con objetos tridimensionales virtuales es vital para lograr con éxito ciertas tareas, algunas de las cuales no serían posibles sin tal combinación de información sensorial por ejemplo: CAD colaborativo y las aplicaciones médicas.

9.2 Laboratorios Virtuales:

Un laboratorio virtual es un ambiente distribuido y heterogéneo para solución de problemas, que permite a un grupo de investigadores, localizados alrededor del mundo, trabajar juntos en proyecto común. Como en cualquier otro laboratorio, las herramientas y técnicas dependen del dominio específico de la investigación.Sin embargo, los requerimientos de infraestructura básica son comunes a través de las distintas disciplinas. Aunque relacionado con tele-inmersión, un laboratorio virtual es posible sin tener un ambiente inmersivo compartido. Laboratorios virtuales han sido propuestos en disciplinas

como biología computacional, radio-astronomía , diseño de fármacos y ciencia de materiales.

9.3 Bibliotecas Digitales

No sólo son copias digitales de algunos libros y revistas, sino acervos que incluyen también video, sonido, mapas, etc., accesibles desde lugares distantes a través de la red, e integrados por los acervos de varias instituciones que colaboran entre sí. Internet 2 es estratégico para el avance de las bibliotecas digitales, ya que más allá de los prototipos actuales, la anchura de banda de telecomunicaciones, la reservación de canales, etc., son imprescindibles para alcanzar sus etapas avanzadas. Investigaciones recientes han mostrado todo lo que se puede hacer con el Internet existente para el desarrollo de sistemas de biblioteca digital. Aunque los sistemas actuales sufren de bajo rendimiento debido a problemas de la Internet, no se necesita un mayor ancho de banda, sólo que la red funcione bien, pero los problemas difíciles no tienen mucho que ver con la red (propiedad intelectual , modelos económicos viables).

Pero los nuevos servicios y capacidades de Internet 2 ofrecen oportunidades para mover a las bibliotecas digitales a nuevas áreas como datos, imágenes, vídeo y audio digitales, así como a los problemas de organizar y dar acceso a éstos materiales no textuales.

9.4 Instrucción Distribuída:

Hay muy poco software de instrucción de alta calidad para servir como base para la instrucción distribuida. Casi todo el que existe se ha diseñado para uso independiente, sobre todo el que utiliza imágenes, sonidos y vídeos. Internet 2 es una oportunidad de desarrollar una arquitectura para el desarrollo de aplicaciones en el aprendizaje colaborativo y su uso en la instrucción distribuida.

Para ello, se requieren tecnologías de componentes, pues permiten el desarrollo distribuido de los materiales. DSOM, Java, Active-X, OpenDoc son algunas de ellas, pero deben extenderse para que incorporen las funcionalidades requeridas y así lograr un sistema de administración instruccional (IMS) que debe permitir: establecer objetivos de aprendizaje, crear o revisar material educativo, determinar nivel del conocimiento del alumno, asignar materiales apropiados a los alumnos , dar acceso al alumno a los componetes o módulos instruccionales, revisar el progreso del alumno, manejo de comunicaciones estudiante-instructor y estudiante-estudiante y evaluar aprendizaje del alumno.

También serán de mucha utilidad

- Servicios basados en Pay Per View (Video sobre demanda) , canales de radio, canales de televisión , etc.
- Juegos on line
- Instrumentación remota.
- Aplicaciones espaciales
- Provisión de QoS extremo a extremo etc.

CONCLUSIONES

1. En la actualidad Internet necesita soportar múltiples aplicaciones y a cada una de éstas es necesario garantizarle un servicio de calidad por lo que se deduce que hay que implementar mecanismos que permitan brindar ésa Calidad de Servicio en función de no rebasar los límites establecidos para el retardo, variación en el retardo y pérdida de paquetes, parámetros importantes en toda aplicación.
2. La arquitectura de Servicios Diferenciados brinda un buen desempeño a las aplicaciones y es una alternativa viable para implementar redes con Calidad de Servicio cuando se tienen diferentes tipos de servicio en una red y existe congestión en los enlaces de salida, permitiendo a una red atender a un mayor número de usuarios y brindar más servicios a través de un solo enlace.
3. El modelo DiffServ no permite lograr calidad de servicio en la red de acceso. Cuando se habla de QoS extremo a extremos con DiffServ se hace referencia a QoS entre los routers extremos origen y destino
4. Clasificando los paquetes en los bordes en distintas clases, se pueden proveer servicios diferenciados a los paquetes sin tener que examinar cada uno en detalle en cada salto. Después de ser marcados una vez mediante precedencia IP o DSCP, mecanismos de manejo y evasión de congestión pueden actuar sobre ellos a medida que circulan por la red
5. Una calidad extremo a extremo solo será alcanzable cuando todos los elementos involucrados en la cadena (Dominios DiffServ) actuén según las mismas políticas.
6. Mientras dure la migración IPv4 a IPv6, existen herramientas comerciales que pueden lograr la convivencia en un entorno en que coexistan IPv4 e IPv6, manteniendo un modelo de Servicios Diferenciados
7. IPv6 utiliza los mismos conceptos involucrados con Servicios Diferenciados, por lo que el despliegue de QoS para éstos ambientes es muy estable, por lo que tiene algunos años de depuración.

RESUMEN DE ACRONIMOS

AAA Authentication Authorisation Accounting

AAAARCH Authentication Authorisation Accounting ARCHitecture

AF Assured Forwarding

ASM Application Specific Module

BA Behaviour Aggregate

BE Best-Effort

DS Differenciated Services

DSCP DiffServ Code Point

DWDM Dense Wavelength Division Multiplexing

EF Expedited Forwarding

FIFO First In, First Out

GPS General Processsor Sharing

HOL Head Of Line

ICMP Internet Control Message Protocol

IETF Internet Engineering Task Force

IP Internet Protocol

IRTF Internet Research Task Force

ISP Internet Service Provider

PDB Per Domain Behaviour

PHB Per-Hop-forwarding Behaviour

RED Random Early Detection

RIO RED Input Output

RTT Round Trip Time

SLA Service Level Agreement

SLS Service Level Specification

WFQ Weighted Fair Queuing

WRED Weighted RED

BIBLIOGRAFIA

1. IETF. DiffServ Working Group: www.ietf.org/html.charters/diffserv-charter.html

2. R. BRADEN, D. CLARK and S. SHENKER: IETF RFC 1633: Referencias Integrated Services in the Internet Architecture: an Overwiew. June 1994.

3. K. MCCLOGHRIE and F. KASTENHOLZ: IETF RFC 2233: The Interfaces Group MIB using SMIv2. November 1997.

4. S. BLAKE, D. BLACK, M. CARLSON, E. DAVIES, Z.WANG and W.WEISS: IETF RFC 2475: An Architecture for Differentiated Services. December 1998.

5. S. BOEYEN, T. HOWES and P. RICHARD: IETF RFC 2587: Internet X.509 Public Key Infrastructure LDAPv2 Schema. June 1999.

6. J. HEINANEN, F. BAKER,W. WEISS and J.WROCLAWSKI: IETF RFC 2597: Assured Forwarding PHB Group. June 1999.

7. V. JACOBSON, K. NICHOLS and K. PODURI: IETF RFC 2598: An Expedited Forwarding PHB. June 1999.

8. J. HEINANEN and R. GUERIN: IETF RFC 2697: A Single Rate Three Colour Marker. September 1999.

9. J. HEINANEN and R. GUERIN: IETF RFC 2698: A Two Rate Three Colour Marker. September 1999.

10. K. NICHOLS and B. CARPENTER: IETF RFC 3086: Definition of Differenciated Services Per Domain Behaviours and Rules for their Specification. April 2001.