ESCUELA POLITÉCNICA DEL EJÉRCITO

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Análisis y definición de un mecanismo basado en servicios diferenciados para ofrecer calidad de servicio en redes IP

Previa a la obtención del Título de:

Ingeniera de Sistemas e Informática

POR: Verónica Anabell Calvache Alvarez

SANGOLQUÍ, 24 de Abril del 2007

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por la Srta. VERÓNICA ANABELL CALVACHE ÁLVAREZ como requerimiento parcial a la obtención del título de INGENIERA DE SISTEMAS E INFORMÁTICA

Sangolquí, 24 de Abril del 2007
Fecha

_____
ING. Hugo Montesdeoca
PROFESOR DIRECTOR

DEDICATORIA

A mis padres por su amor, esfuerzo y comprensión durante toda mi vida, porque siempre han estado ahí para escucharme, apoyarme y ayudarme; ante todo han sido mis amigos incondicionales y me han enseñado que no existen obstáculos ni excusas para alcanzar mis sueños y cumplir mis metas.

Verónica Calvache A.

AGRADECIMIENTOS

A Dios por mi familia, por todas sus bendiciones y su protección.

A mi padre, mi amigo, mi maestro y mi compañía en todo momento, por estar ahí cuando lo he necesitado, por enseñarme que solo con responsabilidad y esfuerzo podemos alcanzar nuestras metas.

A mi madre, mi amiga y mi confidente, quien ha dedicado su vida a cuidarnos y velar por nosotros, gracias por todos sus consejos y ayuda, por su ejemplo y empeño.

A mis hermanos, Evy y Chalito, compañeros en los buenos y malos momentos, por toda su ayuda y cariño.

A Andrés, por todo este tiempo juntos, por su comprensión y ayuda.

Al Ing. Hugo Montesdeoca, por su ayuda en la ejecución de este proyecto.

A la Ing. Lourdes De la Cruz, por su ayuda en la ejecución de este proyecto.

Al Ing. Andrés de la Torre, por toda su ayuda.

Verónica Calvache A.

HOJA DE LEGALIZACION DE FIRMAS

ELABORADO POR

_____

Verónica Calvache

COORDINADOR DE LA CARRERA DE SISTEMAS E INFORMÁTICA

_____

Ing. Ramiro Delgado

Lugar y fecha: Sangolquí, 24 de Abril del 2007

Índice de contenidos

Listado de figuras

Listado de tablas

Listado de fórmulas

Listado de anexos

RESUMEN

Las redes IP ofrecen un entorno multi - servicios que permite la integración de voz, video y datos en una sola red (basada en IP) y garantiza el funcionamiento adecuado de las aplicaciones de acuerdo a sus requerimientos a través de la implementación de mecanismos QoS que administren los parámetros de calidad como: ancho de banda, retardo, jitter y pérdida de paquetes, con lo que se asegura la continuidad en las comunicaciones y la disponibilidad de la información, se entrega un tratamiento diferenciado a las aplicaciones y se evita y/o administra la congestión, sin embargo dicha implementación debe realizarse extremo a extremo, tanto en las premisas de las empresas como en las nubes de los proveedores de servicios de Internet y debe existir un interwoking entre ellas.

El IETF define dos modelos QoS extremo a extremo, IntServ, que realiza previamente la reserva de los recursos en cada dispositivo de la red a lo largo de la trayectoria a través del protocolo RSVP y DiffServ, que marca los paquetes a través del campo DSCP y en función de dicho marcado, los paquetes reciben un tratamiento particular en cada elemento de la red, además diferencia entre las funciones del borde y del núcleo de la red.

El mecanismo propuesto para ofrecer QoS en redes IP consta de las siguientes fases: identificación del tráfico y sus requerimientos, división del tráfico en clases de servicio, definición de las políticas QoS para cada clase, pruebas de las políticas QoS, implementación de las políticas y monitoreo y ajuste.

ACRÓNIMOS

AAA	Authentication, Authorization, Accounting
AAAC	Authentication, Authorization, Accounting, Charging, Autenticación, Autorización, Contabilidad y Facturación
ABR	Available Bit Rate
AF	Assured Forwarding
AR	Router de acceso
ATM	Asyncronuos Transfer Mode, Modo de transferencia asíncrona
BA	Behaviour aggregate, Comportamiento agregado
BB	Bandwidth Broker
BE	Best Effort, Mejor esfuerzo
BECN	Backward Explicit Congestion Notification
BER	Bit Error Rate, Índice de error de bit
BGP	Border Gateway Protocol
BK	Background
BR	Border routers, Routers limítrofes
BWP	BandWidth Proportion
CAC	Call Admission Control, Control de admisión de llamadas
CBQ	Class-Based Queuing
CBR	Constant Bit Rate
CDV	Cell Delay Variation
CER	Cell Error Rate
CIDR	Classless InterDomain Routing
CIR	Committed Information Rate, Tasa de información comprometida

CL	Controlled Load
CLR	Cell Loss Ratio
CMR	Cel – Misinsertion Rate
COPS	Common Open Policy Service
CoS	Class of Service, Clases de servicio
CPE	Customer premises equipment, Equipo en las premisas del cliente
CPU	Central Process Unit, Unidad central de procesamiento
CR	Core routers, Routers del núcleo
CR – LDP	Constrained Routing - Label Distribution Protocol
CS	Class Selector
CTD	Cell Transfer Delay
CU	Currently Unused, No usado actualmente
CVC	Circuitos Virtuales Conmutados
DE	Discard Eligibility
DF	Don't Fragment, No fragmentar
DiffServ	Differentiated Services, Servicios Diferenciados
DNS	Domain Name Service / Domain Name Server
DORA	Dynamic Online Routing Algorithm
DRR	Deficit Round Robin
DS	Differentiated Services
DSBM	Designated Subset Bandwidth Manager
DSCP	Differentiated Service Code Point, Punto de código de Servicios Diferenciados
DTE	Data Terminal Equipment, Equipo terminal de datos
ECN	Explicit Congestion Notification

EE	Excellent Effort
EF	Expedited Forwarding
EH	Extension Headers
ER	Edge Routers, routers del borde
ERP	Enterprise Resource Planning, Planeamiento del recurso de la empresa
FC	Flag Copy
FDDI	Fiber Distributed Data Interface
FEC	Forwarding Equivalency Class
FECN	Forward Explicit Congestion Notification
FIFO	First In First Out, Primero en entrar, primero en salir
Flow Spec	Flow Specification, Especificación del flujo
FQ	Far Queuing
FTP	File Transfer Protocol, Protocolo de transferencia de archivos
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IHL	Internet Header Lenght, Longitud de la cabecera Internet
IntServ	Integrated Services, Servicios Integrados
IP	Internet Protocol, Protocolo de Internet
IPng	IP Next generation, IP nueva generación
IPv4	IP versión 4
IPv6	IP versión 6

ISP	Internet Service Provider, Proveedor de Servicios de Internet
ISSLL	Servicios Integrados sobre Capas de enlace específicas
LAN	Local Area Network, Redes de área local
LDP	Label Distribution Protocol, Protocolo de distribución de etiquetas
LER	Label Edge Routers
LLQ	Low Latency Queuing
LSP	Label Switching Path
LSR	Label Switching Routers
MAC	Media Access Control, Control de acceso al medio
MAN	Metropolitan Area Network, Redes de área metropolitana
MBZ	Must Be Zero, Debe ser cero
MF	More Fragments, Más fragmentos
MF	Multi – field, Multi campo
Modelo OSI	Open System Interconnection, Modelo de interconexión de sistemas abiertos
MPLS	Multi - Protocol Label Switching
MPOA	Multi - Protocol Over ATM, Multi – protocolo sobre ATM
MQC	Modular QoS Commandline Interface
MTU	Maximun Transmission Unit, Unidad de transmisión máxima
NC	Network control, Control de la red
NIC	Network Interface Card, Tarjeta de interface de red
Nrt – VBR	Non real time VBR
OSPF	Open Shortest Path First
P2P	Peer to peer, Punto a punto
PBR	Policy Based Routing

PDB	Per Domain Behavior, Comportamiento por dominio
PDP	Policy Decision Point, Punto de decisión de políticas
PEP	Policy Enforcement Points
PHB	Per Hop Behavior, Comportamiento por salto
Policing	Gestión de políticas
POS	Point of Sales, Punto de ventas
PPV	Path potencial value, Valor potencial de la trayectoria
PQ	Priority Queuing
PVC	Permanent Virtual Circuit, Circuitos Virtuales Permanentes
QCS	QoS Customer Server, Servidor QoS del cliente
QNS	QoS Network Server, Servidor QoS de la red
QoS	Quality of Service, Calidad de servicio
Queuing	Gestión de colas
RA	Router de acceso
RED	Random Early Detection
RFC	Request for comments
RR	Round Robin
RSPEC	Request SPECification
RSVP	Resource Reservation Protocol, Protocolo de reservación de recursos
RSVP – E2E	Resource Reservation Protocol – End to End, Protocolo de reservación de recursos – extremo a extremo
RSVP – TE	RSVP Tunneling Extensions
RT	Real time, Tiempo real
rt – VBR	Real time VBR

RTP	Real Time Protocol, Protocolo de tiempo real
SBM	Subset Bandwidth Manager
Scheduling	Planificación – Estrategias de servicio de colas
SDH	Synchronous Digital Hierarchy, Jerarquía Digital Sincrónica
SIP	Session Initiation Protocol, Protocolo de iniciación de sesión
SIT	Simple Internet Transition
SLA	Service Level Agreement, Acuerdo de nivel de servicios
SNMP	Simple Network Management Protocol
SPF – TE	Shortest Path First with Traffic Engineering
SWPF	Shortest Widest Path First
TCA	Traffic Conditioning Agreement, Acuerdo de condicionamiento de tráfico
TCP	Transmission Control Protocol, Protocolo de control de la transmisión
TE	Traffic Engineering, Ingeniería del tráfico
TOS	Type of Service, Tipo de Servicio
TSPEC	Traffic SPECification
TTL	Time to Live, Tiempo de vida
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
UIT	Unión Internacional de Telecomunicaciones
VBR	Variable Bit Rate
VC	Virtual Circuit, Circuito Virtual
VI	Video
VLAN	Virtual Local Area Network, Red de área local virtual

VO	Voz
VoIP	Voice over IP, Voz sobre IP
VPN	Virtual private network, Redes virtuales privadas
VPT	VLAN Priority Tags, Etiquetas de prioridad VLAN
WAN	Wide Area Network, Redes de área extendida
WFQ	Weight Far Queuing
WRED	Weighted Random Early Detection
WRR	Weighted Round Robin
WSPF	Widest Shortest Path First

CAPÍTULO I

1. INTRODUCCIÓN

1.1. PLANTEAMIENDO DEL PROBLEMA

La Calidad de Servicio consiste en un conjunto de tecnologías que permiten a las aplicaciones de red, solicitar y recibir niveles de servicio basados en parámetros tales como: velocidad de transmisión, nivel de retardo, rendimiento, porcentaje de pérdida de paquetes; contribuyendo así a la mejora del servicio que se brinda a los usuarios de la red IP.

Durante los últimos años, han surgido varios mecanismos para ofrecer a las redes IP Servicio de Calidad (QoS), los cuales proveen un servicio mejorado a los usuarios de dicha red y al mismo tiempo proporcionan un conjunto de herramientas que permiten administrar el uso de recursos de red de una forma controlada y eficaz.

Estos mecanismos incluyen tanto mecanismos de control del tráfico como mecanismos de provisión y configuración. Los mecanismos de control del tráfico incluyen algoritmos de cola y clasificación de paquetes. Éstos se pueden aplicar a acumulaciones de tráfico o a flujos de tráfico por conversación. Los mecanismos de provisión y configuración pueden ser de arriba a abajo o con señalización de host. La provisión de arriba a abajo presenta ciertas dificultades en la clasificación del tráfico y suele ser insuficiente para ofrecer de forma simultánea garantías de

alta calidad y un uso eficaz de los recursos de red (producto de alta calidad / eficacia). La señalización basada en host ofrece información a la red que facilita en gran medida la relación de los recursos de red con aplicaciones y usuarios específicos y permite al administrador de la red realizar un producto mejorado, cuando sea oportuno. Los puntos de decisión de políticas proporcionan una administración unificada de los mecanismos de QoS.

En la actualidad las empresas requieren que a través de una sola infraestructura tecnológica se transporten todas sus aplicaciones sin que esto afecte tanto sus requerimientos como su funcionamiento y que suponga un elevado costo en su implementación, además se debe considerar la adaptabilidad de dicha red a cambios e introducción de nuevas aplicaciones y la simplicidad en su administración; dado lo anterior se necesita aplicar políticas de calidad de servicio que satisfagan dichas necesidades; sin embargo, no existe un mecanismo específico basado en Servicios Diferenciados (DiffServ), que sea capaz de proveer un mejor servicio a las aplicaciones, al mismo tiempo que frene el ritmo al que es necesario aumentar la capacidad de la correspondiente Red IP; además, aún no se superan los inconvenientes y desventajas de otros mecanismos utilizados.

1.2. JUSTIFICACIÓN

Normalmente las redes trabajan con la filosofía del mejor esfuerzo: cada usuario comparte ancho de banda con otros, por lo tanto, la transmisión de sus datos concurre con las transmisiones de los demás usuarios. Los datos empaquetados son encaminados de la mejor forma posible, conforme las rutas y

bandas disponibles. Cuando hay congestión, los paquetes son descartados sin distinción, por esto no hay garantía que el servicio sea realizado con éxito; mientras, aplicaciones como voz sobre IP y videoconferencia necesitan de tales garantías.

Un modelo QoS describe un conjunto de capacidades QoS extremo a extremo para entregar el servicio requerido por ciertos tipos de tráfico de red. Con la implantación de la Calidad de Servicio (QoS), es posible ofrecer más garantía y seguridad para las aplicaciones avanzadas, una vez que el tráfico de estas aplicaciones pasa a tener prioridad en relación con las aplicaciones tradicionales.

Con el uso de la Calidad de Servicio, los paquetes son marcados para distinguir los tipos de servicios y los routers son configurados para crear colas distintas para cada aplicación, de acuerdo con las prioridades de las mismas, así, una parte de ancho de banda, dentro del canal de comunicación, es reservada para que, en el caso de congestión, determinados tipos de flujos de datos o aplicaciones tengan prioridad en la entrega.

Existen distintos mecanismos para garantizar la Calidad de Servicio en las Redes IP, entre los que tenemos: IntServ (Servicios Integrados), basado en la utilización de algún protocolo de reserva (RSVP, Resource ReSerVation Protocol) que permite la reserva de recursos a lo largo de los routers implicados en la comunicación y DiffServ (Servicios Diferenciados), basado en la idea de que la información sobre calidad de servicio se escribe en los datagramas, no en los routers, es decir que divide el tráfico en diferentes clases y asigna prioridades a

estos agregados. Utiliza diferente información de la cabecera de los paquetes (por ejemplo, DSCP – DiffServ Code Point) para distinguir, clasificar los paquetes y conocer el tratamiento que debe recibir el tráfico en los nodos de la red. La diferencia fundamental con IntServ es que éste no permite implementar una calidad de servicio escalable a cualquier cantidad de flujos.

Debido a lo mencionado es necesario el análisis de los mecanismos existentes encargados de proporcionar calidad de servicio en redes IP; de manera que se pueda proponer un mecanismo alternativo basado en servicios diferenciados que proporcione las funcionalidades requeridas para ofrecer calidad de servicio a estas redes.

Con dicho análisis y definición se pretende proveer un mecanismo de QoS, con capacidad adecuada para satisfacer las necesidades de comunicación entre los diferentes usuarios de la red IP, la administración de los recursos de red y el uso apropiado de las diferentes aplicaciones y servicios.

La definición de esta propuesta se considera de gran importancia; sin embargo las pruebas correspondientes previas a su implementación requieren equipos de trabajo con grupos de aproximadamente diez personas, en los que se realizan estudios sobre todos los tipos de tráfico y casos que se pueden presentar en la red IP, los cuales pueden durar varios años; por lo que este proyecto no considera la realización de pruebas o algún tipo de implementación.

1.3. OBJETIVOS

1.3.1. Objetivo General

Proponer un mecanismo alternativo basado en Servicios Diferenciados que optimice el uso de los recursos de las Redes IP y soporte los servicios que posean necesidades cualitativas específicas.

1.3.2. Objetivos Específicos

- Analizar los parámetros relacionados con los elementos que afectan el rendimiento de una red.

- Describir los modelos QoS extremo a extremo y los correspondientes mecanismos empleados para proporcionar calidad de servicio.

- Comparar las ventajas del modelo de Servicios Diferenciados con respecto a otros mecanismos.

- Establecer el modelo de funcionamiento del nuevo mecanismo.

- Determinar el algoritmo de funcionamiento del nuevo mecanismo planteado.

1.4. ALCANCE

En el Análisis se determinarán las características y ventajas de las redes IP, las características, funcionamiento y parámetros tomados en cuenta para ofrecer calidad de servicio, la calidad de servicio en redes ATM, Frame Relay e IP y la importancia de la calidad de servicio en las redes IP; además se establecerán los principales mecanismos empleados para brindar calidad de servicio en dichas redes, haciendo énfasis en la arquitectura y funcionamiento del modelo QoS extremo a extremo definido como DiffServ (Servicios Diferenciados), de manera que se pueda determinar las condiciones requeridas y beneficios obtenidos al emplear dicho modelo.

La definición de un mecanismo alternativo basado en Servicios Diferenciados, en el que se incluya el planteamiento y funcionamiento del algoritmo, la arquitectura, características y beneficios del nuevo mecanismo.

Solo se considera el planteamiento de un nuevo mecanismo debido a que las pruebas e implementación de los mecanismos empleados para calidad de servicio requieren de mayor tiempo y la formación de equipos de trabajo que examinen a detalle el funcionamiento del algoritmo en cada caso que pudiera presentarse en la red IP, considerando aspectos como la velocidad del enlace en el cliente y en la nube del proveedor de servicios, la tecnología de acceso, las aplicaciones y sus prioridades, los cambios en dichas aplicaciones o su prioridad, los dispositivos empleados en el cliente y el proveedor de servicios, así como su configuración, entre las principales.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. GENERALIDADES DE LAS REDES

2.1.1. Definición de red

Es un conjunto organizado de recursos, que proporcionan las vías de comunicación necesarias para establecer la interconexión de dispositivos, permitiendo la transmisión de información del origen al destino[1], además proporciona la facilidad de[2]:

- Compartir recursos: archivos e impresoras.
- Intercambiar información.
- Establecer comunicaciones remotas.
- Aprovechar las prestaciones cliente / servidor.

2.1.2. Estructura de red

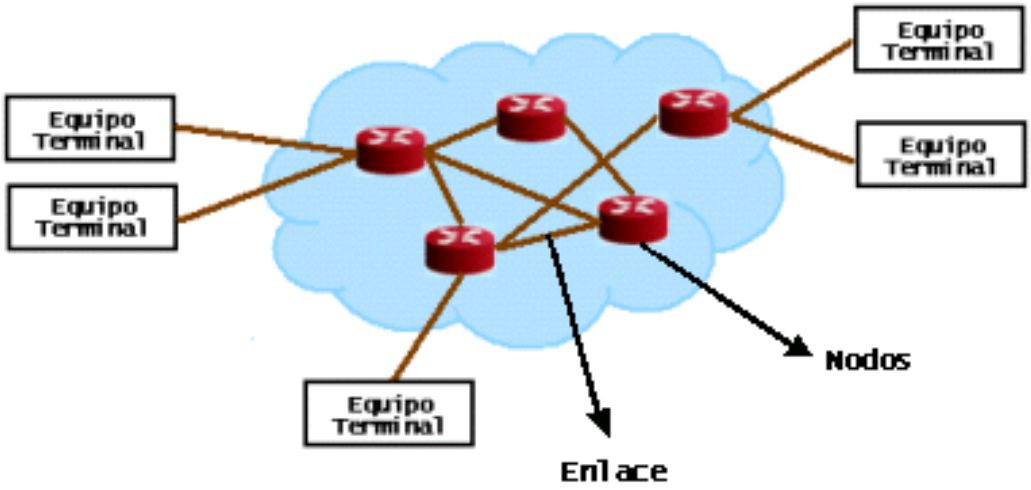


Figura 2.1: Estructura de una red

En la figura 2.1 se aprecia los elementos principales que componen una red[3], que son:

a) Nodo o Terminal: es un elemento capaz de iniciar o terminar una comunicación; físicamente es cualquier tipo de dispositivo de red como un computador.

b) Enlace: corresponde a los medios de transmisión por los cuales se pueden comunicar los nodos.

2.1.3. Clasificación de las redes

2.1.3.1. Basadas en la arquitectura de red y en la técnica de transferencia de la información

2.1.3.1.1. Redes de difusión

Como se observa en la figura 2.2, tienen un canal de comunicación al cual están conectados todos los usuarios, quienes pueden recibir todos los mensajes, pero solamente extraen del canal los mensajes en los que identifican su dirección como destinatarios[4]. Al recibir el paquete, la máquina verifica el campo de dirección, si el paquete esta dirigido a ésta, lo procesa; si está dirigido a otra máquina lo ignora.

Las redes de difusión también ofrecen la posibilidad de dirigir un paquete a todos los destinatarios colocando un código especial en el campo de dirección. Cuando se transmite un paquete con este código, cada máquina en la red lo recibe y lo procesa, este modo de operación se llama: broadcast. Algunos sistemas de difusión también contemplan la transmisión a un subconjunto de máquinas, lo que se conoce como multicast[5].

Los usuarios no pueden transmitir información en todas las redes, por ejemplo, en televisión o radiodifusión, los usuarios son pasivos, es decir, únicamente reciben la información que transmiten las estaciones transmisoras,

mientras que, en telefonía, todos los usuarios pueden recibir y transmitir información. Ejemplos de redes de difusión son:

- Comunicación por radio.
- Comunicación por satélite.
- Comunicación en una red local.

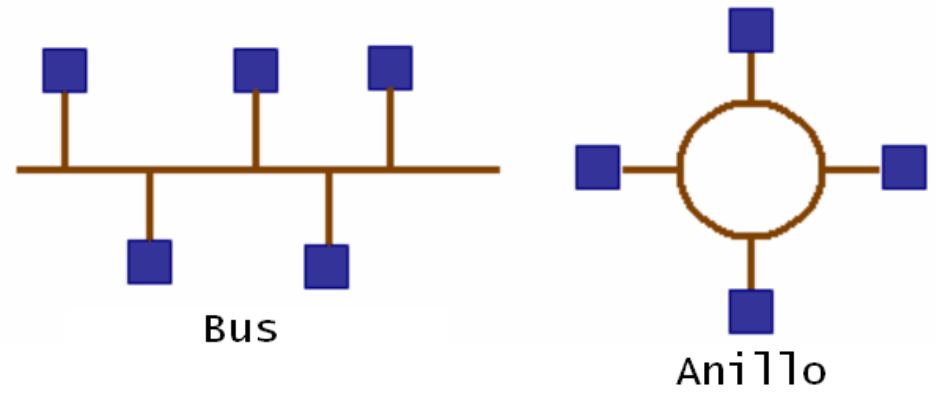


Figura 2.2: Redes de difusión

2.1.3.1.2. Redes Conmutadas

La conmutación es la conexión física o lógica de un camino de entrada al nodo con un camino de salida del nodo, con el fin de transferir la información del primer camino al segundo, permitiendo el uso eficiente de los enlaces.

Las redes conmutadas consisten en un conjunto de nodos interconectados entre sí, a través de medios de transmisión, formando la mayoría de las veces una topología en malla, donde la información se transfiere encaminándola del nodo origen al nodo destino mediante conmutación entre nodos intermedios[2], como se muestra en la figura 2.3. Una transmisión de este tipo tiene 3 fases:

a) Establecimiento de la conexión.

b) Transferencia de la información.

c) Liberación de la conexión.

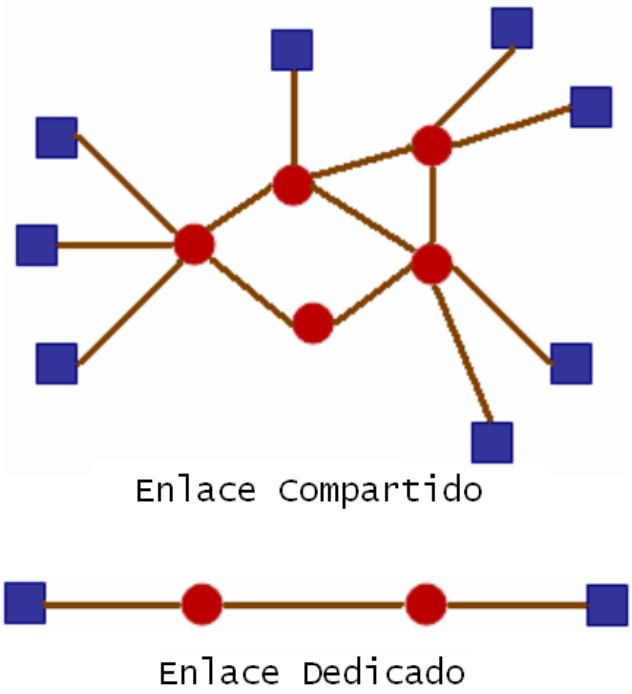


Figura 2.3: Redes conmutadas

Existen dos técnicas de conmutación para establecer la comunicación entre dos nodos de una red:

1. **Conmutación de circuitos**

Esta técnica es la más antigua y consiste en establecer un circuito de comunicación dedicado entre dos nodos; mientras dura la conexión, los recursos del circuito no están disponibles para otros usuarios, como se observa en la figura 2.4[6]. La red telefónica es un ejemplo de este tipo de conmutación.

Entre los problemas de esta técnica tenemos:

- Pérdida de capacidad, dado que casi ninguna transmisión usa el 100% del circuito todo el tiempo.
- Pérdida de la conexión si el circuito falla en medio de una transmisión, por lo que se debe establecer una conexión nueva.

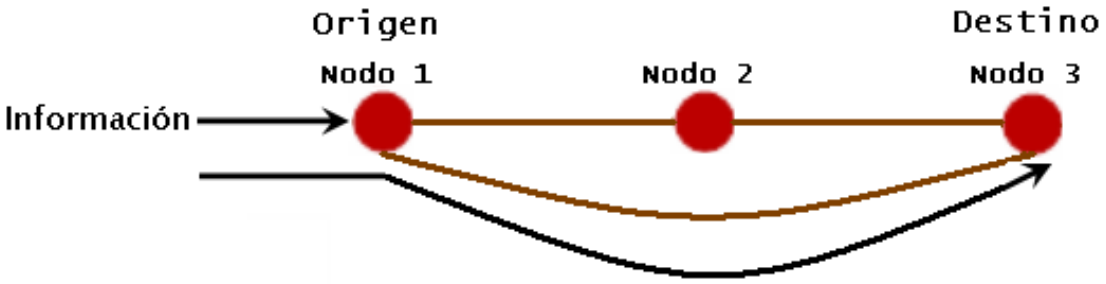


Figura 2.4: Conmutación de circuitos

2. Conmutación de paquetes

En la figura 2.5[6] se especifica el funcionamiento de la conmutación de paquetes, donde los datos son divididos en unidades de información, llamadas paquetes, que son encaminados a través de la red y cada nodo intermedio determina a donde va el paquete de acuerdo a la dirección destino que se encuentra en el encabezado del mismo.

Un paquete no necesita ser enrutado sobre los mismos nodos que otros paquetes relacionados. De esta forma, los paquetes enviados entre dos dispositivos de red pueden ser transmitidos por diferentes rutas, en el caso de que

se caiga un nodo o no funcione adecuadamente. Esta técnica es empleada por las redes basadas en IP.

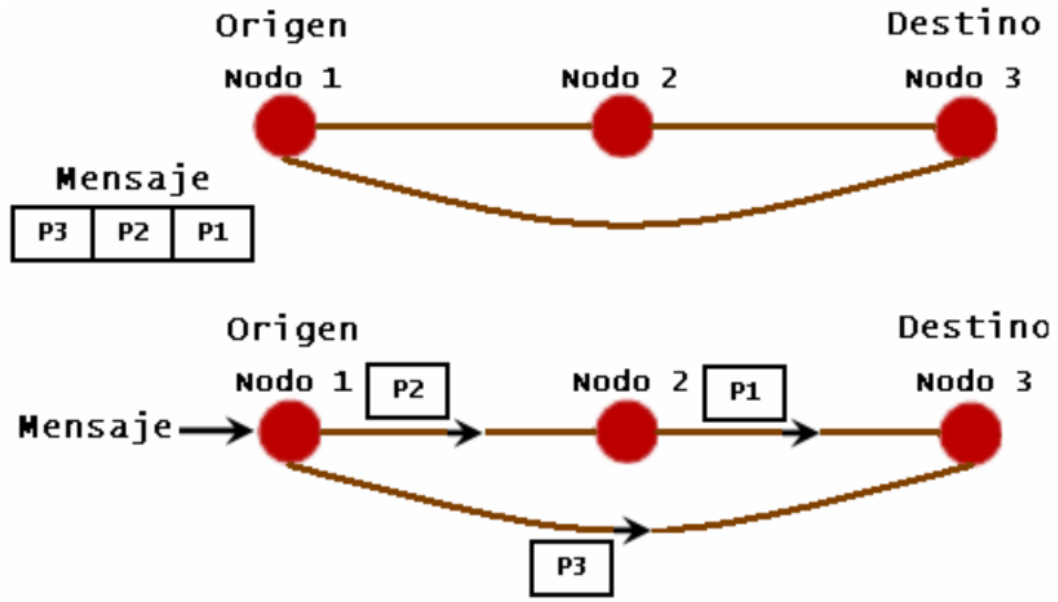


Figura 2.5: Conmutación de paquetes

2.1.3.2. Según el alcance

Una característica importante de una red es su cobertura, ya que ésta limita el área en que un usuario puede utilizar los servicios que le ofrece. Podemos diferenciar las siguientes redes:

2.1.3.2.1. Redes de área local (LAN)

Su corto alcance permite únicamente conectar dispositivos de un mismo edificio. Éstas son mantenidas y administradas por el mismo propietario de la red.

2.1.3.2.2. Redes de área metropolitana (MAN)

Permiten conectar equipos de cómputo a través de líneas privadas o públicas que son propiedad de alguna empresa privada o gubernamental como compañías telefónicas o de televisión por cable. Utilizan protocolos para redes de área local y son administradas y mantenidas por la compañía dueña de las líneas.

2.1.3.2.3. Redes de área extendida (WAN)

Conectan equipos distantes entre sí, su alcance es de kilómetros, típicamente de alcance global. Este tipo de redes no tienen un administrador en particular, más bien son mantenidas por los mismos usuarios quienes prestan sus recursos para conectar redes privadas con el resto del mundo.

2.1.4. Protocolos orientados y no orientados a conexión

2.1.4.1. Orientados a conexión

Se establece una conexión entre los nodos que desean transmitir la información, en este caso se mantiene la información del estado de la conexión, en la que se incluye: control de error (combinación de reconocimiento, detección y corrección de error), control de secuencia (habilidad de cada nodo para reconstruir una serie de mensajes recibidos en el orden apropiado) y control de flujo (habilidad para que ambas partes en un diálogo eviten el sobreflujo de mensajes entre sí) entre los nodos; es decir, el nodo destino notificará al nodo

origen si la información llegó correctamente, si no es así le pedirá que se proceda con la retransmisión. Las fases de los protocolos orientados a conexión son:

a) **Configuración de la conexión:** los nodos correspondientes establecen la conexión y negocian los parámetros que definen la conexión.

b) **Transferencia de datos:** los nodos correspondientes intercambian mensajes (información útil) bajo el amparo de la conexión.

c) **Liberación de la conexión:** ambos nodos acuerdan terminar la conexión.

2.1.4.2. No orientados a conexión

Pasan directamente del estado libre al modo de transferencia de datos, puesto que no toman en cuenta las fases restantes de configuración y liberación de una conexión. No ofrecen confirmaciones, control de flujo y secuencia ni recuperación de errores aplicables a la red.

2.2. REDES IP

2.2.1. Definición

Una RED IP:

- ✓ Es una red multi - servicios, es decir, transmite voz, datos y video.

- ✓ Se basa en la tecnología IP, la cual permite ofrecer servicios diferenciados de acuerdo a la calidad de servicio demandada por las aplicaciones del cliente.

- ✓ Se orienta hacia el uso óptimo del ancho de banda.

2.2.2. Protocolo IP

Es el protocolo de red más popular del mundo, el cual permite que se transmitan los datos a través y entre redes, de ahí su nombre, Inter - net Protocol (protocolo entre redes).

El Protocolo Internet fue diseñado para proporcionar el servicio “best – effort” (mejor esfuerzo: lo más posible, lo antes posible), mediante el cual cada usuario comparte ancho de banda con otros, por lo tanto, la transmisión de sus datos concurre con las transmisiones de los demás usuarios. Los datos empaquetados son encaminados de la mejor forma posible, conforme las rutas y bandas disponibles y cuando hay congestionamiento, los paquetes son descartados sin distinción por lo que no existe garantía de que el servicio sea realizado exitosamente.

Esta filosofía permite la entrega de los paquetes de datos y el funcionamiento en cualquier medio de transmisión y plataforma, de ahí que su popularidad haya cambiado el paradigma de "IP sobre todo," a "Todo sobre IP"; para manejar la multiplicidad de aplicaciones tales como vídeo, Voz sobre IP

(VoIP), comercio electrónico, el planeamiento del recurso de la empresa (ERP), y otras.

IP es un protocolo del tercer nivel (Red) del Modelo OSI (Open System Interconnection), su función es hacer lo mejor que se pueda para entregar un datagrama al host destino, puesto que no se garantiza la entrega fiable de los datagramas, los cuales se pueden destruir en el camino debido a[7]:

- Errores en los bits durante la transmisión por el medio.
- Descarte del datagrama debido a la falta de espacio en el buffer de un router congestionado.
- Temporalmente, no se cuente con un camino hasta el destino.

2.2.2.1. Datagrama IP

Es la unidad de datos creada por IP, que transporta los datos por la red a través de rutas aleatorias de manera independiente unas de otras.

2.2.2.1.1. Formato del datagrama IP

En la Figura 2.6 se indica el formato del datagrama IP, que está constituido por palabras de 32 bits y contiene los datos propios del mensaje y además incorpora una cabecera, en la que se especifica el origen, destino y otra información acerca de los datos.

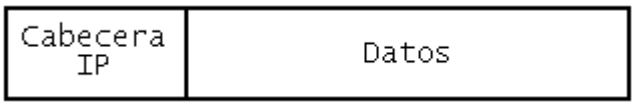


Figura 2.6: Datagrama IP

La Figura 2.7 muestra el formato de la cabecera IP[8], que está formada por 20 bytes y puede llegar como máximo a 60 bytes si se incluye información en el campo Opciones y Relleno.

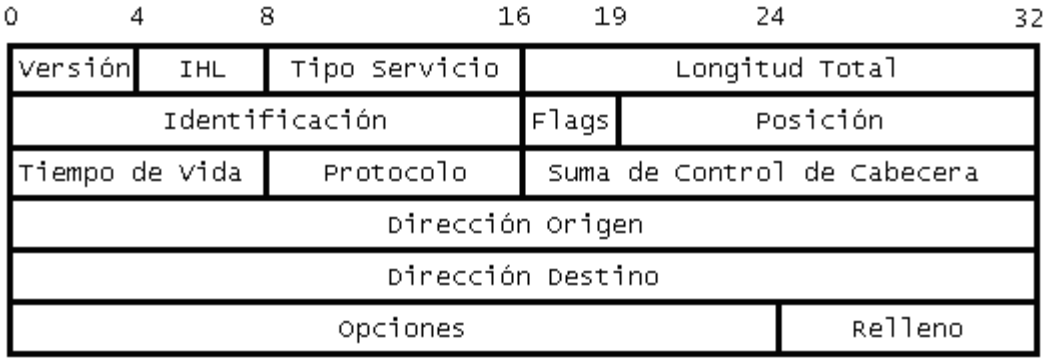


Figura 2.7: Cabecera del datagrama IP

A continuación se presentan los campos de la cabecera del datagrama IP[8]:

- **Versión (4 bits):** indica la versión del protocolo IP. La versión actual es 4.

- **IHL (4 bits):** Longitud de la cabecera Internet, es la longitud de la cabecera en palabras de 32 bits y apunta al comienzo de los datos.

- **Tipo de Servicio (8 bits):** conocido como TOS, proporciona una indicación de los parámetros de calidad de servicio deseada, en la figura 2.8, se especifican los campos de este byte[9].

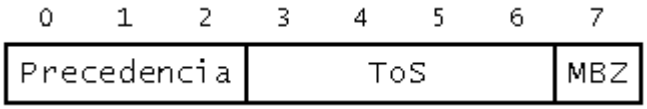


Figura 2.8: Campos de TOS

- **Precedencia (3 bits):** indica la prioridad del datagrama.

  000 = Rutina

  001 = Prioridad

  010 = Inmediato

  011 = "Flash"

  100 = "Flash override"

  101 = Crítico

  110 = Control de red (Internetwork control)

  111 = Control de red (Network control)

- **TOS (4 bits):** corresponde al tipo de servicio

  1000 = Minimizar retardo

  0100 = Maximizar el rendimiento

  0010 = Maximizar la fiabilidad

  0001 = Minimizar el costo monetario

  0000 = Servicio normal

- **MBZ (1 bit):** Must be zero, está reservado para uso futuro, debiendo ser cero, a menos que se partícipe en un experimento con IP que haga uso de este bit.

- **Longitud Total (16 bits):** indica la longitud del datagrama IP (cabecera más datos) especificada en bytes (máximo 65535 bytes). Todos los hosts deben estar preparados para aceptar datagramas de hasta 576 bytes (tanto si llegan completos como en fragmentos), para permitir que un bloque de datos de tamaño razonable sea transmitido junto a la información de cabecera necesaria, admitiendo así un margen para cabeceras de protocolos de nivel superior.

Es necesario introducir conceptos relacionados con la fragmentación, antes de continuar con los siguientes campos de la cabecera:

Encapsulación: consiste en el envío de un datagrama completo en una trama física y depende de su tamaño.

MTU (Unidad de Transmisión Máxima): determina la longitud máxima, en bytes, que podrá tener un datagrama IP para ser transmitido por una red física; este parámetro está determinado por la arquitectura de la red; por ejemplo, el MTU de Ethernet es 1500 bytes por trama, el de FDDI es 4497 bytes por trama.

Fragmentación: consiste en el proceso de dividir en diferentes partes al datagrama, de modo que se permita el paso del mismo de una red a otra que tiene un MTU menor a su tamaño.

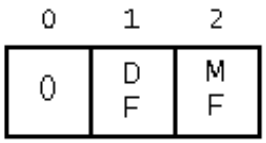
Ensamblado de Fragmentos: es el proceso de reconstrucción del datagrama a partir de sus fragmentos.

Plazo de Ensamblado: es un time out (tiempo fuera) que el host destino establece como máximo para esperar por todos los fragmentos de un datagrama, si este plazo se vence y no han llegado todos los fragmentos, entonces se descartan los que ya han llegado y se solicita el reenvío del datagrama completo.

El control de la fragmentación de un datagrama IP se realiza con los campos de la segunda palabra de su cabecera:

- **Identificación (16 bits):** es el valor de identificación del datagrama asignado por el remitente para permitir el ensamblado del datagrama fragmentado. Los fragmentos de un datagrama tendrán un mismo número de identificación.

- **Flags (3 bits):** son indicadores de control.



Bit 0: Reservado, debe ser cero

Bit 1 – DF (Don't Fragment): no-fragmentación

0 = puede fragmentarse

1 = no puede fragmentarse

Bit 2 – MF (More Fragments): más fragmentos

0 = único o último fragmento

1 = hay más fragmentos

- **Posición del Fragmento (13 bits):** especifica a qué parte del datagrama corresponde el fragmento, su posición se mide en unidades de 8 bytes y el primer fragmento tiene posición 0.

- **Tiempo de Vida (8 bits):** conocido como TTL (Time to live), especifica el tiempo máximo, en segundos, que se permite al datagrama circular por la red antes de ser descartado, se utiliza con la intención de limitar el período de vida máximo de un datagrama

- **Protocolo (8 bits):** especifica el protocolo del siguiente nivel empleado para construir el mensaje transportado en el campo datos. Algunos valores posibles son:

1 = ICMP (Internet Control Message Protocol)

2 = IGMP (Internet Group Management Protocol)

6 = TCP (Transmission Control Protocol)

17 = UDP (User Datagram Protocol)

- **Suma de Control de Cabecera (16 bits):** conocido como Checksum, asegura la integridad de la cabecera; se calcula haciendo el complemento a uno de 16 bits de la suma de los complementos a uno de todas las palabras de 16 bits de la cabecera. Si la suma de control de cabecera falla, el datagrama es descartado inmediatamente por la entidad que detecta el error. Este valor se recalcula y verifica en cada punto donde la cabecera es procesada. El valor inicial de este campo es cero.

- **Dirección Origen (32 bits):** dirección IP del host emisor.

- **Dirección Destino (32 bits):** dirección IP del host receptor.

Cada dispositivo de red tiene al menos una dirección IP que lo identifica de forma única del resto de dispositivos, de esta manera, los nodos intermedios pueden guiar correctamente un paquete enviado desde el origen a su destino.

Clases de Direcciones IP

En la figura 2.9 se indican las cinco clases de direcciones IP:

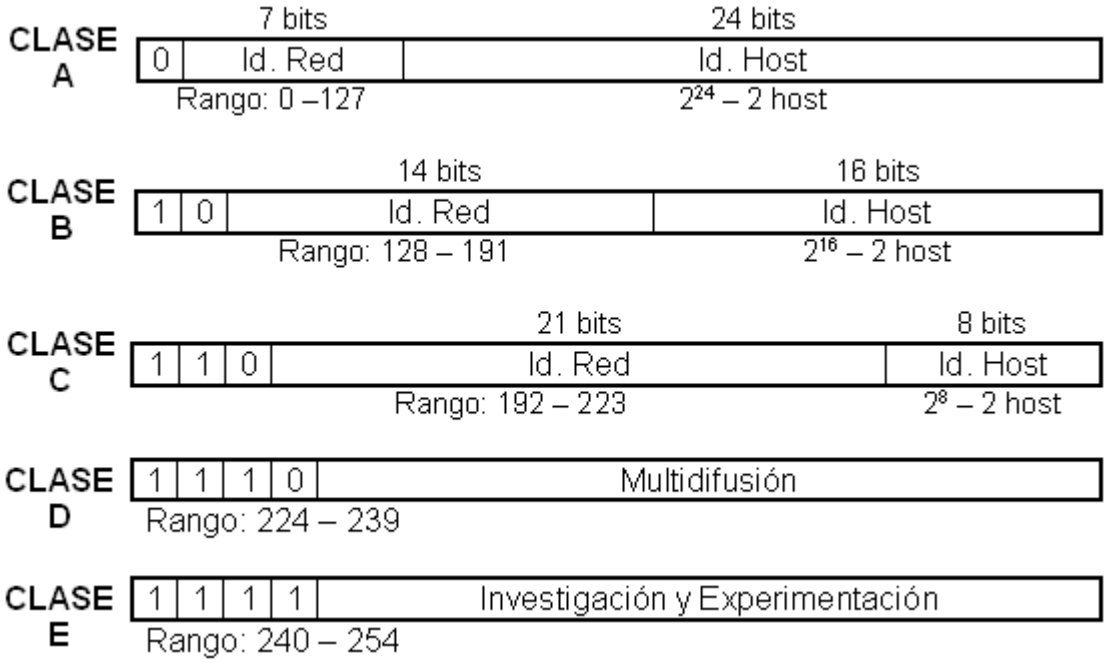
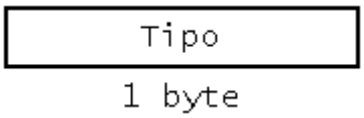


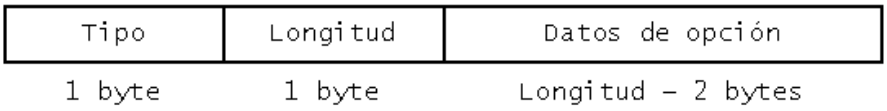
Figura 2.9: Clases de direcciones IP

- **Opciones:** existen hasta 40 bytes extra en la cabecera del datagrama IP, que corresponden a opciones adicionales. El formato de este campo depende del valor del número de opción que se tiene en el primer byte:

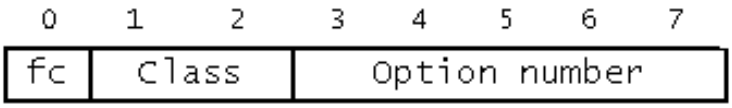
  - **Caso 1:** un solo byte de tipo - opción.



  - **Caso 2:** un byte tipo - opción, un byte longitud - opción y los bytes correspondientes a los datos de opción.



Tipo – opción: tiene la misma estructura en ambos casos, y contiene tres campos:



fc - flag copy (1 bit): indica si el campo de opciones es copiado (1) o no (0) en los fragmentos del datagrama.

class (2 bits): es un entero sin signo, en el que tenemos:

0 = control

1 = reservado para uso futuro

2 = depurado y mediciones

3 = reservado para uso futuro

option number (5 bits): es un entero sin signo.

Longitud – opción: cuenta la longitud de la opción, incluyendo los campos de tipo y longitud.

Datos de opción: no contiene datos relevantes para la opción.

- **Relleno (variable):** es utilizado para asegurar que la cabecera ocupa un múltiplo de 32 bits. El valor de relleno es cero.

2.2.2.2. IPv4 versus IPv6

Los principales inconvenientes de IP Versión 4 son:

- El esquema de direccionamiento IP no es suficiente para todos los host de Internet debido a la creciente cantidad de usuarios, problema que se denomina: Agotamiento de las direcciones IP y que se produce por las siguientes razones[10]:

    - La dirección IP se divide en un número de red y en una parte local que se administra por separado, aunque el espacio de direcciones dentro de una red puede estar poco ocupado; en lo que respecta el espacio efectivo, si se usa un número de red, todas las direcciones de esa red están ocupadas.

    - El espacio de direcciones para redes se estructura en las clases A, B y C, de distintos tamaños, y deben considerarse por separado los espacios de cada una.

    - El modelo de direccionamiento IP requiere que todas las redes IP tengan números unívocos, estén o no conectadas a Internet.

    - El crecimiento del uso de TCP/IP en nuevas áreas podría resultar en una rápida explosión del número de direcciones IP requeridas.

- El proceso de fragmentación hace ineficiente el uso de aplicaciones de tiempo real.

- Se debe disminuir los campos en IPv4 para optimizar el funcionamiento de los routers en la red.

Para solucionar estos inconvenientes, el IETF (Internet Engineering Task Force) impulsó un debate en el que se establecieron los requerimientos para la versión de IP que sustituiría a IPv4, entre los que se encontraban[10]:

- Un espacio de direcciones mucho más grande: al menos 10exp9 redes, preferiblemente 10exp12; y al menos 10exp12 host, preferiblemente 10exp15.

- Permitir la encapsulación de sus propios paquetes o los paquetes de otros protocolos.

- Posibilidad de añadir clases de servicio para distinguir los tipos de datos transmitidos.

- Proporcionar direccionamiento multicast de forma que esté completamente integrado con el resto de la pila que IPv4.

- Proporcionar autentificación y encriptación.

- Preservar las virtudes de IPv4: robustez, independencia de las características de la red física, alto rendimiento, topología flexibilidad, extensibilidad, servicio de datagramas, direccionamiento unívoco a nivel global, protocolo de control integrado y estándares de libre distribución.

- Implementación a través de una transición sencilla.

- Coexistencia de IPng con IPv4.

Después de lo cual se concluyó con la especificación de un nuevo protocolo IP, conocido formalmente como: IPng (IP Next Generation), correspondiente a la versión 6 del Protocolo Internet o IPv6, el cual se encuentra especificado en el RFC 2460[11].

En el apartado 2.2.2.1 se hizo referencia al esquema del datagrama IP definido para el protocolo IP versión 4, por lo que a continuación se describirá brevemente los cambios realizados en el datagrama de IPv6[11] (Figura 2.10), en el que se incrementa la longitud de la cabecera de 20 a 40 bytes; además los campos de direcciones origen y destino tienen 16 bytes, siendo diseñadas para ser usadas con CIDR (Classless InterDomain Routing) y están precedidos de 8 bytes de control, mientras que en IPv4, estas direcciones tiene 4 bytes precedidos de 12 bytes de control y seguidos posiblemente del campo opciones. Con la reducción de la información de control y la eliminación del campo opciones de la

cabecera se pretende optimizar el procesamiento del paquete. Los campos de uso poco frecuente que se han eliminado de la cabecera se han pasado a extensiones de cabecera opcionales.

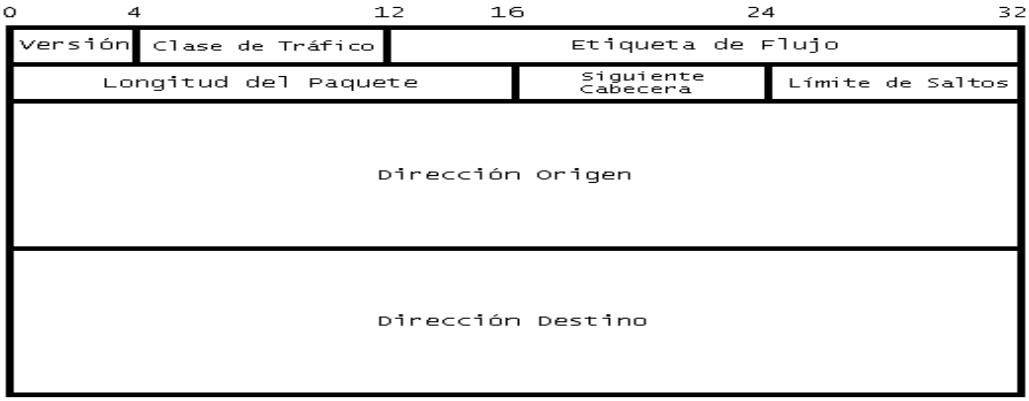


Figura 2.10: Cabecera IP versión 6

Los campos de la cabecera IPv6 son:

- **Versión (4 bits):** número de versión, 6.

- **Clase de tráfico (8 bits):** identifica y distingue entre las diferentes clases o prioridades de paquetes IPv6.

- **Etiqueta de flujo (20 bits):** puede ser usado por un origen para etiquetar secuencias de paquetes para los cuales solicita un manejo especial por los routers IPv6. Además se define un flujo como una serie de paquetes relacionados desde una fuente a un destino que requiere un tipo particular de manipulación de parte de los routers implicados.

- **Longitud del paquete (16 bits):** en bytes, excluyendo la cabecera, está codificado como un entero sin signo.

- **Siguiente cabecera (8 bits):** indica el tipo de cabecera que sigue inmediatamente esta cabecera, corresponde al número de protocolo en IPv4. Se utiliza además para indicar la presencia de cabeceras de extensión, que proporcionan los mecanismos para añadir información opcional al paquete. Algunos valores importantes son:

  41 = IPv6 Header

  43 = IPv6 Routing Header

  44 = IPv6 Fragment Header

  51 = IPv6 Authentication Header

- **Límite de saltos (8 bits):** corresponde al campo Tiempo de Vida de IPv4, pero en este caso se mide en saltos y no en segundos, debido a que IP normalmente envía los datagramas a más de un salto por segundo, el campo TTL se decrementa siempre en cada salto y además muchas implementaciones de IP no causan la expiración de los datagramas en base al tiempo transcurrido.

- **Dirección origen (128 bits):** dirección del host origen.

- **Dirección destino (128 bits):** dirección del host destino.

Estas direcciones se representan como una secuencia de cuatro dígitos hexadecimales separados por comas. La secuencia 0000 se contrae como 0.

Como se puede apreciar algunos de los campos de IPv4 no tienen su equivalente en IPv6, entre éstos tenemos:

- **Identificación, Flags y Posición del Fragmento:** los paquetes fragmentados tienen una extensión en lugar de información de fragmentación en la cabecera IPv6, lo cual reduce el tamaño de la cabecera básica de IPv6.

- **Suma de control de cabecera:** en IPv6 no se monitorea el checksum de los paquetes, puesto que incluye una cabecera opcional que se puede utilizar para asegurar la integridad y además los protocolos de nivel superior implementan este control.

- **Opciones:** todos los valores opcionales asociados con los paquetes IPv6 están contenidos en EH's (Extension Headers) asegurando que la cabecera básica tenga siempre el mismo tamaño.

Frente a este panorama se evidencia la necesidad de realizar la migración de IPv4 a IPv6, cuyas técnicas de conversión se denominan: SIT (Simple Internet Transition), las cuales enfatizan la facilidad del proceso desde el punto de vista del administrador y del usuario y se resumen en:

- Implementaciones de pila dual para los host y routers que deben interoperar entre IPv4 e IPv6, de manera que se establezca la duplicidad en los protocolos de la capa de red.

- Direcciones IPv4 embebidas en direcciones IPv6, a los hosts IPv6 se les asigna direcciones compatibles con IPv4 y las direcciones IPv4 se asocian a IPv6.

- Un mecanismo de tunneling de IPv6 sobre IPv4, para permitir la creación de nodos sólo IPv6, que deben existir en redes IPv6 completamente funcionales.

- Traducción de cabeceras IPv4/IPv6 en los routers situados entre redes IPv4 e IPv6.

Esta migración se plantea a través de dos fases: la primera es una transición a una infraestructura dual IPv6/IPv4 y la segunda, que no es obligatoria, es a una infraestructura sólo IPv6.

Respecto a las direcciones IP, se requiere que todas las referencias a direcciones de 32 bits sean sustituidas por las nuevas de 128 bits, lo que supone el cambio drástico de todas las aplicaciones existentes. Además para el DNS se define un nuevo tipo de registro AAAA, que permitirá realizar la transformación de los nombres de dominio actuales (que no requieren cambio) en direcciones de

128 bits y la traducción inversa de direcciones a nombres se realizará dentro de la nueva zona ip6.int dispuesta a tal efecto.

2.2.3. Características

En la tabla 2.1 se especifican las principales características de las Redes IP con los respectivos beneficios obtenidos.

Tabla 2.1: Características versus beneficios

Características	Beneficios
Las redes IP se basan en la técnica de conmutación de paquetes.	La capacidad disponible se utiliza eficientemente.
Permiten la convergencia de todo tipo de tráfico: datos analógicos (video y voz) y digitales (texto e imágenes) en una sola red.	Ahorro en costos de administración de sistemas, hardware y soporte. Mejoras operacionales. Se optimiza el ancho de banda disponible. Garantiza la continuidad en las operaciones y la disponibilidad de la información y de las aplicaciones.
Permiten reconfigurar la red.	Facilidad para introducir nuevos usuarios y/o servicios adicionales.
Son abiertas y basadas en estándares.	Se pueden introducir nuevos dispositivos y aplicaciones que pueden convertirse en fuentes de ingresos que ofrezcan un valor esencial a empresas y usuarios.
Permiten la variación de las calidades de servicio.	Enfrentar cualquier tipo de aplicación tanto sencillas transferencias de archivos sin limitación de tiempo como aplicaciones multimedia en tiempo real y el flujo de vídeo y voz.
Estructura unificada.	Se satisface con mayor eficacia las necesidades de acceso de los distintos usuarios de toda la red.
Se basan en el uso de un modelo horizontal de provisión de servicios, de acuerdo a un modelo cliente-servidor y *peer-to-peer* (P2P). (Figura 2.11[12])	La implantación de los servicios no tiene impacto en la red, de forma que es más sencillo añadir un nuevo servicio en los equipos del cliente y del servidor. Se preservan las inversiones de red. Se ahorra en costos de explotación y mantenimiento, comparando con las soluciones de red clásicas.

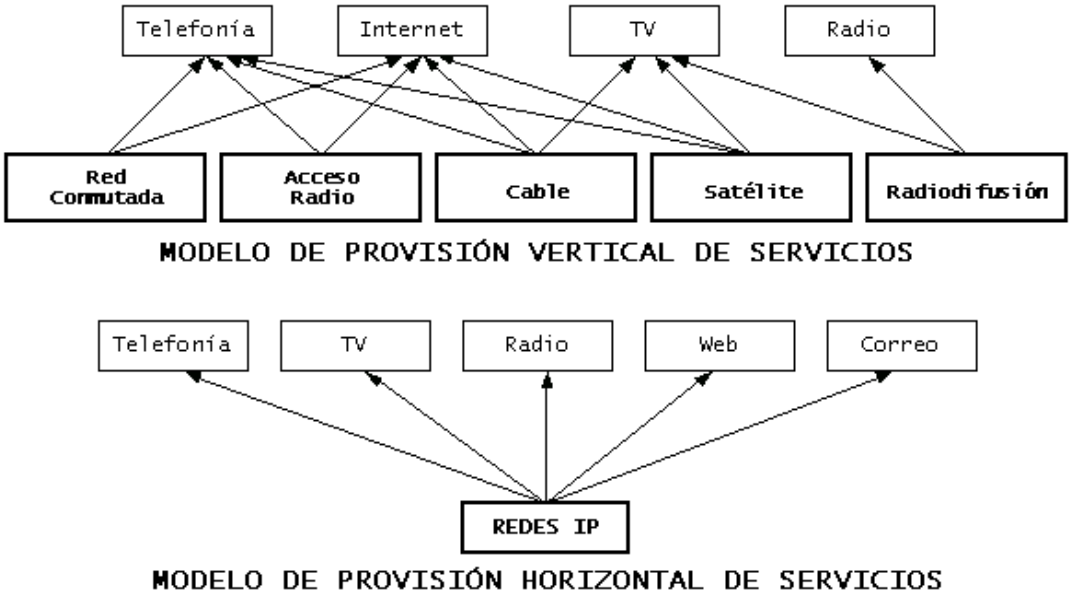


Figura 2.11: Modelos de provisión de servicios

2.2.4. Convergencia IP

Las redes IP utilizan la filosofía “best effort”, en la que los paquetes tienen la misma expectativa de tratamiento a medida que transitan por la red y se caracterizan porque la complejidad se encuentra en los host de las puntas, siendo tontos los routers del núcleo de la red, puesto que solo miran la cabecera, buscan en la tabla de ruteo y definen el siguiente salto. Si llegase a ocurrir congestión, se retardan o descartan los paquetes.

De ahí que inicialmente, las redes IP fuesen diseñadas para proveer el transporte del tráfico de datos; en este sentido se movía por la red, de forma óptima y segura, tráfico sin requerimientos de tiempo real, como aplicaciones de correo electrónico, FTP y navegación, pero después se hizo necesario incluir servicios no tradicionales como: telefonía, radio, televisión, videoconferencia, etc., los cuales requerían una arquitectura de comunicación compartida para todos los

usuarios, de forma que fueran capaces de intercambiar información de cualquier tipo a través de una sola red.

Esta arquitectura debía ser un estándar abierto para soportar diferentes protocolos del nivel de transmisión, particularmente aquellos que pueden ser utilizados sobre una amplia variedad de medios de transmisión, además requería mecanismos de QoS que administren parámetros de calidad, como ancho de banda, retardo y jitter, que son necesarios para permitir la integración de los servicios no tradicionales con las aplicaciones de datos. Afortunadamente las redes IP ofrecen una solución bien diseñada para ajustarse a estos requerimientos.

La convergencia hace referencia a la integración de soluciones de datos, voz y vídeo en una sola red (basada en IP), con esto se optimiza el ancho de banda disponible y se garantiza la continuidad empresarial y la disponibilidad de la información y de las aplicaciones en toda la empresa.

Existen tres factores principales que crean las condiciones para la convergencia IP[13]:

- **Tecnología Digital:** permite que toda información sea texto, sonido o imágenes, se representen como bits y se transmitan como secuencias de ceros y unos.

- **Tecnología de Transmisión:** permite una mejor utilización de la capacidad disponible, en consecuencia los servicios que requieren una alta capacidad pueden ser ofrecidos a partir de infraestructuras que previamente estaban disponibles para proporcionar servicios más simples.

- **Protocolos de comunicación estandarizados**

2.3. CALIDAD DE SERVICIO - QoS

2.3.1. Definición

En la UIT (Unión Internacional de Telecomunicaciones) aparece una primera definición de QoS (Quality of service), en la recomendación E.800, en la que se define calidad de servicio como "el efecto colectivo de prestaciones de servicio que determinan el grado de satisfacción del usuario en lo que respecta al servicio".

"La calidad del servicio (QoS) se refiere a la capacidad de una red para proporcionar un mejor servicio al tráfico de red seleccionado sobre varias tecnologías, incluyendo Frame Relay, Modo de transferencia asíncrona (ATM), redes Ethernet y 802.1, SONET y redes IP que pueden utilizar algunas o todas estas tecnologías subyacentes"[14].

"La calidad de servicio consiste en la capacidad de la red para reservar algunos de los recursos disponibles para un tráfico concreto con la intención de

proporcionar un determinado servicio. Debemos tener en cuenta que en la red se pueden utilizar diferentes tecnologías de transporte (como pueden ser Frame Relay, X.25, SDH, ATM, etc.) de manera que la gestión de QoS implica la interacción de estas tecnologías con los equipos de conmutación, que son los que finalmente determinarán el nivel de QoS alcanzado"[15].

La calidad de servicio consiste en un conjunto de requerimientos que la red debe cumplir para satisfacer las necesidades y expectativas de los usuarios con respecto al funcionamiento de sus aplicaciones, se basa en el rendimiento de extremo a extremo para asegurar un nivel de servicio adecuado para la transmisión de la información.

La QoS se define mediante[16]:

- Clasificación: especifica qué campos de paquetes coinciden con valores específicos, todos los paquetes que concuerden con las especificaciones definidas por el usuario, se clasifican juntos.

- Acción: define la gestión del tráfico, en la que se reenvían los paquetes de acuerdo a su información y los valores de su campo, por ejemplo, prioridad de VLAN (VPT) y DSCP (Punto de Código de Servicios Diferenciados).

La calidad de servicio se puede definir desde dos puntos de vista:

- Como un servicio que un usuario final solicita, ya sea directa o indirectamente de acuerdo a sus requerimientos; este servicio es cuantificado en la máquina de dicho usuario. En este caso es posible para el usuario determinar si el objetivo de QoS se cumple.

- Como los servicios que el administrador de la red puede ofrecer, hace referencia al rendimiento de red, es decir la capacidad de la red para proporcionar las funciones deseadas. En este caso hay objetivos administrativos para los diferentes tipos de tráfico que podrían no ser aparentemente cuantificables para un usuario final, pero si para el administrador de la red.

2.3.2. Políticas de calidad de servicio

La implementación de políticas de calidad de servicio se puede enfocar en varios puntos según los requerimientos de la red, de manera que las características de QoS proporcionen un servicio de red mejorado y más fiable. Entre las principales tenemos:

- Asignar ancho de banda en forma diferenciada.
- Evitar y/o administrar la congestión en la red.
- Fijar prioridades de acuerdo al tipo de tráfico.
- Modelar el tráfico de la red.

- Proporcionar características para manejar la pérdida de paquetes.

2.3.3. Características

- La calidad de servicio en una red permite cuantificar el tratamiento que un paquete debe recibir a medida que circula por la red.

- No crea ancho de banda adicional, sino que maneja el tráfico de manera que el ancho de banda disponible soporte los requerimientos de un amplio rango de aplicaciones.

- Proporciona la capacidad de implementar la prioridad dentro de una red, para ofrecer más garantías y seguridad a las aplicaciones que lo requieren.

- Mejora el flujo del tráfico en función de las políticas definidas, permitiendo obtener un flujo dedicado para el tráfico de mayor demanda.

- Asegura que las aplicaciones tengan suficientes recursos de red para comunicarse eficazmente.

- Al utilizar políticas de QoS se puede configurar una red para que el rendimiento extremo a extremo sea fiable y estable.

- Una garantía de QoS indica un nivel de servicio que permite a un programa transmitir datos a una velocidad especificada y entregarlos en un período de tiempo dado.

2.3.4. Parámetros QoS

Una red debe garantizar un cierto nivel de calidad de servicio para un tipo de tráfico que sigue un conjunto especificado de parámetros. Para QoS se cuenta con los siguientes parámetros[17]:

- Ancho de banda (Bandwidth)
- Retardo (Delay)
- Variación de retardo (Jitter)
- Pérdida de paquetes (Loss)

2.3.4.1. Ancho de banda

Define la capacidad de los medios de transmisión; se refiere al número de bits por segundo que puede entregarse con éxito a través de cierto medio. En algunos casos, el ancho de banda iguala la velocidad física del enlace, en otros casos, el ancho de banda es más pequeño que la velocidad real del enlace.

La tasa de información comprometida (CIR) define cuánto ancho de banda los proveedores garantizan que pasarán a través de sus redes entre el equipo terminal de datos (DTE) y cada extremo de un circuito virtual (VC).

En la Tabla 2.2 se muestran las herramientas de QoS que ayudan a mejorar la utilización del ancho de banda[17].

Tabla 2.2: Herramientas QoS que afectan al ancho de banda

Tipo de herramienta	Cómo afecta al ancho de banda
Compresión	Comprime la carga útil o las cabeceras, mediante la reducción del número total de bits requeridos para transmitir los datos, lo que se hace antes o después del proceso de gestión de colas.
Control de admisión de llamadas – CAC	Reduce la carga total introducida en la red, al decidir si la misma puede aceptar nuevas llamadas de voz y video.
Gestión de colas - Queuing	Afecta a la cantidad de ancho de banda que ciertos tipos de tráfico reciben y se utiliza para reservar cantidades mínimas de ancho de banda para tipos particulares de paquetes. Se crean colas múltiples, de donde se toman los paquetes de acuerdo a un algoritmo de servicio de cola.

2.3.4.2. Retardo

También conocido como latencia, es el tiempo que tarda un paquete entre dos puntos determinados, debido a los diferentes tipos de retardo que pueden presentarse. El delay no afecta a la calidad, pero sí a la interacción.

Se introduce en el flujo de tráfico de una red, puesto que podría tomar demasiado tiempo para que un paquete alcance su destino dependiendo de la ruta que siga, de ahí que todos los paquetes en la red experimenten algún retardo cuando se envían y cuando llegan a su destino. Los tipos de retardo son:

- **Retardo de serialización (fijo):** es el tiempo que toma colocar todos los bits de un paquete sobre la interfaz física, depende de la velocidad del

enlace y del tamaño del paquete y ocurre en cada interfaz física de salida. Se utiliza la siguiente fórmula para calcular el retardo de serialización para un paquete:

$$\frac{\text{\# de bits enviados}}{\text{Velocidad del enlace}}$$

Fórmula 2.1: Cálculo del retardo de serialización

- **Retardo de propagación (fijo):** es el tiempo que le toma a un solo bit atravesar el medio físico de un extremo a otro, puesto que cuando una señal eléctrica u óptica se envía sobre el cable, la energía no se propaga al otro extremo instantáneamente, sino que hay algún retardo. Se basa en la velocidad de la luz sobre ese medio y la longitud del enlace y ocurre en cada medio físico. Se utiliza las siguientes fórmulas para calcular el retardo de propagación:

$$\frac{\text{Longitud del enlace [m]}}{3.0 \times 10^8 \text{ m/s}} \quad \text{Ó} \quad \frac{\text{Longitud del enlace [m]}}{2.1 \times 10^8 \text{ m/s}}$$

Fórmula 2.2: Cálculo del retardo de propagación

Donde:

3.0×10^8 es la velocidad de la luz en un vacío,

2.1×10^8 es una medida más exacta de la velocidad de la luz sobre los medios de cobre y ópticos

- **Retardo en las colas (variable):** es el tiempo que un paquete pasa en las colas de un dispositivo, debido a que se tiene que esperar a que otros

paquetes se envíen; esto ocurre típicamente en las colas de salida de un router.

- **Retardo de procesamiento / forwarding (variable):** es el tiempo tomado para conmutar el paquete en el router o el switch, incluye el tiempo desde que se examina el frame / paquete en la interfaz de entrada, hasta la colocación de éste en la cola de salida de la interfaz de salida para la transmisión, no toma en cuenta el retardo en las colas. Ocurre en cada parte del equipo de conmutación, incluyendo: routers, switches LAN, Frame Relay y ATM.

- **Retardo shaping (variable):** el traffic shaping (conformación del tráfico), si es configurado, retrasa la transmisión de los paquetes para evitar la pérdida de los mismos en la mitad de una red Frame Relay o ATM, por lo que puede crear retardos adicionales al servir las colas más lentamente que si no fuera utilizado. Este retardo ocurre en donde se configure el traffic shaping, siendo más probable en un router que está enviando paquetes a una red Frame Relay o ATM.

- **Retardo en la red (variable):** es el retardo que experimenta un paquete en la red y varía de acuerdo al proveedor, el estado del enlace y la congestión en la red; ocurre en la red del proveedor de servicios. En algunos casos, el proveedor incluirá los límites de retardos en el acuerdo del nivel de servicio (SLA).

En la Tabla 2.3 se muestran las herramientas de QoS que ayudan a mejorar los efectos del retardo en la red[17].

Tabla 2.3: Herramientas QoS que afectan al retardo

Tipo de herramienta	Cómo afecta al retardo
Gestión de Colas – Queuing (Scheduling)	Permite ordenar los paquetes de manera que los sensibles al retardo dejen su cola antes que aquellos en los que éste no influye.
Fragmentación del Enlace e Interleaving (Entrelazado)	Cuando el router empieza a enviar el primer bit de un paquete, continúa hasta que se envíe todo el paquete entero. Con la fragmentación y el Interleaving se divide los paquetes más grandes en fragmentos antes de enviarlos y se introducen sensibles al retardo después de un solo fragmento, en lugar de esperar hasta que el paquete original más grande sea enviado.
Compresión	Se comprime la carga útil o la cabecera del paquete para reducir el número total de bits exigido para transmitir los datos, con esto se reduce el retardo de serialización, sin embargo, también puede aumentarse el retardo de procesamiento requerido para comprimir y descomprimir los paquetes.
Traffic Shaping	Tiene un impacto negativo puesto que incrementa el retardo al intentar reducir la pérdida de paquetes en una red Frame Relay o ATM.

2.3.4.3. Variación del retardo

El jitter es causado por las variaciones de latencia, es decir la variación en los tiempos de llegada de los paquetes que fueron transmitidos uniformemente. Afecta a la calidad de la voz y el video puesto que se requiere que los paquetes sean transmitidos y recibidos de forma constante y uniforme.

Se plantea que la solución al jitter es almacenar los datos en memorias buffer, lo cual introduce un retardo aún mayor; por lo cual se han implementado diversas formas de buffer garantizadas mediante software[18]:

- **Cola prioritaria:** el administrador de la red define varios niveles (máximo 4) de prioridad de tráfico.

- **Cola definida:** el administrador reserva un ancho de banda para cada tipo de protocolo específico.

- **Cola ponderada:** mediante un algoritmo se identifica cada tipo de tráfico y se prioriza el de bajo ancho de banda, permitiendo que en momentos de congestión se estabilice la red.

Algunos tipos de herramientas QoS ayudan a mejorar la variación del retardo; pero se debe tomar en cuenta que la disminución del jitter para un grupo de paquetes provocará el aumento del mismo para otros. Estas herramientas son las mismas que afectan al retardo y su detalle se encuentra en la Tabla 2.3.

2.3.4.4. Pérdida de paquetes

Es el fallo en la transmisión de un paquete debido a las siguientes causas[19]:

- Errores en la transmisión.
- Descarte por congestión.
- Descarte por time-out (delay excesivo), el cual afecta fundamentalmente al tráfico de tiempo real y a las aplicaciones críticas.

- Tasa de error de cada medio de transmisión que condiciona al protocolo que se utiliza para transportar los datos

En la mayoría de redes, el número de paquetes perdidos por errores en los bits es pequeño, típicamente menos de uno en un billón (Indice de error de bit [BER] de 10^{-9} o mejor), por lo que el principal problema es la pérdida de paquetes debido a buffers y colas llenas.

En la Tabla 2.4 se especifican los dos tipos de herramientas QoS que se utilizan para reducir al mínimo el impacto por pérdida de paquetes[17].

Tabla 2.4: Herramientas QoS que afectan a la pérdida de paquetes

Tipo de herramienta	Cómo afecta a la pérdida de paquetes
Random Early Detection (RED)	Se trabaja bajo la premisa que si algunas de las conexiones TCP pueden contraer sus ventanas antes de que las colas de salida se llenen, el número colectivo de paquetes enviados en la red será más pequeño y la cola no se llenará, es decir se administra el final de una cola y se reduce la carga total, acortando la cola congestionada, mientras que se afecta los tiempos de respuesta de algún usuario. TCP retrasará el envío, reduciendo el tamaño de la ventana, cuando se pierden los paquetes.
Gestión de Colas – Queuing	Se evita la pérdida de paquetes mediante la implementación de colas más largas, sin embargo, esto incrementa los retardos. Adicionalmente se puede colocar el tráfico sensible a la pérdida de paquetes en una cola de mayor longitud que la cola del tráfico sensible al retardo.

2.3.5. Requerimientos de los tipos de tráfico

Al integrar voz, vídeo y datos sobre una sola red, la diversidad y la unicidad de cada tipo de tráfico se deben administrar para asegurar una calidad aceptable del servicio.

Los parámetros de QoS deben garantizar los requisitos de tiempo de las aplicaciones multimedia, las cuales son[19]:

a. **Real time o dependientes del tiempo:** no admiten retransmisión ni control de flujo. Tenemos aplicaciones:

- **Interactivas:** no admiten gran retardo ni su variación.
  - Voz (Audio)
    - Telefonía
  - Video
    - Videoconferencia

- **No interactivas:** admiten retardo pero no jitter.
  - Música
  - Video – streaming point to point o multicast
  - Video Vigilancia
  - Broadcasting de voz, música o video

b. **Non – real time o independientes del tiempo:** admiten retransmisión y control de flujo. Tenemos aplicaciones (texto) como:

- POS (Point of Sale)
- E-mail
- Chat
- Transferencia de Archivos
- Browsing: navegación por la red
- Consulta de Bases de Datos
- Web (tendencia a multimedia con contenido real time)

Como se puede apreciar existen diferentes tipos de tráfico, los cuales requieren diversas características de rendimiento (cantidad de datos transmitidos exitosamente desde un dispositivo de red hasta otro en un período de tiempo) en una red; por ejemplo una transferencia de archivos necesita únicamente rendimiento, puesto que el retardo que experimenta un solo paquete podría no importar, sin embargo, las aplicaciones interactivas necesitan tiempos de respuesta constantes, la voz necesita retardo bajo y el video necesita retardo bajo y alto rendimiento, así pues estas aplicaciones tienen un comportamiento variable en una red; la Tabla 2.5 muestra el funcionamiento de la voz, el video y el tráfico de datos en una red sin QoS[17].

Tabla 2.5: Comportamiento del tráfico sin QoS

TIPO DE TRÁFICO	COMPORTAMIENTO SIN QoS
VOZ	Difícil de entender.
	Suena entrecortada.
	El retardo hace difícil la interacción, las personas no saben cuando la otra parte ha terminado de hablar.
	Las llamadas son desconectadas.
VIDEO	Las imágenes se despliegan irregularmente y hay movimientos desiguales.
	El audio no concuerda con el video.
	Desaceleración de los movimientos.
DATOS	Llegan después de mucho tiempo.
	El usuario tiene que esperar a que se presenten los datos en la pantalla.
	Los tiempos de respuesta erráticos frustran a los usuarios.

La calidad de servicio pretende solucionar el rendimiento del tráfico en la red y disminuir el impacto de posibles problemas en el funcionamiento de las aplicaciones, mediante la implementación de características de red (ancho de banda, retardo, jitter y pérdida de paquetes) que permitan satisfacer los requerimientos de voz, vídeo y tráfico de datos; la idea básica consiste en proporcionar los recursos de QoS necesarios para cada aplicación, es decir se puede mejorar una característica QoS para un flujo que la necesita y degradar la misma característica para un flujo que no la necesita, el resultado es un flujo de tráfico mejorado. En la Tabla 2.6 se indican los requerimientos de QoS para diferentes aplicaciones[20].

Tabla 2.6: Parámetros QoS requeridos por aplicaciones IP

APLICACIÓN	PERFORMANCE			
	ANCHO DE BANDA	SENSIBILIDAD A:		
		DELAY	LOSS	JITTER
VoIP	Baja	Alta	Alta	Media
Video Conferencia	Alta	Alta	Alta	Media
Streaming Video on Demand	Alta	Media	Media	Media
Streaming Audio	Baja	Media	Media	Media
Negocios Electrónicos (e-Business – Web Browsing)	Media	Media	Baja	Alta
Correo Electrónico	Baja	Baja	Baja	Alta
Transferencia de Archivos	Media	Baja	Baja	Alta

En el anexo a, se especifican las características de los tipos de tráfico en relación con los requerimientos de las aplicaciones y de la red.

2.3.6. Funcionamiento

2.3.6.1. Problemática

Las aplicaciones generan tráfico a ritmos variables y requieren que la red pueda transportar el tráfico al ritmo que lo generaron, de la misma manera, las aplicaciones son más o menos tolerantes a retardos de tráfico en la red y a variaciones de los mismos; si se tuviera recursos de red infinitos, todo el tráfico de las aplicaciones podría transportarse al ritmo requerido, sin retardo ni pérdida 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.

Las redes están construidas mediante la unión de dispositivos, tales como switches y routers, estos dispositivos intercambian el tráfico entre ellos mediante interfaces. Si la velocidad en la que el tráfico llega a una interfaz es superior a la

velocidad que ésta puede enviar tráfico al siguiente dispositivo, se produce congestión, de esta 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 este recurso en favor de cierto tráfico, para lo cual se emplea el Modelo QoS Básico.

2.3.6.2. Modelo QoS básico

La Figura 2.13, muestra el Modelo QoS Básico[21], en el que se detallan las principales acciones tanto en la entrada como la salida de una interfaz[20].

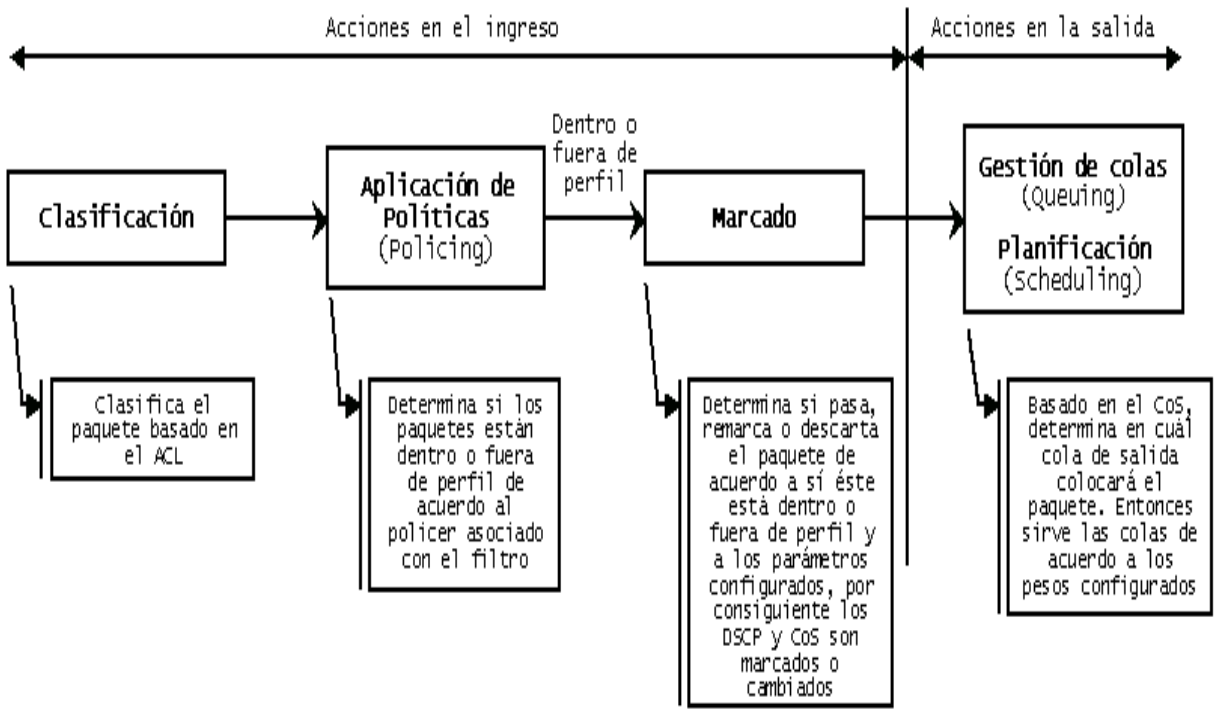


Figura 2.12: Modelo QoS básico

Las acciones al ingreso de la interfaz incluyen:

a) Clasificación de paquetes

Consiste en la identificación de los diferentes tipos de tráficos, para lo cual se examinan los campos de la cabecera de los paquetes y después se procede a separarlos en distintos flujos.

La clasificación viene dada por la asociación del identificador de clasificación (classification key), como: el campo TOS de la cabecera de IPv4, el campo DiffServ y en Ethernet, los 3 bits de prioridad definidos por IEEE 802.1p, contra las reglas de clasificación.

Los esquemas para clasificar paquetes, pueden ser simples como tomar N bits en la cabecera y diferenciar hasta 2^N clases (classification key) o más complicados como involucrar en el identificador de clasificación, múltiples campos del paquete IP, normalmente aquellos que definen el flujo IP (Origen y destino IP y número de puertos TCP / UDP).

b) Aplicación de políticas (Policing)

Tanto Policing y Marking comparten la función de Metering, que permite determinar si un paquete está dentro o fuera de perfil.

Se crea un policer que limita el ancho de banda consumido por un flujo de tráfico y de acuerdo a éste se determina si un paquete está dentro o fuera de profile, el resultado de esta determinación se pasa al marcador. El policer además especifica la acción a tomar para los paquetes que están fuera de profile (paquetes que exceden el límite configurado).

El traffic profile especifica que cada clase de tráfico (clasificada) debe tener ciertos límites de tolerancia en el número de paquetes que pueden llegar en un intervalo temporal específico (cuán rápido pueden llegar los paquetes para una determinada clase).

c) Marcado

Se evalúa el policer para especificar la acción a ser tomada cuando un paquete está fuera de profile, en este caso se puede decidir pasar el paquete sin modificación, marcar el paquete (normalmente en el DSCP) con una prioridad menor para que sea descartado en primer lugar en caso de congestión, o desechar el paquete.

Las acciones a la salida de la interfaz incluyen:

d) Gestión de colas (Queuing)

Una vez que se ha clasificado y tratado el tráfico según su profile, se debe colocar cada clase de tráfico en la cola correspondiente, tomando en cuenta que

el gestor de colas debe colocar todos los paquetes de igual flujo en la misma cola cuando por encima de IP no existen protocolos capaces de reordenar paquetes. La función de queuing implica las siguientes actividades:

- Añadir un paquete a la cola indicada en la fase de clasificación si la cola no está llena.
- Desechar un paquete si la cola está llena.
- Retirar un paquete cuando lo pida el scheduler.
- Monitorear la ocupación de las colas y tomar decisiones proactivas, como:

    - Retirar o no añadir un paquete cuando la cola está casi llena.
    - Marcar un paquete cuando la cola está casi llena.

Es importante mantener baja la ocupación media de las colas para de esta forma absorber ráfagas y evitar retardos altos de los paquetes, debido a que la ocupación de una cola aumenta a medida que la tasa de tráfico de llegada supera la capacidad a la cual el scheduler sirve paquetes de salida, reflejando de esta forma el nivel de congestión (encolamiento de paquetes) existente. Si la congestión es igual al nivel de ocupación de colas y es alta, se tienen dos alternativas:

- De forma transitoria se dimensionan las colas para absorber esas ráfagas.

- En un período considerable, el gestor de colas proporciona feedback al protocolo de cuarto nivel para que inicie su mecanismo de gestión de la

congestión. El feedback se realiza a través de los métodos de dropping de paquetes, entre los que tenemos:

- **Random Early Detection (RED):** utiliza la ocupación media de la cola como parámetro de una función aleatoria que decide cuándo descartar los paquetes y proporciona feedback negativo a los protocolos de cuarto nivel para que éstos disparen su mecanismo de congestion – avoidance (anulación de la congestión) de forma escalonada, evitando así que todos los flujos TCP (Transmission Control Protocol) disparen a la vez sus mecanismos.

- **Weighted Random Early Detection (WRED):** es una variación de RED que permite al gestor de colas seleccionar entre varias curvas de probabilidad de descarte para paquetes de una misma cola.

e) Planificación - Estrategias de servicio de colas (Scheduling)

Esta función dicta las características temporales de salida de los paquetes de cada cola (de una interfaz de salida de un router hacia el siguiente router o host).

Cada interfaz posee un scheduler que comparte la capacidad del enlace de salida entre las diferentes colas asociadas a esa interfaz, además establece un ancho de banda mínimo para una clase de servicio en particular, asegurándose que los paquetes de la cola asociada a esa clase son servidos regularmente con

la cadencia necesaria y proporciona Rate Shaping para imponer un ancho de banda máximo para una clase en particular (limitando la frecuencia con la que la cola asociada es servida). Las funciones y tipos de schedulers son:

- **Restringir ancho de banda por clase**

    - **Rate Shaping o Traffic Shaping (Leaky Bucket):** limita el ancho de banda mediante el encolamiento de los paquetes y es utilizado para suavizar las ráfagas de tráfico. El escenario descrito para la realización del Rate Shaping se conoce habitualmente como Leaky Bucket (los paquetes “gotean” con una cadencia fija), en el que se consigue una tasa de paquetes por segundo fija (shaping IP).

- **Asegurar ancho de banda por clase**

    - **Scheduling Simple:** regula los intervalos de servicio de colas antes que asegurar el ancho de banda por cola, tenemos los siguientes tipos:

        - **Strict Priority:** consiste en ordenar las colas por prioridad descendente y servir una cola de prioridad determinada siempre que las de mayor prioridad estén vacías, lo cual es recomendado para el tráfico sensible al delay y al jitter. Se debe tener el rate shaping apropiado para evitar que las colas de baja prioridad no sean atendidas.

- **Round Robin (RR):** sirve cíclicamente a las colas, transmitiendo un paquete antes de pasar a la siguiente cola en prioridad, con lo que se evita que las colas de baja prioridad no sean atendidas. Las colas vacías son ignoradas. No se recomienda su uso para tráfico sensible al retardo debido a que es muy difícil acotar la latencia.

- **Scheduling Adaptativo:** toma en cuenta la tasa de bits que se debe asegurar a cada cola. Tenemos las siguientes estrategias:

  - **Deficit Round Robin (DRR):** es una variación de RR, en el que se cuenta cuántos bytes han sido enviados por una cola determinada, los compara con el número de bytes que debió enviarse y la diferencia la considera un déficit, que se utiliza para modificar el intervalo de servicio de las colas y regular el bit rate a largo plazo para esa cola.

  - **Weighted Round Robin (WRR):** funciona de forma similar a DRR pero utiliza el déficit por exceso en lugar de por defecto, en este caso se transmiten algunos paquetes de cada cola alternadamente, evitando así que las colas de baja prioridad sean descuidadas totalmente durante períodos de tráfico prioritario. El número de paquetes que envía corresponde a la importancia relativa de la cola, la cual se define por la longitud de la cola.

- **Far Queuing (FQ):** es una variación de RR que recalcula la secuencia del scheduling de forma que la siguiente cola en ser servida sea la cola que lo necesita para así cumplir su bit rate medio a largo plazo, además ordena las transmisiones de paquetes en el orden en que habrían llegado al otro extremo.

- **Weight Far Queuing (WFQ):** es una variación de FQ que permite aplicar diferentes pesos a las colas, en el caso de que una cola esté vacía, su porcentaje se reparte entre el resto de colas en función de los pesos.

2.3.7. QoS en Redes ATM y Frame Relay

2.3.7.1. Redes ATM

2.3.7.1.1. Características

En las redes ATM (Modo de Transferencia Asíncrona), la información se transmite en forma de paquetes de longitud fija de 53 bytes, divididos en una cabecera de 5 bytes, que contiene la información relativa al encaminamiento del paquete y un payload o carga útil de 48 bytes, donde se introduce la información que se desea transportar a través de la red, permitiendo así que se intercalen células procedentes de diferentes fuentes con distintos tipos de tráfico (voz, vídeo y datos) y que se optimice el tráfico.

Es una tecnología orientada a la conexión, puesto que antes de enviar células a través de la red se establece la conexión o fase de negociación entre el usuario y la red, durante la cual se fija un contrato referente a la forma en que se va a realizar la transmisión de las células, es decir, se negocian los parámetros de tráfico y la calidad de servicio. La función CAC (Connection Admission Control) se encarga de decidir si se aceptan o no las condiciones de negociación en función de los recursos (ancho de banda) disponibles en la red y asigna los recursos a cada conexión, es decir, se produce un esquema de asignación dinámica de ancho de banda en función de la demanda, lo cual conlleva a un esquema de compartición de ancho de banda.

Fueron creadas para resolver la integración de aplicaciones con ciertas garantías de tráfico en las redes y garantizan a sus clientes que la latencia extremo a extremo no excederá un nivel especificado al soportar niveles de QoS, lo que constituye una ventaja sobre tecnologías como: Frame Relay y Fast Ethernet, no obstante su aceptación es considerada como una solución de alto costo y administración compleja.

2.3.7.1.2. Parámetros QoS en ATM

En ATM se garantiza la calidad de servicio mediante un contrato de CIR (Committed Information Rate) con el usuario. Se distinguen los parámetros relativos a prestaciones de tráfico que configuran el marco relativo a QoS y las funciones construidas a partir de dichos parámetros, que constituyen las llamadas

clases de servicio y que proporcionan una indicación acerca del tipo de tráfico que tiene lugar en un enlace. Los parámetros que conforman el QoS son[22]:

- **Cell transfer delay (CTD):** es el tiempo medio que utiliza una conexión virtual para transferir una célula desde el origen hasta su destino.

- **Cell loss ratio (CLR):** es la relación entre las células perdidas y el número total de células transmitidas.

- **Cell delay variation (CDV):** es la medida de la diferencia entre el retardo en la transferencia de una determinada célula y el retardo esperado; proporciona una medida del espaciamiento de las células en una conexión virtual.

- **Cell error rate (CER):** es la medida de la fracción de células erróneas transmitidas en el punto de destino.

- **Cel – misinsertion rate (CMR):** es la medida del número de células que proceden de un punto de origen equivocado (vienen de un punto de origen no especificado en el establecimiento de la conexión).

Las clases de servicio definidas en términos de los diferentes parámetros de QoS son[22]:

- **Constant bit rate (CBR):** soporta la transmisión de un flujo continuo de bits y requiere un ancho de banda fijo para proporcionar una conexión constante entre dos puntos. Soporta ajustadamente CTD y CDV para aplicaciones que no pueden tolerar variaciones en la demora. Se adapta especialmente a aplicaciones de voz.

- **Variable bit rate (VBR):** se orienta a las conexiones que conllevan un tráfico en el que el bit rate (equivalente al ancho de banda) es variable, es decir que se adapta especialmente al tráfico con niveles de ráfagas considerables y con requisitos bien definidos en lo que concierne a la capacidad de proceso, como es el caso de las aplicaciones de video. Existen dos tipos de VBR:

    - **rt – VBR (Real time VBR):** soporta aplicaciones sensibles al tiempo y con requerimientos de retardo y jitter, como en el caso de la compresión de vídeo interactivo.

    - **nrt - VBR (Non real time VBR):** soporta aplicaciones que no tengan problemas con la variación del retardo, pero sí determinados niveles de calidad de servicio para ancho de banda o retardo, como aplicaciones que incluyen transmisión de paquetes de datos y transferencia de archivos.

- **Available bit rate (ABR):** no garantiza ancho de banda al usuario salvo el MCR (Mínimo ancho de banda) que proporciona la red, así como algunas funciones basadas en mecanismos de control de flujos con las que se puede minimizar la pérdida de células debido a la congestión de la red, por lo que entra en la categoría de las clases de servicio de mejor esfuerzo. Su meta es proveer dinámicamente el ancho de banda que actualmente no está en uso por otras categorías de servicios a usuarios que pueden ajustar sus transmisiones a esa tasa, como intercambio por esta cooperación del usuario, la red le provee un servicio con una tasa de pérdida muy baja. Algunas aplicaciones son las interconexiones de tipo LAN, transferencias de archivos de alta performance, archivos de bases de datos y web browsers.

- **Unspecified bit rate (UBR):** se encuentra dentro de la categoría de los tipos de servicio de mejor esfuerzo, debido a que solamente se trasmite información en el caso de que exista capacidad suficiente en la red y sin ningún tipo de garantía; es decir, el sistema de gestión de red no contrae ningún compromiso en cuanto a parámetros de QoS. Algunos ejemplos son la emulación de LAN, transferencia de archivos e IP sobre ATM.

2.3.7.2. Redes Frame Relay

2.3.7.2.1. Características

Frame Relay es un protocolo de conmutación de paquetes de longitudes variables, permite el acceso a subred (regula interfaz usuario - red), así como múltiples terminales de usuario y simplifica los servicios que ofrece mediante la separación funcional de la arquitectura del protocolo en plano de usuario (parte por la que circulan los datos del usuario) y plano de control (parte por la que circulan datos entre el usuario y la red para supervisarla).

Es orientado a la conexión puesto que proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuitos punto a punto y es no fiable (errores pueden ser detectados y descartadas en los nodos de la red sin avisar).

Ofrece dos tipos de conexiones: Circuitos Virtuales Permanentes (PVC) y Circuitos Virtuales Conmutados (CVC), aunque los operadores de redes Frame Relay incluyen solo PVC's.

El control de la congestión está implementado en el Plano de Usuario y utiliza el mecanismo de Notificación y Descarte para avisar al origen y al destino sobre la congestión en una parte de la red (cuando se detecta una zona congestionada, se notifica al usuario, quien debe disminuir la tasa de tráfico

inyectado, caso contrario, la red descartará tramas) y para realizar esto se utiliza los siguientes campos del control de la trama:

- **Forward Explicit Congestion Notification (FECN):** notificación de congestión en el sentido de la transmisión.

- **Backward Explicit Congestion Notification (BECN):** notificación de congestión en el sentido contrario a la transmisión.

- **Discard Eligibility (DE):** las tramas que tienen este bit a 1 son susceptibles de descarte en situaciones de congestión.

2.3.7.2.2. Elementos QoS en Redes Frame Relay

Para cada conexión se puede contratar una calidad de servicio distinta, que establece las prestaciones que se obtendrá de la red y se define mediante el CIR, el cual es el caudal medio garantizado que la red se compromete a dar en una conexión durante un intervalo de tiempo.

Adicionalmente se debe tomar en cuenta que Frame Relay no es un protocolo diseñado para soportar tráfico multimedia, audio y vídeo en tiempo real, puesto que no hay garantías sobre el retardo del tráfico, pero en la práctica las redes suelen estar bien dimensionadas, el retardo del tráfico es pequeño y no varía apreciablemente y la disponibilidad de estas redes es muy alta, por lo que muchas empresas las utilizan para transportar los diferentes tipos de tráfico; por

este motivo se están incluyendo funciones QoS que proporcionen servicios diferenciados específicos para ciertas aplicaciones, entre las que se incluyen nuevas clases de servicio que permiten que el tráfico mixto fluya sin problemas por la misma línea Frame Relay[22]:

- **Real time variable frame rate:** es la velocidad de trama variable en tiempo real, que garantiza un cierto nivel de ancho de banda, bajo retardo, variación de retardo y pérdida de tramas. Permite definir acuerdos de nivel de servicio (SLA) con características específicas de entrega para tráfico sensible a los retardos.

- **Non - real time variable frame rate:** es la velocidad de trama variable en tiempo real, que permite asegurar un cierto ancho de banda, un retardo moderado y una baja pérdida de tramas y es utilizado en servicios de LAN a LAN y de acceso Internet / intranet para empresas.

- **Avalaible / Unspecified frame rate:** es la velocidad de trama disponible o sin especificar, que garantiza el mejor servicio posible utilizando cualquier ancho de banda disponible, se utiliza para correo electrónico y transferencia de archivos.

Para que resulte efectiva la calidad de servicio de Frame Relay se incluyen tres elementos principales, que ofrecen clases de servicio con diferentes niveles de prioridad. Estos elementos son:

- **Fair - Share queuing:** ofrece cada clase de servicio con una compartición equitativa del ancho de banda.

- **QoS aware circuit routing:** aporta un algoritmo inteligente y automático que establece las rutas a través de las redes Frame Relay para ofrecer los niveles de servicio requeridos.

- **QoS aware congestion control:** proporciona descarte inteligente de paquetes para cumplir las garantías de la clase de servicio.

2.3.8. Importancia de QoS en Redes IP

2.3.8.1. Problemática

Las redes IP se diseñaron para proporcionar el transporte óptimo y seguro del tráfico de datos, por lo que la calidad de servicio requerida en las mismas se basó únicamente en la integridad de los datos, esto es, no-pérdida de contenido, ni secuencialidad de los mismos y funcionamiento adecuado del tráfico sin requerimientos de tiempo real, como las aplicaciones de mail, FTP y navegación, pero no era apto para otras aplicaciones que no toleran retardos variables o pérdida de datos, como es el caso de servicios de voz y video en tiempo real.

La primera solución que emplearon los proveedores de servicios fue añadir más ancho de banda para reducir los niveles de congestión conforme el volumen de tráfico de Internet aumentaba, pero esta solución, representó pérdidas

económicas significativas para dichos proveedores, debido a que los incrementos de ancho de banda realizados para solventar las necesidades de las aplicaciones, no fueron directamente proporcionales a las ganancias por los servicios prestados en la red, lo que originó un modelo de negocios desventajoso para las empresas.

Posteriormente, los ISP´s (Proveedores de Servicio de Internet) conjuntamente con los grupos de trabajo de la IETF e IEEE, comenzaron a desarrollar mecanismos y esquemas para controlar de forma diferencial los servicios en las redes de datos. Los motivos fueron muy claros:

- Congestión en la red, retardos y pérdida de paquetes puesto que el agregar sólo ancho de banda no era suficiente.

- Incorporación de nuevos servicios de valor agregado.

- Convergencia de voz, video y datos en una sola red.

- Los requerimientos de QoS impuestos por el tráfico necesitaban mecanismos para controlar dichos parámetros de calidad y dar garantías de QoS.

En definitiva, la convergencia IP hace necesaria la incorporación de mecanismos de QoS que permitan la administración de los parámetros de calidad, como: ancho de banda, retardo, jitter y pérdida de paquetes, que son necesarios

para permitir el transporte de todo tipo de tráfico en la red IP. Los beneficios que se obtienen con la implementación de dichos mecanismos son[23]:

- **Usuarios:** posibilidad de contratar conexiones con garantías de calidad de servicio.

- **ISP (Proveedor de servicios de Internet):** ventaja competitiva con respecto a otros ISP's que no oferten servicios QoS.

- **Carriers:** manejo de un volumen mayor de tráfico, puesto que un carrier QoS transportará tráfico QoS + BE (tráfico con políticas de calidad de servicio y tráfico best effort).

2.3.8.2. Objetivo de QoS en las Redes IP

El objetivo fundamental es cuantificar el tratamiento que un paquete debe esperar a medida que circula por la red, tomando en cuenta que la calidad de servicio no puede crear ancho de banda adicional, sino que debe administrar el tráfico de manera que el ancho de banda disponible soporte los requerimientos de un amplio rango de aplicaciones, se proporcione retardo y jitter controlados (requerido por un cierto tráfico de tiempo real e interactivo) y características mejoradas para la pérdida de paquetes, garantizando que la provisión de prioridad a uno o más flujos no hará que otros flujos fallen.

2.3.9. Estándares QoS

A continuación se detallan las principales características de los mecanismos y protocolos empleados para ofrecer calidad de servicio[19]:

- **RSVP: Resource ReSerVation Protocol**

Es un protocolo de señalización de reservas encargado de reservar el ancho de banda en cada nodo y para cada conexión en forma dinámica; con señalización extremo a extremo y para cada flujo, se asigna prioridad según el tipo de tráfico y requiere que todos los nodos lo soporten, una vez que se realiza esta reservación no se puede reducir lo requerido.

- **MPOA: Multi - Protocol Over ATM**

Es un estándar del ATM Forum que especifica como múltiples protocolos de red pueden operar sobre un substrato de ATM, es decir que identifica flujos de datos y los asocia directamente en canales virtuales ATM; además introduce el concepto de router virtual, que emula la funcionalidad de los routers tradicionales y elimina las limitaciones en el rendimiento que tiene el routing salto a salto.

- **MPLS: Multi - Protocol Label Switching**

Este protocolo realiza el enrutamiento mediante la identificación y asociación de los paquetes IP con etiquetas de longitud fija, éstas se insertan

entre la cabecera del segundo y tercer nivel y se utilizan a partir de ese instante para el establecimiento de los caminos LSP (Label Switching Path) por la red.

- **IP Precedence**

Corresponde al campo tipo de servicio (TOS) de la cabecera IP versión 4 y se ha redefinido para su utilización en DiffServ.

- **DiffServ: Differentiated Services**

Estándar del IETF que proporciona clases diferenciadas de servicio a lo largo de una red IP; en función del marcado DSCP (DiffServ Code Point) los paquetes reciben un tratamiento particular o Per Hop Behavior (PHB) en cada elemento de la red.

- **PBR: Policy Based Routing**

Conocido como Layer 4 Switching, provee políticas de enrutamiento basadas en las definiciones del administrador de la red, es independiente del protocolo y utiliza route maps para crear procesos separados y así forzar las decisiones de enrutamiento, permitiendo balanceo de carga y políticas horarias, de seguridad, tarifarias y de backup.

- **COPS: Common Open Policy Service**

Define un modelo cliente / servidor sencillo para proporcionar control de políticas a protocolos de señalización de calidad de servicio, se basa en sencillos mensajes de petición y respuesta utilizados para intercambiar información de políticas de tráfico entre un servidor de políticas (PDP: Policy Decision Point) y sus clientes (PEP's: Policy Enforcement Points).

- **IEEE 802.1p y 802.1Q**

IEEE 802.1p: este esquema define 8 clases de servicio, entre 0 y 7, de manera que se asigna un tipo de prioridad a cada paquete en una etiqueta adicional de cuatro bytes, definida en el estándar IEEE 802.1Q.

IEEE 802.1Q: se utiliza para el etiquetado de tramas y define VLAN's (Virtual LAN's), en las que se asocian usuarios o aplicaciones con requerimientos similares y pueden ser creadas por puerto físico, dirección MAC o protocolo. Introduce un encabezado de etiqueta (se especifican doce bits para el identificador de la VLAN), dentro del encabezado Ethernet, después de la dirección MAC origen.

- **Redes inalámbricas – Estándar 802.11e**

El objetivo del estándar 802.11e es introducir nuevos mecanismos a nivel de la capa MAC para soportar los servicios y aplicaciones multimedia que

requieran garantías de calidad de servicio, dado esto la red debe tolerar valores de transmisión de datos garantizados para servicios individuales o retardos de propagación mínimos dando prioridad a cierto tráfico y previniendo colisiones y retrasos para que sean útiles con multimedia o voz.

CAPÍTULO III

3. ANÁLISIS DE LOS MODELOS DE CALIDAD DE SERVICIO

3.1. MODELOS QoS EXTREMO A EXTREMO

3.1.1. Definición

Los modelos de calidad de servicio se deben implementar globalmente y de extremo a extremo, puesto que de nada sirve priorizar y reservar ancho de banda para una aplicación en una parte de la red, si en el otro punto no se mantiene dicha prioridad, por eso; al hablar de calidad de servicio distinguimos los modelos de QoS extremo a extremo.

Un modelo de calidad de servicio describe un conjunto de capacidades QoS extremo a extremo que permiten entregar el servicio requerido por un tipo de tráfico específico de un extremo al otro de la red, de manera que se pueda estandarizar las políticas de calidad de servicio en la red, basándose en los parámetros: ancho de banda, retardo, jitter y pérdida de paquetes, que fueron analizados en el Capítulo 2, apartado 2.3.4.

3.1.2. Tipos

Los modelos QoS se diferencian uno de otro por la manera cómo permiten a las aplicaciones enviar datos y las formas en que la red procura entregar dichos

datos, por ejemplo, el modelo de calidad de servicio que se aplica en aplicaciones de tiempo real, tales como audio, videoconferencia y telefonía IP, es diferente al modelo que se utiliza en las aplicaciones de transferencia de archivos y de correo electrónico, además para decidir qué modelo QoS es apropiado para desplegar una red se debe considerar los siguientes factores[24]:

- La aplicación o el problema que se intenta solucionar, puesto que cada tipo de modelo es apropiado para ciertas aplicaciones y su elección depende del tipo de requerimientos de dichas aplicaciones.

- La tasa a la cual se puede realmente ampliar la infraestructura de la red, es decir la capacidad que se desea asignar a los recursos de la misma; debido a que existe una trayectoria natural de mejora de la tecnología necesitada para satisfacer a las aplicaciones.

- Análisis de costos y beneficios, puesto que el costo de implementar y desplegar un servicio diferenciado probablemente podría ser mayor que para un servicio best effort.

Los tipos de modelos de calidad de servicio extremo a extremo que pueden proporcionarse a través de una red son:

3.1.2.1. Best Effort – Mejor esfuerzo

Es un modelo de servicio predeterminado, que se conoce como carencia de QoS debido a que proporciona conectividad básica sin garantías, dado que una aplicación envía datos siempre que lo requiera, en cualquier cantidad y sin informar o pedir permiso a la red, de esta forma la red entregará los datos si puede, sin ningún aseguramiento de confiabilidad, límite de retardo o rendimiento.

Es caracterizado por las colas de tipo FIFO (First in first out), que no tienen ninguna diferenciación entre los flujos y no toman en cuenta las modificaciones por QoS y se lo considera conveniente para aplicaciones de red tales como transferencias de archivos y correo electrónico.

3.1.2.2. IntServ – Servicios Integrados

Es conocido como Hard QoS, debido a que proporciona un servicio garantizado, que consiste en la reservación absoluta de los recursos de la red para un tráfico específico y su uso exclusivo aún en momentos de congestión, dicha reservación está basada en la utilización de algún protocolo como RSVP (Resource Reservation Protocol) y se acepta solamente si los routers pueden servirla confiablemente.

En este caso, la aplicación solicita a la red un tipo de servicio específico antes de enviar datos para que así pueda cumplir con sus requerimientos de ancho de banda y retardo; una vez que se obtiene la confirmación de la misma se

procede con el envío de los datos y la red realiza el control de admisión en cada punto, basada en la información de la aplicación y de los recursos disponibles, se satisface el acuerdo mediante el mantenimiento del estado de reserva por cada flujo y realizando la clasificación del paquete, gestión de políticas (policing) y gestión de colas (queuing) de acuerdo a dicho estado.

3.1.2.3. DiffServ – Servicios Diferenciados

Se conoce como Soft QoS, debido a que los recursos no se reservan explícitamente, sino que el tráfico es dividido en diferentes clases, también llamadas clases de servicio (CoS), a las que la red provee un tipo particular de servicio basándose en su prioridad y en la especificación de QoS definida para cada una; además es necesario que la red diferencie el tráfico, controlando la cantidad de tráfico de una determinada clase permitida, para mantener la calidad de servicio que se le brinda a otros paquetes de la misma clase.

Permite la administración de políticas de tráfico y utiliza diferente información de la cabecera de los paquetes (por ejemplo, DSCP – DiffServ Code Point) para distinguir y clasificar los paquetes y así conocer el tratamiento que debe recibir el tráfico en cada nodo de la red.

3.2. MODELOS QoS EXTREMO A EXTREMOS PARA REDES IP

El IETF (Internet Engineering Task Force) ha definido dos modelos para la provisión de calidad de servicio extremo a extremo en una red IP, los cuales son:

a. IntServ - Servicios integrados

b. DiffServ - Servicios diferenciados

3.3. IntServ – ARQUITECTURA DE SERVICIOS INTEGRADOS

3.3.1. Generalidades

El desarrollo de esta arquitectura se basó en la idea de ofrecer una calidad de servicio garantizada a través de la realización de una reserva previa de la capacidad en toda la trayectoria por la que pasaría cada paquete de la aplicación, de manera que se solicite una clase de servicio en particular de la red antes de enviar datos y para esto cada elemento de la red debía conocer la existencia de dicha reserva; de esta forma se concibió un modelo similar en concepto a los circuitos ATM y se supuso el cambio del modelo no orientado a conexión, utilizado en Internet, al orientado a conexión.

Especifica los elementos para garantizar la calidad de servicio extremo a extremo a nivel de flujo de datos en las redes, es decir que mantiene un camino para cada paquete de dicha aplicación en base a los requerimientos necesitados mediante el establecimiento de un circuito virtual con garantías establecidas (Figura 3.1).

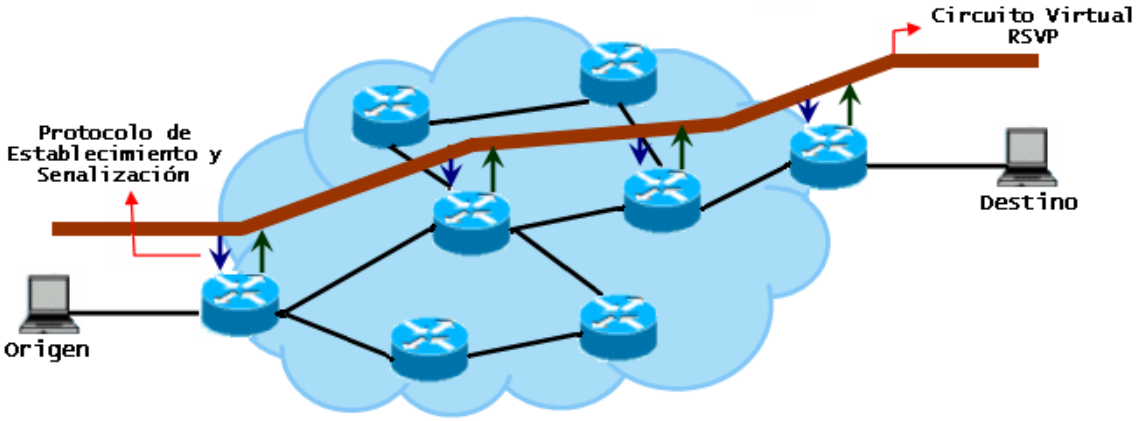


Figura 3.1: Servicios Integrados

Requiere una fase inicial de establecimiento del circuito y de un módulo en cada router a lo largo de la trayectoria para reservar los recursos necesarios de cada sesión y entonces asegurar que cada paquete en tránsito sea chequeado para ver qué recursos le corresponden recibir, este proceso implica:

- Realización de reservas del QoS deseado a lo largo de todo el camino que siguen los paquetes para cada flujo en la red, por lo que no se diferencia entre los distintos tipos de servicio.

- Almacenamiento del estado de los flujos en cada router implicado en dichas comunicaciones.

- Utilización de un conjunto de mecanismos de control de tráfico, métodos de señalización y estados flexibles de la red a través del protocolo RSVP (Resource Reservation Protocol).

- Es fundamental el concepto de flujo, que es una secuencia de datos individual, unidireccional entre dos aplicaciones y es identificado únicamente por la quíntupla (dirección IP origen, número de puerto del origen, dirección IP destino, número de puerto del destino y el protocolo de transporte).

- La reserva es soft - state, debido a que es necesario refrescar cada nodo de manera periódica, provocando una carga de señalización muy significativa.

3.3.2. Arquitectura

El objetivo del modelo IntServ es disponer de una sola red IP que transporte tráfico best effort y multimedia de tiempo real; bajo esta premisa se necesita que los host soliciten una QoS específica de la red para una aplicación o flujo de datos en particular y que los routers envíen las solicitudes de QoS a todos los nodos de la red, a lo largo de la trayectoria del flujo.

En la figura 3.2 se muestra el modelo de referencia de esta arquitectura[25], en la misma se especifican los elementos que deben incluirse en un router IP.

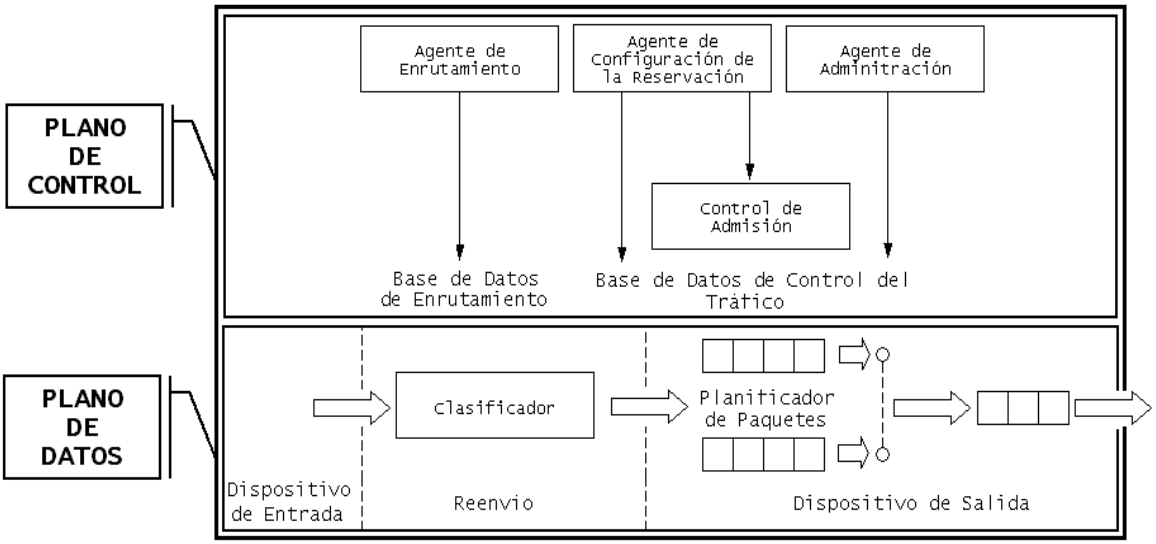


Figura 3.2: Modelo de referencia de IntServ

Como se puede apreciar en la figura 3.2, el router consta de dos divisiones funcionales:

a) Plano de control

Contiene las rutinas (Background code) para crear las estructuras de datos que controlan el plano de datos, las cuales son cargadas en la memoria del router y ejecutadas por el CPU (Unidad central de procesamiento) de uso general. Consta de los siguientes elementos:

- **Agente de enrutamiento:** implementa un protocolo particular de enrutamiento y construye una base de datos de enrutamiento.

- **Agente de configuración de la reservación:** implementa el protocolo usado para establecer las reservaciones del recurso. Si el control de admisión da la aceptación para una nueva petición, los cambios apropiados se realizan tanto en el clasificador como en la base de datos del planificador del paquete y de esta forma se implementa el QoS deseado.

- **Agente de administración:** cada router soporta un agente para la administración de la red, que puede modificar las bases de datos del clasificador y del planificador del paquete para fijar un enlace compartido controlado y las políticas del control de admisión.

b) Plano de datos

La trayectoria de envío (Forwarding path) se ejecuta para cada paquete y debe ser optimizada, por lo tanto, en la mayoría de los routers comerciales, la puesta en práctica de este plano implica la ayuda del hardware. Se divide en tres secciones:

- **Dispositivo de entrada:** corresponde al dispositivo ubicado en el ingreso.

- **Reenvío:** para cada paquete, ejecuta un clasificador y después pasa el paquete al dispositivo de salida apropiado; para esto requiere un mecanismo común para la clasificación del recurso y las operaciones de búsqueda de la ruta.

- **Dispositivo de salida:** implementado por el planificador de paquetes.

La implementación del marco de referencia para un host es generalmente similar a la de un router, con la adición de aplicaciones, puesto que los datos de un host se originan y terminan en una aplicación, que al requerir un QoS específico debe invocar de alguna manera a un agente local para la configuración de la reservación.

3.3.2.1. Componentes

Para proporcionar garantías por flujo, se requieren lo siguientes componentes[25]:

- Control de tráfico
- Reservación de recursos

3.3.2.1.1. Control del tráfico

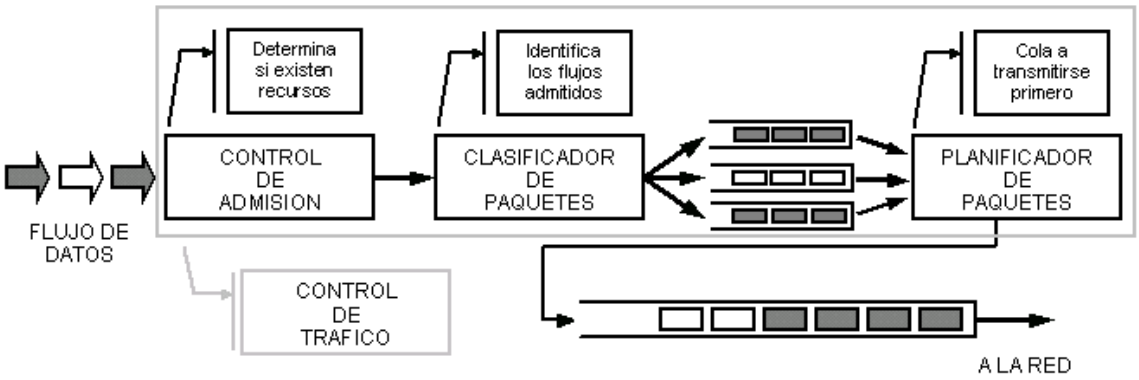


Figura 3.3: Elementos que constituyen el control del tráfico

La figura 3.3[26] identifica las etapas por las que pasa un flujo de tráfico, definidas a través de cada uno de los componentes asociados al Control del tráfico.

En primer lugar es necesario conocer que el flujo se refiere a un tráfico continuo de datagramas relacionados entre sí que se produce como consecuencia de una acción del usuario y que requiere una misma calidad de servicio. Los flujos pueden agruparse en clases, en las que se recibe la misma calidad de servicio.

En IPv4 los flujos se identifican por las direcciones de origen y destino, el puerto de origen y destino (a nivel de transporte) y el protocolo de transporte utilizado (TCP o UDP), mientras que en IPv6 la identificación puede hacerse de la

misma forma que en IPv4, o alternativamente por las direcciones de origen y destino y el valor del campo etiqueta de flujo.

El control del tráfico es la función que permite crear diferentes clases de servicio en un router y para ejecutarse requiere de tres elementos, que se observan en la figura 3.2 y se detallan a continuación:

a) Control de admisión

Implementa el algoritmo de decisión que un router o un host utiliza para determinar si a un nuevo flujo se le puede conceder la calidad de servicio solicitada sin afectar las garantías previamente establecidas y sin comprometer más recursos de los que se encuentran disponibles. Las funciones básicas del control de admisión son:

- Monitorear y medir los recursos disponibles.

- Determinar si una reserva puede ser establecida basándose en las políticas de control de admisión, además de asegurarse que las garantías de QoS estén resueltas, el control de admisión se utiliza para cumplir las políticas administrativas en reservaciones del recurso, entre las que se exige la autentificación de quienes solicitan las reservaciones.

Se invoca en cada nodo a través de la red para decidir localmente si se acepta o rechaza la solicitud de acuerdo a la existencia de recursos suficientes para soportar el servicio y de esta forma encontrar una ruta que satisfaga dichos requerimientos.

El algoritmo del control de admisión debe ser consistente con el modelo de servicio y se encargará de decidir cuándo una petición de reservación debe ser rechazada, puesto que si todas las peticiones fueran aceptadas, eventualmente se introduciría demasiado tráfico en la red y ninguno de los flujos conseguiría el servicio solicitado.

b) Clasificador de paquetes

Coloca cada paquete entrante en colas individuales de acuerdo a una clase, en la cual se consigue el mismo tratamiento del planificador de paquetes. La elección de una clase en particular se basa en el análisis del contenido de los campos de direcciones y puertos de la cabecera del paquete y/o de un cierto número de clasificación adicional añadido a cada paquete.

c) Planificador de paquetes

Se encarga de la transmisión de los diferentes paquetes por un enlace de salida a través de un sistema de colas y quizás otros mecanismos como contadores de tiempo. Debe implementarse en el punto donde se encolan los

paquetes, afectando directamente al retardo que experimentan los paquetes y es el responsable de la asignación de recursos.

3.3.2.1.2. Reservación de recursos

Para que una aplicación solicite un determinado servicio a la red, por ejemplo, el ancho de banda y retardo necesitado por un flujo en particular, se requiere de un protocolo, que entregue la petición al control de tráfico de cada elemento de la red, donde se comprueba si es viable la petición y si la señalización se completa exitosamente, los componentes de la red reservan los recursos necesarios y mantienen información del estado de las reservas de cada uno de los flujos; dicho protocolo transporta información sobre la caracterización del tráfico y los requerimientos de los recursos y se denomina RSVP (Resource Reservation Protocol); se detallarán sus características en el apartado 3.3.4.

3.3.2.2. Tipos de servicio

En la arquitectura IntServ, de acuerdo a los requerimientos de calidad de servicio exigidos por las aplicaciones se definen dos tipos de servicio:

- Servicio garantizado
- Servicio de carga controlada

3.3.2.2.1. Servicio garantizado

Este servicio se define en el RFC 2212, Especificación de la calidad de servicio garantizada, que describe el comportamiento requerido para que cada elemento de red pueda entregar un servicio con un determinado ancho de banda y retardo[27].

Como su nombre lo indica garantiza que los paquetes llegarán dentro del plazo de entrega establecido y no serán descartados debido a los sobreflujos de la cola, siempre que el tráfico del flujo permanezca dentro de los parámetros especificados y por esta razón solo se controla el retardo máximo en las colas y no el jitter.

En este caso cada elemento de la red caracteriza el servicio garantizado para un flujo determinado, asignando un ancho de banda y un espacio de memoria, que representa los recursos que el flujo puede consumir; de esta forma se proporciona un servicio con límites firmes en el retardo extremo a extremo, se asegura el ancho de banda para el tráfico que se conforma con las especificaciones reservadas y no existe pérdida en las colas.

Se utiliza para aplicaciones como voz y video que tienen requerimientos exigentes de tiempo real y necesitan una garantía firme que llegue un paquete después de un cierto tiempo de que fuera transmitido por el emisor.

3.3.2.2.2. Servicio de carga controlada

Las características de este servicio se describen en el RFC 2211, Especificación del servicio de elementos de red de carga controlada, que define que este servicio provee a los clientes, flujos con una calidad de servicio equivalente al QoS que el mismo flujo recibiría de un elemento de red con poca carga y en caso de que dicho elemento esté sobrecargado se utiliza la capacidad del control de admisión para asegurar que este servicio sea recibido[28]; es decir que esta clase de servicio es equivalente al servicio best-effort en condiciones de red ligeramente cargada puesto que suministra un mejor servicio que éste con un buen tiempo de respuesta y con esto el flujo no se deteriora aunque aumente la carga de la red, pero hay que tomar en cuenta que no proporciona garantías estrictas. Asumiendo que la red está funcionando correctamente, las aplicaciones deben considerar lo siguiente:

- Un porcentaje muy alto de paquetes transmitidos será entregado con éxito por la red a los nodos finales, donde el porcentaje de los paquetes no entregados se aproxima al índice de error básico del paquete por el medio de transmisión.

- El retardo experimentado por un porcentaje muy alto de los paquetes entregados no excederá al mínimo retardo experimentado por cualquier paquete entregado exitosamente, donde el retardo mínimo incluye el tiempo de procesamiento en los routers y otros dispositivos de comunicación a lo largo de la trayectoria.

Para asegurar estas condiciones, los clientes que solicitan un servicio de carga controlada deben proporcionar a los elementos intermedios de la red, una estimación del tráfico que generarán y cada elemento que acepta un pedido debe asegurarse que el ancho de banda adecuado y los recursos de procesamiento de paquetes estén disponibles para manejar el nivel de tráfico solicitado. Todos los recursos importantes para la operación del elemento de la red deben ser considerados al admitir una petición, como: ancho de banda del enlace, buffer del puerto del router o el switch y la capacidad para el envío del paquete.

Provee servicio de bajo retardo para así moderar las cargas de la red y la pérdida de paquetes es baja o nula por lo que es adecuado para aplicaciones sensibles a condiciones de congestión en la red.

3.3.3. Funcionamiento

Hasta ahora se han descrito todos los elementos que componen la arquitectura IntServ y a continuación se explicará la interacción de cada uno de ellos y su funcionamiento en un contexto general.

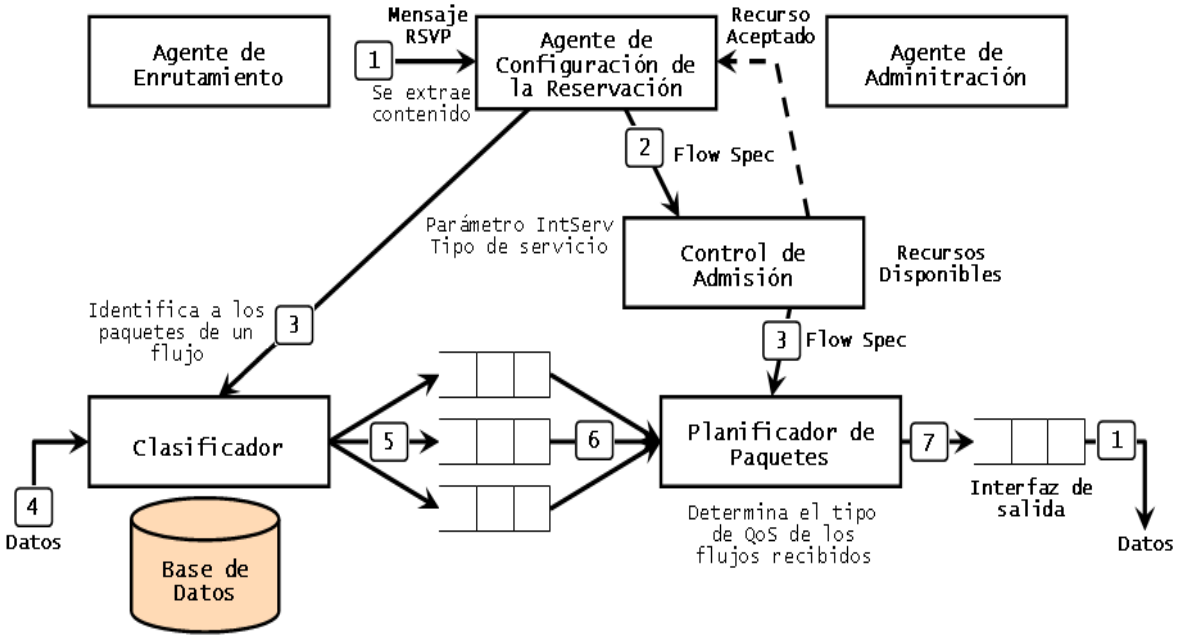


Figura 3.4: Funcionamiento de IntServ

Como se aprecia en la figura 3.4[26], la idea básica de este modelo es que una aplicación debe reservar recursos a lo largo del camino antes de iniciar la transmisión de los paquetes, es decir debe indicar explícitamente sus necesidades de QoS para un flujo y para conseguir esto:

a) El origen inicia el establecimiento de una reserva a través de la caracterización de su flujo de tráfico, conocido como especificación de flujo (Flow Spec: flow specification), que es un contrato de servicios que especifica el tráfico que el origen enviará y los recursos y servicios que la red se compromete a prestar, por lo tanto describe para quiénes es la reservación y envía esta información a cada router de la trayectoria mediante un protocolo de señalización (RSVP), que es el mecanismo subyacente para señalar la reserva a través de la red. Flow Spec consta de dos partes:

- **TSPEC (Traffic SPECification):** son las características del flujo que se inyectará a la red, es decir el patrón de tráfico.

- **RSPEC (Request SPECification):** son los requerimientos de los recursos para el flujo, es decir el QoS deseado.

b) La red puede aceptar este nuevo flujo de aplicación solo si hay suficientes recursos para comprometerse con los recursos solicitados y para esto cada router que recibe la solicitud a través del flow spec que fue llevado por el protocolo de señalización, realiza dos tareas:

   - Interactúa con el módulo de enrutamiento para determinar el siguiente salto al que debe ser enviada la solicitud de reserva.

   - Coordina con el control de admisión para decidir si dispone de recursos suficientes, reservándolos en caso afirmativo y rechazando la sesión en caso negativo.

c) Una vez la reserva es establecida, la información del flujo reservado es instalada en la tabla de reserva de recursos para que la aplicación pueda enviar sus paquetes a lo largo del camino reservado y que la red mantenga su compromiso.

La información de la reserva de recursos se usa para configurar el clasificador de paquetes y el planificador de paquetes, de esta forma cuando

lleguen los flujos, el clasificador de paquetes selecciona aquellos que pertenecen a los flujos reservados y los coloca en las colas apropiadas, de acuerdo a los campos de la cabecera del paquete (llamados quíntupla):

- Dirección IP origen
- Dirección IP destino
- Identificación del protocolo
- Puerto origen
- Puerto destino

Para determinar si un paquete coincide con un flujo, el planificador de paquetes compara la quíntupla del paquete entrante con la quíntupla de todos los flujos de la tabla de reservas y si coinciden, se envía el paquete junto con el estado de la reserva asociada con dicho flujo al planificador de paquetes, donde se asigna los recursos a los flujos basado en la información de la reserva.

3.3.4. Protocolo RSVP (Resource ReserVation Protocol)

3.3.4.1. Definición

Es un protocolo de señalización de QoS que permite a las aplicaciones establecer reservas de recursos a lo largo de una ruta, garantizando de esta forma un cierto nivel de QoS y el establecimiento y el control de los Servicios Integrados[29].

Es un protocolo orientado a conexión, que se desarrolla entre los usuarios y la red y entre los diferentes nodos (routers) de dicha red, consiste en que el host solicite un QoS al router para un aplicación particular y que los routers reserven los recursos necesarios para cada flujo de información de usuario cuando reciben la petición, guarden la información del estado de cada flujo para el que se efectúa la reserva y confirmen la petición con el intercambio de mensajes RSVP entre los nodos de la ruta, de manera que tanto la solicitud de las reservas, como el mantenimiento de éstas durante la comunicación y la posterior cancelación, implica el intercambio de mensajes de señalización para mantener el soft state.

3.3.4.2. Características

Entre las principales características del protocolo RSVP tenemos:

- Reserva ancho de banda en cada nodo y para cada flujo en forma dinámica, mediante la señalización extremo a extremo, además puede solicitar cierta cantidad de retardo.

- Utiliza el soft – state para la renovación de reservas, donde se refresca periódicamente las reservas, lo que conlleva a cierta señalización permanente durante la fase de transferencia de información de usuario, además cuenta con un temporizador (timer) y cuándo éste expira se cancelan las reservas.

- Es independiente de la política de reserva de recursos puesto que no especifica la forma en la que la red debe garantizar los recursos reservados, no es un protocolo de encaminamiento, ni decide sobre qué enlaces se deben hacer las reservas, únicamente se encarga de la señalización.

- Está orientado hacia el receptor, quien inicia, mantiene una reserva para cada flujo de datos y la interrumpe.

- Se realizan reservas simples en una sola dirección, en el caso bidireccional deben ser realizadas por cada extremo.

- Permite la convivencia con routers (tanto IPv4 como Ipv6) que no implementan RSVP sino que ofrecen el clásico servicio best effort.

- Es un protocolo situado en el nivel de transporte y es el más complejo de todas las tecnologías de QoS, tanto para los sistemas finales como para los nodos de la red, puesto que representa el mayor cambio con relación al servicio best effort de IP y una mayor complejidad y procesamiento, lo cual no es apropiado para muchas aplicaciones y partes de la red.

- No permite negociar la reducción de la reserva solicitada, una vez que se reservan los recursos si éstos no se utilizan se pierden.

3.3.4.3. Funcionamiento

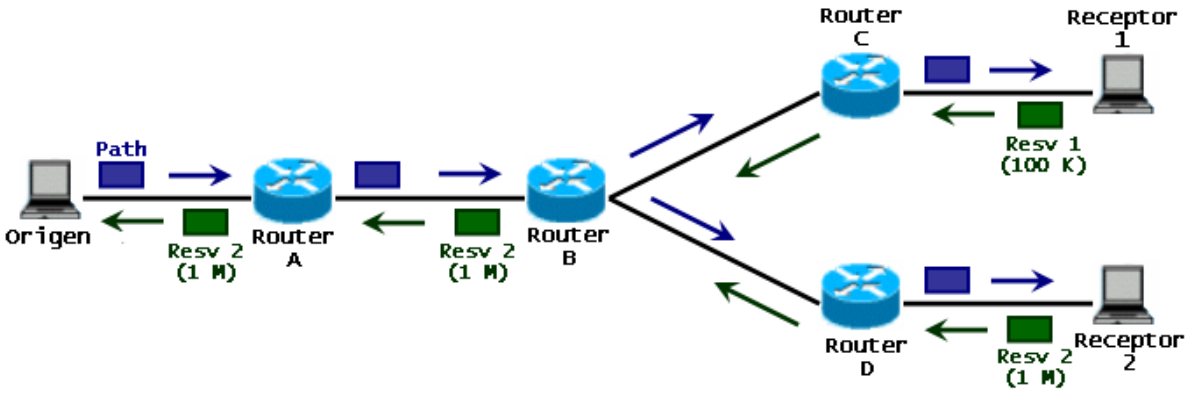


Figura 3.5: Mensajes básicos de RSVP

Los hosts generan mensajes de señalización que describen un tráfico de datos en particular por lo que el protocolo RSVP define dos mensajes básicos (Figura 3.5) a través de los cuales se lleva a cabo la reserva de recursos en la red como paso previo a la comunicación; estos mensajes son:

- **PATH**

Son generados por la fuente de tráfico para indicar al receptor(es), las características del tráfico de usuario y la ruta por donde debe solicitar las correspondientes reservas de recursos y proveer la información de estado necesaria para que los mensajes de reserva encuentren al origen. Su propósito es marcar la ruta entre emisor y receptor además de recolectar información sobre la viabilidad de la solicitud a lo largo del camino.

Estos mensajes se actualizan y retransmiten en su paso por cada router RSVP a través de la dirección IP de dicho router, donde también se almacena la

dirección del router anterior. Los routers que no soportan RSVP transfieren transparentemente estos mensajes.

La ruta que deben seguir estos mensajes es la misma que siguen los datos de usuario y por esto se requiere que previamente se establezca un diálogo entre el proceso RSVP y el de enrutamiento, quien determina la ruta.

- **RESV**

Son producidos por el receptor(es) de los flujos de información de usuario, como respuesta a los mensajes PATH's y de acuerdo a la información de ruta que éstos suministran, solicitan a la red, las correspondientes reservas de recursos para soportar la comunicación con cierta QoS, esto es, por donde se transmitirán los flujos de datos y una vez que se recibe el mensaje RESV, el origen empieza a transmitir información a lo largo de las rutas reservadas.

Los mensajes RESV´s especifican el ancho de banda mínimo que se requiere para obtener determinada demora en un flujo de datos específico, además, es posible efectuar reservas compartidas, esto es, una misma reserva aplicable a varios flujos de datos de usuario.

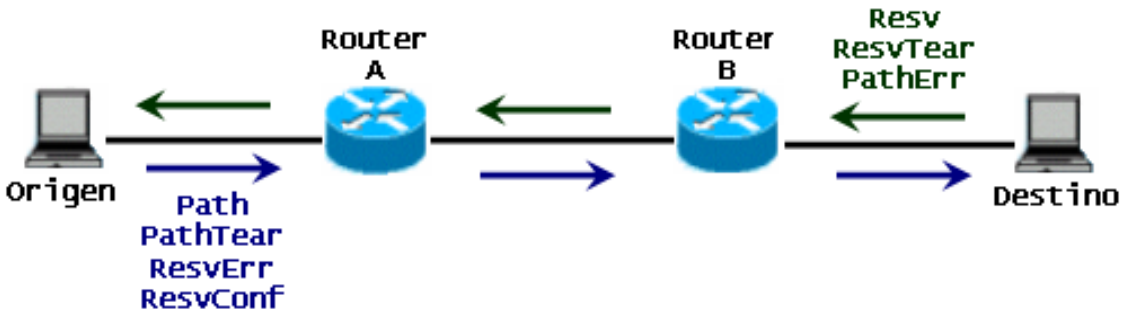


Figura 3.6: Dirección de los mensajes RSVP

Como se observa en la figura 3.6, RSVP además establece dos sentidos para la transferencia de los mensajes de señalización, el flujo downstream que se efectúa desde el origen al receptor y el flujo upstream desde el receptor al origen e incluye otros mensajes como[30]:

- **PATHTEAR:** se genera por la fuente de datos de usuario para eliminar los estados PATH's en todos los routers RSVP o puede ser originado por cualquier nodo cuando se agota el timeout del estado PATH. Este mensaje sigue la misma ruta que los mensajes PATH´s.

- **RESVTEAR:** se genera por los receptores para borrar los estados de reserva en los routers RSVP, por tanto viaja en el sentido upstream, pueden también ser originado por nodos RSVP al agotarse el timeout del estado de reserva de los mismos.

- **PATHERR:** viaja en sentido upstream hacia el origen siguiendo la misma ruta que los mensajes PATH´s y notifica errores en el procesamiento de mensajes PATH´s, pero no modifican el estado del nodo por donde ellos pasan en su viaje hacia la aplicación origen.

- **RESVERR:** notifica errores en el procesamiento de mensajes RESV o la interrupción de una reserva y se transfiere en la dirección downstream hacia el receptor o receptores apropiados.

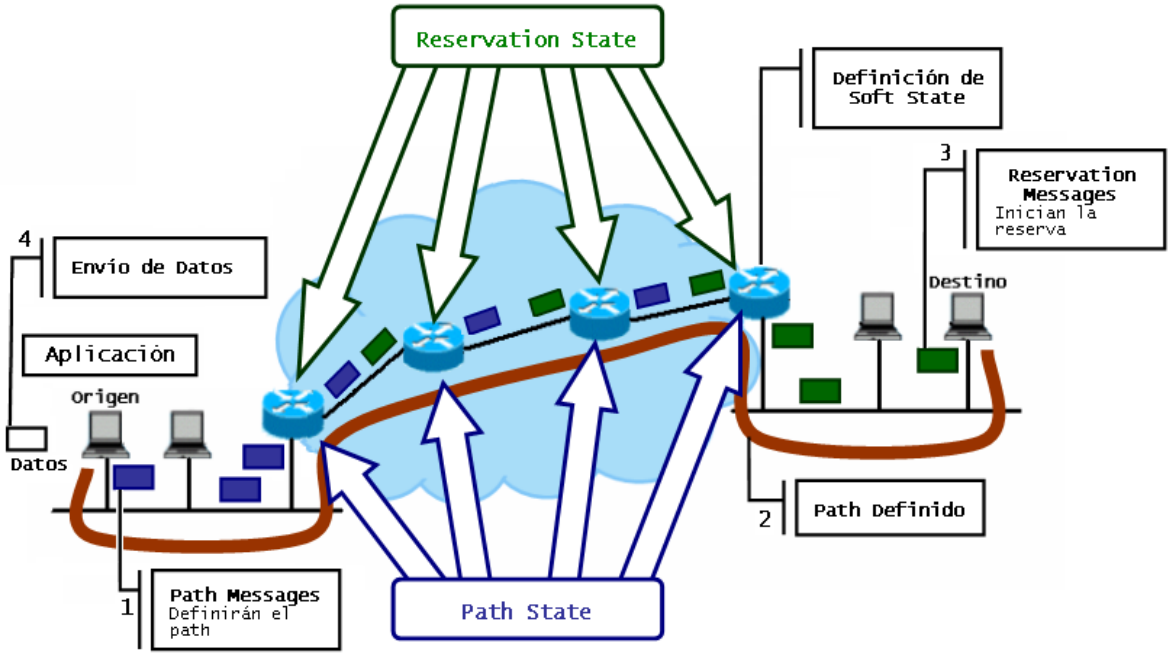


Figura 3.7: Mecanismo de reserva del protocolo RSVP

En la figura 3.7[26] se aprecia el mecanismo que sigue el protocolo RSVP para efectuar la reserva y se describe a continuación:

a) El emisor envía un mensaje PATH, con su especificación de tráfico (TSpec), que incluye los valores máximo y mínimo de ancho de banda, retardo y variación del mismo, hacia el destino.

b) Cada router va grabando la ruta por la que circula el mensaje PATH y añade la dirección IP de donde viene el mensaje, para después reconstruir

la ruta de regreso. Cuando llega el mensaje PATH al receptor, pueden medir qué tipo de servicio puede soportar la red.

c) El receptor realiza la reserva de recursos, al enviar por el camino inverso a PATH, un mensaje RESV, que incluye la especificación de tráfico (TSpec) recibida del emisor y la especificación requerida por el receptor (Rspec), 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 routers está compuesto por el tipo de Servicio Integrado y el filtro.

d) Cuando un router recibe un mensaje tipo RESV, usa el control de admisión para aceptar o no la reserva. En caso positivo se hace la reserva, asignando los recursos necesarios y se pasa el mensaje RESV al siguiente router en la dirección del emisor, en caso contrario se envía un mensaje de error ResvErr al receptor. Si el router no soporta RSVP retransmite los mensajes RSVP de forma transparente y no se garantiza el QoS.

e) Si el último router efectúa la reserva envía un mensaje de confirmación al receptor.

f) Para actualizar las rutas ante eventuales fallos se envía mensajes PATH cada cierto tiempo, desencadenando el envío por parte de los receptores de nuevos mensajes RESV para mantener la reserva o realizar otra por la

nueva ruta. La liberación de recursos reservados mediante RSVP puede originarse por:

- Parte del emisor o de un receptor, cuando así lo decide la aplicación correspondiente, en cuyo caso esto se produce mediante la generación de un mensaje PATHTEAR o un mensaje RESVTEAR, respectivamente.

- Parte de un nodo, cuando vence el timeout correspondiente del estado PATH o del estado de reserva, lo que origina la emisión de un mensaje PATHTEAR o un mensaje RESVTEAR, respectivamente.

3.4. DiffServ – ARQUITECTURA DE SERVICIOS DIFERENCIADOS

3.4.1. Generalidades

Es un estándar del IETF, que a diferencia de IntServ (Servicios Integrados), proporciona clases predeterminadas de servicio a agregados de tráfico unidireccionales en toda la trayectoria de una red IP; a través de métodos para categorizar y marcar el tráfico, asignar prioridades a los agregados y posteriormente recibir los parámetros de calidad de servicio requeridos.

Los servicios diferenciados proporcionan mecanismos de calidad de servicio que asocian los flujos de tráfico a los niveles de servicio deseados y

especifican nuevas funcionalidades en los routers para permitir un mejor control en la distribución de recursos o en los tiempos de transmisión de los paquetes y reducir la carga en estos dispositivos, básicamente se administra y asigna prioridades a los diferentes paquetes que son enviados a la red.

El modelo DiffServ está orientado hacia un servicio extremo a extremo a través de un dominio único y define que los paquetes deben clasificarse en el punto de ingreso a la red, en este caso los paquetes que pertenecen a una determinada clase se marcan usando un campo de 6 bits, denominado DSCP (DiffServ CodePoint), que se encuentra en la cabecera IP y permite 64 clasificaciones diferentes; en función de dicho marcado, los paquetes reciben un tratamiento particular o Per Hop Behavior (PHB) en cada elemento de la red.

El objetivo principal de esta arquitectura es asignar el ancho de banda de la red a diferentes usuarios en una forma controlada durante períodos de congestión y se utiliza para aplicaciones como: transferencia de archivos, acceso a bases de datos, servidores Web y aplicaciones de audio o video en tiempo real. Los Servicios Diferenciados pueden proveer a los usuarios, una expectativa predecible del servicio que la red le entregará en caso de congestión y permite que los usuarios obtengan diferentes niveles de servicio.

3.4.2. Características

El enfoque básico del modelo de Servicios Diferenciados presenta las siguientes características:

- Diferencia el tráfico a nivel de agregados que recibirán tratamiento similar, puesto que no existen flujos individuales ni paquetes best effort.

- Se establece un número limitado de clases de servicio denominadas forwarding classes (clases de reenvío), cada una de las cuales representa un comportamiento predefinido en términos de asignación de ancho de banda y descarte de paquetes y es independiente del número de flujos o usuarios y de complejidad compleja.

- En un dominio de Servicios Diferenciados (DS) se realiza funciones de marcado, clasificación de paquetes y reenvío de paquetes mediante la asignación de recursos por clase.

- Se clasifica los paquetes en clases (según el tipo de servicio solicitado) a la entrada de la red (dominio), donde se marcan los paquetes, para que posteriormente los routers traten cada paquete según su clase, que viene marcada en su cabecera y así ofrecer un servicio diferenciado por clase, que se conoce como comportamiento agregado.

- Cada tipo de tráfico se etiqueta en un campo de la cabecera del paquete IP, que se denomina: DSCP (Differentiated Services CodePoint), que permite marcar paquetes para seleccionar el comportamiento en cada salto.

- Garantiza los recursos que se asignan a cada servicio (tipo de tráfico) por provisionamiento y no por establecimiento de la reserva.

- El control de políticas / control de admisión se efectúa únicamente en los routers de entrada a la red del proveedor y en los que atraviesan fronteras entre proveedores diferentes (normalmente en las fronteras entre sistemas autónomos).

- A cada clase le corresponde un Acuerdo de nivel de servicio (SLA) que se negocia previamente con el ISP a través de un contrato que suele tener carácter estático y que especifica qué clases de tráfico serán proporcionadas, qué garantías son necesarias para cada clase y cuántos datos serán enviados para cada clase.

3.4.3. Arquitectura

Existe una clara necesidad por métodos relativamente simples que permitan mantener clases diferenciadas de servicio para el tráfico de Internet, apoyar todo tipo de aplicaciones y los requisitos comerciales específicos[31]. El servicio diferenciado proporciona calidad de servicio en las redes que emplean un bien definido conjunto de bloques de construcción en los cuales una variedad de comportamientos agregados pueden definirse.

Esta arquitectura está compuesta por varios elementos funcionales implementados en los nodos de la red, incluyendo un pequeño conjunto de

comportamientos de reenvío por salto, funciones de clasificación de paquetes y funciones de condicionamiento del tráfico, incluyendo: medición (metering), marcado (marking), conformación (shaping) y gestión de políticas (policing). Se mantiene una distinción entre [31]:

- El servicio proporcionado a un agregado de tráfico.

- Las funciones de condicionamiento y comportamiento por salto usadas para cumplir los servicios.

- El valor del campo DS (punto de código DS) permite marcar los paquetes para seleccionar el comportamiento por salto.

- Los mecanismos de implementación de nodos particulares que realizan el comportamiento por salto.

- Esta arquitectura sólo proporciona la diferenciación del servicio en una dirección de flujo de tráfico.

La arquitectura de servicios diferenciados está basada en un modelo simple donde el tráfico que ingresa a una red es clasificado y posiblemente condicionado y asignado a diferentes comportamientos agregados en los límites de la red. Cada comportamiento agregado se identifica por un solo codepoint DS. En el núcleo de la red, los paquetes son reenviados de acuerdo al comportamiento por salto asociado con el codepoint DS. A continuación se

describirán los elementos que permiten entregar la calidad de servicio extremo a extremo, los principales componentes de esta arquitectura y sus funciones.

3.4.3.1. Campo DS (Differentiated Services)

3.4.3.1.1. Generalidades

DiffServ categoriza el tráfico en diferentes clases, también llamadas Clase de Servicio (CoS) y aplica los parámetros de QoS a esas clases; para lograr esto, los paquetes son divididos en clases, marcando un nuevo campo en la cabecera IP. Este modelo establece un campo que reemplaza a las definiciones existentes del campo ToS (Tipo de servicio) en el caso de IPv4 y del campo Clase de tráfico en IPv6, que se conoce como Campo Servicios Diferenciados (DS), por el modelo al que pertenece y se define en el RFC 2474, Campo Servicios Diferenciados[32].

Este campo indica el nivel de calidad de servicio que se va a recibir de acuerdo a la definición de prioridades de los paquetes, es decir que el tráfico es clasificado en una red y que toda la clase de servicio está dada por una prioridad; en este caso de acuerdo a la etiqueta que lleva cada paquete se obtiene el tratamiento en cada nodo de la red.

El campo DS es utilizado por los routers o host que envían tráfico a una red DiffServ para marcar cada paquete transmitido con el valor DSCP, mientras que los routers de ingreso de la red DiffServ utilizan este valor para clasificar los paquetes y aplicar un comportamiento específico basado en los resultados de

dicha clasificación. El tráfico de varios flujos con requisitos de calidad de servicio similares se marca con el mismo valor DSCP, para agregar el flujo a una cola común o definir el comportamiento.

La principal función del campo DS es el marcado de paquetes, el cual puede ocurrir en dos lugares:

- Fuente original del tráfico, cuya ventaja es que el clasificador puede tener conocimiento explícito de la aplicación en uso y puede por consecuencia marcar paquetes dependiendo de la aplicación.

- El primer router que encuentra, clasifica y marca el tráfico; para lo cual se requiere de alguna capacidad extra en los routers.

3.4.3.1.2. Estructura

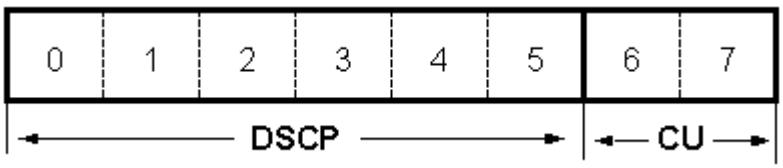


Figura 3.8: Campo DS

La arquitectura DiffServ se basa en que la información sobre calidad de servicio debe almacenarse en los datagramas y no en los routers de la red y para conseguir esto se utiliza el campo DS, cuya estructura se muestra en la Figura 3.8, en la que se observa que el campo se compone de ocho bits, divididos de la siguiente manera:

- **DSCP (Differentiated Service CodePoint), Punto de Código de Servicios Diferenciados**

Seis bits corresponden a este subcampo y se usa para marcar un paquete con un patrón específico de bits llamado código DS, de modo que seleccione el comportamiento por salto, es decir el tratamiento particular de envío que el paquete recibirá en cada nodo.

Permite definir hasta 2^6 = 64 posibles codepoints (categorías / clases de tráfico) diferentes, que es un valor específico del campo DS. En la práctica se utilizan 32 posibles categorías, correspondientes a los cinco primeros bits del campo DS, cuyos valores se dividen en los grupos descritos en la Tabla 3.1:

Tabla 3.1: Grupos de Puntos de Código del campo DS

Codepoint	Valores	Uso
xxxyy0	32	Estándar
Xxxx11	16	Local/Experimental
Xxxx01	16	Reservado

En el grupo Estándar los tres primeros bits (‘xxx’) indican la clase y los dos siguientes (‘yy’) se usan para el marcado intra clase (mayor o menor precedencia de descarte). Los códigos extra restantes permiten la innovación y optimizaciones operacionales locales.

- **CU (Currently unused), No usado actualmente**

Dos bits corresponden a este subcampo, cuyo valor es ignorado por los nodos DS cuando se determina el comportamiento por salto que se debe aplicar al paquete recibido, debido a que es reservado para uso futuro o se lo utiliza de forma experimental para el ECN (Explicit Congestion Notification), que es un mecanismo de control de la congestión.

3.4.3.1.3. Comparación de los campos ToS y Clase de tráfico

Cada paquete IP incluye en su cabecera un campo de ocho bits, denominado Tipo de Servicio (ToS) en el caso de IPv4 y Clase de tráfico para IPv6, que se constituye como una característica poco utilizada de IP puesto que no se ha implementado comúnmente en los routers.

En el caso de IPv4, el RFC 791, Protocolo IP, definió como parte del datagrama IPv4, un campo llamado ToS (Tipo de servicio) que permitiría marcar un paquete para el tratamiento con herramientas de QoS y cuya estructura fue posteriormente redefinida en el RFC 1349, Campo ToS, en el que se dividen los tres primeros bits para la Precedencia IP, qué puede marcarse para los propósitos de involucrar una clase particular de servicio e implica qué cuánto más grande es el valor, más importante es el tráfico; los siguientes cuatro bits se utilizan para el campo ToS, que tiene banderas para proporcionar un servicio QoS específico y finalmente el último bit corresponde a MBZ y tiene el valor de cero; dicho campo se analizó en el apartado 2.1.1.1. Formato del Datagrama IP del Capítulo 2.

El campo ToS prácticamente no ha sido utilizado y ha tenido un despliegue limitado, pues los routers no procesaban esta información, además, con igual resultado se empleaban los bits de prioridad y por este motivo el campo DS redefine el byte ToS en la cabecera IP, en primer lugar eliminando la definición de los cuatro bits ToS (bits 3 al 6) y creando un reemplazo para el campo de Precedencia con un nuevo campo de seis bits llamado campo de Servicios Diferenciados (DS). La figura 3.9 muestra los campos dentro del byte ToS[9] y el campo DS[32].

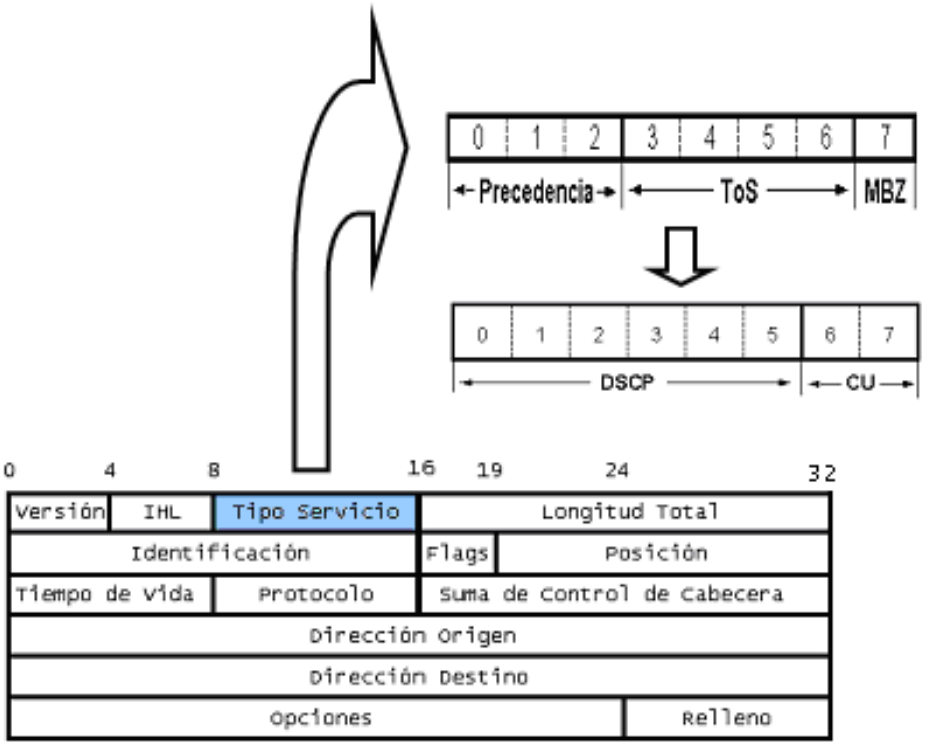


Figura 3.9: Campo ToS y DS en IPv4

Para evitar los problemas de compatibilidad con el campo ToS, DiffServ se aprovechó del hecho que el subcampo ToS (bits 3 al 6) no fue usado comúnmente, por lo tanto solo se encargó de construir la compatibilidad con el subcampo Precedencia; en este caso dado que DiffServ casi siempre utiliza solo

los tres primeros bits de DSCP para marcar los paquetes y que los servicios de más prioridad, se asocian con los valores más altos de esos tres bits y que el campo Precedencia no hacía uso de los dos niveles de prioridad más altos, que quedaban reservados para mensajes de gestión de la red, como datagramas del protocolo de enrutamiento; en DiffServ se han reservado también los dos valores más altos de los tres primeros bits, con lo que se mantiene la compatibilidad entre los dos campos (Tabla 3.2); sin embargo el avance fundamental que provee esta arquitectura, sobre TOS, es que este aplica el mecanismo de control de admisión en el punto de entrada de una red.

Tabla 3.2: Correspondencia entre los subcampos Precedencia de ToS y DSCP de DS

Valor Campo Precedencia	Servicio DiffServ correspondiente
7	Reservado
6	Reservado
5	Expedited Forwarding
4	Assured Forwarding Clase 4
3	Assured Forwarding Clase 3
2	Assured Forwarding Clase 2
1	Assured Forwarding Clase 1
0	Best Effort

En el caso de IPv6 para realizar el marcado de paquetes se reemplaza el campo “Clase de tráfico” por el campo DS, que tiene el mismo significado que en IPv4, lo que implica que este campo es válido en las dos versiones. La figura 3.10 muestra el formato de la cabecera de IPv6.

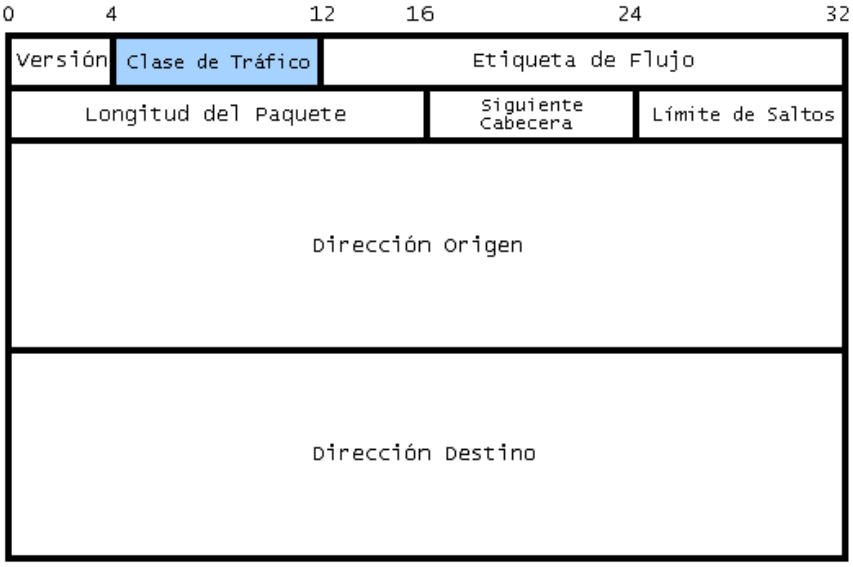


Figura 3.10: Cabecera de IPv6

3.4.3.2. Comportamiento por salto – PHB (Per Hop Behavior)

3.4.3.2.1. Definición

La arquitectura de servicios diferenciados consiste en agrupar los flujos de tráfico IP en agregados, dentro de los cuales, los paquetes recibirán un tratamiento específico salto a salto a lo largo de la red, denominado comportamiento por salto (PHB).

Se define el comportamiento por salto como "el comportamiento externamente observable del reenvío aplicado en un nodo DiffServ dócil a un comportamiento agregado (BA: behaviour aggregate)"[31]; es decir que los paquetes pertenecientes a cierto agregado serán tratados de la misma forma en cada nodo de la red de acuerdo a un nivel de servicio (SLA) o política. Un PHB determina el comportamiento específico de envío utilizado por cada dispositivo al manejar el tráfico para asignar recursos como buffer y ancho de banda y

características observables como límites para el retardo, jitter y pérdida de paquetes a los comportamientos agregados.

Los PHB's son implementados en cada nodo por medio de algunos mecanismos de administración de buffer y planeación de paquetes (packet scheduling) y se definen de acuerdo a las características de comportamiento relevantes a las políticas de provisionamiento del servicio y no en términos de mecanismos particulares de implementación, siendo posible implementar en un nodo y utilizar dentro de un dominio algunos grupos PHB.

Un comportamiento agregado (BA) consiste en la agrupación de paquetes con el mismo código DSCP y envío en una sola dirección particular, de modo que paquetes de múltiples orígenes o aplicaciones pueden pertenecer al mismo BA y el comportamiento por dominio (PDB) es el trato esperado que un agregado de tráfico va a recibir entre los bordes de una red DiffServ.

Un grupo PHB es un conjunto de uno o más PHB's que pueden estar especificados e implementados simultáneamente, debido a un limitante común que se aplica a todos los PHB's y proporciona un bloque de construcción que permita que un conjunto de comportamientos de reenvío relacionados se especifiquen juntos (por ejemplo, cuatro prioridades de descarte). Un solo PHB es un caso especial de un grupo de PHB.

Para determinar el grupo PHB al que pertenece un paquete IP, se codifica un valor DSCP en el campo DS de su cabecera, que determina el tratamiento que

recibirá el paquete en cada nodo y además permite tener paquetes con distinta prioridad dentro de un mismo PHB. Cuando un paquete entra en un router, la lógica de ruteo selecciona su puerto de salida y el valor DSCP es usado para conducir el paquete a una cola o tratamiento específico en ése puerto.

Los PHB's estándares se asocian a un codepoint recomendado, seleccionado del espacio de codepoint reservados del grupo estándar. Todos los codepoints se deben asociar a algún PHB y en ausencia de alguna política local, los codepoints que no se asocian a un PHB estándar deberían asociarse a un PHB predeterminado.

El ejemplo más simple de un PHB es uno que garantiza la asignación mínima de ancho de banda del X% de un enlace (sobre cierto intervalo de tiempo razonable) a un comportamiento agregado; este PHB se puede medir fácilmente bajo una variedad de condiciones del tráfico, mientras que un PHB levemente más complejo garantizaría la asignación mínima del ancho de banda del X% de un enlace, con compartición proporcional de cualquier exceso de la capacidad del enlace. El comportamiento observable de un PHB puede depender generalmente de ciertos limitantes en las características del tráfico de un comportamiento agregado asociado o de otros comportamientos agregados.

La especificación del comportamiento por salto debe incluir la descripción de la configuración y la administración que pueden afectar su operación, además se debe estandarizar las características del comportamiento de un PHB y no los algoritmos particulares o los mecanismos usados para implementarlos.

3.4.3.2.2. Tipos

- **Expedited forwarding – PHB EF**

PHB de reenvío priorizado[33] o servicio Premium, debido a que proporciona un comportamiento equivalente a una línea dedicada virtual, conexión punto a punto o a un circuito ATM CBR o VBR – rt (emula un circuito); siendo entonces el de mayor calidad, al ofrecer un SLA que garantiza un ancho de banda mínimo, bajo retardo, jitter y pérdida de paquetes, así como demora reducida en la cola. Es equivalente al servicio garantizado de IntServ.

Se compone de un solo codepoint que corresponde al valor binario '101110' y '46' en decimal y es el nivel de prioridad más alto, puesto que los paquetes IP marcados en su cabecera DS con el código EF tendrán prioridad absoluta de servicio frente a los demás, independientemente de la intensidad de otros tráficos que atraviesen el nodo, para lo cual se debe configurar los nodos de manera que el agregado tenga una tasa mínima de salida y acondicionar el agregado tal que su tasa de llegada en cualquier nodo sea siempre menor que la tasa de salida mínima configurada para ese nodo y para realizar esto se basa en planificadores por prioridades que permiten que sus agregados tengan casi siempre o siempre la cola vacía; pero sin ofrecer garantías cuantitativas para el retardo, jitter y pérdidas. Los paquetes marcados con el codepoint PHB EF, pueden ser remarcados en el borde de un dominio DS solo si pasan a ser códigos que satisfagan el PHB EF.

Se sugiere utilizar dos herramientas de calidad de servicio para conseguir este PHB[33]:

a. Gestión de Colas (Queuing): usado para minimizar el tiempo que los paquetes EF pasan en una cola, debido a que si un paquete está esperando, entonces envía los paquetes de esta cola y reduce la longitud de la cola, que a su vez reduce la oportunidad de descarte debido a una cola llena. Se utiliza PQ (Priority Queuing), con tráfico EF en la cola más importante para dar preferencia a dicho tráfico.

b. Gestión de Políticas (Policing): se utiliza una limitación de la tasa en cada clase (o BA), de manera que si la carga de la entrada de paquetes EF excede una tasa máxima definida, los paquetes excedentes son descartados y así se tiene un nivel de servicio bueno, pero en referencia a la cantidad de ancho de banda contratada.

Un PHB EF debe ser específicamente dirigido a las aplicaciones más críticas, porque si se tiene congestión, no es posible tratar todo o más tráfico con prioridad alta; por lo que es utilizado para soportar aplicaciones como los flujos de tiempo real, la voz y el tráfico de telefonía IP que requieren retardo, jitter y pérdidas de paquetes bajos.

- **Assured forwarding – PHB AF (AFxy)**

PHB de reenvío asegurado que ofrece un trato preferencial, similar a CIR de Frame Relay, pero no garantiza recursos como ancho de banda, retardo, jitter o pérdida de paquetes por lo que se utiliza para servicios real time y non real time[34]. Se puede comparar con la categoría VBR-nrt de ATM y es equivalente al servicio de carga controlada de IntServ.

Un PHB AF contiene dos funciones realizadas por herramientas QoS, la primera es la gestión de colas (queuing) en la que cada router clasifica los paquetes en clases diferentes y entonces se los pone en una cola separada, además se especifica el método soportado por la habilidad de reservar un mínimo ancho de banda configurado para cada clase; la segunda función es la anulación de congestión, donde los routers descartan los paquetes cuando una cola está llena, esperando que pocos paquetes sean descartados.

El PHB AF asegura que las herramientas de queuing (gestión de colas) proveerán suficiente ancho de banda para cada clase, con la habilidad de descartar el tráfico menos importante si ocurre la congestión.

El PHB Assured Forwarding permite ofrecer distintos niveles de garantía de entrega y puede expresarse como AFxy, donde se definen cuatro clases de reenvío AFx: AF1, AF2, AF3 y AF4, que se indican en los tres primeros bits del campo DSCP y a cada una de éstas se le reservan recursos como espacio en buffers y ancho de banda, que debe estar garantizado a corto y largo plazo en

cada uno de los nodos DS, de forma que los retardos y/o pérdidas de una clase sean siempre inferiores a los de una clase de menor prioridad.

En cada clase AFx se definen tres categorías de descarte de paquetes con probabilidad alta, media y baja, que se especifican en los dos bits siguientes y son equivalentes al bit DE (Discard Eligibility) de Frame Relay y el último bit del campo es siempre ‘0’. En caso de congestión la preferencia de descarte determina la importancia relativa del paquete dentro de la clase, de acuerdo a la siguiente pauta:

$$dP(AFxy) >= dP(AFxz) >= dP(AFxv)$$

Fórmula 3.1: Preferencia de descarte

Donde: dP (AFxy) es la probabilidad de que los paquetes de la clase AFxy sean descartados, en otras palabras, ‘y’ denota el valor de descarte dentro de una clase AFx.

Existen por tanto doce codepoints asociados con este tipo de servicio, y sus nombres se deben a que el primer dígito después de AF hace referencia a la clasificación de queuing y el segundo dígito implica la precedencia de descarte. Estos valores se detallan en la tabla 3.3.

Tabla 3.3: Codepoints del PHB AF

Clase	Precedencia de Descarte		
	Baja '01'	**Media '10'**	**Alta '11'**
4 '100'	AF41 100010	AF42 100100	AF43 100110
3 '011'	AF31 011010	AF32 011100	AF33 011110
2 '010'	AF21 010010	AF22 010100	AF23 010110
1 '001'	AF11 001010	AF12 001100	AF13 001110

El ordenamiento de las clases es tal que los paquetes marcados con AF4 tienen la mayor prioridad de ser descartados y los marcados con AF1 la menor prioridad, mientras que la precedencia de descarte baja tiene una menor probabilidad y la alta una mayor probabilidad. En este caso el proveedor ofrece servicios que se basan en las diversas clases de AF y aplica el método de policing al tráfico de modo que si el usuario excede lo pactado dicho proveedor puede descartar paquetes o aumentar la precedencia de descarte. Este ordenamiento de clases también facilita la compatibilidad con routers que soportan solamente el campo de Precedencia IP e ignorarán los tres bits menos significativos de los codepoints AF.

Los paquetes que lleven el byte DS marcado con alguno de los niveles del AF tendrán prioridad de servicio más baja que los del servicio Premium, pero su prioridad será más alta (en servicio o descarte) que la de los paquetes del servicio del mejor esfuerzo; incluso bajo ciertas condiciones, este PHB podría garantizar cierto ancho de banda medio (no retardo por paquete) para los flujos y la clase AF puede ser configurada para recibir más recursos que los mínimos previstos cuando hay exceso de recursos en otras clases AF o de otros grupos.

- **Class selector – PHB CS**

Este PHB se detalla en el RFC 2474, Definición del campo servicios diferenciados (campo DS) en las cabeceras IPv4 e IPv6[32], fue creado para facilitar la compatibilidad con los routers tradicionales que soportan únicamente el esquema de Precedencia IP, que define clases de servicio a través de los tres bits del subcampo precedencia del campo ToS de la cabecera IP y se basa en la clasificación y el envío. La figura 3.11 muestra los bits del campo ToS que se utilizan para Precedencia IP y DSCP.

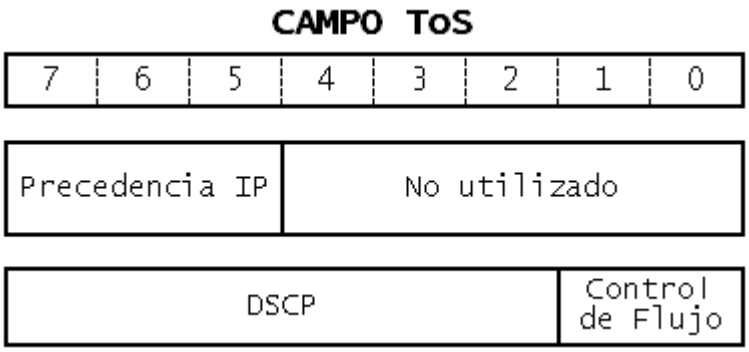


Figura 3.11: Relación entre Precedencia IP y DSCP

Especifica ocho niveles de prioridad de acuerdo a los valores de los codepoints que se asignan en el subcampo DSCP, donde cada uno de ellos tiene una mayor probabilidad de envío a tiempo que su predecesor. Este PHB mantiene casi el mismo comportamiento de envío que los nodos que implementan la Precedencia IP y al igual que éste, mientras más grande el número binario del codepoint, mejor es el PHB, e incluso el ordenamiento de sus codepoints es idéntico a la Precedencia IP, como se observa en la Tabla 3.4.

Tabla 3.4: Codepoints del PHB CS

DSCP CS		Precedencia IP
Nombre	**Valores**	
CS7	111000	111
CS6	110000	110
CS5	101000	101
CS4	100000	100
CS3	011000	011
CS2	010000	010
CS1	001000	001
CS0	000000	000

Como se puede apreciar estos valores DSCP, también conocidos como Codepoints Class Selector, se definen de la forma 'xxx000', donde x es 0 ó 1 y van desde CS7 con el valor '111000' que corresponde a la prioridad más alta y obtiene un tratamiento de envío preferencial; hasta CS1 con el valor '001000' para la prioridad más baja y CS0 con el valor '000000' que es el valor DSCP compatible con los requisitos del PHB predeterminado, que se describe más adelante.

Los PHB's CS aseguran que los nodos DS dóciles puedan coexistir con los nodos basados en Precedencia IP puesto que si se coloca un valor binario apropiado en el campo DSCP se puede reaccionar al DSCP entero o simplemente a los primeros tres bits, según sea el caso. Además, los PHB's seleccionados por los codepoints '11x000' deben dar a los paquetes un tratamiento de reenvío preferencial por la comparación del PHB seleccionado por el codepoint '000000' para preservar el uso común de los valores de Precedencia IP '110' y '111' que se reservan para paquetes de control de la red y el tráfico de enrutamiento. Los PHB's seleccionados por distintos codepoints class selector se deben reenviar independientemente; es decir, los paquetes marcados con diferentes codepoints

class selector pueden ser reordenados, mientras que un nodo de red puede hacer cumplir límites en la cantidad de recursos del nodo que se puede utilizar por cada uno de estos PHB's.

Un nodo de red DS dócil se puede desplegar con un conjunto de uno o más grupos PHB class selector, los cuales se implementan mediante una variedad de mecanismos como WFQ, WRR, entre los principales.

- **Default forwarding (Best effort) – PHB Predeterminado**

El PHB predeterminado se detalla en el RFC 2474, Definición del campo servicios diferenciados (campo DS) en las cabeceras IPv4 e IPv6[32]; se caracteriza por ser un servicio básico, donde el comportamiento de reenvío es exactamente igual al servicio por defecto que utiliza el Internet, es decir del mejor esfuerzo sin garantías y se utiliza para el tráfico que no requiere niveles de calidad superiores, como Expedited o Assured Forwarding, es decir cuando no hay otros acuerdos, se asume que los paquetes pertenecen a este agregado.

El valor recomendado para el DSCP del PHB predeterminado es compatible con el RFC 791, que se utiliza actualmente y corresponde al patrón de bits '000000', lo que implica que si un paquete tiene marcado este valor recibirá el servicio tradicional del mejor esfuerzo en un nodo DS dócil y también si el valor de DSCP del paquete que llega al nodo DS dócil, no se asocia con otro PHB estandarizado o local, dicho paquete se asociará con el PHB predeterminado.

Se debe tomar en cuenta que un paquete marcado inicialmente para recibir el tratamiento del comportamiento predeterminado puede ser remarcado con otro codepoint mientras pasa un límite en un dominio DS, de modo que debido a un acuerdo entre dominios DiffServ, sea reenviado usando un PHB diferente dentro de ese dominio.

Es necesario que en todos los nodos DS dóciles esté disponible un PHB predeterminado, de modo que los paquetes se puedan enviar utilizando este comportamiento y sin adherirse a cualquier regla particular, así estos paquetes serán entregados como sea posible y cuánto antes de acuerdo a los condicionantes establecidos en la política de recursos.

La implementación de este PHB se la realiza a través de la gestión de colas (queuing) que envía los paquetes de este agregado siempre que no se requiera el enlace de salida para satisfacer otro PHB, además debe asegurar que este agregado de comportamiento predeterminado sea atendido, lo que se consigue mediante un mecanismo en cada nodo que reserva recursos mínimos, como espacio en buffer y ancho de banda y de esta forma se permite además que los remitentes que no conocen del servicio diferenciado puedan seguir utilizando la red como habitualmente lo hacen.

La tabla 3.5 presenta las características relevantes de los diferentes tipos de PHB's utilizados en DiffServ y hace una analogía con respecto a las clases de servicio establecidas en ATM.

Tabla 3.5: PHB's de DiffServ

Tipo	Componentes Claves	Nombre de los DSCP's	Equivalencia en ATM
Default Forwarding	Best effort sin prioridad. No existen garantías. No se consigue un tratamiento de QoS específico. Codepoint: 000000.	DSCP BE predeterminado	UBR
Class Selector CS	Best effort con prioridad. No tiene garantías pero proporciona un trato preferente frente a best effort sin prioridad. Usa ocho DSCP's, con la forma: 'xxx000'. Usado para la compatibilidad con la Precedencia IP. Usa la lógica "más grande es mejor": cuánto más grande es el DSCP, mejor es el tratamiento de QoS	CS0, CS1, CS2, CS3, CS4, CS5, CS6, CS7	ABR
Assured Forwarding AF	Asegura un trato preferente, pero sin fijar garantías (no hay SLA). Se definen cuatro clases y en cada una tres niveles de descarte de paquetes. DSCP's no siempre siguen la lógica "más grande es mejor". El PHB tiene dos componentes: • Gestión de colas para proporcionar un ancho de banda mínimo a cuatro diferentes colas. • Tres umbrales de descarte en cada cola.	AF11, AF12, AF13, AF21, AF22, AF23, AF31, AF32, AF33, AF41, AF42, AF43	VBR - nrt
Expedited Forwarding o Premium EF	Ofrece más garantías. Equivale a una línea dedicada. Garantiza ancho de banda, retardo, jitter y tasa de pérdidas. Codepoint: 101110. El PHB también tiene dos componentes: • Gestión de colas para proporcionar bajo retardo, jitter, pérdida de paquetes y ancho de banda garantizado. • Policing para prevenir a EF de evitar que otros tipos de tráfico consigan bastante ancho de banda.	EF	CBR VBR - rt

3.4.3.3. Región de Servicios Diferenciados

También conocida como Región DS está compuesta por uno o más dominios DS contiguos, los cuales pueden soportar internamente distintos grupos de PHB's y diferentes asociaciones de los codepoints. Para permitir servicios a través de sus dominios se puede:

- Establecer en cada dominio DS contiguo un SLA que define un TCA (Acuerdo de condicionamiento de tráfico) para especificar cómo el tránsito del tráfico es condicionado en la frontera de dos dominios DS.

- Adoptar en varios dominios DS una política común de provisionamiento del servicio y así soportar un conjunto común de grupos PHB y de asociaciones de los codepoints para eliminar la necesidad de condicionamiento del tráfico entre esos dominios DS.

El Acuerdo de nivel de servicio (SLA: Service Level Agreement) se define en la frontera del dominio DiffServ y es un contrato de servicio entre un cliente y un proveedor de servicio que especifica el servicio de envío que un cliente debe recibir a largo plazo, siendo el cliente un usuario, organización u otro dominio DS. Este SLA puede incluir reglas de condicionamiento del tráfico que se constituyen como un TCA.

El Acuerdo de condicionamiento del tráfico (Traffic Conditioning Agreement) especifica las reglas de clasificación y perfiles de tráfico

correspondientes, mediciones, marcado, descarte y/o reglas de conformación que son aplicables a los flujos de tráfico seleccionados por el clasificador. Este TCA abarca todas las reglas de condicionamiento de tráfico definidas explícitamente en el SLA junto con las reglas implícitas de los requisitos relevantes del servicio y/o de la política de provisionamiento del servicio de un dominio DS.

3.4.3.4. Dominio DS

Consiste en una o más redes, conocidas como nodos, que poseen un conjunto de políticas de calidad de servicio o reglas de configuración comunes, utiliza los valores de DSCP y los diferentes grupos de PHB's implementados en cada nodo bajo la misma administración; la cual es responsable de asegurar que los recursos sean provisionados y/o reservados adecuadamente para soportar el SLA ofrecido por dicho dominio.

La complejidad se transfiere al borde del dominio, donde se clasifica, se condiciona el tráfico entrante y se asigna a diferentes comportamientos agregados (BA's: behaviour aggregates) para asegurarse que los paquetes que transitan el dominio estén apropiadamente marcados en el campo DS y se mantiene una funcionalidad simple en el núcleo del dominio que trabaja con agregados de tráfico para reenviar los paquetes de acuerdo a determinado PHB asociado al código DS, con lo que se obtiene un mejor desempeño en todo el dominio.

El comportamiento agregado, también llamado agregado de tráfico, es una colección de paquetes con el mismo código DS, atravesando un enlace en una

dirección particular y permite identificar el tratamiento de envío que cada agregado va a recibir, en este caso los agregados del interior podrían estar conformados por paquetes de varios clientes y ser tratados de forma diferente en el borde, pero con la misma expectativa de envío una vez en el interior.

3.4.3.4.1. Nodo DS

Contiene un conjunto de políticas y grupos de comportamiento por salto que determinan el tratamiento que los paquetes recibirán en la red para lo cual asocian el valor del código DS a uno de los PHB's soportados y de acuerdo a esto seleccionan el comportamiento de envío, se conocen como nodos DS dóciles debido a que obedecen a todos los requisitos del núcleo DiffServ, además no agregan overhead a IPv4 y están condicionados por el TCA.

3.4.3.4.2. Tipos de nodos

De acuerdo a la funcionalidad requerida para una red particular dentro del dominio de Servicios Diferenciados se tienen tres tipos de nodos, como se aprecia en la figura 3.12[20].

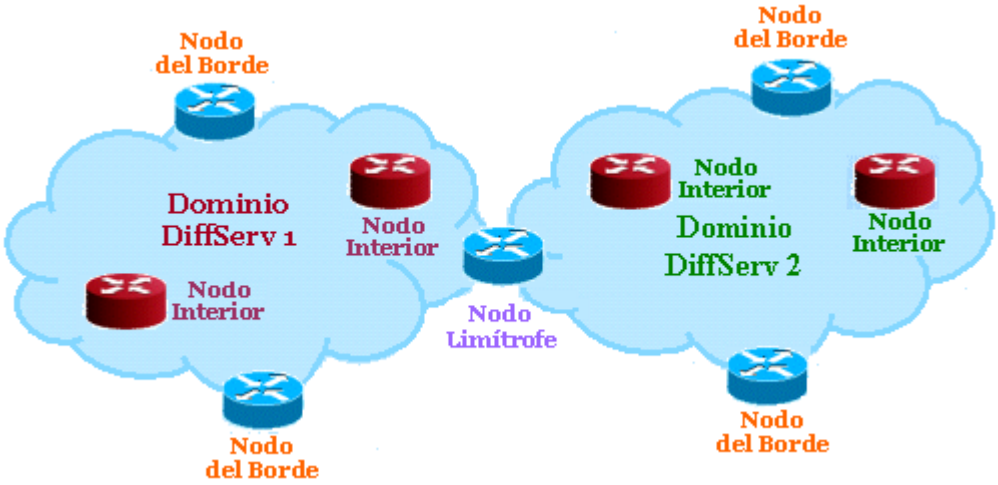


Figura 3.12: Tipos de nodos DiffServ

La Tabla 3.6 describe las principales características y las funciones que deben realizar los diferentes tipos de nodos DS.

Tabla 3.6: Nodos DS

Nodo	Ubicación	Funciones
De Borde o Periférico (Edge Node)	Primer nodo IP dócil en la red.	Aplica políticas de QoS en el borde del dominio DS. Actúa como punto de demarcación. Conecta un dominio DS con una red no DiffServ. Interconecta fuentes no confiables. Da servicio a los clientes finales.
De Frontera o Limítrofe (Boundary Node)	Primer dispositivo IP dócil.	Interconecta dos o más dominios DS. Proporciona políticas de QoS mediante la aplicación del PHB apropiado a los paquetes basándose en el código DS. Clasifica y establece las condiciones de ingreso de los flujos de tráfico en función de: dirección IP y puertos origen y destino, protocolo de transporte, etiqueta de flujo (IPv6), campo DS, interfaz de entrada, etc. Condiciona el tráfico de acuerdo a la política definida entre los dominios contiguos.

	Según la dirección del tráfico:	**Nodo de Ingreso** (Ingress Node) En los puntos de entrada al dominio DS.	Clasifica los paquetes basándose en el campo DS o en múltiples campos de su cabecera. Asegura que el tráfico entrante al dominio DS cumple con los requisitos de las políticas entre los dominios al cuál este nodo se conecta. En estos nodos se agregan los distintos flujos de los dominios de los clientes, usuarios finales y sistemas autónomos.
		Nodo de Salida (Egress Node) En los puntos de salida del dominio DS.	Controla el tráfico. Clasifica los paquetes basándose solo en el campo DS de su cabecera. Conforma el tráfico de salida de un ISP, según un servicio establecido con otro proveedor Puede realizar el condicionamiento y reenvío de tráfico a un dominio contiguo directamente conectado, dependiendo de los detalles de la política definida entre los dos dominios. Los flujos agregados salen del dominio DS de un proveedor y entran en el dominio de un cliente o de otro proveedor.
Interno o Interior (Core Node)	Dentro del dominio DS.		Permite la interconexión de fuentes confiables, como otros nodos DS interiores o nodos limítrofes dentro del mismo dominio DS. Selecciona el PHB definido para cada flujo de datos basándose solo en el campo DS. Agrupa los flujos, clasifica y reenvía los paquetes. Puede realizar funciones simples de condicionamiento del tráfico y remarcado del codepoint DS.

3.4.3.4.3. Módulos de un Nodo DS

Un nodo DS normalmente constituye un router y el SLA acordado puede especificar la clasificación del tráfico y las reglas de remarcado, así como perfiles

de tráfico y acciones a los flujos de tráfico que están dentro o fuera de perfil (in-out profile). Los nodos limítrofes traducen el TCA de cada cliente en un perfil de tráfico, que es un componente opcional que especifica las propiedades temporales de un flujo de tráfico seleccionado por el clasificador y provee las reglas para determinar si un paquete está dentro o fuera de perfil y así aplicar determinadas acciones de condicionamiento para implementar una política de QoS, por ejemplo los paquetes dentro de perfil pueden ser enviados sin ningún otro procesamiento, marcado o remarcado mientras que los paquetes fuera de perfil pueden ser encolados hasta que estén dentro del perfil (conformados), desechados (política) o remarcados con un código nuevo (re-marcado); para que posteriormente los paquetes reciban un trato uniforme dentro de las nubes.

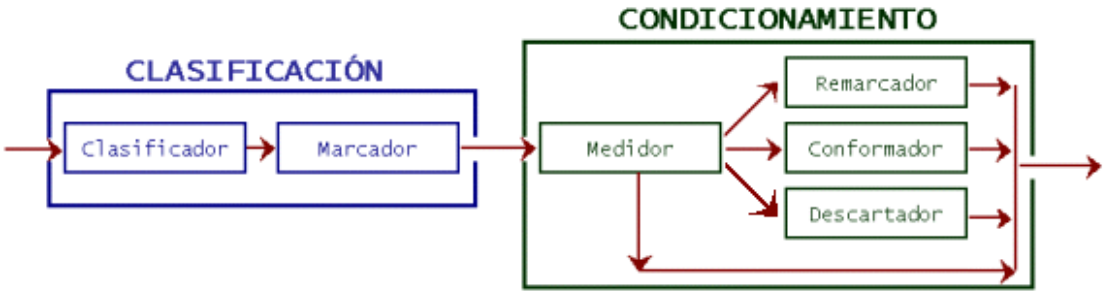


Figura 3.13: Bloques constructivos básicos

En la figura 3.13 se muestra el diagrama de los elementos constructivos que definen los módulos funcionales para DiffServ en un router y como se puede apreciar tenemos dos bloques que se describen a continuación:

a. **Clasificación de paquetes:** identifica el subconjunto de tráfico que puede llegar a recibir un servicio diferenciado, al ser condicionado y/o asociado a uno o más BA, después que un paquete ha sido clasificado, accede al QoS

en la red. Al usar la clasificación de paquetes, se puede dividir el tráfico de la red en múltiples niveles de prioridad o clases de servicio, sus elementos son:

- **Clasificadores (Classifiers):** dividen el tráfico entrante en múltiples grupos de acuerdo con unas reglas predefinidas, además deben autentificar la información que usan para clasificar el paquete, solo se realizan en el host o el router de entrada a clases agregadas puesto que los routers internos no clasifican por flujos. La clase del paquete se marca en la cabecera. Existen dos tipos:

    - **Clasificador BA (Behavior aggregate) o Comportamiento Agregado:** selecciona paquetes basado solo en el campo DSCP, que es incluido dentro de la tabla de comportamiento PHB. La política determina como el PHB es configurado para cada DSCP.

    - **Clasificador MF (Multi – field) o Multi - Campo:** se basa en el valor de la combinación de uno o más campos de la cabecera IP como: dirección IP origen o destino, puerto TCP o UDP origen, puerto TCP o UDP destino, número del protocolo (FTP, ICMP, Telnet, SNMP, etc.); esta quíntupla se conoce como microflujo.

- **Marcadores (Packet Markers):** asignan un codepoint particular en el campo DS de un paquete por el origen o el primer salto y pueden cambiar de asociación desde DSCP a ToS IP. En los nodos del

borde se marca el DSCP inicial basado en las políticas QoS del dominio y en los nodos limítrofes se remarca el DSCP basado en las políticas DiffServ entre dominios.

b. **Condicionamiento del tráfico:** se realiza en los bordes de un dominio DiffServ a través de la medición, conformación, política y/o remarcado para asegurarse que el tráfico entrante al dominio respeta las reglas especificadas en el TCA y obedece al servicio que provisiona la política del dominio. El condicionador del tráfico (traffic conditioner) es una entidad que realiza las funciones de condicionamiento del tráfico para aplicar el PHB seleccionado; cuando los paquetes salen del condicionador de tráfico de un nodo DS frontera, el código DS de cada paquete debe tener un valor apropiado. Los condicionadores de tráfico están usualmente localizados dentro de los nodos de frontera de ingreso y salida. En la tabla 3.6 se observa la síntesis de los principales condicionadores de tráfico utilizados:

Tabla 3.7: Condicionadores de tráfico

Condicionador de Tráfico	Características
Medidor (Traffic Meter)	Mide la tasa del tráfico para determinar si el tráfico está conforme o excede la política establecida, es decir determina si el paquete está dentro o fuera de perfil. Pasa la información de estado a otras funciones de condicionamiento para tomar cierta acción para cada paquete tanto dentro como fuera de perfil. Típicamente ocurre por clase.
Marcador (Packet Marker)	Asocia el campo DS con un código particular o un código de un grupo de códigos para seleccionar un PHB de un grupo, agregando el paquete marcado a un comportamiento agregado (BA) particular. Si el tráfico excede el contrato (paquetes no conformes) o en cambios de dominio se remarca el DSCP (se cambia el código de un paquete) con un valor diferente para promoverlo o degradarlo de PHB.
Conformador (Shaper)	Si el tráfico excede el contrato, se puede conformar el tráfico, que implica almacenar o encolar el tráfico, retardándolo, de modo que el flujo cumpla con el perfil de tráfico acordado y para asegurar que no se tenga tráfico en exceso en la red. Tiene un buffer de tamaño finito y los paquetes pueden ser descartados si no hay suficiente espacio de buffer para esperar a los paquetes retrasados. Es apropiado para aplicaciones basadas en UDP. Se lleva a cabo dentro de determinado compromiso en las interfaces de salida.
Descartador (Dropper)	Si el tráfico excede el contrato, se puede descartar algunos paquetes, para que el flujo cumpla con el perfil de tráfico acordado. Se puede implementar como un caso especial de un conformador, al colocar el tamaño del buffer del conformador igual a cero (o muy pocos) paquetes. Permite anular la congestión, que supervisa las cargas de tráfico de la red para evitar la congestión en los cuellos de botella de la red. Uno de los mecanismos usados es WRED que utiliza el valor de DSCP para calcular la probabilidad de descarte de un paquete. Su implementación se denomina: Policing

Además se debe considerar los mecanismos de **Policing** que controla la cantidad de tráfico que ingresa al dominio DiffServ, es decir que limita el volumen de cualquier tipo de tráfico entrante, de acuerdo a esto un paquete puede

transmitirse, descartarse, o remarcarse con un valor de DSCP diferente, dependiendo de la política QoS configurada y **Scheduling** o Administración de la congestión que se logra a través de la planificación del tráfico (traffic scheduling) y la gestión de colas (traffic queuing) para colocar el tráfico en una cola apropiada, basado en el valor de DSCP y se aplica al tráfico saliente de un puerto.

En la arquitectura DiffServ, los paquetes son clasificados y entonces condicionados, a través del marcado, medición, conformación y/o descarte. La figura 3.14 presenta el diagrama equivalente a las funciones de clasificación y condicionamiento del tráfico[31].

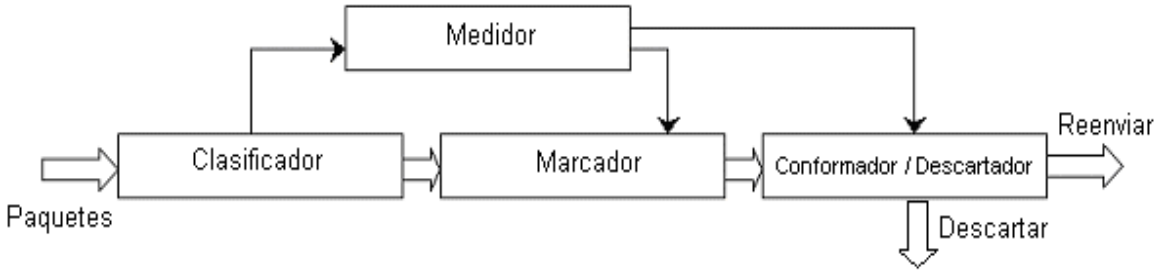


Figura 3.14: Vista lógica de un clasificador de paquetes y condicionador de tráfico

3.4.3.5. Modelo Arquitectónico DS

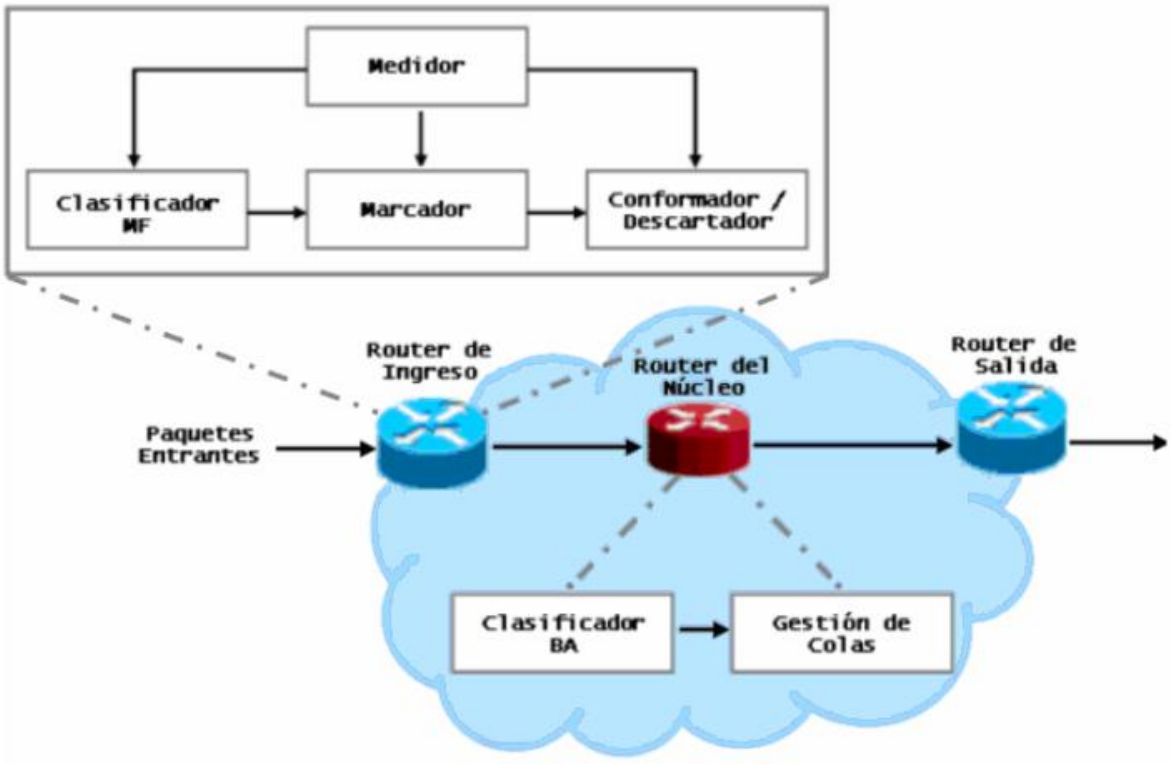


Figura 3.15: Arquitectura DiffServ

En la figura 3.15 se aprecia un diagrama global del modelo arquitectónico de Servicios Diferenciados[20] de acuerdo a los módulos de los Nodos DS, así en el router de ingreso se cuenta con clasificador multi – campo, marcador, medidor, conformador y descartador, es decir se clasifican, establecen las condiciones de ingreso de los flujos de tráfico y se marcan los paquetes adecuadamente, mientras que en los routers interiores se tiene el comportamiento agregado y la gestión de colas para seleccionar el PHB definido para cada flujo de datos. Las funciones de estos elementos se describieron en el apartado 3.4.3.4.3.

3.4.3.5.1. Componentes DS

a) Servidor de políticas QoS: Bandwidth Broker - BB

El servidor de políticas es un punto centralizado que determina los flujos de tráfico de acuerdo al perfil y la clase de tráfico y distribuye las políticas a los dispositivos del borde y limítrofes, para que dichos dispositivos puedan supervisar los flujos y marcar los paquetes con un valor que represente el comportamiento por salto a aplicarse en el nodo.

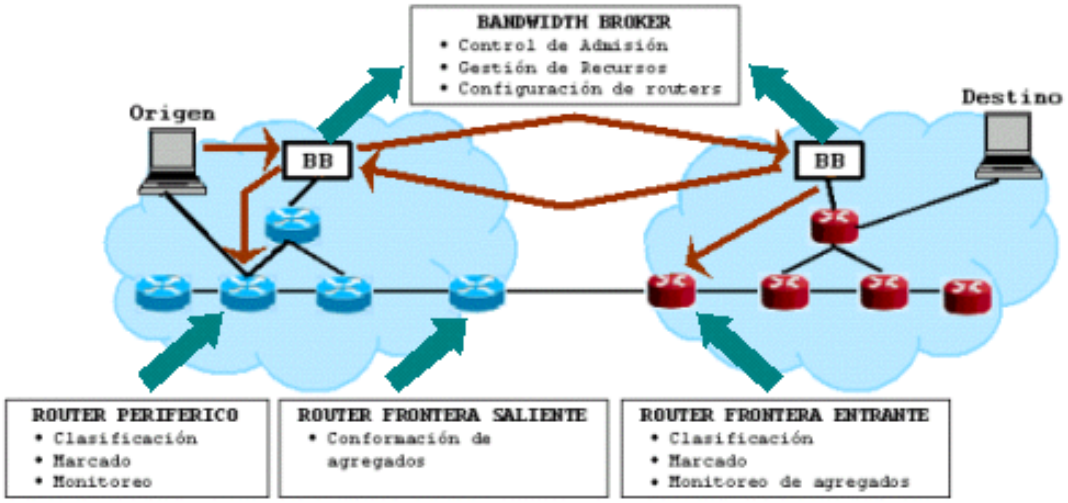


Figura 3.16: Bandwidth Broker en la red DiffServ

Como se observa en la figura 3.16, en cada dominio DiffServ se incorpora un servidor que permite administrar tanto los recursos utilizados como los usuarios y evita el uso indebido de la red, dicho servidor se conoce como: Bandwidth Broker (BB), que es un agente que tiene cierto conocimiento de las prioridades y de las políticas de una organización y asigna ancho de banda con respecto a esas políticas[35], es decir es un agente servidor que centraliza la

gestión de políticas y mantiene la información necesaria para ejecutar los controles administrativos y las respectivas políticas mediante la asignación del código DiffServ a cada flujo de datos. Las principales funciones de un Bandwidth broker son:

- Tomar las decisiones de control de admisión para controlar el acceso de los usuarios a los servicios del dominio DiffServ y hacer cumplir el SLA contratado. Dependiendo de los requerimientos del tráfico de un usuario, como ancho de banda, prioridad, retardo, etc, 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.

- Gestionar los recursos de red disponibles en un dominio DiffServ: mediante los informes de uso del ancho de banda que le envían periódicamente los routers y conociendo los recursos de la red y los usuarios registrados realiza la asignación, control y monitoreo de recursos.

- Configura los dispositivos periféricos y de frontera (routers de acceso).

- Asigna tráfico al router.

Puede intercambiar información con los bandwidth broker de otros dominios, e incluso los ISP's pueden acordar políticas de intercambio mutuo para así lograr una asignación de recursos extremo a extremo. El protocolo de comunicación empleado para distribuir las políticas de calidad de servicio entre los

elementos de la red es COPS (Common Open Policy Service), que define un modelo cliente / servidor que se basa en un servidor, conocido como PDP (Policy Decision Point), que devuelve decisiones a las peticiones realizadas por los clientes, llamados PEP (Policy Enforcement Point), que informan al servidor si se logró instalar localmente con éxito la decisión recibida y borran cualquier estado que no sea válido debido a eventos en el propio cliente o a decisiones enviadas por el servidor. Es un protocolo apropiado para el intercambio de información entre un servidor de políticas y diversos clientes que mantienen perfiles de usuario o aplican métodos de QoS bajo la disposición de dicho servidor y utiliza TCP como protocolo de transporte (puerto 3288) para asegurar así fiabilidad en el intercambio de mensajes entre los clientes y el servidor. Los clientes PEP pueden ser:

- **Router de acceso (RA):** cliente de políticas (PEP) que gestiona, planifica y monitorea las colas QoS configuradas por el BB, además captura información de los tráficos que lo atraviesan para luego preguntar por ellos al BB y clasifica los tráficos salientes hacia las colas según el DSCP del tráfico y bajo orden del BB.

- **AAAC QoS (Autenticación, Autorización, Contabilidad y Facturación):** es otro tipo de cliente de políticas (PEP) que obtiene el perfil contratado de un usuario de la base de datos de usuarios autorizados, lo instala en el BB y obtiene los DSCP's de sus servicios de red asociados, además actualiza o borra dichos perfiles según sus permisos.

b) Dispositivos de frontera

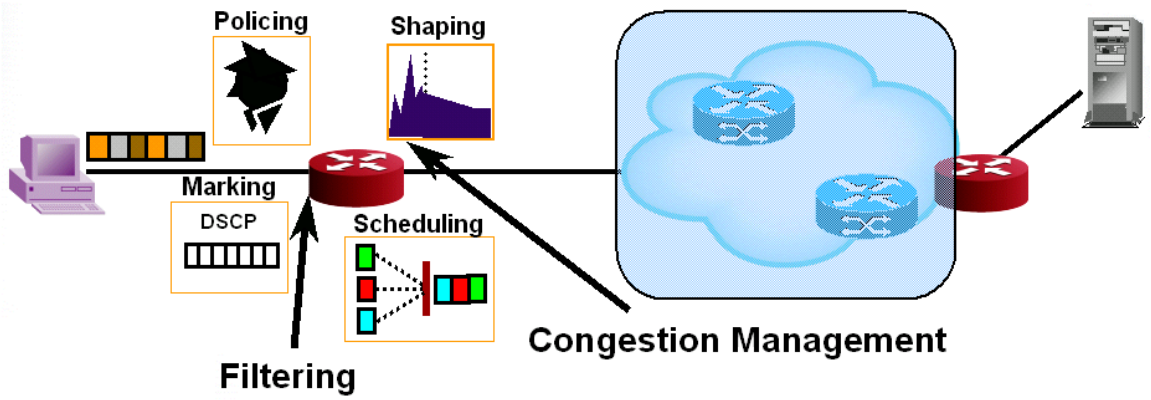


Figura 3.17: Tratamiento de paquetes en un nodo de borde y limítrofe

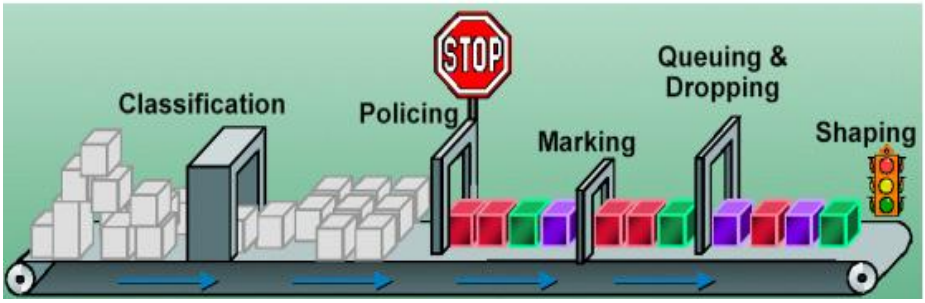


Figura 3.18: Implementación de DiffServ en los nodos de ingreso

En los nodos del borde se realiza el trabajo fuerte de clasificación (filtrado) y condicionamiento del tráfico porque hay menos flujos que en las regiones interiores de una red DiffServ, en la figura 3.17[20] se ilustran las funciones realizadas por un nodo DiffServ del borde y en la figura 3.18[36], las del nodo limítrofe de ingreso y se describen a continuación:

- **Clasificación:** corresponde al filtrado, donde el clasificador multi – campo identifica y separa los paquetes en las diferentes clases.

- **Gestión de Políticas (Policing):** para asegurar que un flujo determinado cumple con las políticas de calidad de servicio de la red, es decir está conforme a los niveles definidos por el SLA.

- **Marcado (Marking):** marca el flujo con el DSCP apropiado de acuerdo a la política QoS de la red y señala los paquetes de baja prioridad que se pueden descartar en casos de alta congestión.

- **Scheduling – Queuing (Estrategias del servicio de colas):** asegura que se dé servicio a las colas de acuerdo a las prioridades, usa diferentes métodos de planificación como WFQ, WRR, etc.

- **Conformación (Shaping - Delaying):** mejora la eficiencia de los enlaces, controla el tráfico de ráfagas y conforma el tráfico.

c) Dispositivos internos

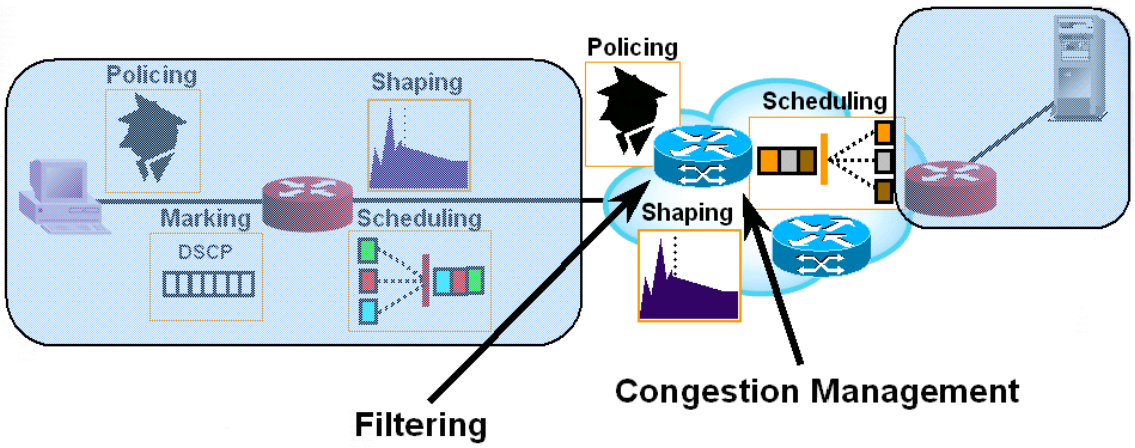


Figura 3.19: Tratamiento de paquetes en un nodo interior

Los nodos del núcleo DiffServ realizan una clasificación simple (filtrado) basada en el DSCP y condicionan el tráfico que pasa por el dominio; la complejidad es menor en estos nodos debido a que los flujos se clasificaron en el borde y existe un menor número de flujos en las regiones interiores de la red, además existiría un funcionamiento degradado si un nodo interior clasificara un alto volumen de tráfico. La figura 3.19[20] ilustra las funciones realizadas por el nodo interior de DiffServ, que se detallan a continuación:

- **Clasificación:** el clasificador BA o comportamiento agregado se basa en el campo DSCP para identificar los paquetes.

- **Gestión de Políticas (Policing):** para asegurar que el flujo esté conforme a las políticas QoS de la red, es decir conforme al acuerdo definido.

- **Conformación (Shaping - delaying):** mejora la eficiencia.

- **Scheduling:** asegura que se dé servicio a las colas de acuerdo a las prioridades establecidas.

Tanto en los dispositivos limítrofes como interiores se incluye la administración de la congestión (congestion management), realizada a través de:

- **Prioridad de descarte (Drop preference):** incrementa la prioridad de descarte del paquete para que reciba una alta probabilidad de ser descartado por los dispositivos bajo congestión.

- **Anulación de la congestión (Congestion avoidance):** utiliza RED para descartar randomicamente los paquetes.

3.4.3.6. Requerimientos de la Arquitectura

La arquitectura de servicios diferenciados debe ser capaz de soportar el crecimiento continuo de la cantidad y variedad de aplicaciones, así como de la capacidad de la infraestructura de la red, por lo tanto debe cumplir con los siguientes requisitos[31]:

- Adaptar una amplia variedad de servicios y proveer políticas, extendiendo una red extremo a extremo o dentro una red particular.

- Trabajar con aplicaciones existentes sin la necesidad de cambios en interfaces de aplicaciones programables o modificaciones de software en el host (asumiendo el despliegue conveniente de clasificadores, marcadores y otras funciones de condicionamiento del tráfico).

- Desacoplar las funciones de condicionamiento de tráfico y provisionamiento de servicios de comportamientos de reenvío implementados en los nodos del núcleo de la red.

- No debe depender de la señalización de la aplicación salto a salto.

- Requerir solo una pequeña cantidad de comportamientos de reenvío, cuya complejidad de implementación no domine el costo de un dispositivo de red.

- Evitar estados por microflujo o por clientes dentro de los nodos del núcleo de la red.

- Utilizar solo el estado de clasificación de agregados dentro del núcleo de la red.

- Permitir implementaciones simples de clasificación de paquetes en los nodos del núcleo de la red (clasificador BA).

- Permitir interoperabilidad razonable con nodos de red no DS dóciles.

3.4.4. Funcionamiento

En esta arquitectura se tiene una nube DiffServ que es una colección de dispositivos que son capaces de responder a un servicio específico de acuerdo al código DSCP marcado en los paquetes, por lo que los paquetes se clasifican y marcan para recibir un trato particular en cuanto a su envío en cada salto.

La región DiffServ como se ha especificado anteriormente está compuesta por uno o más dominios DS que utilizan DSCP y los diferentes PHB's de acuerdo a la política establecida que tienen los nodos del borde, donde se clasifica el

tráfico, aplican políticas, conforma el tráfico y se marcan los paquetes por prioridad y del núcleo donde se soporta la clasificación DSCP y el tratamiento de la prioridad.

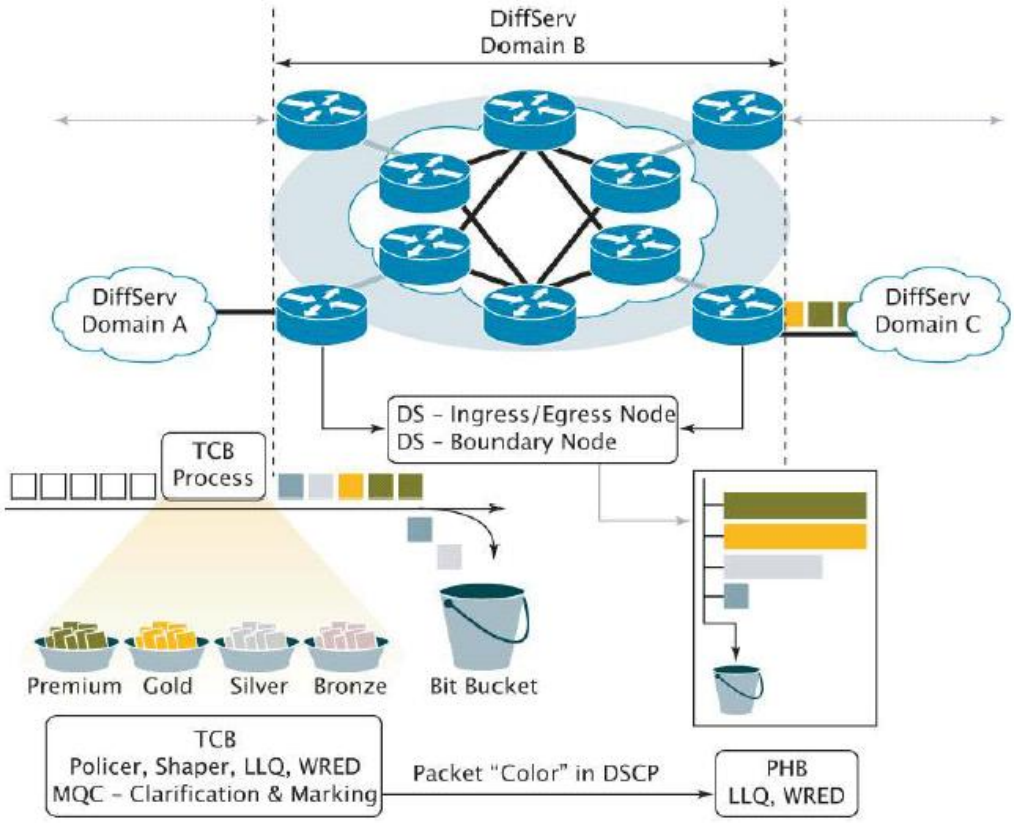


Figura 3.20: Funcionamiento de DiffServ

La figura 3.20 muestra la trayectoria completa de un paquete a través de una red DiffServ[37], en este caso las políticas de servicio definen el tráfico con las siguientes clases y su correspondiente asignación de ancho de banda así: premium 10 por ciento, oro 40 por ciento, plata 30 por ciento, bronce 10 por ciento y el tráfico del mejor esfuerzo (clase predeterminada) el restante 10 por ciento del ancho de banda; en este caso oro, plata y bronce se asocian a las clases AF1, AF2 y AF3 y premium a EF. Las funciones típicas desarrolladas en una red DiffServ son:

1. El tráfico entrante a una red DiffServ es clasificado en flujos por el origen, que fija el campo DSCP en la cabecera IP, según la clase de los datos, en la entrada a la red se aplica una política a los flujos clasificados. Al marcar los paquetes cerca del origen se toma en cuenta más fácilmente las preferencias de las aplicaciones para decidir qué paquetes deben recibir mejor tratamiento de envío y la clasificación de paquetes es más simple antes que el tráfico ha sido agregado con paquetes de otros orígenes.

2. Dentro de la nube DiffServ, los dispositivos dan una mayor prioridad a los paquetes con el valor más alto en el campo DSCP, además puede existir una política de descarte para las frecuencias con las cuales cada tipo de paquete se desecha si el dispositivo está fuera del espacio del buffer; de esta forma si tráfico excesivo ingresa a la red, los paquetes de los flujos de baja prioridad son descartados.

3. El tráfico conformado entonces se asigna a un agregado de comportamiento particular, para que cuándo pase a través de la red DiffServ, el DSCP accione un PHB en el interior de la red.

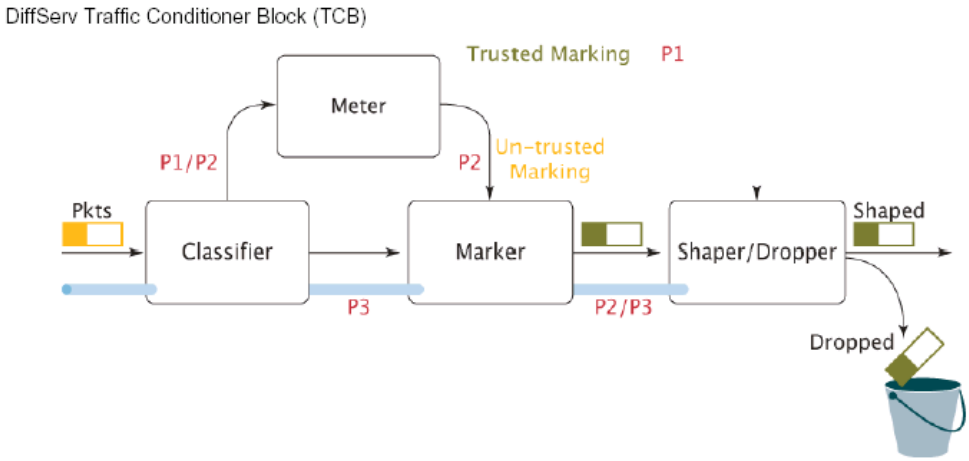


Figura 3.21: Funcionamiento del condicionador del tráfico

En la figura 3.21 se ilustra el esquema del condicionador del tráfico que se emplea en el nodo del borde de ingreso y salida[37] y está compuesto por los elementos descritos en el apartado 3.4.3.4.3. Algunos mecanismos de condicionamiento del tráfico son:

- **LLQ para el PHB EF:** utilizado en cada salto para el tráfico sensible al retardo, como VoIP, que necesita tener prioridad estricta en toda la trayectoria del paquete y para asegurar que el tráfico de voz excesivo no interfiera con el tráfico de otras clases.

- **WRED para el PHB AF:** se emplea MQC (Modular QoS Commandline Interface) para establecer el ancho de banda entre varias clases definidas. Se utiliza el esquema de precedencia de descarte WRED para descartar los paquetes de una clase AF.

- **Policer PHB AF:** se pueden aplicar políticas para implementar el PHB en el núcleo, para pasar a un agregado más alto.

Se debe considerar que una calidad extremo a extremo será alcanzable solo si todos los elementos involucrados en los dominios DiffServ actúan según las mismas políticas, puesto que el valor del campo DS podría ser modificado en cualquier equipo intermedio de acuerdo a las políticas de tráfico y los contratos SLA que existan entre los ISP's.

Existen elementos adicionales que interactúan en una red DiffServ y que le permiten un mejor funcionamiento, como es el servidor de recursos Bandwidth Broker, que evita un uso indebido de la red, administra los recursos utilizados y los usuarios y se detalla en el apartado 3.4.3.5.1. Además se emplean mecanismos para enfrentar las congestiones transitorias como el buffer de datos, que implica el armado de una cola de espera y el retardo correspondiente dependiendo de la prioridad asignada en dicha cola y para las congestiones de larga duración se emplea el descarte de paquetes a través de RED, que se basa en el descarte aleatorio de paquetes tras la detección temprana de la congestión, una vez superado un umbral del tamaño medio de la cola.

3.4.5. Aplicaciones

Se distinguen algunas aplicaciones o servicios que pueden utilizar esta arquitectura, además de las redes IP que requieren calidad de servicio extremo a extremo, entre las que tenemos:

- Servicios basados en suscripción, como video sobre demanda (pague por ver), canales de radio y de televisión; debido a que el origen es el

encargado de realizar la reserva y en este caso el proveedor de contenidos seleccionaría la calidad de servicio que recibirían los usuarios y obtendría cierto ingreso por cada evento distribuido.

- Creación de VPN's (Redes virtuales privadas) sobre una red IP, puesto que el origen y el destino pertenecen a la misma organización y de esta manera comparten los mismos criterios sobre QoS.

- Videoconferencias, donde se puede incluir cualquier tipo de escenario VoIP (Voz sobre IP) porque requieren el desarrollo e implementación de tecnologías de calidad de servicio sobre el actual Internet.

- Juegos en línea, porque son aplicaciones que a pesar de no requerir un gran ancho de banda, si dependen del retardo. La existencia de una gran plataforma de videojuegos está supeditada a la provisión de calidad de servicio.

3.5. IntServ versus DiffServ

3.5.1. Características

En la tabla 3.8 se especifican las características específicas de IntServ y DiffServ:

Tabla 3.8: Comparación entre IntServ y DiffServ

Característica	IntServ	DiffServ
Desarrollo	-	Se ha extendido más.
Esquema de funcionamiento	Se basa en el protocolo RSVP. Reserva recursos. Establece y mantiene el estado de las conexiones por flujo. Crea información de estado a lo largo de la ruta para cada flujo individual. Define servicios.	Usa el campo DSCP. Clasifica y marca los paquetes para tener un tratamiento diferenciado en los routers. Define y utiliza diferentes tipos de nodos. Define tratamientos de reenvío.
Tipo de servicio	Por flujo individual.	Por agregado de tráfico.
Procesamiento complejo (Funciones de clasificación y policing)	En los dispositivos del núcleo.	En los dispositivos de los bordes.
Garantía de QoS	Severas	-
Información de estado	Almacenada en los routers.	Almacenada en los paquetes.
Protocolo	Señalización.	Provisionamiento.
Control de QoS	Receptor.	Emisor.
Escalabilidad	-	Permite agregar flujos. Apropiado para grandes redes.
Implementación en los dispositivos y las redes	-	Mayor aceptación de los fabricantes de dispositivos e ISP's.

3.5.2. IntServ

3.5.2.1. Ventajas

Puede considerarse una solución adecuada para entornos más limitados y para redes de acceso, donde los enlaces son de baja capacidad y los routers soportan pocos flujos, también se puede utilizar RSVP en MPLS y funciones de ingeniería de tráfico, donde el número de flujos no suele ser muy grande.

3.5.2.2. Desventajas

El modelo IntServ no ha sido implementado en los equipos por los fabricantes ni se ha desarrollado en las redes de los proveedores de Internet, por las desventajas que presenta, entre las que tenemos:

- Cada dispositivo a lo largo de la trayectoria de un paquete, incluyendo elementos finales como: servidores y computadores debe conocer el protocolo RSVP y ser capaz de señalar el QoS requerido.

- La reserva de recursos para cada flujo y el mantenimiento de ésta en cada nodo conduce a un considerable tráfico de señalización que aporta a la congestión de la red y a la complejidad en el hardware debido a la ocupación de recursos en cada dispositivo para cada flujo.

- Existe mayor complejidad y elevados requerimientos en cada nodo de la red debido al control de admisión, al mantenimiento de la información del estado de la reserva y al estado soft – state que deben tener las reservaciones en cada dispositivo a lo largo de la trayectoria, de modo que la implementación en hardware supone un elevado costo para los fabricantes, puesto que éste crece cuando menos linealmente con la complejidad de la red.

- Los dispositivos a lo largo de la trayectoria de la red necesitan software apropiado tanto para el envío de paquetes como para las funciones de control.

- Baja escalabilidad debido a que la información de estado en el dispositivo es proporcional al número de flujos, es decir que la reserva de recursos y el mantenimiento del estado de cada flujo resulta poco eficiente si el número de flujos es muy elevado, por lo que no se considera una solución adecuada para grandes entornos, como el núcleo de Internet, donde se deben soportar miles de conexiones activas.

- No es flexible puesto que no permite definir clases de servicio cualitativamente distintas sino que se basa en requisitos cuantitativos.

- El fracaso de IntServ se debe principalmente a que adoptó la noción en la que QoS significa conexiones y el modelo orientado a la conexión no puede ser usado para conseguir calidad de servicio extremo a extremo viable.

3.5.3. DiffServ

3.5.3.1. Ventajas

- Reduce la carga en los dispositivos y la complejidad puesto que no se mantiene la información del estado de la reserva en cada elemento de la red y esto permite que fácilmente se escale con el crecimiento de la red.

- Es un mecanismo de tratamiento del tráfico que permite transportar varios miles de conversaciones, por lo tanto es apropiado para grandes redes enrutadas, donde no resulta práctico tratar el tráfico por conversación individual.

- Debido a la simplicidad de este modelo se lo puede asociar fácilmente con el modelo de servicios QoS que un ISP ofrece.

- Otorga una mayor flexibilidad al permitir que se definan más tipos de tráfico a diferencia de IntServ que solo tiene dos tipos.

- Es compatible con los métodos existentes de calidad de servicio para redes IP, como el esquema de priorización de capa 3, a través del campo ToS.

- La mayor parte de los fabricantes permiten que sus dispositivos de red soporten la arquitectura DiffServ y que se combinen dispositivos DiffServ con cualquier equipo que tenga habilitado ToS.

- Alivia los cuellos de botella a través de la administración eficiente de los recursos de red actuales.

- Logra escalabilidad con la implementación de las funciones de clasificación y condicionamiento sólo en los nodos del borde de la red y con la aplicación de comportamiento por salto a los agregados del tráfico que han sido apropiadamente marcados usando el campo DS de las cabeceras IP.

3.5.3.2. Desventajas

- Necesita ser provisionado, lo que implica consumo de tiempo en el proceso de descubrimiento de la aplicación y su definición, es decir para conocer las aplicaciones y estadísticas de tráfico para los respectivos agregados y así configurar las diferentes clases a lo largo de la red.

- La administración de este modelo todavía es un gran problema, puesto que la naturaleza cualitativa de las aplicaciones puede provocar una percepción diferente en el usuario, no siendo suficiente demostrarle que sus paquetes obtuvieron un tipo de tratamiento en todo momento.

- Es difícil predecir el comportamiento extremo a extremo debido a que los detalles de cómo los routers individuales se ocupan del campo ToS son arbitrarios, lo que se complicaría si el paquete cruza dos o más nubes DiffServ antes de alcanzar su destino.

- Es un mecanismo para decidir qué paquetes se retrasarán o descartarán a expensas de otros en una situación donde no hay suficiente capacidad de la red y el tráfico en el enlace está cercano a la saturación, por lo tanto es inferior a agregar suficiente capacidad a la red para evitar la pérdida de paquetes en todas las clases de tráfico.

- No se puede garantizar el éxito de un solo flujo debido a que se ofrece calidad de servicio agregada.

3.5.4. Conclusión

Por lo expuesto anteriormente se concluye que la arquitectura DiffServ tiene mejores características, ventajas y relativamente pocas desventajas en comparación con IntServ; puesto que reduce la carga en los dispositivos y la complejidad a diferencia de IntServ, donde existen elevados requerimientos en cada nodo de la red debido a la reserva de recursos, al mantenimiento de la información del estado de la reserva y al estado soft – state lo que conduce a un considerable tráfico de señalización que aporta a la congestión en la red, DiffServ proporciona una mejor administración de los recursos y un mayor número de tipos de tráfico, mientras que IntServ se basa en requisitos cuantitativos y su implementación en hardware es costosa, DiffServ es flexible y compatible con otros mecanismos de calidad de servicio, por lo que es el modelo QoS extremo a extremo a utilizar para el desarrollo del algoritmo propuesto en este proyecto.

CAPÍTULO 4

4. ELABORACIÓN DE LA PROPUESTA

4.1. ARQUITECTURA PARA OFRECER QoS EXTREMO A EXTREMO

4.1.1. Consideraciones

Una arquitectura práctica de calidad de servicio diferenciada para varias aplicaciones y usuarios y extremo a extremo en un red IP debe proveer un ambiente multi - servicios entre las premisas de las grandes empresas sobre el núcleo de la red del proveedor de servicios, para lo cual se requiere el interworking bien definido entre los ISP's (proveedores de servicios de Internet) y las redes de los clientes; esto ocurrirá en varios niveles incluyendo la señalización IP, la configuración VoIP y CAC (Control de admisión de la llamada) y la política de interworking.

La obtención de un solo marco de trabajo y su implementación a corto plazo requiere de los siguientes componentes esenciales: implementación de QoS en todas las partes de la red para alcanzar el funcionamiento extremo a extremo, coordinación cercana entre las redes WAN del proveedor de servicios y las premisas del cliente, implementación de entidades interworking tal como el servidor QoS del cliente y el servidor QoS de red, combinación de los mecanismos QoS del IETF con los aspectos QoS en la LAN y de QoS para VoIP, despliegue de la estrategia integrada de VoIP y una trayectoria de migración hacia

el establecimiento de una red basada en políticas a través de los diferentes mecanismos[38]:

- Tecnologías de red de área local (LAN), por ejemplo Ethernet switched full-duplex, IEEE 802.1D user_priorities, Subset bandwidth manager (SBM) y mecanismos basados en host incluyendo marcado del 802.1D y campos DiffServ, señalización RSVP inicial y señalización del control de la llamada.

- Mecanismos QoS de redes de área extendida (WAN) incluyendo la arquitectura de servicios diferenciados (DiffServ) y MPLS (Multi Protocol Label Switching).

- Interworking entre la LAN y los mecanismos QoS WAN, como la operación de servicios integrados (IntServ) sobre redes DiffServ.

- Infraestructura de servicios y políticas que definan y hagan cumplir los acuerdos de nivel de servicios (SLA's), implementaciones QoS diferenciadas y control de admisión de llamadas para voz sobre IP.

La figura 4.1 muestra una visión total de la red en una arquitectura diferenciada que incluye la disposición de QoS con los componentes esenciales de la arquitectura, así como los protocolos y los mecanismos usados en cada una de las partes.

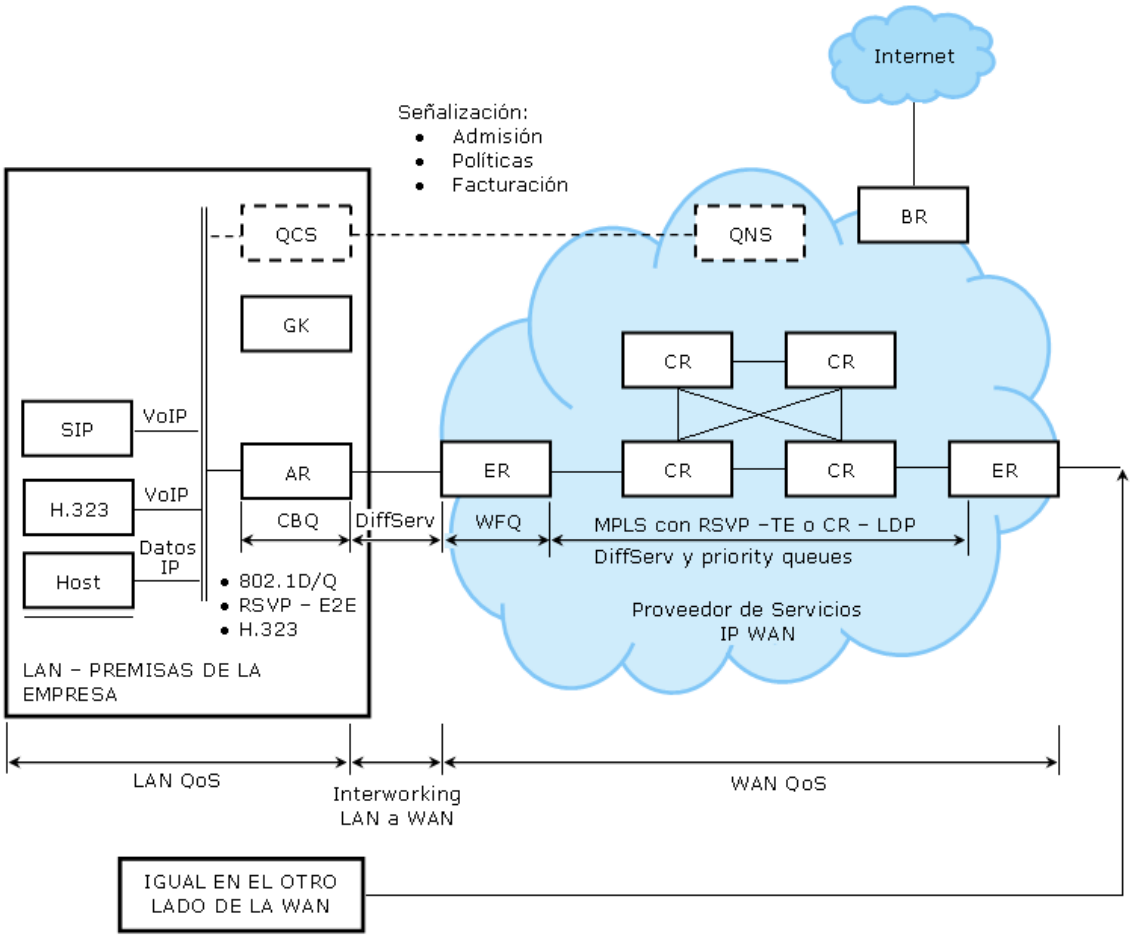


Figura 4.1: QoS extremo a extremo en las premisas de las empresas

Como se aprecia en la figura 4.1, la metodología para ofrecer calidad de servicio extremo a extremo en un ambiente IP debe considerar tres áreas: QoS en las premisas del cliente (LAN QoS), QoS en el núcleo de la red del ISP (QoS WAN) y su interrelación (interworking) para definir y cumplir con las necesidades del cliente, por ejemplo, el ambiente LAN implementará tecnologías probadas y las desarrollará de acuerdo con las recomendaciones del vendedor, los ISP's adaptarán las redes y los SLA's a los requerimientos de sus clientes e intentarán optimizar la utilización de sus recursos de red y el interworking LAN a WAN estará presente en las premisas de la empresa por medio del servidor de QoS del cliente (QCS: QoS customer server) para asegurar que el tráfico se conforme

correctamente para la entrega en la WAN y que la señalización provea suficiente información para la clasificación y la política de interworking. A continuación se describen los aspectos claves en la LAN, la WAN y el QoS LAN a WAN.

4.1.2. Parámetros en la red LAN

El ambiente LAN varía entre las premisas de la empresa y hay casos individuales que pueden requerir consideraciones especiales, sin embargo, al desarrollar una solución general para un ISP, se puede asumir que una gran cantidad de sus clientes será equipado con las tecnologías estándares del flujo principal o estará dispuesto a implementarlas; por lo que se analizan algunas tecnologías empresariales, su impacto en QoS y las interacciones entre varios mecanismos QoS LAN (como, Ethernet con user_priorities 802.1D, RSVP-E2E, SBM H.323 con RSVP para reservar recursos para llamadas VoIP específicas) que aseguren el tratamiento QoS diferenciado de varios flujos.

4.1.2.1. Tecnologías LAN

4.1.2.1.1. Ethernet basado en QoS

En Ethernet se permite que los pares de nodos reciban y envíen los datos simultáneamente, puede implementarse en las tasas de transmisión de 10 Mbps, 100 Mbps (Fast Ethernet), 1 Gbps (Gigabit Ethernet) y 10 Gbps y admite la adopción de los estándares IEEE 802.1Q y D que amplían el frame Ethernet por

cuatro octetos para incluir las etiquetas virtual LAN (VLAN) e información explícita del user_priority para los datos transportados sobre Ethernet.

El 802.1D user_priority (definido formalmente en IEEE 802.1p) usa tres bits en la etiqueta de la VLAN 802.1Q para definir ocho tipos de tráficos llevados en el frame Ethernet, para un número dado de colas en un puerto de un switch, 802.1D define los tipos de tráfico a usar y cómo asignarlos a las colas, como se indica en la tabla 4.1[38].

Tabla 4.1: Asociación IEEE 802.1D de los tipos de tráfico en las colas

Nº de Colas	**Tipos de Tráficos**							
1	BE							
2	BE				VO			
3	BE				CL		VO	
4	BK		BE		CL		VO	
5	BK		BE		CL	VI	VO	
6	BK		BE	EE	CL	VI	VO	
7	BK		BE	EE	CL	VI	VO	NC
8	BK	-	BE	EE	CL	VI	VO	NC

BE: Best effort (000); **BK:** Background (001); spare – (010); **EE:** Excellent effort (011); **CL:** Controlled load (100); **VI:** Video (101); **VO:** Voice (110); **NC:** Network control (111)

4.1.2.1.2. RSVP – E2E

Además del QoS diferenciado basado en los estándares LAN del IEEE descrito en el apartado 4.1.2.1.1, los nodos de la empresa pueden soportar la arquitectura IntServ y utilizar RSVP como protocolo de señalización para dos funciones separadas como se ilustra en la figura 4.1; RSVP extremo a extremo (RSVP E2E) usado para reservaciones por flujo que fue analizado en el Capítulo 3

apartado 3.3.4.3 y RSVP-TE usado para la señalización MPLS en la WAN, tratado en el apartado 4.1.3.2.2 literal 2.

4.1.2.1.3. RSVP asociado a Ethernet

El grupo de trabajo del IETF, Servicios Integrados sobre Capas de enlace específicas (ISSLL), ha desarrollado el protocolo de señalización Subset Bandwidth Manager (SBM) para asociar RSVP en las redes estilo IEEE 802 puesto que RSVP es un protocolo de configuración del nivel de Internet iniciado en el ambiente LAN y aunque todos los dispositivos capa 3 en la trayectoria del flujo de datos son RSVP-capaces, todavía no pueden proporcionar garantías del servicio en el nivel de la capa 2.

SBM define el control de admisión LAN y la administración del ancho de banda, que, combinados con la conformación por flujo en los sistemas finales y definido por el IEEE en la capa de enlace, permite alguna aproximación del servicio garantizado y de los servicios de carga controlada sobre la LAN a través del protocolo Designated SBM (DSBM), entidad en cada segmento de la capa 2, que se inserta con eficacia como nodo intermedio entre el origen y el receptor, para que todos los mensajes RSVP pasen a través de él y así admitir los flujos basados en la disponibilidad del ancho de banda en la LAN. Los host SBM-capaces soportan RSVP y seleccionan una clase de tráfico para sus flujos de datos basados en 802.1D user_priorities; sin embargo debe tomarse en cuenta que SBM es un nuevo estándar y puede tomar tiempo hasta que sea soportado por la mayoría de equipos de capa 2; mientras que una LAN puede proporcionar

QoS transparente aprovechándose del ancho de banda más significativo ofrecido por Fast Ethernet y Gigabit Ethernet.

4.1.2.2. Funciones QoS

4.1.2.2.1. En los hosts

Los hosts en el ambiente LAN incluyen a clientes, servidores, PC's, etc, la figura 4.2 ilustra los componentes relacionados con el QoS de un host, que en muchos casos puede clasificar sus flujos de aplicaciones y solicitar el tipo de servicio (ToS) DiffServ y marcado 802.1D apropiado, así las tarjetas de red (NIC) pueden marcar frames y paquetes basados en políticas de red predefinidas o distribuidas dinámicamente.

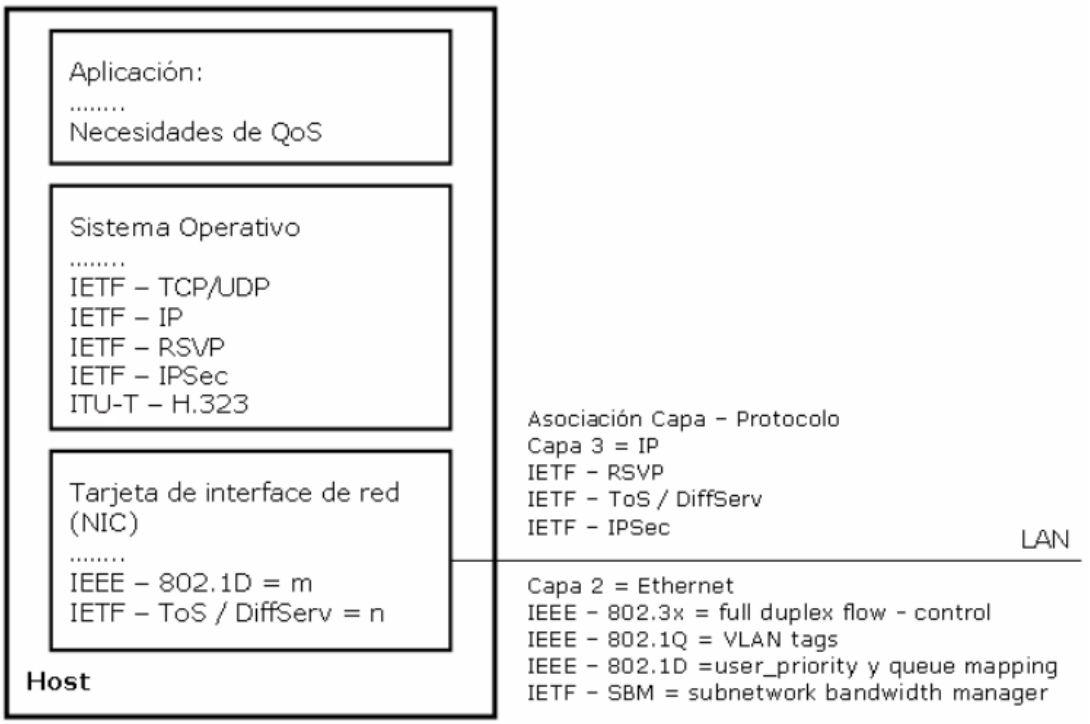


Figura 4.2: Componentes QoS de un host

4.1.2.2.2. En los routers LAN

Un ambiente LAN puede incluir routers para conectar subredes IP, los cuales pueden ser RSVP-capaces para permitir su participación en las reservación RSVP y eventualmente acomodarse a la señalización SBM o RSVP-no capaces para pasar los mensajes RSVP transparentemente.

Como se muestra en la figura 4.1, el router de acceso (AR) se interconecta con la WAN y debe clasificar, gestionar políticas, conformar correctamente todos los flujos que ingresan a la red del ISP y comunicar la clasificación del tráfico a los routers WAN; una vez que se clasifica y encola el tráfico, el AR lo gestiona en la respectiva cola y lo conforma en la salida, además controla los valores DiffServ apropiados para varios flujos de tráfico, los cuales pudieron marcarse originalmente en los hosts y entonces ser preservados o redefinidos por este router, puede asignar los valores DiffServ como método de clasificación del tráfico y proporcionar la información adicional de la clasificación al router WAN, que es una funcionalidad del interworking LAN a WAN.

Se puede emplear un router que use CBQ, Class-based queuing es una variación de priority queuing donde las colas se definen en términos de la preferencia con la cuál ellos son servidos y la cantidad de tráfico encolado drenado desde ellos en cada rotación del servicio, porque puede distinguir entre numerosas aplicaciones, usuarios, afiliaciones de usuarios y así sucesivamente y clasifican el tráfico en centenares de colas basadas en software

4.1.2.3. QoS para VoIP en la LAN

VoIP es una aplicación crítica para el QoS diferenciado debido a que la transmisión del tráfico de voz conlleva requisitos rigurosos en pérdida de paquetes, retardo y jitter y aún más con la presencia de otros flujos en la red; además, las llamadas de voz requieren el proceso de configuración de la llamada y control de admisión de la llamada (CAC).

El tráfico de VoIP se define en términos de media flow y señalización. Un framing recomendado para los media flow VoIP es RTP/UDP/IP (RTP = Real Time Protocol). Considerando que todos los flujos IP son simples (unidireccionales), las llamadas VoIP requieren la asignación del ancho de banda en ambas direcciones de la comunicación.

4.1.3. Parámetros en la red WAN

Los proveedores de servicio usualmente implementan el QoS en el núcleo WAN para identificar correctamente todo el tráfico para el cual escribió los acuerdos de nivel de servicio basados en el QoS diferenciado, entonces debe asegurarse que el tráfico reciba el QoS contraído y finalmente, obtener un detalle del tráfico y procesar esta información para la facturación. Los mecanismos QoS son implementados en:

4.1.3.1. Los routers WAN

Las funciones del router WAN incluyen a los routers del borde (edge routers - ER's), los routers del núcleo (core routers - CR's) y los routers limítrofes (border routers – BR's), como se muestra en la figura 4.1. Los routers ER's recogen el tráfico de los routers AR's de los clientes, lo clasifican, gestionan las políticas y lo conforman para la entrega en la WAN. Si MPLS es implementado en la WAN, los routers ER's sirven como etiqueta de los routers de borde (label edge routers – LER's) y son usados para accionar el protocolo de distribución de etiquetas (Label Distribution Protocol – LDP), añadir y quitar las cabeceras de MPLS. Los routers CR's se encargan de leer las cabeceras IP o etiquetas MPLS y enviar los paquetes a altas velocidades. Los BR's proporcionan interfaces a otras redes y suelen tratarse como routers ER.

Los routers WAN funcionan en velocidades mucho más altas que los routers de una empresa e implementan la clasificación, gestión de colas y funciones de planificación de colas (scheduling) en hardware, usando Weighted Fair Queuing (WFQ), es un mecanismo de priority queuing que clasifica e interpola paquetes individuales por flujo y encola cada flujo basado en el volumen del tráfico, procurando proporcionar tiempos de respuesta fiables, para la planificación de colas y RED (Random Early Detection) como mecanismo de descarte de paquetes.

Es común tener un número relativamente pequeño de colas basadas en hardware (por ejemplo, ocho), lo que significa que un número alto de flujos

manejados por el router AR debe ser colocado en varias colas y diferentes flujos de aplicaciones deben ser combinados y conformados cuidadosamente para trabajar correctamente; por ejemplo, si un router WAN tiene ocho colas, se pueden utilizar para las siguientes clases de servicios de red:

- Real time (RT) unicast: VoIP, video conferencia.
- RT multicast.
- Administración de la red: SNMP.
- Señalización: RSVP, OSPF.
- Transacciones, es decir, pequeños mensajes con bajos requerimientos de pérdida de paquetes.
- Transferencia de archivos, es decir, aplicaciones elásticas, por ejemplo, ftp y e-mail.
- No – RT multicast.
- Tráfico BE (clase por defecto para el tráfico que no se clasifica en otra parte).
- El tráfico de VPN se puede asignar a una cola basada en la clase especificada en el SLA.

4.1.3.2. Mecanismos QoS en la red WAN

Los mecanismos QoS WAN dominantes son DiffServ y MPLS (Multi – protocol Label Switching) y aunque se han considerado por separado, actualmente el grupo de trabajo IETF MPLS está definiendo MPLS con el marco de trabajo de DiffServ para habilitar las garantías de QoS en las redes MPLS.

4.1.3.2.1. DiffServ

Es un estándar del IETF basado en un conjunto de mejoras al protocolo IP que permiten el provisionamiento del tratamiento diferenciado para diversas clases de servicio (CoS's) sin la necesidad de un estado por flujo y la señalización en cada salto, específicamente se utiliza para la agregación de tráfico, sus características y funcionamiento se detallan en el Capítulo 3 apartado 3.4.

4.1.3.2.2. MPLS

Facilita el envío de paquetes y proporciona QoS diferenciada mediante la conmutación de etiquetas en lugar del enrutamiento basado en la dirección IP, se utiliza principalmente para la agregación de tráfico, el balanceo de carga y la optimización de recursos de la red, siendo su aplicación más importante la Ingeniería de Tráfico (TE), donde el tráfico se envía por rutas específicas, posiblemente no óptimas, conocidas como label switched paths (LSP's) y los routers, label switching routers (LSR's), divididos en LSR's del borde proporcionan la interfaz entre la red IP externa y el LSP, en el ingreso aceptan los paquetes IP y añaden las etiquetas MPLS y en la salida termina el LSP quitando las etiquetas MPLS y retornando al envío IP normal y los LSR's del núcleo proveen servicios de tránsito a través de la nube MPLS.

Los LSR's del borde al ingreso se basan en las políticas de la red para transportar la información de clasificación del flujo en las cabeceras MPLS, a través de dos mecanismos: E-LSP, donde el campo de 3 bits Exp en la cabecera

lleva la información de CoS y se la puede asociar directamente a la precedencia ToS o DSCP y L-LSP, en el que la etiqueta lleva la información de CoS y la asociación QoS necesita ser refinada.

MPLS puede ser provisionado estáticamente o utilizar un protocolo de señalización, como RSVP tunneling extensions (RSVP – TE) o LDP, que soportaba LSP's basado en el enrutamiento IP del siguiente salto pero no soportaba la ingeniería de tráfico, por lo que se creó Constrained Routing Label Distribution Protocol (CR – LDP).

1. **CR – LDP:** es un protocolo hard state que no requiere refrescar estados, proporciona la comprensión común entre dos LSR's del significado de etiquetas y se usa para enviar tráfico entre ellos, establece la reservación de recursos en la trayectoria de envío e incluye cuatro categorías de mensajes:

    - Descubrimiento: enviado periódicamente por los LSR's para anunciar su presencia.

    - Sesión: establece, mantiene y termina una sesión entre dos peers LDP.

    - Anuncio: crea, cambia y borra las asociaciones de etiquetas para clases equivalentes de envío (FEC's: forwarding equivalency classes) después de que una sesión se ha establecido.

- Notificación: se encarga de la señalización.

2. **RSVP – TE:** fue desarrollado como extensión de RSVP - E2E mientras que CR - LDP era todavía definido, proporciona señalización entre routers, crea un estado para una colección de flujos entre los puntos de ingreso y salida de un tráfico, utiliza un firm state donde los mensajes Path y Resv son periódicamente refrescados, pero su volumen se reduce perceptiblemente, comparado al soft state, por el uso de actualizaciones incrementales y agregadas.

Un protocolo de señalización, puede realizar una variedad de funciones, tales como crear el estado de la trayectoria en cada LSR al realizar la asignación de etiquetas, distribución y enlazado; reserva de recursos en cada LSR, incluyendo ancho de banda, retardo y límites de pérdida de paquetes; reasignar los recursos de red cuando sea necesario; reennrutamiento dinámico durante la congestión y fallas de red; monitorear y mantener explícitamente el estado LSP enrutado y proporcionar información LSP al sistema de administración de la red, entre otras.

4.1.3.3. QNS (QoS Network Server)

El servidor QoS de red es una entidad funcional esencial en la red del ISP que tiene una vista total de la red y soporta una variedad de funciones incluyendo interworking con las premisas del cliente, señalización VoIP y CAC, acceso a los directorios y bases de datos, compilación de la información del uso y

disponibilidad de los recursos de la red para la facturación y control de políticas puesto que se convertirá en un punto de decisión de política (PDP: Policy Decision Point). En el futuro, podrá también incluir los módulos para la optimización de los recursos de la red y balanceo de carga que serán utilizados en la distribución de la etiqueta de MPLS.

Para permitir los servicios comprensibles de VoIP, el QNS debe ofrecer un conjunto de características, incluyendo media servers que despliegan reconocimiento de la voz y generan avisos y una plataforma de desarrollo que permite la configuración personalizada de los servicios de red a los clientes y usuarios individuales, además debe acomodar rápidamente cualquier nuevo protocolo de control de la llamada y el interwork de éste con el resto de los protocolos.

La implementación exitosa de VoIP requiere protocolos IP QoS como IEEE 802.1D, RSVP y DiffServ que proporcionan servicios de red diferenciados basados en la clasificación del tráfico y además mecanismos específicos de voz. La calidad de servicio para las aplicaciones de VoIP en la WAN consiste de tres partes:

- **Señalización extremo a extremo para configurar una llamada**: proporcionada por H.323 o el protocolo de iniciación de la sesión (SIP: Session Initiation Protocol), que permite crear, modificar y terminar sesiones de voz sobre redes IP.

- **Establecimiento de una trayectoria provisionada para el media flow** dependiendo del volumen del tráfico de voz y los patrones, la cantidad de otro tráfico en la red y su QoS a través de varias opciones como una cola de un router WAN dedicada a VoIP con un ancho de banda asignado en cada salto de la red, DiffServ podría identificar los paquetes de voz para la asignación a esta cola, proveer LSP's MPLS entre todos los bordes de la red que intercambian tráfico VoIP o una solución híbrida utilizará MPLS para el enrutamiento explícito pero sin reservaciones de ancho de banda, mientras que DiffServ será utilizado para la asignación de ancho de banda agregada.

- **CAC:** se utiliza en redes IP para prevenir el deterioro de una llamada VoIP si el volumen de la misma excede el ancho de banda asignado. En la arquitectura QoS extremo a extremo, se proporciona usando interacciones entre el QCS, que solicitará la admisión a nombre de las llamadas VoIP originadas en su dominio y el QNS que vigilará los recursos de la red.

4.1.4. Interworking LAN a WAN

Hasta el momento se han analizado los mecanismos QoS relacionados con el ambiente LAN de la empresa y el núcleo WAN del proveedor de servicios; sin embargo, la implementación QoS extremo a extremo también requiere un bien definido interworking LAN a WAN, es decir el trabajo conjunto de todas las partes de la red. En la figura 4.1 se muestran los niveles de interworking, entre los que

tenemos: media flows, intercambios de señalización, CAC, distribución de políticas y generación de información de facturación.

La señalización interworking consiste en intercambios de información que conducen a la clasificación apropiada de los flujos; estos ajustes privados en la interfaz LAN - WAN requerirán la coordinación cercana de políticas entre el ISP y la empresa.

El interworking entre la LAN y la WAN puede lograrse por intercambios de señalización con la implementación de la funcionalidad QCS – QNS, que habilitará la presencia del proveedor de servicios en las premisas del cliente, según acuerdos individuales entre ISP's y sus clientes, que determinarán si el QCS será poseído y operado por el ISP o conformado con las especificaciones del ISP pero pertenece a la empresa, o solamente las interfaces estándares serán utilizados. Se incluye las necesidades de señalización específica de configuración de llamadas VoIP y la señalización general relacionada al tráfico IP; que contiene información acerca de las configuraciones privadas ToS/DSCP entre el AR y ER. En un caso más general, será necesario trabajar entre diversas implementaciones de la arquitectura IP en la LAN y WAN, por ejemplo, un ambiente LAN puede utilizar la arquitectura IntServ con RSVP-E2E como su protocolo de señalización, mientras la WAN puede seguir la arquitectura DiffServ, para preservar el QoS entre estos tipos de dominios comunes, el grupo IETF ISSLL ha desarrollado el IntServ al estándar interworking DiffServ.

Las necesidades de desarrollo de redes QoS basadas en políticas requieren la coordinación entre la empresa y los servidores de política del ISP, así, el QCS y el QNS se ampliarán en la funcionalidad de PDP (Policy Decision Point). El intercambio de información de políticas incluirá áreas de marcado del paquete, decisiones de admisión, usuarios prioritarios, enrutamiento explícito, descarte de paquetes, asignación de ancho de banda en la cola, reacción ante la congestión en la red y muchas otras.

4.2. ANÁLISIS DE LOS MECANISMOS

Las aplicaciones de tiempo real requieren considerar factores como ancho de banda, delay y jitter para su correcto funcionamiento y debido a esto los investigadores, proveedores de servicio y operadores de red han considerado seriamente políticas de calidad de servicio, las cuales se pueden implementar a través de mecanismos proveídos por las arquitecturas DiffServ o IntServ, que proporcionan en primer lugar un medio adecuado para establecer las rutas que satisfagan los requisitos de la aplicación, las cuales son computadas por el funcionamiento de un algoritmo QoS y después por la aplicación de un mecanismo que permita controlar los parámetros de calidad de servicio.

A continuación se detallan las características principales de los algoritmos de enrutamiento QoS principales y los mecanismos de gestión de colas que influyen directamente sobre los parámetros de calidad de servicio que afectan a las aplicaciones y de acuerdo a los criterios establecidos posteriormente en el apartado 4.3.3 Fase 3, se seleccionará tanto el algoritmo de enrutamiento QoS

como el mecanismo para el control del delay, jitter y loss que se empleará en el mecanismo propuesto.

4.2.1. Algoritmos de enrutamiento QoS

Un algoritmo es una secuencia finita de instrucciones o pasos que permiten obtener un resultado determinado, ejecutar una tarea o resolver un problema y debe ser modular, eficiente y estructurado para desarrollarse en el menor tiempo posible.

La meta principal de un algoritmo de enrutamiento es encontrar una trayectoria factible que utilice los recursos de la red eficientemente y que considere aspectos como: la carga de los enlaces no es constante y el mejor camino no siempre será el mismo puesto que el tráfico varía con el tiempo y el camino óptimo también dependerá del instante en que se observe la red; cambios en la topología de la red: nodos caídos, eliminados o nuevos; recursos limitados y cambios en la definición de las políticas de calidad de servicio.

Para optimizar el funcionamiento de la red, los algoritmos de enrutamiento de calidad de servicio se basan en dos técnicas diferentes; la primera consiste en seleccionar la trayectoria con el número mínimo de saltos para reducir el consumo de recursos y la segunda escoge la trayectoria menos cargada para balancear la carga de la red; esta optimización de la utilización de la red no es fácilmente realizable al usar un algoritmo de enrutamiento simple puesto que estas dos

metas pueden ser opuestas, por esta razón, la utilización de un algoritmo QoS de cómputo de la ruta debe tomarse en cuenta.

A continuación se presentan algunos algoritmos de enrutamiento QoS que ofrecen los mejores resultados en el contexto de una red IP:

4.2.1.1. WSPF (Widest Shortest Path First)

Considera dos métricas, primero el número de saltos y después el ancho de banda disponible. El algoritmo procede como sigue: en la primera etapa se computan todas las trayectorias más cortas existentes entre cada origen y todos los destinos en la red, en la segunda etapa, el ancho de banda se utiliza para romper lazos entre las trayectorias que tienen el mismo número de saltos y se selecciona la trayectoria que tiene la cantidad más alta de ancho de banda disponible, de esta forma se selecciona la trayectoria con el mínimo número de saltos y si más de una trayectoria es seleccionada entonces se escoge la del ancho de banda residual máximo (MRB: maximum residual bandwidth), estas trayectorias Widest-Shortest se pueden computar por versiones modificadas de los algoritmos de Bellman-Ford o de Dijkstra.

El objetivo principal de este algoritmo es reducir el costo de la red. El consumo de recursos de red es limitado porque las trayectorias más cortas se favorecen sobre trayectorias más anchas, puesto que la preservación del recurso es especialmente importante cuando se congestiona la red, este tipo de algoritmo muestra un funcionamiento muy bueno cuando la carga de la red es alta y cuando la decisión del

enrutamiento se toma sobre la información del estado de la red que es inexacta, porque la métrica principal (número de saltos) no es influenciada perceptiblemente por la inexactitud de la información de enrutamiento debido a que cambia menos a menudo que el ancho de banda disponible. WSP funciona bien porque conserva simultáneamente recursos eligiendo la trayectoria más corta y balancea la carga eligiendo la trayectoria más ancha entre los que tengan la misma longitud.

4.2.1.2. SWPF (Shortest Widest Path First)

Es una propuesta contraria a WSPF, donde el primer criterio es el ancho de banda residual máximo y el segundo el número de saltos, el objetivo de este algoritmo es encontrar las trayectorias con la cantidad más alta de ancho de banda disponible, es decir la trayectoria más ancha. En una segunda fase, si hay varias trayectorias con la misma cantidad de ancho de banda disponible, se selecciona la trayectoria más corta según la métrica de longitud usada, sea el número de saltos o el delay extremo a extremo, en la mayoría de los casos se selecciona la que tiene el menor número de saltos.

El balanceo de la carga alcanzado con la selección de la trayectoria con la disponibilidad más alta de ancho de banda es el objetivo principal de este algoritmo y sus ventajas son la simplicidad y la capacidad de pre - cómputo, sin embargo, tiene dos desventajas, la primera consiste en el aumento en el costo en la red porque la trayectoria más ancha corresponde generalmente a una trayectoria más larga y la segunda, la degradación del funcionamiento del tráfico, debido al comportamiento egoísta del algoritmo del cómputo de la trayectoria; por lo tanto, la utilización de la

trayectoria más ancha puede restringir la admisión de flujos con requisitos más estrictos, que podrían ser evitados de otra manera computando una trayectoria con apenas el bastante ancho de banda disponible para satisfacer los requisitos del flujo; pero para esto se requeriría un algoritmo más complejo.

4.2.1.3. DORA (Dynamic Online Routing Algorithm)

Es un algoritmo de enrutamiento en línea dinámico para la construcción de trayectorias con ancho de banda garantizado en las redes, su objetivo es evitar el enrutamiento sobre enlaces que tienen un alto potencial de ser parte de cualquier otra trayectoria y tener ancho de banda residual disponible bajo.

El funcionamiento de DORA tiene dos etapas: la primera calcula el llamado arreglo (array) del valor de trayectoria potencial (PPV: path potencial value) asociado con el par origen-destino. El potencial de un enlace que tiene más probabilidad de ser incluido en una trayectoria que otros enlaces es caracterizado por un PPV asociado. Formalmente, para cada par origen - destino, se asocia a cada enlace un número entero llamado PPV con un valor inicial de cero. Cada par origen – destino *(S, D)* es asociado con un arreglo, $PPV_{(S,\ D)}$. Cuando una trayectoria puede ser contraída sobre un enlace *L* para un par origen – destino dado *(S1, D1)*, se reduce $PPV_{(S1,\ D1)}(L)$ por 1. Cuando una trayectoria puede ser construida sobre el mismo enlace *L* para un par origen – destino diferente *(S2, D2)*, se incrementa $PPV_{(S2,\ D2)}(L)$ por 1. Puesto que hay muchas trayectorias entre un par origen – destino dado, se consideran solamente las trayectorias distintas (disjoints paths). La segunda etapa combina el PPV con el ancho de banda

residual del enlace (residual link bandwidth) para formar un valor del peso de cada enlace de la trayectoria, que es usado para computar una trayectoria con peso optimizado de la red, para esto se retiran todos los enlaces con un ancho de banda residual menor que el ancho de banda requerido. El PPV y ancho de banda residual actual de cada enlace son combinados para formar el peso del enlace. El contenido del peso del enlace es controlado por un parámetro llamado BWP (BandWidth Proportion). Finalmente, se corre el algoritmo de Dijsktra para computar una trayectoria de peso optimizado en la topología residual[39].

4.2.2. Mecanismos para el control del delay, jitter y pérdida de paquetes

La gestión de colas, conocida como Queuing, tiene un impacto directo en los parámetros de QoS, ancho de banda, delay, jitter y pérdida de paquetes y en la administración de la congestión, por lo que los mecanismos para el control de dichos parámetros se basan en las herramientas de queuing que se analizaron en el Capítulo 2, apartado 2.3.6.2, literales d y e, dichas herramientas de gestión de colas (Queuing), planificación y estrategias de servicio de colas (Scheduling) definen el número de colas y el tamaño de la cola de salida, que afecta al retardo, jitter y pérdida de paquetes, considerando que la cola tiene un tamaño finito; si ésta se llena y otro paquete necesita ser agregado a la cola, el tail drop (si llega un paquete y no le interesa lo descarta) causaría que el paquete sea descartado; se debe considerar lo siguiente con respecto a la longitud de la cola:

- Con una cola más larga, la oportunidad de tail drop disminuye con respecto a una cola más corta, pero el delay y jitter promedio aumentan.

- Con una cola más corta, la oportunidad de tail drop aumenta con respecto a una cola más larga, pero el delay y jitter promedio disminuyen.

A continuación se presentan algunos mecanismos para el control del delay, jitter y pérdida de paquetes:

4.2.2.1. FIFO (First in – First out)

Es el esquema básico para la gestión de colas, utiliza una sola cola, con la planificación primero en entrar, primero en salir (FIFO), es decir que se toma el siguiente paquete de la cola, considerando el que llegó antes que todos los otros paquetes en la cola, en este caso el router no requiere las funciones de clasificación para decidir la cola en la cuál el paquete debe ser colocado ni planificación para escoger de cuál cola se toma el paquete siguiente o cómo se ordenarán los paquetes en cada cola; considera únicamente la longitud de la cola y su influencia en el retardo y la pérdida de paquetes y el tail drop para decidir cuándo descartar o encolar los paquetes.

4.2.2.2. PQ (Priority Queuing)

Este mecanismo se caracteriza por su scheduler (planificador) que administra el tráfico de manera que las colas de alta prioridad son siempre servidas y tiene un máximo de cuatro colas, llamadas alta, media, normal y baja, lo que provoca que cuando hay congestión, los paquetes en las colas más bajas

tomen significativamente más tiempo para ser servidas que bajo cargas más ligeras.

Clasifica los paquetes basado en el contenido de su cabecera y utiliza como política de descarte a tail drop, es decir que después de clasificar el paquete, si la cola apropiada está llena, el paquete es descartado. La tabla 4.2 resume las principales características de PQ[17].

Tabla 4.2: Características de Priority Queuing

Características	Explicación
Clasificación	Basada en la asociación de un ACL para todos los protocolos de Capa 3, interfaces entrantes, tamaño del paquete, si el paquete es un fragmento y números de puerto TCP y UDP.
Política de descarte	Tail drop
Número máximo de colas	4
Longitud máximo de la cola	Infinito, que significa que los paquetes no serán descartados, pero serán encolados.
Scheduling dentro de una cola	FIFO
Scheduling entre las colas	Siempre sirve primero las colas con la prioridad más alta; cuyo resultado es un gran servicio para la cola alta, con el 100% del ancho de banda del enlace. El servicio se degrada rápidamente para las colas de baja prioridad.

4.2.2.3. CQ (Custom Queuing)

Este mecanismo permite servir a todas las colas, incluso durante la congestión, tiene 16 colas disponibles, implicando 16 categorías de clasificación, lo que proporciona un gran servicio para el tráfico sensible al delay y jitter; sin embargo el planificador de CQ no tiene una opción para servir siempre una cola

primero, como en el caso de PQ, sino que garantiza el ancho de banda mínimo para cada cola. La tabla 4.3 identifica algunas de las características de CQ[17].

Tabla 4.3: Características de Custom Queuing

Características	Explicación
Clasificación	Basada en la asociación de un ACL para todos los protocolos de Capa 3, interfaces entrantes, tamaño del paquete, si el paquete es un fragmento y números de puerto TCP y UDP.
Política de descarte	Tail drop
Número máximo de colas	16
Longitud máximo de la cola	Infinito, que significa que los paquetes no serán descartados, pero serán encolados.
Scheduling dentro de una cola	FIFO
Scheduling entre las colas	Sirve los paquetes de una cola hasta que la cuenta del byte se alcanza; utiliza round-roubin en las colas, sirviendo las diferentes cuentas de bytes para cada cola. Se reserva un porcentaje del ancho de banda del enlace para cada cola.

4.2.2.4. WFQ (Weighted Fair Queuing)

Este mecanismo se introduce para solventar los problemas presentados por los diferentes mecanismos de encolamiento como FIFO, PQ y CQ, clasifica los paquetes basado en flujos que se identifican con los siguientes elementos: dirección IP origen y destino, protocolo de capa de transporte (TCP o UDP) según lo definido por el campo de la cabecera del protocolo IP, puerto origen y destino TCP o UDP. Cada flujo usa una cola diferente, siendo 4096 colas por interfaz como máximo, sin embargo el número de flujos y por lo tanto el número de colas, cambia muy rápidamente.

El planificador de WFQ tiene dos metas principales, la primera es proporcionar la imparcialidad entre los flujos actualmente existentes, para lo cual da a cada flujo una cantidad igual de ancho de banda, así, los flujos de bajo volumen prosperan y los flujos del alto volumen sufren y la segunda es proporcionar más ancho de banda a los flujos con valores más altos de precedencia. Si los flujos de bajo volumen tienen valores de precedencia alta, las características de ancho de banda/delay/jitter/loss mejoran aún más. La política de descarte es el tail drop modificado que incluye un límite por cola, un límite agregado para todas las colas, con la habilidad de desencolar un paquete previamente encolado si el nuevo paquete tiene un mejor número de secuencia.

No tiene un desempeño adecuado para la voz y para el tráfico de video interactivo, porque ambos necesitan bajo delay y jitter y éste no proporciona una cola de prioridad para reducir al mínimo el delay y el jitter, incluso el delay puede incrementarse cuando hay demasiados flujos concurrentes. La tabla 4.4 muestra las características de este mecanismo[17].

Tabla 4.4: Características de Weighted Fair Queuing

Características	Explicación
Clasificación	Clasifica sin configuración, basado en la dirección IP, puerto origen/destino, tipo de protocolo (TCP/UDP) y ToS.
Política de descarte	Tail drop modificado
Número máximo de colas	4096
Longitud máximo de la cola	El umbral del descarte por congestión por cola (máximo 4096), con un límite global basado en el sostenimiento para todas las colas (máximo 4096).
Scheduling dentro de una cola	FIFO
Scheduling entre las colas	Sirve el número de secuencia más bajo. El número de secuencia se asigna cuando el paquete se coloca en la cola, como una función de longitud y la precedencia.

4.2.2.5. CBWFQ (Class-Based Weighted Fair Queuing)

Combina algunas de las mejores características de las otras herramientas en un solo mecanismo, como CQ puede reservar ancho de banda mínima para cada cola (máximo 64), puede utilizar WFQ dentro de una cola particular, como comportamiento predeterminado para tráfico sin clasificar. El comportamiento de la pérdida de paquetes puede aprovecharse de WRED, que reduce las posibilidades de sincronización global. Además, de todas las herramientas que hacen cola, CBWFQ tiene la variedad más grande de campos directamente asociables para clasificar los paquetes. El problema de CBWFQ es la carencia de una característica como PQ. Los tráficos sensibles al delay y el jitter sufren, aún cuando bastante ancho de banda ha sido reservado por CBWFQ, porque el planificador de CBWFQ puede servir otro colas cuando un paquete de VoIP o está esperando en una cola.

4.2.2.6. LLQ (Low Latency Queuing)

Es una variante de CBWFQ que aplica políticas basado en el ancho de banda configurado, para lo cual, los paquetes en la cola que todavía no se envían tienen latencia muy baja, pero LLQ también evita que el tráfico de baja latencia consuma más que su cantidad de ancho de banda configurada. Para descartar el exceso de tráfico, LLQ puede proporcionar garantías de ancho de banda a las colas no prioritarias. La función de gestión de políticas (Policing) de LLQ protege a las otras colas de la cola de baja latencia, pero descarta los paquetes para lograr esa meta. Siempre sirve primero la cola de baja latencia, pero en estas colas se aplica una política para prevenir que dominen el enlace, por lo que es usado para tráfico Real Time y puede utilizar como política de descarte de paquetes el tail drop o WRED.

4.3. PLANTEAMIENTO DEL NUEVO MECANISMO

4.3.1. Consideraciones previas

Como se ha analizado hasta ahora la tendencia actual es hacia la convergencia de las aplicaciones de voz, video y datos en una sola infraestructura debido a la simplicidad y ahorro en costos que esto conlleva, esto se logra a través de las redes IP que permiten la interacción entre diferentes tecnologías y la posibilidad de ofrecer servicios diferenciados acordes a la calidad de servicio demandada por las aplicaciones del cliente en función del delay, el jitter, la capacidad del ancho de banda y la pérdida de paquetes.

El modelo de Servicios Diferenciados, DiffServ, seleccionado debido a sus beneficios como el diseño de baja complejidad, fácil administración y mantenimiento, control del provisionamiento de recursos por clase y escalabilidad permite la definición de un mecanismo para ofrecer calidad de servicio acorde a las necesidades de las aplicaciones y las perspectivas de los ISP's. En la figura 4.3[40] se ilustra el funcionamiento de DiffServ, que se describió en el Capítulo 3, apartados 3.4.3.5 y 3.4.4

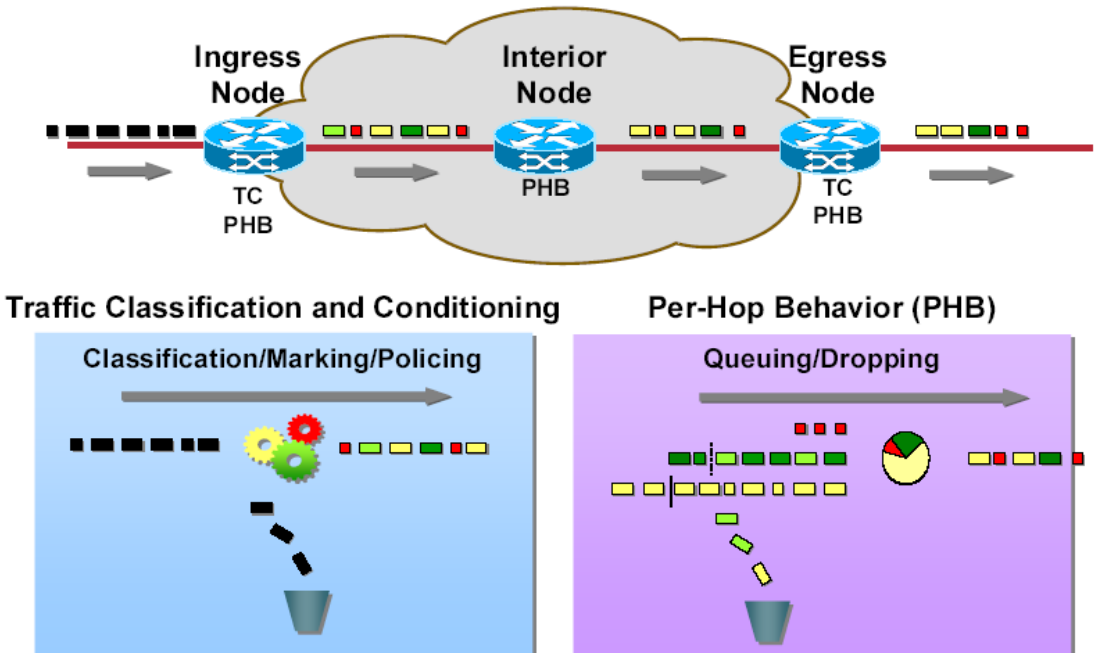


Figura 4.3: Arquitectura de servicios diferenciados

Como se observa en la figura 4.3[40], el modelo DiffServ permite la diferenciación de las aplicaciones dependiendo de los parámetros de calidad de servicio requeridos por éstas, así cuando el tráfico ingresa a la nube, el primer router realiza las funciones de clasificación y condicionamiento del tráfico, donde se divide y marca el tráfico de acuerdo a las clases de servicio configuradas, el router interior aplica el respectivo PHB según la política definida y decide la cola

en la que se colocará el tráfico o si se descartará y finalmente el router de salida envía el tráfico al destinatario; de acuerdo a lo expuesto anteriormente y basados en el funcionamiento de DiffServ se planteará el mecanismo para implementar la calidad de servicio extremo a extremo en redes IP.

4.3.2. Definición del mecanismo

La figura 4.4 ilustra las seis fases en las que se divide el mecanismo propuesto, que se describe a continuación.

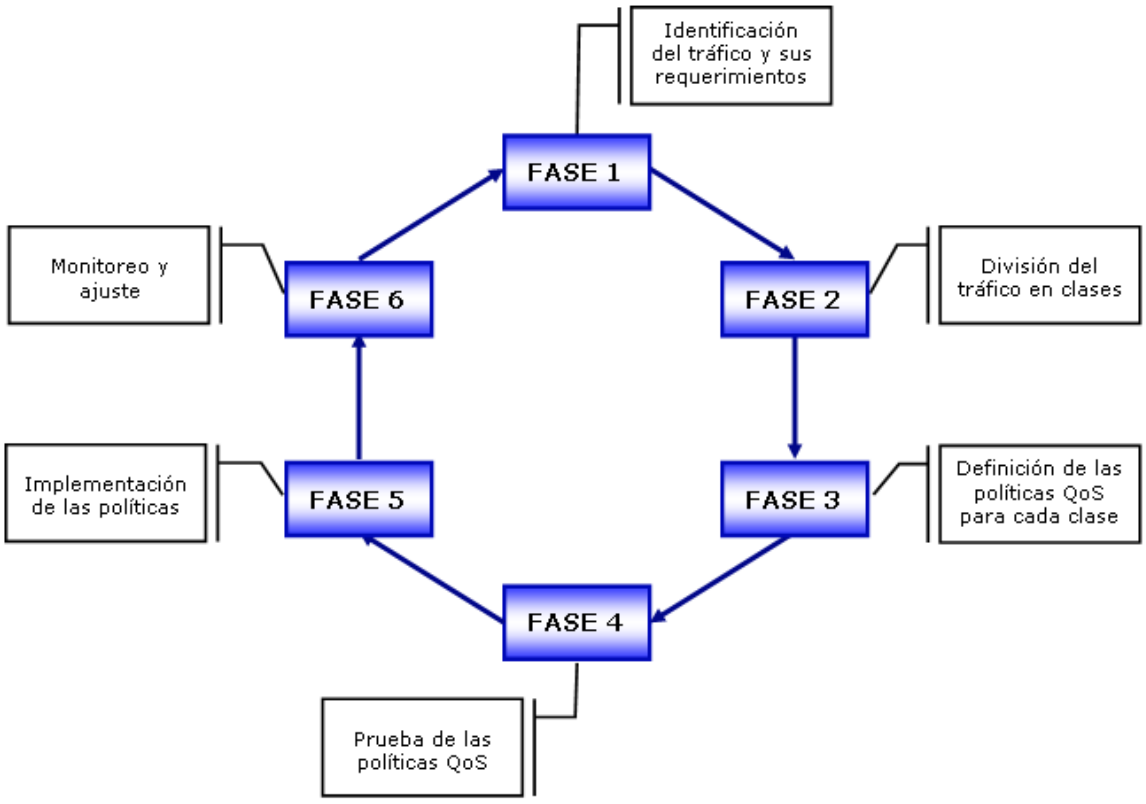


Figura 4.4: Mecanismo propuesto

Se debe identificar el tráfico y sus requerimientos, definir los objetivos de comunicación de la empresa que se alcanzarán a través de la implementación de

QoS, para lo cual se establecerán las aplicaciones críticas para el negocio, su prioridad, características, funcionamiento, los recursos de red necesarios para satisfacer dichas aplicaciones y finalmente los requerimientos de calidad de servicio, es decir la sensibilidad de estas aplicaciones a los parámetros de QoS como delay, jitter y pérdida de paquetes.

Una vez que se han analizado las aplicaciones de los clientes y se han determinado sus características y prioridades se debe clasificarlas de acuerdo a los requerimientos del nivel de servicio de las clases de tráfico establecidas previamente, para lo cual se debe considerar el número de clases necesarias para abarcar a todos los tipos de aplicaciones; en el caso del mecanismo propuesto estas clases se definen en el apartado 4.3.3, fase 2.

Cada clase de tráfico debe ser asociada a una política de calidad de servicio, en la que se establece las definiciones para la configuración de los parámetros QoS, como: mínimo ancho de banda garantizado, límite máximo de ancho de banda, prioridad de cada clase y el manejo del flujo de tráfico en caso de congestión. Se debe considerar la topología de la red, la capacidad tanto en los enlaces de la red (velocidad, congestión, etc.) como de los dispositivos (CPE: equipo en las premisas del cliente, software, etc.) y los enlaces con y sin cuellos de botella, además se debe especificar el algoritmo de enrutamiento QoS y el mecanismo para el control de los parámetros de QoS, delay, jitter y pérdida de paquetes, que fueron tratados en el apartado 4.2; la selección se realizará en base a los criterios de comparación propuestos en el modelo de funcionamiento.

Posteriormente se debe realizar una serie de pruebas para verificar si las políticas QoS, el algoritmo de enrutamiento QoS y el mecanismo definido satisfacen los requerimientos de calidad de servicio de las aplicaciones, primero se las debe realizar en el laboratorio y posteriormente en una pequeña parte de la red, analizando los resultados con QoS como sin QoS para así comparar el funcionamiento de la aplicación, si los resultados no son los esperados se debe regresar a la tercera fase para revisar y corregir las definiciones de las políticas, caso contrario se continúa con la implementación de las políticas QoS, que deben aplicarse cuidadosa e incrementalmente; la clasificación y el marcado deberá ser tan cerca al borde como sea posible, es decir trabajar hacia el núcleo, aplicando políticas de entrada y salida; considerando también la implementación del mecanismo para el control de los parámetros QoS y del algoritmo de enrutamiento.

Es necesario monitorear el funcionamiento de las aplicaciones en las diferentes clases, con respecto al delay, jitter y pérdida de paquetes, para verificar si se están cumpliendo los requerimientos de las aplicaciones y si no es así se regresa a la primera fase para revisar los requisitos establecidos para las aplicaciones, añadir o eliminar aplicaciones e incluso puede ser necesario ajustar las políticas, cambiar el algoritmo de enrutamiento y/o el mecanismo para el control de las parámetros QoS en la tercera fase; siendo este un proceso cíclico en continua observación.

4.3.3. Modelo de funcionamiento

Como se aprecia en la figura 4.4 el mecanismo propuesto consiste en un ciclo de seis fases, sin embargo en el modelo de funcionamiento no se consideran las pruebas e implementación de los mecanismos empleados para calidad de servicio, puesto que requieren de mayor tiempo y la formación de equipos de trabajo que examinen a detalle el funcionamiento de las aplicaciones con y sin la utilización de dichas políticas, además deben tomar en cuenta las distintas tecnologías de acceso como Ethernet, Frame Relay, ATM, entre otras, velocidades de los enlaces del cliente y en la nube del ISP, las aplicaciones y su prioridad; así como los cambios en dichas prioridades y la introducción o eliminación de aplicaciones, los dispositivos empleados y su configuración, etc, es decir todos los casos que se pueden presentar, para así determinar si es necesario realizar un ajuste sobre las mismas.

A continuación se detallan los aspectos que se deben considerar en cada una de las fases de acuerdo al planteamiento presentado:

Fase 1: Identificación del tráfico y sus requerimientos

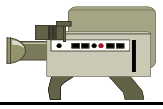
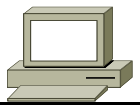
Las aplicaciones de los clientes se agrupan en tres tipos de tráfico básicos, cuyas características y requerimientos se trataron en el Capítulo 2, apartado 2.3.5. En esta fase se especifican todas las aplicaciones del cliente, si bien la Voz sobre IP y la videoconferencia están claramente diferenciadas, en el caso de los datos, el cliente será el responsable de determinar la prioridad de cada una de sus

aplicaciones con respecto a las otras, relacionando sus requerimientos frente al funcionamiento esperado; la figura 4.5 identifica esta fase con sus respectivas entradas, constituidas por las aplicaciones del cliente y en la salida están los requerimientos de las mismas.

Figura 4.5: Entradas y salidas en la fase 1

Esta clasificación previa de las aplicaciones varía entre las necesidades de los clientes por lo que es customizada; por ejemplo, en la tabla 4.5[41] se muestran algunas características.

Tabla 4.5: Tipos de tráfico

VOZ/IP	VIDEO/IP	DATOS
		
Delay = 150ms en un sentido Jitter = 30ms Pérdidas = 1% 17 – 106 Kbps por llamada (VoIP) + Señalización de la llamada (150 bps para control de tráfico)	Delay = 150ms en un sentido Jitter = 30ms Pérdidas = 1% Sobre provisionamiento del flujo en un 20% para contar con cabeceras + ráfagas Ancho de banda	Misión crítica Transaccional Best Effort Menos que Best Effort

Cabe recalcar que tanto las aplicaciones de voz sobre IP y videoconferencia también son conocidas como tráfico de tiempo real interactivo, el video sobre demanda y las películas como tráfico de tiempo real no interactivo y en el caso de los datos tenemos aplicaciones transaccionales como el

procesamiento de órdenes y la facturación, los sistemas de inventarios, contabilidad y reportes; aplicaciones de contenido web como el browsing, shopping y otras aplicaciones como e-mail, backups de datos, transferencias de archivos, archivos de impresión, etc.

Fase 2: División del tráfico en clases de servicio

La red IP que utilizará el mecanismo propuesto soportará seis clases de servicio (CoS), la primera reservada para los mensajes de los protocolos de enrutamiento, las cuatro siguientes para las distintas aplicaciones del cliente y la última para el tráfico hacia el Internet, además se determinó que cada clase sería identificada con un color y nombre distintivo, como se observa en la figura 4.6.

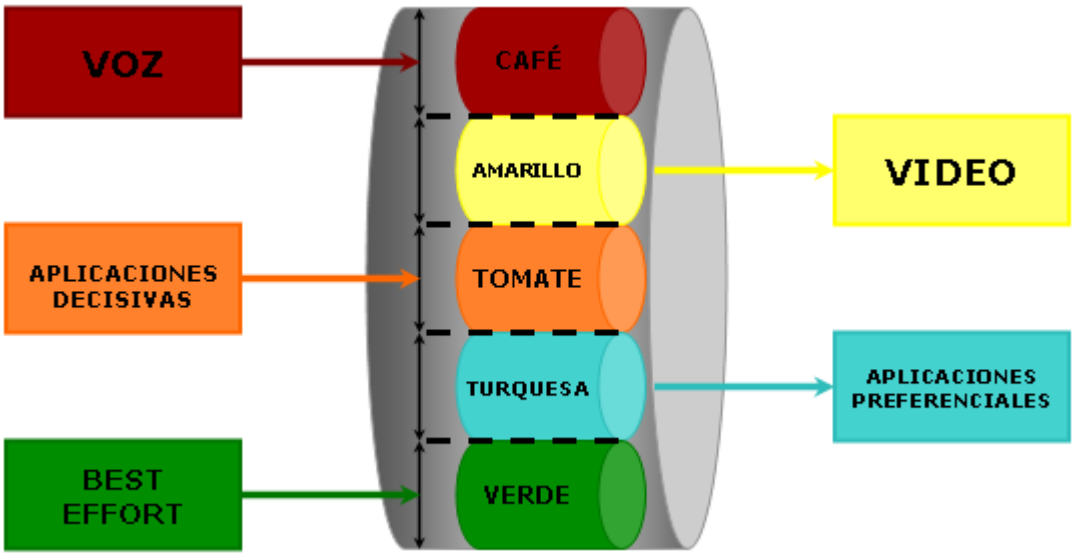


Figura 4.6: Clases de servicio

- **Enrutamiento:** reservada para los mensajes intercambiados por los protocolos de enrutamiento como BGP y OSPF; el marcado con esta CoS es realizado automáticamente por estos protocolos.

- **Café:** se utiliza para los paquetes que transportan Voz sobre IP (VoIP) y señalización sobre IP puesto que tiene prioridad absoluta frente a las otras clases y una cola de bajo retardo.

- **Amarillo:** se utiliza para diferenciar los paquetes que transportan información para aplicaciones de video.

- **Tomate:** se utiliza para las aplicaciones que el cliente considera decisivas en su negocio.

- **Turquesa:** empleada para las aplicaciones preferenciales, el cliente es el responsable de diferenciar sus aplicaciones, programas y servicios entre las clases de servicio tomate y turquesa.

- **Verde:** es la clase del mejor esfuerzo, empleada para los paquetes destinados a la red pública IP.

Una vez que se han establecido las características y prioridades de las aplicaciones, servicios y programas de los diferentes clientes, pasan a esta fase para ser divididas de acuerdo a las clases de servicio especificadas

anteriormente, la figura 4.7 ilustra los datos de entrada a esta fase y los respectivos datos de salida.

Figura 4.7: Entradas y salidas en la fase 2

Fase 3: Definición de las políticas QoS para cada clase

- **Asociación de cada clase de servicio con su respectivo valor de DSCP y/o Precedencia IP,** como se indica en la tabla 4.6.

Tabla 4.6: Clases de servicio con sus valores de DSCP y Precedencia IP

Clase de Servicio	DSCP	PRECEDENCIA IP
ENRUTAMIENTO	Reservada	IP6, IP7
VOZ	EF	IP5
VIDEO	AF41	IP4
APLICACIONES DECISIVAS	AF31	IP3
APLICACIONES PREFERENCIALES	AF21	IP2
BEST EFFORT	BE	IP0

Para cada clase de servicio se asocia un tratamiento especial, que podrá ser definido por el cliente de acuerdo a las características de utilización de la red

de su parte o será recomendado por el proveedor de servicios y además considerará los parámetros analizados en la Tabla 4.7.

Tabla 4.7: Parámetros definidos para las clases de servicio

Clase de Servicio	Parámetros en función de la velocidad de acceso a la red IP	Velocidad vs. Porcentaje máximo	
		Velocidad	Porcentaje máximo
VOZ	Ancho de banda y delay fijo máximo y garantizado	≤ 1 Mbps > 1 Mbps	20% 15%
VIDEO	Ancho de banda garantizado	≤ 1 Mbps > 1 Mbps	20% 15%
APLICACIONES PREFERENCIALES	No tienen fijadas limitantes con respecto a ancho de banda, solo la resultante de la aplicación de las reglas anteriores	≤ 1 Mbps > 1 Mbps	40% 50%
APLICACIONES DECISIVAS			
BEST EFFORT	Ancho de banda fijo mínimo	≤ 1 Mbps > 1 Mbps	20%

- **Selección del algoritmo de enrutamiento QoS,** cuya eficiencia en una red se determinará al medir los siguientes parámetros[39]:

  a. **Probabilidad de bloqueo:** es el cociente del número de las peticiones de conexión rechazadas al número total de peticiones dadas a la red.

  b. **Tiempo de respuesta:** se define como la suma del tiempo de cómputo de la trayectoria y el tiempo necesitado realmente para establecer esta trayectoria sí una existe.

  c. **Longitud promedio de las rutas:** corresponde al número de saltos que forman la ruta seleccionada, esto induce a la eficacia de la utilización de los recursos de la red.

d. **Requerimientos de hardware:** implica los requisitos que deben cumplir los dispositivos para utilizar determinado algoritmo.

e. **Complejidad del algoritmo:** en cuanto a su configuración e implementación.

Para seleccionar el algoritmo de enrutamiento QoS se propone evaluar estos criterios mediante el análisis de la topología de red, en la que se considere los nodos, el número de enlaces y su capacidad. Los criterios mencionados anteriormente están como una función de la carga aplicada a la red dada por:

$$\mathbf{Load = (Lb/C)*(\Lambda/\mu)}$$

Fórmula 4.1: Función de la carga aplicada a la red

Donde:

$\Lambda = \Sigma_s \lambda_s$: tasa de llegada de la petición de conexión de la red acumulativa con **λ_s** representando la petición de conexión de la clase s. Las llegadas de la petición se asumen para ser Poisson.

L: longitud promedio de la ruta seleccionada.

b: ancho de banda promedio para las conexiones solicitadas, en la simulación, se fija b a 1.1 Mbps.

C: capacidad total de la red igual a la suma de todas las capacidades de los enlaces.

1/μ: duración promedio de la conexión.

- **Selección del mecanismo para el control del delay, jitter y pérdida de paquetes,** de acuerdo a las siguientes características de las herramientas para la gestión de colas[17] que se muestran en la Tabla 4.8.

Tabla 4.8: Criterios para comparar los mecanismos para el control del delay, jitter y pérdida de paquetes

Característica	Definición	Parámetro QoS Afectado
Clasificación	Capacidad de examinar los paquetes para determinar en cuál cola el paquete debería ser colocado. Algunas opciones están disponibles.	Ninguno
Política de descarte	Cuándo la cola se ha determinado, la política de descarte define las reglas por las cuales el router elige el paquete a descartar. Algunas opciones son: tail drop, tail drop modificado y WRED.	Loss
Scheduling dentro de una cola	Dentro de una cola, los paquetes son reordenados. En la mayoría de los casos, se utiliza la lógica FIFO.	Ancho de banda Delay Jitter Loss
Scheduling entre diferentes colas	Lógica que define cómo la gestión de colas escoge el siguiente paquete a tomar de la cola de salida y colocarlo en la cola de transmisión.	Ancho de banda Delay Jitter Loss
Número máximo de colas	Número máximo de colas diferentes que el mecanismo soporta, que implica el número máximo de clasificaciones del tráfico que pueden ser tratadas diferencialmente por un mecanismo.	Ninguno
Longitud máxima de la cola	Número máximo de paquetes en una sola cola	Delay Loss

La figura 4.8 ilustra los datos que se requieren al ingreso de esta fase, entre los que se encuentran las clases de servicio, enrutamiento, café amarillo, tomate, turquesa y verde, los algoritmos de enrutamiento QoS, WSPF, SWPF y DORA y los mecanismos para el control de los parámetros QoS, FIFO, PQ, CQ, WFQ, CBWFQ y LLQ, además tenemos como datos de salida el valor de DSCP y/o Precedencia IP asignado a cada clase de servicio, el algoritmo de enrutamiento QoS y el mecanismo QoS seleccionado de acuerdo a los resultados de la comparación entre los criterios planteados en cada caso.

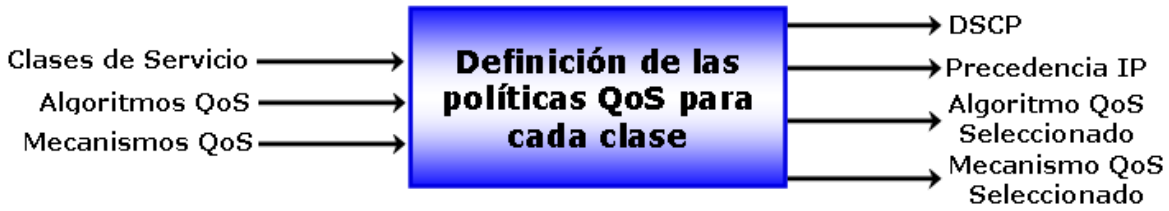


Figura 4.8: Entradas y salidas en la fase 3

Fase 4: Pruebas de las políticas QoS

Una vez que las clases de servicio tienen su respectivo valor de DSCP o Precedencia IP, al cual se asocian las políticas que se aplican para cada clase y que se han seleccionado tanto el algoritmo de enrutamiento QoS como el mecanismo para el control de los parámetros QoS, se debe verificar el funcionamiento e interacción de estos elementos en el laboratorio y posteriormente en un parte de la red con y sin la aplicación de estos parámetros para así determinar si se cumplen los requerimientos de las aplicaciones; además las pruebas deben considerar las distintas tecnologías de acceso como Ethernet,

Frame Relay, ATM, la velocidad del enlace en el cliente y el ISP, etc. En la figura 4.9 se ilustra los datos de entrada a esta fase con sus respectivos datos de salida.

Figura 4.9: Entradas y salidas en la fase 4

Fase 5: Implementación de las políticas

Si los resultados de las pruebas con la aplicación de las políticas, el algoritmo de enrutamiento QoS y el mecanismo para el control del delay, jitter y pérdida de paquetes son apropiados para los requerimientos y el funcionamiento de las aplicaciones se procede con la implementación en las redes del cliente y del ISP. La figura 4.10 muestra los datos de entrada que se constituyen por los valores de DSCP o Precedencia IP con sus respectivas políticas, el algoritmo QoS y el mecanismo QoS seleccionado y en la salida está la política implementada.

Figura 4.10: Entradas y salidas en la fase 5

Las políticas definidas se deben configurar tanto en el router del cliente (CPE) como en el router del ISP, como sigue:

- Marcación y clasificación de los paquetes de voz con el DSCP EF.

- Marcación y clasificación de los paquetes de video con el DSCP AF41.

- Clasificación de los paquetes de aplicaciones mediante listas de acceso, para después colocarlas en una de las clases de servicio definidas en el apartado 4.3.3, fase 2, de acuerdo al diseño realizado para el cliente.

- Marcación de los paquetes de aplicaciones, con el valor DSCP que les corresponde según la tabla 4.3, para que sean posteriormente reconocidos en los nodos sin configuración adicional en éstos.

- Definición de la política y aplicación del mecanismo QoS, tomando en cuenta lo siguiente:

    - La suma de todo el ancho de banda establecido en la política no debe pasar el 75% del ancho de banda total, definido según la tecnología de acceso utilizada.

    - La distribución por clase se realiza de acuerdo a la tabla 4.4.

    - No todos los enlaces tendrán todas las clases, puesto que esto depende de las aplicaciones que utilice el cliente.

- Aplicación de la política.

Se debe considerar las siguientes funciones para controlar la congestión y proporcionar el transporte de QoS:

- **Algoritmo de enrutamiento QoS:** la decisión de enrutamiento puede basarse en el número de saltos y el ancho de banda, se empleará el algoritmo seleccionado en la fase 3.

- **Mecanismo para el control del delay, el jitter y la pérdida de paquetes:** para administrar la congestión y mantener una política de atención en cola que considere las necesidades de todos los flujos; este mecanismo se seleccionó en la fase 3.

Fase 6: Monitoreo y ajuste

En esta fase se realiza el seguimiento de la política implementada para determinar si se están cumpliendo los requerimientos de las aplicaciones y de ser así no se realizarían cambios, caso contrario se tendrían tres casos, que consisten en: cambios en la definición de las políticas, cambios en la definición de las prioridades de las aplicaciones y añadir o eliminar aplicaciones según las necesidades del cliente, para lo cual se debe realizar un ajuste en la fase correspondiente. La tabla 4.11 identifica la entrada a esta fase con las respectivas salidas.

Figura 4.11: Entradas y salidas en la fase 6

La figura 4.12 muestra el funcionamiento global del mecanismo con la aplicación de las CoS's definidas para implementar la calidad de servicio extremo a extremo en la Red IP.

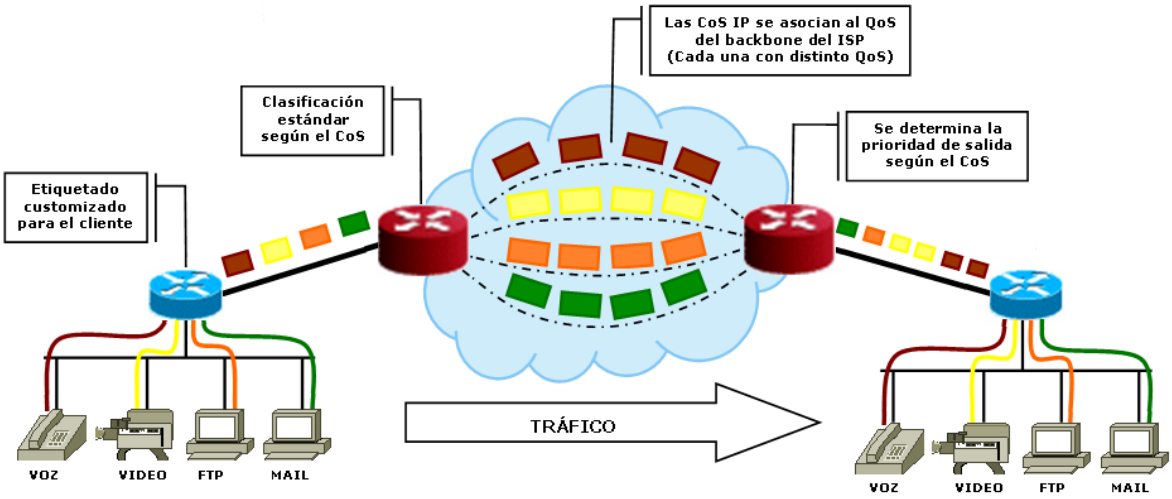


Figura 4.12: Modelo de funcionamiento del mecanismo

Como se puede observar se encuentran especificadas las aplicaciones y en el equipo del cliente, conocido como CPE (Customer premises equipment), se divide y etiqueta el tráfico en clases, que llegan al router del borde de la red para que clasifique y conforme los paquetes; en la nube se los asocie al PHB correspondiente para que así obtengan la calidad de servicio deseada y en el router de salida se determina su prioridad de salida de acuerdo al CoS para así enviarlo al cliente.

Se debe considerar que la configuración de la calidad de servicio debe realizarse en cada salto IP entre el equipo del cliente (CPE) y el equipo del ISP y además que cada equipo que realiza alguna función de priorización o reservación de ancho de banda la aplica en sus interfaces de salida.

4.3.4. Algoritmo de funcionamiento

El algoritmo de funcionamiento del mecanismo propuesto se representará mediante un diagrama de flujo (Figura 4.13), que identifica las diferentes fases y las funciones que se cumplen en cada una.

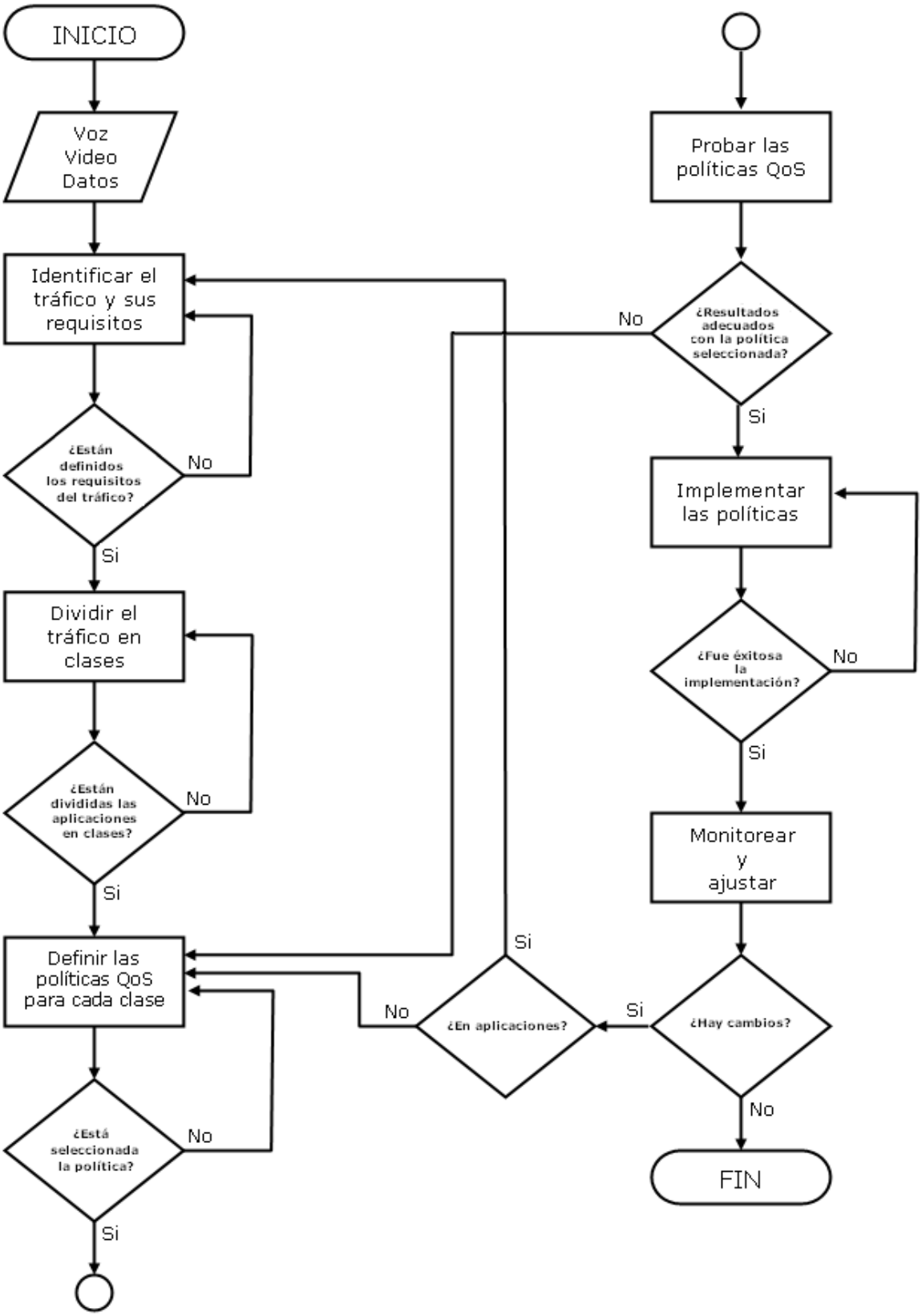


Figura 4.13: Diagrama de flujo del algoritmo

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- En la actualidad existe una clara necesidad hacia la convergencia de voz, video y datos en una sola red, porque las empresas requieren que sus aplicaciones sean transportadas a través de una sola infraestructura tecnológica, pero cumpliendo con los requerimientos que tienen sus aplicaciones.

- La utilización adecuada de las políticas de QoS permite cumplir los requisitos de las aplicaciones para así obtener el funcionamiento deseado.

- Una red IP permite ofrecer servicios diferenciados y acordes a la calidad de servicio demandada por las aplicaciones del cliente, la cual es imprescindible para diferenciar las aplicaciones sensibles a ciertos parámetros como delay, jitter, pérdida de paquetes y el tratamiento en caso de congestión.

- La congestión puede producirse por poco espacio en los buffers, agregación de nuevos puntos y la baja velocidad de los enlaces en la red del ISP.

- La calidad de servicio se analiza desde dos perspectivas; la del usuario, quien puede percibir si sus aplicaciones funcionan adecuadamente y la del administrador de la red, quien debe gestionar la asignación del ancho de banda, controlar el delay, jitter y pérdida de paquetes y otros factores que influyen en el funcionamiento deseado de la aplicación.

- Un modelo de calidad de servicio permite entregar el servicio requerido por un tipo de tráfico específico de un extremo al otro de la red, para así estandarizar las políticas de calidad de servicio en la red, basándose en los parámetros de la misma: ancho de banda, delay, jitter y pérdida de paquetes.

- El delay puede reducirse al incrementar la capacidad del enlace, priorizar los paquetes sensitivos a este parámetro y al comprimir el payload o la cabecera.

- Para prevenir la pérdida de paquetes se puede utilizar mecanismos de gestión de colas y de traffic policing y shaping.

- La implementación de la calidad de servicio en las redes IP permite asignar ancho de banda de forma diferenciada a las aplicaciones, modelar el tráfico de la red, administrar la congestión y las prioridades de acuerdo a las necesidades de los usuarios en cada punto de la red.

- Una red basada en políticas requiere implementar la calidad de servicio en cada parte de la red, considerando tres áreas: las premisas del cliente, las redes WAN del proveedor de servicios y el interworking entre ambos, a través de entidades como el servidor QoS del cliente y de red.

- Se describieron las características, beneficios y desventajas de los modelos QoS extremo a extremo definidos por el IETF, Servicios Integrados – IntServ y Servicios Diferenciados – DiffServ.

- El modelo DiffServ presenta mejores características respecto a IntServ como su baja complejidad, diferenciación entre las funciones en el borde y el núcleo de la red, fácil administración y mantenimiento, además de su escalabilidad, flexibilidad, reducción de la carga en los dispositivos de la red, gestión eficiente de los recursos de red, lo que lo convierte en un modelo apropiado para grandes redes.

- El mecanismo propuesto satisface los requerimientos de calidad de servicio de las empresas y permite su implementación en cualquier red a través de la definición de seis fases que corresponden a la identificación de las aplicaciones y sus requisitos, la definición de las clases de servicio, la definición de políticas, las pruebas, la implementación y el monitoreo y ajuste de las políticas.

- Se definen seis clases de servicio que se ajustan a las necesidades de los usuarios y permiten establecer claramente las prioridades entre éstas, a

través de la agrupación por los siguientes colores: café para voz, amarillo para video, tomate para las aplicaciones decisivas, turquesa para las aplicaciones preferenciales del cliente y verde para el resto de aplicaciones, para así asociarlas a un DSCP que contiene la definición del tratamiento que recibirán en la red.

- Para garantizar la calidad de servicio en cada punto de la red se deben definir y aplicar políticas que consideren la definición del tratamiento que recibirá cada clase de servicio, la selección del algoritmo de enrutamiento y del mecanismo apropiado para controlar los parámetros QoS.

- El algoritmo de enrutamiento QoS se selecciona de acuerdo a su eficiencia en una red al medir los siguientes parámetros: probabilidad de bloqueo, tiempo de respuesta, longitud promedio de la ruta, requerimientos de hardware y complejidad del algoritmo.

- El mecanismo para el control de los parámetros QoS depende directamente de las características de las herramientas para la gestión de colas: clasificación, política de descarte, scheduling en la cola y entre colas, número máximo de colas y longitud máxima de la cola.

- El algoritmo representado mediante un diagrama de flujo identifica el proceso a seguir para emplear dicho mecanismo, las funciones realizadas en cada fase y la interacción entre las mismas.

5.2. RECOMENDACIONES

- En base al estudio realizado se recomienda realizar las pruebas de las políticas definidas para de esta forma determinar los resultados con y sin la aplicación de las mismas y así establecer la efectividad de las políticas definidas en el mecanismo.

- Se debería realizar pruebas considerando distintos tipos de aplicaciones y velocidades para así establecer el impacto e influencia de la capacidad del enlace en la aplicación de las políticas.

- Es necesario verificar el funcionamiento de las políticas en caso de congestión, caída o escasez de recursos en alguna trayectoria.

- Considerar diferentes tecnologías de acceso como Ethernet, Frame Relay, ATM, etc. para determinar los parámetros a configurar en los dispositivos.

- Realizar pruebas considerando la influencia que tiene en determinadas aplicaciones, el algoritmo de enrutamiento y el mecanismo para el control de los parámetros QoS seleccionado.

- Se debe evaluar los dispositivos que actualmente existen en el mercado para verificar qué opciones incluyen para calidad de servicio y si permiten la configuración e implementación de las políticas planteadas.

- Los administradores de la red de las empresas como los proveedores de servicios de Internet deben implementar políticas de calidad de servicio en sus redes para de esta forma garantizar que se cumplan con los requerimientos de calidad de las aplicaciones.

- Se recomienda continuar con este trabajo de investigación mediante la implementación de las políticas definidas.

BIBLIOGRAFÍA

[1] GOMEZ, Mariano. Presentación de redes y protocolos de comunicaciones. 2005.

[2] GONZÁLEZ, Jonathan. Teoría de redes informáticas.1998.

[3] Apuntes de redes,
http://www.monografias.com/trabajos12/redes/redes.shtml

[4] Redes de difusión,
http://www.cft.gob.mx/cofetel/html/la_era/info_tel/it26.shtml

[5] Redes,
http://www.elet.itchihuahua.edu.mx/academia/cmonarre/red-co/trab1/trab1.htm

[6] Clasificación de las redes,
http://www.forest.ula.ve/~mana/cursos/redes/clasifica.html

[7] Protocolo de Enrutamiento o Protocolo de Internet (IP)**,**
http://www.solont.com/z-net/tcp-04/tcp_04.htm

[8] RFC 791. Internet Protocol, Protocol Especification. Septiembre 1981.

[9] RFC 1349. Type of Service in the Internet Protocol Suite. Julio 1992.

[10] Tutorial y descripción técnica de TCP/IP,
http://ditec.um.es/laso/docs/tut-tcpip/3376fm.html

[11] RFC 2460. Internet Protocol, Version 6 (IPv6) Specification. Diciembre 1998.

[12] PEÑA, Jesús; LOPEZ DA SILVA, Rafael y ARANDA, Pedro. Redes IP de Nueva generación. 2002.

[13] White paper: Las redes IP: Conceptos básicos,
http://www.axis.com/es/documentacion/Las%20redes%20IP.pdf

[14] Internetworking Technologies Handbook. Quality of Service Networking. Capítulo 49. Cisco. 2003.

[15] Diffserv como solución a la provisión de QoS en Internet,
http://www.it.uc3m.es/cgarcia/articulos/cita2002_diffserv.pdf

[16] Configuración de qos,
http://docs.us.dell.com/support/edocs/network/pc5324/sp/ug/qos.htm

[17] ODOM, Wendell y CAVANAUGH Michael. IP Telephony Self-Study - Cisco DQOS - Exam Certification Guide. Cisco Press. 2004

[18] Calidad de servicio en redes IP -1210. 2000.

[19] JACOBS, Eric. Presentación Seminario de calidad de Servicio en Redes Multimedia. Vanguard Manager Solutions.

[20] RABADÁN, Jorge. Presentación Calidad de Servicio en Redes IP. 2003.

[21] Cisco, Catalyst 2950 and Catalyst 2955 Switch Software Configuration Guide. Configuring QoS. Capítulo 28, http://www.cisco.com/en/US/products/hw/switches/ps628/products_configuration_guide_chapter09186a00801a6ba6.html

[22] QoS en ATM, http://www.idg.es/comunicaciones/articulo.asp?id=60995

[23] GAZO, Alfonso y GONZÁLEZ José Luis. Una arquitectura multiprotocolo para la implantación incremental de un modelo de servicio con garantías QoS sobre redes IP. 2003.

[24] Cisco IOS Quality of Service Solutions Configuration Guide. Quality of Service Overview. 2003.

[25] RFC 1633. Integrated Services in the Internet Architecture: an Overview. Junio 1994.

[26] Modelo IntServ / Protocolo RSVP, http://www.labredes.unb.br/material/APRC_OSDI/RSVP.pdf

[27] RFC 2212. Specification of Guaranteed Quality of Service. Septiembre 1997.

[28] RFC 2211. Specification of the Controlled-Load Network Element Service. Septiembre 1997.

[29] RFC 2205. Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification RSVP. Septiembre 1997.

[30] MORENO, Manuel. Señalización para QoS en redes IP. Revista de Telecomunicacones Nª 90. 2002.

[31] RFC 2475. An Architecture for Differentiated Services. Diciembre 1998.

[32] RFC 2474. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers. Septiembre 1998.

[33] RFC 3246. An Expedited Forwarding PHB (Per-Hop Behavior), Marzo 2002 (Reemplaza al Obsoleto RFC 2598. Julio 1999).

[34] RFC 2597. Assured Forwarding PHB Group. Julio 1999.

[35] RFC 2638. A Two-bit Differentiated Services Architecture for the Internet. Julio 1999.

[36] FELICI, Santiago. Presentación Servicios Diferenciados y MPLS. 2005.

[37] White Paper: DIFFSERV — THE SCALABLE END – TO - END QUALITY OF SERVICE MODEL. Cisco. 2005, http://www.cisco.com/application/pdf/en/us/guest/tech/tk766/c1550/ccmigration_09186a00800a3e2f.pdf

[38] FINEBERG, V. A practical architecture for implementing end-to-end QoS in an IP network. Communications Magazine, IEEE. Volumen 40. 2002. pág(s):122 – 130.

[39] MAALAOUI, K.; BELGHITH, A.; BONNIN, J.-M.; TEZEGHDANTI, M. Performance evaluation of QoS routing algorithms. Computer Systems and Applications, 2005. AS/IEEE Third International Conference. Pág.(s): 66.

[40] ALVAREZ, Santiago. Optimizing the Service Provider Network for Voice, Video, and Data. Internet Technologies Division. Cisco 2005.

[41] Cisco IOS Quality of Service Update. Cisco Internet Technologies Division. 2005.

[42] Clasificación de las redes, http://www.geocities.com/TimesSquare/Chasm/7990/clasific.htm

[43] Redes, http://www.monografias.com/trabajos5/redwan/redwan.shtml

[44] Tipos de conmutación, http://iio.ens.uabc.mx/~jmilanez/escolar/redes/01090000.html

[45] ESCALONA, Maritza. Redes IP: revolución. Revista El Mundo. 2001. http://www.elmundo.com.ve/ediciones/2001/03/27/p1-6s3.htm

[46] Protocolo IP, http://www.monografias.com/trabajos7/protoip/protoip.shtml

[47] Nueva generación IPv6, http://www.rediris.es/rediris/boletin/33/enfoque3.html

[48] Resumen de los mecanismos de QoS y cómo interoperan, http://www.microsoft.com/latam/technet/articulos/windows2k/qosmech/

[49] Voz sobre IP, http://www.ub.edu.ar/investigaciones/tesinas/33_crocco.PDF

[50] Calidad de Servicio (QoS), http://www.disca.upv.es/jvila/sdc05/sdc05-qos.pdf

[51] HERNÁNDEZ, Enrique, Transmisión de datos en Tiempo Real, http://www.disca.upv.es/enheror/pdf/Doctorado2Creditos.PDF

[52] IntServ, http://jpadilla.docentes.upbbga.edu.co/QoS/IntServ2%20Modelos%20de%20Servicio.pdf

[53] PADILLA Jhon, Arquitectura de servicios integrados (Intserv). 2004.

[54] Revisión y Clasificación de Protocolos para Redes de Tecnología ATM, http://www.rediris.es/rediris/boletin/46-47/ponencia10.html

[55] Redes Inalámbricas. Estándares y mecanismos de seguridad, http://www.enterate.unam.mx/Articulos/2004/agosto/redes.htm

[56] ELIZONDO, Antonio y GARCÍA, María Luisa. Calidad de servicio en redes de servicios diferenciados. Comunicaciones de Telefónica I+D. Número 24. 2002.

[57] DELFINO, Adrián y RIVERO, Sebastián. Diffserv: Servicios Diferenciados. Monografía de Evaluación de Performance en Redes de Telecomunicaciones. 2004, http://iie.fing.edu.uy/ense/asign/perfredes/trabajos/trabajos_2003/diffserv/Trabajo%20Final.pdf

[58] RFC 3086. Definition of Differentiated Services Per Domain Behaviors and Rules for their Specification. Abril 2001.

[59] Wille, E.C.G.; GARETTO, M.; MELLIA, M.; LEONARDI, E.; MARSAN, M.A. Considering end-to-end QoS in IP network design Telecommunications Network Strategy and Planning Symposium. Networks 2004. pág(s):69 – 74.

[60] Deploying quality of service for converged networks. Cisco Networkers 2004.

ANEXOS