PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA ESCUELA DE SISTEMAS

TRABAJO DE TITULACIÓN DE GRADO PREVIA LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN SISTEMAS Y COMPUTACION

PROPUESTA DE IMPLEMENTACIÓN DE CALIDAD DE SERVICIO (QoS) EN REDES LOCALES VIRTUALES (VLAN) MEDIANTE LAS NORMAS 802.1D Y 802.1Q. APLICADO A LA EMPRESA SINERGY HARD

DIEGO FERNANDO RUANO CHINGUERCELA

DIRECTOR: SUYANA ARCOS

QUITO – 2016

DEDICATORIA

A mis padres,

Mi hermana,

Mis amigos y

A la persona que me acompaño en toda mi carrera,

porque me brindaron todo el apoyo,

la motivación y su colaboración incondicional.

AGRADECIMENTO

A mis queridos profesores por sus sabios conocimientos y consejos que me han formado en la parte académica, técnica, profesional y sobre todo en la personal.

Mi eterna gratitud a la facultad de Ingeniería, por ser forjadora de profesional de gran calidad.

A la Ing. Suyana Arcos, Ing. Andrés Jiménez y el Ing. Damian Nicolalde que supieron guiarme con entusiasmo, motivación, solvencia y aportaron con su colaboración desinteresada en el desarrollo del proyecto.

A la empresa Sinergy Hard Ltda.., y en especial al Ing. Gencys Segarra, que supieron brindarme la información y el apoyo incondicional en todo momento.

Para mis amigos por cada semestre compartido, cada momento disfrutado siempre tendrán un lugar especial entre mis recuerdos.

Para mis padres y mi hermana porque con su sacrificio y esfuerzo supieron brindarme la oportunidad de estudiar y con su apoyo lograr culminar mi carrera.

Y, a Dios por ser mi fuente de guía de inspiración, sabiduría y sacrificio.

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. CAPÍTULO

FUNDAMENTACIÓN TEÓRICA

1.1. REDES LOCALES VIRTUALES[1]

"Una VLAN (Red de área local virtual o LAN virtual) es una red de área local que agrupa un conjunto de equipos de manera lógica y no física. Efectivamente, la comunicación entre los diferentes equipos en una red de área local está regida por la arquitectura física. Gracias a las redes virtuales (VLAN), es posible liberarse de las limitaciones de la arquitectura física (limitaciones geográficas, limitaciones de dirección, etc.), ya que se define una segmentación lógica basada en el agrupamiento

[1] (CCM, 2016)

de equipos según determinados criterios (direcciones MAC, números de puertos, protocolo, etc.).”[23]

1.1.1. Definición de una VLAN[4]

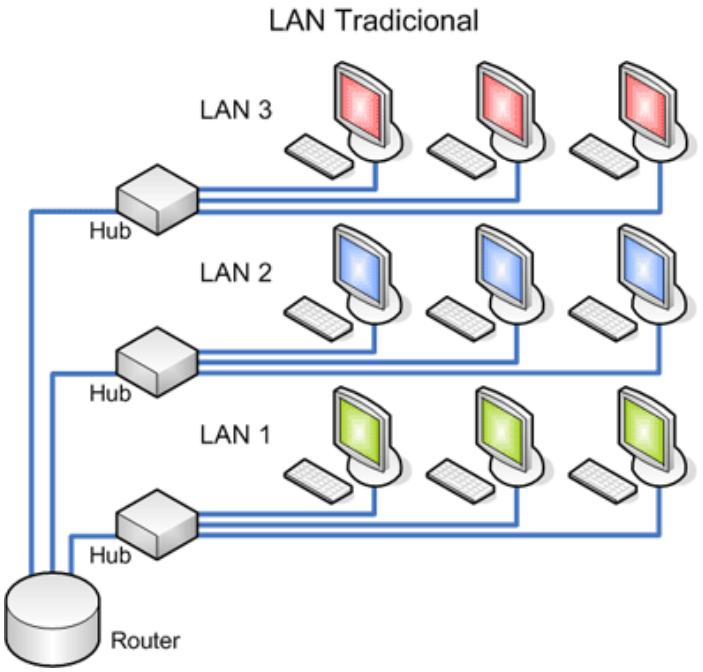
Para pode definir una VLAN es necesario poder entender como trabajaba una LAN y porque surgió la necesidad de crear las VLAN , por esta razón entendemos que “una red de área local (LAN) está definida como una red de computadoras dentro de una misma área geográfica como puede ser una empresa o una corporación. Trabajando de esta manera se pudo concluir que la confidencialidad entre los usuarios de la red no era segura y se aprovechaba la capacidad del ancho de banda que existía dentro la corporación o empresa.

Así es como surge una VLAN ya que se encuentra conformada por un conjunto de dispositivos de red interconectados (hubs, bridges, switches o estaciones de trabajo) la definimos como como una subred definida por software y es considerada como un dominio de Broadcast que pueden estar en el mismo medio físico o bien puede estar sus integrantes ubicados en distintos sectores de la corporación (Figura 1).

La tecnología de las VLANs se basa en el empleo de Switches, en lugar de hubs, de tal manera que esto permite un control más

[2] (CCM, 2016)
[3] (Group, 2015)
[4] (TextosCientificos.com, 2006)

inteligente del tráfico de la red, ya que este dispositivo trabaja a nivel de la capa 2 del modelo OSI y es capaz de aislar el tráfico, para que de esta manera la eficiencia de la red entera se incremente. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra el incremento del ancho de banda en dicho grupo de usuarios."[56]



[5] (TextosCientificos.com, 2006)
[6] (TextosCientificos.com, 2006)

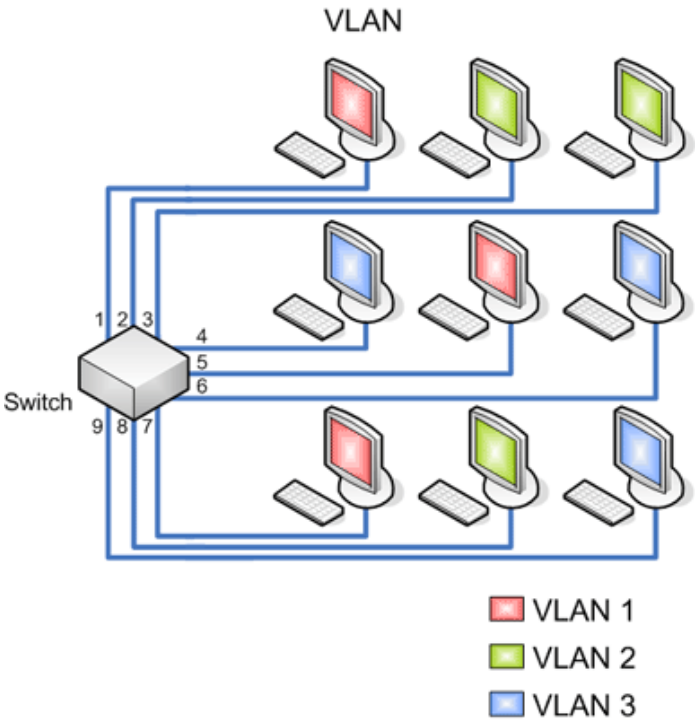


Figura 1.1.1.1

Fuente: (TextosCientificos.com, 2006)

"Por la razón de que hay varias formas en que se puede definir una VLAN, se dividen éstas en cuatro tipos principales:

- Basadas en puertos.
- Basadas en MAC.
- VLANs de capa 3.
- Basada en reglas (policy based)."[7]

1.1.2. Características

Cuando hablábamos de una arquitectura dentro de una organización, "los grupos de trabajo en red eran creados por la asociación física de

[7] (Icc, 2005)

los usuarios en un mismo segmento de la red, o en un mismo concentrador"[8] o Switch. El problema principal al trabajar de esta forma tradicional era que todos los usuarios del grupo compartían el ancho de banda disponible y los dominios del broadcast, además la limitación geográfica de cada uno de los usuarios era otra consecuencia de crear grupos de trabajo de esta forma.

"Para solventar dicha situación se crea el concepto de Redes de Área Local Virtuales (VLANs), configuradas dentro de los switches, que dividen en diferentes "dominios de broadcast" a un switch, con la finalidad de no afectar a todos los puertos del switch dentro de un solo dominio de broadcast, sino crear dominios más pequeños y aislar los efectos que pudieran tener los mensajes de broadcast a solamente algunos puertos, y afectar a la menor cantidad de máquinas posibles.

Las redes virtuales permiten que la ubicación geográfica no se limite a diferentes concentradores o plantas de un mismo edificio, sino a diferentes oficinas intercomunicadas mediante redes VLAN, nuestros compañeros de área, dirección, sistemas, administrativos, etc., estarán conectados dentro de la misma VLAN, y quienes se encuentren en otro edificio, podrán "vernos" como una Red de Área Local independiente a las demás."[9] [10]

1.1.3. Subredes y VLAN's[11]

[8] (Puchele, 2011)
[9] (Ecotec, Diseño e Implementacion de VLANS, 2012)
[10] (Azuay, 2013)
[11] (ConsultasCCNA, ConsultasCCNA, 2012)

“Una VLAN es también una subred, ya que si no sale de la subred mediante un router, toda la información de broadcast se queda en ella. Cada subred necesita un direccionamiento IP y una dirección de subred. Para transmitir los datos de una subred a otra se necesita un router.

Existen 3 subredes separadas con un direccionamiento diferente y que nos e alcanzan entre ellas mediante broadcast. Para enviar información de una subred a otra, deben transmitir a su gateway por defecto, o sea, el interface que los une, o sea, el router. Una diferencia entre los bridges y los switches es que los bridges necesitan un puerto independiente del router para cada subred, mientras que un switch se basta con un puerto del router, ya que usa las sub interfaces de un mismo puerto de un router.

Cisco recomienda una cantidad de dispositivos límite para las subredes.[12]

Protocolo	Numero de Dispositivos
IP	500
IPX	300
NetBIOS	200
AppleTalk	200
Mixed Protocols	200

1.1.4. Escalabilidad de una VLAN

[12] (ConsultasCCNA, ConsultasCCNA, 2012)

Cuando utilizamos VLAN's el sistema se vuelva más escalable ya que las VLAN's proveen más flexibilidad a la hora de conectarse a la red. No estamos limitados a una conexión en un único punto, sino que podemos conectarnos a la misma red desde varias posiciones. Esto hace que se deban de tener unas políticas de seguridad más estrictas.

La única limitación respecto esta libertad de movimiento de un usuario respecto su posición física es que siempre estará conectado a la misma subred y que para salir del nivel 3 deberá de pasar a través de un router.

Aquí vemos las limitaciones de cada switch."[13][14]

Modelo de Switch	Versión de Software	Número de VLAN
1900	Enterprise IOS	64
2950 s	IOS Estándar Image (SI)	64
2950	IOS Enhaced Image (EI)	250

gnación a una VLAN dinámicamente o estáticamente[15]

Cada dispositivo de una VLAN puede ser determinado de dos maneras.

- Estáticas
- Dinámicas

Estos dos métodos definen como un puerto de un switch que se asocia a una VLAN en concreto. Puedes designar este puerto manualmente o dinámicamente.[16]

[13] (ConsultasCCNA, ConsultasCCNA, 2012)
[14] (ConsultasCCNA, ConsultasCCNA, 2012)
[15] (ConsultasCCNA, ConsultasCCNA, 2012)

"Las VLAN estáticas también se denominan VLAN basadas en el puerto. Las asignaciones en una VLAN estática se crean mediante la asignación de los puertos de un switch o conmutador a dicha VLAN. Cuando un dispositivo entra en la red, automáticamente asume su pertenencia a la VLAN a la que ha sido asignado el puerto. Si el usuario cambia de puerto de entrada y necesita acceder a la misma VLAN, el administrador de la red debe cambiar manualmente la asignación a la VLAN del nuevo puerto de conexión en el switch.

En las VLAN dinámicas, la asignación se realiza mediante paquetes de software tales como el CiscoWorks 2000. Con el VMPS (acrónimo en inglés de VLAN Management Policy Server o Servidor de Gestión de Directivas de la VLAN), el administrador de la red puede asignar los puertos que pertenecen a una VLAN de manera automática basándose en información tal como la dirección MAC del dispositivo que se conecta al puerto o el nombre de usuario utilizado para acceder al dispositivo. En este procedimiento, el dispositivo que accede a la red, hace una consulta a la base de datos de miembros de la VLAN. Se puede consultar el software FreeNAC para ver un ejemplo de implementación de un servidor VMPS."[16][17][18]

1.1.6. VLAN basada en puertos[19]

[16] (ConsultasCCNA, ConsultasCCNA, 2012)
[17] (VLAN, 2012)
[18] (Charris, 2012)
[19] (Icc, 2005)

"Según este esquema, la VLAN consiste en una agrupación de puertos físicos que puede tener lugar sobre un conmutador o también, en algunos casos, sobre varios conmutadores. La asignación de los equipos a la VLAN se hace en base a los puertos que están conectados físicamente.

Muchas de las primeras implementaciones de las VLANs definían la pertenencia a la red virtual por grupos de puertos (por ejemplo, los puertos 1, 2, 3, 7 y 8 sobre un conmutador forman la VLAN A, mientras que los puertos 4, 5 y 6 forman la VLAN B). Además, en la mayoría, las VLANs podían ser construidas sobre un único conmutador.

La segunda generación de implementaciones de VLANs basadas en puertos contempla la aparición de múltiples conmutadores (por ejemplo, los puertos 1 y 2 del conmutador 1 y los puertos 4, 5, 6 y 7 del conmutador 2 forman la VLAN A; mientras que los puertos 3, 4, 5, 6, 7 y 8 del conmutador 1 combinados con los puertos 1, 2, 3 y 8 del conmutador 2 configuran la VLAN B)"[20]. Como se muestra en la figura 2

[20] (Icc, 2005)

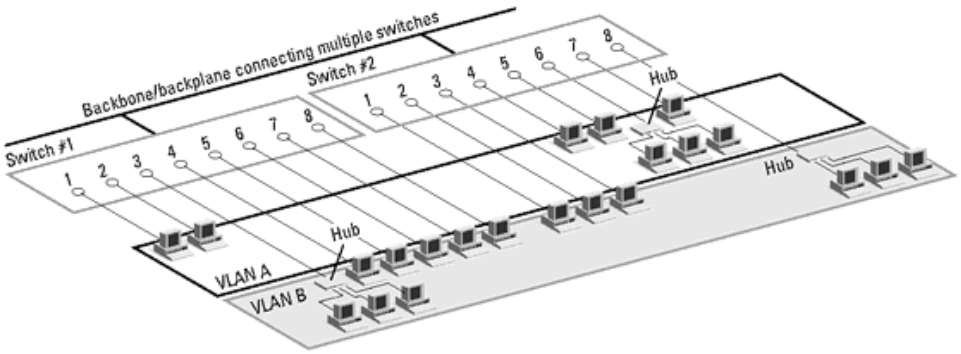


Figura 1.1.6.1

Fuente: (Icc, 2005)

Este tipo de estructura es el más fácil ya que un grupo de puertos forman una VLAN, la asignación de los equipos a la VLAN se hace en base a los puertos que están conectados físicamente. En las primeras implementaciones de las VLAN´s basadas en puertos fueron construidas sobre un solo conmutador, es decir que la pertenencia a una VLAN A era por la agrupación de algunos puertos del conmutador. [21]

1.1.7. VLAN basada en MAC[22]

"Constituye la segunda etapa de la estrategia de aproximación a la VLAN, y trata de superar las limitaciones las VLANs basadas en puertos. Operan agrupando estaciones finales en una VLAN en base a sus direcciones MAC. Este tipo de implementación tiene varias ventajas y desventajas.

(Icc, 2005) [21]
[22] (Icc, 2005)

Desde que las direcciones MAC (media access control - control de acceso al medio) se encuentran implementadas directamente sobre la tarjeta de interface de la red (NIC - network interface card), las VLANs basadas en direcciones MAC permiten a los administradores de la red el mover una estación de trabajo a una localización física distinta en la red y mantener su pertenencia a la VLAN. De este modo, las VLANs basadas en MAC pueden ser vistas como una VLAN orientada al usuario.

Entre los inconvenientes de las VLANs basadas en MAC está el requerimiento de que todos los usuarios deben inicialmente estar configurados para poder estar en al menos una VLAN. Después de esa configuración manual inicial, el movimiento automático de usuarios es posible, dependiendo de la solución específica que el distribuidor haya dado. Sin embargo, la desventaja de tener que configurar inicialmente la red llega a ser clara en redes grandes, donde miles de usuarios deben ser asignados explícitamente a una VLAN particular. Algunos distribuidores han optado por realizar esta configuración inicial usando herramientas que crean VLANs basadas en el actual estado de la red, esto es, una VLAN basada en MAC es creada para cada subred.

Las VLANs basadas en MAC que son implementadas en entornos de medios compartidos se degradarán seriamente como miembros de diferentes VLANs coexistiendo en un mismo conmutador. Además, el principal método de compartición de información entre miembros de

una VLAN mediante conmutadores en una red virtual basada en MAC también se degrada cuando se trata de una implementación a gran escala.[23]

1.1.8. VLAN basadas en reglas

Este esquema es el más potente y flexible, ya que permite crear VLANs adaptadas a necesidades específicas de los gestores de red utilizando una combinación de reglas. Estas reglas pueden ser, por ejemplo, de acceso, con objeto de alcanzar unos ciertos niveles de seguridad en la red. Una vez que el conjunto de reglas que constituyen la política a aplicar a la VLAN se implementa, sigue actuando sobre los usuarios al margen de sus posibles movimientos por la red."[24][25]

1.1.9. Tecnología

Existen algunas opciones que se pueden considerar como aproximaciones que pueden implementarse para para proporcionar redes virtuales:

- Conmutación de puertos
- Conmutación de segmentos con funciones de bridging
- Conmutación de segmentos con funciones de bridging/routing

Estas tres soluciones están basadas en arquitecturas de red que emplean conmutadores, aunque las tres soluciones son capaces de

[23] (Icc, 2005)
[24] (Icc, 2005)
[25] (Icc, 2005)

proporcionar redes virtuales, solo la última, con funciones de bridge/router, proporciona todas las ventajas de una VLAN.[26]

1.1.9.1. Conmutadores de Puertos[27]

"Los conmutadores de puertos son concentradores con varios segmentos, cada uno de los cuales proporciona el máximo ancho de banda disponible, según el tipo de red, compartido entre todos los puertos existentes en dicho segmento. Se diferencian de los conmutadores tradicionales en que sus puertos pueden asociarse dinámicamente a cualquiera de los segmentos, mediante comandos software. Cada segmento se asocia a un backplane (medio físico de gran velocidad que enlaza todos los puertos de los switch's), el cual equivale a su vez a un grupo de trabajo. De este modo, las estaciones conectadas a estos puertos pueden asignarse y reasignarse a diferentes grupos de trabajo o redes virtuales.

Se pueden definir los conmutadores de puertos como software patch panels, y su ventaja fundamental es la facilidad para la reconfiguración de los grupos de trabajo. Tienen, sin embargo, graves limitaciones; dado que están diseñados como dispositivos que comparten un backplane físico, las reconfiguraciones de grupo de trabajo están limitadas al

[26] (Redes Virtuales, 2011)
[27] (VLAN, 2012)

entorno de un único concentrador y por tanto, todos los miembros del grupo deben de estar físicamente próximos.

Las redes virtuales con conmutadores de puertos adolecen de conectividad con el resto de la red. Al segmentar sus propios backplanes no proporcionan conectividad integrada entre los mismos, y por tanto están separados de la comunicación con el resto de la red.

Requieren para ello un bridge/router externo. Ello implica mayores costes, además de la necesidad de reconfigurar el bridge/router cuando se producen cambios en la red. Por último, los conmutadores de puertos no alivian el problema de saturación del ancho de banda de la red. Todos los nodos deben de conectarse al mismo segmento o backplane, por tanto compartirán el ancho de banda disponible en el mismo, independientemente de su número.[28]

1.1.9.2. Conmutadores de segmentos con bridging

A diferencia de los conmutadores de puertos, suministran el ancho de banda de múltiples segmentos de red, manteniendo la conectividad entre dichos segmentos. Se emplean para ello los algoritmos tradicionales de los puentes (bridges), o subconjuntos de los mismos para proporcionar conectividad entre varios segmentos a la velocidad máxima que permite la topología y protocolos de dicha red.

[28] (Redes Virtuales, 2011)

Mediante estos dispositivos, las VLAN no son grupos de trabajo conectados a un solo segmento o backplane Sino grupos lógicos de nodos que pueden conectarse a cualquier número de segmentos de red físicos. Estas VLAN son dominios de broadcast lógicos: conjuntos de segmentos de red que reciben todos los paquetes enviados por cualquier nodo en la VLAN como si todos los nodos estuvieran conectados físicamente al mismo segmento.

Al igual que los conmutadores de puertos, se puede reconfigurar y modificar la estructura de la VLAN mediante comandos software, con la ventaja añadida de ancho de banda repartido entre varios segmentos físicos. De esta forma, según va creciendo un grupo de trabajo, y para evitar su saturación, los usuarios del mismo pueden situarse en diferentes segmentos físicos, aun manteniendo el concepto de grupo de trabajo independiente del resto de la red, con lo que se logra ampliar el ancho de banda en función del número de segmentos usados.

Aun así, comparten el mismo problema con los conmutadores de puertos en cuando a su comunicación fuera del grupo. Al estar aislados, para su comunicación con el resto de la red necesitan encaminadores, con las consecuencias que ya se han

mencionado en el caso anterior, relativas al coste y la reconfiguración de la red.[29]

1.1.9.3. Conmutadores de segmentos con bridging/routing

Es la solución evidente de las dos soluciones anteriores. Dispositivos que comparten todas las ventajas de los conmutadores de segmentos con funciones de bridging, pero además con funciones añadidas de encaminamiento (routing), lo que les proporciona fácil reconfiguración de la red, así como la posibilidad de crear grupos de trabajo que se expanden a través de diferentes segmentos de la red. Además, sus funciones de encaminamiento facilitan la conectividad entre las redes virtuales y el resto de los segmentos o redes, tanto locales como remotas.

Mediante las redes virtuales se puede crear un nuevo grupo de trabajo, con tan solo una reconfiguración del software del conmutador. Ello evita el recableado de la red o el cambio en direcciones de subredes, permitiendo así asignar el ancho de banda requerido por el nuevo grupo de trabajo, sin afectar a las aplicaciones de red existentes.

En las VLAN con funciones de encaminamiento, la comunicación con el resto de la red se puede realizar de dos modos distintos: permitiendo que algunos segmentos sean miembros de varios grupos de trabajo, o mediante las

[29] (Redes Virtuales, 2011)

funciones de encaminamiento multiprotocolo, que facilitan el tráfico incluso entre varias VLAN."[30][31]

1.1.10. Introducción del caso de estudio con las VLAN´s

"Durante todo el proceso de configuración y funcionamiento de una VLAN es necesaria la participación de una serie de protocolos entre los que destacan el IEEE 802.1Q, STP y VTP (cuyo equivalente IEEE es GVRP). El protocolo IEEE 802.1Q se encarga del etiquetado de las tramas que es asociada inmediatamente con la información de la VLAN. El cometido principal de Spanning Tree Protocol (STP) es evitar la aparición de bucles lógicos para que haya un sólo camino entre dos nodos. VTP (VLAN Trunking Protocol) es un protocolo propietario de Cisco que permite una gestión centralizada de todas las VLAN." [32]

1.1.11. Normas de VLAN´s

Con el avance notorio de la tecnología en el campo de las VLAN´S se presenta necesidad de estandarizar mediantes normas las VLAN.

En base a esto se originaron las siguientes normas:

- 802.10 " VLAN normal", en 1995 la CISCO Sistemas propuso el uso de IEEE 802.10 que se estableció originalmente en LAN

[30] (VLAN, 2012)
[31] (Redes Virtuales, 2011)
[32] (Wikipedia, 2015)

que serviría de garantía para las VLANs. CISCO intentó tomar a la 802.10 con un título optativo de Marco de Estructura y rehusó a llevar a VLAN a la idea de etiqueta en lugar de garantizar la información.

- 802.1 "Internet Working Subcomitte", en marzo de 1996, el IEEE completó la fase inicial de investigación para el desarrollo de una VLAN normal y paso resoluciones de tres emisiones:
    - El acercamiento arquitectónico a VLAN
    - Dirección futura de regularización de VLAN
    - Regularizó el formato de marco de etiqueta.

La IEEE 802,10 incorpora técnicas de la autentificación y del cifrado para asegurar secreto e integridad de los datos a través de la red. El protocolo 802,10 permite a tráfico del LAN llevar un identificador de VLAN, así permitiendo la conmutación selectiva de paquetes.

“El switch detectará la identificación de VLAN y remitirá el paquete solamente a las estaciones finales que contienen la misma identificación. Existe una sola unidad de datos de protocolo conocida como intercambio de datos seguro (SDE). Es un marco de la capa del MAC con la cabecera insertada entre la cabecera del MAC y los datos del marco según lo mostrado abajo.

Cabecera MAC	Limpiar la Cabecera			Protegida la Cabecera	Datos	ICV
	←			Pueden ser encriptadas		→
Cabecera MAC	802.10 LSAP	SAID	MDF	Estación Fuente de Direcciones	Datos	ICV

La cabecera clara incluye un identificador de la asociación de la seguridad (DICHO) y un campo definido gerencia opcional (MDF), que pueden llevar la información para facilitar el proceso de la PDU (Protocol Data Unit). La cabecera protegida repliega el direccionamiento de la fuente contenido en la cabecera del MAC para validar la dirección. Así evitando que otra estación sea identificada como la fuente verdadera.

Las salvaguardias del valor del cheque de la integridad (ICV) contra la modificación interna desautorizada de los datos usando un algoritmo de la seguridad. El cifrado para la cabecera 802,10 es opcional. Los gastos indirectos en la cabecera se pueden reducir al mínimo solamente incluyendo las funciones básicas, es decir, el designador de SDE y la identificación real de VLAN.

Cuando una colección arbitraria de subnets de LAN se configura como VLAN, los paquetes nativos que originan las estaciones asociadas a estas LANs adquieren una cabecera 802,10 que contenga la identificación apropiada de VLAN mientras que los paquetes se remiten sobre el backbone.

La propagación de tales paquetes es controlada y contenida solamente por otras LANs dentro de la misma topología virtual. Esto es logrado por los otros dispositivos del establecimiento de una red en el backbone, que realizan un emparejamiento de la identificación de VLAN."[33] [34]

1.1.12. Beneficio de implementar una VLAN

Entre las ventajas de esta topología virtual están las siguientes:

- Reducción de costos de cambios y movimientos de los usuarios.
- Grupos de trabajo virtuales.
- Reducción del enrutamiento

1.1.12.1. Reducción de costos de cambios y movimientos de los usuarios

"La principal excusa para implementar una VLAN es la reducción en el coste de los cambios y movimientos de usuarios. Desde que estos costes son bastante sustanciales, este argumento es suficientemente obligatorio para la implementación de una VLAN.

Muchos fabricantes están prometiendo que la implementación de una VLAN resultará más conveniente a la hora de habilitar la administración de redes dinámicas, y que esto supondrá bastante ahorro. Esta promesa se puede aplicar con buenos

[33] (VLAN, 2012)
[34] (Redes Virtuales, 2011)

resultados a redes IP, ya que, normalmente, cuando un usuario se mueve a una diferente subred, las direcciones IP han de ser actualizadas manualmente en la estación de trabajo.

Este proceso consume gran cantidad de tiempo que podría ser aprovechado para otras tareas, tales como producir nuevos servicios de red. Una VLAN elimina ese hecho, porque los miembros de una red virtual no están atados a una localización física en la red, permitiendo que las estaciones cambiadas de sitio conserven su dirección IP original. Sin embargo, cualquier implementación de VLAN no reduce este coste. Una VLAN añade una nueva capa de conexión virtual que ha de ser administrada al mismo tiempo que la conexión física. Esto no quiere decir que no se puedan reducir los costes hablados anteriormente. Sólo que no hay que precipitarse a la hora de implementar una VLAN y es mejor estar bien seguro de que la solución no genera más trabajo de administración de red que el que se pueda ahorrar. [35]

1.1.12.2. Grupos de trabajo virtuales

Uno de los objetivos más ambiciosos de una red virtual es el establecimiento del modelo de grupos de trabajo virtuales. El concepto es que, con una completa implementación de una VLAN a través de todo el entorno de red del campus, miembros del mismo departamento o sección puedan aparentar

[35] (Segmentacion de VLAN, 2003)

el compartir la misma red local, sin que la mayoría del tráfico de la red esté en el mismo dominio de broadcast de la VLAN. Alguien que se mueva a una nueva localización física pero que permanezca en el mismo departamento se podría mover sin tener que reconfigurar la estación de trabajo.

Esto ofrece un entorno más dinámicamente organizado, permitiendo la tendencia hacia equipos con funciones cruzadas. La lógica del modelo virtual por grupos de trabajo va la siguiente forma: los equipos pueden estar conectados virtualmente a la misma LAN sin necesidad de mover físicamente a las personas para minimizar el tráfico a través de una red troncal colapsada. Además, estos grupos serán dinámicos: un equipo destinado a un proyecto puede ser configurado mientras dure ese proyecto, y ser eliminado cuando se complete, permitiendo a los usuarios retornar a sus mismas localizaciones físicas.[36]

1.1.12.3. Seguridad

El único tráfico de información en un segmento de un sólo usuario será de la VLAN de ese usuario, por lo que sería imposible "escuchar" la información si no nos es permitida, incluso poniendo el adaptador de la red en modo promiscuó,

[36] (Segmentacion de VLAN, 2003)

porque ese tráfico de información no pasa físicamente por ese segmento."[37] [38]

1.1.13. Implementaciones infraestructurales de VLAN´s

"Se basa en la estrategia tradicional de las VLANs, el formar grupos de trabajo de acuerdo a como están distribuidas las organizaciones. Cada grupo, departamento o sección tiene unívocamente definida su VLAN, basado a en la regla del 80/20, es decir, se asume que la mayoría de tráfico se da dentro de la VLAN.

Normalmente existirán sobrelapamientos al acceder fuentes comunes a todas las VLAN, lo cual se resolverá al ubicar estos recursos en servidores; esto evita que se empleen routers para poder controlar el tráfico al acceder estos recursos.

Esto incluye todas las ventajas que pueda tener este tipo de implementación: Administración sencilla y centralizada, permite mantener fronteras organizacionales discretas, Bajo costo de desarrollo, Buen grado de privacidad y Permite alcanzar una alta eficiencia de la red. [39]

1.1.14. Implementación basada en el servicio

En esta clase de aproximación, no se tienen grupos o algo similar, cada VLAN presta un servicio, es responsable de administrar un recurso específico y ningún servidor podrá pertenecer a múltiples VLANs.

[37] (Icc, 2005)
[38] (VLAN, 2003)
[39] (Ecotec, Diseño e implementacion de VLANS , 2012)

A diferencia de los usuarios que accederán a servicios de correo, bases de datos, aplicaciones, etc. a través de una VLAN independiente. Por naturaleza, esta clase de implementación, más dinámica que la anterior, posee serios inconvenientes para administrar la memoria a cada VLAN.

Esto conlleva a un alto grado de automatización en la configuración de las VLANs. Las VLANs perderán la característica estática o semi-estática de dominios previamente definidos, para cambiar a canales a los cuales suscribirse. Los usuarios, simplemente ejecutaran determinada aplicación por cierto tiempo, el cual será limitado dependiendo de si la persona posee una cuenta o habilita a pagar por ello."[40][41]

1.2 CALIDAD DEL SERVICIO (QoS)

1.2.1. Introducción a QoS

El QoS se aplica para proporcionar mejor servicio al tráfico escogido de la red sobre varias tecnologías, inclusive Frame Relay, Modo de Transferencia Asíncrono (ATM), Ethernet, redes 802,1, SONET, y las redes IP-Router que pueden utilizar cualquier o todas estas tecnologías.

[40] (Ecotec, Diseño e Implementacion de VLANS, 2012)
[41] (Ecotec, Diseño e implementacion de VLANS , 2012)

Dado que “.”[42] En este caso se va a trabajar sobre un entorno empresarial en cual se enfocará en la satisfacción que tienen los usuarios con la red local. [43]

El control sobre recursos

Utilizando QoS se tiene el control sobre los recursos (ancho de banda, el equipo, las facilidades de ancho-área, etcétera) son utilizados. Por ejemplo, se puede limitar el ancho de banda consumida sobre una conexión de elemento principal por transferencias de FTP o da la prioridad a un acceso importante de la base de datos.

- El uso más eficiente de la administración del análisis de la red de recursos. Usando una red e instrumentos de contabilidad, se puede lo que en la red se utiliza y estar preparado para atender el tráfico más importante de la red.
- Atender hecho a la medida. El control y la visibilidad proporcionados por QoS permiten a proveedores de servicios de Internet ofrecer grados de seguridad hechos a la medida de la diferenciación del servicio a sus clientes.
- La coexistencia de aplicaciones de misión crítica. QoS se asegura de que su WAN sea utilizada eficientemente por las aplicaciones de misión crítica que es muy importante en su negocio, esas demoras de ancho de banda, tiempo mínimo sensible requerido para multimedia, las aplicaciones de voz

[42] (Microsoft, 2016)
[43] (Microsoft, 2016)

estén disponible, y que otras aplicaciones que utiliza la conexión obtiene su servicio justo sin intervenir con el tráfico de misión crítica.

- La base para una red completamente integrada en el QoS futuro. La implementación de tecnología en la red puede ser ahora un primer paso hacia la red multimedia completamente integrada necesaria a un futuro próximo.

1.2.2. Definición de QoS[44][45]

"Para establecer una correcta definición del término QoS, calidad de servicio, debemos acudir primero a estudiar la asignada por el Diccionario de la Lengua de la Real Academia Española. Según éste, la Calidad es el "Valor intrínseco de una cosa y el valor relativo resultante de compararla con otras de su misma categoría". Así mismo Servicio es "La acción y el efecto de servir. Estar hecho para algo concreto". Las dos definiciones llevan contenidas de forma inherente la propiedad de comparación; por lo tanto, para determinar si un servicio ofrece mayor o menor calidad será necesario establecer una comparación con el resto de servicios de ese nivel.

Al tratarse la anterior de una descripción demasiado genérica, son múltiples las definiciones concretas que actualmente se realizan sobre el término QoS, si bien difieren en significados dependiendo del ámbito de aplicación de tales siglas. En el ámbito de las

[44] (Pérez, 2003)
[45] (Gutierrez, 2014)

telecomunicaciones, desde la publicación en 1984 del documento E-800 de la UIT, no debería existir discusión posible ante su definición: “el efecto colectivo del rendimiento de un servicio que determina el grado de satisfacción del usuario de dicho servicio”. Es una definición comúnmente aceptada, que no deja ninguna duda de que se trata de una percepción del usuario, pues es éste quién, al final, establece unos requerimientos mínimos para cualificar.

En el ámbito de la telemática, QoS es la capacidad de un elemento de red (bien una aplicación, un servidor, un router, un switch, etc.) de asegurar que su tráfico y los requisitos del servicio previamente establecidos puedan ser satisfechos. Habilitarla requiere además la cooperación de todas las capas de la red, así como de cada elemento de la misma. Desde este punto de vista, la QoS también suele ser definida como un conjunto de tecnologías que permiten a los administradores de red manejar los efectos de la congestión del tráfico usando óptimamente los diferentes recursos de la red, en lugar de ir aumentando continuamente capacidad. En este punto es necesario prestar una atención especial al hecho de que la QoS no crea ancho de banda.

La QoS tiene, básicamente, cuatro variantes estrechamente relacionadas:

- La QoS que el usuario desea
- La que el proveedor ofrece

- La que el proveedor consigue realmente
- La que percibe el usuario"[46]

1.2.3. Problemas dentro de QoS

Se entiende por calidad de servicio la posibilidad de asegurar una tasa de datos en la red (ancho de banda), un retardo y una variación de retardo (jitter) acotados a valores contratados con el cliente. En las redes Frame Relay o ATM la calidad de servicio se garantiza mediante un contrato de CIR (Commitated Information Rate) con el usuario. Para disponer de una calidad de servicio aceptable en redes soportadas en protocolo IP se han diseñado herramientas a medida como ser los protocolos de tiempo real RTP y de reservación RSVP. Por otro lado, un problema evidente es que cuando se soporta un servicio de voz sobre IP (VoIP) por ejemplo, los paquetes son cortos y el encabezado es largo comparativamente. En este caso se requiere un encabezado reducido y un proceso de fragmentación e intercalado LFI. Mediante QoS (Quality of Service) se tiende a preservar los datos con estas características.

Los servicios tradicionales de la red Internet (SMTP o FTP) disponen de una calidad denominada "best effort"; es decir que la red ofrece el mejor esfuerzo posible para satisfacer los retardos mínimos; lo cual no es mucho pero es suficiente para servicios que no requieren tiempo-real como el web. Para servicios del tipo "real- time" (voz y video) se requiere una latencia mínima.

[46] (Gutierrez, 2014)

LATENCIA JITTER. Se denomina latencia a la suma de los retardos en la red. Los retardos están constituidos por el retardo de propagación y el de transmisión (dependiente del tamaño del paquete), el retardo por el procesamiento "store and forward" (debido a que los switch o router emiten el paquete luego de haber sido recibido completamente en una memoria buffer) y el retardo de procesamiento (necesario para reconocimiento de encabezado, errores, direcciones, etc.). Un tiempo de latencia variable se define como jitter (fluctuación de retardo) sobre los datos de recepción.

La solución al jitter es guardar los datos en memorias buffer, lo cual introduce un retardo aún mayor. Se han implementado diversas formas de buffer garantizados mediante software:

- Cola prioritaria: donde el administrador de la red define varios niveles (hasta 4) de prioridad de tráfico.
- Cola definida: donde el administrador reserva un ancho de banda para cada tipo de protocolo específico.
- Cola ponderada: mediante un algoritmo se identifica cada tipo de tráfico priorizando el de bajo ancho de banda. Esto permite estabilizar la red en los momentos de congestión.

1.2.4. Clasificación de QoS

“Todas las aplicaciones dejan huellas sobre los paquetes que pueden ser utilizadas para identificar la aplicación fuente.

El proceso de clasificación examina estas huellas y discierne qué aplicación ha generado el paquete.

Los cuatro métodos de clasificación son:

- **Protocolo:** algunos protocolos, especialmente los utilizados por algunos de los dispositivos más antiguos, son extremadamente "charlatanes" y su sola presencia origina retardos de tráfico; pero estos retardos se pueden minimizar identificando y priorizando datos en función del protocolo. Las aplicaciones pueden ser identificadas por su EtherType. Por ejemplo, AppleTalk utiliza 0x809B e IPX utiliza 0x8137. La priorización basada en este mecanismo representa una buena manera de controlar o detener estos protocolos "charlatanes".
- **TCP y UDP Socket Number:** muchas aplicaciones utilizan ciertos sockets UDP para comunicar. Por ejemplo, HTTP utiliza TCP Port 80. Examinando el número de socket del paquete IP, la red inteligente determina qué tipo de aplicación ha generado el paquete. Esta función es conocida como conmutación de Nivel 4 debido a que TCP y UDP pertenecen a la capa 4 del modelo OSI.
- **Source IP Address:** muchas aplicaciones son identificadas por su dirección Source IP (fuente IP). Como a veces algunos servidores están dedicados exclusivamente a soportar una sola aplicación -correo electrónico, por ejemplo-, el análisis de la

dirección Source IP de un paquete permite identificar qué aplicación lo ha generado.

Esto resulta particularmente útil cuando el conmutador identificante no está directamente conectado al servidor de la aplicación y llegan a él diferentes corrientes de datos.

- **Physical Port Number:** como las direcciones Source IP, el Physical Port Number (número de puerto físico) puede indicar qué servidor está enviando los datos. Esta técnica, que se basa en el mapeado de los puertos físicos en un conmutador a un servidor de aplicación, es la forma más simple de clasificación, pero exige que el servidor esté conectado directamente al conmutador, sin hubs ni conmutadores intermedios."[47]

1.2.5. Parámetros de QoS[48]

"Son muchos los términos manejados en el estudio de la calidad de servicio, que, a su vez, son aplicables no sólo a éste área, sino a otros ámbitos de las telecomunicaciones y de la informática, por lo que se explicarán aquellos considerados clave para el completo entendimiento de este tema. Para la consulta de otros vocablos relacionados será necesario acudir a alguno de los glosarios que las empresas ponen a disposición pública en sus páginas web, figurando alguna de estas direcciones en las referencias al final de este proyecto.

[47] (Rueda, 2012)
[48] (Pérez, 2003)

Tráfico de red: De forma simple, se podría decir que tráfico de una red son los datos que la atraviesan. Es pues dependiente del tipo de aplicación que por ella circulan. De esta manera se podría establecer una diferenciación del tráfico.

2. **Según el tipo de aplicación:** Se tendrá tráfico habitual, multimedia, multicast, broadcast, tiempo real, etc.
3. **Según la sensibilidad al retardo:** En este caso se tendrá:
   - **Tráfico algo sensible al retardo:** Ejemplos son los procesos de transacción on-line, la entrada de datos remota y algunos protocolos como SNA. Este tipo de aplicaciones requieren retardos de un segundo o, incluso, menos. Retardos mayores supondrían hacer esperar a los usuarios por la contestación a sus mensajes antes de que puedan continuar trabajando, disminuyendo así la productividad de los negocios."[49]
   - **Tráfico muy sensible al retardo:** El tráfico en tiempo real es de este tipo, tal y como las conversaciones vocales, la videoconferencia y multimedia en tiempo real. Todos ellos requieren un retraso de tránsito muy pequeño y típicamente menos de una décima de segundo en un sentido, incluyendo el procesamiento en las estaciones finales y un nivel de variación (jitter) mínimo.

[49] (OoCities.org, 2009)

- **Tráfico muy sensible a las pérdidas:** Ej. Datos tradicionales.
- **Tráfico nada sensible:** Ej. Servicios de noticias.

Retardo: Indica la variación temporal y/o retraso en la llegada de los flujos de datos a su destino. Es una característica que se hace muy evidente en aplicaciones como el video-conferencia, donde todos han experimentado alguna vez el retraso en la recepción de algún mensaje vocal enviado por nosotros y, por supuesto, el retardo existente entre la señal de voz y la señal de vídeo. Teniendo en cuenta hacia qué tipo de aplicaciones se están orientando las telecomunicaciones es evidente la llegada de la voz sobre IP, además es necesario que en las políticas de QoS definidas para nuestra red este parámetro sea reducido al mínimo.

Latencia: Es el tiempo entre el envío de un mensaje por parte de un nodo y la recepción del mensaje por otro nodo. Abarca los retardos sufridos durante el propio camino o en los dispositivos por los que pasa.

Jitter (Inestabilidad o variabilidad en el retardo): Es lo que ocurre cuando los paquetes transmitidos en una red no llegan a su destino en debido orden o en la base de tiempo determinada, es decir, varían en latencia. Algo semejante a la distorsión de una señal. En redes de conmutación de paquetes, jitter es una distorsión de los tiempos de llegada de los paquetes recibidos, comparados con los tiempos de los paquetes transmitidos originalmente. Esta distorsión es particularmente perjudicial para el tráfico multimedia. Una solución ante el jitter es la

utilización de buffers en el receptor. Pero esta es una medida poco eficaz, dado que sería necesario un gran tamaño para los buffers, lo que implica un costo económico en los equipos, y porque estos buffers incrementarían la latencia.

El tamaño de uno de estos buffers debería ser al menos dos veces el valor del jitter y la latencia adicional introducida por el buffer podría superar el máximo de latencia permitido por la aplicación.

Ancho de Banda: Una medida de la capacidad de transmisión de datos, expresada generalmente en Kilobits por segundo (kbps) o en Megabits por segundo (Mbps). Indica la capacidad máxima teórica de una conexión, pero esta capacidad teórica se ve disminuida por factores negativos tales como el retardo de transmisión, que pueden causar un deterioro en la calidad. Aumentar el ancho de banda significa poder transmitir más datos, algo así como aumentar el número de carriles de una autopista, pero también implica un incremento económico y, en ocasiones, resulta imposible su ampliación sin cambiar de tecnología de red.

Pérdida de Paquetes: Indica el número de paquetes perdidos durante la transmisión. Normalmente se mide en tanto por ciento. Por ejemplo: 1% o menos de media de pérdida de paquetes mensual de ancho de red.

Disponibilidad: Indica la utilización de los diferentes recursos. Suele especificarse en tanto por ciento.

Rendimiento: Mide el rendimiento de la red en relación a los servicios acordados llamados también SLAs o acuerdos de nivel de servicio. El rendimiento es definido también por algunos profesionales como la velocidad teórica de transmisión de los paquetes por la red. Esta depende directamente del ancho de banda y su variación de las posibles situaciones de congestión de la red.

Priorización: Priorizar consiste en la asignación de un determinado nivel de QoS al tráfico que circula por una red, asegurando así que las aplicaciones de mayor importancia sean atendidas con anterioridad a las de menor importancia, estando o no ante una situación de congestión. Es necesaria únicamente cuando la red no proporciona la suficiente capacidad para atender todo el tráfico presente en la misma.

Encolado: El encolado consiste en dividir y organizar el tráfico ante un determinado dispositivo de red para su posterior retransmisión por la misma según un determinado algoritmo que define a la cola y que permite que determinados paquetes sean reexpedidos antes que otros. Es una de las herramientas más utilizadas por la QoS. La idea es ofrecer un mejor servicio al tráfico de alta prioridad al mismo tiempo que se asegura, en diferentes grados, el servicio para los paquetes de menor prioridad. Los sistemas de colas, sin embargo, no garantizan que los datos importantes lleguen a su destino a tiempo cuando se produce congestión, lo único que aseguran es que los paquetes de alta prioridad llegarán antes que los de baja prioridad. Las colas se suelen situar en los

routers, siendo áreas de memoria dentro del mismo. Son, por lo tanto, una solución costosa, económicamente hablando, y complicadas de gestionar.

Planificación: Es el proceso de decidir qué paquetes enviar primero en un sistema de múltiples colas.

Flujo: Es el conjunto de datos pertenecientes a una misma secuencia que, debido a su gran tamaño, han de ser enviados mediante distintos paquetes. Tienen la misma dirección IP fuente y destino, el mismo puerto de destino y el mismo protocolo. El flujo, necesita, por tanto, llegar secuencialmente a su destino con una frecuencia constante. Por lo tanto, el parámetro más importante para caracterizar un flujo será su frecuencia constante de bit o constant bit rate, CBR, que nos dará la frecuencia a la que debería ser transmitido cada bit de datos.

Agreement(SLA) o Acuerdo de Nivel de Servicio: Es un contrato de servicios entre un proveedor de servicios y su cliente, el cual define las responsabilidades del proveedor en términos del nivel de funcionamiento de la red es decir el rendimiento, tasa de pérdidas, retrasos, variaciones y la disponibilidad temporal, el método de medida, las consecuencias cuando los niveles de servicio no se consiguen o si los niveles de tráfico definidos son superados por el cliente, así como el precio de todos estos servicios. Evidentemente, y suele ser lo más común, el SLA puede incluir reglas de condicionamiento del tráfico.

Los SLA suelen subdividirse en:

- **SLS: Service Level Specifications o Especificaciones del Nivel de Servicio:** El SLS lleva a cabo el estudio del rendimiento de la red, la probabilidad de 'drop', la latencia, la espera en las entradas y/o salidas de los puntos donde se proporciona el servicio, indicando el 'scope' del mismo, así como de los perfiles del tráfico que se deben adherir para que el servicio solicitado pueda ser proporcionado y de la disposición del tráfico.
- **SLO: Service Level Objetives u Objetivos del Nivel de Servicio:** Un SLO divide un SLA en objetivos individuales, definiendo métricas para hacer cumplir, para limpiar, y/o para vigilar el SLA, para así determinar en que SLA se están cumpliendo los servicios.

1.2.6. Especificaciones del condicionamiento del trafico

Aparte del acuerdo de nivel de servicios es necesario adjuntar unas funciones de control de los requisitos del tráfico para estudiar su comportamiento, observando el flujo de las aplicaciones, o cualquier otro subgrupo de tráfico operativo como por ejemplo actualizar tablas de encaminamiento. Algunas de estas funciones de control son la medición del tráfico, las políticas, el 'shaping' y el uso de marcas en los paquetes. Se suelen utilizar en algunas de los protocolos utilizados

para proporcionar QoS. En Diffserv, por ejemplo, se usa para hacer cumplir acuerdos entre los dominios.

Un Traffic Conditioning Agreement (TCA) o Acuerdo de Condicionamiento del Tráfico, es un acuerdo que especifica las reglas para clasificar el tráfico bajo cualquier perfil. Abarca todas las reglas de condicionamiento del tráfico especificadas explícitamente dentro de un SLA, junto con todas las reglas implícitas de los requisitos del servicio. Como ejemplo pongámonos en el caso de una red IP.

1.2.7. Algoritmos para la obtención de QoS[50]

Una vez introducidas las principales características del término calidad de servicio es necesario exponer el tipo de algoritmos utilizados actualmente en la transmisión de paquetes para comprobar cómo estos realizan un control de la congestión y a qué nivel son capaces de proporcionar calidad. Así, teniendo en cuenta la clase de servicio que son capaces de ofrecer los algoritmos de transmisión de paquetes se puede hacer tres divisiones principales:

1. Algoritmos de Mejor Esfuerzo (Best Effort): En este tipo de algoritmos se encuentran los algoritmos tradicionales, que no ofrecen ningún tipo de garantías de transmisión, por lo que podría decirse que el nivel de calidad de servicio ofrecido es nulo. Un ejemplo muy representativo es el FIFO (First In First Out). El principal problema de este tipo de algoritmos es que, si se tiene varios flujos de datos, una

[50] (Pérez, 2003)

ráfaga de paquetes en uno de ellos va a afectar a todos los demás flujos, retardando su transmisión. Es decir, que el tiempo de llegada de los paquetes de un flujo puede verse afectado por otros flujos. Cuando esto ocurre decimos que el algoritmo utilizado no es capaz de aislar flujos. Es también un modelo simple de servicio, en el cual, una aplicación envía información cuando ella lo desea, en cualquier cantidad, sin ningún permiso requerido, y sin informar previamente a la red. Además, la red para estos algoritmos reparte o envía la información si puede, sin asegurar ningún retraso, throughput o fiabilidad

2. Algoritmos Deterministas: Son aquellos en los que, para evitar la posible congestión, antes de aceptar la transmisión de un flujo, se asegura que podrá transmitirse sin problemas incluso en las peores condiciones. Esto se hace reservando ancho de banda. El ancho de banda reservado es el equivalente a lo que supondría un pico de una transmisión en ráfaga de ese flujo, con lo que se asegura que el flujo nunca se va a salir de su ancho de banda reservado. Si se supone que este comportamiento en cada uno de los flujos de la red, se podrá ver que la congestión es imposible, puesto que incluso en el caso en el que todos los flujos presentaran un pico al mismo tiempo, tendrían reservado el suficiente ancho de banda para que no hubiera congestión. En caso de que, por límites físicos de la red, no pudiera asegurarse ese ancho de banda, el algoritmo rechazaría la transmisión del flujo.

Este tipo de algoritmos fueron los primeros en aparecer cuando surgió la necesidad de asegurar las velocidades de transmisión. Es obvio que consiguen su objetivo, pero lo consiguen a un precio muy elevado, puesto que son muy ineficientes respecto al uso de la red. Como ya se ha explicado antes, las situaciones de ráfaga en un flujo son poco frecuentes y de muy corta duración, con lo que en la mayoría de los casos las necesidades de ancho de banda del flujo son mucho menores. Al reservar el equivalente al peor caso, la mayor parte del tiempo se está reservando una capacidad de transmisión que no se usa, y si esto se lo hace con varios flujos el resultado es que los algoritmos rechazan flujos por no poder darles la reserva adecuada cuando en realidad la red presenta una utilización muy por debajo de sus posibilidades. Como se puede deducir, los algoritmos deterministas aíslan completamente los flujos.

3. Algoritmos Intermedios: Aquellos algoritmos cuyo objetivo es ofrecer calidad de servicio y al mismo tiempo hacer un uso eficiente de los recursos. Entre estos se puede diferenciar entre los que ofrecen servicios estadísticos, servicios de degradación limitada y servicios predictivos. Estos algoritmos no aseguran una QoS tan estricta como los deterministas, pero en la mayoría de los casos consiguen un buen comportamiento y aprovechan mucho más los recursos disponibles. Como consecuencia, en estos algoritmos sí que es posible el retraso ocasional de algún paquete, con lo que si el algoritmo en cuestión se

da cuenta de que un paquete ha superado su tiempo de expiración puede descartarlo directamente.

- **Servicios Estadísticos:** Este tipo de servicios trabaja estadísticamente, asegurando una QoS con una probabilidad determinada. Para ello, antes de aceptar la transmisión de un flujo, obtienen los parámetros que lo modelan. Una vez obtenidos los parámetros se calcula el porcentaje de QoS que se le puede asignar, y si es mayor o igual al porcentaje requerido, se acepta el flujo. Para entender sus ventajas se puede suponer por ejemplo una red con un ancho de banda de 10 Mbps y flujos que requieren 1Mbps de frecuencia constante y 2 Mbps en ráfagas. En un algoritmo determinista se podría transmitir como máximo cinco flujos. En cambio en uno estadístico se podría transmitir hasta nueve con una probabilidad bastante alta, puesto que presentarían un comportamiento correcto exceptuando los casos en los que dos o más flujos transmitieran en ráfaga al mismo tiempo. No obstante hay que recordar que el tener una probabilidad no implica que tenga que cumplirse necesariamente. Este es el principal inconveniente de esta técnica, que garantiza una probabilidad y no un resultado. Aun así gran cantidad de algoritmos de este tipo han resultado ser bastante exactos y usados con probabilidades de fallos del orden 105 presentan un

comportamiento casi determinista aventajándose mucho más la capacidad de la red.

- **Servicios de Degradación Limitada:** Una característica de los flujos es que se puede permitir la pérdida de algunos datos. Los algoritmos de degradación limitada aprovechan este hecho en la gestión de los paquetes consiguiendo una capacidad de decisión más alta. Por ejemplo, en una aplicación de comunicación por voz, se puede permitirnos perder algunos paquetes, teniendo en cuenta que estas pérdidas de paquetes están limitadas por la aplicación, puesto que una perdida excesiva provocaría que la voz fuera ininteligible. Con este método, cuando un flujo entra en la red divide sus paquetes en varios tipos, cada uno con una prioridad distinta y con un retardo máximo diferente. Así, en caso de congestión, los paquetes importantes tendrán mayor prioridad.
- **Servicios Predictivos:** Se caracterizan por utilizar datos obtenidos midiendo las características de los flujos. En la admisión del flujo es necesario confiar en la información que da el servidor del flujo, pero una vez dentro de la red se calculan dinámicamente sus parámetros. Con esto se asegura una información fiable y real, puesto que proviene del compartimiento actual del flujo. Este hecho ayuda a tomar decisiones más precisas sobre las necesidades del flujo y, por

tanto, lleva a un funcionamiento bastante correcto con una utilización elevada de los recursos.

Otra característica que tienen es organizar los flujos en grupos con necesidades similares. La mayor ventaja reside en que es posible aplicar políticas distintas en cada grupo. Así se puede establecer prioridades entre grupos o limitar el uso de los recursos dependiendo del grupo al que pertenezcan. Añaden con mucha facilidad comunicaciones sin calidad de servicio simplemente añadiendo un grupo con prioridad mínima y sin reserva de ancho de banda. Esto hace que la utilización de la red sea más alta.

1.2.8. Beneficios del QoS

Este punto de estudio estará centrado en los beneficios que ofrece QoS para las aplicaciones, empresas y proveedores de servicio.

1.2.9. Ventajas para las aplicaciones

Hoy en día, todas las empresas están considerando Internet como una nueva vía para incrementar su negocio y, en consecuencia, las expectativas que se tienen para garantizar una calidad son las mismas que si se tratase de una red privada o controlada. Internet está siendo utilizada para la formación y el crecimiento de intranets dentro de la empresa y extranets que permiten el comercio electrónico con los socios del negocio. Es evidente, por tanto, que se está incrementando el acercamiento de los negocios hacia la Web, siendo cada vez más

importante que los administradores de las redes aseguren que éstas entreguen unos niveles apropiados de calidad. Es aquí donde las tecnologías de QoS cobran especial importancia, proporcionando a los administradores las utilidades para la entrega de datos críticos del negocio en los periodos y con unas garantías determinadas.

1.2.10. Beneficios para los proveedores de servicio

Claramente, las empresas y las corporaciones se están convirtiendo en negocios con requerimientos de "misión crítica" sobre la red pública. Están delegando los servicios de sus redes a proveedores de servicio (outsourcing), lo que les permite centrarse más en el negocio interno y así reducir costosos capitales. Esto significa que los proveedores de servicio son quienes podrán ofrecer las garantías de calidad para el tráfico extremo-a-extremo o end-to-end de la empresa. Las tecnologías de QoS permitirán a los proveedores de servicio ofrecer muchas más prestaciones, como el soporte del tráfico en tiempo real, o como la asignación específica de ancho de banda, que se suele especificar en los acuerdos de nivel de servicio (SLAs) "este tipo de funcionamiento de QoS se ve sustentado con los Service Level Agreement (SLA) o acuerdos de nivel de servicio entre el cliente y su proveedor de servicios como por ejemplo, Internet Service Provider (ISP).

Un SLA básicamente especifica las clases de servicio soportadas y la cantidad de tráfico permitida en cada clase. Los SLA pueden ser estáticos o dinámicos, según si la negociación se hace de forma cuasi

permanente (mensualmente) o de forma dinámica según las necesidades de cada momento.”[51]

1.2.11. Gestión del ancho de banda versus QoS

Es de todo el profesional informático conocido el hecho de que la capacidad de cualquier tipo de sistema siempre, o casi siempre, acaba por agotarse; así, los discos duros se llenan o las líneas telefónicas de una centralita se saturan. Pero donde este límite se suele alcanzar con particular rapidez es en la capacidad de la línea que conecta una organización con Internet o en general con una red IP ante el imparable crecimiento de las aplicaciones sobre este medio. Lo normal es que, cuando las conexiones van lentas, se contrate más capacidad. Pero, aun así, las líneas vuelven a saturarse tras un breve período de tiempo y es una solución costosa. Esta es la técnica conocida como sobre ingeniería o método de la fuerza bruta. Es necesario preguntarse entonces si ésta es la solución correcta y al estudiar otras alternativas se ve que con éstas se pueden obtener mayores capacidades por menos costes mediante la optimización de la gestión del ancho de banda. También conocida como gestión de políticas.

Por lo tanto, el ampliar el ancho de banda debe utilizarse como una solución puntual para resolver determinadas situaciones de congestión en determinados puntos de la red y para determinados tipos de redes.

[51] (DocShare, 2015)

Es medianamente factible para redes LAN y prácticamente imposible para redes WAN, mientras los precios sigan siendo tan elevados. Es por tanto, una solución costosa, con durabilidad mínima debido al crecimiento del tráfico de la red y de las necesidades de ancho de banda de determinados tipos de tráfico. La QoS sin embargo, conlleva, entre otras cosas, una correcta gestión del ancho de banda. Presentándose como la forma más eficiente, hoy en día, para la mejora de toda red que se precie. Es, en definitiva, la solución por la que deberían apostar todas las empresas para mejorar su red y, en consecuencia, su negocio.[52]

1.2.12. Protocolos y arquitecturas del QoS[53]

"RSVP surgió en 1990 como el método definitivo para alcanzar el nirvana QoS, pero el protocolo fue diseñado para una única arquitectura de red, y no para el mundo heterogéneo que hoy cunde en el networking. En consecuencia, no faltaron voces que solicitaban su sustitución por otras alternativas más adaptadas a la realidad, pero la reunión del IETF del mes de agosto de 1998 permitió contemplar la posibilidad de que las diferentes tecnologías de QoS trabajasen juntas para proporcionar los tan deseados niveles de QoS, pensando en usar RSVP en los routers de extremo, Diffserv en la parte central para agregar tráfico, MPLS para especificar la mejor ruta para el tráfico a través de la red utilizando etiquetas y 802.1p/q para redes 802.

[52] (Pérez, 2003)
[53] (DocShare, 2015)

1.2.13. Protocolos[54]

Las aplicaciones, la topología de la red y la política de QoS dictan qué tipo de QoS es más apropiado para un flujo individual o para varios. De entre todas las opciones, los protocolos y algoritmos más utilizados son:

1.2.13.1. Reservation Protocol (RSVP): Protocolo de reserva de recursos[5556]

Proporciona la señalización para permitir la reserva de recursos de la red conocida también como Servicios Integrados o Integrated Services. Aunque se usa típicamente para un solo flujo (per flow), RSVP también se utiliza para flujos agregados (per aggregates). Se hablara de flujos agregados cuando circule más de un flujo por la red.

El Protocolo de Reserva de Recursos [RFC2205, Versión 1 Functional Specification] es un protocolo de señalización que proporciona un control para la reserva, orientado fundamentalmente a redes IP. Es un componente clave de la arquitectura de los Servicios Integrados en Internet IETF (IntServ) en la que se define el funcionamiento y la forma de petición e intercambio de información entre y para cada elemento de la red y así realizar un control de la calidad de servicio.

[54] (DocShare, 2015)
[55] (Pérez, 2003)
[56] (DocShare, 2015)

La reserva de recursos se realiza en los routers intermedios situados a lo largo de toda la ruta de datos de la aplicación. Es, hasta el momento, la más compleja de todas las tecnologías de QoS para las aplicaciones (hosts) y para los distintos elementos de la red (encaminadores y puentes).

Como resultado, representa el mayor estándar creado desde el servicio best effort de las redes IP, proporcionando el mayor nivel de QoS en términos de servicio garantizado, granularidad de localización de recursos y el mayor detalle sobre la forma de actuación de aplicaciones y usuarios que proporcionan QoS.

RSVP fue creado en 1990 por IETF, definiendo un modelo de asignación de QoS en el que cada receptor para una sesión, fuese responsable de elegir su propio nivel de reserva de recursos, iniciando la reserva y manteniéndola activa tanto tiempo como desee. Consistiendo, pues, en una solución distribuida que permite a múltiples receptores heterogéneos efectuar reservas específicamente dimensionadas según sus propias necesidades. Además, para mantener el control el receptor puede enviar sus especificaciones a la fuente encargada de solicitar las reservas de la red.

En definitiva, RSVP permite que las aplicaciones soliciten una calidad de servicio específica a la red. En vez de un protocolo de encaminamiento es más bien un protocolo de control de Internet. Su tarea consiste en establecer y mantener las reservas

de recursos en un árbol de distribución, con independencia de cómo se hayan creado. El grupo de trabajo Integrated Services del IETF ha considerado la existencia de varias clases de QoS, si bien actualmente sólo dos de éstas han sido formalmente especificadas para ser utilizadas con RSVP:

Servicios garantizados (Guaranteed Service) (service_number 2) [RFC2211]: Este servicio proporciona un nivel de ancho de banda y un límite en el retardo, garantizando la no existencia de pérdidas en colas. Está pensado para aplicaciones con requerimientos en tiempo real, tales como ciertas aplicaciones de audio y vídeo. Cada router caracteriza el SG para un flujo específico asignando un ancho de banda y un espacio en buffer.

Servicio de Carga Controlada (Controlled-Load Service) (service_number 5) [RFC2212]: A diferencia del SG este servicio no ofrece garantías en la entrega de los paquetes. Así, será adecuado para aquellas aplicaciones que toleren una cierta cantidad de pérdidas y un retardo mantenidos en un nivel razonable. Los routers que implementen este servicio deben verificar que el tráfico recibido siga las especificaciones dadas por el Tspec, y cualquier tráfico que no las cumpla será reenviado por la red, como tráfico best-effort."[57]

A continuación un resumen de los tipos de servicio en IntServ.

[57] (DocShare, 2015)

Servicio	Características	Equivalencia en ATM
Garantizado	▪Garantiza un caudal mínimo y un retardo máximo ▪Cada router del trayecto debe dar garantías ▪A veces no puede implementarse por limitaciones del medio físico (Ej. Ethernet compartida	CBR VBR-rt
Carga Controlada ('Controlled Load')	▪Calidad similar a la de una red de datagramas poco cargada ▪Se supone que el retardo es bajo, pero no se dan garantías	VBR-nrt
'Best Effort'	▪Ninguna garantía (como antes sin QoS)	UBR

Tabla 1.2.13.1.1 Tipos de servicio IntServ

Fuente: J. Carlos López Ardao, "Redes de Banda Ancha"

Figura 1.2.13.1.2 Reparto de recursos IntServ

Fuente: J. Carlos López Ardao, "Redes de Banda Ancha"

1.2.13.2. Toma de decisiones[58][59]

[58] (Ardao, Abril 2005)
[59] (DocShare, 2015)

"Para la toma de decisiones de QoS asociadas a los paquetes de una aplicación, RSVP interactúa con las entidades denominadas packet classifier"[60] o clasificador de paquetes y packet scheduler o "programador de paquetes instaladas en el host. Primero consulta a los módulos las decisiones locales para saber si la QoS deseada puede ser provista mediante decisiones basadas en recursos o bien mediante decisiones basadas en políticas y, en consecuencia, establece los parámetros requeridos en el clasificador y en el programador del paquete. El clasificar de paquetes determina la ruta del paquete y el programador toma las decisiones de envío para alcanzar la QoS deseada, negociando si es necesario, con aquellos host que tengan capacidad propia de gestión de QoS, para proporcionar la calidad solicitada por RSVP.

Algunas características o aspectos fundamentales en el RSVP son:

Merging: En los diferentes nodos que se van atravesando en la red por el camino de datos, se va realizando un proceso de concentración de los diferentes mensajes de petición de reservas.

Estado de reserva en cada nodo: El estado soft RSVP se crea y refresca periódicamente por mensajes Path y Resv. Permite

[60] (DocShare, 2015)

observar el estado en que se encuentran las reservas de recursos.

Estilos de reserva: Una petición de reserva incluye un conjunto de opciones que se conocen como el estilo de reserva. Las distintas combinaciones de estas opciones conforman los tres estilos de reserva en uso, Wildcar- Filter"[61] o filtro libre (WF), Fixed-Filter o filtro fijado (FF) y Shared-Explicit o explícito compartido (SE).

1.2.13.3. Proceso RSVP[62]

Por razones de eficiencia, los receptores o clientes son las entidades responsables de manejar el tráfico con QoS. La aplicación del host receptor si ha pasado un proceso local RSVP. Luego el RSVP envía la respuesta a todos los nodos (routers y hosts) a lo largo de la ruta por los mensajes path(s) hasta los mensajes de origen, pero solo tan lejos como la distribución multicast de los routers este conformada. La figura No. 1.2.13.3.1, se presenta el proceso de RSVP y sus elementos.

[61] (DocShare, 2015)
[62] (Practical IP Network QoS, 2012)

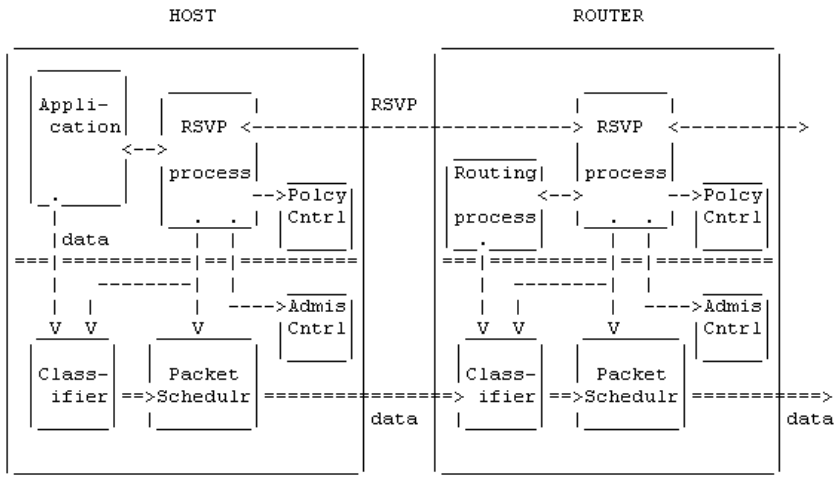


Figura 1.2.13.3.1 Proceso general del RSVP

Fuente: (Practical IP Network QoS, 2012)

QoS es implementado por mecanismos no pertenecientes a RSVP, llamados "Traffic control". El mecanismo es:

- **Packet classifier:** Determina la clase de QoS, y a veces de los routers para cada paquete.
- **Packet scheduler:** Logra el QoS prometido.
- **Admission control:** Determina si el módulo tiene recursos disponibles suficientes para abastecer el QoS pedido.
- **Policy control:** Determina si el usuario tiene permiso administrativo para hacer la reserva.

1.2.13.4. Tipos de mensajes [6364]

"Existen dos tipos de mensajes en RSVP fundamentales, Resv y Path. Una aplicación solicita participar en una sesión RSVP como emisor, enviando un mensaje Path en el mismo sentido que el flujo de datos, por las rutas uni/multicast proporcionadas por el protocolo de routing. A la recepción de este mensaje, el receptor transmite un mensaje Resv, dirigido hacia el emisor de los datos, siguiendo exactamente el camino inverso al de los mismos, en el cual se especifica el tipo de reserva a realizar en todo el camino."[65]

Los mensajes RSPV ofrecen la siguiente información a la red:

- Qué soy es decir que origina la aplicación y el subflujo. Por ejemplo, flujo de impresión frente a transacción crítica en el tiempo.
- Quién soy que es el ID. de usuario autorizado.
- Qué deseo que es el tipo de servicio QoS necesario.
- Cuánto deseo que es las ciertas aplicaciones cuantifican los requisitos de recursos de forma precisa.
- Cómo se me puede reconocer que es el criterio de clasificación de tupla 5 por el que se reconoce el tráfico de datos.

[63] (Martin, 2011)
[64] (DocShare, 2015)
[65] (DocShare, 2015)

- Qué recursos de dispositivos de red se verán afectados por el tráfico de datos asociado.

La señalización basada en host ofrece ventajas importantes a los sistemas de administración de QoS. Como ventaja evidente se puede destacar que la señalización basada en host proporciona enlaces fuertes entre la información de clasificación y los usuarios y las aplicaciones. Además, este tipo de señalización ofrece control de admisión dinámica compatible con la topología.

“En su paso por cada router RSVP los mensajes PATH´s se actualizan y se retransmiten, consistente esto en poner la dirección IP del router que lo actualiza y reenvía. Cada router RSVP también almacena la dirección del router anterior. Así, con los mensajes PATH´s se posibilita indicar al receptor, o receptores, no solo las características del tráfico de usuario, sino también la ruta por donde debe solicitar las correspondientes reservas de recursos. Los routers que no soporten RSVP transfieren transparentemente los mensajes PATH´s.

Los mensajes RESV´s son producidos por el receptor o receptores de los flujos de información de usuario, como «respuesta» a los mensajes PATH´s, y solicitan a la red a los routers RSVP las correspondientes reservas de recursos para

soportar la comunicación con cierta QoS, fluyendo hasta la fuente del stream de datos de usuario, es decir, en sentido upstream. Con la información de ruta que suministran previamente los mensajes PATH´s, los mensajes RESV´s dirigen las solicitudes de reservas a los routers RSVP apropiados, esto es, por donde fluirán los streams de datos.

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

Estas reservas de recursos en los routers RSVP de la red se materializan mediante soft-states en dichos routers, estados que requieren para mantenerse de «refrescamientos» periódicos, por lo que durante toda la comunicación se necesita «señalizar» para mantener las reservas previamente efectuadas. En consecuencia, esto conlleva a cierta señalización «permanente» durante la fase de transferencia de información de usuario, con la consiguiente carga de tráfico que implica. Vale decir también que la reserva de recursos extremo a extremo que posibilita RSVP será válida si, y solo si, la congestión y demora que introduzcan los routers no RSVP no es significativa.

Algunos de los mensajes del protocolo RSVP son:

- **PATHTEAR:** son mensajes generados por la fuente de datos de usuario para eliminar los estados PATH's en todos los routers RSVP. Siguen la misma ruta que los mensajes PATH´s. También pueden ser originados por cualquier nodo cuando se agota el timeout del estado path.
- **RESVTEAR:** son generados por los receptores para borrar los estados de reserva en los routers RSVP, por tanto viajan en el sentido upstream. Pueden ser también originados por nodos RSVP al agotarse el timeout del estado de reserva de los mismos.
- **PATHERR:** viajan en sentido upstream hacia el emisor siguiendo la misma ruta que los mensajes PATH´s, y notifican errores en el procesamiento de mensajes PATH´s, pero no modifican el estado del nodo por donde ellos pasan en su «viaje» hacia la aplicación emisora.
- **RESVERR:** notifican errores en el procesamiento de mensajes RESV, o notifican la interrupción de una reserva. Se transfieren en la dirección downstream hacia el receptor o receptores apropiados.

1.2.13.5. Funcionamiento básico RSVP[66]

En la figura No. 1.2.13.5.1, se presenta el funcionamiento básico de los mensajes RSVP.

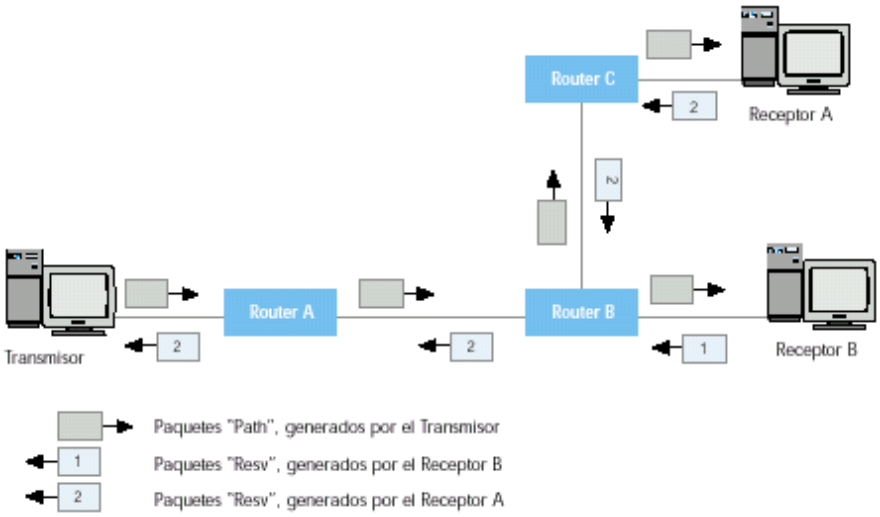


Figura 1.2.13.5.1 Protocolo RSVP resumido. Intercambio básico de mensajes

Fuente: (Martin, 2011)

En la figura No. 3.11.1.4, se muestra de forma muy simplificada el intercambio de mensajes RSVP, específicamente mensajes PATH´s y RESV´s entre un emisor y dos receptores (A y B), indicándose que la reserva representada por el mensaje RESV 2 prevalece sobre la reserva representada por el mensaje RESV1, de manera que esto

[66] (Martin, 2011)

sugiere que la reserva solicitada por el receptor A es mayor que la solicitada por el receptor B. Esto es, la reserva «mayor» prevalece sobre la reserva «menor», así el *router* B sólo solicita al *router* A la mayor de las dos solicitudes de reservas a él llegadas desde el *router* C originada por el receptor A y desde el receptor B. Esto es una característica de RSVP.

Estas solicitudes de reserva conducen a que en cada *router* RSVP se establezca un estado *soft* o *Soft-State*, es decir, una reserva en cada *router* es un estado *Soft* con un determinado *timeout*, que debe ser refrescada periódicamente por los receptores, de lo contrario vence el *timeout* y se deshace la correspondiente reserva, con la consecuente generación de un mensaje RESVTEAR.

La liberación de recursos reservados mediante RSVP se puede materializar de diferentes maneras, así la solicitud para dar baja a determinada reserva puede ser originada:

- Por el emisor,
- Por el receptor, o
- Por un nodo de la red.

Por parte del emisor o de un receptor acontece 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. Por parte de un

nodo se lleva a cabo 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."[67]

1.2.13.6. Implementaciones RSVP/QoS[68]

"A partir de las especificaciones publicadas en los diferentes RFCs ([2205], [2206], [2207], [2208], [2209]), más de 30 empresas del mundo de la informática y las telecomunicaciones han decidido realizar diferentes implementaciones del protocolo, tanto en su comportamiento como router como en el de host, junto con la realización de diferentes herramientas de aplicación. Se va analizar el estado actual de dichas implementaciones para aquellas empresas más destacadas del sector, teniendo en cuenta el sistema operativo utilizado, la tecnología de red, la capacidad de QoS, las aplicaciones, qué características no son soportadas, la interoperabilidad y la disponibilidad del producto. Así:

La tecnología de red utilizada es prácticamente común en casi todas ellas: ATM, Frame Relay, Ethernet shared, Ethernet switched, Token Ring y FDDI. Respecto a la capacidad de QoS, todos los productos cumplen con las especificaciones de RSVP y de Integrated Services ofreciendo servicio Controlled

[67] (Guayaquil, 2008)
[68] (DocShare, 2015)

Load. El Guaranteed Service sólo está disponible en una decena de implementaciones. La opción Differentiated Services es minoritaria encontrándose en proceso de implantación en algún caso. Es interesante conocer cuáles son las características del protocolo que todavía no están implementadas y que cada fabricante, en función del grado de desarrollo que tenga su producto, indica como futuras realizaciones. Así, la compatibilidad con el protocolo IPv6, el servicio Guaranteed y el IPSEC son las referencias de no implementación más señaladas. Además, algunos productos no contemplan encapsulación UDP, realización de túneles para el paso por redes no-RSVP, mensajes de diagnóstico y autentificación.

1.2.13.7. RSVP API (RAPI)[69]

Se estudiara ahora el posible funcionamiento de la RSVP API o RSVP Aplication Programming Interface en un sistema UNÍX. Esta va a proporcionar a la aplicación los mecanismos necesarios para comunicarse con el RSVP daemon de tal forma que se pueda realizar la reserva oportuna en todo el camino de datos. Un proceso RSVP se inicia a partir de la llamada SESSION definida por la dirección destino, el identificador de protocolo y un puerto destino. Si la llamada tiene éxito, retorna un identificador de sesión. Cuando una aplicación desea iniciar

[69] (DocShare, 2015)

el envío de un flujo de datos, activa la llamada SENDER que define los atributos de dicho flujo, a partir de unos parámetros determinados.

1.2.13.8. Descripción de problemas[70][71]

Se describe ahora los problemas sobre la experiencia realizada sobre RSVP. Hay tres problemas fundamentales que afectan al funcionamiento del protocolo RSVP, la escalabilidad, el routing y el no poder trabajar sobre redes no RSVP.

El problema de la escalabilidad existe, dada la gran cantidad de señalización que aparecerá conforme la red vaya aumentando de tamaño, tanto en cuanto a rutas como en cuanto a usuarios.

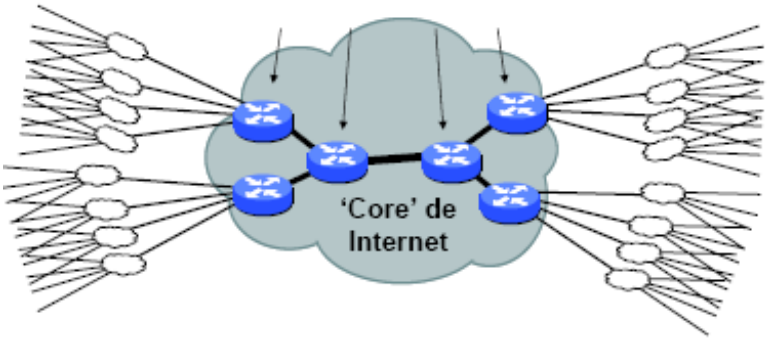


Figura 1.2.13.8.1 El problema de la escalabilidad

Fuente: (Martin, 2011)

[70] (Martin, 2011)
[71] (DocShare, 2015)

Estos routers han de mantener información sobre muchos flujos y por tanto mucha información de estado. El routing conlleva un problema, dado que el proceso de encaminamiento se realiza en el instante de establecer la sesión y enviar el mensaje Path. En este punto, los algoritmos de encaminamiento utilizados no tienen en cuenta cuales van a ser las características de reserva solicitadas por el receptor, con lo cual puede que la decisión adoptada para establecer la ruta, no sea la más adecuada teniendo en cuenta sólo los parámetros de caracterización del tipo de QoS elegido. La certeza de que la ruta establecida podrá contener dispositivos intermedios que no implementen el protocolo RSVP, hará que la reserva extremo a extremo esté condicionada por dichos sistemas. Respecto a las experiencias realizadas, es preciso comentar que es necesario conseguir una interoperabilidad completa entre los diferentes sistemas tanto para sesiones unicast como para sesiones multicast junto con la obtención de reservas correctas en los diferentes nodos en presencia de tráfico interferente.

1.2.14. Differentiated Services (DIFFSERV): Servicios diferenciados[72][73]

Permite el dividir y el dar prioridad al tráfico de la red mediante el uso de etiquetas en las cabeceras de los paquetes. Es un protocolo de QoS

[72] (Pérez, 2003)
[73] (DocShare, 2015)

propuesto por IETF [RFC 2475 y RFC 2474] que permite distinguir diferentes clases de servicio marcando los paquetes. Permite a los proveedores de servicios Internet y a usuarios de grandes redes IP corporativas desplegar rápidamente diferentes niveles QoS en la troncal. A diferencia de RSVP no especifica un sistema de señalización, consiste en un método para marcar o etiquetar paquetes, permitiendo a los routers modificar su comportamiento de envío. Cada tipo de etiqueta representa un determinado tipo de QoS y el tráfico con la misma etiqueta se trata de la misma forma.

Para proporcionar los diferentes niveles de servicio utiliza el campo type of service (TOS) o Diffserv Codepoint (DSCP) de la cabecera del estándar Ipv4 e Ipv6. "Éste es un campo de 8 bits, estando los 2 últimos reservados. Con los 6 bits restantes se consiguen 64 combinaciones: 48 para el espacio global y 16 para uso local."[74] Este tipo de funcionamiento de QoS se ve sustentado con los Service Level Agreement (SLA) o acuerdos de nivel de servicio entre el cliente y su proveedor de servicios como por ejemplo, Internet Service Provider (ISP).

Un SLA básicamente especifica las clases de servicio soportadas y la cantidad de tráfico permitida en cada clase. Los SLA pueden ser estáticos o dinámicos, según si la negociación se hace de forma cuasi permanente (mensualmente) o de forma dinámica según las

[74] (OoCities.org, 2009)

necesidades de cada momento, en este caso los clientes deben usar protocolos de señalización como RSVP. A continuación se va a explicar los componentes que forman parte de este protocolo, así como su funcionamiento.

1.2.14.1. Tipos de marcas[75][76]

Para clasificar el tráfico mediante DiffServ, se proponen básicamente tres opciones de marcas:

- **None (Ninguna):** Ofrece el servicio Best Effort convencional.
- **Assured and in profile (asegurado y definida dentro del perfil):** Definida en el SLA entre el cliente y el proveedor de servicio.
- **Assured and out of profile (asegurado y fuera de perfil):** No cumpliría lo definido en el SLA entre el cliente y el proveedor de servicio.

1.2.14.2. Clases de servicio[77]

El protocolo Diffserv ha definido dos tipos de clases de servicio: el servicio Premium y el servicio Asegurado o Assured Service, aunque soporta, además, el convencional servicio Best Effort.

[75] (Ardao, Abril 2005)
[76] (DocShare, 2015)
[77] (DocShare, 2015)

- **Premium Service:** proporciona bajo retardo y bajo nivel de jitter para aquellos clientes que generen grandes picos tráfico. Este nivel de servicio está especificado en el SLA que el cliente contrata con el ISP. El SLA especifica la velocidad pico deseada y ofrecida y el ancho de banda proporcionado. El ISP debe responsabilizarse de proporcionarla y el cliente en no superar esa tasa. Este tipo de servicio es el apropiado para la Telefonía por Internet, la videoconferencia o, por ejemplo, para la creación de líneas virtuales en redes privadas virtuales (VPNs). Su precio es mayor que para el Assured Service.
- ***Assured Services:*** Es escogido por aquellos clientes que necesitan un cierto nivel de fiabilidad de sus ISPs incluso si existe congestión. Sus especificaciones también vienen determinadas en los SLAs. En éste se indica la cantidad de ancho de banda disponible para el cliente, pero será el cliente el responsable de decidir cómo compartirán sus aplicaciones el ancho de banda. Las aplicaciones apropiadas son las mismas que las que utilizarían el servicio Best Effort.

1.2.14.3. El Bandwidth Broker (BB) en DIFFSERV[78]

[78] (DocShare, 2015)

La información necesaria para realizar la monitorización y gestionar los recursos de red disponibles es mantenida para todo el dominio por un agente servidor denominado el Bandwidth Broker (BB). Los clientes en los routers intercambian información con el servidor mediante el protocolo BBTP o Bandwidth Broker Transport Protocol. La BB puede intercambian información con otros BB de otras redes (dominios). Los ISPs pueden acordar políticas de intercambio mutuo.

1.2.14.4. Arquitectura DIFFSERV[79][80]

A continuación se presenta la arquitectura DiffServ de manera general con nodos exteriores, es decir routers de frontera y nodos interiores o routers interiores."[81]

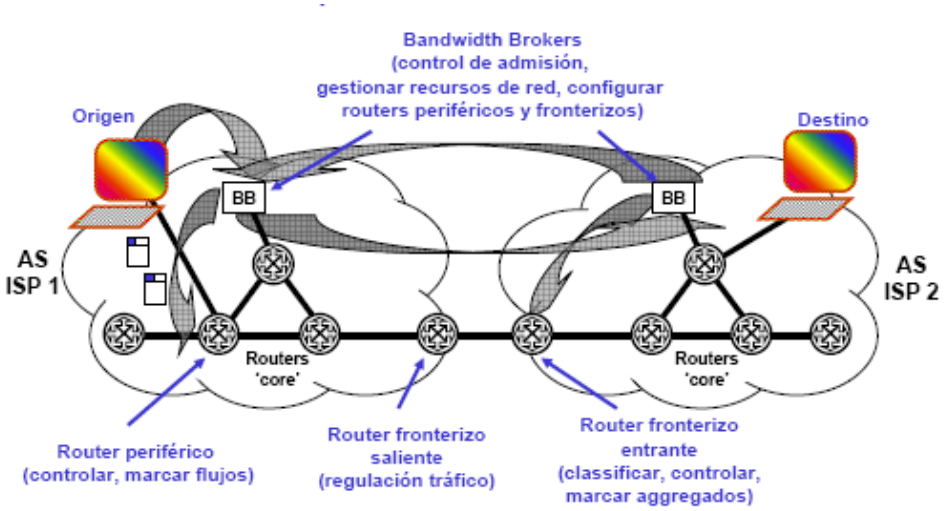


Figura 1.2.14.4.1 Arquitectura general DiffServ

[79] (Belzarena, 2003)
[80] (DocShare, 2015)
[81] (DocShare, 2015)

Fuente: (Ardao, Abril 2005)

El tráfico es separado en clases en el ingreso a la red y marcado para registrar la clase a la que pertenece. Esa marca llamada DSCP o Diferentiated Service Code Point usa 6 bits para distinguir una clase de otra.

Estos seis bits se registran en el byte de Type of Service en el cabezal de IPv4 o en el de Traffic Class en el de IPv6. A cada DSCP le corresponderá luego un tratamiento específico en cada nodo de la red. Este tratamiento específico que se le brinda a cada clase de tráfico se llama en DiffServ PHB o Per Hop Behavior. El DSCP es seteado en la frontera de la red y en los routers internos es examinado para asociarlo con el PHB correspondiente.

A continuación se presenta la arquitectura de un nodo exterior e interior para Diffserv

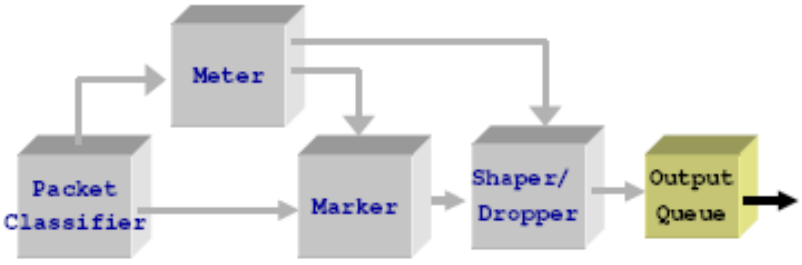


Figura 1.2.14.4.2 Arquitectura de un Nodo exterior en DiffServ

Fuente: (Belzarena, 2003)

En este sentido la mayor complejidad residirá en los nodos de la frontera, aunque en los nodos interiores habría que configurar políticas de scheduling y dropping que pueden ser complejas.

En la figura No. 1.2.14.4.2, se ve la arquitectura de un nodo exterior en Diffserv. Existen dos funciones principales en esta arquitectura:

1. **El clasificador:** que selecciona paquetes de acuerdo a ciertos criterios y los re direcciona en base a esta selección.
2. **El acondicionador de tráfico:** que de acuerdo al SLA y en particular al perfil de tráfico acordado, acondiciona el tráfico que ingresa de cada clase.

La clasificación puede ser de dos tipos: MF o MultiField, es decir que analizando diferentes campos del paquete se define la clase a la que pertenece el paquete o simplemente basado en el campo DSCP si el paquete ya venía marcado. El paquete en este modelo puede venir marcado desde el cliente ya sea este un usuario final u otro ISP. La función de acondicionamiento del tráfico clasifica los paquetes en In-profile o out-of-profile. In-profile puede ser mandado sin ningún otro procesamiento.

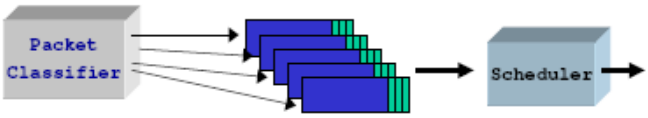


Figura 1.2.14.4.3 Arquitectura de un Nodo interior en DiffServ

Fuente: (Belzarena, 2003)

La arquitectura de un nodo interior de la red se muestra en la figura No. 1.2.14.4.3 En esta figura se aprecia que la arquitectura de un nodo interior es algo más simple. En un nodo interior se examina el DSCP y se define el PHB que debe darse al paquete. El PHB está definido como una descripción del comportamiento de reenvió observado exteriormente. Esto quiere decir que en un PHB se especifica cómo debe observarse como caja negra el tratamiento que reciben los paquetes de esa clase. La implementación de un PHB puede ser hecha por diferentes mecanismos. En general los mecanismos usados actualmente para implementar un PHB son mediante políticas de scheduling para reservar ancho de banda y dropping como RED o Random early detection o RIO conocido como Red In-profile out-profile.

1.2.14.5. Envío de paquetes[82]

[82] (DocShare, 2015)

"El proceso de envío de los paquetes modificados por Diffserv desde un router se conoce como PHB, Per Hop Behavior policies o "comportamiento por salto". El PHB indica qué tratamiento han recibido los paquetes a lo largo de su transmisión para entregar Diffserv, tales como: tipos de políticas aplicados, conformación del tráfico, posibles remarcados en el campo DS, encolamientos y gestión del tráfico.

Existen varios tipos de PHBs:

- **Expedited Forwarding (EF):** Tiene un solo valor de DiffServ (codpoint). Minimiza el retardo, el jitter y asegura baja pérdida de paquetes, proporcionando el mayor nivel de QoS."[83] Se caracteriza por su reenvió priorizado en base a planificadores de prioridad, además que puede expulsar otros tráficos, garantiza que la tasa de partida de cualquier paquete debe ser igual o superior a una tasa configurable y fue pensado principalmente para construir servicios de bajo retraso y sin perdidas.
- **Assured Fordwarding (AF):** Los paquetes se etiquetan con «alta prioridad», aunque no se garantiza un ancho de banda. Se posibilita una QoS superior al

[83] (DocShare, 2015)

servicio tradicional *best-effort* de Internet. Brinda cuatro clases de servicios, cada una con tres niveles diferentes de «dropping». Un nodo DS es, en principio, una combinación de cinco módulos funcionales, aunque no todo *router* DS tiene que contener la totalidad de éstos:

- **Clasificador de tráfico:** clasifica los paquetes en base a uno o varios campos de su cabecera.
- **Medidor de tráfico (Traffic Meter):** mide las propiedades temporales de los paquetes.
- **Marcador de paquetes (Packet Markers):** establece un codepoint en el campo DS del paquete
- **Conformador (Shapers):** establece cierta demora para uno o más paquetes de un stream.
- **Droppers:** descarta algunos o todos los paquetes de un stream de tráfico.
- **Default (DE):** Funciona como el servicio Best Effort, tradicional. "El borrador de Diffserv define además la implementación del protocolo en dos tipos de routers: condicionadores de tráfico y capacitados para DS."[84]

[84] (DocShare, 2015)

1.2.14.6. Clasificador de tráfico (Capacitados para DS)[85][86]

"El clasificador de tráfico selecciona los paquetes basándose en uno o varios campos de cabecera. Aportan, por lo tanto, funciones de programación y deben modificar su comportamiento de envío en función de las marcas o etiquetas. Como se puede ver, esta diferenciación se realiza utilizando el campo ToS (Ipv4) que cambio por DS (Ipv6), proporcionando un máximo de 64 clases de servicio. Cada router ordena los paquetes en colas basándose en el citado campo, aplicando diferentes políticas de priorización a las mismas. Los routers capacitados para DS suelen ser los routers de troncal. "[87]

El formato de los paquetes Ipv6 es:

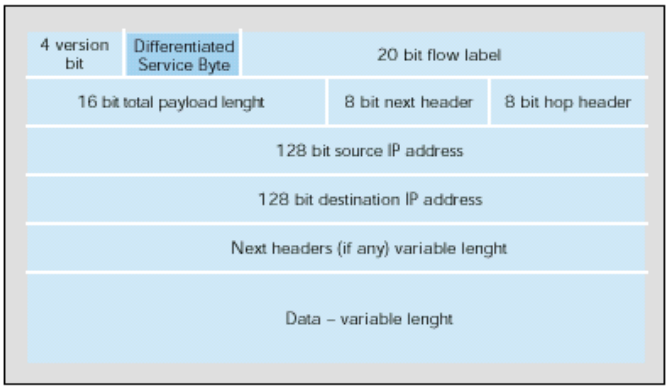


Figura 1.2.14.6.1 Formato del paquete Ipv6

Fuente: (Martin, 2011)

[85] (Martin, 2011)
[86] (DocShare, 2015)
[87] (DocShare, 2015)

La estructura del campo Tipo de servicio de los datagramas IP en Ipv4 era de la siguiente manera:

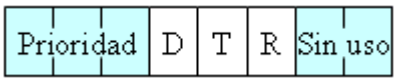


Figura 1.2.14.6.2 Campo DS en Ipv4

Fuente: (Chafla, 2003)

En donde los campos D, T y R son usados para el transporte donde se fijan los parámetros correspondientes. Actualmente se ha definido el campo DS, para IPv4 e IPv6 y está compuesto por:

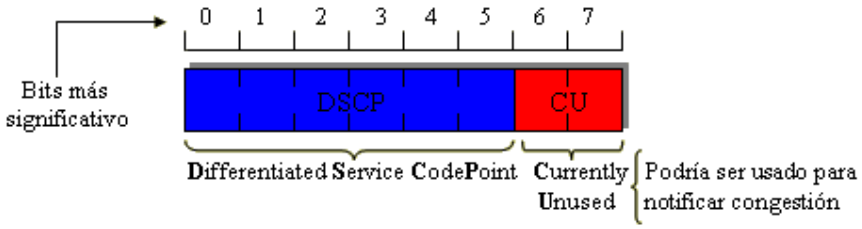


Figura 1.2.14.6.3 Campo DS en IPv4/IPv6 actual

Fuente: (Chafla, 2003)

La asignación de valores para el campo DSCP y el recomendado es como aparece en la figura No. 1.2.14.6.4

111110	Reservado (routing y control)
111100	Reservado (routing y control)
111010	Reservado (routing y control)
111000	Reservado (routing y control)
110110	Reservado (routing y control)
110100	Reservado (routing y control)
110010	Reservado (routing y control)
110000	Reservado (routing y control)
101110	Expedited (Premium)
101100	Configurable por el usuario
101010	Configurable por el usuario
101000	Configurable por el usuario
100110	Assured Clase 4 Preced. Alta
100100	Assured Clase 4 Preced. Media
100010	Assured Clase 4 Preced. Baja
100000	Configurable por el usuario

011110	Assured Clase 3 Preced. Alta
011100	Assured Clase 3 Preced. Media
011010	Assured Clase 3 Preced. Baja
011000	Configurable por el usuario
010110	Assured Clase 2 Preced. Alta
010100	Assured Clase 2 Preced. Media
010010	Assured Clase 2 Preced. Baja
010000	Configurable por el usuario
001110	Assured Clase 1 Preced. Alta
001100	Assured Clase 1 Preced. Media
001010	Assured Clase 1 Preced. Baja
001000	Configurable por el usuario
000110	Configurable por el usuario
000100	Configurable por el usuario
000010	Configurable por el usuario
000000	Best Effort (default)

Figura 1.2.14.6.4 Valores Estandarizados para DSCP

Fuente: (Felici, 2012)

1.2.14.7. Condicionadores de tráfico[88]

"Altera los paquetes para que cumplan las reglas de los servicios. Rinden, por lo tanto, funciones sofisticadas de etiquetado, modelado y monitorización. Normalmente se trata de los routers de acceso a la red. El funcionamiento de los PHBs o comportamiento por salto en los encaminadores, cómo se clasifican, marca y condiciona el tráfico en los mismos de acuerdo a unos criterios de política predeterminados son las características principales. El tráfico será marcado y encaminado de acuerdo a las marcas."[89]

1.2.14.7.1. Clasificación de tipos de routers en redes DIFF-SERV

[88] (DocShare, 2015)
[89] (DocShare, 2015)

- **First Hop Router:** es el router más próximo al host emisor de paquetes. Los flujos de paquetes son clasificados y marcados acorde a la etiqueta SLA. Es responsable de que el tráfico esté acorde con el ancho de banda del perfil.
- **Ingrees Router:** se sitúan en los puntos de entrada al backbone DiffServ (dominio DS), efectuando la clasificación de los paquetes en base al campo DS o en base a múltiples campos de la cabecera de éstos.
- **Egress Router:** se ubican en los puntos de salida de redes DiffServ (dominio DS), controlando el tráfico. Efectúan la clasificación de paquetes en base solo al campo DS de las cabeceras.
- **Interior router:** tienen la misión de «sumar» flujos, realizar la clasificación DS y reenvió de paquetes. Se sitúan dentro del backbone DS (dominio DS).

En la versión 4 de IP (Ipv4) se emplea, como ya antes se dijo, el campo ToS o *Type of Service* en la cabecera,

que posibilita «marcar» cada paquete en base a cuatro tipos de servicios, a saber:

- Mínimo costo económico.
- Máxima fiabilidad.
- Máximo *throughput.*
- Mínimo retardo.

Sin embargo, este byte prácticamente no ha sido utilizado, pues los *routers* no procesaban esta información, además, con igual resultado se empleaban los bits de prioridad. No obstante, es una posibilidad de obtener diferentes grados de QoS en IPv4, y puede emplearse como byte DS en redes DiffServ. Tanto IntServ como DiffServ están en fase de experimentación, y ambas soluciones están basadas en modelos opuestos, en DiffServ la QoS es controlada por el emisor y en IntServ la QoS se controla por el receptor. Ahora bien, dadas las mejores características en cuanto a escalabilidad y grado de generación de tráfico de señalización que presenta la solución DiffServ, ésta se vislumbra como la mejor oferta para cubrir el sector *backbone*. Y de cara a las redes de acceso al *backbone*, parece ser lo más adecuado la

solución IntServ. No obstante, todavía no se puede afirmar lo anterior categóricamente.

1.2.14.8. Tipos de servicio en DIFFSERV

En la Tabla No. 1.2.14.8.1, se presenta un resumen de los tipos de servicios y reparto de recursos para el protocolo Diffserv.

Servicio	Características	Equivalencia en ATM
'Expedited Forwarding' o 'Premium'	▪Es el que da más garantías. Equivale a una línea dedicada ▪Garantiza Caudal ⇨ Tasa de pérdidas, retardo y jitter muy bajos ▪Valor 101110 en DSCP	CBR VBR-rt
'Assured Forwarding'	▪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	VBR-nrt
'Best Effort' con prioridad	▪Sin garantías, pero obtendrá trato preferente frente a 'best effort sin prioridad'	ABR
'Best Effort' sin prioridad	▪Ninguna garantía, obtiene solo las migajas	UBR

Tabla 1.2.14.8.1 Tipos de Servicios Diffserv

Fuente: (Ardao, Abril 2005)

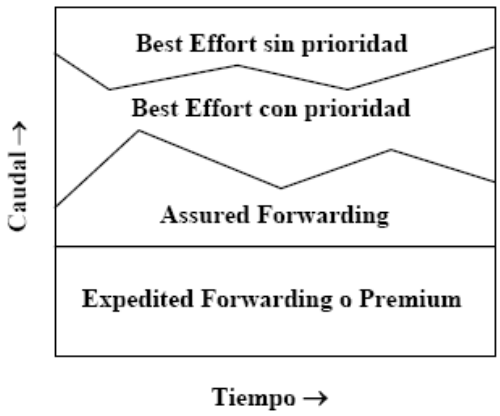


Figura 1.2.14.8.2 Reparto de Recursos en Diffserv

Fuente: (Ardao, Abril 2005)

1.2.14.9. Fundamentos de QoS en servicios diferenciados

- Principio 1: Diferenciación de los tipos de tráfico
- Principio 2: Aislamiento y tratamiento diferenciado de los tipos de tráfico
- Principio 3: Alta utilización de recursos
- Principio 4: Control de admisión de tráfico

1.2.15. Protocolos con uso de QoS

Primeramente hay que saber que los protocolos para redes tanto LAN como WAN, como por ejemplo Frame Relay y ATM que son los más usados fueron diseñados bajo el modelo de Datagrama donde los paquetes son tratados de manera independiente. ATM es una tecnología de capa de vínculo que ofrece un tratamiento del tráfico de alta calidad. ATM divide los paquetes del mismo tamaño en celdas de capa de vínculo y, a continuación, se envían a la cola y se controlan con los algoritmos de administración de cola adecuados para uno o varios servicios ATM. Los paquetes o celdas contienen información básica lo que hacía que los envíos por los routers sean eficientes, el gran problema es que no se puede clasificar tráfico según las características de uso. En cambio con Frame Relay los paquetes tiene diferentes tamaños por lo que permite un eficaz envió, los routers escogen la mejor ruta, además tiene manejo de errores y utiliza PVC, pero igualmente el problema era la clasificación de tráfico y

optimización de recursos. Su evolución genera aplicaciones de tiempo real y multimedia que no se adaptan fácilmente al modelo de Datagrama, la fiabilidad y robustez ya no son suficientes. Las redes solo constaban de un servicio que es el de Best Effort o mejor esfuerzo pero que no brindaba garantías. Las redes sin QoS se basaban en el ancho de banda y Buffers, los paquetes se enviaban tan pronto como se generaban, en cambio en redes con QoS existe asignación de recursos y control de admisión fundamentalmente. Aparece el control de asignación con el protocolo TCP a través del uso de la ventana deslizante para el control de flujo y la modificación del Stack del TCP para comportamientos diferentes. Posteriormente es lo que aparece Diffserv e IntServ con RSVP. Sin embargo existieron algunos inconvenientes como problemas de escalabilidad, SLA, señalización en aplicaciones cortas, asignación de recursos, etc.; por lo que se plantean la creación de nuevas redes y protocolos con el uso de QoS basándose en la optimización de recursos (utilización y asignación) y aparece MPLS que fue concebido como una alternativa a IP sobre ATM en el año de 1997. También aparecen una serie de protocolos y aplicaciones, algunas de estas integradas a los sistemas operativos que permiten operar y administrar QoS. Actualmente redes FR y ATM utilizan QoS con una serie de protocolos adicionales. A continuación se menciona los más importantes.

1.2.15.1. Multi Protocol Labeling Switching (MPLS): Conmutación de etiquetas multiprotocolo[90][91]

"Proporciona la posibilidad de administrar el ancho de banda de la red a través de etiquetas en las cabeceras de los paquetes llamado también encapsulamiento y de encaminadores específicos capaces de reconocerlas. El Multiprotocolo de etiquetado de conmutación MPLS es un estándar emergente del IETF que surgió para consensuar diferentes soluciones de conmutación multinivel, propuestas por distintos fabricantes a mitad de los 90. Cisco ha sido una empresa pionera al proporcionar una solución pre-estandarizada MPLS a la conmutación por etiquetas. Las implicaciones que supone su implementación real son enormemente complejas. Según el énfasis o interés que se ponga a la hora de explicar sus características y utilidad, MPLS se puede presentar como un sustituto de la conocida arquitectura IP sobre ATM. También como un protocolo para hacer túneles sustituyendo a las técnicas habituales de "tunneling". O bien, como una técnica para acelerar el encaminamiento de paquetes... incluso, ¿para eliminar por completo el routing? En realidad, MPLS hace un poco de todo eso, ya que integra sin discontinuidades los niveles 2 (transporte) y 3 (red), combinando eficazmente las funciones de control del routing con la simplicidad y rapidez

[90] (Diaz, 2009)
[91] (DocShare, 2015)

de la conmutación de nivel. Se deberá considerar MPLS como el avance más reciente en la evolución de las tecnologías de routing y forwarding en las redes IP, lo que implica una evolución en la manera de construir y gestionar estas redes, las redes IP que se verá en el próximo milenio. Los problemas que presentan las soluciones actuales de IP sobre ATM, tales como la expansión sobre una topología virtual superpuesta, así como la complejidad de gestión de dos redes separadas y tecnológicamente diferentes, quedan resueltos con MPLS. MPLS ofrece nuevas posibilidades en la gestión de backbones, así como en la provisión de nuevos servicios de valor añadido. MPLS usa, básicamente, un esquema de etiquetado del tráfico hacia delante: el tráfico es marcado en su entrada a la red pero no en los puntos de salida. Reside únicamente en los routers y es independiente del protocolo utilizado, de ahí lo de "multiprotocol", lo que permite que pueda ser utilizado sobre otros protocolos distintos a IP, como IPX, TME, PPP, Ethernet, Frame Relay, sobre SONET y Token Ring. Este protocolo combina algunas de las prestaciones de las redes orientadas a la conexión con las de las redes sin conexión. Permite a un router o a un conmutador asignar una etiqueta a cada una de las entradas de la tabla de routing y comunicar esa etiqueta a los routers y conmutadores vecinos. Cuando uno de estos dispositivos pasa un paquete al más próximo, el router o

el conmutador añade a ese paquete una etiqueta asociada con la entrada de tabla de routing. La etiqueta permite al router o conmutador identificar el próximo salto o saltos sin mirar la dirección. La idea es, por tanto, posibilitar que los paquetes etiquetados fluyan de extremo a extremo sin forzar a los routers o conmutadores a mirar las direcciones.

1.2.15.2. Operación del MPLS

El funcionamiento básico de MPLS se lo presenta a continuación en la figura No. 1.2.15.2.1

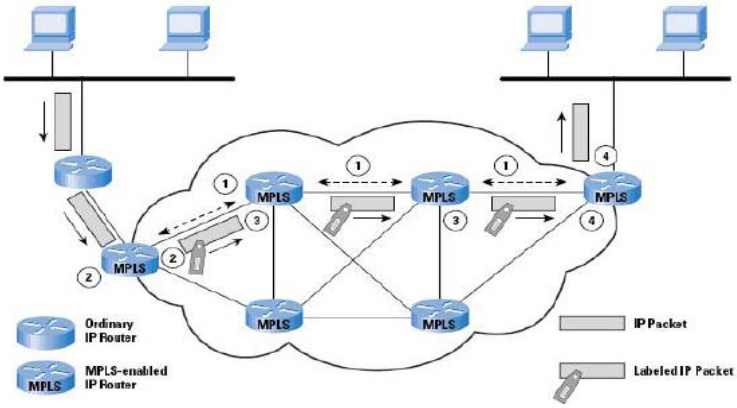


Figura 1.2.15.2.1 Operación del MPLS

Fuente: (Diaz, 2009)

1.2.15.3. Formato de las etiquetas

Cada paquete MPLS tiene una cabecera que contiene 20 bits para etiquetado, un campo de 3 bits para especificar la Clase de Servicio (CoS), 1 bit que funciona como indicador de etiquetas

y un campo de 8 bits que indica el tiempo de vida o Time-to-live (TTL).”[92]

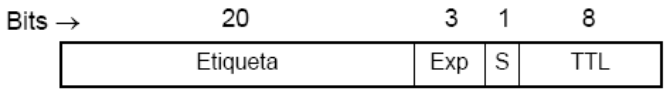


Figura 1.2.15.3.1 Formato de las etiquetas MPLS

Fuente: (Diaz, 2009)

El campo **Etiqueta** es el que utilizan los routers MPLS para decidir por donde encaminar el paquete. Todos los paquetes que recibe un router por una interfaz dada con la misma etiqueta pertenecen a la misma FEC.

FEC (Forwarding Equivalence Class): Conjunto de paquetes que entran en la red MPLS por la misma interfaz, que reciban la misma etiqueta y por lo tanto siguen la misma ruta a lo largo de la red MPLS. Normalmente se trata de datagramas que pertenecen a un mismo flujo origen-destino. No obstante aunque un mismo flujo no puede pertenecer a más de una FEC, una FEC si puede agrupar varios flujos.

- El campo **Exp** no tiene definida una función en la norma. Se prevé que pueda utilizarse para transmitir información sobre el paquete que deba ser conocida por los routers MPLS. Una propuesta es él envió de información QoS para Diffserv que permita a los

[92] (DocShare, 2015)

routers saber el nivel de prioridad que tiene cada paquete o que PHB utilizar.

- Las etiquetas pueden anidarse, formando una pila añadiéndose de derecha hacia arriba a izquierda hacia abajo. Esto permite ir agregando o segregando flujos. El campo **S** indica (cuando vale 1) que se trata de la última etiqueta en la pila. En el caso de haber más de una etiqueta MPLS todas tendrán a cero el campo S salvo la última.
- El campo **TTL** cumple una función equivalente al de IPv4. Cuando el paquete recibe una etiqueta nueva en el router MPLS de entrada, el campo TTL hereda el valor del datagrama IP reducido en una unidad. En el router MPLS de salida, el campo TTL de la etiqueta se traslada al campo TTL del datagrama IP. En el caso de redes ATM y Frame Relay no se utiliza. Durante el viaje del paquete por la red MPLS el campo TTL de la etiqueta disminuye en uno por cada salto. Si en algún momento el TTL vale 0 el paquete es descartado. Si hay etiquetas apiladas, solo cambia el TTL de la etiqueta situada más arriba más a la izquierda). Cuando se añade una etiqueta, esta hereda el valor de la inferior; cuando se quita, pasa su valor menos uno a la de abajo.

1.2.15.4. Situación de las etiquetas MPLS

- MPLS funciona sobre multitud de tecnologías de nivel de enlace: PPP, LANs, ATM o FR.
- La etiqueta MPLS se coloca antes del paquete IP y tras la cabecera de nivel de enlace.
- El router sabe que tras una etiqueta MPLS con S=1 se encuentra el paquete de red.

1.2.15.5. Situación de las etiquetas MPLS para redes LANS

En la figura No. 1.2.15.5.1, se puede apreciar el formato de la etiqueta MPLS, en donde el campo Pila de etiquetas se encuentra antes que la cabecera debido a que el paquete antes de ingresar a un host debe ser encaminado por los routers a través de este etiquetado, obviamente después de realizar la resolución de nombres con MAC.

Figura 1.2.15.5.1 Formato de la etiqueta MPLS para redes LAN

Fuente: (Diaz, 2009)

1.2.15.6. Elementos de MPLS y su funcionamiento[93]

[93] (DocShare, 2015)

“Dentro de la terminología de las redes MPLS se va a oír hablar mucho del LSP y del LSR.

- **Label Switched Paths (LSP):** Es el protocolo que utiliza MPLS para la distribución de etiquetas. Está incluido dentro de un protocolo genérico denominado Label Distribution Protocol (LDP). Un LSP es similar a un circuito virtual en ATM y es, además unidireccional, desde el emisor hasta el receptor.
- **Label Switched Router (LSR):** Es el tipo de routers que permiten MPLS. Los MPLSs miran la escritura de la etiqueta asociada a un paquete entrante, y la utilizan como índice en un vector para determinar la conexión de salida a la cual el paquete debe ser remitido. El LSR entonces asignará típicamente una nueva escritura de la etiqueta y remitirá el paquete en la conexión de salida. Cada paquete es remitido salto a salto a través de la red de MPLS, tan solo con escribir en la etiqueta en cada nodo LSR.

Mientras que cada escritura de la etiqueta tiene significación local solamente es decir, puede ser diferente en cada conexión, el efecto es crear un camino extremo a extremo a través de la red de MPLS. Observe que la red de MPLS no encamina el tráfico basado en los direccionamientos IP del paquete, ni

encamina basándose en la información del ATM VCI/VPI o identificador del circuito virtual o del camino. Así una red abarcada de nodos de LSR no es una red IP o una red ATM -- es una nueva y diversa red de MPLS. Una de las capacidades que hace MPLS especial es que el primer MPLS LSR en la red es decir, el nodo del ingreso de MPLS, puede establecer una ruta explícita a través de la red de MPLS; el nodo del ingreso puede especificar exactamente qué secuencia de MPLS LSRs y conexiones se debe utilizar para diversos tipos de tráfico para alcanzar cada destino.

Las rutas explícitas de MPLS se pueden elegir en respuesta a muchos y diversos criterios, incluyendo cargas del tráfico de la red, anchura de banda disponible, costos administrativos, retardo del camino, la variación del retardo o inquietud, la cuenta del salto, la relación de transformación de la pérdida de la célula, etc. Esta capacidad, a veces llamado "constraint-based routing" como un sobre conjunto del encaminamiento de QoS, es inexistente en los routers IP, la mayoría de los cuales utilizan solamente la métrica del camino más corto para calcular las rutas y su comportamiento está limitado al salto-a-salto. Con este tipo de encaminamiento o constraint based routing y las rutas explícitas, las redes de MPLS se pueden diseñar para resolver muchas métricas de calidad del servicio, haciéndolas ideales para las redes troncales de los ISPs. El

nodo del ingreso de la red de MPLS tiene que ser bastante inteligente para clasificar el tráfico y determinar el camino apropiado (LSP) para cada flujo; este nodo de ingreso aplica la misma escritura de la etiqueta a todos los paquetes con el mismo nivel de QoS y los envía al mismo nodo de salida de MPLS. Sin embargo, esta opción no tiene por qué ser realizada por todos los nodos de la red MPLS; algunos sencillamente marcan las etiquetas y las reexpiden.

1.2.15.7. Elementos claves para la operación del MPLS

Como se puede ver en la figura No. 1.2.15.7, la interacción de los LSP son en cada segmento de la red, por otra parte el LSR controla como un filtro controlando el ingreso de las etiquetas.

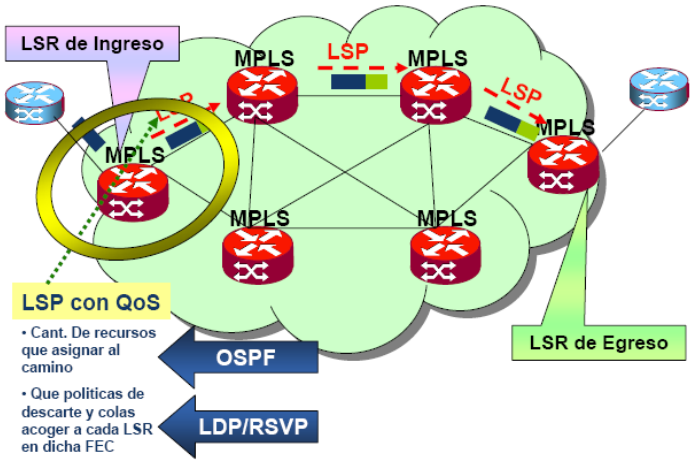


Figura 1.2.15.7.1 Elementos claves MPLS

Fuente: (Diaz, 2009)

1.2.15.8. Principales Aplicaciones de MPLS

Las principales aplicaciones que hoy en día tiene MPLS son:

- Ingeniería de tráfico
- QoS
- Redes de alto rendimiento
- Soporte multiprotocolo
- Diferenciación de niveles de servicio mediante clases (CoS).
- Servicio de redes privadas virtuales (VPN)

1.2.15.9. Conclusiones de MPLS

Podrían resumirse las características más importantes de MPLS en las siguientes:

- MPLS es la manera más eficaz de integrar redes IP y ATM en la misma red.
- MPLS reduce los gastos indirectos de proceso en los routers IP, mejorando el funcionamiento de la expedición de paquete.
- MPLS es otra manera de proporcionar QoS en las espinas dorsales de la red (backbone), compitiendo con otros protocolos tales como DiffServ, IntServ/RSVP y ATM QoS.
- MPLS es superior a IP en la manera en que encamina tráfico, basando decisiones de encaminamiento en algo más que calcular el camino más corto.

- Un PHB particular puede ser asignado a una determinado FEC.
- Algunos paquetes pueden pertenecer a los mismos puntos finales pero también pueden pertenecer a diferentes FECs.
- MPLS será la mejor manera para que los proveedores de servicio ofrezcan VPNs que permitan medir la calidad de servicio del cliente.
- MPLS permitirá a los ISPs escalar sus redes y que resuelvan requisitos de la ingeniería del tráfico sin tener que recurrir a redes ATM.
- El FEC de los paquetes se puede especificar por varios parámetros, tales como:
    - Dirección IP destino o fuente
    - Puerto destino o fuente
    - ID de protocolo
    - Punto de código de servicios diferenciados
    - Etiqueta de flujo de Ipv6

Su aplicación es mayoritariamente en redes WAN. MPLS es, por tanto, una técnica con futuro, pues se trata una técnica prometedora para integrar las redes ATM e IP, siguiendo las tendencias generales de convergencia de redes que se suceden en la industria de hoy.

1.2.16. Subnet Bandwidth Management (SBM): administración del ancho de banda de la subred 802.1P[94]

Es un protocolo de señalización que permite la comunicación y coordinación entre los distintos nodos de la red, definiendo cómo relacionar los distintos protocolos de QoS superiores con las diferentes tecnologías de capa 2 o de enlace en el modelo OSI. Ha sido desarrollado para aplicarlo con LANs IEEE. Hasta ahora se ha estudiado cómo obtener QoS extremo a extremo entre el emisor y el receptor, esto significa que cada router a lo largo de la ruta debe soportar la tecnología de QoS que se esté usando, tal y como se vio en la descripción de los anteriores protocolos de QoS, pero también hay que tener en cuenta la posibilidad de conseguir QoS en los nodos finales conocido como top-to-bottom. Para ello es necesario que:

- Los host emisor y receptor deben permitir la obtención de QoS, siendo necesario que las aplicaciones la permitan explícitamente o, en su nombre, que lo permita el sistema implícitamente. Cada capa OSI, desde la de aplicación a capas inferiores, deben utilizar también QoS para asegurar que las peticiones de alta prioridad sean tratadas desde el host.
- Suponiendo que los sistemas finales se conecten a una red de área local, éstas deben permitir QoS, de forma que las tramas de alta prioridad sean tratadas primeramente mientras circulan por la red como por ejemplo de host-a-host, host-a-router o

[94] (Pérez, 2003)

router-a-router. De esta forma se está proporcionando QoS en la capa 2 de OSI, capa de enlace, mientras que los protocolos anteriores ofrecían QoS en otras capas: Diffserv en la capa 3 y RSVP y MPLS en capas superiores.

Existen algunas tecnologías creadas para proporcionar QoS en la capa de enlace, como ATM, pero ésta es una tecnología imposible de implementar por algunas empresas, debido a su coste económico y a su complejidad. Todas estas empresas, por el contrario, utilizan otras tecnologías más comunes para sus LANs, tales como Ethernet, que originalmente no fueron diseñadas para ofrecer QoS. Ethernet proporciona, simplemente, un servicio análogo al prestado por IP, el servicio Best Effort, en el que existe la posibilidad de que se produzcan retardos y variaciones que pueden afectar a aplicaciones de tiempo real. Por todas estas cosas, IEEE ha redefinido el estándar Ethernet y otras tecnologías de la capa de enlace para proporcionar QoS, mediante diferenciación de tráfico.

Los estándares de IEEE 802.1p, 802.1q y 802.1D definen cómo los conmutadores Ethernet pueden clasificar las tramas para poder entregar en primer lugar el tráfico considerado crítico. El grupo de trabajo del IETF para la especificación de las capas de conexión (ISSL) se encarga de definir cómo relacionar los distintos protocolos de QoS de capas superiores con las diferentes tecnologías de la capa 2, como Ethernet. Entre otras cosas, el ISSL ha desarrollado el protocolo

Subnet Bandwidth Manager (SBM) o “Gestión del ancho de banda de la subred” para aplicarlo con LANs 802. SBM es un protocolo de señalización que permite la comunicación y coordinación entre nodos de la red y su relación con protocolos de QoS de capas superiores. Un requisito fundamental en SBM es que todo el tráfico debe pasar por lo menos por un conmutador que utilice SBM.

1.2.16.1. Componentes de SBM

Los principales componentes de SBM son:

- **Distribuidor de ancho de banda (Bandwidth Allocator, BA):** gestiona la asignación de los recursos y realiza el control de admisión de acuerdo a su disponibilidad y al resto de criterios definidos en la política de servicio.
- **Módulo del cliente (Requestor Module, RM):** reside en cada estación final. La relación entre el RM y los parámetros de protocolos de QoS superiores son definidas de acuerdo a una política determinada. La localización del BA determina el tipo de configuración de SBM en uso: centralizado o distribuido. Además, cuando existe más de un BA por segmento de red, uno de ellos será elegido como SBM (Designated SBM o DSBM).

1.2.16.2. Funcionamiento

Este protocolo utiliza un mecanismo de señalización entre RM y BA para iniciar las reservas, consultar al BA los recursos disponibles y cambiar las reservas. Este mecanismo suele ser RSVP. Para comprobarlo, se tomara como ejemplo cómo se realiza de forma genérica el procedimiento del control de admisión en SBM:

- El DSBM inicializa: consigue la disponibilidad de los recursos.
- El cliente DSBM que puede ser cualquier host o router RSVP busca el DSBM. Esta tarea esta monitorizada con el campo "AllSBMAddress", estando reservada como dirección IP multidifusión la 224.0.0.17.
- El cliente envía un mensaje PATH con el campo "DSBMLogicalAddress".
- Una vez recibido el PATH, el DSBM indica su estado en el conmutador, almacenando la dirección de origen de capa 2 y capa 3 (L2/L3) y la pone en el mensaje, encaminándolo al próximo conmutador. Cuando el mensaje es un RSVP RESV, éste se envía hasta llegar al primer encaminador. DSBM evalúa la petición y si los recursos solicitados están disponibles se lo indica al emisor.

Es, como se aprecia, un proceso muy parecido al ocurrido en los routers RSVP. Por otro lado, cualquier DSBM puede añadir un objeto denominado TCLASS a los mensajes Resv o Path del protocolo RSVP. Este objeto contiene información de prioridad basada en la norma 802.1p. De esta manera la información de clase de servicio de las redes IEEE 802 puede ser transmitida por la red.

1.2.17. 802.1P[95]

Estándar integrado dentro de la norma 802.1D (LAN's con puentes) que permite dar prioridad al tráfico y filtrar el tráfico Multicast de forma dinámica. Puede diferenciar entre 8 tipos de clases de tráfico clasificados como "prioridades de usuario" por cada puerto (actuando a nivel 2). 802.1p"[96] es un mecanismo de control del tráfico de acumulación apropiado para el uso en muchas redes de área local. Define un campo en el encabezado de acceso al medio (MAC) de los paquetes Ethernet, que puede transportar uno de los ocho valores preferentes. Los hosts o los enrutadores que envía tráfico a una LAN marcan cada paquete transmitido con el valor de preferencia adecuado. Los dispositivos LAN, tales como modificadores, puentes o concentradores deben tratar los paquetes de forma adecuada. El ámbito de la marca de preferencia 802.1p está limitado a la LAN.

[95] (Jacobs, Seminario de Calidad de Servicio en Redes Multimedia, 2011)
[96] (DocShare, 2015)

1.2.18. IP PRECEDENCE

IP Precedente es el campo original en el header IP que tiene tipos de servicio (TOS) en IP v.4 (8 bits), y es redefinido para su utilización en DiffServ.

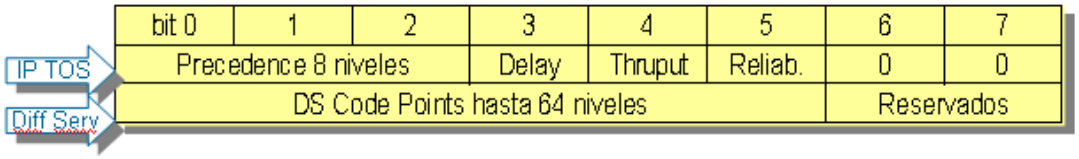


Figura 1.2.18.1 Formato IP Precedence

Fuente: (Jacobs, Seminario de Calidad de Servicio en Redes Multimedia, 2011)

1.2.19. POLICY-BASED ROUTING: PBR

También conocido por Layer 4 switching, provee políticas de ruteo basadas en definiciones del administrador de red, convierte a las políticas en el comportamiento de la red

Además permite:

- Balance de carga
- Políticas horarias
- Políticas de seguridad
- Políticas tarifarías
- Políticas de backup

Ítems de decisión:

- MAC address (nivel 2)

- Dirección IP o subred IP (nivel 3) origen y destino
- TCP/UDP port number (nivel 4)
- URL Uniform Resource Locator (nivel de aplicación)
- TOW (Time of Week)

1.2.20. SERVER DE CONTROL DE QoS

Administra en forma centralizada las políticas de QoS, resulta complejo administrar todo configurando cada equipo, por lo que se centraliza en este server. Las políticas definen que tráfico es prioritario y esto puede ser dinámico, cambiando para distintas horas del día. El server genera los comandos necesarios para cada Terminal. También se caracteriza por el COPS: Common Open Policy Service del IETF, per-flow protocol. Usan SNMP y/o LDAP (Lightweight Directory Access Protocol) para distribuir las políticas. Está restringido a redes corporativas y no es escalable a un backbone público

1.2.21. ISSLOW y otros

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

Se han definido otros mecanismos de control del tráfico para diversos medios, incluidos módems por cable, plantas coaxiales de fibra híbrida (HFC), P1394, etc.

1.2.22. Arquitectura del QoS[97]

"A continuación, varias de las posibles arquitecturas que se pueden dar de calidad de servicio mediante la utilización simultánea de varios de los protocolos citados anteriormente.

Excepto para el caso de SBM que utiliza RSVP para la señalización, para el resto de protocolos se estudió cómo actuaban de forma independiente extremo a extremo; sin embargo, en la realidad se utilizan varios de estos protocolos para la obtención de QoS extremo-a-extremo y en los nodos finales, conformándose varias arquitecturas de QoS de las que se van a describir las más utilizadas:

- **RSVP Y Diffserv Extremo a Extremo:** RSVP proporciona recursos para el tráfico de la red, mientras que Diffserv simplemente marca y prioriza el tráfico. RSVP es más complejo y demanda más actividad a los routers que Diffserv, por eso, normalmente se utiliza DiffServ en el backbone. A pesar de todo, Diffserv y RSVP se complementan perfectamente para ofrecer QoS extremo a extremo. Los hosts finales pueden utilizar peticiones RSVP con alta granularidad.

[97] (DocShare, 2015)

Los routers situados a la entrada de la espina dorsal de la red pueden asociar esas reservas RSVP a una determinada clase de servicio, indicada por un byte DS y acordada en los acuerdos de servicios (SLAs).

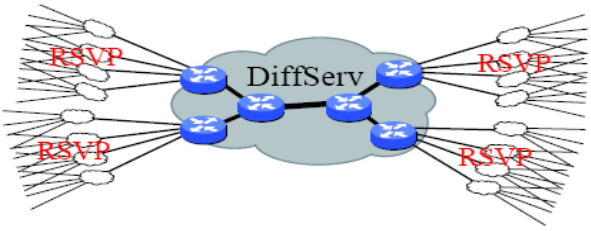


Figura 3.12.1 Combinación de RSVP y DiffServ

Fuente: (Martin, 2011)

En la periferia de la red el uso de RSVP no plantea problemas y puede ser necesaria la reserva estricta de recursos. En este caso el router que conecta con el core 'traducirá' la petición al servicio DiffServ más parecido.

- **MPLS para RSVP:** Existe una propuesta del IETF de usar un objeto en RSVP, denominado, EXPLICIT_ROUTE, para predeterminar caminos que puedan ser usados por flujos de RSVP. Estos flujos usan tuberías virtuales establecidos a través de routers MPLS. Incluso sin el citado objeto, es posible para MPLS asignar etiquetas de acuerdo al campo flowsepc de RSVP.
- **MPLS para Diffserv:** Al ser DiffServ y MPLS similares, asociar el tráfico DiffServ sobre tuberías MPLS (LSPs) es bastante sencillo. Para soportar el modelo de DiffServ, un

operador de red MPLS necesita asignar una serie de recursos para cada clase Diffserv transmitida en cada router MPLS y asignar, a su vez, etiquetas."[98]

1.2.23. Modelo conceptual de QoS[99]

Como se puede ver en la figura No. 1.2.23.1, se divide en 3 partes, la primera consta sobre la administración de QoS en donde se utiliza políticas para los servidores como políticas de control, admisión de control especialmente para los usuarios y aplicaciones; también mediante aplicaciones se puede administrar operar y control el tráfico; además del monitoreo, manejo de cuentas y operaciones de usuarios y muy importante lo que es la administración de recursos como por ejemplo el ancho de banda.

Con respecto a la señalización, control y transporte se encargan los protocolos ya mencionados como son el IP Diffserv, IP ToS, RSVP, MPLS, Remote Transport Protocol (RTP), y Remote Transport Control Protocol (RTCP) y las aplicaciones de gestión de tráfico como por ejemplo Ethereal. En la última división se tiene el manejo de los paquetes, como se menciona el clasificador de paquetes, luego los paquetes se dirigen al manejador de congestión y tráfico donde se determina que paquetes son enviados antes que otros en base a varios parámetros, y por último los paquetes llegan al programador de

[98] (DocShare, 2015)
[99] (Martin, 2011)

Paquetes en donde se basa en criterios como ancho de banda, priorización, mejor esfuerzo.

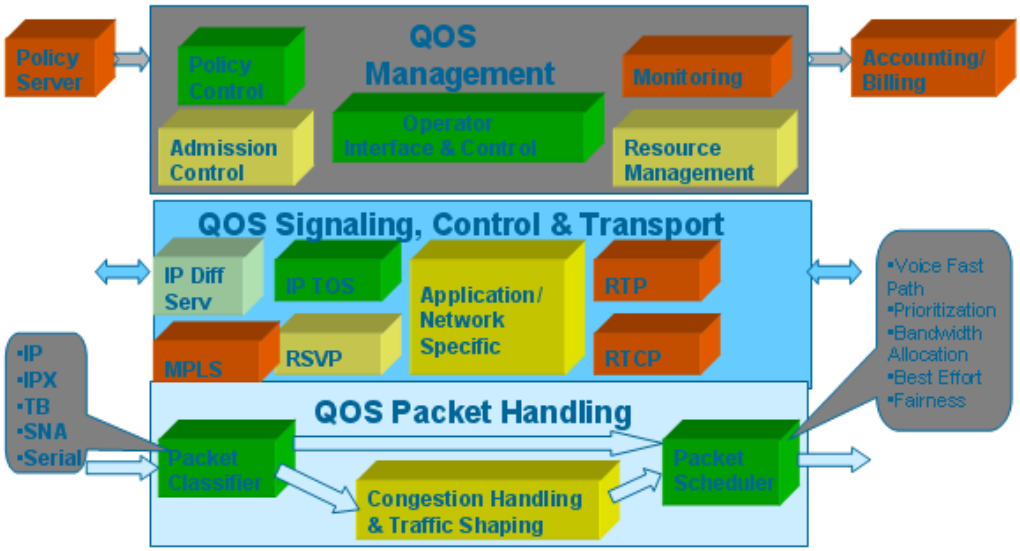


Figura 1.2.23.1 Modelo conceptual QoS

Fuente: (Martín, 2012)

1.2.24. Capas del QoS

La estructura de las capas está ordenada y agrupada según los tipos de protocolos, consta de 4 niveles y uno de Aplicación. En el primer nivel constan el protocolo Asymmetric Digital Subscriber Line (ADSL), Jerarquía digital síncrona (SDH), Multiplexación por división de longitud de onda (WDM), Multiplexación por división de tiempo (TDM) y el protocolo 802.3; en este nivel se encarga del tipo de conexiones, ancho de banda, velocidad de transmisión, etc. En el

nivel 2 tiene la capa de red o tipo de redes en la cual constan Frame Relay, Modo de Transferencia Asincrónico (ATM), Point to Point Protocol (PPP), High-Level Data Link Control (HDLC) y el protocolo donde se puede configurar con prioridades el 802.1P/Q. En el nivel 3 consta únicamente del protocolo IP que se encarga de realizar la clasificación de paquetes, el marcado, priorización, señalización. El nivel 4 se encarga del transporte con los protocolos TCP y UDP, los ACK, PDU, MTU, duplicaciones, retardos, segmentos perdidos, etc.; y por último se tiene la capa de Aplicación. Se puede ver en la figura No. 3.14.1 (Pino, 2016), la QoS relativa se lo aplica en la en los protocolos 802.3 y 802.1 P/Q, en el resto de protocolos con una configuración debidamente realizada se puede obtener QoS absoluta a excepción de los protocolos SDH, WDM, PPP y HDLC que también se puede tener QoS con servicio de mejor esfuerzo.

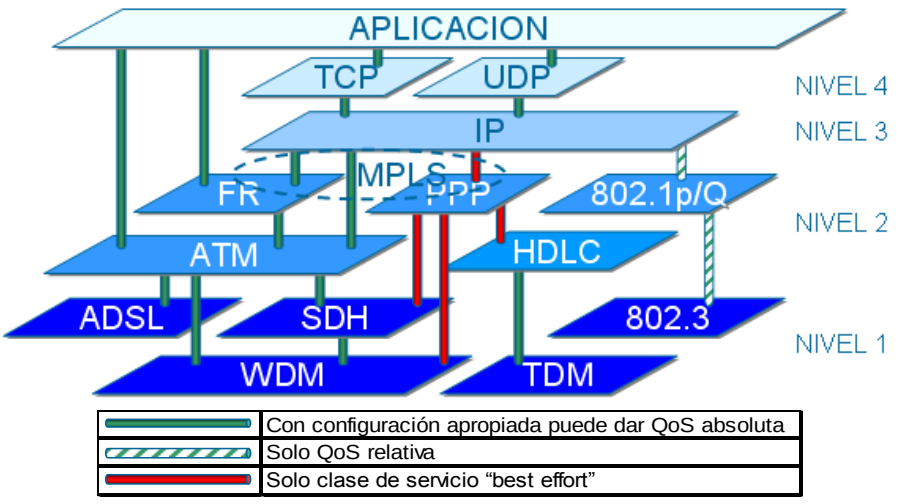


Figura 1.2.24.1 Capas y QoS

Fuente: (Martín, 2012)

1.3 ESTANDARES[100]

1.3.1. IEEE (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS)

IEEE corresponde a las siglas de The Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros de telecomunicaciones, ingenieros electrónicos, Ingenieros en informática. A través de sus miembros, más de 360.000 voluntarios en 175 países, el IEEE es una autoridad líder y de máximo prestigio en las áreas técnicas derivadas de la eléctrica original: desde ingeniería computacional, tecnologías biomédica y aeroespacial, hasta las áreas de energía eléctrica, telecomunicaciones y electrónica de consumo, entre otras.

1.3.1.1. IEEE 802.1D

1990 (IEEE Standard for local and metropolitan área networks: mediaaccess control (MAC) bridges): Este Standard, define una arquitectura para la interconexión del IEEE 802 de redes de área local bajo el nivel de servicio MAC, transparente para LLC y altas capas de protocolos.

[100] (IEEE, 2016)

1.3.1.2. IEEE 802.1Q

2003 (IEEE standards for local and metropolitan area networks. Virtual bridged local área networks): Proceso para desarrollar un mecanismo que permite múltiples puentes de red ser transparentes compartiendo la misma red física enlazada sin información adicional entre las redes. IEEE 802.1Q también define el significado de una LAN Virtual LAN o VLAN con respecto a un especifico modelo conceptual sobreponiendo los puentes en la capa MAC y el IEEE 802.1D. Además IEEE 802.1Q define GVRP, una aplicación de Generic Attribute Registration Protocol, permitiendo a los puentes negociar el conjunto de VLANs para ser truncados sobre una específica vía.

1.4 EQUIPOS

1.4.1. Herramientas

1.4.2. Aplicabilidad

La aplicabilidad de estas herramientas es grande en el campo de las redes, debido a que no solo abracan la calidad de servicio, también involucran campos como la ingeniería de tráfico, muy útiles también para realizar consultarías y auditorias, monitoreo de la red, etc. Cabe recalcar que las herramientas pueden ser utilizadas sobre diferentes dispositivos de red, es decir algunos ayudaran a analizar la transmisión de datos por el medio físico como cable por ejemplo, otras ayudaran sobre ciertas terminales, PCs, o servidores, y otras

específicamente en los routers, switches, Firewalls. Es decir las herramientas que pueden utilizarse son numerosas por lo tanto se hará referencia a algunas de estas.

1.4.3. Monitoreo y gestión de redes[101]

Estas son algunas de las herramientas más importantes para el monitoreo y gestión de la red. Algunas herramientas contienen servicios adicionales como pruebas de conectividad. Para la implementación de las soluciones de QoS se escogerán un par de estas herramientas para el monitoreo y la captura de datos. A continuación, las herramientas más importantes en el mercado y sus principales características.

[101] (Pino, 2016)
(NetLimiter, 2016)

NOMBRE	CARACTERÍSTICAS
TCP Dump	Tcpdump es una excelente herramienta que nos permite monitorizar a través de la consola de Linux todos los paquetes que atraviesen la interfaz indicada. A su vez, los múltiples filtros, parámetro y opciones que tcpdump nos ofrece, nos permite infinidades de combinaciones, al punto de poder monitorizar todo el tráfico completo que pase por la interfaz, como el tráfico que ingrese de una ip, un host o una página especifica, podemos solicitar el tráfico de un puerto especifico o pedirle a esta magnífica herramienta que nos muestre todos los paquetes cuyo destino sea una dirección MAC específica.
Wireshark	Wireshark es un sniffer que te permite capturar tramas y paquetes que pasan a través de una interfaz de red. Cuenta con todas las características estándar de un analizador de protocolos. Posee una interfaz gráfica fácil de manejar, permite ver todo el tráfico de una red (usualmente en una red Ethernet, aunque es compatible con algunas otras).
Hyperic	Aplicación open source que nos permite administrar infraestructuras virtuales, físicas y nube este programa auto-detecta muchas tecnologías.Cuenta con dos versiones una open source y una comercial Algunas de las características de esta aplicación son: Optimizado para ambientes virtuales que integran vCenter y vSphere Construido para funcionar en 75 componentes comunes tales como: base de datos, dispositivos de red, servidores de red, etc. Detecta automáticamente todos los componente de cualquier aplicación virtualizada
IPLOG	Detección de ataques externos Registra trafico TCP, UDP, ICMP Detección de escaneos
IPFILTER	Filtro de puertos Filtro de direcciones Filtro de paquetes TCP/IP
NAT	Explora Servicios NetBIOS Acceso a archivos con permiso del sistema Auditoria remota
NET LIMITER	Control de downloads/uploads Trafico de Internet Rangos de transmisión (aplicaciones simple conexión)
NETMETER	Trafico de Internet Medición de retardos y jitter Medición de ancho de banda
NAGIOS	Nagios es un sistema de monitorización que permite a cualquier empresa identificar y resolver cualquier error critico antes de que afecte los procesos de negocio. Esta aplicación monitoriza toda infraestructura de la información para asegurarse de que sistemas, aplicaciones, servicios y procesos de negocios estén funcionando correctamente. En el caso de un error la aplicación se encarga de alertar al grupo técnico para que rápidamente resuelvan el problema sin que afecte a los usuarios finales.
PANDORA FMS	Pandora FMS es un software de monitorización que otorga a cualquier empresa la posibilidad de monitorizar en un mismo panel redes, sistemas, servidores, aplicaciones y procesos de negocio. Debido a la posibilidad de monitorización bottom-up de Pandora FMS, el panel de monitorización permite personalizar los accesos por rol para que cada rol vea la información que le interesa.

Tabla N. 1.4.3.1 Herramienta para monitoreo de redes

1.4.4. Herramienta KYPUS

Como se mencionó anteriormente existen herramientas de software como de hardware para el análisis, administración y monitoreo de las redes para obtener una mejor calidad de servicio, pero el presente trabajo se enfocará en una herramienta de hardware especial debido a que esta hecho por una empresa Ecuatoriana. En Ecuador la oferta es

variada cuando se trata de combatir los ataques externos y en ésta se incluye también la empresa ecuatoriana Nova Devices con la tecnología denominada Kypus. A diferencia de la mayoría de soluciones de seguridad, Kypus fue desarrollada en Ecuador. Por el momento, muchas empresas e instituciones públicas en el país utilizan este sistema de seguridad, diseñado para proteger a las empresas de diversos ciberintrusos.

Estos equipos se clasifican en servidores y clientes y se denominan:

- Servidores: KYPUS SERVER APPLIANCE
- Clientes: KYPUS THIN CLIENT

1.4.4.1. KYPUS SERVER APPLIANCE[102]

1.2.4.1.1. Características

Figura 1.4.4.1.1.1 Equipo KYPUS KMSA

Fuente (KYPUS, 2015)

.4.4.1.1.1. Administración Centralizada

- ✓ Interfaz gráfica intuitiva, permite realizar configuraciones y cambios de forma rápida e instantánea, local o remota, de uno o varios KMSAs.

[102] (KYPUS, 2015)

- ✓ Fácil instalación por su arquitectura cliente servidor.
- ✓ Elimina el nivel de dependencia de personal especializado, disminuyendo el costo total de propiedad a corto mediano y largo plazo.
- ✓ Respaldo y recuperación de configuración de datos vía FTP, correo electrónico o servidor Windows.

.4.4.1.1.2. Seguridad

- ✓ Firewall Industrial de Hardware y Software con capacidad para edición de reglas en línea.
- ✓ Sistema operativo de embebido en una memoria flash de estado sólido (ROM) que lo hace seguro y eficiente.
- ✓ Seguridades predefinidas con actualizaciones automáticas. Alarmas SNMP.

.4.4.1.1.3. Gestión de Comunicaciones

- ✓ Control de Ancho de Banda dinámico, con capacidad para calendarizar el acceso.
- ✓ Permite controlar y establecer horarios para navegación, correo electrónico, respaldos y actualizaciones de forma automática.
- ✓ Integración de redes remotas mediante VPNs reduciendo el alto costo de enlace.

.4.4.1.1.4. Filtrado de Contenido

- ✓ Filtrado por extensiones, usuarios, IP`s, grupos de usuarios, redes y puertos.

- ✓ Aplicaciones (P2P, MSN, Aplicaciones de red.)
- ✓ Provisión y actualización de listas negras y listas blancas.

.4.4.1.1.5. Servidor de Correo

- ✓ Control de tamaño de correos.
- ✓ Soporte de múltiples dominios.
- ✓ Pasarela de correo a Exchange, Lotus, Zimbra, etc.
- ✓ Anti SPAM, Antivirus

.4.4.1.1.6. Estadística y Reportes gráficos

- ✓ Logs de auditoría.
- ✓ Uso de canal, navegación, correo, fecha, hora y tiempo de conexión.
- ✓ SPAM y Virus.

.4.4.1.1.7. Soporte Técnico

- ✓ Soporte 7x24 y 9x5.

.4.4.1.1.8. Modelos KMSA

- ✓ Definidos por usuarios concurrentes y nivel de transaccionabilidad.
- ✓ Dimensiones estándar para rack.
- ✓ No requiere licenciamiento por módulos.

1.2.4.1.2. Especificaciones Técnicas

Marca	Kypus
Modelo	KMSA
Usuarios	100
Nivel de soporte en Hardware	9x5 con soporte en sitio máximo en 4 horas
Soporte Técnico	Entregado por el fabricante
Ingenieros Certificados	Con el mas alto nivel de certificación entregado por el fabricante, con experiencia en implementaciones en el país de al menos 3 años.
Soporte Técnico (Durante la garantía técnica)	Soporte Técnico (Nivel Nacional) Call Center mediante línea 1800 NOVASA Correo electrónico ilimitado Sistema automático de tickets Data - Conference Chat en línea portal de fabircante
Mantenimiento Preventivo de Hardware	Será realizado una vez al año de acuerdo a la disponibilidad de la entidad
Garantía del fabricante	36 meses
Interfaces de Red	2 x 10/100/1000 Mbps configurables (LAN, DMZ, WAN), expandible a 4 interfaces
Puerto serial de consola	1
Flash Memory para el Sistema Operativo	Sistema Operativo Embebido (100 Mb Máximo) y Ecriptación que corra sobre memoria de estado sólido
Administración Remota	No Web - Basado (Propietario GUI)
Actualizaciones de Firmware y Software	Si (gratis por el período de garantía)
Administración de MultiNode	Si (ilimitado)
Instalación	Instalación herramienta de administración - configuración de todos los servicios

Tabla N. 1.4.4.1.2.1 Especificaciones Técnicas del equipo

Fuente: (KYPUS, 2015)

1.2.4.1.3. Servicios

Firewall (Inspección Packet Stateful)

- Capacidad de editar reglas en línea

Email Protection Service

Antivirus

- Detección de Virus para correo electrónico
- Embebido en el sistema operativo
- Detección de otro tipos de amenazas

AntiSpam (Filtrado de correo no deseado)

- Creación de listas Blancas
- Creación de listas Negras
- Filtrado de Extensiones
- Filtrado de Contenido

Content Filtering

- Filtrado por Usuarios
- Filtrado por IP’s
- Filtrado por Grupos
- Filtrado Individual
- Soporte Listas Blancas
- Actualización automática de Listas Negras
- Filtrado de Aplicaciones (P2P, MSN, Aplicaciones de red)

VPN (IPSec Compliant)

- Red a Red
- Host a Read (PPTP)
- Encriptación AES, 3DES
- Autenticación por certificados x.509v3 (PKI e IKE)

Mail Server (SMTP, POP3, IMAP)

- Soporte para SMTP autentificación
- Control del tamaño en envío de los correos
- Soporte para pasarela de correo
- Soporte para múltiples dominios

Advance Web Server

- Soporte Host Virtuales
- Soporte para pasarela de páginas WEB

Web Mail

FTP Server

- Configuración de cuenta por usuario

DNS Server

DHCP Server

Web Caching Proxy

- Caché de páginas web configurable

Traffic Shaping

- Soporte para calidad de servicio
- Control de ancho de banda dinámico
- Soporte por grupos y usuarios
- Soporte de ancho de banda por servicio

LDAP Server

Radius Server

RAS Server

- Con capacidad para calendarizar al acceso

Smart Reports

- Reporte de navegación con detalle de fecha
- Hora y tiempo de acceso
- Reportes estadísticos
- Reporte uso canal
- Reporte de uso de correo
- Reporte Spam y Virus

Administración Centralizada

Administración Remota Segura

- Con soporte SSL
- No se debe administrar por línea de comandos (no SSL, no Telnet)

Interface Gráfica (Ambiente Windows)

Alarmas SNMP

Gestión Centralizada de clientes

1.4.4.2. KYPUS THIN CLIENT

Kypus Thin Client está enfocado a beneficios remplazando el escritorio a una administración mínima del dispositivo, corriendo aplicaciones basándose en servidores, sus principales beneficios son:

- Administración centralizada y reducción de costos de mantenimiento del desktop.
- Incrementa seguridades
- Reduce tiempo de downloads y uploads.
- Mejor producción de acceso remoto.
- Maximiza acceso a servicios de las computadoras a través de un control de tráfico en la red.
- Reduce costos de administración de la red
- Baja adquisición de productos de hardware
- Control centralizado de software, aplicaciones y archivos.
- Soporta legalmente Frames (Unix Terminal Emulation)
- Reduce los requerimientos de la banda de ancha de las aplicaciones a una fracción de lo que normalmente requiere y habilita gran capacidad de envió de paquetes en la infraestructura de la red.

Las computadoras basadas en Servidores deben tener los mismos sistemas operativos y aplicaciones para acceder a la red en cada computadora, en cambio con esta tecnología estas aplicaciones son administradas por los servidores centralizadamente. Estos son los beneficios de seguridad:

1) Los clientes no pueden almacenar datos o aplicaciones localmente
2) Los clientes no necesitan Firewalls ni antivirus personales.
3) No hay necesidad de respaldos en las computadoras de los clientes
4) Los clientes pueden instalar sus propias aplicaciones, servicios, periféricos no autorizados, etc.
5) No existen archivos temporales o residuales después de ejecutar una aplicación o sesión web.
6) Los datos no viajan por los cables de red o la red inalámbrica, la verificación y control ocurre en el nivel de red.
7) No se gasta tiempo en la reinstalación de aplicaciones en caso de desastres en la PC.
8) Los clientes puedes ser replicados en minutos con el servidor con las aplicaciones y datos.
9) Pocos servicios significa pocas oportunidades de provocar problemas.

10) Mantenimiento de campos centralizados permite mejorar las seguridades en la red.

2. CAPÍTULO

CASO DE ESTUDIO, EMPRESA SINERGY HARD

2.1. Entorno de la empresa Sinergy Hard

2.1.1. Antecedentes históricos

- En el año 2008 nace como una empresa Business Partner IBM para la provisión de soluciones de infraestructura.
- En 2009 la empresa Sinergy Hard pasa a nivel Premier en canales IBM, logran alcanzar ser Business Partner Premier de Software IBM, inauguran oficina en la ciudad de Guayaquil y obtienen el premio Business Partner con mayor crecimiento.
- En 2011 obtienen el premio a la mejor gestión comercial.
- En 2012 se habré la oficina en la ciudad de Ambato.
- En 2013 obtienen premio al canal con el Mayor Cantidad de Small Deals en Soluciones de Software.

2.1.2. Misión

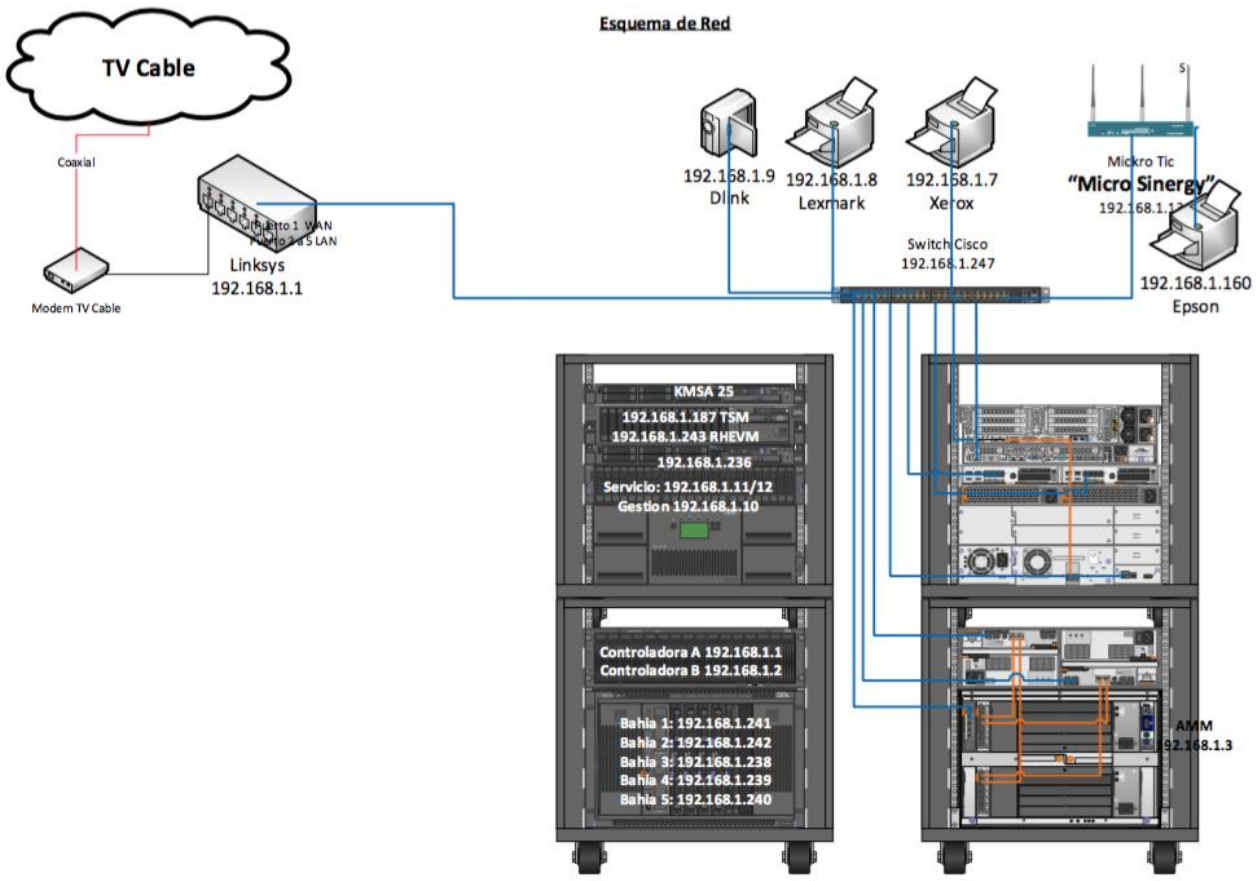
La misión de la empresa Sinergy Hard es “Somos la solución en tecnología de la información. Su satisfacción es nuestra meta y nuestra experiencia su tranquilidad”.

2.1.3. Visión

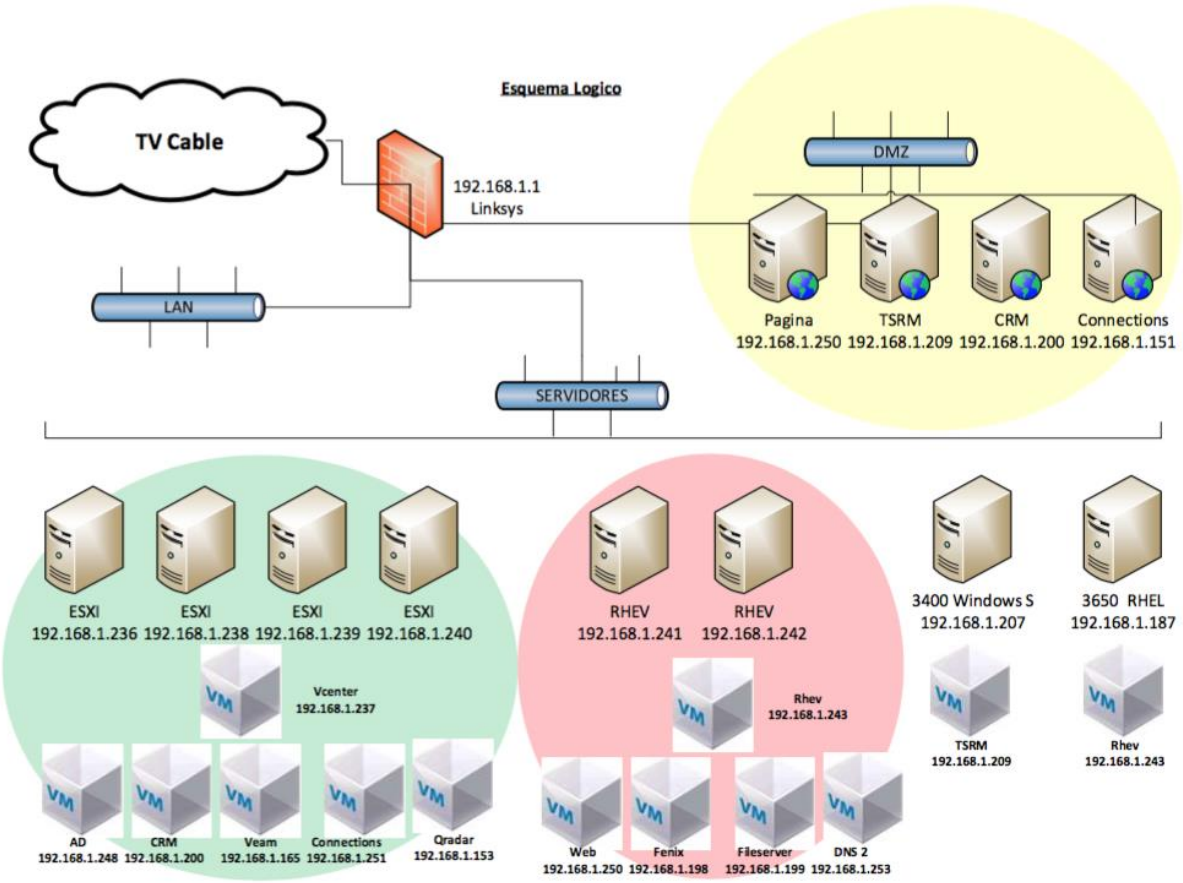
La visión de la empresa Sinergy Hard es “Para el 2.017 seremos reconocidos como el principal proveedor de servicios de tecnología de las marcas de clase mundial que representamos; alcanzando un incremento en 3 puntos porcentuales de nuestra rentabilidad durante el periodo, gracias al crecimiento innovación en nuestro portafolio de productos y servicios, y a la eficiencia de nuestra operación; haciendo evidente nuestra contribución al bienestar de nuestros clientes internos y externos. Con un equipo humano competente, calificado y apasionado por el servicio; con la capacidad para aportar soluciones a medida de las necesidades de nuestros clientes y de los objetivos de la compañía”.

2.2. Estructura de la red interna de Sinergy Hard

2.2.1. Esquema de Red



2.2.2. Esquema Lógico



2.2.3. Equipos

2.2.3.1. Switch Cisco[103]

"La serie 200 de Cisco (Figura 2.2.3.1.1) es un conjunto de switches inteligentes y asequibles que combinan un potente rendimiento y confiabilidad de red con las funciones esenciales de administración de red que usted necesita para una red empresarial sólida. Estos switches Fast Ethernet o Gigabit

[103] (Cisco, 2013)

Ethernet expandibles ofrecen funciones básicas de administración, seguridad y calidad de servicio (QoS) superiores a las que ofrece un switch no administrado o para uso de consumidores, a un costo menor que los switches administrados. Gracias a una interfaz de usuario web fácil de usar, el protocolo de detección de Cisco y Cisco Smartports, usted puede implementar y configurar una red empresarial sumamente sólida en pocos minutos."[104]

Figura 2.2.3.1.1 Switch Cisco

Fuente: (Cisco, 2013)

2.2.3.2. KMSA 25[105]

Se especializa en el rendimiento y seguridad de Internet, enfocado para un máximo de 25 usuarios que necesitan simultáneamente acceder a una variedad de servicios en la red.

[104] (Cisco, 2013)
[105] (KYPUS, 2015)

Figura 2.2.3.2.1 Equipo KMSA 25

Fuente: (KYPUS, 2015)

2.2.3.3. TSM – IBM[106]

"IBM Tivoli Storage Manager for System Backup and Recovery proporciona un método de copia de seguridad flexible para los sistemas IBM AIX. Incluye funciones de copia de seguridad, restauración y reinstalación del sistema para proteger datos críticos de fallos en el equipo y factores medioambientales. Puede ejecutar este software desde la línea de mandatos de AIX o utilizando la interfaz del menú de System Management Interface Tool (SMIT).

Tivoli Storage Manager for System Backup and Recovery:

- Proporciona programas de utilidad para crear planificaciones y scripts de copia de seguridad: para facilitar la automatización de tareas en empresas de todos los tamaños.
- Habilita la elección de diversos tipos de copia de seguridad: los tipos incluyen sistema completo (imagen de instalación), grupo de volumen, sistema de archivos, archivo o directorio y volumen lógico en bruto.

[106] (IBM, 2015)

- Admite la configuración de puertos de red para comunicarse a través de cortafuegos: proporciona soporte a través para entornos locales de idioma con sistema operativo AIX.
- Habilita la clonación: instale una imagen de instalación de sistema en otro sistema con configuraciones de hardware idénticas o diferentes.
- Permite el almacenamiento de objetos de copia de seguridad en un servidor IBM Tivoli Storage Manager: Tivoli Storage Manager for System Backup and Recovery puede realizar copias de seguridad de datos que no sean de rootvg."[107]

Figura 2.2.3.3.1 Equipo TSM - IBM

Fuente: Esquema de Red

2.2.3.4. Librería de cintas IBM[108]

"Características principales:

- Soporta la última generación de la tecnología Linear Tape-Open® (LTO®) con hasta dos unidades de cinta LTO Ultrium® con factor de forma 2U

[107] (IBM, 2015)
[108] (IBM, IBM, 2015)

- Simplifique el acceso de los usuarios a datos almacenados en cartuchos de cinta mediante el uso de tecnología IBM Spectrum Archive con tecnología IBM Linear Tape File System
- Gestione librerías remotamente a través de una interfaz web estándar que ofrece flexibilidad y mejor control administrativo de las operaciones de almacenamiento.
- La gestión remota de librerías a través de una interfaz web estándar ofrece la máxima flexibilidad y un mejor control administrativo de las operaciones de almacenamiento.

La librería de cintas IBM® TS3100 y sus aplicaciones de administración del almacenamiento han sido diseñadas para superar sus requisitos de capacidad, rendimiento, protección de datos, fiabilidad, disponibilidad, asequibilidad y aplicaciones. La TS3100 ha sido concebida como una solución de nivel básico con una gran cantidad de funciones que incorpora la tecnología de cintas LTO. La TS3100 es una solución magnífica para copias de seguridad en cinta de gran capacidad o alto rendimiento con o sin acceso aleatorio, además de una elección excelente para la automatización de cintas para IBM Power Systems y otros sistemas abiertos. La TS3100 es muy apropiada para la gestión de las necesidades de copia de

seguridad, restauración y archivado de datos en entornos de PYMES. Gracias al uso de una unidad de cinta de altura completa LTO o hasta dos unidades de cinta de media altura LTO y a su capacidad para 24 cartuchos de cintas, el modelo IBM TS3100 aprovecha la tecnología LTO y hace frente, de manera económica, a las crecientes necesidades de almacenamiento. La TS3100 se configura con dos módulos para cartuchos de cinta extraíbles: uno en el lado izquierdo (12 ranuras para cartuchos de datos) y uno en el lado derecho (12 ranuras para cartuchos de datos). Además, el almacén izquierdo incluye una única ranura para correo que le permite seguir funcionando durante la entrada y salida de soportes. La librería incluye de serie un lector de código de barras, que permite su funcionamiento en modo de acceso secuencial o aleatorio. La TS3100 incluye de serie capacidades de gestión remota que permite la administración remota de la librería de cintas a través de una interfaz web. La función opcional Failover de rutas (Path Failover) está diseñada para ofrecer failover automático de rutas de control en una ruta de control redundante preconfigurada en el caso de que se pierda un adaptador de host o una unidad de ruta de control sin interrumpir el trabajo actual en curso."[109]

[109] (IBM, IBM, 2015)

Figura 2.2.3.4 Equipo Librería de cintas IBM

Fuente: (IBM, IBM, 2015)

2.2.3.5. MIKROTIK[110]

"Características principales:

- Control de Seguridad: La seguridad es algo primordial en una red, es por eso que las técnicas que se utiliza en la configuración del Firewall en el Router de Borde permite tener el control, tanto del tráfico de ingreso así como el generado por los usuarios o host en la red, con el cual podrá controlar los accesos a su red, así como bloquear aplicaciones, mensajeros y chats, servicios y sistemas de intercambio de archivos (p2p).
- Control de VPN's: Esta característica le ofrece unir sus sucursales o redes a través de Redes Privadas Virtuales, asimismo ingresar a la misma desde su Laptop como si estuviera dentro de ella desde cualquier lugar del mundo, pudiendo acceder a sistemas y recursos, con

[110] (Anrrango, 2016)

toda la extrema seguridad que sus datos requieren. Seguridad con túneles L2TP/PPTP además de una encriptación superior con IPSEC, le permiten tener la privacidad necesaria.

- Control de Calidad de Servicio: Un acceso a Internet que no esté bien administrado, en la navegación sobre sitios importantes da igual una bajada de un archivo ftp, p2p o voIp, todos tienen la misma PRIORIDAD, con esta solución podrá racionalizar y priorizar inteligentemente el ancho de banda disponible privilegiando aplicaciones interactivas, VoIP, navegación, correo electrónico, ftp e intercambio de archivos P2P entre otros."[111]

Figura 2.2.3.5.1 Equipo MikroTik

Fuente: (Anrrango, 2016)

[111] (Anrrango, 2016)

3. CAPÍTULO

PROPUESTA DE IMPLEMENTACIÓN DE QoS EN LA VLAN DE SINERGY HARD

3.1. Introducción

Las aplicaciones están consiguiendo ser cada vez más exigentes y obligan a las empresas a seguir este ritmo. Los comentarios para el mejoramiento presionan para brindar cada vez más calidad, confiabilidad, y asegurar la puntualidad en la entrega. Un ejemplo claro son las aplicaciones de voz o vídeo con las que se trabaja dentro de la empresa Sinergy Hard, éstas deben ser manejadas cuidadosamente dentro de una red del IP para preservar su integridad, ya que al ser distribuidores de los productos de IBM es necesario garantizar una calidad en los cierres de negociación de proyectos o venta de productos. Además hay que tener en cuenta que el tráfico no es predecible, ni constante, si no que funciona a ráfagas, produciéndose en ocasiones picos máximos de tráfico que son los causantes, en parte, de la saturación de la red. Ejemplos clarificadores de este tipo de tráfico es el producido por el mundo Web al que está sometido diariamente cada usuario con la red de la empresa debido al correo electrónico y las transferencias de ficheros, que son virtualmente imposibles de predecir. Las tecnologías de QoS permiten a los administradores de red:

- Manejar las aplicaciones sensibles al jitter, como las que manejan audio y vídeo.
- Manejar el tráfico sensible al retardo, como la voz en tiempo real.

- El control de pérdidas en los momentos en los que la congestión sea inevitable.

3.2. Propuesta

Uno de los principales propósitos de esta investigación es garantizar la satisfacción de los usuarios con la red de la empresa Sinergy Hard, se encontraron problemas de satisfacción con la velocidad de la red en las líneas de tráfico, problemas en el envío de archivos y conflictos de uso. Dado lo anteriormente sustentado, la propuesta de implementación de calidad de servicio (QoS) en Redes Locales Virtuales (VLAN) mediante las normas 802.1D y 802.1Q en la empresa Sinergy Hard sería:

- Aumentar un proveedor de servicio de internet, en este caso Netlife que trabaja con fibra óptica para garantizar mayor velocidad de flujo en comparación a la conexión coaxial que maneja TVCable.
- Aumentar un MikroTik para la administración del Wireless que va a tener conexión con el servicio de TVCable.
- Se usaría la conexión directa de Netlife para poder subir y consumir los servicios dejando cómo reserva a la conexión de TVCable.
- Con el aumento de Netlife se proporciona a la red un dispositivo de seguridad (firewall) Fortigate 40c el cual nos brinda:
    - Prevención de intrusión
    - Filtración de capa de aplicación
    - Filtración de contenido Web
    - Vulnerability Assessment

- Antivirus
- Anti-spam
- Anti-spyware
- Control de Acceso

- Cambiar el equipo KMSA 25 ya que sus años de uso lo dan a depreciación y obsoleto dado que la nueva versión del equipo es el modelo KMSA las características y beneficios se encuentran en el capítulo 1 sección 1.4.

En la propuesta sobre QoS es necesario mostrar una configuración para garantizar que se cumpla la calidad del servicio a continuacion un ejemplo de configuración de la red:

Escenario 1: Correo y Web

Existe una red interna en la que se generan flujos salientes de tipo Web (HTTP) y correo electrónico (SMTP, POP3), ambos con un volumen de tráfico similar:

Se considera al tráfico HTTP poco importante y a limitar, salvo para una máquina de dirección IP 192.168.1.112, en cuyo caso es de relevancia muy alta.

Red existente:

AB de subida del enlace externo: 1024 Kbps

AB de bajada del enlace interno: 100 Mbps

Configuración de QoS:

(debe ajustarse a los AB anteriores)

Tráfico de salida máximo para la interfaz externa (NIC1): 1024 Kbps

Tráfico de salida máximo para la interfaz interna (NIC2): 100 Mbps

Ancho de banda reservado: 5 %

Se crean las siguientes reglas:

Regla	IP origen	Protocolo	AB garantizado	AB límite	Prioridad
1	192.168.1.112/32	HTTP	300 Kbps	No limitado	alta
2	192.168.1.0/24	HTTP	0 Kbps	200 Kbps	baja
3	192.168.2.0/24	HTTP	0 Kbps	200 Kbps	baja
4	Cualquiera	SMTP	400 Kbps	No limitado	media
5	Cualquiera	POP3	100 Kbps	No limitado	media

Regla 1

Concede un AB garantizado de 300 Kbps al tráfico originado en la dirección IP 192.168.1.112 y que sea de tipo HTTP. Además tendrá prioridad alta para poder conseguir –si lo necesita- el AB que se encuentre libre.

Regla 2

Para el resto de la subred 192.168.1.0/24, el tráfico HTTP no tiene garantizado AB y, además, se limitará a 200 Kbps. Su prioridad será baja para que no compita por el AB libre.

Regla 3

Para la totalidad de la subred 192.168.2.0/24 se procede como en la regla anterior, limitando el tráfico HTTP a 200 Kbps y asignándole una prioridad baja.

Regla 4

El protocolo SMTP, cualquiera que sea el origen, se garantiza en 400 Kbps de salida y tendrá una prioridad media.

Regla 5

El protocolo POP3, cualquiera que sea el origen, se garantiza en 100 Kbps de salida y tendrá igualmente una prioridad media.

Escenario 2: Web

Existe una red interna en la que se generan flujos de tráfico saliente de tipo Web (HTTP, HTTPS) y tráfico que no se ajusta a reglas.

Se considera al tráfico HTTP y HTTPS importante y, existe en menor volumen, tráfico relativo a otros protocolos y que es de menor importancia.

Red existente:

AB de subida del enlace externo: 512 Kbps

AB de bajada del enlace interno: 100 Mbps

Configuración de QoS:

(debe ajustarse a los AB anteriores)

Tráfico de salida máximo para la interfaz externa (NIC1): 512 Kbps

Tráfico de salida máximo para la interfaz interna (NIC2): 100 Mbps

Ancho de banda reservado: 5 %

Se crean las siguientes reglas:

Regla	IP origen	Protocolo	AB garantizado	AB límite	Prioridad
1	cualquiera	HTTP	200 Kbps	No limitado	alta
2	cualquiera	HTTPS	200 Kbps	No limitado	alta

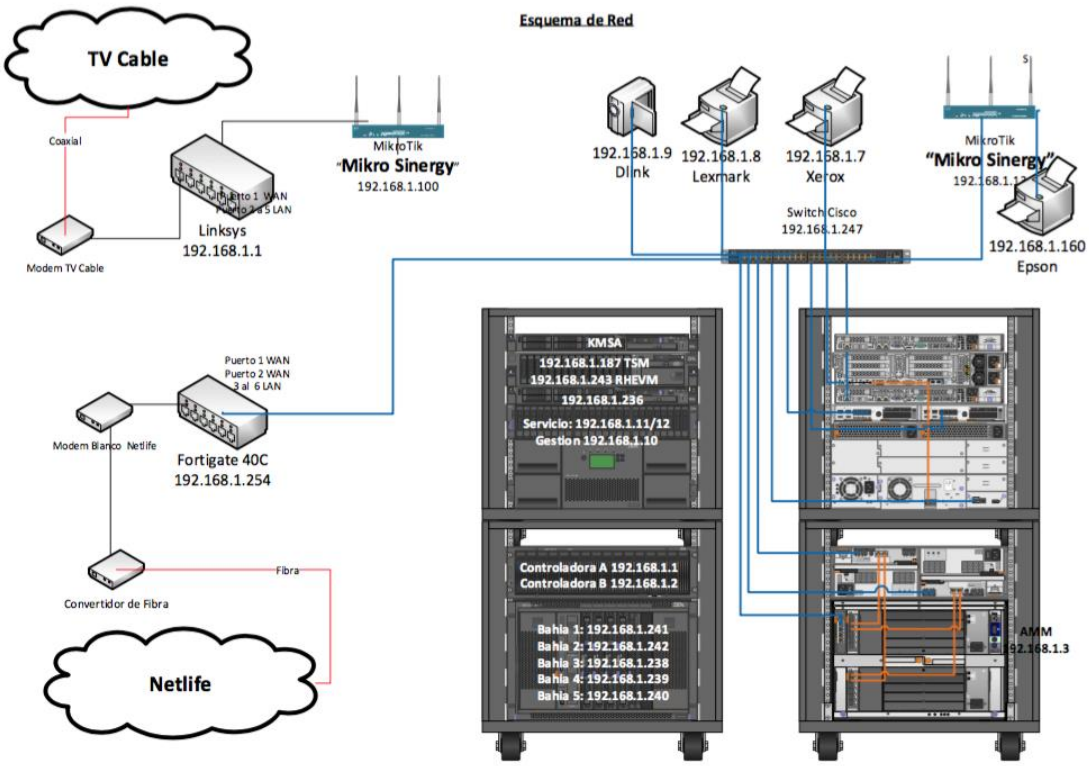
Regla 1

Concede un AB garantizado de 200 Kbps al tráfico de tipo HTTP. Además tendrá prioridad alta para poder conseguir -si lo necesita- el AB que se encuentre libre.

Regla 2

Concede un AB garantizado de 200 Kbps al tráfico de tipo HTTPS. Además tendrá prioridad alta para poder conseguir -si lo necesita- el AB que se encuentre libre. El resto del tráfico existente tendrá una prioridad media, con lo cual no competirá por el AB libre.

3.3. Esquema de Red



3.4. Costo – Beneficio

Equipo	Costo	Beneficio
Netlife	$ 105,00	100 Mbps
		Compartición 2:1
MikroTik	$ 220,00	Control de Seguridad
		Control de VPN
		Control de Calidad de Servicio
		Control de Acceso
		Control Hotspot
		Control de Ancho de Banda
KMSA	$ 1.800,00	Administración Centralizada
		Seguridad
		Gestión de Comunicaciones
		Filtrado de Contenido
		Servidor de Correo
		Estadística y reportes gráficos
		Soporte Técnico

Gastos de Equipamiento	
Netlife	$ 105,00
MikroTik	$ 220,00
KMSA	$ 1.800,00
Total	$ 2.125,00

4. CAPÍTULO

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

1) La Calidad de Servicio en la red de la empresa Sinergy Hard necesita de algunas modificaciones para la satisfacción completa de los usuarios ya que es fundamental para obtener un mejor rendimiento.
2) Para establecer una mejor calidad de servicio en una red se debe conocer y determinar las clases y tipos de servicio que se están manejando, para posteriormente administrarlos según los intereses de la empresa.
3) La utilización de la Calidad de servicio trae muchos beneficios, ya sea a nivel de una red LAN, VLAN o WAN, e inclusive para los proveedores de servicio, es decir QoS es ilimitado y permite brindar más servicios exigidos por la tecnología actual a través del soporte de tráfico en tiempo real, administración del ancho de banda, acuerdos de nivel de servicio, mecanismos de colas, etc.
4) La nueva herramienta Kypus ofrece servicios para la administración y gestión del tráfico de la red con QoS, el cual permite administrar el

ancho de banda desde el servidor; los usuarios usan terminales tontas para evitar ataques de intrusos. Se caracteriza por que maneja QoS a nivel de la capa de aplicación.

5) Tener un buen proveedor de internet es fundamental para poder administrar de manera correcta la red y tener un proveedor de respaldo es muy importante para que los servicios de la empresa no se tarden mucho tiempo en volver a funcionar en caso de una perdida de servicio.
6) Para estar regido a estándares internacionales con el funcionamiento y ordenamiento de la red se debe tomar en cuentas normas, estándares y referencias internacionales, como por ejemplo de la Unión internacional de telecomunicaciones (UTI), publicaciones o comentarios como los Request For Comment, donde ayuda a informarse más sobre el tema y aclarar inquietudes.
7) Después de realizar el análisis de factibilidad económico, para la implementación de soluciones de QoS en la empresa Sinergy Hard, se determinó que la empresa tiene los recursos económicos para la inversión de nueva infraestructura para obtener una mejor operación de la QoS.
8) La implementación de soluciones de QoS se basó en parámetros como el ancho de banda, tráfico de red, retardo de paquetes, latencia, jitter, rendimiento, perdida de paquetes, en el cual se determinó las clases de tráfico y servicio, clasificación y fundamentalmente la

utilización de los protocolos Diffserv y RSVP conjuntamente con las políticas en los servidores y el estándar de etiquetado 802.1P.

4.2 Recomendaciones

1) Todos los estándares para la implementación de QoS deben tomarse en consenso y deben ser respaldadas por el personal técnico de cada empresa.
2) De manera oficial se debe reglamentar la documentación de cualquier cambio realizado en la red y que se mantengan actualizados para mantener un seguimiento del mismo.
3) Es recomendable, establecer como mínimo una persona encargada para el manejo del Controlador de dominio, otra persona para el control de los servidores miembros y otra para el soporte técnico de los usuarios de la empresa.
4) Dar a conocer al personal técnico de la empresa la importancia de la implementación de soluciones de QoS.
5) El tipo de direccionamiento IP estático es recomendable en el caso de que la empresa tenga pocos usuarios, caso contrario se es recomendable tener direccionamiento IP dinámico.
6) Es recomendable que la administración de los usuarios de la red de una empresa se encuentren organizados mediante Unidades Organizacionales o Grupos Globales para una mejor manipulación y administración con respecto a la asignación de ancho de banda.

7) Se recomienda analizar y monitorear el tráfico de la red en periodos determinados de tiempo, para observar falencias futuras que se pueden presentar.
8) Recomendar a las empresas que consideren implementar este tipo de soluciones que puede generar ahorros importantes a la empresa y no inversiones innecesarias.

5. BIBLIOGRAFIA

Group, C. (Septiembre de 2015). *CCM*. Obtenido de http://es.ccm.net/contents/286-vlan-redes-virtuales

TextosCientificos.com. (Noviembre de 2006). Obtenido de http://www.textoscientificos.com/redes/redes-virtuales

Wikipedia. (9 de Noviembre de 2015). Obtenido de VLAN: https://es.wikipedia.org/wiki/VLAN

Redes Virtuales. (Julio de 2011). Obtenido de http://vlan610.blogspot.com/

Ecotec, U. (2012). *Diseño e implementacion de VLANS* . Obtenido de http://gye.ecomundo.edu.ec/doc_aula_virtual_ecotec/tareas/2012D/COM355/alum/2012290085_738_2012D_COM355_Dise_o_e_Implementacion_de_VLANs.pdf

Microsoft. (2016). *Developer Network*. Obtenido de Documentación Microsoft: https://msdn.microsoft.com/es-es/library/hh831679%28v=ws.11%29.aspx

Pérez, J. A. (2003). *Calidad de Servicio en Redes (QoS), Sistemas Multimedia, Especialización en Teleinformática.* EAFIT.

Ardao, J. C. (Abril 2005). *Redes de Banda Ancha, Provisión de QoS en IP*.

Practical IP Network QoS. (2012). Obtenido de http://web.opalsoft.net/qos/default.php

Belzarena, P. (2003). *Ingeniería de tráfico en línea en redes Mpls aplicando la teoría de grandes desviaciones.*

Pino, L. (2016). *LP23*. Obtenido de http://www.lp23.com/bmextreme/

NetLimiter. (5 de 9 de 2016). *NetLimiter*. Obtenido de https://www.netlimiter.com

KYPUS. (2015). *KYPUS*. Obtenido de http://www.kypus.com/contenido/catalog/kmsa.pdf

Jacobs, E. (s.f.). *Seminario de Calidad de Servicio en Redes Multimedia.*

IEEE. (2016). Obtenido de IEEE Explore Digital Library: http://ieeexplore.ieee.org/document/1389253/

Cisco. (2013). *Switches inteligentes Cisco de la serie 200 Cisco Small Business* . Obtenido de http://www.cisco.com/c/dam/en/us/products/collateral/switches/small-business-100-series-unmanaged-switches/data_sheet_c78-634369_Spanish.pdf

IBM. (2015). *IBM*. Obtenido de Tivoli Storage Manager for System Backup and Recovery: http://www-03.ibm.com/software/products/es/tivostormanaforsystbackandreco

IBM. (2015). *IBM*. Obtenido de Librería de cintas IBM TS3100: http://www-03.ibm.com/systems/ec/storage/tape/ts3100/

Anrrango, R. (2016). *ConfigurarMikrotikWireless*. Obtenido de http://configurarmikrotikwireless.com/blog/caracteristicas-importantes-equipos-mikrotik.html

Chafla, G. (2003). *Servicios Diferenciados.*

Charris, A. (2012). *VLAN*. Obtenido de http://redes2vlans.blogspot.com/p/vlans-estatica.html

ConsultasCCNA. (2012). *CONSULTASCCNA*. Obtenido de http://consultasccna.comoj.com/informacion/vlan/introduc/subnets.php

ConsultasCCNA. (2012). *ConsultasCCNA*. Obtenido de http://consultasccna.comoj.com/informacion/vlan/introduc/escalab.php

ConsultasCCNA. (2012). *ConsultasCCNA*. Obtenido de http://consultasccna.comoj.com/informacion/vlan/introduc/miembros.php

Diaz, N. M. (2009). *Multiple Protocol Label Switching.*

Felici, S. (2012). *Calidad de servicio (CoS y QoS).*

Jacobs, E. (2011). *Seminario de Calidad de Servicio en Redes Multimedia.*

Martin, M. M. (2011). *Señalización para QoS en redes IP*.

Martín, M. C. (2012). *"EL VALOR DE LA EMPRESA DE INTERNET Y LA CALIDAD DEL SERVICIO OFRECIDO".*

Segmentacion de VLAN. (2003). Obtenido de http://ecovi.uagro.mx/ccna2/course/module3/3.1.1.2/3.1.1.2.html

VLAN. (2003). Obtenido de Sitio Google: https://sites.google.com/site/isaacivantorresgonzalezvlan/home/ventajas-de-las-vlan

Azuay, U. d. (2013). Obtenido de http://www.uazuay.edu.ec/estudios/electronica/proyectos/redes_de_datos_lan2.pdf

DocShare. (2015). *Protocolos y arquitecturas de QoS*. Obtenido de http://docshare01.docshare.tips/files/4815/48158459.pdf

Gutierrez, J. A. (2014). *Información sobre Tecnologías de la Información y Comunicaciones y otros aspectos de interés cultural*. Obtenido de http://jgutierrez1965.blogspot.com/p/calidad-de-servicio-qos.html

OoCities.org. (Octubre de 2009). *OoCitites*. Obtenido de http://www.oocities.org/es/leidamorenogalvis/hwct/STEG/CAPITULOII.htm

Rueda, C. (2012). *SOLUCIONES MULTIMEDIA BAJO PLATAFORMAS WEB (LIVIANAS).*

CCM. (Diciembre de 2016). *VLAN - Redes virtuales*. Obtenido de http://es.ccm.net/contents/286-vlan-redes-virtuales

Icc. (2005). *Redes Locales Virtuales*. Obtenido de http://www.lcc.uma.es/~eat/services/rvirtual/rvirtual.html#link3

Puchele, N. (Junio de 2011). *ENRUTAMIENTO ENTRE VLAN*. Obtenido de http://vlan610.blogspot.com/

Ecotec, U. (2012). *Diseño e Implementacion de VLANS*.

VLAN. (2012). Obtenido de VLAN Estática vs VLAN Dinamica: http://redes2vlans.blogspot.com/p/vlans-estatica.html

Guayaquil, U. d. (2008). *FACTIBILIDAD DE IMPLEMENTACIÓN DE UNA RED DE VOZ SOBRE IP VoIP EN EL CAMPUS DE LA UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL.*