ESTUDIO E IMPLENTACION DE CALIDAD DE SERVICIOS (QoS) EN DISPOSITIVOS CAPA 3

ROCIO CAZÉS ORTEGA

SANDRA MILENA GIL HIGUITA

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FÍSICO – MECÁNICAS
ESCUELA DE INGENIERIAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
BUCARAMANGA
2008

ESTUDIO E IMPLENTACION DE CALIDAD DE SERVICIOS (QoS) EN DISPOSITIVOS CAPA 3

ROCIO CAZÉS ORTEGA

SANDRA MILENA GIL HIGUITA

Monografía para optar al título de Especialista en Telecomunicaciones

Director
ING. RICARDO ALVARADO JAIMES
Especialista en Telecomunicaciones

UNIVERSIDAD INDUSTRIAL DE SANTANDER
FACULTAD DE INGENIERIAS FÍSICO – MECÁNICAS
ESCUELA DE INGENIERIAS ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES
BUCARAMANGA
2008

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

RESUMEN

TITULO: **ESTUDIO E IMPLENTACION DE CALIDAD DE SERVICIOS QoS EN DISPOSITIVOS CAPA 3***

AUTOR: **CAZES ORTEGA, Rocio. GIL HIGUITA, Sandra Milena.****

PALABRAS CLAVES: Calidad de Servicio *(QoS)*, Diffserv (Diferentes servicios), WFQ – basado en flujo.

DESCRIPCIÓN:

A medida que las aplicaciones de usuario continúan impulsando el crecimiento y desarrollo de la red, la demanda para el soporte de diferentes perfiles de tráfico también aumenta. Donde aplicaciones con diferentes requisitos de red crean la necesidad de introducir tecnologías y políticas administrativas que controlen la forma de tratar aplicaciones individuales que les provea servicios seguros, fiables, mensurables y garantizados, donde se le pueda asignar especial tratamiento a las aplicaciones delicadas, críticas y sensibles a retrasos. El despliegue y la ejecución de las políticas de calidad y servicios (QoS) dentro de una red juegan un papel esencial para permitir que los administradores de la red y arquitectos encuentren las demandas conectadas a redes convergentes. QoS es un elemento crucial para cualquier política administrativa que determina cómo manejar el tráfico de aplicación en una red.

Este documento es una ayuda para ingenieros, técnicos e investigadores de la industria de las telecomunicaciones, para quienes buscan conocer más sobre los conceptos y aspectos prácticos de las tecnologías QoS y específicamente características, funcionamiento y ventajas de configuración de la tecnología QoS.

---

* Monografía

** Universidad Industrial de Santander (UIS); Facultad de Ingenierías Físico – Mecánicas; Escuela de Ingeniería Eléctrica, Electrónica y Telecomunicaciones; Ricardo Alvarado Jaimes, Director del Proyecto.

SUMMARY

TITLE: STUDY AND IMPLEMENTATION OF QUALITY OF SERVICES QoS IN DEVICES LAYER 3th. *

AUTHORS: CAZES ORTEGA, Rocío. GIL HIGUITA, Sandra Milena. **

KEY WORDS: *Quality of Service (QoS)*, Diffserv (Different Service), WFQ – Based on flow

DESCRIPTION:

As the user's applications continue stimulating the growth and development of the network, the demand for the support of different profiles of traffic also increases. Where applications with different requirements of network create the need to introduce technologies and administrative policies that control the way of treating individual applications that it provides sure, trustworthy, measurable and guaranteed services, where it could assign special treatment to the delicate applications, critical and sensitive to delays. The unfolding and the execution of the quality policies and services (QoS) inside a network play an essential paper to allow that the managers of the network and architects should find the demands connected to converged networks. QoS is a crucial element for any administrative politics that it determines how to handle the traffic of application in a network.

This document is a help for engineers, technical personnel and investigators(of the industry of the telecommunications, for those who seek to know more on the concepts and practical aspects of the technologies QoS and specifically characteristics, functioning and advantages of configuration of the technology QoS.

---

* Monograph

** Universidad Industrial de Santander (UIS); Faculty of Engineering Physical-Mechanical; School of Engineering electrical, Electronic and telecommunications; Specialization in Telecommunication; Ricardo Alvarado Jaimes, Adviser.

1. CALIDAD DE SERVICIO QoS

Calidad de servicio (QoS, Quality of Service) es un conjunto de requerimientos de servicio que la red debe cumplir para garantizar un nivel de servicio apropiado en la entrega de los datos.

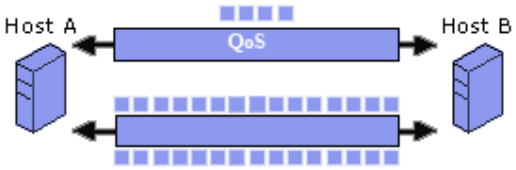


Figura 1. QoS, Quality of Service
Fuente: http://technet2.microsoft.com

El objetivo de QoS es conseguir un sistema de entrega garantizada del tráfico de la red, como los paquetes de Protocolo Internet (IP Internet Protocol).

1.1 CONCEPTO

Calidad de Servicio (QoS[1]): El concepto de QoS está relacionado con la planificación de los elementos de la red de acuerdo con la demanda de las aplicaciones, para ofrecer un mínimo nivel de garantía que satisfaga los requerimientos de distintos perfiles de tráfico: mínimo retraso de envió de los datos, mínima variación de los retrasos, ancho de banda adecuado para el envió satisfactorio de datos con el propósito que sean tratados adecuadamente respecto a otros. La calidad de servicio es el término que define la capacidad que tiene la red de proveer diferentes niveles de servicio para asegurar distintos perfiles de tráfico y ofrecer un mínimo nivel de garantía que satisfaga los requerimientos de tráfico.

La calidad puede ser implementada en diferentes situaciones, sea para gestionar la congestión o para evitarla. La técnica utilizada para gestión de congestión da prioridad al tráfico donde las aplicaciones requieren más ancho de banda de lo que se puede ofrecer en la red. Dando prioridad a los servicios

[1]http://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/electronica/Diciembre_1999/Pdf/02_calidad.pdf

con requisitos de tiempo real es posible operar en un entorno de congestión con un alto grado de disponibilidad y controlar algunas características significativas de la transmisión de paquetes. Estas características pueden especificarse en términos cuantitativo o estadístico, definidos por cuatro parámetros: ancho de banda, retraso temporal, variación de retraso (o jitter) y probabilidad de error (o pérdida de paquetes o fiabilidad). De esta manera se asegura un grado de fiabilidad preestablecido que cumpla los requisitos de tráfico en función del perfil y ancho de banda para un determinado flujo de datos.

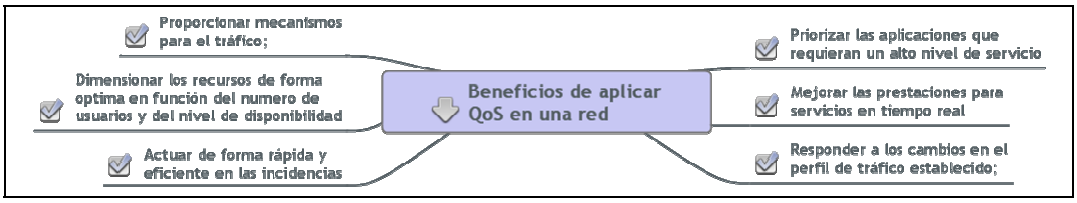


Figura 2. Beneficios de aplicar QoS
Fuente: Autoras

1.2 PARÁMETROS[2]

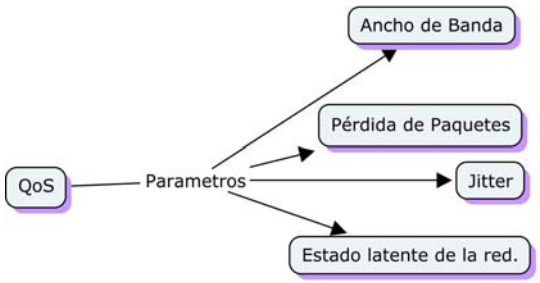


Figura 3. Parámetros de Qos
Fuente: Autoras

1.2.1 Ancho de banda

Es la media del número de bits por segundo que pueden ser transmitidos correctamente a través de la red. El caudal de medida suele encontrarse desde Kbps ó Mbps hasta Gbps2

[2] GARCÍA DUARTE, Gabriel. Desarrollo de Plano de Gestión Para Una Red MPLS. CATALUÑA Sistemas de Distribución de Tráfico sobre Redes Locales (SDTRL). Barcelona: 2005. p. 5.

1.2.2 Retardo punto a punto

Es el tiempo medio acumulado durante el trayecto de un paquete para atravesar la red de un punto a otro. Para medir con exactitud el retardo, se deben tener en cuenta los puntos donde éste se produce:

1.2.3 Retardo de propagación

Es el retardo que se obtiene del tiempo que tarda la luz en recorrer la fibra óptica por la que se transmite. El retardo medio suele ser del orden de 5m/s por cada 10.000Km aunque puede variar en función de los eventos que se sucedan sobre el medio de
Transmisión.

1.2.4 Retardo de conmutación

Se produce por el tiempo consumido en el procesado realizado para cambiar el enlace por el que un paquete ha entrado al *router.*

1.2.5 Retardo de clasificación (*scheduling*)

El retardo de *scheduling* o *queueing* se debe a la acción de clasificar el tráfico en las diferentes colas de los equipos de red. Desde el momento en el que un paquete llega a una cola, se decide cual es su clase correspondiente, se añade a esa cola y luego, se vuelve a transmitir a la salida de la cola generando un retardo en la transmisión. Según el tipo de algoritmo utilizado para la clasificación del tráfico este tiempo pude sufrir variaciones.

1.2.6 Retardo de serialización.

El retardo de serialización aparece cuando un paquete es adaptado a un medio por el cual se va a transmitir. La velocidad de ese mismo medio y el tamaño del paquete son determinantes para este retardo.

1.2.7 Jitter

Variación del retardo punto a punto de los paquetes causada por la clasificación y los retardos de acceso en el nodo fuente, y por el retardo de los nodos de tránsito y el *buffer* del nodo de recepción. Las variaciones que suceden durante estos procesos, por no tener comportamientos fijos, son los causantes de la aparición del *jitter*. Para muchas aplicaciones multimedia el *jitter* puede tener un efecto más dañino que un alto retardo de transmisión.

1.2.8 Pérdida de paquetes

La pérdida de paquetes es medida como un porcentaje de los paquetes transmitidos. Son los paquetes que siendo enviados nunca llegan a su destino. Los motivos que provocan una pérdida de paquetes son múltiples siendo la congestión el primer causante de ello. Concretamente, el límite de capacidad de los *buffers* de los dispositivos de red es el punto donde se registra el problema. A esto se añade, la retransmisión realizada por las aplicaciones cuando detectan que los paquetes no llegan. Una alternativa para evitar esta pérdida de paquetes es disponer de una velocidad de salida de datos mayor que la de entrada.

2. ALGORITMOS DE CLASIFICACIÓN[3]

2.1 WFQ (WEIGHTED FAIR QUEUING).

A cada cola se le asigna un "peso". Durante un espacio de tiempo (*time quantum)* se envía el tráfico pendiente en una cola en función del peso que le es asignado. Esto permite el envío de un mayor número de paquetes con alta prioridad sin dejar en el olvido a los paquetes con menos prioridad. La variable identificativa del modelo, además de los pesos es el *time quantum,* el cual depende de varios parámetros para ser calculado.

2.2 LLQ (LOW LATENCY QUEUING).

Este algoritmo aporta prioridad para aquellos paquetes que son clasificados como sensibles al retardo frente a los demás paquetes a transmitir. Las políticas de descarte determinan cuando un paquete se debe desechar. Estas medidas son necesarias para implementar cualquier esquema de clasificación. De hecho, no es estrictamente necesario esperar a que se llene una cola para proceder a descartar un paquete. Una política adecuada puede proceder a tomar estas medidas antes de que aparezca el problema en el buffer de la cola.

[3] GARCÍA DUARTE, Gabriel. Desarrollo de Plano de Gestión Para Una Red MPLS. CATALUÑA Sistemas de Distribución de Tráfico sobre Redes Locales (SDTRL). Barcelona: 2005. p. 16.

3. POLÍTICAS DE DESCARTE[4]

RED y WRED son dos ejemplos de políticas de descarte:

3.1 RED (RANDOM EARLY DETECTION).

Esta política establece, a partir de un valor específico de capacidad, una probabilidad de descarte linealmente creciente en función de la ocupación de la cola. Llegado a un umbral de ocupación (que no tiene que ser necesariamente el total de capacidad de la cola) se procede a descartar el paquete.

3.2 WRED (WEIGHTED RANDOM EARLY DETECTION).

La política WRED es la misma RED con la diferencia que utiliza diferentes probabilidades de descarte y valores umbrales en función de la clase de tráfico.

4. HERRAMIENTAS PARA LA ADMINISTRACION DE LA CONGESTION[5]

Figura 4. Herramientas administración de Congestión
Fuente: Autoras

4.1 FIFO (*First In First Out*)

Es una sencilla política que estable un orden de salida relacionado directamente con el orden de entrada a la cola. El primer paquete en entrar es el primero en salir. En su forma más simple, FIFO dispone de una cola de espera que supone guardar paquetes cuando la red está congestionada y los envía por orden de llegada cuando la red no está congestionada. FIFO es el algoritmo por defecto, dispone de una cola de espera que en algunos casos, no requiere ninguna configuración, pero tiene algunos defectos. El más importante, FIFO dispone de una cola de espera que no toma decisión sobre la prioridad del paquete; el orden de llegada determina el ancho de banda, la puntualidad, y la asignación de buffer. FIFO no suministra la protección contra

[4] GARCÍA DUARTE, Gabriel. Desarrollo de Plano de Gestión Para Una Red MPLS. CATALUÑA Sistemas de Distribución de Tráfico sobre Redes Locales (SDTRL). Barcelona: 2005. p. 17.

[5] Cisco CCNP V.5.0. Module 3.2.2 Congestion—Management Tools.

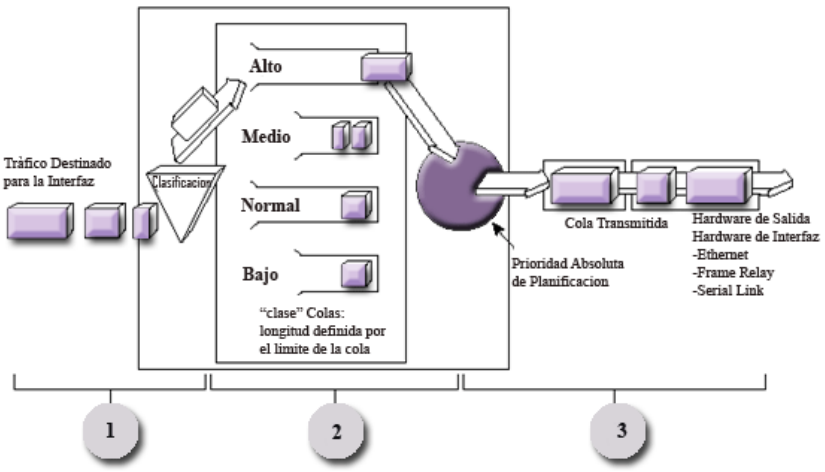
aplicaciones o malos comportamientos de flujos (fuentes). Las ráfagas de fuentes pueden causar retrasos largos de tiempo en el tráfico de aplicaciones sensibles como mensajes de señalización y control de la red.

4.2 PQ (*Prioritizing Traffic*)

Asegura que el tráfico importante reciba un servicio rápido en cada punto de la red, donde está mecanismo este presente. La prioridad de los paquetes puede diferenciarse por diversos medios, como: el protocolo de red, el interfaz del router por el que llegue el paquete, el tamaño del paquete y la dirección de origen o destino.

En PQ, cada paquete es puesto en una de cuatro colas que son: máxima, media, normal, o baja basadas en una prioridad asignada. Los paquetes que no son clasificados por este mecanismo de lista de prioridad se ubican en la cola normal. Durante la transmisión, el algoritmo da un tratamiento preferencial absoluto a la más alta prioridad sobre las colas de baja prioridad.

- Inconveniente: este método es estático y no se adapta a los requerimientos de la red.
- Además, pueden crear inanición, es decir dejar fuera de servicio a tráfico de menos prioridad.



1. *Clasificación por protocolo*
2. *Manejo de Interfaz*
3. *asignar enlace de ancho de banda por prioridad de la fuente*

Figura 5. Priorizar Tráfico
Fuente: http://informatica.uv.es/doctorado/SST/docto-2-qos.ppt

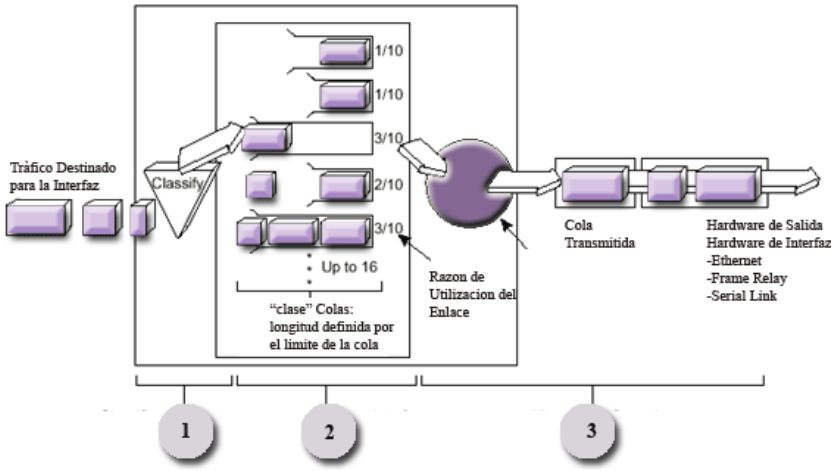
4.3 CQ: Garantizar el ancho de banda.

CQ fue diseñado para permitir que varias aplicaciones compartieran la red, y que además tuvieran asignado un ancho de banda mínimo garantizado, y unas garantías aceptables en cuanto a los retrasos

CQ permite que varias aplicaciones u organizaciones compartan la red con ancho de banda específico o requisitos de latencia mínimos entre aplicaciones. En estos ambientes el ancho de banda debe ser compartido proporcionalmente entre aplicaciones y usuarios.

CQ maneja colas de tráfico mediante la asignación de una cantidad determinada de espacio en la cola para cada clase de paquetes de servicios y a continuación, las colas en un round-robin.

- El ancho de banda se reparte equitativamente.
- En este método el acho de banda debe de ser compartido proporcionalmente entre las aplicaciones o usuarios en forma de Round Robin o quantos de tiempo, sin dejar tráfico fuera de servicio.



1. *Clasificación por protocolo*
2. *Manejo de Interfaz*
3. *asignar configuración en proporción al enlace de ancho de banda*

Figura 6. Garantizar Ancho de Banda
Fuente: http://informatica.uv.es/doctorado/SST/docto-2-qos.ppt

4.4 WFQ basado en flujo: crear imparcialidad entre los flujos

Para la situación en las que se debe suministrar un tiempo de respuesta constante a usuarios de la red sin añadir ancho de banda excesivo, la solución es WFQ – basado en flujo (llamado sólo WFQ comúnmente).

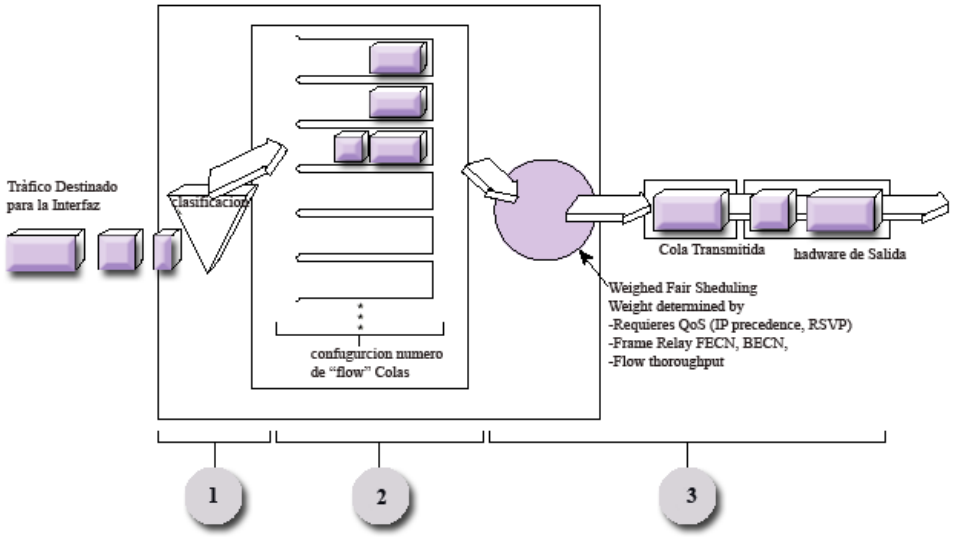
WFQ asegura que las colas no se desabastezcan de ancho de banda y que el tráfico consiga un servicio fiable para volúmenes de flujos bajos que comprenden la mayoría del tráfico, además reciben incrementó del servicio, transmitiendo algún número de bytes como si fueran volúmenes de flujos altos. Este comportamiento resulta en lo que parece ser un trato preferencial para tráfico de volumen bajo, cuando en realidad está creando imparcialidad.

4.5 WFQ basado en Clase: asegura el ancho de banda de la red

CBWFQ permite que un administrador de red cree clases de ancho de banda mínimas garantizadas. En lugar de suministrar una cola para cada flujo individual, el administrador define una clase que consta de uno o varios flujos, cada clase con una cantidad garantizada de ancho de banda.

CBWFQ impide a múltiples flujos de baja prioridad la introducción de una circulación máxima con una sola prioridad. Por ejemplo, WFQ proveerá un flujo de video que necesita la mitad del ancho de banda de un T1 si hay dos flujos. Pero, si más flujos son añadidos, el flujo de video tendrá menos ancho de banda porque el mecanismo de WFQ crea la imparcialidad. Si hay 10 flujos, el de video conseguirá solamente 1 / 10 del ancho de banda, que no es suficiente.

CBWFQ provee el mecanismo que suministra la mitad del ancho de banda que el video necesita. El administrador de la red define una clase, pone el flujo de video en la clase, y dice al router que provea 768 de kbps de servicio (la mitad de de un T1) para la clase. El video por lo tanto consigue el ancho de banda que necesita. El resto del flujo recibe una clase por defecto. La clase por defecto usa esquemas de WFQ - de circulación basados en que asignan el resto del ancho de banda (la mitad de del T1, en este ejemplo).



1. *Clasificación por protocolo*
2. *Manejo de Interfaz*
3. *Asignar "Fair" Proporcional al enlace de ancho de banda*

Figura 7 CBWFQ
Fuente: http://informatica.uv.es/doctorado/SST/docto-2-qos.ppt

5. MODELOS DE SUMINISTRO DE QoS

El diseño básico de Internet provee la entrega de paquetes de mejor esfuerzo y no ofrece garantías. Este enfoque es aún predominante en Internet hoy en día y sigue siendo adecuado para la mayoría de los propósitos. Este tipo de algoritmo se centra en garantizar la llegada de cada uno de los paquetes peno no, del tiempo que transcurre durante su recorrido, lo cual hace que la red no sea eficiente en el transporte de tráfico como el multimedia o teletrabajo. En base a esto se hace necesario el uso de otros algoritmos más eficientes que permitan dar una cuota de respeto al límite de llegada de los paquetes.

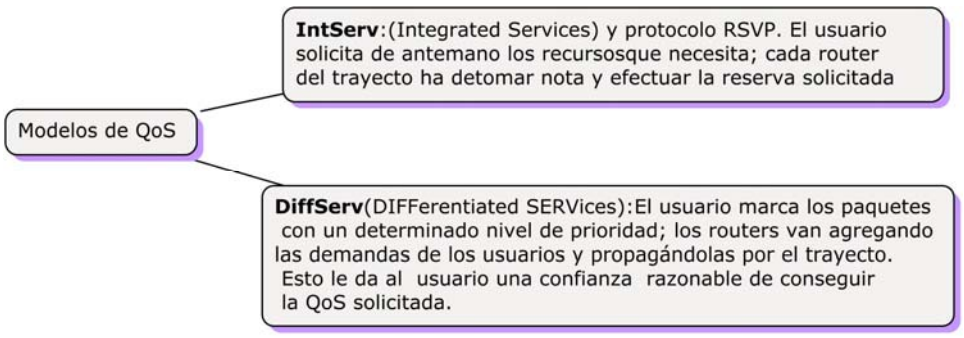


Figura. 8 Tipos de calidad de servicio IntServ
Fuente: Autoras

5.1 MODELO DE QoS *INTSERV*

El modelo de servicios diferenciados o *IntServ*[6] (*INTegrated SERVices*) realiza una reserva previa de recursos antes de establecer la comunicación. El protocolo que lleva a cabo la reserva de recursos y la señalización de establecimiento de rutas es el RSVP[7]. Para el modelo *IntServ* existen tres tipos de calidad de servicio:

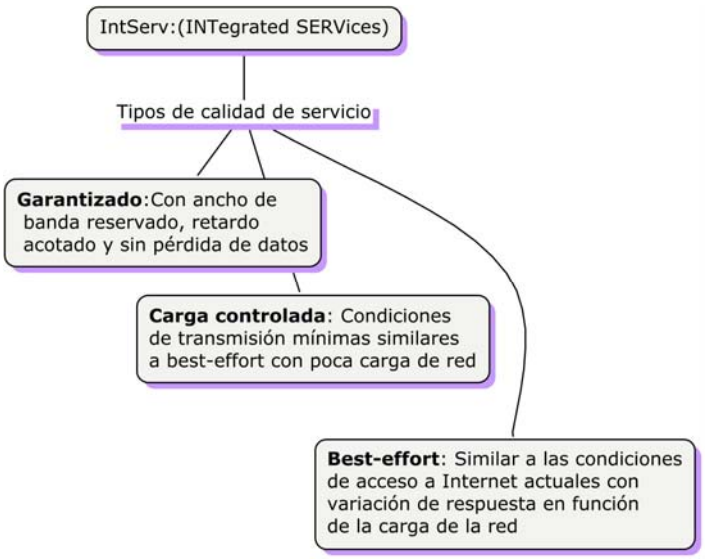


Figura 9: Tipos De Calidad De Servicio Intserv
Fuente: Autoras

5.2 MODELO DE QoS *DIFFSERV*

El usuario marca los paquetes con un determinado nivel de prioridad; los routers van agregando las demandas de los usuarios y propagándolas por el trayecto. Esto le da al usuario una confianza razonable de conseguir la QoS solicitada

El modelo de servicios diferenciados o *DiffServ*[8] *(DIFFerentiated SERVices*) es propuesto por la IETF para habilitar una cierta clasificación del tráfico IP en un número limitado de clases de servicio. Si bien los *DiffServ* no establecen una ruta extremo a extremo para conocer el estado de la red. Con todos los dispositivos de red con clases de servicio configuradas se llega a obtener un

[6] RFC2205 Resource ReSerVation Protocol (RSVP) Version 1 Especificaciones funcionales 1997.
[7] RFC 2206 RSVP Management Information Base using SMIv2 1997.

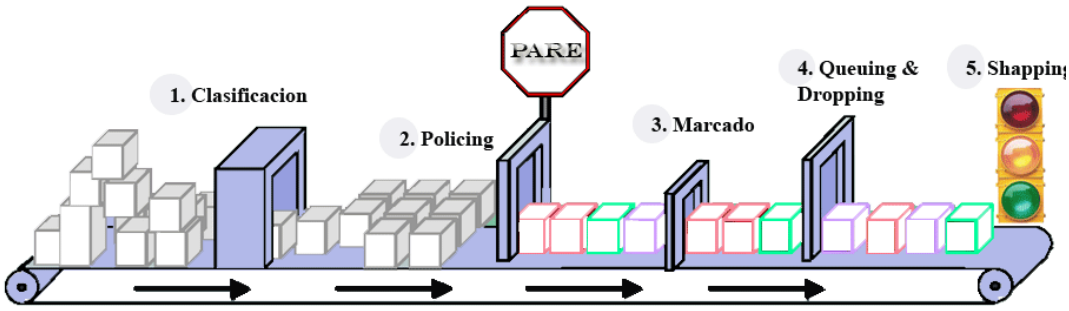
[8] RFC 2474 Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers 1998.

resultado preferente para tráfico prioritario con respecto a los demás cuando la red está congestionada.

Los servicios diferenciados son propuestos para resolver problemas que aparecen en los servicios integrados y en RSVP, siendo el modelo *DiffServ* más escalable, flexible y sencillo. El modelo *DiffServ* propone la división del tráfico en función de su prioridad, resolviendo el problema de la señalización marcando el mismo paquete en los campos de su cabecera. De hecho, tan solo se definen los valores del campo DS de la cabecera IP y los PHBs (*Per Hop Behaviour*). Es el proveedor el responsable del tratamiento del tráfico y de los servicios que desea implementar.

Se han desarrollado y estandarizado los dos mecanismos de QoS, reserva y prioridad:

- IntServ (Integrated Services) y protocolo RSVP. El usuario solicita de antemano los recursos que necesita; cada router del trayecto ha de tomar nota y efectuar la reserva solicitada.
- DiffServ (Differentiated Services). El usuario marca los paquetes con un determinado nivel de prioridad; los routers van agregando las demandas de los usuarios y propagándolas por el trayecto. Esto le da al usuario una confianza razonable de conseguir la QoS solicitada. *Es el más interesante actualmente.*



1. *Identificar y separar tráfico en las diferentes clases*
2. *Descartar tráfico que se comporta mal para garantizar la integridad de la red*
3. *Marcar tráfico, si es necesario. Asigna al DSCP el valor que corresponde*
4. *Priorizar, proteger y aislar tráfico*
5. *Controlar ráfagas y controlar tráfico*

Figura 10. Implementación de Diffserv en los Routers
Fuente: www2.ing.puc.cl/~iee3542/amplif_4.ppt

SERVICIOS INTEGRADOS (INTSERV)	SERVICIOS DIFERENCIADOS (DIFFSERV)
• Introducido por IETF en 1994 RFC1633 • Son aplicables en redes pequeñas • Funciona en el nivel 4 del modelo OSI • Permite solicitudes de calidad de servicio con gran granularidad • Necesitan periódicamente refrendar el tipo de servicio. • Utilizan un protocolo para designar recursos. • Emulan conmutación de circuitos • Posee un mecanismo complejo y mas exigente	• Presenta un buen desempeño tanto en redes pequeñas como grandes. • Trabaja en el nivel 3 del modelo OSI, el cual lo hace tranparente para el usuario. • Tiene solo 12 posibilidades de servicio. • Los tipo de servicio son permanentes • Los recursos son asignados en el ruteado de frontera. • Los nodos internos procesan los paquetes de acuerdo al campo DS. • Tiene una forma sencilla de clasificar y priorizar el tráfico

Tabla 1. Comparativo entre las dos principales arquitecturas de QoS
Fuente: LANDA ROSALES, Oscar Gonzalo. Sistemas de Distribución de Tráfico sobre Redes Locales (SDTRL). México: 2004. p. 20.

6. USO DE MQC PARA IMPLEMENTAR QoS[9]

MQC[10] permite a los usuarios crear políticas de tráfico y luego adjuntar estas políticas a una interfaz. Una política QoS contiene una o más clases de tráfico y una o más características de QoS. Una clase de tráfico clasifica el tráfico, y las características de QoS en la política QoS determinan cómo tratar el tráfico clasificado.

MCQ al permitir la separación de la clasificación del tráfico de las definiciones de la política QoS, da facilidad en la implementación inicial QoS y mantenimiento a medida que nuevas clases de tráfico y políticas de QoS emergen para la evolución de la red.

6.1 PASO 1: CONFIGURACION DEL MAPA DE CLASE

Un mapa de clase define el tráfico dentro de grupos con plantillas de clasificación que son usadas en mapas de política donde mecanismos de QoS son vinculados a las clases. Se puede configurar más de 256 clases de mapas sobre un router. Por ejemplo, asignar aplicaciones de video a un mapa de clase llamado video, y tráfico de aplicaciones de e-mail a un mapa de clase llamado mail.

El comando de configuración global **class-map** crea un mapa de clase. Cada mapa de clase contiene una o más condiciones que definen cuáles paquetes pertenecen a la clase.

Sintaxis de configuración del comando **class-map.**

Router(config)#
Class-map [match-all ı match-any] class-map-nombre

Router(config-cmap)#
match any
match not match-criteria

Router(config-cmap)#
description descripción

[9] Quality of Service (QoS)
[10] Cisco CCNP V.5.0. Module 3.4.3 Modular QoS CLI.

Hay dos maneras de procesar condiciones cuando hay más de una condición en el mapa de clase:

- **Match all:** debe conocer todas las condiciones para unir el paquete a la clase.
- **Match any:** conoce por lo menos una condición para unir el paquete a la clase.

La estrategia match por defecto de mapas de clase es el match all.

Los comandos **match** especifican varios criterios para clasificar los paquetes. Los paquetes son revisados para determinar si ellos coinciden con los criterios que son especificados en los comandos match. Si un paquete coincide con el criterio especificado, ese paquete es considerado un miembro de la clase y es enviado de acuerdo al set de especificaciones QoS en la política de tráfico. Los paquetes que fallan al conocer los criterios de coincidencia son clasificados como miembros de la clase de tráfico por defecto.

MQC no requiere necesariamente que los usuarios asocien una sola clase de tráfico a una política de tráfico. Múltiples tipos de tráfico pueden ser asociados con una clase de tráfico usando el comando **match any.**

El comando **match not** invierte la condición especificada. Este comando especifica un valor de criterio de coincidencia que evita a los paquetes ser clasificados como miembros de una clase de tráfico específica. Todos los otros valores de este criterio de coincidencia particular pertenecen a la clase.

El comando **description** es usado para documentar un comentario acerca del mapa de clase.

Hay muchas maneras de clasificar el tráfico cuando configuramos mapas de clases. La siguiente sintaxis muestra una posible manera de clasificar tráfico utilizando listas de control de acceso (ACLs) para especificar el tráfico que necesita ser asociado para la política de QoS. Los mapas de clases soportan estándar ACLs y ACLs extendido.

Router (config)#
access-list access-list-number {permit ı deny ı remark} source [mask]

Router (config)#
access-list access-list-number {permit ı deny} protocol source
source-wildcard [operator port] destination destination-wildcard
[operator port] [established] [log]

Router (config-cmap)#
Match access-group access-list-number

El comando **match access-group** permite a una ACL ser usada como un criterio de asociación para la clasificación del tráfico.

El comando **match not** es usado para especificar un valor de política de QoS especifico que no es usado como un criterio de adición. Cuando usamos el comando **match not,** todos los otros valores de la política de QoS se convierten en un criterio de adición exitoso.

A continuación se muestra la tabla con los comandos resumidos para la configuración de la clase y su propósito:

Comando	Propósito
Router(config)**# class-map** class-map-name	Especifica el nombre definido por el usuario para la clase de tráfico. Los nombres pueden tener un máximo de 40 caracteres. En este caso, el tráfico debe cuadrar con todos los criterios de clasificación del tráfico.
Router(config)**# class-map match-all** class-map-name	Especifica que todos los criterios de comparación deben darse en el tráfico entrante para poder ser clasificado como parte del tráfico de la clase.
Router(config)**# class-map match-any** class-map-name	Especifica que uno de los criterios de clasificación debe darse para poder clasificar el tráfico entrante como tráfico de la clase.
Router(config-cmap)**# match any**	Especifica que todos los paquetes serán comparados
Router config-cmap)**# match class-map** class-name	Especifica el nombre de la clase de tráfico que sera usada como criterio de comparación
Router(config-cmap)**# match ip dscp** ip-dscp-value	Especifica up to eight differentiated services code point (DSCP) values used as match criteria. The value of each service code point is from 0 to 63.
Router (config-cmap)**# match protocol** *protocol*	Especifica el nombre del protocolo usado.

Tabla 2. Resumen de comandos configuración de clase
Fuente: Autoras

6.2 PASO 2: CONFIGURACIÓN DEL MAPA DE POLÍTICA.

El comando **policy-map** crea una política de tráfico. El propósito de una política de tráfico es configurar las características de QoS que deberían ser asociadas con el tráfico el cual luego es clasificado en una clase o en clases de tráfico. Se puede asignar mayor cantidad de ancho de banda o ajustar cualquier prioridad que se necesite para una clase determinada. Una política de tráfico contiene tres elementos: un nombre (case-sensitive), una clase de tráfico (especificada con el comando **class**), y las políticas de QoS.

El comando **policy-map** específica el nombre de una política de tráfico (por ejemplo, colocando el comando **policy-map class1** crearía una política de tráfico llamada class 1). Después se entra al modo de configuración **policy-map**, y se introduce el nombre de la clase de tráfico. Se debe estar en el modo de configuración **policy-map** para introducir características QoS que se aplican al tráfico que coincida con la clase llamada. Un paquete solo puede asociar una clase dentro de una política de tráfico. Si un paquete asocia más de una clase en la política de tráfico, la primera clase definida en la política de tráfico es usada.

MQC no requiere necesariamente que se asocie una clase de tráfico a una sola política de tráfico. Cuando los paquetes se asocian a mas de un criterio de adicción, múltiples clases de tráfico pueden ser asociadas con una sola política de tráfico.

Un mapa de política puede tener más de 256 clases usando el comando class con el nombre de mapa de clase configurado. A continuación se muestra la siguiente sintaxis de los comandos **policy-map** y **class**.

Router (config)#
policy-map policy-map-nombre

Router (config-pmap)#
Class {class-name ı class-default}

Router (config-pmap)#
Class class-name condición

Una clase inexistente puede también ser usada dentro de un modo de configuración de mapa de política sí la condición de adición es especificada después del nombre de la clase. La configuración que se está corriendo se reflejara como una configuración por medio del uso de la estrategia match-any e insertando toda una configuración de mapa de clase.

Todo el tráfico no identificado en cualquiera de todos los mapas de clase que son usados dentro del mapa de política, se convierten en parte de la clase por defecto. Esta clase no tiene garantías de QoS por defecto, la clase por defecto, cuando es usada sobre salidas, puede usar cola FIFO o WFQ.

A continuación se muestra la tabla con los comandos resumidos para la configuración de la política y su propósito:

Comando	Propósito
Router (config-pmap)# ***class*** *class-name*	Especifica que esa clase de tráfico (puede ser predefinida), que fue configurada con el commando class-map, se usa para clasificar el tráfico en la política de tráfico.
Router (config-pmap)# ***class class-default***	Para utilizar en la política la clase por defecto, se utiliza este commando.
Router (config-pmap-c)# ***bandwidth*** *{bandwidth-kbps |* ***percent*** *percent}*	Especifica un ancho de banda mínimo que se garantiza a una clase de tráfico en periodos de congestión.
Router (config-pmap-c)# ***default*** *command*	Establece cualquier commando a su valor por defecto
Router (config-pmap-c)# ***fair-queue*** *number-of-queues*	Especifica en número de colas reservadas para una clase de tráfico
Router (config-pmap-c)# ***police*** *bps burst-normal burst-max* ***conform-action*** *action* ***exceed-action*** *action* ***violate-action*** *action*	Especifica un ancho de banda máximo utilizable por una clase de tráfico usando el algoritmo token bucket..
Router (config-pmap-c)# ***queue-limit*** *packets*	Especifica el máximo número de paquetes encolados para una clase de tráfico (en ausencia del commando random-detect)
Router (config-pmap-c)# ***random-detect***	Habilita la política WRED (Weighted Random Early Detection) para una clase de tráfico que tiene un ancho de banda garantizado..
Router (config-pmap-c)# ***set ip dscp*** *ip-dscp-value*	Especifica el valor IP DSCP de paquetes dentro de una clase de tráfico. El valor IP DSCP está en el rango 0 a 63.
Router (config-pmap-c)# ***service-policy*** *policy-map-name*	Especifica el nombre de una política de tráfico que se usará como criterio de equiparación.

Tabla 3. Resumen de comandos configuración de política
Fuente: Autoras

6.3 PASO 3: ADJUNTAR UNA POLITICA DE SERVICIO A LAS INTERFACES.

En una ACL, se debe aplicar el mapa de política a una interfaz especifica que se quiera afectar. Se puede aplicar el mapa de política en cualquier modo salida o entrada. El último paso de configuración es adjuntar un mapa de política a los paquetes de entrada o de salida usando el comando **service-policy**.

El router inmediatamente verifica los parámetros que son usados en el mapa de política. Si hay un error en la configuración del mapa de política, el router muestra un mensaje explicando que esta mal el mapa de política.

Después de que se defina una política de tráfico con el comando **policy-map**, se puede adjuntarla a una o más interfaces para especificar la política de tráfico para estas interfaces por medio del uso del comando **service-policy** en el modo de configuración de interfaz. Aunque se puede asignar la misma política de tráfico para múltiples interfaces, cada interfaz puede tener solo una política de tráfico adjunta a la salida como a la entrada.

6.4 CONFIGURACIÓN DE CLASE DE TRÁFICO POR DEFECTO.

El tráfico no clasificado (tráfico que no conoce el criterio de asociación especificado en las clases de tráfico) es tratado como pertenecientes a la clase de tráfico por defecto. Si el usuario no configura una clase por defecto, los paquetes siguen siendo tratados como miembros de la clase por defecto. Sin embargo, la clase por defecto no tiene ninguna característica habilitada. Por lo tanto, paquetes pertenecientes a una clase por defecto sin características configuradas no tienen funcionalidad de QoS. Estos paquetes son luego puestos dentro de una cola FIFO y enviados a una tasa determinada por el ancho de banda disponible del enlace. Esa cola FIFO es gestionada por caída de cola[11].

[11] Caída de cola es un medio que evita congestión y que trata todo el tráfico por igual y no diferencia entre clases de servicio. Llenar colas durante el periodo de congestión. Cuando la cola de salida esta llena y la caída de cola se esta efectuando, los paquetes se dejan caer hasta que la congestión sea eliminada y la cola no sea mas llenada.

7. MAPAS DE CLASES ANIDADOS.

Si se quiere combinar características match-any y match-all, se crea una clase de tráfico usando una instrucción de criterio de adición (sea match-any o match-all) y luego usar esta clase de tráfico como un criterio de adición en una clase de tráfico que use un diferente tipo de criterio de adición.

El único método de incluir ambas características match-any y match-all en una sola clase de tráfico es con el uso del comando match class-map. Para combinar características match-any y match-all en una sola clase, una clase de tráfico creada con la instrucción match-any debe usar una clase configurada con la instrucción match-all como criterio de adición (a través del comando match class-map), o viceversa.

La analogía ilustrada en la figura 11, servirá para clarificar el concepto. Se asume que se busca una base de datos que contenga los salarios de profesores de ingenierías o profesores de arquitectura en una base de datos. En términos boléanos, su búsqueda está representada por la frase (salarios AND {profesores de ingenierías OR profesores de arquitectura}). Eso es una "búsqueda anidada", una búsqueda dentro de otra. La parte de la búsqueda encerrada en corchetes, profesores de ingenierías OR profesores de arquitectura, será llevada a cavo primero, seguida de la operación AND. En esta búsqueda se recuperaran objetos sobre salarios y profesores de ingenierías y también como salarios y profesores de arquitectura.

Figura 11. Diagrama de Ven
Fuente: Autoras

El diagrama de Venn muestra seis sectores diferentes, tres de los cuales se superponen en un grado. El área de superposición en el centro incluye salarios, profesores de arquitectura y profesores de ingenierías. El área a la derecha del centro contiene objetos sobre salarios y profesores de arquitectura. El área de superposición a la izquierda del centro contiene objetos sobre salarios y profesores de ingenierías. Sólo la parte izquierda del centro y la derecha coinciden con nuestro criterio.

El siguiente ejemplo se refiere a la creación de mapas de clase. Suponiendo que A, B, C, y D son todos los criterios de adición separados, y se quiere tráfico asociado con A, B, o, C, y, D para ser clasificado como perteneciente a la clase de tráfico. En términos boléanos, la ecuación anidada es (A or B or {C y D}). Fuera de la clase de tráfico anidada, el tráfico o bien tiene que coincidir con todos los cuatro criterios de adición (A and B and C and D) o coincidir cualquiera de los criterios de adición(A or B or C or D) para ser considerado parte de la clase de tráfico. No es posible combinar declaraciones “and” (match-all) y “or” (match-any) dentro de la clase de tráfico.

La solución es crear una clase de tráfico usando match-all para C y D (el cual llamaremos criterio E), y luego crear una clase de tráfico match-any usando A, B, y E. la nueva clase de tráfico tendría la secuencia de evaluación correcta (A or B or E, el cual también podría ser A or B or {C and D}). La configuración de clase de tráfico deseada está completa.

El único método de incluir ambas características match-any y match-all en una sola clase de tráfico es con el uso del comando match class-map. Para combinar características match-any y match-all en una sola clase, una clase de tráfico creada con la instrucción match-any debe usar una clase configurada con la instrucción match-all como criterio de adición (a través del comando match class-map), o viceversa.

8. CLASIFICACIÓN Y MARCADO

La clasificación, marcado y formación de colas son funciones críticas de cualquier implementación de QoS exitosa. La clasificación permite a los dispositivos de red identificar el tráfico como perteneciente a una clase específica con los requerimientos de QoS, determinados por una política administrativa de QoS. Después de que el tráfico de la red se ordena, los paquetes individuales son marcados de modo que otros dispositivos de la red puedan aplicar características de QoS uniformemente a estos paquetes que se relacionan con la política de QoS definida. Las colas despachan los paquetes de acuerdo a sus marcas.

8.1 CLASIFICACIÓN:

La clasificación es el proceso de identificar el tráfico y categorizar ese tráfico en las clases. La clasificación usa un descriptor de tráfico para categorizar un paquete dentro de un grupo específico y definir ese paquete. Entre los descriptores de tráfico se encuentran:

- La interfaz entrante
- IP precedence
- Diferenciación de los servicios codifican el punto (DSCP)
- Fuente o dirección del destino
- La aplicación

Después de que el paquete ha sido clasificado o identificado, el paquete es entonces accesible para la calidad de servicio que se maneja en la red.

Usando la clasificación, los administradores de red pueden dividir el tráfico de la red en múltiples clases de servicio (CoS siglas en ingles para class of service).

Los varios mecanismos de calidad de servicio, como policing de tráfico, shaping de tráfico y técnicas de colas, usan el descriptor de tráfico del paquete (es decir, la clasificación del paquete) para asegurar la fidelidad a ese acuerdo.

- **policing de tráfico**: Cuando el flujo de tráfico alcanza el flujo máximo configurado, el exceso de tráfico es descartado (o remarcado). El resultado es un rendimiento que aparece como una señal diente de sierra con cimas y valles.

- **shaping de tráfico**: en contraste con el policing, el shaping de tráfico conserva paquetes de exceso en una cola y luego programa el exceso para una transmisión posterior sobre incrementos de tiempo. El resultado del shaping de tráfico es una taza de salida de paquetes suavizada.

8.2 MARCACIÓN:

Marcar permite los dispositivos de la red clasificar un paquete o trama basado en un descriptor de tráfico específico.

Las herramientas de clasificación de QoS categorizan los paquetes examinando los contenidos de las cabeceras de las tramas y paquetes; mientras que las herramientas de marcación permiten que las herramientas de QoS cambien bits en la cabecera del paquete para indicar el nivel de servicio que el paquete debería recibir de otras herramientas QoS. El marcado (marking) consiste en colocar un valor dentro de uno de los números de trama definidos, paquetes, o campos de cabecera de celda especialmente diseñados para QoS marking. El marcado (marking) puede ser usado para poner la información en la trama de capa 2 o en la cabecera de los paquetes de capa 3.

Los descriptores de tráfico que son usados típicamente se incluyen en la siguiente tabla:

Capa de enlace	CoS (Inter-Switch Link [ISL], 802.1p)
	Multiprotocol Label Switching (MPLS) experimental (EXP) bits
	Frame Relay
Capa de red	DSCP
	Precedencia IP

Tabla 4. Descriptores de tráfico
Fuente: Autoras

8.3 COMPORTAMIENTOS PER-HOP.

Los routers que conocen DiffServ implementan conductas per-hop (PHBs), el cual define las propiedades de envió del paquete asociado con una clase de tráfico. Diferentes PHBs pueden ser definidas para ofrecer, por ejemplo, la baja pérdida, propiedades de envió de baja latencia o propiedades de envió de mejor esfuerzo. Todo el tráfico que fluye a través de un router que pertenece a la misma clase está catalogado como un agregado de conducta (BA).

Los valores DSCP marcan los paquetes para seleccionar un PHB. Dentro del núcleo de la red, los paquetes son enviados de acuerdo al PHB que es asociado con el DSCP. El PHB es un comportamiento observable exterior aplicado a un nodo compatible con DiffServ, a una colección de paquetes con el mismo valor de DSCP. Los distintos comportamientos son principalmente observados cuando múltiples BAs compiten por recursos del ancho de banda y buffer en un nodo.

La relación entre PHBs en un grupo puede ser en términos de la prioridad absoluta o relativa, aunque no siempre se requieren varios debido a que un solo PHB definido en forma aislada ya es un caso especial de un grupo PHB.

Los grupos PHB deben ser definidos de tal manera que la asignación del recurso apropiada entre los grupos puede ser inferida y mecanismos integrados puedan ser implementados y que puedan simultáneamente soportar dos o más grupos. Una definición de un grupo PHB debe indicar los posibles conflictos con grupos PHB previamente documentados que podrían prevenir el funcionamiento simultáneo.

El IETF define los siguientes PHBs:

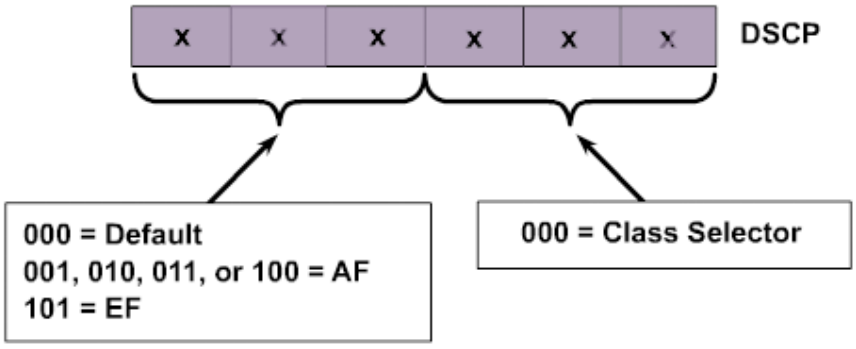


Figura 12. PHBs
Fuente: Autoras

- **Default PHB**: Usado para servicios de mejor esfuerzo (los bits del 5 a 7 del DSCP iguales a 000)
- **Expedited Forwarding (EF) PHB**: Usado para servicios de bajo retardo (los bits del 5 a 7 del DSCP iguales a 101)
- **Assured Forwarding (AF) PHB**: Usado para servicios de ancho de banda garantizado (los bits del 5 a 7 del DSCP iguales a 001, 010, 011, o 100)

8.3.1 EF PHB

La siguiente figura es una vista detallada del EF PHB usado en DSCP. El EF PHB se identifica basado en lo siguiente:

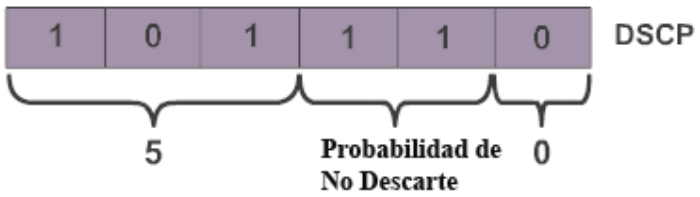


Figura 13. EF PHB usado en DSCP
Fuente: Autoras

- **El EF PHB garantiza una mínima tasa de salida**: El EF PHB proporciona el retraso más bajo posible a las aplicaciones sensibles al retraso.
- **El EF PHB garantiza el ancho de banda**: El EF PHB previene la inanición de la aplicación si hay múltiples aplicaciones usando EF PHB.
- **El EF PHB vigila el ancho de banda cuando la congestión ocurre:** El EF PHB previene inanición de otras aplicaciones o clases que no están usando este PHB.

Los paquetes que requieren EF deben ser marcados con un valor DSCP binario de 101110 (46 o 0x2E).

Los dispositivos que no comprenden DiffServ consideran el valor EF DSCP 101110 como precedencia IP 5 (101). Esta precedencia es la precedencia IP de usuario-definible más alta y se usa típicamente para el tráfico sensible al retardo (como VoIP). Los bits 5 a 7 del valor EF DSCP son 101 que coinciden con la precedencia IP 5 y permiten la compatibilidad.

8.3.2 AF PHB

El AF PHB es identificado basado en lo siguiente:

- El AF PHB garantiza un cierto monto de ancho de banda a una clase AF.
- El AF PHB permite el acceso a un ancho de banda extra, si es disponible.

Los paquetes que requieren AF PHB deben se marcados con un valor DSCP de aaadd0 dónde aaa es el número de la clase y dd es la probabilidad de la caída.

Hay cuatro clases estándar de AF definidas: AF1, AF2, AF3, y AF4. Cada clase debe ser tratada independientemente y debe de tener asignado un ancho de banda que esta basado sobre la política de QoS.

Hay tres valores de DSCP asignados a cada uno de las cuatro clases de AF como se muestra en la siguiente figura, y la tabla de valores de DSCP Asignados a las Clases de AF.

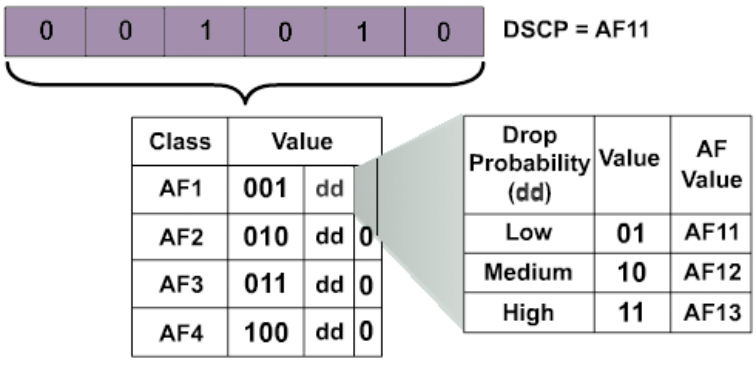


Figura 14. AF PHB
Fuente: Autoras

	Clase 1	**Clase 2**	**Clase 3**	**Clase 4**
Precedencia con baja probabilidad de descarte	AF11 = 10 (001010)	AF21 = 18 (010010)	AF31 = 26 (011010)	AF41 = 34 (100010)
Precedencia con probabilidad de descarte media	AF12 = 12 (001100)	AF22 = 20 (010100)	AF32 = 28 (011100)	AF42 = 36 (100100)
Precedencia con alta probabilidad de descarte	AF13 = 14 (001110)	AF23 = 22 (010110)	AF33 = 30 (011110)	AF43 = 38 (100110)

Tabla 5. Marcado DSCP AF
Fuente: Autoras

9. SELECCIÓN DEL MODELO DE CALIDAD SERVICIO

Después del estudio realizado en el apartado anterior, se determina que la solución más apropiada para ofrecer Calidad de Servicio en un modelo de red en fig. 15 es utilizar DiffServ. Se llego a esta conclusión tomando en cuenta que (los modelos de red) soportan tanto Inserv como Diffserv, pero DiffServ envía información de calidad de servicio en los datagramas, lo que permite implementar calidad de servicio escalable a cualquier cantidad de flujos.

La Arquitectura de Servicios Integrados, InffServ es utilizada principalmente en Redes de Acceso debido a que se adapta fácilmente a las necesidades de recursos de los usuarios pero a su vez tiene problemas de escalabilidad debido al agotamiento de los recursos de la red. Por otro lado, la Arquitectura de Servicios Diferenciados es muy escalable (soporta una gran cantidad de usuarios) pero a cambio, no puede adaptarse fácilmente a las necesidades de recursos de los usuarios, por tanto, *DiffServ* es utilizada principalmente en Redes de Transporte.

En IntServ es necesario hacer una reservación previa del canal y se requiere señalización para mantener dicha reservación, además no es un modelo escalable. También es importante mencionar que actualmente el mercado dispone modelos de red que soportan DiffServ, lo que hace posible la utilización del protocolo.

9.1 PRÁCTICA DE CALIDAD DE SERVICIO QoS

Objetivo

Configurar calidad de servicio en el modelo de red que se muestra en la figura 15, haciendo uso de la herramienta GNS3[12] para emular la topología con los respectivos routers, un analizador de redes o snifer WIRESHARK[13] para observar el tráfico a través de los enlaces de la topología.

Herramientas de Software Utilizadas

GNS3 es un simulador gráfico de redes que permite diseñar fácilmente topologías de red y luego ejecutar simulaciones en el. Hasta este momento GNS3 soporta el IOS de routers, ATM/Frame Relay/switchs Ethernet y PIX firewalls.

[12] http://pfe.epitech.net/frs/download.php/541/GNS3-0.3.1_documentation.pdf
[13] www.wireshark.com

GNS3 esta basado en Dynamips, PEMU (incluyendo el encapsulador) y en parte en Dynagen, fue desarrollado en python a través de PyQt la interfaz grafica (GUI) confeccionada con la poderosa librería Qt, famosa por su uso en el proyecto KDE. GNS3 también utiliza la tecnología SVG (Scalable Vector Graphics) para proveer símbolos de alta calidad para el diseño de las topologías de red.

Dynamips es un emulador de routers Cisco escrito por Christophe Fillot. Emula a las plataformas 1700, 2600, 3600, 3700 y 7200, y ejecuta imágenes de IOS estándar.

Este tipo de emulador es útil para:

- *Ser utilizado como plataforma de entrenamiento, utilizando software del mundo real. Permite la familiarización con dispositivos Cisco, siendo Cisco el líder mundial en tecnologías de redes.*

- *Probar y experimentar las funciones del Cisco IOS.*

- *Verificar configuraciones rápidamente que serán implementadas en routers reales.*

- *Este emulador no puede reemplazar a un router real, es simplemente una herramienta complementaria para los administradores de redes.*

INSTALACIÓN DE GNS3

GNS3[14] es el software utilizado en la práctica de Calidad de Servicio (QoS). Y para su previa utilización se deben hacer los siguientes pasos.

1. Según la figura 15 se ejecuta el setup.exe

[14] **GNS-3** es un entorno gráfico de simulación de redes complejas, utilizando dispositivos emulados **CISCO** como routers y switches.

Figura 15. Setup.exe de instalación de GSN3
Fuente: Autoras

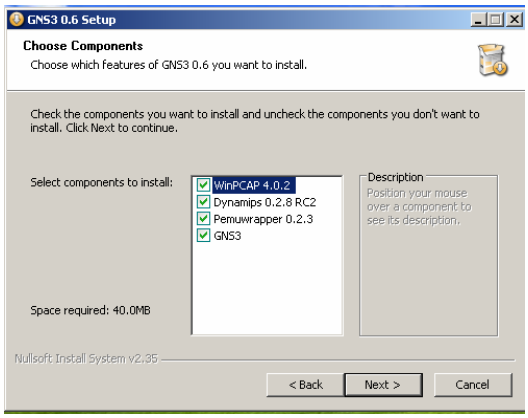


Figura 16. Aplicativos a Instalar
Fuente: Autoras

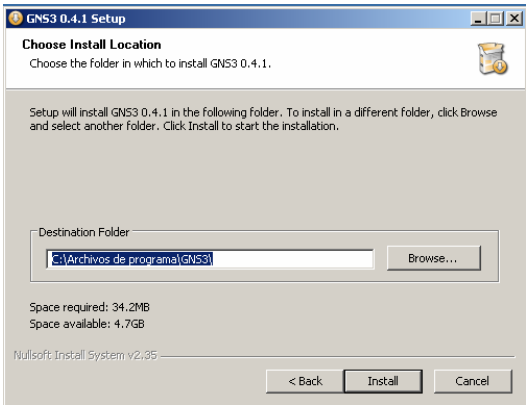


Figura 17. Localización de la instalación
Fuente: Autoras

2. Se ingresa en la carpeta donde quedo instalado la ruta, C:\Archivos de programa\GNS3, se crean dos carpetas llamadas **Lab** y **IOS** respectivamente; en esta última carpeta se guardan todas las IOS con las que se trabajan. Ver figura 18.

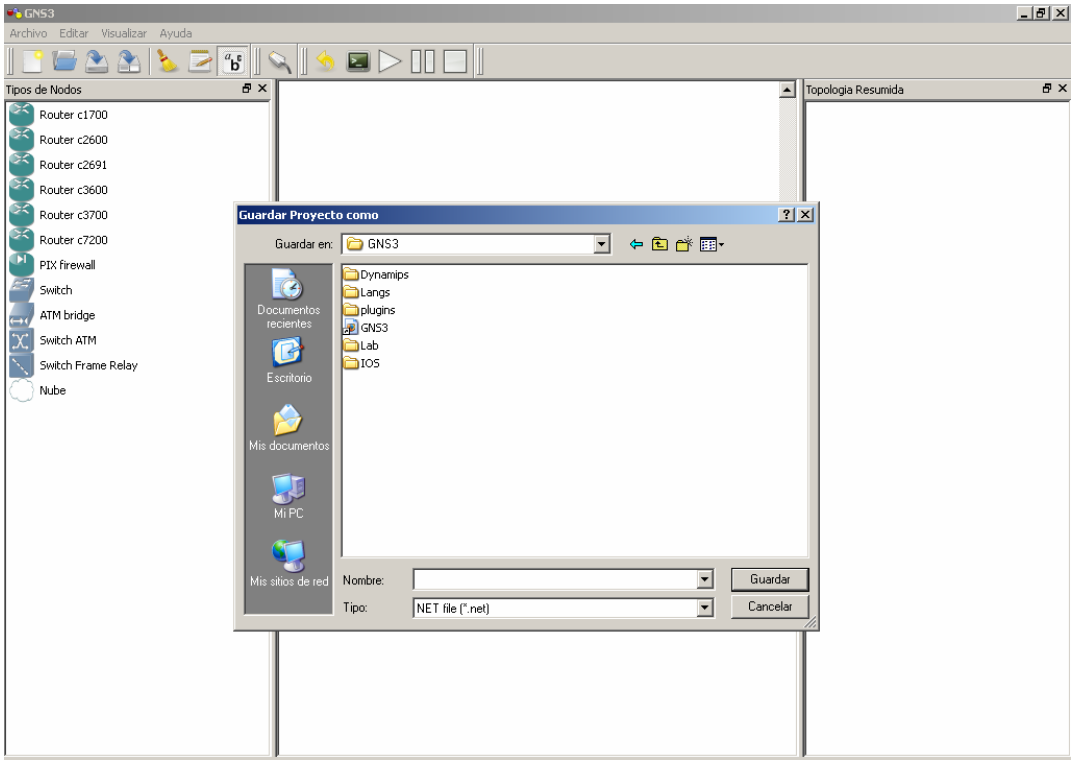


Figura 18. Ruta para creación de carpetas de Trabajo
Fuente: Autoras

3. En la opción editar\preferencias se configura el idioma, los directorios de trabajo y el ejecutable de Dynamips. Ver Figura 19.

- Lenguaje: Español(es)
- Comando de Terminal: C:\putty.exe –telnet %h %p
- Directorio del Proyecto: C\Archivos de Programas\GNS3\Lab
- IOS/PIX directory: C:\Archivos de programas\GNS3\Lab

Para trabajar los routers en modo consola; se trabajara con el putty y su ruta será C:\putty.exe, previamente hay que pegar el ejecutable en disco C; aplicar, aceptar y guardar cambios. Ver figura 20.

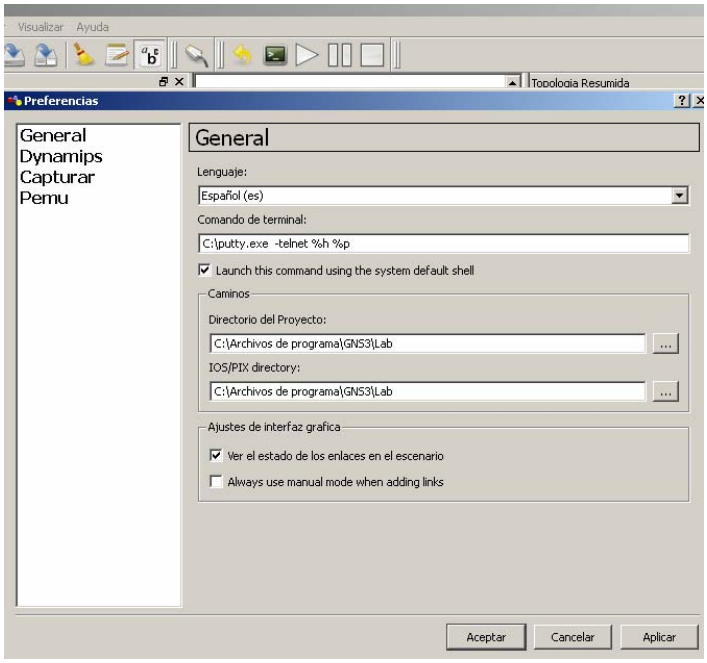


Figura 19. Configuración General de GNS3
Fuente: Autoras

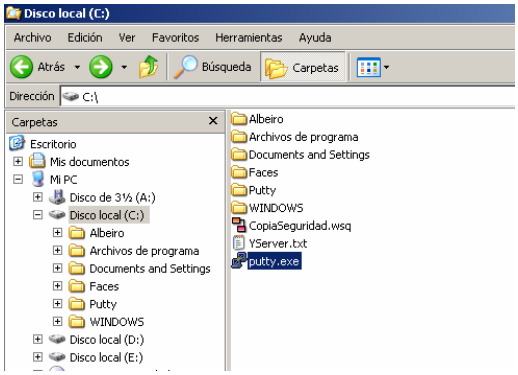


Figura 20. Ejecutable de putty.exe en disco C
Fuente: Autoras

4. En la opción Dynamips, ver figura 21 se ajusta el ejecutable y el directorio de trabajo; para el directorio de trabajo se le asigna la ruta de la carpeta creada con el nombre Lab, para el ejecutable se selecciona el cuadro que sale enfrente y se abrirá la siguiente ventana. Ver Figura 22.

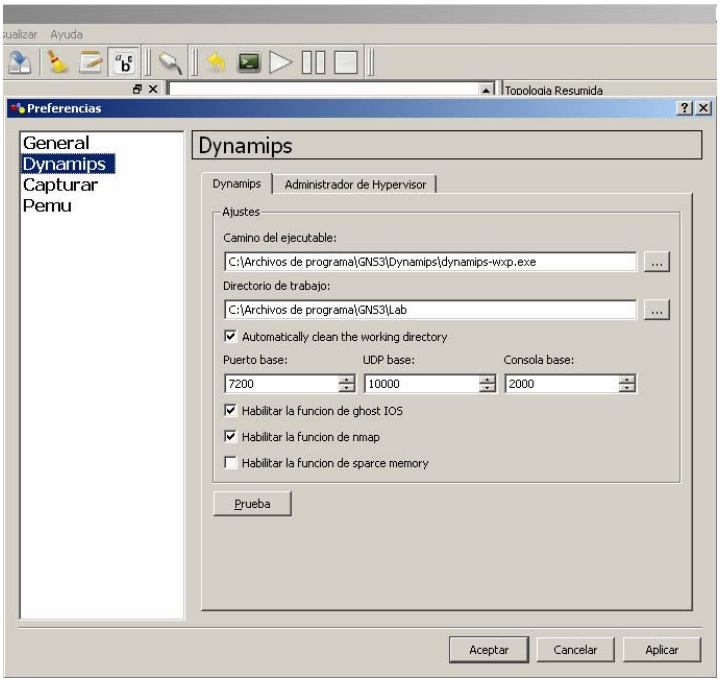


Figura 21. Ventana de Configuración Dynamips
Fuente: Autoras

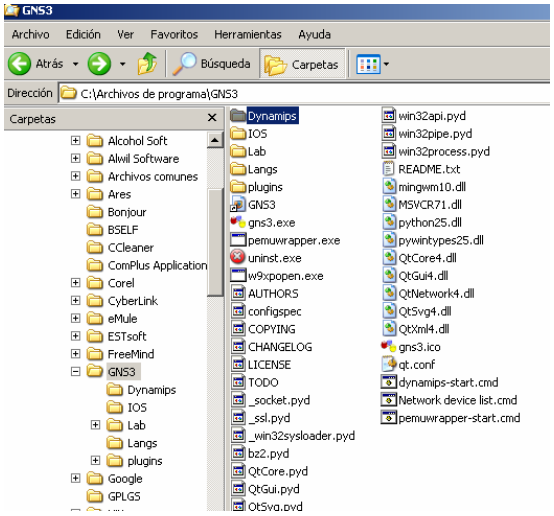


Figura 22. Ubicación de la carpeta Dynamips
Fuente: Autoras

Entramos en la carpeta Dynamips y allí se busca el ejecutable que diga dynamips-wxp, se selecciona y abrir. Ver figura 23.

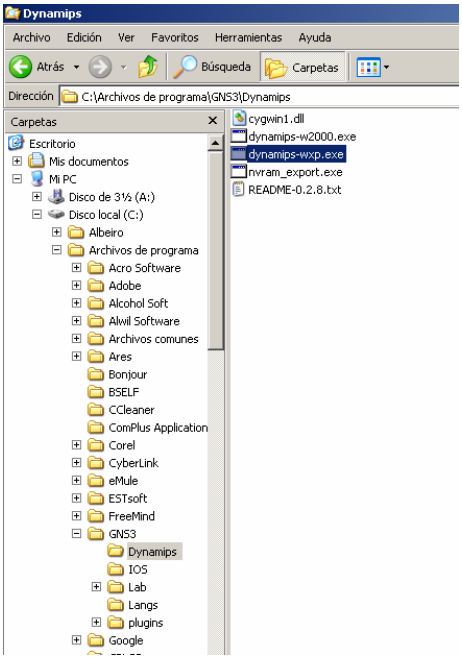


Figura 23. Ubicaciones del ejecutable dynamips-wxp.exe
Fuente: Autoras

5. Se aplican cambios y click en Prueba; saliendo al frente lo siguiente: **Dynamips succssefully started,** indicando que dynamips fue correctamente encendido, y por ultimo aceptar para que tome los cambios. Ver Figura 24.

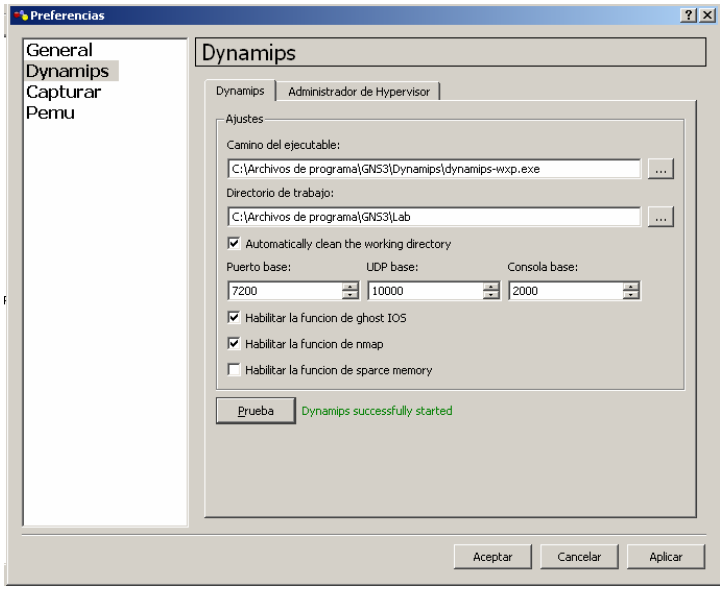


Figura 24. Prueba de correcto encendido de Dynamips
Fuente: Autoras

6. Configuración de la venta de Captura. Ver figura 25.

- Working directory for capture files: C:\Archivos de progrmas\GNS3\lab.
- Command to launch Wireshark or a capture file reader: C:\Archivos de programas\Wireshark.exe %c.

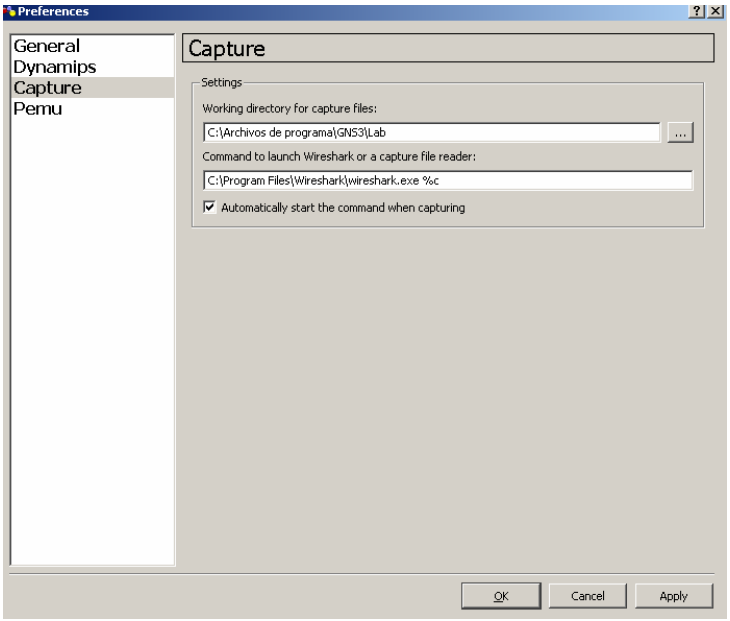


Figura 25. Configuración de la captura
Fuente: Autoras

7. Configurar las IOS de los Routers a trabajar, entrar en Editar\ imágenes de IOS y hypervisors. Ver Figura 26.

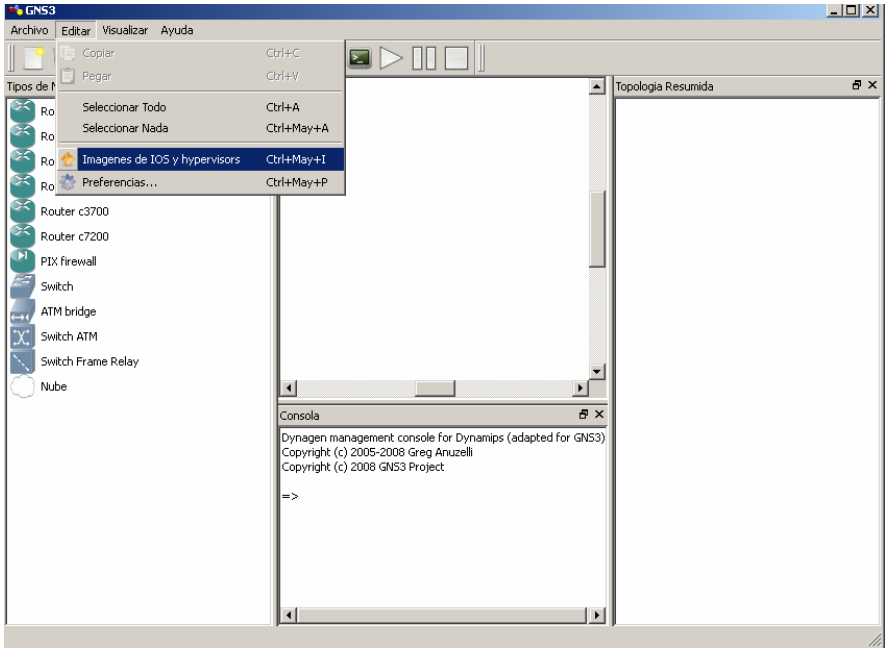


Figura 26. Configuración IOS de los Routers
Fuente: Autoras

En la ventana que sale a continuación, ver figura 27 se carga la IOS del Router, se da clic en el cuadro de **Archivo de imagen**; y se abre inmediatamente una ventana en la que hay que indicar la ruta en donde guardamos las IOS que fueron creadas en la carpeta anteriormente C:\Archivos de programa\GNS3\IOS.

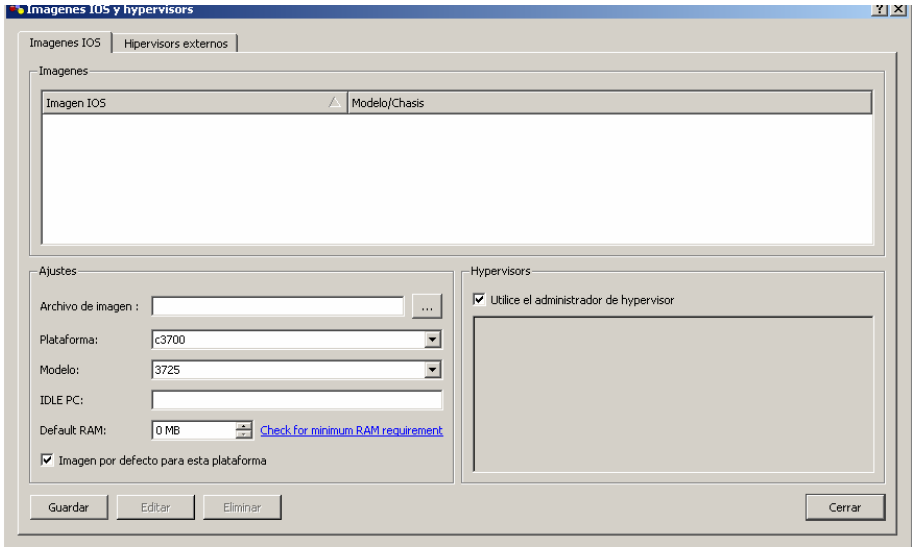


Figura 27. Imágenes IOS
Fuente: Autoras

Para observar la selección de una IOS, ver figura 28 se abre después de cargada, guardar y cerrar.

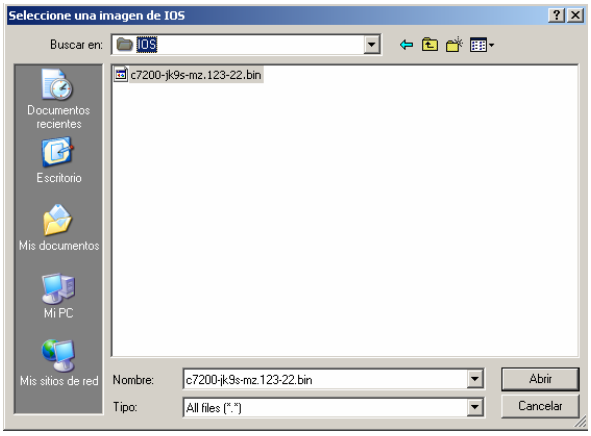


Figura 28. Selección de la IOS
Fuente: Autoras

Después de esto se puede empezar a trabajar con el GNS3 perfectamente.

Preparación

Inicialmente se configura en los routers la calidad de servicio o *Quality of Service (QoS)* utilizando información de capa 3-4 (dirección IP, puerto, protocolo), uno de los router será el encargado de generar tráfico a la red y otro será programado de tal manera que sea el encargado del encolamiento. De forma complementaria a la QoS, se realizara una práctica para la configuración de compresión de cabecera TCP.

Topología:

En la topología a implementar se hará uso de las interfaces Ethernet y seriales. Se utilizaran dos routers 7200 para el análisis de tráfico y configuración de los métodos de encolamiento y el router 2600 para generar el tráfico utilizando el IOS paget[15].

[15] IOS (Internetworking Operating System) Las IOS implementadas son material de práctica de los laboratorios de las Unidades Tecnológicas de Santander

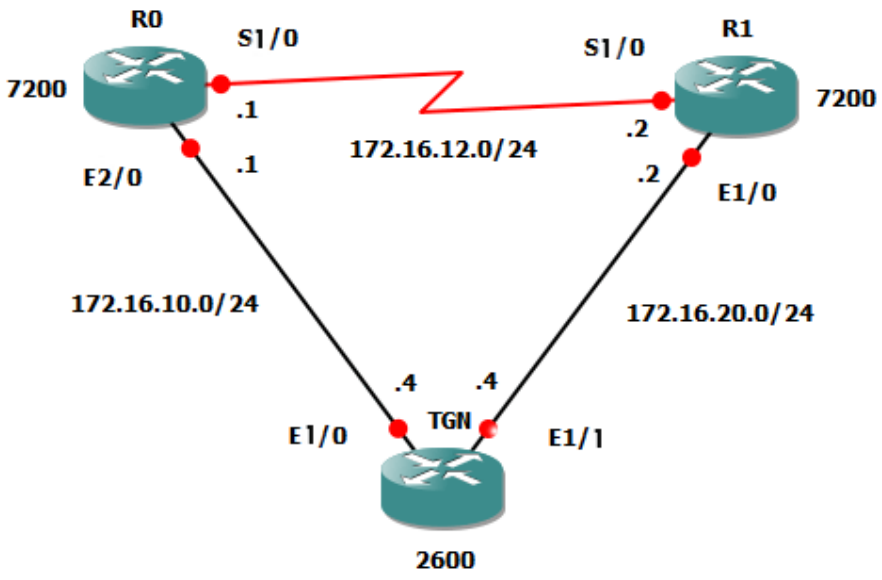


Figura 29. Esquema de red
Fuente: Autoras

Materiales:

- GNS3 configurado
- IOS de Router 7200
- IOS pagent con licence key para router 2600
- Wireshark instalado y configurado con el GNS3

Paso 1: Análisis de Tráfico con la herramienta software Wireshark

Objetivos Específicos:

- Instalar el Wireshark y configurarlo para que trabaje con el GNS3.
- Implementar la topología y realizar la configuración de los routers.
- Realizar ping y telnet y capturar el tráfico entre router.

Procedimiento:

1. Adicionar interfaces seriales y Ethernet para realizar el enlace entre routers. Se adicionan bahías PA-4E y PA4t+ para los roters 7200. Ver figura 30.

Figura 30. Configurador de nodo R0
Fuente: Autoras

2. Implementar la topología, subir las interfaces y configurar eigrp como protocolo de enrutamiento.

3. Configurar el directorio para guardar los archivos de captura. Ver figura 31.

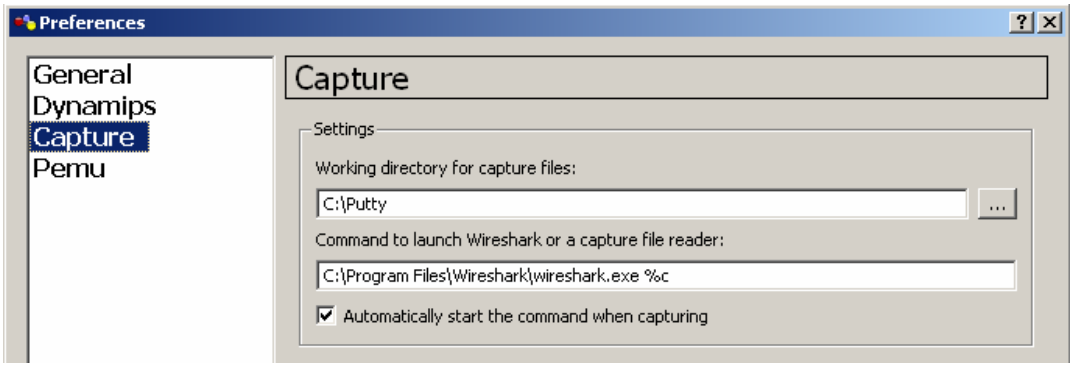


Figura 31. Preferencias-Captura
Fuente: Autoras

4. Realizar la captura del enlace. Ver figura 32.

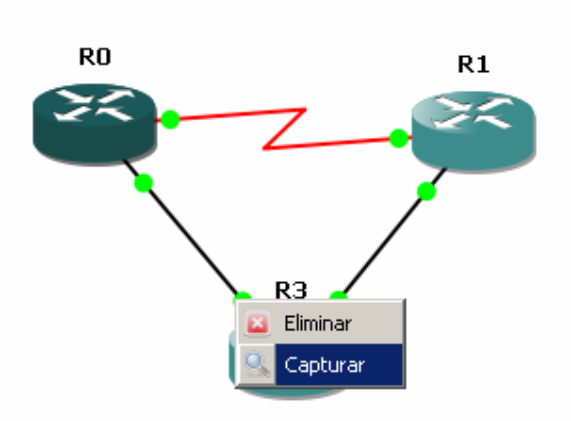


Figura 32. Captura del enlace
Fuente: Autoras

5. Determinar uno de los enlaces para la captura. Ver figura 33.

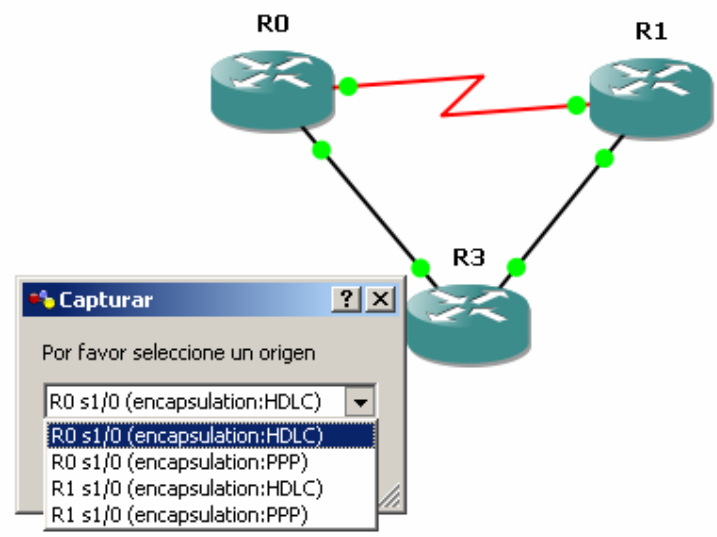


Figura 33. Selección del enlace
Fuente: Autoras

6. Realizar ping y telnet entre los routers que unen el enlace.

7. Abrir el archivo de captura. Tipo de archivo **.cap**

Paso 2: Análisis de Tráfico con la herramienta software Wireshark

Objetivos Específicos:

- Verificar el método de encolamiento de las interfaces.
- Observar estadísticas en las interfaces y diferencias entre FIFO y WFQ.
- Configurar en las interfaces los dos tipos de encolamiento.

1. Observar el ancho de banda y los métodos de encolamiento por defecto de las interfaces del router.

R0#show interface ethernet 1/0
Ethernet1/0 is up, line protocol is up
Hardware is AmdP2, address is ca00.0dfc.001c (bia ca00.0dfc.001c)
Internet address is 172.16.10.1/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)

La carga La carga de transmisión "txload" se define como la proporción entre la tasa o velocidad de salida y el ancho de banda.

WFQ es un algoritmo de cola basado en flujos (o sesiones), que realiza dos tareas simultáneamente y de forma automática:

- ✓ Organiza el tráfico (de tiempo real), poniéndolo al principio de la cola, reduciendo así el tiempo de respuesta.
- ✓ Comparte equitativamente el resto del ancho de banda, entre el resto de tráfico de alta prioridad

WFQ asegura que las diferentes colas no se priven de un mínimo ancho de banda, así el servicio proporcionado al tráfico será más eficiente.

Router#show interface serial 1/0
Internet address is 172.16.12.1/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 15420
Queueing strategy: weighted fair
Reserved Conversations 0/0 (allocated/max allocated)
Available Bandwidth 1158 kilobits/sec

El ancho de banda que se puede utilizar en la interface WFQ es del 75% del valor total. El 25 % restante es usado para sobrecargas de tráfico de control, tráfico best-effort etc. Si hay necesidad de asignar más del 75 % para RSVP, CBWFQ, LLQ, RTP, o Frame Relay PIPQ, se puede utilizar el comando **max-reserved-bandwidth.**

2. Configurar WFQ en la interface Ethernet. El valor de salida en la interface debe ser del 75% del total del ancho de banda.

3. Configurar el protocolo de enrutamiento en R0 y R1.

R0(config)# router eigrp 123
R0(config-router)# no auto-summary
R0(config-router)# network 172.16.0.0
R1(config)# router eigrp 123
R1(config-router)# no auto-summary
R1(config-router)# network 172.16.0.0

Se varía el valor de BW y se verifica la configuración en la interface y los valores *tx load* y *rxload.*

R0(config)# interface serial 1/0
R0(config-if)# bandwidth 800
R1(config)# interface serial 2/0
R1(config-if)# bandwidth 800

Si se configura la interface serial con FIFO y se realiza un mensaje ICMP (ping) se puede perder la conectividad de la interface, ya que FIFO no separa ancho de banda para mensajes de control o los mensajes de adyacencia de EIGRP.

Paso 3: Implementación de las políticas de QoS según el diagrama de Venn mostrado en la figura 34.

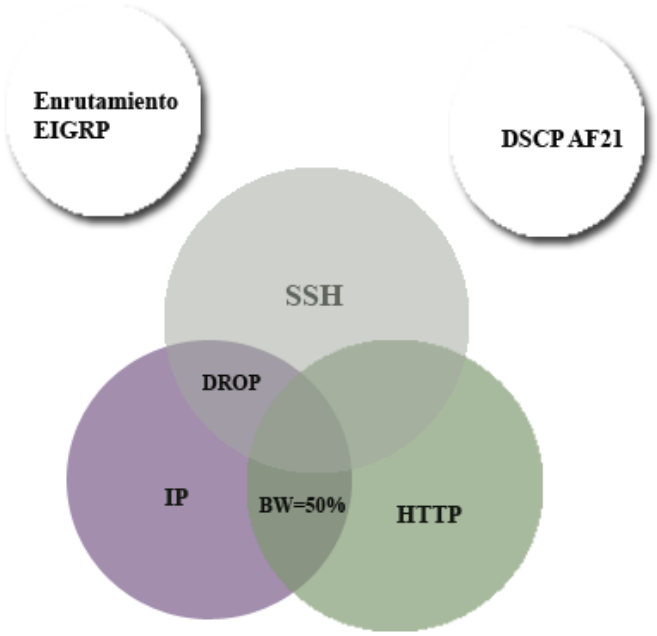


Figura 34. Criterios de selección
Fuente: Autoras

- Para la clase “interactive” se deniegan todos los paquetes que vienen de la dirección IP (172.16.10.0) hacia los routers marcados con el protocolo SSH
- Para la clase “web” se asigna el 50% del ancho de banda total para los paquetes marcados con el protocolo HTTP que vienen de la ip (172.16.10.0).
- Para la clase “critical” se marca todos los paquetes del protocolo de enrutamiento EIGRP con DSCP af21

1. **Configuración de las interfaces físicas**

R0

Router>enable
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface s1/0
Router(config-if)#ip address 172.16.12.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit

Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface e2/0
Router(config-if)#ip address 172.16.10.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit

Router#copy running-config startup-config

R1

Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface s1/0
Router(config-if)#ip address 172.16.12.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit

Router>ena
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface e2/0
Router(config-if)#ip address 172.16.20.2 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit

Router#copy running-config startup-config

2600

Router>ena
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface e1/0
Router(config-if)#ip address 172.16.10.4 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit

Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface e1/1
Router(config-if)#ip address 172.16.20.4 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#exit

Router#copy running-config startup-config

2. **Configuración EIGRP AS 123:** protocolo usado para el control de la red

Router0(config)#router eigrp 123
Router0(config-router)#no auto-summary
Router0(config-router)#network 172.16.0.0
Router0(config-router)#exit
Router0(config)#exit

Router1(config)#router eigrp 123
Router1(config-router)#no auto-summary
Router1(config-router)#network 172.16.0.0
Router1(config-router)#exit
Router1(config)#exit

Router#copy running-config startup-config

3. **Creación de las 3 clases de tráfico:**

Critical: EIGRP, protocolo usado para el control de la red

Interactive: SSH, protocolo usado para la administración remota

Web: HTTP, protocolo usado para la web y acceso e-mail

Router0#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router0(config)#class-map match-all critical
Router0(config-cmap)#match protocol eigrp
Router0(config-cmap)#class-map match-all interactive
Router0(config-cmap)#match protocol ssh
Router0(config-cmap)#class-map match-all web
Router0(config-cmap)#match protocol http
Router0(config-cmap)#exit

Con el comando show class-map se verifica la creación de las clases, a continuación se muestra en la figura 35 las clases creadas para la práctica realizada:

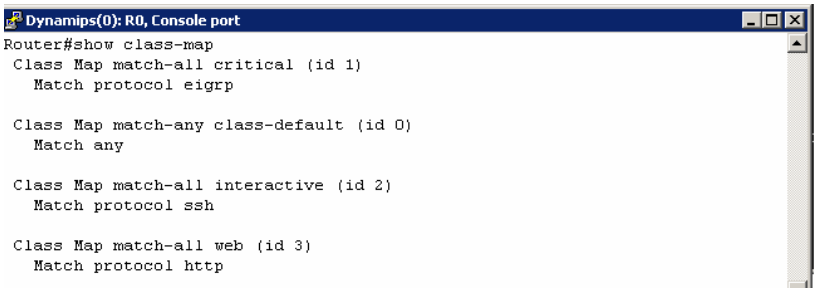


Figura 35. show class-map
Fuente: Autoras

4. **Configuración del mapa de política "calidad":**

Critical: Marcado de paquetes con DSCP af21

Interactive: Denegar paquetes del protocolo SSH

Web: Asignar ancho de banda al protocolo HTTP

Router0(config)#policy-map calidad
Router0(config-pmap)#class interactive
Router0(config-pmap-c)#drop
Router0(config-pmap-c)#exit
Router0(config-pmap)#class web
Router0(config-pmap-c)#bandwidth percent 50
Router0(config-pmap)#class critical
Router0(config-pmap-c)#set ip dscp af21
Router0(config-pmap-c)#exit

Con el comando show policy-map se verifica la creación de las políticas, a continuación se muestra en la figura 36 las políticas creadas para la práctica realizada:

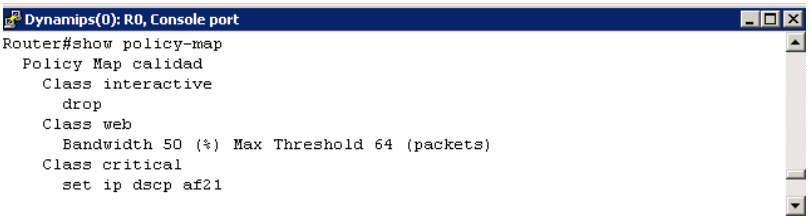


Figura 36. show policy-map
Fuente: Autoras

- Para la clase “interactive” se deniegan todos los paquetes que vienen del generador de tráfico hacia los routers marcados con el protocolo SSH
- Para la clase “web” se asigna el 50% del ancho de banda total para los paquetes marcados con el protocolo HTTP
- Para la clase “critical” se marca todos los paquetes del protocolo de enrutamiento EIGRP con DSCP af21

5. Adjuntar la política de servicio a las interfaces:

Router0(config-pmap)#interface s1/0
Router0(config-if)#service-policy output calidad
Router0(config-if)#router eigrp 1
Router0(config-router)#network 172.16.0.0
Router0(config-router)#no auto-summary
Router0(config-router)#exit
Router0(config)#exit

Router0#show run
Router0#show class-map
Router0#show policy-map calidad
Router0#show policy-map interface s1/0

access-list 100 permit ip any any dscp af21
access-list 100 permit tcp any host 172.16.10.1

Router0#copy running-config startup-config

Con el comando **show policy-map interface** se verifica el mapa de política aplicado a la interface, a continuación se muestra en la figura 37 las políticas creadas a través de la interface serial 2/0 para la práctica realizada:

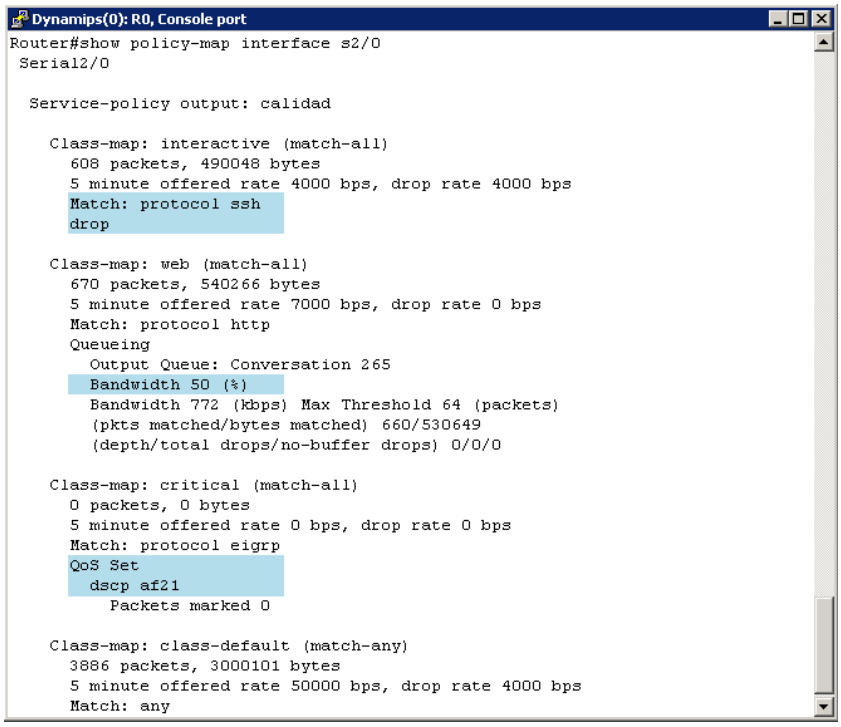


Figura 37. show policy-map interface
Fuente: Autoras

```
Router#show run
!
hostname Router0
!
class-map match-all critical
  match protocol eigrp
class-map match-all interactive
  match protocol ssh
class-map match-all web
  match protocol http
!
policy-map calidad
  class interactive
   drop
  class web
   bandwidth percent 50
  class critical
   set ip dscp af21

!
interface Ethernet1/0
 ip address 172.16.10.1 255.255.255.0
 duplex half
!
interface Serial2/0
 ip address 172.16.12.1 255.255.255.0
 serial restart-delay 0
 service-policy output calidad
!
router eigrp 123
 network 172.16.0.0
 no auto-summary
!
access-list 100 permit ip any any dscp af21
access-list 100 permit tcp any host 172.16.10.1
!
end
```

PASO 4: Configuración Del Router (IOS Pagent) Generador de Tráfico.

1. creación base pagent IOS y configuraciones de TGN

ethernet 1/0
add tcp
rate 1000
L2-dest ca00.02ac.001c
L3-src 172.16.10.4
L3-dest 172.16.20.4
L4-dest 23
length random 16 to 1500
burst on
burst duration off 1000 to 2000
burst duration on 1000 to 3000
add ethernet1/0 1
l4-dest 80
data ascii 0 GET /index.html HTTP/1.1
add ethernet1/0 1
l4-dest 21
add ethernet1/0 1
l4-dest 123
add ethernet1/0 1
l4-dest 110
add ethernet1/0 1
l4-dest 25
add ethernet1/0 1
l4-dest 22
add ethernet1/0 1
l4-dest 6000
!
End

Puerto	Protocolo
80	http
21	ftp
123	ntp
110	Pop3
25	smtp
22	ssh
6000	xwindows

Tabla 6. Descripción de los puertos utilizados
Fuente: Autoras

En el router 2600 que actúa como generador de tráfico se debe especificar la interface ehternet o fastethernet por la cual se inyecta el tráfico al sistema, además se debe especificar la dirección MAC de la interface hacia donde se dirige el tráfico, en este caso la interface e1/0 del router 7200 R0.

Para iniciar la generación de tráfico se debe ingresar el comando start, para detenerlo con el comando stop.

2. Verificación del tráfico de entrada en la interface e1/0 del router R0.

#show interface Ethernet e1/0

3. Captura del tráfico con del wireshark. Serial 1/0 del R0

La primera columna que se observa en la figura 24, contiene el número de cada paquete transmitido en el transcurso de la captura; la segunda columna muestra el tiempo de captura; la tercera columna muestra las estaciones fuente; la cuarta columna muestra las estaciones destino; la quinta columna muestra el tipo de protocolo en el cual no se observan los paquetes ssh los cuales se descartaron para la práctica. Estos parámetros se pueden modificar según la necesidad de cada usuario. En la figura 38 se puede mostrar la información de la captura realizada por el puerto serial 1/0 del router R0.

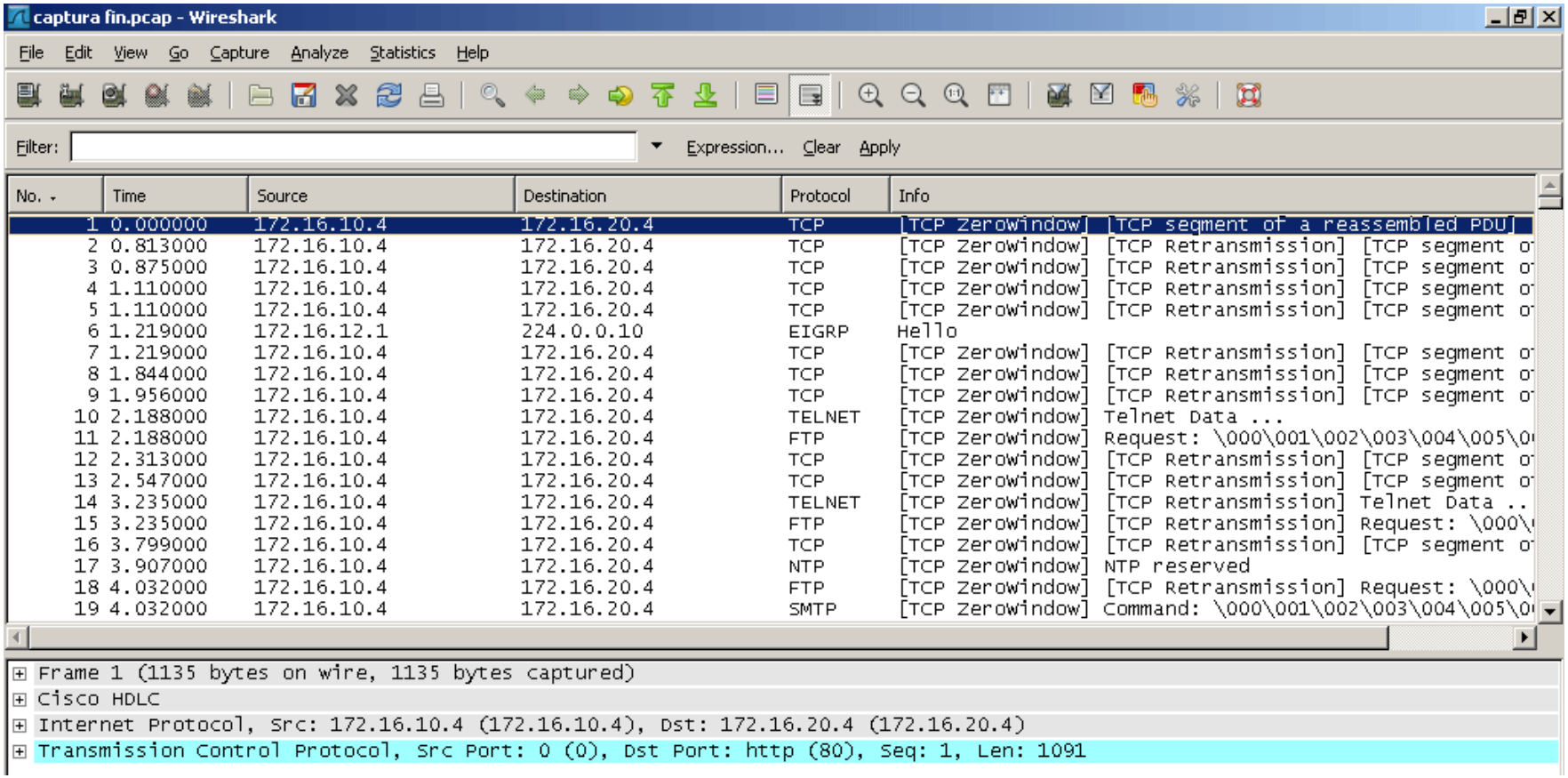


Figura 38. Captura de Tráfico
Fuente: Autoras

Paso 5: CONFIGURACIÓN DE COMPRESIÓN DE CABECERA TCP

Compresión de cabeceras TCP

R0

Configuración de dirección:

Router0(config)#interface s1/0
Router0(config-if)#ip address 172.16.12.1 255.255.255.0
Router0(config-if)#no shutdown

Activación de compression de cabecera TCP:

Router0(config)#interface s1/0
Router0(config-if)#ip tcp header-compression

Router0#show run
!
hostname Router0
!
interface Serial1/0
ip address 172.16.12.1 255.255.255.0
ip tcp header-compression
no shutdown
!
end

R1

Configuración del dirección:

Router1(config)#interface s1/0
Router1(config-if)#ip address 172.16.12.2 255.255.255.0
Router1(config-if)#no shutdown

Activación de compresión de cabecera TCP:
Router1(config)#interface s1/0
Router1(config-if)#ip tcp header-compression

Activación del Acceso a Telnet en R1

Router1(config-line)#line vty 0 4
Router1(config-line)#password 12345

Router1#show run
!
hostname Router1
!
interface Serial1/0
ip address 172.16.12.2 255.255.255.0
ip tcp header-compression
no shutdown
!
line vty 0 4
password 12345
login
!
End

*Con el comando **show ip tcp header-compression** se puede observar la compresión de cabeceras de los paquetes:*

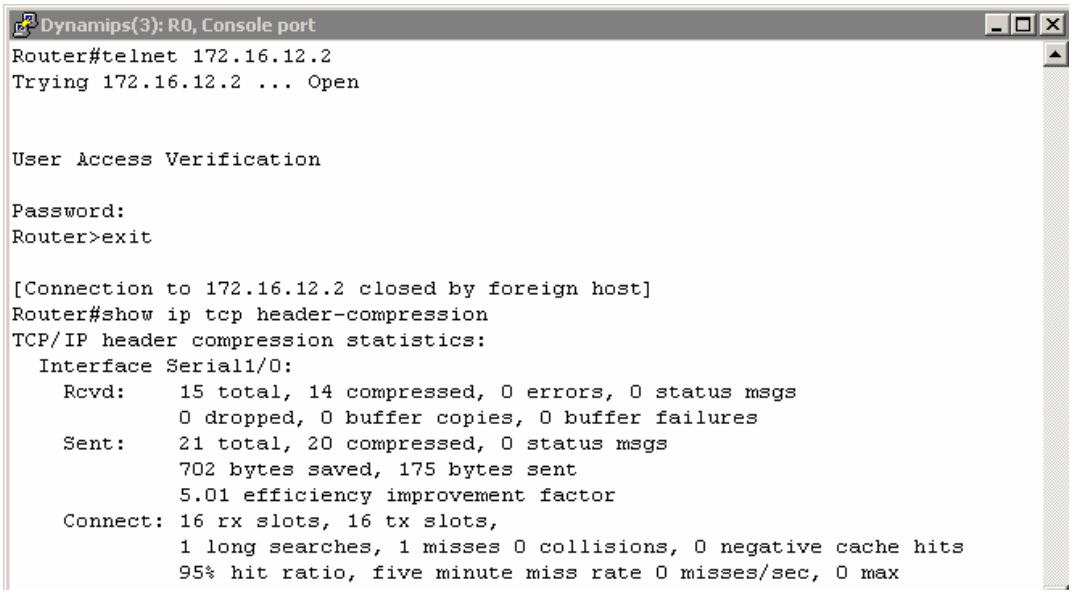


Figura 39. show ip tcp header-compression
Fuente: Autoras

CONCLUSIONES Y RECOMENDACIONES

Para aplicar QoS primero se debe establecer un modelo que depende de la topología y las aplicaciones que se van a manejar dentro de la red IP. En el caso específico de la práctica implementada, el modelo adecuado y que mejor se ajusta para ofrecer calidad de servicio es DiffServ.

Se seleccionó como herramienta de administración de la congestión WFQ, porque sitúa el tráfico interactivo a principio de la cola para reducir el tiempo de respuesta y permite compartir el resto de ancho de banda entre aplicaciones que requieran gran ancho de banda. Como se puede comprobar en el paso 2 de la práctica de calidad de Servicio.

La herramienta software GNS3 es un aplicativo tan completo que permite personalizar la memoria con que se desee trabajar en cada router, memoria que se toma de la RAM que se tenga disponible en el equipo de trabajo. La importancia de este aplicativo esta en la capacidad de permitir hacer simulaciones, que implementarlas en caso real requieren mayores esfuerzos.

Para trabajar con el software GSN3 se sugiere un PC con las siguientes especificaciones, esto debido al gran consumo de RAM para correr el programa: Procesador Intel Core 2 Duo; 2GB de memoria.

Se sugiere continuar la labor de búsqueda de nuevos modelos de calidad de servicio que promuevan la interacción en redes IP.

En caso de continuar este tipo de proyectos se puede hacer uso de otro de los mecanismos para asignar prioridad al ancho de banda a un tráfico específico.

BIBLIOGRAFÍA

ARCE, José Luis. "Análisis de la provisión de calidad de servicio para redes móviles utilizando INTSERV y DIFFSERV". Quito: Tesis EPN, 2005.

ARIZA, A. "Encaminamiento en Redes con Calidad de Servicio". Universidad de Málaga, Departamento Tecnología Electrónica, 2001. (Tesis Doctoral).

BLAKE, D.; BLACK, M.; CARLSON, E.; DAVIES, Z.; WANG, W. "An Architecture for Differentiated Services", RFC 2475, IETF 1998.

CISCO. CCNP: Optimizing Converged Networks v5.0 – Lab Configuration Guide.

CISCO. CCNP ONT Official ExamCertification Guide. Indianapolis, IN 46240 USA.

HUIDOBRO, José Manuel; ROLDÁN, David. "Redes y servicios de Banda Ancha. Tecnología y Aplicaciones". Primera Edición. España: McGraw-Hill, 2004.

WROCLAWSKI, J. "The Use of RSVP with IETF Integrated Services", RFC 2210, IETF. 1997.

ARTÍCULOS Y REVISTAS

ARIZA; CASILARI; SANDOVAL Y FABREGAT. “Encaminamiento en redes con DiffServ”. España: Universidad de Girona.

BARENCO, Claudia. “Modelo IntServ/Protocolo RSVP”. 2003.

ESCRIBANO, Jorge y otros. “Diffserv como solución a la provisión de QoS en Internet”. España: Universidad Carlos III de Madrid.

GOZDECKI, Janusz.” Quality of Servicios Terminology in IP Netwoks”. IEEE Comminications Magazine March 2003.

MONTAÑANA, Rogelio. “Calidad de Servicio (QoS)”. España:Universidad de Valencia.

DIRECCIONES ELECTRÓNICAS:

“Glosario de términos de calidad de servicio”, Vicky Jonson e Interconnect Technologies Corp., http://www.qosforum.com/docs/glossary/glossary.htm

PQ(Priority Queuing), CQ (Custom Queuing), WFQ (Weighted Fair Queuing), http://www.cisco.com

http://www.cisco.com/en/US/products/sw/cscowork/ps2064/products_user_guide_chapter09186a00800807f7.html#9701

http://www.it.uc3m.es/cgarcia/articulos/tesis-carlos-garcia-15jun.pdf

http://www.gns3.net/download

http://www.gns3.net/screenshots

ABREVIATURAS

AF	Assured Forwarding
BE	Best Effort
Diffserv	Different Service
DSL	Digital Subscriber line
FIFO	First In – First out
FF	Fixed Filter
Intserv	Integrated Service
IP	Internet Protocol
IETF	Internet Engineering Task Force
IEEE	Institute of Electrical and Electronics Engineers
IOS	Internetworking Operating System
ISO	International Organization for Standarization
IPSEC	Internet Protocol Security
Kbps	Kilo Bit Por Segundo
Mbps	Mega Bit Por segundo
QoS	Quality of Service
RSVP	Resource reservation Protocol