ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICAIONES Y REDES

"ANALISIS COMPARATIVO DE PROTOCOLOS QoS USADOS EN LA IMPLEMENTACIÓN DE SISTEMAS DE SEGURIDAD Y VIGILANCIA BASADOS EN TECNOLOGIAS IP: CASO PRACTICO DESITEL"

TESIS DE GRADO

Previo a la obtención del título de:

INGENIERÍA EN ELECTRÓNICA Y COMPUTACIÓN

Presentado por:

Ricardo Ramiro Fiallos Proaño

Riobamba – Ecuador

2011

AGRADECIMIENTO

Quisiera agradecer a mi director de tesis el Ing. Daniel Aro y al Doc. Giovani Vallejo por su constante apoyo en el desarrollo del presente trabajo de tesis, por sus conocimientos, paciencia y guía que fueron fundamentales en la orientación del correcto desarrollo de la investigación, razones por las cuales tendrán siempre mi admiración y respeto ya que inculcaron un sentido de seriedad y responsabilidad, valores fundaménteles en la formación de un profesional.

DEDICATORIA

En primera instancia dedico mi trabajo de tesis a Dios ya que él fue el que me lleno de fuerza y perseverancia que permitieron concluir la lucha que hace varios años eh empezado.

A mis padres que nunca dudaron de mis capacidades y fortalezas y siempre estuvieron prestos a brindarme su amor y apoyo en el arduo trabajo del rigor académico.

Y a todas aquellas personas que estuvieron a mi lado y supieron darme una voz de aliento en momentos de decepción y tristeza.

FIRMAS DE RESPONSABLES Y NOTA

NOMBRE	FIRMA	FECHA
Dr. Romeo Rodríguez **DECANO FACULTAD INFORMÁTICA Y ELECTRÓNICA**	_____	_____
Ing. Pedro Infate **DIRECTOR DE LA ESCUELA DE INGENIERÍA ELECTRONICA Y COMPUTACION**	_____	_____
Ing. Daniel Haro **DIRECTOR DE TESIS**	_____	_____
Doc. Geovanny Vallejo **MIEMBRO DEL TRIBUNAL**	_____	_____
Tlgo. Carlos Rodríguez **DIRECTOR CENTRO DE DOCUMENTACIÓN**	_____	_____

“Yo Ricardo Ramiro Fiallos Proaño, soy el responsable de las ideas, doctrinas y resultados expuestos en esta Tesis de Grado y el patrimonio intelectual de la misma pertenecen a la Escuela Superior Politécnica de Chimborazo”.

_____

Ricardo Ramiro Fiallos Proaño

ÍNDICE GENERAL

PORTADA

AGRADECIMIENTO

DEDICATORIA

FIRMAS RESPONSABLES

RESPONSABILIDAD DEL AUTOR

ÍNDICE GENERAL

ÍNDICE ABREVIATURAS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

CAPITULO I

1. MARCO REFERENCIAL.......19

1.1 Antecedente……...19

1.2 Justificación……...20

1.3. Objetivos……..……21

1.3.1. Objetivo General……..……21

1.3.2. Objetivos Especificos……..……21

1.4 Hipótesis……..……22

CAPITULO II

2. MARCO TEORICO

2.1. Sistemas de vigilancia basados en tecnologías IP……23

2.1.1. Cámaras IP……23

2.1.1.1Características……..23

2.1.1.2 Visión a tiempo real……..24

2.1.1.3 Microordenador……25

2.1.1.4 Comparación con cámaras de video……25
2.1.2 Medios de conexión……26
2.1.2.1 Medios guiados……26
2.1.2.1.1 El Par trenzad……..27
2.1.2.1.2 Cable Coaxial……27
2.1.2.1.3 La Fibra Óptica……28
2.1.2.2 Medios no guiados ……..29
2.2 Video sobre IP……..30
2.2.1 Video broadcast sobre IP……31
2.2.2 Video bajo demanda sobre IP (VoD)……..31
2.2.3 Videoconferencia……31
2.3 QoS (Quality of Service)……..32
2.3.1 Introducción……33
2.3.2 Clasificación de QoS……33
2.3.2.1 Según la sensibilidad del tráfico……34
2.3.2.2 Según el solicitante de calidad de servicio……34
2.3.2.3 Según las garantías……34
2.3.2.4 Según el sitio de aplicación……35
2.3.2.4.1 QoS Extremos a Extremo……..35
2.3.2.4.2 QoS Borde a Borde……35
2.3.3 Problemas en las redes de datos conmutados……..35
2.3.3.1 Latencia (Delay)……..36
2.3.3.2 Jitter (Variación de la latencia)……37
2.3.3.3 Paquetes perdidos……37
2.3.3.4 Disponibilidad de ancho de banda……37
2.3.3.5 Confiabilidad……38
2.3.4 Procedimientos para proporcionar diferenciación de QoS……39
2.3.4.1 Primero en entrar, primero en salir (FIFO)……39
2.3.4.2 Encolamiento basado en clases (CBQ)……40
2.3.4.3 Encolamiento equitativo ponderado (WFQ)……41
2.3.4.4 Tasa de Acceso Comprometida (CAR, Committed Access Rate)……..42
2.3.4.4.1 Clasificación de paquetes……42
2.3.4.4.2 Limitación de la tasa de transmisión……42
2.3.4.5 Descarte Aleatorio Anticipado (RED, Random Early Detection)……..43

2.3.5 Algoritmos para la Obtención de QoS……..43

2.3.5.1 Algoritmo del Mejor Esfuerzo ……43

2.3.5.2 Algoritmo Determinìstico……..44

2.3.5.3 Algoritmos Intermedios……..44

2.3.5.3.1 Servicios Estadísticos……44

2.3.5.3.2 Servicios de Degradación Limitada……45

2.3.5.3.3 Servicios Predictivos……45

2.3.6 Mecanismos de Calidad de Servicio……..45

2.3.6.1 Mecanismos de Control de Tráfico……45

2.3.6.1.1 Servicios diferenciados (DiffServ, Differentiated Services)……46

2.3.6.1.2 Servicios integrados (IntServ, Integrated Services)……46

2.3.6.1.3 IEEE 802.1p……...46

2.3.6.1.5 Sistema de Servicios Integrados para Líneas de baja Tasa de Transferencia……47

2.3.7 Protocolos de Calidad de Calidad de Servicio……47

2.3.7.1 Protocolo de Reserva de Recursos……..48

2.3.7.2 Operación de RSVP……48

2.3.7.3 Situación actual de RSVP……..49

2.3.8 Arquitectura de Calidad de Servicios……50

2.3.4.1 Arquitectura de Servicios Integrados (IntServ)……51

2.3.4.1.1 Niveles de Calidad de Servicio……..51

2.3.4.1.2 Componentes de IntServ……..52

2.3.4.1.3 Protocolo de Reserva……53

2.3.4.2 Arquitectura de Servicios Diferenciados (DiffServ)……54

2.3.4.2.1 Funciones de la Arquitectura DiffServ……54

2.3.4.2.4 Operación de la Arquitectura DiffServ……55

2.3.4.2.5 Elementos básicos del Modelo Diffserv……..58

2.3.4.2.6 Tipos de Marcas……58

2.3.4.2.7 Grupos de PHB……59

2.3.4.2.8 Aplicaciones de DiffServ……59

CAPITULO III

3. MARCO METODOLÓGICO E HIPOTÉTICO……61

3.1 Tipode Investigacion……61

3.1.1 Experimental……61

3.1.2 Correlacional……62

3.2 Método de investigación……62

3.3 Sistema de hipótesis……63

3.3 Oeracionalizacion de las variables……63

3.3.1 Operacionalización conceptual.....64

3.3.2 Operacionalización. Metodológica.....65

3.4 Población y muestra……66

3.5 Procedimientos generales……66

3.6 Instrumentos y herramientas……66

3.6.1 Instrumentos de hardware……66

3.6.2 Herramientas de software.....67

3.7 Validacion de los instrumentos……67

CAPITULO IV

4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS……68

4.1 Procesamiento de la Información……70

4.2 Resumen de los Experimentos……71

4.2.1 Ambiente de Simulación……72

4.2.2. Resultados del Ambiente 1……72

4.2.3. Resultados del Ambiente 2……74

4.2.4. Resultados del Ambiente 3……..75

4.3. Análisis de los Resultados de los Ambiente de Simulación……75

4.3.1. Variable Independiente……75

4.3.2. Variable Dependiente……..85

4.4. Resumen de los Pesos Obtenidos para Indicadores de la Variable Independiente……91

4.5. Resumen de los Pesos Obtenidos Para Indicadores de la Variable Dependiente……92

4.6. Análisis de Resultados.....93

4.6.1. Variable Independiente……93

4.6.2. Variable Dependiente.....94

4.7. Prueba de la Hipótesis.....96

CAPITULO V

5. MARCO PROPOSITIVO.....99

5.1 Alternativas de solución……..99

5.2 Evaluación de las alternativas……101

5.3 Implementación de la solución……102

CONCLUSIONES

RECOMENDACIONES

RESUMEN

SUMARY

GLOSARIO

ANEXOS

BIBLIOGRAFÍA

INDICE DE ABREVIATURAS

KBPS: Kilobyte por segundo

IRC: Internet Relay Chat

RDSI: Red Digital de Servicios Integrados

ADSL: Asymmetric Digital Subscriber Line

UMTS: Universal Mobile Telecommunications System

WLAN: Wireless Local Area Network

IEEE: Instituto de Ingenieros Electricistas y Electrónicos

QoS: Quality of Service

MAC: Media Access Control

NQSTA : Non Quality of Service Station

QSTA: Calidad de la Estación de Servicio

HCF: Función de Coordinación Hibrida

EDCA: Mejora del Canal de Acceso Distribuido

HCCA: Control de HCF canal de Acceso

Wi-Fi: Wireless Fidelity

VoIP: Voz Sobre Ip

FTP: File Transfer Protocol

AP: Access Point

HCF: Hybrid Fiber Coax

INTSERV: Integrated Services

SSID: Service Set IDentifier

BSSID: Basic Service Set IDentifier

DHCP: Dynamic Host Configuration Protocol

AC_BK: Background

AC_BE: Best Effort

AC_VI: Video

AC_VO: Voice

GNU: No es Unix

SFPT: Secure File Transfer Protocol

SSL: Secure Sockets Layer

LAN: **red** de área local

MAN: **Red** de Área Metropolitana

OSI: Open Systems Interconnection

ISO: International Systems Interconnection

HDLC: alto nivel de enlace de datos de control

LLC: logical link Control

CSMA / **CD**: Carrier Sense Multiple Access / Collision Detection Mbits: millón de bits

MAN: **Red** de Área Metropolitana

ANSI: American National Standard de identificación

IBM: International Business Machines

FDDI: Fiber Distributed Data Interface

DQDB: Distributed Bus de cola doble

SMDS: Switched Multimegabit Data Service

ISDN: Integrated Services Digital Network

ATM: Asynchronous Transfer Mode

WEP: Wired Equivalent Privacy

WPA: Wi-Fi Protected Access

IPsec: Internet Protocol Security

VPN: Virtual Private Network

GPRS: General Packet Radio Service

UMTS: Universal Telecommunications System

QBSS: QBone Service Scanverger

CR: Cognitive radio

ER: Entidad Relacion

TCS: Sistema de Comando Táctico

IBSS : Independiente Basic Service Set

BSS: BASIC Servicio Set

ESS: Extended Service Set

DSCP: Servicios Diferenciados Punto de Codigo

UDP: User Datagram Protocol

SLAs : Acuerdos de Nivel de Servicio

SD: Señalización Digital

TCP / **IP:** Transmisión Control Protocol / Internet Protocol

BOOTP: Bootstrap Protocol

BIA: Business Intelligence Accelerator

PCF: Funcion de Control de Paquetes

HTTP: Hypertext Transfer Protocol

EF: Bandera de Extensión

PC: Personal Computer

AF: Assured Forwarding

FIFO: First In – First Out (primero en entrar - primero en salir)

CWmin: Contention Window Mínimo (mínima ventana de contención)

CWmax: Contention Window Máximo (mínima ventana de contención)

CW: Contention Window (ventana de contención)

IFS: Interframe space (Espacio entre tramas)

AIFS: Arbitration Inter Frame Space (Espacio entre tramas arbitrario)

SIFS: Short Inter Frame Space (Espacio entre tramas corto)

AIFSN: Arbitration Inter Frame Space Number (Número arbitrario de espacio entre tramas)

NAV: Vector de Asignación de Red

ISP: Proveedor de Servicios de Internet

TS: traffic stream

TID: identificador de prioridad de usuario

TXOP: Transmisión Opportunity

RED: Random Early Detection

RSVP: Resource Reservation Protocol

ÍNDICE DE FIGURAS

Figura I.01 Modelo de referencias de Servicios Integrados……..……..…41
Figura II.01 Ejemplo de la compartición de enlace en CBQ……..…41
Figura II.2 Dominio de Servicios Diferenciados……56
Figura III.1 Escenario de Pruebas (Hadware)……..66
Figura IV.1. Esquema de ambiente de simulación.....72
Figura. IV.2. Diagrama de comparación de paquetes transmitidos en el ambiente 1……76
Figura. IV.3. Diagrama de porcentaje de pesos de paquetes transmitidos en el ambiente 1……..76
Figura. IV.4. Diagrama de comparación de porcentaje de pérdida paquetes en el ambiente 1……..78
Figura. IV.5. Diagrama de porcentaje de pesos de pérdida de paquetes en el ambiente 1……..78
Figura. IV.6. Diagrama de comparación de ancho de banda en el ambiente 1..80
Figura. IV.7. Diagrama de porcentaje de ancho de banda en el ambiente 1.....80
Figura. IV.8. Diagrama de comparación de retardo en el ambiente 1.....82
Figura. IV.9. Diagrama de porcentaje de retardo en el ambiente 1.....82
Figura IV.10. Diagrama de comparación de jitter en el ambiente 1.....84
Figura IV.11. Diagrama de porcentaje de jitter en el ambiente 1.....84
Figura IV.12 Comparación rendimiento IntServ……..……89
Figura IV.13 Comparación rendimiento DiffServ……90
Figura. IV.14. Diagrama de Barras de los resultados de la Variable Independiente……..93
Figura. IV.15. Diagrama de Barras de los resultados de la Variable Dependiente……..95
Figura. IV.16. Diagrama de fijación del nivel de significación……98

INDICE DE TABLAS

TABLA II.I Características de los cables usados para medios guiados 28
TABLA II.II Frecuencias de los medios no guiados 30
TABLAII.III Requerimientos de ancho de banda para distintas aplicaciones34
TABLA II.IV Categorías para descarte de paquetes 57
TABLA II.V Correspondencia de campo de preferencia con DiffServ 58
TABLA II.VI Ejemplo de asignación de clases para diferentes asignaciones 60
TABLA IV.I Detalles Técnicos de los equipos del Ambiente de Simulación 72
TABLA IV.II. Detalles Técnicos del uso de cada equipo 73
TABLA IV.IV. Datos obtenidos en escenario con trafico FTP 74
TABLA IV.V. Datos obtenidos en Video Arquitectura IntServ 74
TABLA IV.VI. Datos obtenidos en Video Arquitectura DiffServ 75
TABLA IV.VII. Comparación de paquetes transmitidos en el ambiente 1. 76
TABLA IV.VII. Comparación de pérdida de paquetes en el ambiente 1 77
TABLA IV.IX. Comparación de ancho de banda en el ambiente 1 80
TABLA IV.X. Comparación de retardo en el ambiente 1 82
TABLA IV.XI. Comparación de jitter en el ambiente 1 83
TABLA IV.XII. Pesos Indicadores e Indices para la valoración del rendimiento 86
TABLA IV.XIII. valoración del rendimiento BestEffort sin tráfico en la red……. 87
TABLA IV.XIV. Valoración del rendimiento BestEffort con tráfico en la red 87
TABLA IV.XV. Valoración del rendimiento IntServ 88
TABLA IV.XVI. Comparación del Rendimiento IntServ 88
TABLA IV.XVII. Valoración del rendimiento DiffServ 89
TABLA IV.XVIII. Comparación del Rendidito IntServ 90
TABLA IV.XIX. Pesos de los indicadores de la variable Independiente 91
TABLA IV.XX. Pesos de los indicadores de la variable dependiente 92
TABLA IV.XXI. Análisis de Resultados para la Variable Independiente: Total Indicadores 93
TABLA IV.XXII. Análisis de Resultados para la Variable Dependiente: Total Indicadores 94
TABLA IV.XXIII. Prueba de la Hipótesis, valores del test de Chi-cuadrado 97
TABLA V.1 Direccionamiento de las dispositivos capa 3
TABLA V.2 Direccionamiento dispositivos finales

ITRODUCCIÓN

A continuación procederemos a describir uno a uno los pasos necesarios para la implementación de la solución propuesta.

En presente trabajo de investigación se presentan los resultados obtenidos para determinar en Protocolo que mejor rendimiento presente para la mejora de la calidad del servicio en la transmisión de video IP.

El desarrollo del trabajo se lo realizo de la siguiente manera.

Se realizo un escenario de simulación en el cual se simula una red WAN con dos routers Cisco, dos Switch Cisco, dos Computadores y dos Cámaras Web, en dicho entorno de simulación se implemento las arquitecturas expuestas a estudio con la finalidad de valorar el rendimiento de cada uno de ellos.

El trabajo de tesis contendrá 5 capítulos que presentaran el desarrollo de la investigación de la siguiente manera. El Capitulo I Marco Referencial detalla los antecedentes, justificación, objetivos e hipótesis la cual será valorada al finalizar el trabajo de investigación.

El Capitulo II Marco Teórico presenta la información teórica de las arquitecturas expuestas a estudio. El Capítulo III Marco Metodológico e Hipotético presenta el tipo y método de investigación a realizarse, el sistema de hipótesis y la operacionalización de las variables, validación de instrumentos la población y muestra en los que se basara el trabajo.

El Capítulo IV Análisis e Interpretación de Resultados valoraremos las el rendimiento de cada uno de los escenarios de prueba, tanto de la variable dependiente e independiente para llegar a la comprobación de nuestra hipótesis.

Por último en el Capitulo V Marco Propositivo se desplegara la evolución de las alternativas y la implementación de la arquitectura de mejor rendimiento para el trabajo requerido.

CAPÍTULO I

MARCO REFERENCIAL

1.1 ANTECEDENTES

La utilización de cámaras IP presenta notables mejoras en la calidad y administración de las imágenes ya que pueden ser visualizadas por medio de un navegador de internet desde cualquier punto de la red.

Uno de los usos más usuales de las cámaras IP es en la implementación de sistemas de seguridad cerrados ya que pueden ser instaladas con facilidad en redes ya existentes.

Ahora bien, esto representa un crecimiento considerable en el tráfico de las redes en mención, ya que según el método de compresión que usemos tendríamos una rata aproximada de 1.3Mbs por cada cámara instalada. Lo que implica que requeriríamos de un ancho de banda considerable para la transmisión de dicho tráfico, si es que deseamos tener una visualización de video a tiempo real, lo que es indispensable para un sistema de seguridad.

Una de los métodos más confiables para asegurar un tratamiento constante en la transmisión de un determinado tráfico es la utilización de protocolos y arquitecturas de QoS. .

Estos métodos surgieron ante la convergencia de todas las redes de datos sobre el protocolo IP lo que provoca retardos de la información y perdidas de paquetes que implicaron un mal funcionamiento de algunas aplicaciones e incluso el que otras no puedan ser ejecutadas.

Existen varios tipos de protocolos para QoS entre los cuales citaremos los más utilizados:

RSVP Protocolo de reserva de recursos, proporciona la señalización para permitir la reserva de recursos de la red.

DiffServ Servicios Diferenciados, permite el dividir y el dar prioridad al tráfico de la red mediante el uso de etiquetas en las cabeceras de los paquetes.

MPLS Conmutación de etiquetas multiprotocolo, proporciona la posibilidad de administrar el ancho de banda de la red a través de etiquetas en las cabeceras de los paquetes y de en caminadores específicos capaces de reconocerlas.

SBM Administración del ancho de banda de la subred, es un protocolo de señalización que permite la comunicación y coordinación entre los distintos nodos de la red

1.2 JUSTIFICACIÓN

Como hemos visto la convergencia de las redes de datos al protocolo IP a conllevado a la necesidad de protocolos y técnicas dedicadas al tratamiento de la fiabilidad y calidad en la transmisión de dichos datos.

Un caso muy común de dicha convergencia de datos en el protocolo IP son las conocidas cámaras IP que en la actualidad son muy utilizadas en la implementación de sistemas de seguridad.

Debido al aumento desmedido de la delincuencia, las instituciones tanto públicas como privadas se ven en la obligación de tomar medidas en lo que se refiere a la seguridad de sus bienes, las facilidades que presentan las cámaras IP han llevado a hacer lo estos los más utilizados en el mercado.

Ahora bien tomando en cuenta la cantidad aproximada de cámara IP que se necesitan para la seguridad de un edificio de tamaño mediano y que estas imágenes deberán ser visualizadas a tiempo real, conlleva a la necesidad de que

la red que albergue dicho sistema deberá tener una QoS adecuada para el trabajo requerido.

Debemos tomar en cuenta también el performance de la red que albergará el sistema de seguridad, puesto que este, en la mayoría de los casos es usado también para otros tipos de tráfico.

El presente trabajo de investigación está orientado a realizar un completo estudio comparativo de los diferentes protocolos QoS que pueden ser utilizados para la implementación de sistemas de seguridad basados en tecnologías IP, con la finalidad de que al termino del mismo podremos definir el protocolo más idóneo para el trabajo requerido.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

- ✓ Comparar, evaluar los diferentes protocolos de QoS usados en sistemas de seguridad y vigilancia basados en tecnologías IP, e implementar el protocolo más idóneo.

1.3.2 OBJETIVOS ESPECÍFICOS

- ✓ Estudiar los diferentes protocolos de QoS usados para mejorar la transmisión de video en los sistemas de seguridad basados en tecnología IP.
- ✓ Comparar escenarios de prueba con los diferentes protocolos en el estudio.
- ✓ Evaluar los resultados obtenidos tanto en los escenarios de prueba como en los estudios realizados.
- ✓ Escoger el protocolo de QoS idóneo para la transmisión de video de seguridad generados por medio de cámaras IP.
- ✓ Implementar el sistema de vigilancia con cámaras IP con el protocolo QoS escogido.

1.4 HIPÓTESIS

La evaluación de protocolos QoS usados para la implementación sistemas de seguridad basados en tecnologías IP permitirá conocer a ciencia cierta el protocolo más robusto en el área del trabajo requerido.

CAPITULO II

MARCO TEÓRICO

2.1 SISTEMAS DE VIGILANCIA BASADOS EN TECNOLOGÍAS IP

2.1.1 CÁMARAS IP

2.1.1.1 CARACTERÍSTICAS

Una cámara de red incorpora su propio miniordenador, lo que le permite emitir vídeo por sí misma.

Además de comprimir el vídeo y enviarlo, según su modelo puede tener una gran variedad de funciones. .

- Envío de correos electrónicos con imágenes.
- Activación mediante movimiento de la imagen.
- Activación mediante movimiento de sólo una parte de la imagen.
- Creación de una máscara en la imagen, para ocultar parte de ella o colocar un logo. O simplemente por adornar.
- Activación a través de otros sensores.
- Control remoto para mover la cámara y apuntar a una zona.
- Programación de una secuencia de movimientos en la propia cámara.
- Posibilidad de guardar y emitir los momentos anteriores a un evento.
- Utilización de diferente cantidad de fotogramas según la importancia de la secuencia. Para conservar ancho de banda.
- Actualización de las funciones por software.

Las cámaras IP permiten ver en tiempo real qué está pasando en un lugar, aunque esté a miles de kilómetros de distancia. Son cámaras de vídeo de gran calidad que tienen incluido un ordenador a través del que se conectan directamente a Internet.

Una cámara IP (o una cámara de red) es un dispositivo que contiene:

- Una cámara de vídeo de gran calidad, que capta las imágenes
- Un chip de compresión que prepara las imágenes para ser transmitidas por Internet.
- Un ordenador que se conecta por sí mismo a Internet

2.1.1.2 VISIÓN A TIEMPO REAL

A diferencia de las cámaras web las cámaras IP no necesitan un computador para enviar las imagines a través del Internet, ya que estas se pueden conectar a un punto de la red a través de una hab, switch o un punto de acceso.

Las cámaras IP posen su propia dirección IP que las identifica en el entorno de red. Gracias a esto cada cámara IP puede transmitir video usando el Internet como medio a cientos de kilómetros de distancia, lo que faculta el monitoreo y vigilancia remota a tiempo real.

El acceso a estas imágenes está totalmente restringido: sólo las personas autorizadas pueden verlas. También se puede ofrecer acceso libre y abierto si el vídeo en directo se desea incorporar al web site de una compañía para que todos los internautas tengan acceso.

2.1.1.3 MICROORDENADOR

Una cámara IP tiene incorporado un ordenador, pequeño y especializado en ejecutar aplicaciones de red. Por lo tanto, la cámara ip no necesita estar conectada a un PC para funcionar. Esta es una de sus diferencias con las denominadas cámaras web.

Una cámara ip tiene su propia dirección IP y se conecta a la red como cualquier otro dispositivo; incorpora el software necesario de servidor de web, servidor o cliente FTP, de correo electrónico... y tiene la capacidad de ejecutar pequeños programas personalizados (denominados scripts).

También incluye entradas para alarmas y salida de relé.

Las cámaras de red más avanzadas pueden equiparse con muchas otras funciones de valor añadido como son la detección de movimiento y la salida de vídeo analógico.

2.1.1.4 COMPARACIÓN CON CÁMARAS DE VIDEO

Las cámaras IP incorporan todas las funciones de una cámara de vídeo y añaden más prestaciones.

La lente de la cámara enfoca la imagen en el sensor de imagen (CCD). Antes de llegar al sensor, la imagen pasa por el filtro óptico que elimina cualquier luz infrarroja y muestra los colores correctos.

Actualmente están apareciendo cámaras día/noche que disponen de un filtro de infrarrojos automático, este filtro se coloca delante del ccd sólo cuando las condiciones de luz son adecuadas proporcionándonos de esta manera imágenes en color, cuando las condiciones de luz bajan este filtro se desplaza y la cámara

emite la señal en blanco y negro produciendo más luminosidad y de esta manera podemos iluminar la escena con luz infrarroja y ver en total oscuridad.

El sensor de imagen convierte la imagen, que está compuesta por información lumínica, en señales eléctricas. Estas señales eléctricas se encuentran ya en un formato que puede ser comprimido y transferido a través de redes.

Como las cámaras de vídeo convencionales, las cámaras IP gestionan la exposición (el nivel de luz de la imagen), el equilibrio de blancos (el ajuste de los niveles de color), la nitidez de la imagen y otros aspectos de la calidad de la imagen. Estas funciones las lleva a cabo el controlador de cámara y el chip de compresión de vídeo.

Las cámaras IP comprimen la imagen digital en una imagen que contiene menos datos para permitir una transferencia más eficiente a través de la Red, cámaras MPEG4.

2.1.2 MEDIOS DE CONEXIÓN

2.1.2.1 MEDIOS GUIADOS

Los medios de transmisión guiados están constituidos por un cable que se encarga de la conducción (o guiado) de las señales desde un extremo al otro.

Las principales características de los medios guiados son el tipo de conductor utilizado, la velocidad máxima de transmisión, las distancias máximas que puede ofrecer entre repetidores, la inmunidad frente a la interferencia electromagnética, la facilidad de instalación y la capacidad de soportar diferentes tecnologías de nivel de enlace.

La velocidad de transmisión depende directamente de la distancia entre los terminales, y de si el medio se utiliza para realizar un enlace punto a punto o un enlace multipunto. Debido a esto los diferentes medios de transmisión tendrán diferentes velocidades de conexión que se adaptarán a utilizaciones dispares.

Dentro de los medios de transmisión guiados, los más utilizados en el campo de las comunicaciones y la interconexión de computadoras son:

2.1.2.1.1 EL PAR TRENZADO

Consiste en un par de hilos de cobre conductores cruzados entre sí, con el objetivo de reducir el ruido de diafonía. A mayor número de cruces por unidad de longitud, mejor comportamiento ante el problema de diafonía.

Existen dos tipos de par trenzado:

- Protegido: Shielded Twisted Pair (STP)

- No protegido: Unshielded Twisted Pair (UTP)

El UTP son las siglas de Unshielded Twisted Pair. Es un cable de pares trenzado y sin recubrimiento metálico externo, de modo que es sensible a las interferencias. Es importante guardar la numeración de los pares, ya que de lo contrario el Efecto del trenzado no será eficaz disminuyendo sensiblemente o incluso impidiendo la capacidad de transmisión. Es un cable Barato, flexible y sencillo de instalar.

En el caso de las redes se emplea UTP Cat.5 o Cat.6 para transmisión de datos. Consiguiendo velocidades de varios centenares de Mbps. Un ejemplo de este uso lo constituyen las redes 10/100/1000BASE-T.

2.1.2.1.2 EL CABLE COAXIAL

El cable coaxial fue creado en la década de los 30, y es un cable utilizado para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado vivo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes eléctricas. Entre ambos se encuentra una capa de aíslate eléctrico llamada dieléctrico, de cuyas características dependerá principalmente la calidad del cable. Todo el conjunto suele estar protegido por una cubierta aislante.

El conductor eléctrico central puede estar constituido por un alambre sólido o por varios hilos retorcidos de cobre; mientras que el exterior puede ser una malla

trenzada, una lámina enrollada o un tubo corrugado de cobre o aluminio. En este último caso resultará un cable semirrígido.

Debido a la necesidad de manejar frecuencias cada vez más altas y a la digitalización de las transmisiones, en años recientes se ha sustituido paulatinamente el uso del cable coaxial por el de la fibra óptica, en particular para distancias superiores a varios kilómetros, porque el ancho de banda de esta última es muy superior.

2.1.2.1.3 LA FIBRA ÓPTICA.

La fibra óptica es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o plástico, por el que se envían pulsos de luz que representan los datos a transmitir. El haz de luz queda completamente confinado y se propaga por el núcleo de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, en función de la Ley de Snell. La fuente de luz puede ser laser un LED.

Las fibras se utilizan ampliamente en las telecomunicaciones, ya que permiten enviar gran cantidad de datos a una gran distancia, con velocidades similares a las de radio o cable. Son el medio de transmisión por excelencia al ser inmune a las interferencias electromagnéticas, también se utilizan para redes locales, en donde se necesite aprovechar las ventajas de la fibra óptica sobre otros medios de transmisión.

Medio de Transmisión	Razón de datos total	Ancho de Banda	Separación entre repetidores
Par Trenzado	4 Mbps	3 Mhz	2 a 10 km
Cable Coaxial	500 Mbps	350MHz	1 a 10 km
Fibra Óptica	2Gbps	2GHz	10 a 100 km

TABLAII.01 Características de los cables usados para medios guiados

Cabe destacar que hay una gran cantidad de cables de diferentes características que tienen diversas utilidades en el mundo de las comunicaciones.

2.1.2.2 MEDIOS NO GUIADOS

Los medios de transmisión no guiados son los que no confinan las señales mediante ningún tipo de cable, sino que las señales se propagan libremente a través del medio. Entre los medios más importantes se encuentran el aire y el vacío.

Tanto la transmisión como la recepción de información se lleva a cabo mediante antenas. A la hora de transmitir, la antena irradia energía electromagnética en el medio. Por el contrario en la recepción la antena capta las ondas electromagnéticas del medio que la rodea.

La configuración para las transmisiones no guiadas puede ser direccional y omnidireccional.

En la direccional, la antena transmisora emite la energía electromagnética concentrándola en un haz, por lo que las antenas emisora y receptora deben estar alineadas.

En la omnidireccional, la radiación se hace de manera dispersa, emitiendo en todas direcciones pudiendo la señal ser recibida por varias antenas. Generalmente, cuanto mayor es la frecuencia de la señal transmitida es más factible confinar la energía en un haz direccional.

La transmisión de datos a través de medios no guiados, añade problemas adicionales provocados por la reflexión que sufre la señal en los distintos obstáculos existentes en el medio. Resultando más importante el espectro de frecuencias de la señal transmitida que el propio medio de transmisión en sí mismo.

Según el rango de frecuencias de trabajo, las transmisiones no guiadas se pueden clasificar en tres tipos: Radio, Microondas, Infrarrojos o Láser.

Banda de Frecuencia	Nombre	Modulación	Razón de Datos	Aplicaciones Principales
30-300 kHz	LF (low frequency)	ASK, FSK, MSK	0,1-100 bps	Navegación
300-3000 kHz	MF (medium frequency)	ASK, FSK, MSK	10-1000 bps	Radio AM Comercial
3-30 MHz	HF (high frequency)	ASK, FSK, MSK	10-3000 bps	Radio de onda corta
30-300 MHz	VHF (very high frequency)	FSK, PSK	Hasta 100 kbps	Television VHF, Radio FM
300-3000 MHz	UHF (ultra high frequency)	PSK	Hasta 10 Mbps	Television UHF, Microondas Terrestres
3-30 GHz	SHF (super high frequency)	PSK	Hasta 100Mbps	Microondas terrestres y por satélite
30-300 GHz	EHF (extremely high frequency)	PSK	Hasta 750 Mbps	Enlaces cercanos con punto a punto experimentales

TABLA II.02 Frecuencias de los medios no guiados

2.2. VIDEO SOBRE IP

En la actualidad, la utilización de la redes para la transmisión de vídeo ha tenido un crecimiento masivo, ya que el Internet se utiliza para muchos fines como ver películas, descargar videos, clases remotas, televisión, etc. Estas aplicaciones demandan gran ancho de banda, lo que contribuye a la presencia de problemas como cuellos de botella, lentitud en la reproducción de imágenes, errores de transmisión y pérdidas de datos.

A pesar de que las señales de video son de naturaleza analógica, podemos transmitirlas también de forma digital teniendo grandes ventajas como mayor fiabilidad, mecanismos de detección de errores, inmunidad a interferencias y ruido, mejor codificación y encriptado, etc. Los avances en la tecnología han permitido capturar, digitalizar, secuenciar y transmitir señales compuestas de video y voz sobre Internet. La señal procesada y comprimida, se almacena en un

servidor de video para luego enviarla a través de la red. La compresión del vídeo generalmente involucra pérdida de información y disminución de calidad. El vídeo

Comprimido es más sensible a los errores ya que un error puede hacer ilegible la imagen.

Existen tres tipos de Video sobre IP:

2.2.1 VIDEO BROADCAST SOBRE IP

Consiste en la transmisión de un archivo con contenido de vídeo, hacia ciertos puntos de la red. La transmisión es unidireccional, es decir los puntos de destino son visualizadores pasivos y no tienen ningún tipo de control en la sesión.

Los videos pueden ser a tiempo real o pregrabados.

El Video broadcast se origina en el servidor y puede ser Unicast. Generalmente la configuración Multicast se implementa en ambientes corporativos para capacitación o presentaciones, y en centros de educación para difundir material didáctico.

2.2.2 VIDEO BAJO DEMANDA SOBRE IP (VOD)

VoD sobre IP (Video on Demand over IP), es un servicio que permite a un usuario seleccionar y ver contenido de video almacenado en un servidor de una red. Es diferente de Video broadcast, porque se trata de un video interactivo, en donde el usuario puede visualizar a tiempo real, iniciar y suspender un vídeo almacenado en un servidor central de vídeo. Entre sus aplicaciones se encuentran:

Capacitación, aprendizaje, entretenimiento y cualquier área donde el usuario precise visualizar los archivos según su itinerario.

2.2.3 VIDEOCONFERENCIA

El servicio Videoconferencia (VC) sobre IP combina transmisiones full dúplex tanto de video como de audio, permitiendo que usuarios ubicados en distintos

puntos geográficos puedan verse y escucharse como si estuvieran en el mismo lugar.

El abaratamiento y disponibilidad de los equipos y servicios de videoconferencia han ocasionado que esta industria sea de gran crecimiento en el mercado de teleconferencias. Se puede tener videoconferencia punto - punto o punto - multipunto.

No se debe confundir la Videoconferencia con la "televisión interactiva" que consiste en la interacción entre una persona y un programa educativo grabado con anterioridad, pero que no requiere de la transmisión de video.

Las normas H323 permiten Videoconferencia sobre IP. La conferencia puede iniciarse desde cualquier computador que disponga de cámara y micrófono. Entre las aplicaciones más conocidas se encuentra: e-learning, telemedicina, reuniones corporativas, capacitación. Para tener un buen funcionamiento de video a tiempo real en Internet, se debe implementar mecanismos de priorización de tráfico de vídeo y voz (Calidad de Servicio). Se debe utilizar el bit llamado Tipo de Servicio (TOS, Type of Service) que se encuentra en el encabezado IP. La Calidad de Servicio consiste en parámetros que proporcionan un buen desempeño de la red frente a tráfico sensible al retardo o a errores de transmisión.

2.3 QOS (QUALITY OF SERVICE)

2.3.1 INTRODUCCIÓN

Dado que distintas aplicaciones como, por ejemplo, teléfono, correo electrónico y video vigilancia, pueden utilizar la misma red IP, es necesario controlar el uso compartido de los recursos de la red para satisfacer los requisitos de cada servicio. Una solución es hacer que los enrutadores y los conmutadores de red funcionen de maneras distintas para cada tipo de servicio (voz, datos y vídeo) del tráfico de la red. Al utilizar la Calidad de servicio (QoS), distintas aplicaciones de red pueden coexistir en la misma red sin consumir cada una el ancho de banda de las otras.

El término Calidad de servicio hace referencia a una cantidad de tecnologías, como DSCP (Differentiated Service Codepoint), que pueden identificar el tipo de datos que contiene un paquete y dividir los paquetes en clases de tráfico para priorizar su reenvío. Las ventajas principales de una red sensible a la QoS son la priorización del tráfico para permitir que flujos importantes se gestionen antes que flujos con menor prioridad, y una mayor fiabilidad de la red, ya que se controla la cantidad de ancho de banda que puede utilizar cada aplicación y, por lo tanto, la competencia entre aplicaciones en el uso del ancho de banda. El tráfico, que se considera crítico y requiere una latencia baja, es un caso típico en el que la QoS puede garantizar respuestas rápidas a solicitudes de movimiento.

2.3.2 CLASIFICACIÓN DE QOS

2.3.2.1 SEGÚN LA SENSIBILIDAD DEL TRÁFICO

Existen distintos tipos de tráfico, cada uno con diferentes requerimientos de retardo, latencia y ancho de banda. Así, se puede distinguir los siguientes tipos:

- QoS muy sensible al retardo. Se trata de tráfico que requiere la garantía de cierta disponibilidad, gran ancho de banda reservado y mínimo retardo y jitter.

Para lograrlo se utilizan mecanismos de prioridad. Ej. Video comprimido y videoconferencia.

- QoS algo sensible al retardo. Se originan en aplicaciones que precisan de retardos de máximo un segundo para no ocasionar pérdida de tiempo para el usuario. También requiere garantía de ancho de banda, pero menos que el caso anterior. Ej. Transacciones online.

-QoS muy sensible a pérdidas. Es el caso del tráfico tradicional, que es más tolerante al retardo pero menos tolerante a pérdidas. Se busca no descartar paquetes ni desbordar los buffers de almacenamiento. La garantía se da a nivel de acceso al medio o en capas superiores, pero no a nivel físico. Ej. Correo electrónico y datos tradicionales.

- QoS no sensible. Se trata del tráfico que no requiere garantías, y puede aprovechar cualquier oportunidad de transmisión restante, asumiendo que los buffers posteriores tendrán la capacidad de envío suficiente para este tipo de tráfico, por lo que se le asigna la prioridad más baja. El algoritmo del mejor esfuerzo responde a este tipo de QoS. Ej. Tráfico de noticias

2.3.2.2 SEGÚN EL SOLICITANTE DE CALIDAD DE SERVICIO

La petición de QoS puede ser solicitada por el usuario final o por los conmutadores de la red. Se tiene dos tipos:

- QoS implícita. Un ruteador o conmutador asigna de manera automática los niveles de calidad servicio, según criterios señalados por el administrador.

- QoS explicita. El usuario o aplicación solicita directamente un determinado nivel de servicio que los ruteadores o conmutadores aceptarán.

TIPO DE APLICACIÓN	ANCO DE BANDA	RETADO	JITTER	TASA DE PERDIDAS
Interactiva (Telnet, Web)	Bajo	Bajo	Medio/Alto	Media
e-mail, ftp, etc.	Alto	Alto	Alto	Alta
Telefonia	Bajo	Bajo	Bajo	Baja
Video Interactivo	Alto	Bajo	Bajo	Baja
Video Unidireccional	Alto	Medio/Alto	Bajo	Baja
Gragil (Emulacion de circuitos)	Bajo	Bajo	Medio/Alto	Nula

TABLAII.03 Requerimientos de ancho de banda para distintas aplicaciones.

2.3.2.3 SEGÚN LAS GARANTÍAS

Tiene relación con la reserva de recursos del sistema para los servicios y son:

- QoS Garantizada (Hard QoS). Realiza reserva absoluta de los recursos de la red para un tráfico determinado lo que proporciona niveles máximos de garantías para dicho tráfico.

- QoS No Garantizada (Lack of QoS). No posee garantías, se trata del tipo de QoS para servicios del Mejor esfuerzo.

- QoS Servicios Diferenciados (Soft QoS). Es un tipo intermedio entre QoS garantizada y no garantizada. Se realiza diferenciación de tráfico, dando preferencias a los que lo requieran. Es utilizado por DiffServ.

2.3.2.4 SEGÚN EL SITIO DE APLICACIÓN

2.3.2.4.1 QOS EXTREMO A EXTREMO

Se lo llama QoS absoluta, en este caso las políticas de Calidad de Servicio se aplican entre los extremos de la red. Existen varias técnicas para conseguirlo ya que proporciona ciertas ventajas, como la selección dinámica del nivel de QoS por parte de las aplicaciones, siempre y cuando se almacene información en la red acerca de las clases de servicio.

2.3.2.4.2 QOS BORDE A BORDE

Se tiene este tipo de QoS, cuando las políticas se aplican entre dos puntos cualesquiera de la red. El administrador no toca los extremos, menos dispositivos manejan QoS y aumenta la seguridad de la red frente a intrusos. No se necesita conocer las reglas de QoS de cada uno de los sistemas operativos de los servidores como en el caso de QoS extremo-a extremo. Se la llama QoS relativa.

2.3.3 PROBLEMAS EN LAS REDES DE DATOS CONMUTADOS

El término Calidad de Servicio o QoS hace referencia a la calidad de la voz, video u otros tipos de datos percibida y los métodos empleados para la correcta transmisión de éstos

Las redes de datos han sido diseñadas para el transporte eficiente de estos, para lo cual no debe perderse información en las mismas, o esta pérdida debe ser mínima, es decir debe asegurarse una QoS a los servicios ofrecidos. En términos cualitativos la QoS se basa en la percepción que tienen los usuarios finales sobre el servicio que están recibiendo, y a esto se conoce también como QoE (Quality of

Experience); pero en términos cuantitativos, la calidad de servicio se refleja en una serie de factores o parámetros técnicos que se pueden medir y ajustar convenientemente de acuerdo a los requerimientos de la aplicación. Entre los más importantes, y que se tomarán en cuenta en este estudio están: latencia, jitter o variación del retardo, paquetes perdidos, disponibilidad de ancho de banda y confiabilidad del canal de datos.

2.3.2.1 LATENCIA (DELAY)

Un sencillo ejemplo para entenderlo de forma fácil:

Una persona navegando por Internet, esperando a que se descargue una página web, o descargando un archivo puede asumir cierta cantidad de tiempo de espera.

Esto no es así en el servicio a tiempo real, sensible a la latencia, a los retardos.

Si la latencia entre extremos llegase a ser muy larga (Por ejemplo 250 ms) la calidad del servicio, en general, podría ser considerada pobre, generaría dificultades reales en el entendimiento de los participantes en la transmisión.

Si en alguna parte, el uso de la red excede el ancho de banda disponible, los usuarios pueden experimentar retardo, también conocido como latencia.

El retraso es el tiempo requerido por una señal para atravesar la red. El retraso entre extremos es el tiempo requerido por una señal generada en el dispositivo de entrada, sea este una cámara o teléfono IP hasta la recepción en el otro extremo de la comunicación. Por lo tanto, el retraso entre extremos es la suma de todos los retrasos en los diferentes apartados de la red y a lo largo de los enlaces por los cuales pasa el tráfico mencionado. Hay muchos factores que contribuyen al retraso entre extremos y se deben tener en cuenta.

El retraso del almacenamiento, el tiempo en espera, y la conmutación o encaminamiento de routers IP, determina en una primera instancia la latencia de la red IP.

2.3.2.2 JITTER (VARIACIÓN DE LA LATENCIA)

La variación de la latencia es la diferencia en el retraso mostrado por el flujo de los diferentes paquetes que forman parte del mismo tráfico. Una alta frecuencia de variación de la latencia es conocida como Jitter.

El Jitter es causado principalmente por las diferencias en los tiempos de espera en cola por los paquetes consecutivos dentro de un flujo y es la consecuencia más importante para QoS.

Teniendo en cuenta que todos los sistemas de transporte presentan algo de Jitter es importante saber que tipos especiales de tráfico especialmente en tiempo real, como la voz, transmisión de video son muy intolerantes al Jitter.

Diferencias en los tiempos de llegada producen cortes en el video o la voz.

2.3.2.3 PAQUETES PERDIDOS

IP no es un protocolo 100% fiable, lo cual significa que en determinadas circunstancias los paquetes de datos pueden ser descartados (perdidos) por la red.

Esto normalmente ocurre cuando la red está especialmente congestionada.

La pérdida de múltiples paquetes de un flujo y secuencia puede causar un ruido que puede llegar a ser molesto para el usuario.

Para mantener la calidad deseada, los paquetes perdidos no deberían de exceder, del entorno al 3% de todos los paquetes.

2.3.2.4 DISPONIBILIDAD DE ANCHO DE BANDA

Como ya se ha dicho, por falta de conocimientos, muchas veces se relaciona únicamente a este término con la Calidad de Servicio, pues se suele pensar que basta con incrementar el ancho de banda para mejorar las prestaciones de una red, lo que en un principio puede ser verdad, pero QoS depende también de otros parámetros como se está viendo; y al aumentar el ancho de banda

innecesariamente se llega a sobredimensionar la red, lo que implica costos innecesarios y muchas veces sin alcanzar los resultados deseados. A pesar de lo mencionado, se debe tener en cuenta que este es el parámetro técnico más importante a considerarse al momento de proporcionar calidad de servicio.

De manera general se puede definir al ancho de banda como la máxima velocidad de transferencia de datos entre dos extremos de una red. El límite lo impone la infraestructura física de los canales y los flujos que comparten algunos de los enlaces. Aunque el ancho de banda no es infinito y depende de las leyes físicas que rigen para un medio físico dado, constantemente se hacen avances en lo referente a técnicas de modulación para aprovechar de manera más eficiente dicho medio.

2.3.2.5 CONFIABILIDAD

Se concibe como la tasa media de error de la red, siendo una propiedad del sistema de transmisión en su conjunto. Diversos factores pueden afectar a la confiabilidad, como por ejemplo ruteadores mal configurados o de bajas prestaciones; exceso de tráfico, que ocasiona congestión en la red; insuficiente espacio de almacenamiento en los nodos, etc. Otro factor muy importante en el momento de considerar la confiabilidad de un sistema es el medio físico que está siendo usado, ya que hay tasas medias de error asociadas a cada uno de estos.

Si se consideran aplicaciones basadas en el protocolo de transporte TCP, este corrige las deficiencias de confiabilidad mediante retransmisiones, lo que se traduce en obligar al emisor a disminuir su velocidad de envío.

En cambio, para aplicaciones basadas en UDP, la falta de confiabilidad causa por ejemplo

Distorsión en las señales analógicas que se reproducen en el destino, puesto que no hay retransmisiones. En cualquier caso, la falta de confiabilidad en una red causa una baja calidad del enlace, lo que puede llegar a significar incluso que este no esté disponible en ciertos momentos.

Al analizar estos factores hay que tomar en cuenta que no existen de forma aislada, sino que están fuertemente relacionados entre sí. Como ya se ha mencionado, los enlaces tienen características inherentes al medio de transmisión de retardo, ancho de banda y confiabilidad. Si el nivel de tráfico que selecciona un

salto determinado excede el ancho de banda correspondiente a ese enlace durante un tiempo prolongado, la calidad de servicio se degrada.

Entre otros factores que degradan la calidad de servicio se puede tener protocolos de enrutamiento inestables, que pueden generar alteraciones en la selección de rutas causando problemas de entregas desordenadas de paquetes y retardos innecesarios.

2.3.4 PROCEDIMIENTOS PARA PROPORCIONAR DIFERENCIACIÓN DE QOS

Los procedimientos para proporcionar diferenciación de QoS son muy variados y actúan sobre las diferentes capas (enlace, red, transporte, etc.) dependiendo de los problemas específicos que se quieran resolver. Todos ellos requieren modificar la ingeniería de la red en su conjunto, aunque hay que tener en cuenta que, en último término, las medidas de calidad de servicio solo se podrán aplicar dentro de la propia red del proveedor.

Se estudian estos procedimientos porque son la base en la que se sustentan las arquitecturas de calidad de servicio, que serán objeto de estudio posteriormente en este mismo capítulo.

Entre los principales procedimientos de calidad de servicio se destacan los siguientes:

2.3.4.1 PRIMERO EN ENTRAR, PRIMERO EN SALIR (FIFO)

El encolamiento FIFO (First Input First Output) básicamente involucra almacenar los paquetes entrantes cuando la red se encuentra congestionada y enviarlos en el mismo orden de llegada cuando la red se ha liberado o se encuentra con bajos niveles de congestión.

Este es el mecanismo por defecto utilizado en la mayoría de dispositivos de red, puesto que el algoritmo no requiere ningún tipo de configuración especial.

Los principales inconvenientes relacionados con este procedimiento son:

- No distingue los paquetes entrantes según la prioridad de cada uno de los mismos.
- El orden de llegada determina el ancho de banda, el retardo y la localización en el búfer del dispositivo.

- Cuando se tiene tráfico a ráfagas, este algoritmo puede causar importantes retardos en la entrega de los paquetes causando graves inconvenientes, especialmente si se trata de aplicaciones sensibles al retardo, y mensajes de control y señalización de la red, ya que no distingue sus distintas prioridades.
- Este ha sido uno de los primeros procedimientos implantados en las redes, pero no estrictamente para proporcionar calidad de servicio, puesto que no realiza una distinción en el tipo de tráfico o reservas de recursos; y es así como se ha visto la necesidad de implementar nuevos procedimientos que se valen de algoritmos sofisticados, como los que se estudian adelante.

2.3.4.2 Encolamiento basado en clases (CBQ)

El procedimiento CBQ (Class Based Queuing) consiste en un mecanismo de colas basado en la clase de tráfico: el tráfico se cataloga en diferentes clases y luego, según estas, se lo asigna a una determinada cola de salida. Agrega las conexiones en clases estableciendo una jerarquía. Con este mecanismo, cada clase tiene una prioridad y un determinado rendimiento.

Como se ve en la figura 3.1, cada clase tiene asignado el porcentaje de ancho de banda que puede utilizar. Este parámetro puede ser estático, si es asignado permanentemente por el administrador de la red o; dinámico si varía dependiendo de las condiciones actuales de la red, según el algoritmo en uso. En dicha figura, como ejemplo, se han asignado ciertos valores o porcentajes de ancho de banda a algunas aplicaciones, los que varían de acuerdo a los requerimientos de cada red.

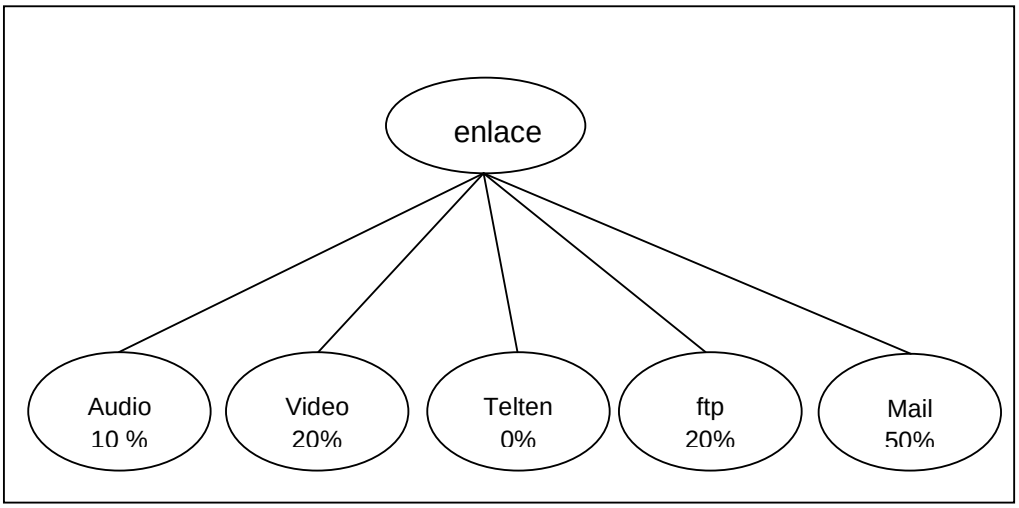


Figura II.1 Ejemplo de la compartición de enlace en CBQ

Los objetivos principales del encolamiento basado en clases son los de asegurar que cada clase con una demanda suficiente, recibirá aproximadamente el ancho de banda que le corresponde en los intervalos de tiempo adecuados cuando exista congestión y; que la distribución del ancho de banda sobrante generado si alguna de las clases no se encuentra haciendo uso del recurso que tiene asignado, no debe ser aleatoria, sino que ha de seguir un cierto procedimiento.

En este procedimiento se realiza una especie de multiplexación en tiempo, en la que se van tomando alternadamente paquetes de las distintas colas con un tamaño que depende de la asignación de recursos y, se los va despachando hasta que el umbral prefijado se supera o la cola correspondiente se vacía.

2.3.4.3 ENCOLAMIENTO EQUITATIVO PONDERADO (WFQ)

WFQ (Weighted Fair Queuing) es un procedimiento de garantía de ancho de banda basado en una disciplina de colas de reparto equitativo de recursos, en donde el tráfico de poco volumen o de mejor comportamiento recibe un trato preferencial para reducir su tiempo de respuesta y; el tráfico de gran volumen se reparte el ancho de banda restante de forma proporcional.

Este algoritmo es una mejora al esquema denominado Fair Queuing (FQ), en el cual el dispositivo de conmutación mantiene múltiples colas, las que son

atendidas de forma cíclica, tomándose un paquete en cada turno de cada cola no vacía.

Tanto en FQ como en WFQ, cada flujo de datos tiene una cola FIFO separada. En FQ, con un enlace de velocidad de transmisión de datos de R, en un momento dado los N flujos de datos activos (los únicos con colas no vacías) son servidos a la vez, cada uno a un promedio velocidad de transmisión de datos de R / N. Dado que cada flujo de datos tiene su propia cola, un mal comportamiento de flujo (que ha enviado los paquetes más grandes o más paquetes por segundo que los otros desde que esta activo) solo se castigará así mismo y no a otras sesiones.

WFQ es un algoritmo sumamente eficiente ya que puede utilizar todo el ancho de banda disponible para enviar tráfico de baja prioridad en el caso de que no exista ninguna cola con tráfico de mayor importancia. Otra de las ventajas de este procedimiento es que las colas se atienden de manera cíclica, consistente y equitativa, lo que permite una estabilización del jitter o variación de retardo.

2.3.4.4 TASA DE ACCESO COMPROMETIDA (CAR, COMMITTED ACCESS RATE)

Es un mecanismo de garantía que se basa en las siguientes funcionalidades:

2.3.4.4.1 CLASIFICACIÓN DE PAQUETES

Consiste en distribuir el tráfico en Clases de Servicio según diferentes políticas como las direcciones IP, el tipo de acceso, etc., considerando el bit de precedencia IP del campo ToS de la cabecera IP.

A cada Clase de Servicio le corresponde determinada QoS, con su política de gestión de tráfico que incluye gestión de congestión, asignación de ancho de banda y límites de retardo.

2.3.4.4.2 LIMITACIÓN DE LA TASA DE TRANSMISIÓN

Consiste en limitar la máxima velocidad de transmisión de tráfico en la interfaz de acceso de la red. Cuando el tráfico excede la tasa límite, se aplican políticas de acción de tráfico. Si el tráfico está dentro del límite se le permite pasar, caso contrario es transmitido con la prioridad más baja o descartado. Esta función se realiza en tres fases:

Equiparación de tráfico. Consiste en identificar el tipo de tráfico para limitar la tasa de transferencia y configurar la precedencia. Se basa en criterios como el tráfico IP, precedencia IP, grupos de QoS y direcciones MAC.

Medición de tráfico. Consiste determinar si el tráfico excede o no la tasa de transferencia límite, se utiliza el mecanismo de medida Token Bucket que se basa en los parámetros Token Bucket Size (Profundidad del cubo) y Token Bucket Rate (Tasa de Testigos).

Política de acción. Es la acción a ejecutarse con el tráfico previamente medido, si está dentro de la tasa límite se ejecuta la acción de conformidad correspondiente, de lo contrario se ejecuta la acción de exceso correspondiente. Las acciones pueden ser: transmitir, fijar la precedencia y transmitir, descartar, fijar precedencia y continuar, fijar nivel de QoS y transmitir, fijar el nivel de QoS y continuar.

2.3.4.5 DESCARTE ALEATORIO ANTICIPADO (RED, RANDOM EARLY DETECTION)

Este mecanismo evita la congestión mediante el control del tamaño de cola, indicando a los sistemas finales el momento de suspender el envío de paquetes.

Descarta paquetes en forma aleatoria y notifica al emisor que debe disminuir y adaptar su tasa de transmisión a la de la red para retrasar el tráfico hasta que termine la congestión. Si lo anterior no resulta se descarta paquetes indiscriminadamente.

2.3.5 ALGORITMOS PARA LA OBTENCIÓN DE QOS

Existen varios algoritmos de Calidad de Servicio, que realizan control de congestión a cierto nivel. Considerando la Clase de Servicio, se tiene los siguientes algoritmos:

2.3.5.1 ALGORITMO DEL MEJOR ESFUERZO

Se los llama así, porque no ofrecen ninguna garantía de transmisión, el nivel de calidad de servicio ofrecido es prácticamente nulo. Aquí se encuentran los algoritmos tradicionales como FIFO. Su principal problema es que no puede aislar

flujos, es decir el tiempo de llegada de los paquetes de un flujo, puede verse afectado por otros flujos.

2.3.5.2 ALGORITMO DETERMINÌSTICO

Estos algoritmos reservan ancho de banda para asegurar la transmisión de un flujo en las peores condiciones, pero evitando congestiones. Se reserva un equivalente al ancho de banda del pico de una transmisión en ráfaga de dicho flujo, con lo cual la congestión es prácticamente imposible. Si debido a limitaciones físicas no se puede reservar ancho de banda, el algoritmo rechazaría la transmisión del flujo, lo que implica una utilización muy por debajo de las posibilidades de la red.

Los algoritmos determinísticos aíslan completamente los flujos, ocasionando un uso ineficiente de los recursos de la red, ya que las ráfagas son muy cortas y poco frecuentes.

2.3.5.3 ALGORITMOS INTERMEDIOS

Estos algoritmos buscan hacer un uso eficiente de los recursos y ofrecer Calidad de Servicio, aunque no tan estrictamente como los determinísticos, pero logran un buen desempeño de la red y buen aprovechamiento de los recursos disponibles.

Es posible el retraso ocasional de algún paquete, pero si un paquete supera su tiempo de expiración puede ser descartado directamente. Los algoritmos intermedios ofrecen los siguientes tipos de servicio:

2.3.5.3.1 SERVICIOS ESTADÍSTICOS

Trabajan estadísticamente, asegurando una QoS con una determinada probabilidad. Antes de aceptar la transmisión de un flujo, obtienen los parámetros que lo modelan, calculan el porcentaje de QoS que se le puede asignar, y si es mayor o igual al requerido, el flujo se acepta. Con este algoritmo es posible transmitir mayor cantidad de flujos que con un determinístico, pero como es una probabilidad, no se garantiza un resultado. Sin embargo, muchos de ellos han resultado ser muy exactos, su comportamiento es casi determinístico, aprovechando más la capacidad de la red.

2.3.5.3.2 SERVICIOS DE DEGRADACIÓN LIMITADA

En la transmisión de flujos, se puede permitir la pérdida de algunos datos. Estos algoritmos aprovechan lo anterior durante la gestión de los paquetes, obteniendo una capacidad de decisión más alta. Cuando un flujo ingresa a la red, sus paquetes son separados en diferentes tipos con su respectiva prioridad y retardo máximo. Si se presenta una congestión, tendrán prioridad los paquetes más importantes.

2.3.5.3.3 SERVICIOS PREDICTIVOS

Utilizan datos obtenidos al medir las características de los flujos. Para admitir un flujo se debe confiar en la información dada por el servidor del flujo, pero es necesario también calcular dinámicamente sus parámetros dentro de la red para asegurar que la información sea confiable y verdadera. Así, se toman mejores decisiones acerca de los requerimientos del flujo, lo que provoca un correcto funcionamiento y una utilización elevada de los recursos.

Los flujos son organizados en grupos con necesidades similares, pudiéndose aplicar políticas distintas por grupo, asignar prioridades entre grupos o limitar el uso de los recursos según el grupo. Incluso, añaden comunicaciones sin calidad de servicio (grupo con prioridad mínima y sin reserva de ancho de banda), lo que aumenta la utilización de la red.

2.3.6 MECANISMOS DE CALIDAD DE SERVICIO

Existen dos mecanismos para QoS, los mecanismos de control del tráfico y los mecanismos de provisión y configuración.

2.3.6.1 MECANISMOS DE CONTROL DE TRÁFICO

Estos mecanismos incluyen algoritmos de cola y clasificación de paquetes. Se pueden aplicar a acumulaciones de tráfico o a flujos de tráfico por conversación.

Los mecanismos de control del tráfico pueden clasificarse en:

Mecanismos por conversación. Tratan por separado cada flujo de tráfico para cada conversación.

Mecanismos por acumulación. Agrupan varios flujos de tráfico en una única clase.

Se puede hacer una analogía con un avión, donde en el cual los pasajeros son clasificados en primera clase, clase de negocios y clase turista. Los pasajeros de la misma clase tienen el mismo tratamiento (mecanismos de acumulación). El tratamiento por conversación se asemeja a un avión privado para cada pasajero, lo que resulta lujoso pero caro.

2.3.6.1.1 SERVICIOS DIFERENCIADOS (DIFFSERV, DIFFERENTIATED SERVICES)

Es un mecanismo de tratamiento de tráfico por acumulación, adecuado para redes enrutadas. Define el campo DSCP (DiffServ Codepoint) en los encabezados IP, los dispositivos que envían tráfico a una red Diffserv marcan con el mismo valor DSCP a los paquetes de flujos con similares requisitos de QoS, al agregar el flujo a una cola común o al programar el comportamiento. Los ruteadores utilizan DSCP para clasificar paquetes y aplicar un comportamiento de cola específico según los resultados de la clasificación.

2.3.6.1.2 SERVICIOS INTEGRADOS (INTSERV, INTEGRATED SERVICES)

IntServ es una estructura para definir servicios, por lo que contiene un conjunto de mecanismos de control de tráfico subyacentes. Los servicios IntServ se suelen aplicar por conversación individual. Generalmente, IntServ se asocia con el Protocolo de Reserva de Recursos (RSVP, Resource ReServation Protocol)

2.3.6.1.3 IEEE 802.1P

Es un mecanismo de control del tráfico de acumulación, conveniente para redes LAN, actualmente integrado en el estándar IEEE 802.1D (LANs con puentes). Su objetivo es describir el modo de asignar prioridades de usuario y filtrar de forma dinámica el tráfico multicast en una LAN. Define un campo en el encabezado MAC de los paquetes Ethernet, donde los hosts o ruteadores que envían tráfico a una LAN, marcan cada paquete transmitido con un nivel de prioridad entre 0 y 7.

Requiere una etiqueta adicional de 4 bytes opcional en redes Ethernet y solo puede ser soportado en una LAN, pues las etiquetas 802.1Q se eliminan al pasar por un ruteador.

Los paquetes con prioridad más baja no son enviados si es que hay paquetes en la cola de niveles más altos. 802.1Q no describe protocolos de control de

admisión, si fuera posible dar control de prioridad a todos los paquetes, la red se congestionaría fácilmente. Por sí mismo, 802.1p no limita la cantidad de recursos que utiliza una aplicación, pero muchas implementaciones lo hacen.

2.3.6.1.4 MODO DE TRANSFERENCIA ASÍNCRONO (ATM, ASYNCHRONOUS TRANSFER MODE)

ATM es una tecnología de telecomunicación de capa de enlace que provee tratamiento del tráfico de alta calidad. Divide los paquetes en celdas de capa de enlace y los envía a la cola, donde se aplican algoritmos de administración de cola adecuados para uno o varios servicios ATM.

Para aprovechar completamente la capacidad de los sistemas de transmisión, la información se transmite en forma de paquetes muy pequeños llamados “celdas ATM” de longitud fija y que se pueden enrutar individualmente mediante canales y trayectos virtuales. Debido al pequeño tamaño de las celdas, se puede programar el tráfico muy precisamente y con baja latencia.

2.3.6.1.5 SISTEMA DE SERVICIOS INTEGRADOS PARA LÍNEAS DE BAJA TASA DE TRANSFERENCIA

ISSLOW es un mecanismo especial de encolamiento que divide los paquetes IP conforme se transmiten a velocidades relativamente lentas, como conexiones telefónicas a módems. Su propósito es reducir la latencia que se puede experimentar en ciertos paquetes, cuando la capacidad de la red es muy baja, lo cual es intolerable en audio y video, ya que disminuye la calidad.

2.3.7 PROTOCOLOS DE CALIDAD DE CALIDAD DE SERVICIO

El tipo más apropiado de Calidad de Servicio para uno o varios flujos depende de la topología de la red, las aplicaciones y la política de QoS.

El Protocolo RSVP nació en 1990 como método definitivo para la aplicación de QoS, pero fue diseñado solamente para una arquitectura de red. En vista de aquello, el Grupo de Trabajo de Ingeniería en Internet (IETF, Internet Engineering Task Force), contempló la posibilidad de que las diferentes tecnologías de QoS actúen juntas para suministrar los niveles de QoS deseados, así, se utilizaría RSVP en los ruteadores de extremo, DiffServ en la parte central para agregar

tráfico, MPLS para definir la mejor ruta a través de la red utilizando etiquetas y 802.1p/q para redes 802. Entre los protocolos más utilizados se tiene a RSVP y SBM.

2.3.7.1 PROTOCOLO DE RESERVA DE RECURSOS (RSVP, RESOURCE RESERVATION PROTOCOL)

RSVP es un protocolo de señalización orientado principalmente a redes IP y que proporciona control para la reserva. Opera sobre IPv4 e IPv6. Debido a que IP no permite realizar reserva de recursos, los mensajes RSVP se envían en paralelo con los paquetes IP. RSVP no es un protocolo de transporte ni de encaminamiento, más bien funciona sobre cualquiera de ellos ya sea unicast o multicast, podría decirse que es un protocolo de control de Internet. El protocolo de encaminamiento envía sus mensajes a un destino y a continuación los mensajes RSVP para reservar los recursos (QoS). RSVP reserva recursos en todos los nodos de la ruta.

El nodo extremo utiliza RSVP para solicitar Calidad de Servicio para uno o varios flujos. Los nodos intermedios lo utilizan para entregar solicitudes simplex (las reservas se hacen en una dirección) de Calidad de Servicio y para establecer y mantener el estado de servicio solicitado. RSVP hace responsable a los múltiples receptores heterogéneos de la solicitud de QoS según sus propias necesidades ya que podría necesitar reservar recursos para distintas aplicaciones. Una misma aplicación puede actuar como emisor y receptor.

RSVP es un componente clave de la arquitectura de los Servicios Integrados (IntServ), donde proporciona señalización para permitir la reserva de recursos de la red y define el funcionamiento y la forma de petición e intercambio de información entre los elementos de la red, con el objetivo de realizar control de la calidad de servicio. Una sesión RSVP está definida por la dirección destino (unicast o multicast), el ID del Protocolo IP y el Puerto Destino.

2.3.7.2 OPERACIÓN DE RSVP

Para brindar Calidad de Servicio en una transmisión, el protocolo consulta localmente si la QoS deseada puede ser provista y establece los parámetros requeridos en el clasificador y en el planificador de paquetes. El clasificador

establece la ruta y el planificador toma las decisiones de envío con el fin de entregar la QoS deseada, incluso puede negociar con los hosts responsables de su propia gestión de QoS, para proporcionar la calidad solicitada por RSVP.

La aplicación del emisor genera una sesión RSVP. Se genera un mensaje de ruta a lo largo del trayecto establecido por el protocolo de encaminamiento, cada nodo analiza el mensaje de ruta y almacena el estado de ruta que contiene la dirección IP del nodo anterior. Cuando el mensaje de ruta llega a su destino, se genera el mensaje de reserva que viaja hacia el emisor.

Cuando el mensaje de reserva llega al emisor, pasa a los componentes la Arquitectura de Servicios Integrados (ISA, Integrated Services Architecture) que realizan pruebas y si hay un fallo, envían un mensaje de error de Reserva. Si no hay error, se activa el clasificador de paquetes y el planificador de paquetes, que a su debido tiempo envía el mensaje de reserva hacia el siguiente nodo.

El mensaje de reserva se propaga a través de la red hasta encontrar un nodo con reserva igual o superior. El último nodo recibe y acepta el mensaje de reserva, luego envía una confirmación en caso de que el receptor la haya solicitado.

2.3.7.3 SITUACIÓN ACTUAL DE RSVP

La arquitectura de Servicios Integrados con el protocolo RSVP, se originó con el fin de garantizar Calidad de Servicio mediante la reserva de recursos. Sin embargo hay tres problemas principales que afectan al funcionamiento de RSVP, la escalabilidad, el enrutamiento y el no poder trabajar sobre redes no RSVP.

La escalabilidad es un problema debido a que la señalización e información de estado necesaria para todos los flujos y nodos, aumenta conforme crece la red.

La infinidad de nodos en Internet, hace cuestionable la escalabilidad del modelo y ha impedido un gran despliegue, excepto por las áreas donde las rutas no se obtienen de algoritmos de enrutamiento. También se ha considerado a RSVP como alternativa al uso del Protocolo de Distribución de Etiqueta (LDP, Distribution Protocol), en la arquitectura MPLS.

El enrutamiento constituye otro problema debido a que el enrutamiento se da en el instante de establecer la sesión, y los algoritmos de enrutamiento utilizados no saben las características de la solicitud de reserva del receptor, es posible que la

decisión adoptada al establecer la ruta, no sea la más apropiada considerando sólo los parámetros de caracterización del tipo de QoS elegido.

No todos los nodos intermedios de la ruta establecida tendrán implementado RSVP, por esta razón la reserva extremo a extremo estará condicionada por dichos sistemas.

2.3.8 ARQUITECTURA DE CALIDAD DE SERVICIOS

En un principio, el Internet contemplaba un servicio del “mejor esfuerzo”, pero debido al gran crecimiento de la demanda para aplicaciones de videoconferencia y multimedia en tiempo real, fue necesario adaptar los protocolos de Internet para ofrecer algún tipo de Calidad de Servicio. En la cabecera IPv4, existe el campo denominado TOS, que indica la prioridad de un paquete, pero aunque la prioridad permite clasificar los datagramas en categorías, no ofrece una garantía estricta ya que puede haber congestión debido a un caudal excesivo de datagramas con la misma prioridad.

Las arquitecturas de QoS son implementadas con el objetivo de proveer Calidad de Servicio en una red. En dichas arquitecturas, los elementos de control de carga de servicio son muy importantes y deben tomar en cuenta la señalización de la aplicación extremo-extremo, la señalización del servicio extremo-extremo y la señalización de gestión de recursos para control basado en vigilancia de tráfico y recursos de red.

Para controlar la carga se puede realizar una negociación del nivel de servicio, una solicitud de servicio sin negociación previa o también se puede utilizar un método eficiente para la selección de rutas con Calidad de Servicio que incluye ingeniería de tráfico y redes privadas virtuales.

Se estableció tres arquitecturas para brindar QoS en Internet, el modelo de Servicios Integrados (IntServ), el modelo de Servicios Diferenciados (DiffServ) y MPLS. IntServ incluye servicios de mejor esfuerzo, tiempo real y compartición controlada de los enlaces. DiffServ personaliza los servicios que obtienen los usuarios según la asignación de diferentes niveles de servicio a cada usuario.

MPLS es una solución estándar, aplicable a cualquier protocolo de capa red y envía los paquetes según su etiqueta.

2.3.8.1 ARQUITECTURA DE SERVICIOS INTEGRADOS (INTSERV)

El modelo de Servicios integrados está basado en la reserva de recursos, para garantizar niveles calidad de servicio a las aplicaciones siempre y cuando haya suficientes recursos y no haya gran cogestión. Para ésto, se requieren definiciones uniformes de los niveles de QoS, de los parámetros que los especifican y de un protocolo de reserva de recursos en los nodos extremos y lo elementos intermedios de la red.

En IntServ, el concepto de flujo es muy importante. Un flujo es un tráfico continuo unidireccional de datagramas, relacionados entre sí, producidos por una acción del usuario y que requieren la misma Calidad de Servicio. Los flujos de una misma clase reciben la misma Calidad de Servicio.

En IPv4 los flujos se identifican por las direcciones de origen y destino, el puerto de origen y destino, y el protocolo de transporte utilizado (TCP o UDP).

2.3.8.1.1 NIVELES DE CALIDAD DE SERVICIO

Un flujo es el tráfico continuo de datagramas relacionados entre sí que requieren la misma Calidad de Servicio y que se origina por una operación del usuario. Los flujos pueden agruparse en clases, para recibir la misma calidad de servicio. En la arquitectura IntServ se tiene tres tipos de servicio:

- **Mejor Esfuerzo (BE).** Servicio que no tiene ninguna garantía

- Carga controlada (SCL). Ofrece un comportamiento comparable al mejor esfuerzo, cuando hay baja carga en la red, es decir, ofrece un buen tiempo de respuesta, pero sin garantía estricta. No existe un límite superior en el retardo de cola, sin embargo se utiliza el control de admisión incluso en caso de congestión, con el fin de mantener muy baja la tasa de pérdidas y el retardo, y garantizar que la mayoría de paquetes se entreguen con éxito. Es adecuado

para aplicaciones tolerantes a cierta cantidad de pérdidas y de retardo.

- Servicio Garantizado (SG). Este servicio garantiza la QoS solicitada conforme a la tasa límite. Se establece un nivel de ancho de banda y un tiempo máximo de transmisión extremo-extremo, pero pueden existir variaciones del retardo.

Se diseñó para aplicaciones con requerimientos en tiempo real, como audio y vídeo por lo que no existen pérdidas en la cola. Todos los dispositivos intermedios

de la ruta deben ofrecer las garantías solicitadas para un flujo específico, asignando un ancho de banda y un espacio en buffer, aunque esto depende del medio físico.

Las aplicaciones deben transmitir una Tspec (especificación de tráfico) para definir el tipo de tráfico. La Tspec está basada en parámetros como la tasa de transmisión, el tamaño máximo de paquetes, entre otros.

Los niveles de calidad de servicio integrados y las especificaciones de RSVP son independientes, lo que permite utilizar servicios integrados con diferentes mecanismos de reserva, o RSVP con distintos tipos de servicio.

2.3.8.1.2 COMPONENTES DE INTSERV

Un ruteador debe implementar Calidad de Servicio en cada flujo, la función que crea diferentes calidades de servicio se denomina “Control de Tráfico”, y está formada por el clasificador de paquetes, el planificador de paquetes y el control de admisión.

Los componentes de la arquitectura de Servicios Integrados son:

- Clasificador de paquetes. Clasifica localmente los paquetes entrantes en clases de servicio según el contenido de sus cabeceras.

- Planificador de paquetes. Controla el orden de envío de los paquetes mediante colas y el exceso de paquetes.

- Control de admisión. Lo realiza un algoritmo de decisión. Consiste en determinar si existen recursos suficientes para la QoS solicitada para admitir o no los flujos.

- Protocolo de Reserva. Establece la conexión con cierta Calidad de Servicio, entre los nodos extremos de la red.

Un ruteador realiza dos clases de funciones para la Arquitectura de Servicios Integrados:

- Funciones de Respaldo. Crean y mantienen el conjunto de bases de datos utilizadas por las funciones de reenvío y son las siguientes:

- Agente de encaminamiento. Crea y mantiene las bases de datos de enrutamiento.

- Agente de reserva. Implementa el protocolo de reserva de recursos que mantiene la información de estado de flujo.

- Control de admisión. Determina si hay recursos disponibles con la Calidad de Servicio solicitada.

- Agente de gestión. Modifica la base de datos de Control de Tráfico y dirige el Control de Admisión para determinar las políticas de Control de Admisión.

- **Funciones de Reenvío.** Se realizan de forma óptima para cada paquete y son:

  - Clasificación y selección de ruta. Organiza los paquetes según su clase, y dependiendo de la clase y la dirección IP destino, se determina el siguiente salto.

  - Planificación de Paquetes. Determina la forma de distribución y el orden de envío de los paquetes en las colas de los puertos de salida, a partir de la clase del paquete, la base de datos de control de tráfico y la actividad del puerto de salida.

2.3.8.1.3 PROTOCOLO DE RESERVA

IntServ utiliza el protocolo RSVP, para la reserva de recursos. RSVP es un protocolo de control que permite reservar una cierta cantidad de ancho de banda para cierta ruta entre los nodos extremos de la red.

Cada nodo realiza un proceso o demonio RSVP, para mantener el protocolo entre los nodos y gestionar los componentes del nodo local. El demonio RSVP recibe las peticiones de reserva y decide si el usuario y flujo están autorizados para la reserva solicitada. El control de admisión determina si existen recursos disponibles. Si la reserva es aceptada. RSVP configura los parámetros según el nivel de servicio solicitado en el clasificador de paquetes y en el encolador de paquetes.

El funcionamiento de RSVP está definido para grupos mulitcast (el tráfico unicast es un caso particular), ya que es un tipo de tráfico adecuado para flujos de audio y vídeo en tiempo real. En una emisión multicast los usuarios pueden integrarse o eliminarse del grupo multicast dinámicamente y sin aviso previo. Cada ruteador lee el mensaje de reserva y garantiza el ancho de banda solicitado o devuelve un mensaje de error si no hay capacidad disponible.

A pesar del interés que el modelo IntServ despertó en un principio, su uso no se ha difundido, ni entre los fabricantes ni en los ISPs debido que su problema de escalabilidad, es decir que el costo de su implementación crece por lo menos linealmente con la complejidad de la red. Esto se debe a que RSVP es un protocolo orientado a conexión, por lo que los ruteadores deben mantener información de estado de todos los flujos activos que los atraviesan. La información de estado puede ser aceptable en los ruteadores de la periferia, pero es inmanejable en los ruteadores de núcleo de la red, que soportan miles de conexiones activas.

2.3.8.2 ARQUITECTURA DE SERVICIOS DIFERENCIADOS (DIFFSERV)

Debido al problema de escalabilidad de IntServ, aparece un modelo alternativo llamado DiffServ (Arquitectura de Servicios Diferenciados), en el cual cada paquete tiene un código que indica su clase, los ruteadores deberían conocer el tratamiento para cada clase, es decir no mantienen información sobre conexiones o flujos determinados. La cantidad de clases es limitada e independiente del número de hosts o de flujos que atraviesan los ruteadores. Por ésta razón la arquitectura DiffServ es escalable. Se da importancia al campo ToS de IPv4.

El objetivo de Diffserv es hacer posible una diferenciación de servicios escalable en Internet y redes IP. DiffServ separa las operaciones de reenvío y control en los ruteadores. El reenvío utiliza el Comportamiento por Salto (PHB, Per Hop Behavior), en cada nodo de la red, con independencia de la forma de construcción de los servicios extremo-extremo.

2.3.8.2.1 FUNCIONES DE LA ARQUITECTURA DIFFSERV

En la Arquitectura de Servicios Diferenciados se realizan las siguientes funciones:

- Clasificación y Agregación de Tráfico.
- Marcación del tráfico a nivel de capa 3 mediante el campo DS (DiffServ) queredefine a ToS en datagramas IP, y que pretende unificar los campos similares en IPv4 e IPv6.
- Clasificación y marcación de los paquetes para que reciban cierto tratamiento por salto de la ruta (no extremo-a-extremo).
- La clasificación, marcación, políticas y acondicionamiento del tráfico solo se realizan en los nodos frontera.

Cada nodo realiza un proceso o demonio RSVP, para mantener el protocolo entre los nodos y gestionar los componentes del nodo local. El demonio RSVP recibe las peticiones de reserva y decide si el usuario y flujo están autorizados para la reserva solicitada. El control de admisión determina si existen recursos disponibles. Si la reserva es aceptada. RSVP configura los parámetros según el nivel de servicio solicitado en el clasificador de paquetes y en el encolador de paquetes.

El funcionamiento de RSVP está definido para grupos mulitcast (el tráfico unicast es un caso particular), ya que es un tipo de tráfico adecuado para flujos de audio y vídeo en tiempo real. En una emisión multicast los usuarios pueden integrarse o eliminarse del grupo multicast dinámicamente y sin aviso previo. Cada ruteador lee el mensaje de reserva y garantiza el ancho de banda solicitado o devuelve un mensaje de error si no hay capacidad disponible.

A pesar del interés que el modelo IntServ despertó en un principio, su uso no se ha difundido, ni entre los fabricantes ni en los ISPs debido que su problema de escalabilidad, es decir que el costo de su implementación crece por lo menos linealmente con la complejidad de la red. Esto se debe a que RSVP es un protocolo orientado a conexión, por lo que los ruteadores deben mantener información de estado de todos los flujos activos que los atraviesan. La información de estado puede ser aceptable en los ruteadores de la periferia, pero es inmanejable en los ruteadores de núcleo de la red, que soportan miles de conexiones activas.

2.3.8.2.4 OPERACIÓN DE LA ARQUITECTURA DIFFSERV

En DiffServ, los paquetes son clasificados sólo en el dispositivo de acceso a la red. Dentro de la red, el tipo de procesamiento que reciban los paquetes depende del encabezado. En la Figura 1.21 se puede observar la operación de DiffServ.

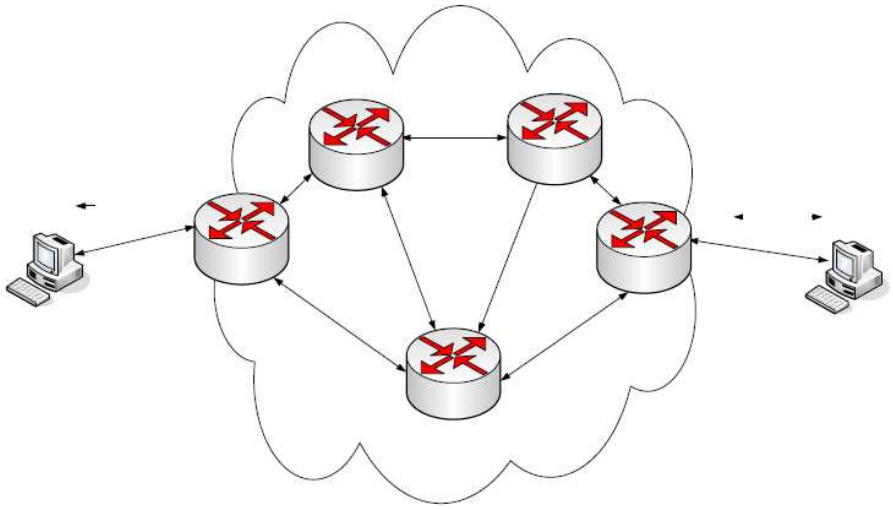


Figura II.2 Dominio de Servicios Diferenciados

Los ruteadores de borde clasifican los paquetes y los marcan con la precedencia IP o el valor DSCP para la red DiffServ. Otros dispositivos en el núcleo que soportan Diffserv, utilizan el valor DSCP en la cabecera IP, para seleccionar un comportamiento PHB para el paquete y entregarle el tratamiento de Calidad de Servicio apropiado. La información sobre Calidad de Servicio en cada datagrama viaja en un campo de 8 bits llamado DS.

Los seis bits más significativos se llaman DSCP y a los dos menos significativos se los llama CU (Currently Unused) ya que no están definidos en la arquitectura DiffServ, pero se los utiliza para ECN (Notificación de Congestión Explícita).

El estándar DiffServ utiliza los mismos bits de precedencia que ToS (los más significativos DS5, DS4 y DS3) para establecer la prioridad, pero aclara la definición al usar los siguientes tres bits en DSCP. DiffServ reorganiza y renombra lo niveles de precedencia (aún definidos por los tres bits más significativos de DSCP). En DiffServ se definen tres tipos de servicio:

- **Servicio de Reenvío Ágil o Premium (EF, Expedited Forwarding).** Entrega la mayor calidad, pues garantiza ancho de banda mínimo, tasa máxima de pérdida de paquetes, retardo medio máximo y jitter máximo. Se especifican en el SLA contratado al ISP. El valor del subcampo DSCP correspondiente es

101110. Es un servicio apropiado para aplicaciones a tiempo real y VPNs. Su costo es el más alto.

- **Servicio de Reenvío Asegurado (AF, Assured Forwarding).** Asegura un trato preferente, pero no garantiza ancho de banda, retardos, etc. Es adecuado para clientes que requieren cierto nivel de fiabilidad incluso durante congestiones. Se especifica en el SLA contratado al ISP. Existen cuatro clases, a cada una se le puede asignar una cantidad de recursos (ancho de banda, espacio en buffers, etc.) en los ruteadores. Los tres primeros bits del DSCP indican la clase. Para cada clase se definen tres categorías de descarte de paquetes (probabilidad alta, media y baja), que se especifican en los bits cuarto y quinto, como se detalla en la TABLA II.04

	Presencia de descarte		
Clase	Baja	Media	Alta
4	10001	10010	10011
3	01101	01110	01111
2	01001	01010	01011
1	00101	00110	00111

TABLA II.04 Categorías para descarte de paquetes

- **Servicio Mejor Esfuerzo.** Le corresponde el valor de 0 para los tres primeros bits del DSCP. Los dos restantes pueden servir para marcar una prioridad, dentro del grupo “Mejor esfuerzo”. No se ofrece garantías.

El servicio de Reenvío Ágil es equivalente al Servicio Garantizado de IntServ y el Servicio de Reenvío Asegurado corresponde al Servicio de Carga Controlada.

Algunos ISPs ofrecen servicios para diferentes categorías, generalmente basados en las clases del servicio de Reenvío Asegurado. DiffServ suele utilizar solo los tres primeros bits del DSCP para marcar los paquetes (valores altos indican mayor prioridad), en la práctica hay bastante compatibilidad entre el campo DSCP en DS y el campo Precedencia de ToS, como se puede observar en la TABLA II.05

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

TABLA II.05 Correspondencia de campo de preferencia con DiffServ

2.3.8.2.5 ELEMENTOS BÁSICOS DEL MODELO DIFFSERV

Los elementos básicos de DiffServ son:

- **Nodo frontera.** Realizan las funciones necesarias para conectar un dominio

DS a otro sea o no DS.

- **Nodo interno.** Realiza las funciones requeridas en los nodos conectados a

nodos DS.

- **Nodo de entrada**. Realiza las funciones que permiten manejar el tráfico

entrante en un dominio DS.

- **Nodo de salida.** Realiza las funciones que permiten manejar el tráfico saliente

en un dominio DS.

Generalmente los nodos frontera contienen todas las funciones y los nodos internos parte de ellas. Las SLA (Acuerdos de Nivel de Servicio) y TCA (Acuerdo de Acondicionamiento de Tráfico) se pueden aplicar a un ISP y un cliente, que podría estar en otro dominio.

2.3.8.2.6 TIPOS DE MARCAS

DiffServ utiliza básicamente tres tipos de marcas para clasificar el tráfico:

- **Ninguna (None).** Entrega el servicio convencional del “mejor esfuerzo”.

- **Asegurado y definido en un perfil (Assured and in profile).** Se establece en el SLA entre el cliente y el ISP.
- **Asegurado y fuera de perfil (Assured and out of profile).** Podría no cumplir lo establecido en el SLA.

2.3.8.2.7 GRUPOS DE PHB

El proceso de envío de los paquetes modificados por la arquitectura Diffserv, en un ruteador, se conoce como Comportamiento por salto (PHB, Per Hop Behavior).

Un PHB es una descripción abstracta del comportamiento del BA (Behavior Aggregate), que es un conjunto de paquetes con un mismo valor de DSCP enviados al mismo destino. Un PHB describe el tratamiento que han recibido los paquetes durante su transmisión para entregar Diffserv, es decir indica una combinación de comportamientos de reenvío, clasificación, planificación, y descarte. El DSCP de un paquete define el PHB e informa a los nodos de la red acerca del PHB del paquete. Los PHB estandarizados son los siguientes:

- **PHB por defecto (DE, Default).** Equivalente al servicio del mejor esfuerzo.
- **PHB selector de clase.** Su objetivo es la compatibilidad con los bits de precedencia del campo ToS para dar prioridades.
- **PHB de reenvío ágil (EF).** Pretende entregar servicios con pérdidas, latencia y jitter bajos, y garantizar ancho de banda.
- **PHB de reenvío asegurado (AF).** Busca satisfacer la demanda, para asegurar el reenvío de paquetes IP, tanto en Internet como en intranets.

2.3.8.2.8 APLICACIONES DE DIFFSERV

Dimensionar una red con DiffServ es muy complejo, ya que se deben tomar en cuenta las cargas de los enlaces, el comportamiento de las aplicaciones, el tráfico en hora pico, etc. El Servicio PHB EF puede utilizarse para VPNs (Redes Privadas Virtuales), debido a la lta calidad, con bajo retardo y poca pérdida de paquetes. El PHB AF puede servir para dar el llamado “Servicio Olímpico” que consiste en tres clases, oro, plata y bronce para la asignación de recursos, (oro 60%, plata 30% y bronce 10%). En la Tabla 1.6 se puede observar algunas aplicaciones con los servicios correspondientes.

Aplicación	Clase	PHB
Video	Premiun	EF
Voz		
Seciones interactivas	Oro	AF31
Telnet	Plata	AF21
HTTP		AF22
SMTP	Bronce	
FTP		AF12

TABLA II.06 Ejemplo de asignación de clases para diferentes asignaciones

El servicio EF PHB se puede utilizar para transmisión de VoIP. El servicio PHB AF puede utilizarse por ejemplo, oro para aplicaciones interactivas, plata para Telnet y HTTP y bronce para FTP y SMTP.

CAPITULO III

MARCO METODOLÓGICO E HIPOTÉTICO

3.1 TIPO DE INVESTIGACION

Por la naturaleza de la investigación se considera que el tipo de estudio que se va a realizar es una investigación experimental y correlacional.

3.1.1 EXPERIMENTAL

Teniendo en cuenta que al variar condiciones de que influyen en el rendimiento de los protocolos expuestos a investigación, generaremos datos y variables experimentales no comprobadas, en condiciones rigurosamente controladas, a fin de definir parámetros de comportamiento frente a las condiciones expuestas a valoración en los protocolos en cuestión.

La investigación está ligada no solamente a establecer una comparación entre conceptos de funcionamiento, sino a establecer parámetros de comparación reales, capaces de demostrar de una manera clara el protocolo que presente

mayor fiabilidad al afrontar las demandas de calidad requeridas en la transmisión de Video IP para un sistema de seguridad y vigilancia.

3.1.2 CORRELACIONAL

En este tipo de investigación se persigue fundamentalmente determinar el grado en el cual las variaciones en uno o varios factores son concomitantes con la variación en otro u otros factores.

Gracias a que nuestro estudio contempla la obtención de datos que permitan comparar los protocolos sometidos a estudio podemos realizar una correlación entre variable dependiente e independiente.

Mediante la manipulación de condiciones en los escenarios de prueba, que vendrían a ser el ancho de banda de la conexión y el tráfico en la red podremos valorar parámetros como son el retardo, jiter y la pérdida de paquetes podremos definir la calidad de la transmisión.

3.2 MÉTODOS DE INVESTIGACIÓN

Se utilizará para este proyecto los siguientes métodos de investigación:

Método Científico y de Observación: ya que mediante la implementación y análisis de un escenario de prueba se pretende estudiar y observar cambios en los rendimientos de los protocolos expuestos a estudio.

Método Inductivo: A través del cual se deducirá el protocolo que mejor se adapte al trabajo requerido por la implementación.

Método de Análisis: Ya que tendremos que considerar factores estrictamente necesarios al momento de realizar las pruebas.

Métodos Empírico, Experimental, Comparativo y Estadístico: Para complementar procesos que se ejecutarán dentro de la investigación, como es analizar estadísticamente los resultados de los diferentes escenarios para poder llegar a una conclusión mediante un método matemáticamente comprobado.

Se ha realizado las siguientes consideraciones para esta investigación:

- Se plantea la investigación en base a la problemática al momento de escoger un protocolo de QoS en la implementación de sistemas de seguridad y vigilancia basados en tecnologías IP.
- Se trazan los objetivos de la investigación que llevaran a comparar y escoger el protocolo idóneo para el tipo de implementación.
- Se justifica los motivos por los cuales se propone realizar la presente investigación.
- Se elabora un marco teórico que ayude a tener una idea general para la realización del trabajo y un horizonte más amplio.
- Se plantea una hipótesis la cual es una posible repuesta al problema planteado.
- Se propone la operacionalización de las variables en base a la hipótesis planteada.
- Se realiza la prueba de la hipótesis con los resultados obtenidos.
- Se elabora las conclusiones y recomendaciones producto de la investigación realizada.

3.3 SISTEMA DE HIPÓTESIS

La evaluación de protocolos QoS usados para la implementación sistemas de seguridad basados en tecnologías IP permitirá conocer a ciencia cierta el protocolo más robusto en el área del trabajo requerido.

3.3 OPERACIONALIZACION DE LAS VARIABLES

De acuerdo a la hipótesis planteada se han identificado dos variables:

Variable Independiente:

- Rendimiento de los protocolos en la transmisión de video IP.

Variable Dependiente:

- Calidad de Servicio en la transmisión de video IP.

3.3.1 OPERACIONALIZACIÓN CONCEPTUAL

VARIABLE	TIPO	DEFINICIÓN
Rendimiento en la transmisión de video IP.	Independiente	Cuantificación de la productividad de un cada uno de los protocolos sometidos a estudio.
Calidad de Servicio en la transmisión de video IP.	Dependiente	Parámetro requerido para la transmisión en diferentes tipos tráfico que, en el caso de tráfico de video asegura una recepción adecuada con retardos aceptables para el uso de la información.

Tabla III.01. Operacionalización Conceptual de las variables del proyecto

3.3.2 OPERACIONALIZACIÓN METODOLÓGICA

HIPÓTESIS	VARIABLES	INDICADORES	ÍNDICES	INSTRUMENTOS
La evaluación de protocolos QoS usados para la implementación sistemas de seguridad basados en tecnologías IP permitirá conocer a ciencia cierta el protocolo más robusto en el área del trabajo requerido.	**Variable Independiente** Rendimiento en la transmisión de video IP.	Paquetes transmitidos,	1. Número de paquetes Totales	Simulaciones Pruebas Analizador de Red, Observer
			2. Paquetes Perdidos	
		Velocidad en la transmisión o trafico Útil	3. Ancho de Banda	
		Tiempo de Transmisión	4. Retardo en la Transmisión	
			5. Jitter	
	Variable Dependiente Calidad de Servicio en la transmisión de video IP	Rendimiento IntServ	Comparación IntSer con BestEffort	Iniciativas Intuición Simulación Razonamiento
		Rendimiento DiffServ	Comparación DiffServ con BestEffort	

TABLA III.02. Operacionalización Metodológica de las variables del proyecto

3.4 POBLACIÓN Y MUESTRA

La población es el conjunto de todos los elementos a ser evaluados y en la presente investigación la conforman los Administradores de los sistemas de seguridad basado en tecnologías IP.

De esta población se seleccionó una muestra no probabilística, esta es un entorno de red Wan de prueba, que se implemento para tomar los datos necesarios para el desarrollo de este proyecto.

3.5 PROCEDIMIENTOS GENERALES

Se ha procedido a detallar los métodos utilizados en la presente investigación:

MÉTODO: Comparativo – experimental

TÉCNICAS: Experimentos y pruebas

INSTRUMENTOS: Analizador de Protocolos (wireshark)

3.6 INSTRUMENTOS Y HERRAMIENTAS

3.6.1 INSTRUMENTOS DE HARDWARE

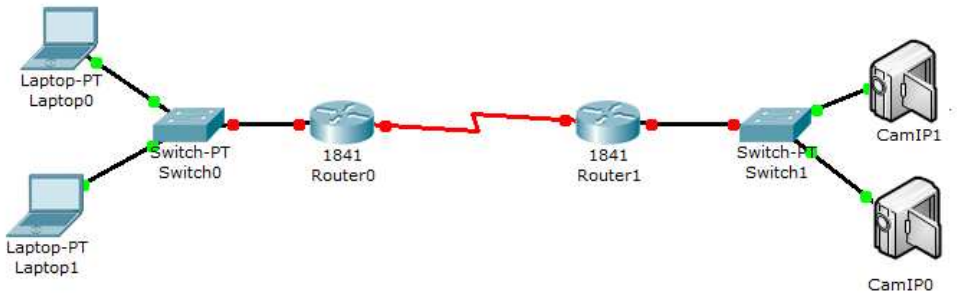


Figura III.1. Escenario de Pruebas (Hadware)

El esquema muestra el escenario para las pruebas compuesto por:

- Dos Routers Cisco 2800
- Dos Switchs Cisco

- Dos computadora
- Dos Cámaras IP

3.6.2 HERRAMIENTAS DE SOFTWARE

Plataforma de Equipos Cisco

- Router Cisco IOS 12.3
- Switch Cisco IOS 9.3

Analizadores de Paquetes

1. Wireshark

Clientes

- Mozilla Firefox
- FileZilla Cliente y Servidor

3.7 VALIDACION DE LOS INSTRUMENTOS

La validez de los instrumentos depende del grado en que se mide el dominio específico de las variables que intervienen en la investigación. Todo instrumento aplicado debe tener como característica fundamental: la validez y la confiabilidad. La validez se refiere al grado en que un instrumento realmente mide la variable que pretende medir.

Wireshark, antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos. Por su compatibilidad, y fácil de aprender y realizar rutinas sencillas el **Wireshark**, según el Foro Neoteo (http://www.neoteo.com/wireshark-analisis-de-protocolos-de-red-15483.neo).

Filezilla administrador de sitios: permite a un usuario crear una lista de sitios FTP con sus datos de conexión, como el número de puerto a usar, o si se utiliza inicio de sesión normal o anónima. Para el inicio normal, se guarda el usuario y, opcionalmente, la contraseña.(http://es.wikipedia.org/wiki/FileZilla)

CAPITULO IV.

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

La calidad requerida en la transmisión de video de un sistema de seguridad se puede estimar de acuerdo a parámetros establecidos como son el retardo, jitter, perdida de paquetes; la valoración de cada uno de estos parámetros en nuestros escenarios de prueba permitirá establecer esquemas de comparación fiables. En lo que refiere a la transmisión de video los retardos y perdida de paquetes deben de ser bajos, ya que, al existir con una mayor incidencia no podremos garantizar una transmisión que cumpla eficientemente con el propósito del sistema en sí, lo que en el caso de un sistema de seguridad implicaría una visualización oportuna de los acontecimientos ocurridos en el sitio.

En primera instancia se plantea la implementación de un entorno de prueba donde que simule una conexión típica de internet mediante dos routers Cisco

2850, los cuales proporcionaran los esquemas de ruteo necesarios en lo que a QoS refiere, trabajaran bajo la arquitectura BestEffort en el cual se variara la carga de trafico adicional en la red con el fin de valorar el cambio de los parámetros que definen una buena QoS, en la segunda parte de nuestro proceso de comparación se implementara una arquitectura QoS IntServs con la cual se valorara idénticamente los parámetros antes mencionados.

Por último se cambiara una vez más la arquitectura QoS, esta vez procederemos a usar DiffServs, seguida e idénticamente procederemos a valorar los parámetros mencionados con anterioridad en los escenarios anteriores.

4.1. PROCESAMIENTO DE LA INFORMACIÓN

En el proceso de estudio se realizaron varias pruebas en diferentes escenarios en los que podemos ver, a través de los indicadores de las variables dependiente e independiente la cuantificación del rendimiento de cada una de las arquitecturas implementadas.

Para la cuantificación de cada índice se utilizó un nivel de medición de valores que van bajando desde 100 % conforme los valores sigan bajando desde el valor máximo de acuerdo a la aplicabilidad de cada ámbito del índice.

Se asignó pesos a cada uno de los índices que conforman un indicador, resultando de esta manera una calificación total por cada experimento. Se calcula luego porcentaje promedio de los experimentos, para comparar con el porcentaje individual de la Propuesta de la Investigación. Posteriormente para cuantificar las variables dependiente e independiente, se procede a calcular la media ponderada de sus respectivos Indicadores, fijando ponderaciones repartidas equitativamente de porcentaje total por cada una de las variables.

Entonces para calcular el valor de una variable se la realizó utilizando la fórmula 1:

$$Variable = \sum_{i=1}^{n} Peso_i \, Indicador_i$$

Para propósitos de comparación se calculó las medias ponderadas de los indicadores tanto de la variable dependiente como de la variable independiente.

4.2. RESUMEN DE LOS EXPERIMENTOS

Dentro del estudio de calidad de servicio en la transmisión de video generado por un sistema de vigilancia, se realizo varios experimentos en los cuales se busco encontrar el protocolo más robusto, de acuerdo a la valoración de sus rendimientos.

Para el análisis de los protocolos en mención se realizo varios experimentos variando las condiciones de los ambientes de simulación. Estas pruebas, expuestas en los anexos de esta tesis nos ayudaran a determinar el protocolo que presente el mejor rendimiento para el trabajo destinado a estudio.

En la transmisión de video los aspectos de mayor importancia al momento de definir la calidad necesaria son: La pérdida de paquetes, el retardo en el transmisión y el jitter.

Para considerar el consumo de ancho de banda por diferentes tipos de tráfico en las redes de datos, para motivo de estudio, transmitiremos trafico FTP conjuntamente con el tráfico de video, con la finalidad de valorar el porcentualmente la mejora de QoS en cada uno de nuestros protocolos.

Al tener la necesidad de un parámetro de comparación, se realizo los siguientes experimentos previos. Se considero un enlace dedicado para la transmisión de video, es decir, un escenario en el cual no existe ningún otro tipo de trafico que no sea el generado por el sistema de seguridad. En un segundo escenario se valoro una red BestEffort(sin calidad de servicio) con trafico FTP.

Con estos experimentos previos, tenemos dos punto de valoración real, un rendimiento de un enlace dedicado, que sería lo óptimo en nuestro caso, y el escenario bombardeado de tráfico sin ningún tipo de calidad de servicio, lo que vendría a ser el caso de menor eficiencia.

4.2.1. AMBIENTE DE SIMULACIÓN

El ambiente de simulación implementado se muestra en la figuraIV.1. la implementación consiste de dos Routers Cisco xxx, un Switch Cisco xxx, dos Cámaras IP DLink DCS-920y dos Computadores portátiles.

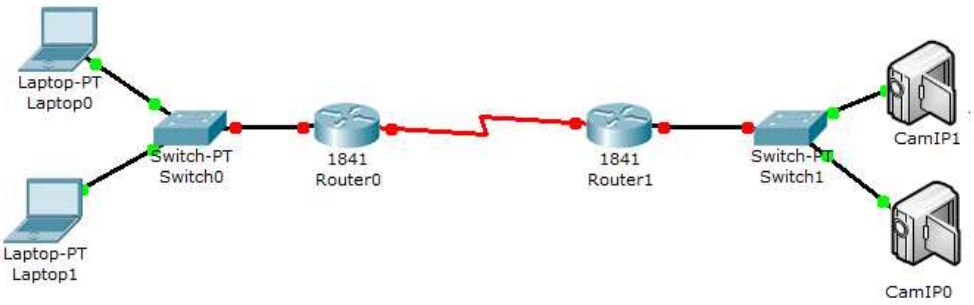


Figura IV.1. Esquema de ambiente de simulación

Cantidad	Equipo	Descripción
2	Router	Router Cisco xxx
1	Switch	Switch Cisco xxx
2	Camaras IP	Camara IP D-Link CSD-920
1	PC1	HP Pavillon dv6000
1	PC2	TOSHIBA Satellite A215

Tabla IV.1. Detalles Técnicos de los equipos del Ambiente de Simulación

En el ambiente de simulación mostrado en la Figura IV.1 se realizaron las pruebas de los diferentes escenarios con las variaciones de configuración de los Routers mencionadas a continuación:

En el ambiente de simulación 1, se configuro las interfaces de los routers y del mecanismo necesario para el ruteo entre los mismos. (Ver anexos 1)

En el ambiente de simulación 2, se configuro las interfaces de los routers y del mecanismo necesario para el ruteo entre los mismos y se configuro también InttServs. (Ver anexos 2)

En el ambiente de simulación 3, se configuro las interfaces de los routers y del mecanismo necesario para el ruteo entre los mismos y se configuro también DiffServs. (Ver anexos 3)

En la Tabla IV.2 se muestra el detalle de la función de cada equipo en el ambiente de simulación.

Equipo	**Descripción**
Router	Ruteo y mecanismos QoS.
Switch	Conexión LAN Cámaras IP.
Camaras IP	Captura y transmisión de video.
PC1	Servidor FTP, Cliente Cámaras IP, Analizador de Tramas.
PC2	Cliente FTP, Manager Cámaras IP.

Tabla IV.2. Detalles Técnicos del uso de cada equipo

4.2.2. RESULTADOS DEL AMBIENTE 1

En las pruebas realizadas en el ambiente de simulación 1 se obtuvieron dos parámetros importantes para la comparación:

El primero fue el de una transmisión de video a través de una red WAN simulada con un enlace dedicado, sin ninguna arquitectura QoS establecida.

El segundo, de una transmisión de video por una red WAN simulada, con tráfico existente y sin ninguna arquitectura QoS establecida.

Experimento 1, Escenario 1, Enlace Dedicado Cámaras IP

Paquetes Totales Transmitidos	Perdida de Paquetes	Ancho de Banda (bytes)	Retardo (segundos)	Jitter (mili segundos)
612	85	6750	116,87s	190,9ms

Tabla IV.3. Datos Obtenidos en escenario de enlace dedicado.

Experimento 2, Escenario 1, Trafico Cámaras IP+ Trafico FTP

Paquetes Totales Transmitidos	Perdida de Paquetes	Ancho de Banda (bytes)	Retardo (segundos)	Jitter (mili segundos)
399	115	3625	124.83s	312,8ms

Tabla IV.4. Datos obtenidos en escenario con trafico FTP

4.2.3. RESULTADOS DEL AMBIENTE 2

En el segundo ambiente de simulación se vario las condiciones en el tratamiento de la información de la siguiente manera. Se implemento una arquitectura IntServ reservando ancho de banda en la conexión para la transmisión de nuestro tráfico de video.

Escenario 2, Transmisión de Video arquitectura IntServ

Paquetes Totales Transmitidos	Perdida de Paquetes	Ancho de Banda (bytes)	Retardo (segundos)	Jitter (mili segundos)
423	103	4000	120.74s	285,4ms

Tabla IV.5. Datos obtenidos en Video Arquitectura IntServ

4.2.4. RESULTADOS DEL AMBIENTE 3

En el segundo ambiente de simulación se vario las condiciones en el tratamiento de la información de la siguiente manera. Se implemento una arquitectura DiffServ reservando ancho de banda en la conexión para la transmisión de nuestro tráfico de video.

Escenario 3, Transmisión de Video arquitectura DiffServ

Paquetes Totales Transmitidos	Perdida de Paquetes	Ancho de Banda (bytes)	Retardo (segundos)	Jitter (mili segundos)
400	93	5750	121,67s	304,19ms

Tabla IV.6. Datos obtenidos en Video Arquitectura DiffServ

4.3. ANÁLISIS DE LOS RESULTADOS DE LOS AMBIENTE DE SIMULACION

4.3.1 VARIABLE INDEPENDIENTE

Rendimiento en la transmisión de video IP.

INDICADOR 1: Paquetes transmitidos, con Best Effort sin tráfico en la red, Best Effort con tráfico en la red.

INDICE 1: Número de paquetes Totales

Tomando en cuenta que a mayor numero de paquetes enviados tendremos una pérdida considerable de más paquetes, un mayor consumo de ancho de banda. El mayor peso se lo dará al escenario con menor número de paquetes transmitidos.

Paquetes transmitidos		
	Cantidad	Porcentaje
BestEfort sin trafico	612	65,19%
BestEfort con trafico	399	100%

Tabla IV.7. Comparación de paquetes transmitidos en el ambiente 1

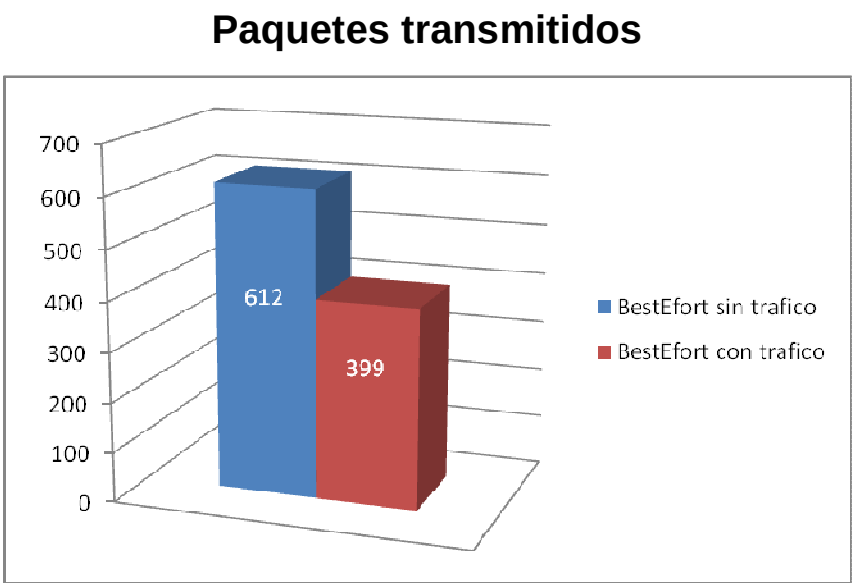


Figura. IV.2. Diagrama de comparación de paquetes transmitidos en el ambiente 1

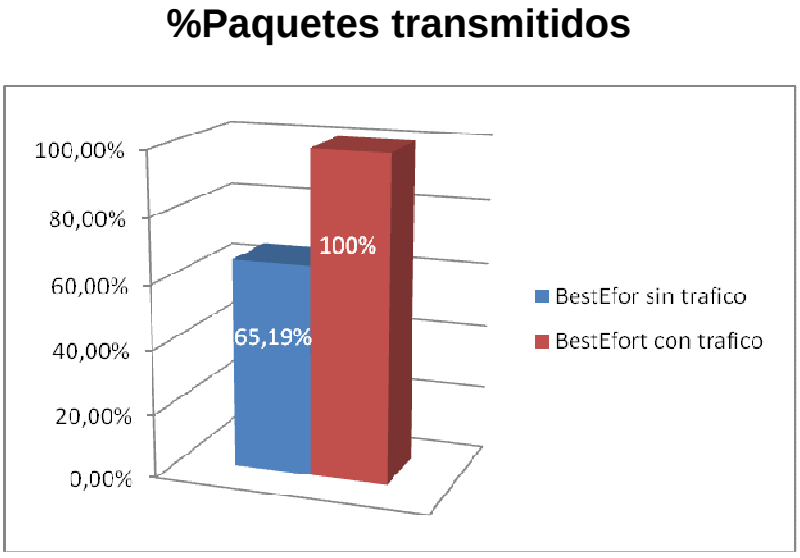


Figura. IV.3. Diagrama de porcentaje de pesos de paquetes transmitidos en el ambiente 1.

Interpretación:

Los paquetes transmitidos en cada uno de los escenarios de prueba, son un factor importante para el análisis, ya que entre menos paquetes se transmita la red se va a congestionar menos.

En el análisis puntual del indicador, observamos que el ambiente con mayor transmisión de paquetes es BestEfort sin tráfico, esto se debe a que el hecho de tener una red sin ningún otro trafico que no sea el de video, prácticamente tendremos un enlace dedicado para nuestro sistema de seguridad lo que conlleva a una transmisión mayor de paquetes.

INDICE 2: Paquetes Perdidos

En el análisis de este índice tomaremos en cuenta el porcentaje de paquetes perdidos por cada arquitectura implementada en relación con los enviados, ya que al tener una variación en la cantidad de paquetes transmitidos en cada uno de los escenarios no podemos considerar como mejor el escenario en el que menos paquetes se perdió.

Posteriormente para la construcción de nuestra tabla y diagrama de barras, otorgaremos el peso del 100% a la arquitectura que menor porcentaje de perdidas presento.

Paquetes Perdidos				
	Cantidad	Paquetes Perdidos	% Paquetes Perdidos	Porcentaje
BestEfort sin trafico	612	85	13,89%	100%
BestEfort con trafico	399	115	38,82%	28,19%

Tabla IV.8. Comparación de pérdida de paquetes en el ambiente 1

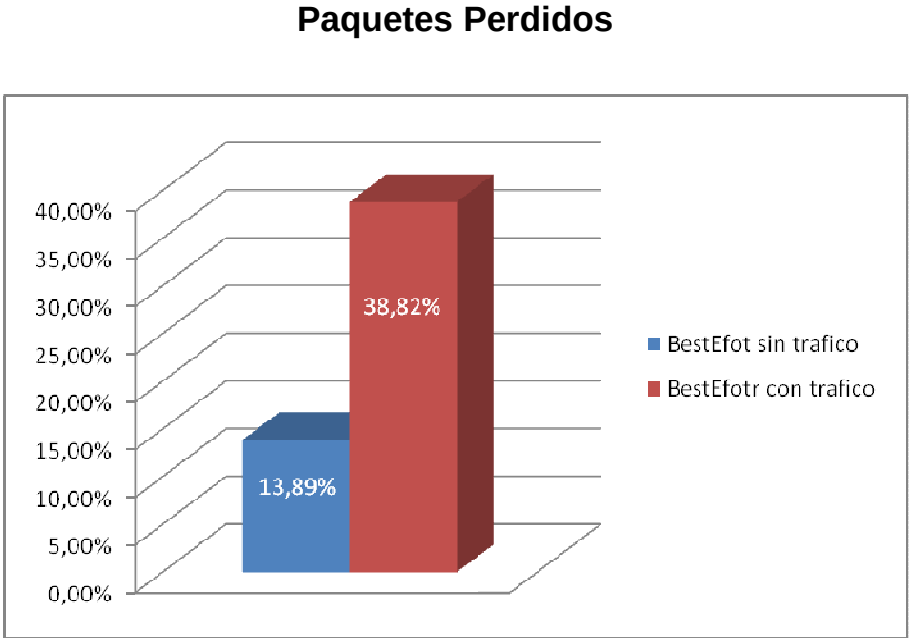


Figura. IV.4. Diagrama de comparación de porcentaje de pérdida paquetes en el ambiente 1

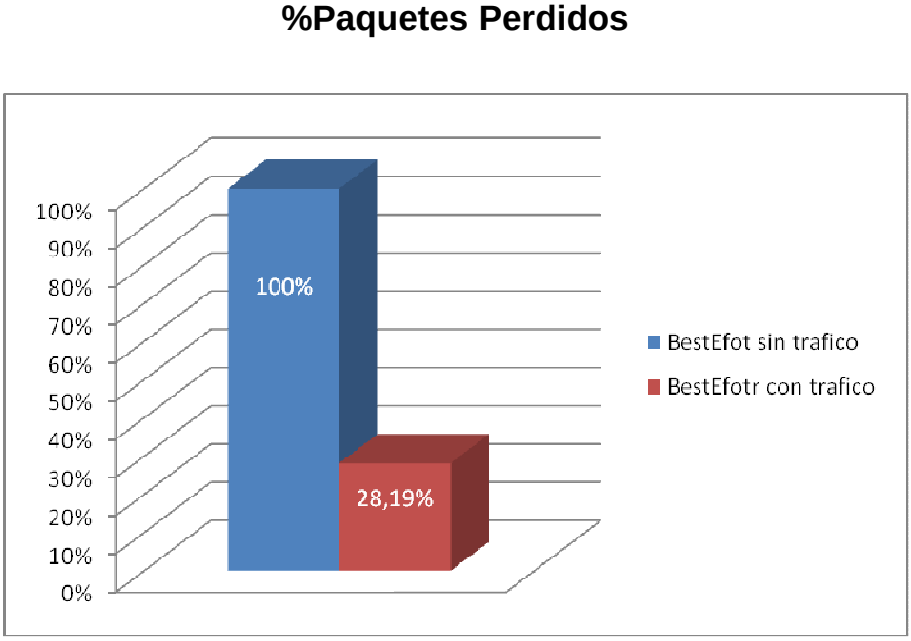


Figura. IV.5. Diagrama de porcentaje de pesos de pérdida de paquetes en el ambiente 1

Interpretación:

Al analizar la calidad de servicio un factor muy importante en la transmisión de video en tiempo real es la perdida de paquetes puesto que al tener una pérdida considerable el video será de baja calidad y poca fluidez.

Considerando puntualmente cada uno de los ambientes de simulación llegamos a las siguientes interpretaciones:

En el ambiente de simulación BestEfort sin tráfico, que representa un enlace dedicado para la transmisión del trafico en mención obtuvimos la menor perdida porcentual de paquetes en relación con el numero de paquetes recibidos.

En nuestro segundo experimento BestEfort con tráfico, pudimos observar que la perdida de paquetes fue la mayor obtenida en el estudio, puesto que al no presentar ninguna arquitectura de QoS no tenemos ninguna distinción en el trafico de nuestras cámaras con el resto del tráfico en la red. Lo que conlleva a una perdida porcentual considerable de datos.

INDICADOR 2: Velocidad en la transmisión

El ancho de banda definido para una determinada conexión a la red se reparte para gestionar las demandas de procesos existentes en la sub red. Esto se realiza según el proceso de encolamiento existente. Según la arquitectura que utilicemos en la red tendremos diferentes maneras de gestionar el espacio y tiempo en el ancho de banda disponible.

INDICE 3: Ancho de Banda

En el análisis del ancho de banda destinado al tráfico de video IP por cada una de las arquitecturas de red implementadas los resultados recogidos fueron los siguientes.

Ancho de Banda		
	Ancho de banda (Bytes)	Porcentaje
BestEfort sin trafico	6750	100,00%
BestEfort con trafico	3625	53,70%

Tabla IV.9. Comparación de ancho de banda en el ambiente 1

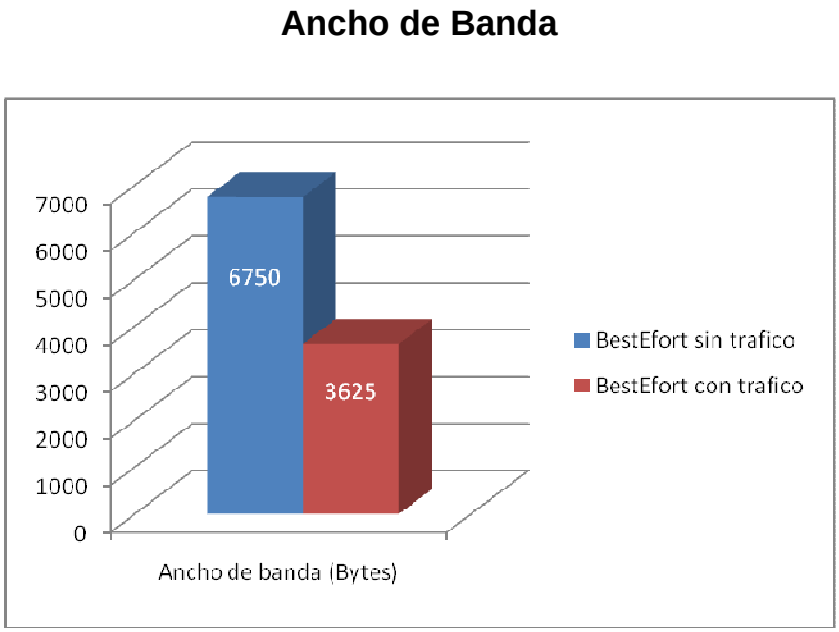


Figura. IV.6. Diagrama de comparación de ancho de banda en el ambiente 1

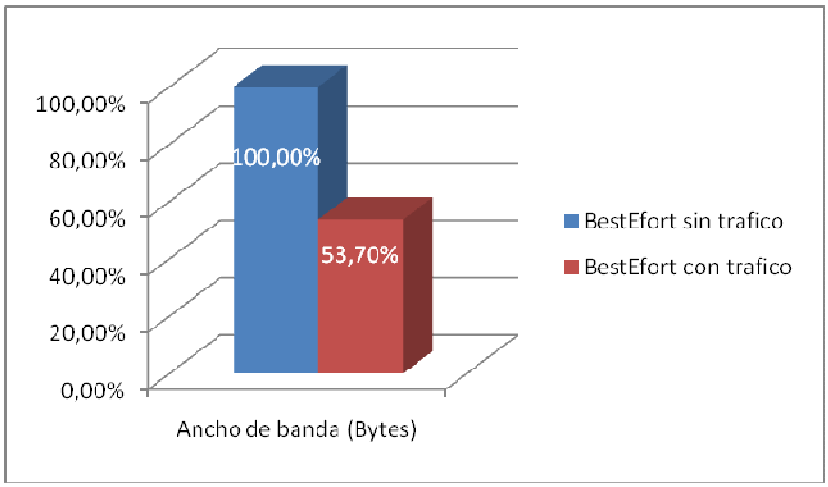


Figura. IV.7. Diagrama de porcentaje de ancho de banda en el ambiente 1

Interpretación:

El ancho de banda es un punto muy importante en lo que se refiere a calidad de servicio, puesto que al tener un ancho de banda amplio cada proceso podrá hacer uso de él sin mayor dificultad. En la actualidad la convergencia de servicios en el internet provoca que los anchos de banda de las redes sean insuficientes.

En esta parte del estudio observaremos la priorización que cada una de las arquitecturas presenta con el tráfico de Video IP.

Como era de esperarse nuestro escenario BestEfort sin tráfico obtuvo el mayor ancho de banda para el proceso, puesto que al no existir más tráfico en la red que el de Video IP el proceso puede disponer del ancho de banda de la red.

Por otra parte el escenario BestEfort con trafico otorgo el ancho de banda más bajo en los escenarios para el trafico de Video IP, puesto que al no tener ninguna distinción del resto del trafico fue tratado igual que el trafico que no necesita mayores condiciones de calidad.

INDICADOR 3: Tiempo de Transmisión.

El retardo depende de el tiempo en que se demora un paquete en transmitirse, este se mide en segundos; por lo que para este estudio se desea que el retardo sea el menor posible en la transmisión.

ÍNDICE 4: Retardo de la transmisión

En cuanto respecta a Retardo realizamos una relación en los escenarios del ambiente 1para construir la tabla IV.9 y el diagrama de la *figura IV.8 y la figura IV.9.* Cabe decir que el porcentaje fue calculado dándole un peso de 100% al número menor de retardo.

Retardo		
	Retardo (Segundos)	Porcentaje
BestEfort sin trafico	116,87	100,00%
BestEfort con trafico	174,83	48,62%

Tabla IV.10. Comparación de retardo en el ambiente 1

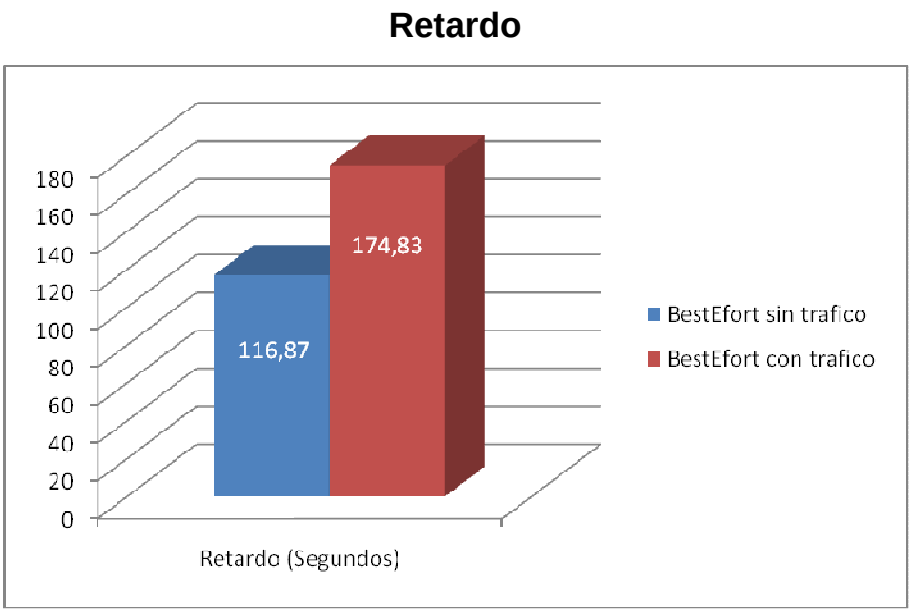


Figura. IV.8. Diagrama de comparación de retardo en el ambiente 1

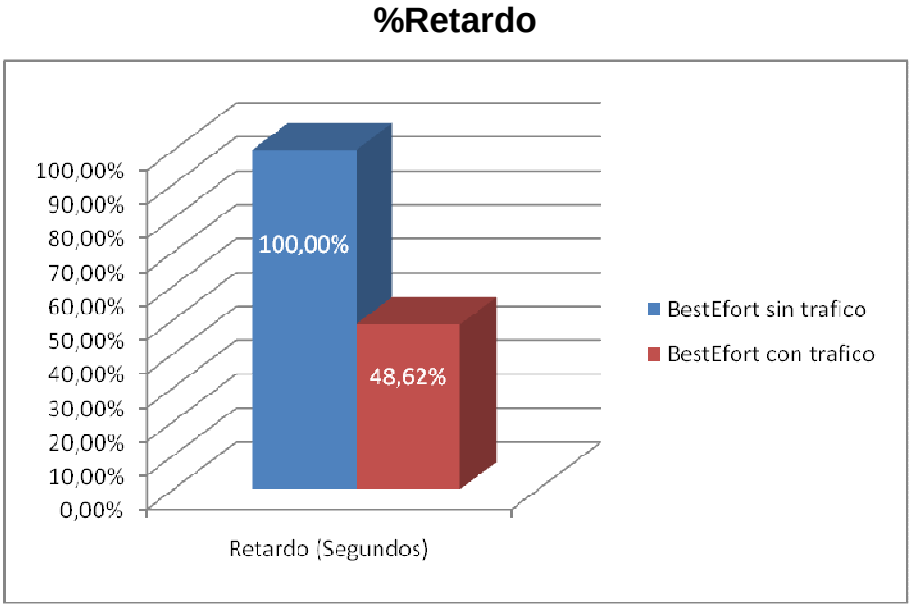


Figura. IV.9. Diagrama de porcentaje de retardo en el ambiente 1

Interpretación:

En lo que se refiere a las comunicaciones a tiempo real, el análisis del retardo es uno de los puntos más importantes, ya que al hacerlo podemos observar el tratamiento de los datos por cada arquitectura implementada.

Al obtener y analizar los datos obtenidos observamos datos que bien pudieron haber sido deducidos con facilidad, como el hecho de que un enlace dedicado para el trafico de Video Ip va a presentar mucho menos retardo en la trasmisión de los paquetes que el resto de nuestros escenarios.

Otro aspecto deducible fue que una red con tráfico sin ninguna arquitectura de QoS va a presentar un retardo considerable al momento de trasmitir nuestros datos.

ÍNDICE 5: Jitter

El jitter se considera el tiempo en que se demora un paquete en llegar a su destino, sabiendo esto lo que lo espera es tener menos jitter en la transmisión.

En cuanto respecta a Jitter se realizó una relación entre en el ambiente 1 para construir la tabla IV.10 y el diagrama de la *figura IV.10 y la figura IV.11*: Se puede mencionar que el porcentaje fue calculado dándole un peso de 100% al menor jitter existente en la transmisión.

Jitter		
	Jitter (ms)	Porcentaje
BestEfort sin trafico	190,9	100,00%
BestEfort con trafico	312,8	61,02%

Tabla IV.11. Comparación de jitter en el ambiente 1

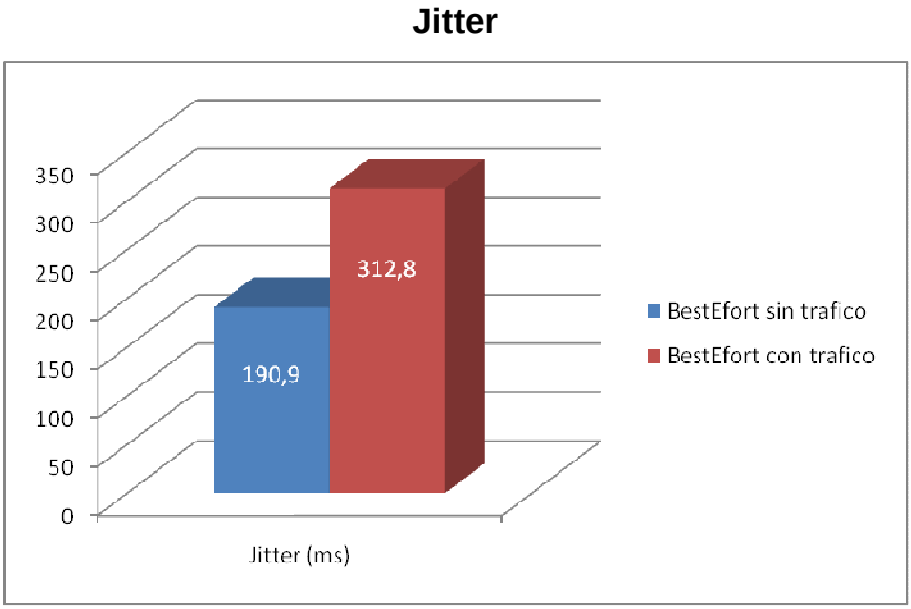


Figura IV.10. Diagrama de comparación de jitter en el ambiente 1.

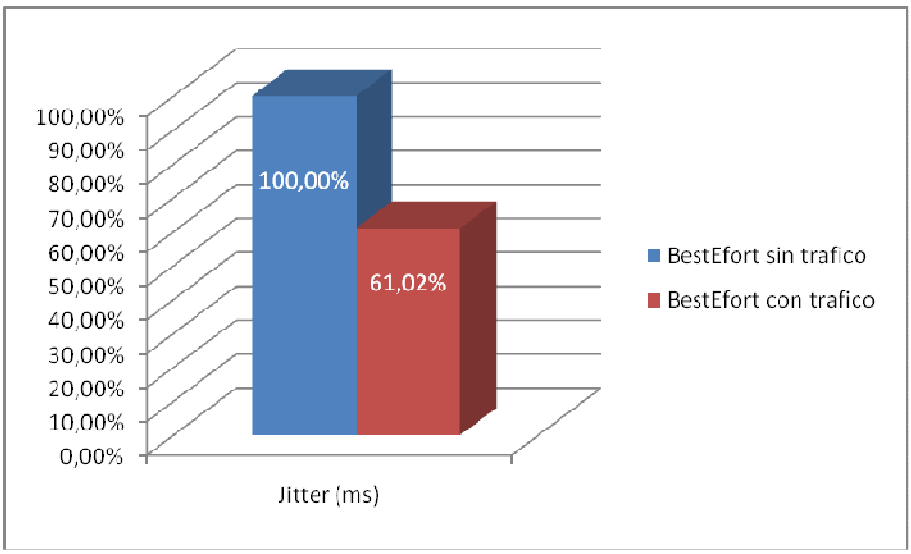


Figura IV.11. Diagrama de porcentaje de jitter en el ambiente 1

Interpretación:

En nuestro estudio para considerar una buena calidad en el servicio el Jitter debe ser el menor posible más aun si nos referimos a la calidad de un servicio de un proceso en tiempo real como lo es el Video IP.

Durante el proceso de investigación se considero al resto de tráfico como un parámetro que consume recursos de nuestra red alterando el desempeño del proceso. A continuación valoraremos los resultados obtenidos en cada de nuestros escenarios con la condiciones expuestas con anterioridad.

Tomando en cuenta que el Jitter está ligado al retardo podemos anticipar que los resultados de este indicador van a tener mucha relación con los obtenidos en la valoración del retardo. Con la variación de que la diferencia entre los valores recogidos en más sutil que en el indicador antes valorado, excluyendo al escenario BestEfort sin tráfico.

4.3.1. Variable Dependiente

Calidad de Servicio en la transmisión de video IP.

Para la valoración de las arquitecturas implementadas se comparara los datos obtenidos en los ambientes de simulación IntsServ y DiffServ con los datos obtenidos en el escenario BestEffort con y sin tráfico en la red, ya que el motivo de nuestra investigación encontrar la arquitectura con mayor mejora de calidad para un sistema de seguridad basados en tecnologías IP.

Para esto se dio los pesos a cada Indicador e Índice de valoración de acuerdo a los siguientes criterios.

Considerando que lo mas importante en una transmisión de Video IP es la fluidez de las imágenes se considero darle un peso mayor al Tiempo de Transmisión, en el cual el Jitter será el índice que mayor porcentaje presente en la obtención del rendimiento, ya que en explícitamente se considera también la cantidad de paquetes enviados en la transmisión.

El segundo indicador en orden de importancia será Los Paquetes Transmitidos y por último el ancho de banda, ya que el principal objetivo de una red implementada con alguna arquitectura QoS es mejorar la calidad sin la necesidad de cambiar la red física para obtener un mayor ancho de banda. Los pesos de los Indicadores e Índices se expresan en la Tabla IV.11

Pesos de los Indicadores e Índices			
Indicador	Peso	Índice	Peso
Paquetes Trasmitidos	30	Total Paquetes Transmitidos	10
		Paquetes Perdidos	20
Velocidad de Trasmisión	20	Ancho de banda	20
Tiempo de Trasmisión	50	Retardo en la transmisión	20
		Jitter	30

Tabla IV.12 Pesos Indicadores e Indices para la valoración del rendimiento

INDICADOR 1: Rendimiento Intserv

ÍNDICE: Comparación con BestEfort

Para realizar el estudio del rendimiento del protocolo realizaremos una comparación con el escenario BestEfort en sus dos condiciones:

Sin tráfico en la red, que vendría a ser la mejor condición de transmisión puesto que representara un enlace dedicado para nuestro sistema de seguridad y con tráfico en la red el cual será nuestro punto de partida para la valoración del rendimiento del protocolo.

Con la finalidad de obtener un resultado más significativo relazaremos el cálculo del porcentaje de rendimiento con el mejor de los casos es vendría a ser BestEfort sin tráfico en la red.

Con los datos obtenidos de los escenarios 1y 2 realizamos las siguientes tablas comparativas.

Valoración del rendimiento BestEffort sin tráfico en la red				
Indicador	Índice	% de Valoración	Peso	Sub Total
Paquetes Trasmitidos	Total Paquetes Transmitidos	65,19%	10	6,519
	Paquetes Perdidos	100%	20	20
Velocidad de Trasmisión	Ancho de banda	100%	20	20
Tiempo de Trasmisión	Retardo en la transmisión	100%	20	20
	Jitter	100%	30	30
Total			100	96,519

Tabla IV.13 valoración del rendimiento BestEffort sin tráfico en la red

Valoración del rendimiento BestEffort con tráfico en la red				
Indicador	Índice	% de Valoración	Peso	Sub Total
Paquetes Trasmitidos	Total Paquetes Transmitidos	100,00%	10	10
	Paquetes Perdidos	28%	20	5,638
Velocidad de Transmisión	Ancho de banda	54%	20	10,74
Tiempo de Transmisión	Retardo en la transmisión	48%	20	9,724
	Jitter	61%	30	18,306
Total			100	54,408

Tabla IV.14 Valoración del rendimiento BestEffort con tráfico en la red

Valoración del rendimiento IntServ				
Indicador	Índice	% de Valoración	Peso	Sub Total
Paquetes Trasmitidos	Total Paquetes Transmitidos	94,32%	10	9,432
	Paquetes Perdidos	57%	20	11,408
Velocidad de Transmisión	Ancho de banda	59%	20	11,85
Tiempo de Transmisión	Retardo en la transmisión	97%	20	19,358
	Jitter	67%	30	20,064
Total			100	72,112

Tabla IV.15 Valoración del rendimiento IntServ

La Tabla IV.16 muestra los resultados obtenidos para la comparación del escenario IntServ

Comparación del Rendimiento IntServ	
Arquitectura	Puntuación
BestEfort sin trafico	96,519
BestEfort con trafico	54,408
IntServ	72,112

Tabla IV.16 Comparación del Rendimiento IntServ

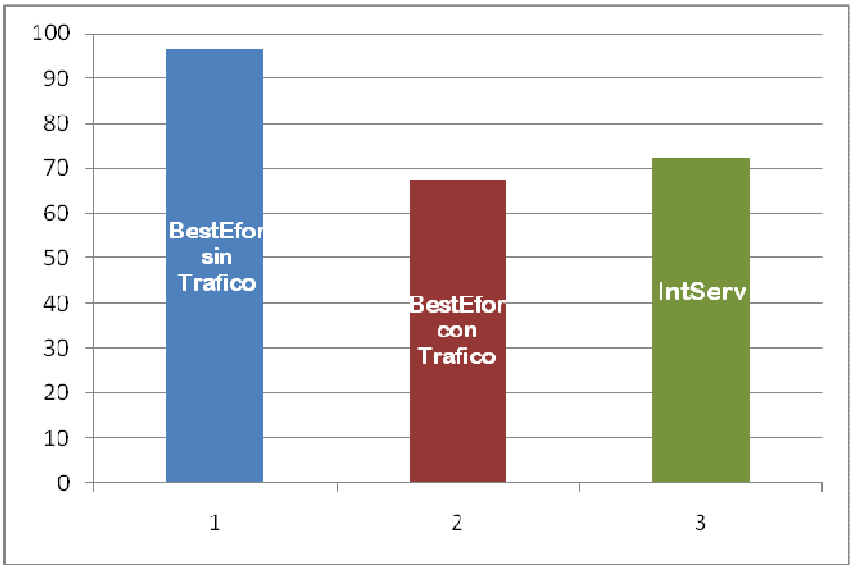


Figura IV.12 Comparación rendimiento IntServ

INDICADOR 2: Rendimiento DiffServ

ÍNDICE: Comparación con BestEfort

La tabla IV.17 muestra la valoración de rendimiento del protocolo DiffServ

Valoración del rendimiento DiffServ				
Indicador	Índice	% de Valoración	Peso	Sub Total
Paquetes Trasmitidos	Total Paquetes Transmitidos	99,75%	10	9,975
	Paquetes Perdidos	60%	20	11,948
Velocidad de Transmisión	Ancho de banda	85%	20	17,036
Tiempo de Transmisión	Retardo en la transmisión	96%	20	19,21
	Jitter	63%	30	18,825
Total			100	76,994

Tabla IV.17 Valoración del rendimiento DiffServ

Comparación del Rendidito IntServ	
Arquitectura	Puntuación
BestEfort sin trafico	96,519
BestEfort con trafico	54,408
DiffServ	76,994

Tabla IV.18 Comparación del Rendidito IntServ

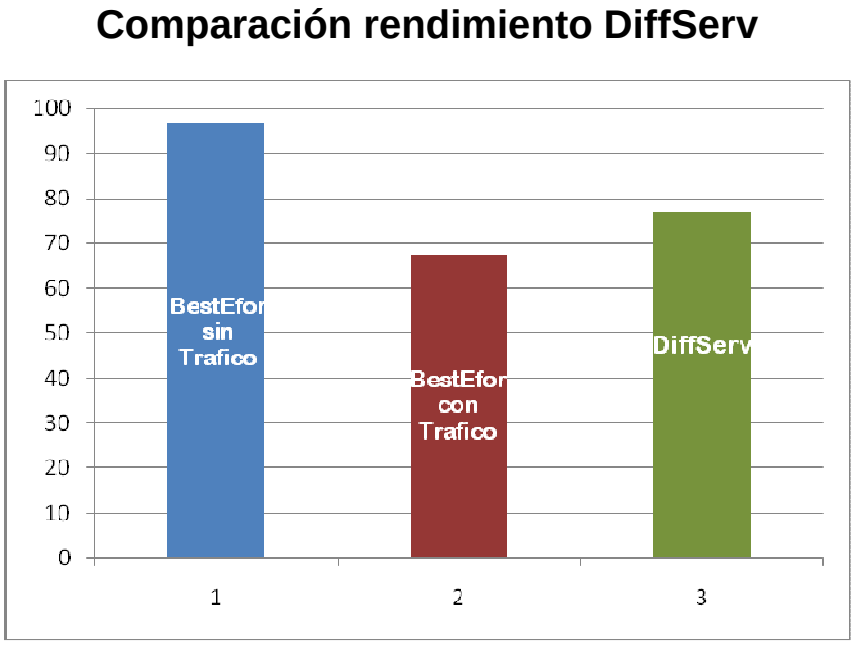


Figura IV.13 Comparación rendimiento DiffServ

4.4. RESUMEN DE LOS PESOS OBTENIDOS PARA INDICADORES DE LA VARIABLE INDEPENDIENTE

Pesos Obtenidos para indicadores de la Variable Independiente					
Arquitecturas	Paquetes Totales	Perdida de paquetes	Ancho de Banda	Retardo de transmisión	Jitter
BestEfor sin trafico	65,19%	100,00%	100,00%	100,00%	100,00%
BestEfor con trafico	100,00%	28,20%	53,70%	48,06%	61,02%

TABLA IV.19. Pesos de los indicadores de la variable Independiente

4.5. RESUMEN DE LAS EQUIVALENCIAS DE LOS PESOS OBTENIDOS PARA INDICADORES DE LA VARIABLE DEPENDIENTE

Pesos de los Indicadores e Índices						
Indicador	**Índice**	**Peso**	**IntSer**	**Sub Total**	**DiffServ**	**Sub Total**
Paquetes Trasmitidos	Total Paquetes Transmitidos	10	94,32%	9,432	99,75%	9,975
	Paquetes Perdidos	20	57%	11,408	60%	11,948
Velocidad de Transmisión	Ancho de banda	20	59%	11,85	85%	17,036
Tiempo de Transmisión	Retardo en la transmisión	20	97%	19,358	96%	19,21
	Jitter	30	67%	20,064	63%	18,825
Total				72,112		76,994

TABLA IV.20. Pesos de los indicadores de la variable dependiente

4.6. ANÁLISIS DE RESULTADOS

4.6.1. VARIABLE INDEPENDIENTE

Tomando en cuenta que cada indicador tiene su peso entonces se desglosa cada uno de los promedios de los indicadores.

Pesos de los Indicadores e Índices		
Indicador	BestEfort con trafico	BestEfort sin trafico
Paquetes Trasmitidos (30)	15,64	26,52
Velocidad de Trasmisión (20)	10,74	20
Tiempo de Trasmisión (50)	28,03	50

TABLA IV.21. Análisis de Resultados para la Variable Independiente: Total Indicadores

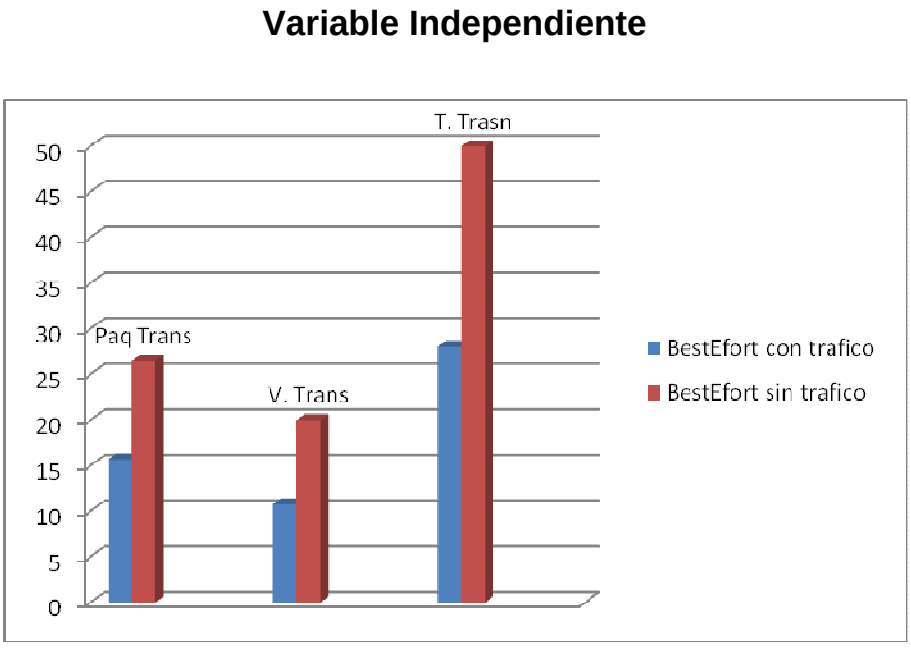


Figura. IV.14. Diagrama de Barras de los resultados de la Variable Independiente

Para saber el porcentaje de mejora entre IntServ y BestEfort se calculo la variabilidad de la siguiente manera:

V.I. (BestEfort con tráfico) = 15.64 + 10,74 + 28,03 = 54,41%

V.I (BestEfort sin tráfico) = 26,52 + 20 + 50 = 96,52%

Variabilidad = V.I. (BestEfort sin tráfico) – V.I. (BestEfort con tráfico)

Variabilidad = 96,52% - 54,41% = 42,11%

Variabilidad = 42,11%

Interpretación:

Claramente se puede apreciar la pérdida de calidad de un canal congestionado con tráfico diferente al de estudio en relación con uno dedicado para la transmisión de Video IP.

Con el presente trabajo lo que se desea es conocer el protocolo que mejore rendimiento tenga en el trabajo de mejorar una trasmisión.

4.6.2. VARIABLE DEPENDIENTE

Tomando en cuenta que cada indicador tiene su peso entonces se desglosa cada uno de los promedios de los indicadores.

Pesos de los Indicadores e Índices				
Indicador	BestEfort sin trafico	BestEfort con trafico	IntSer	DiffServ
Paquetes Trasmitidos (30)	26,52	15,64	20,84	21,92
Velocidad de Trasmisión (20)	20	10,74	11,85	17,04
Tiempo de Trasmisión (50)	50	28,03	39,42	38,03

TABLA IV.22. Análisis de Resultados para la Variable Dependiente: Total Indicadores

Variable Dependiente IntServ

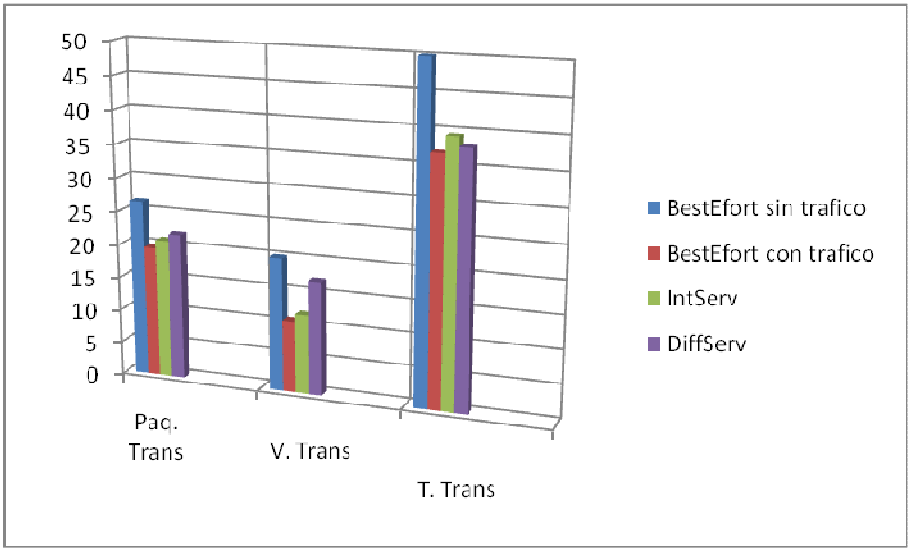


Figura. IV.15. Diagrama de Barras de los resultados de la Variable Dependiente

V.D. (BestEfort sin trafico) = 26,52 + 20 + 50 = 96,52%

V.D. (BestEfort con trafico) = 15.64 + 10,74 + 28,03 = 54,41%

V.D. (IntServ) = 20,84 + 11,85 + 39,42 = 72,11%

V.I (DiffServ) = 21,92 + 17,04 + 38,03 = 76,99%

Variabilidad IntServ = V.D. (DiffServ) – V.D. (BestEfort con trafico)

Variabilidad IntServ = 54,41% - 72,11%

Variabilidad IntServ = 17,7%

Variabilidad DiffServ= V.D. (DiffServ) – V.D. (BestEfort con trafico)

Variabilidad DiffServ = 54,41% - 76,99%

Variabilidad DiffServ = 22,58%

Interpretación:

Se concluye que las transmisión de Video IP con DiffServ, mejoran la calidad de la transmisiones en un 22.58%; mientras que IntServ mejora en un 17,7% siendo así DiffServ en el que mayor rendimiento presento en el estudio.

4.7. PRUEBA DE LA HIPÓTESIS

Las hipótesis científicas son sometidas a prueba para determinar si son apoyadas o refutadas de acuerdo con lo que el investigador observa, ahora bien, en realidad no podemos probar que una hipótesis sea verdadera o falsa, sino argumentar que fue apoyada o no, con ciertos datos obtenidos en la investigación.

Por lo tanto no existe un método que permita saber con seguridad que una desviación es el resultado exclusivo del azar, sin embargo hay pruebas estadísticas que permiten determinar algunos límites de confianza. Una de estas es la prueba del **Chi-cuadrado** que permite calcular la probabilidad de obtener resultados que únicamente por efecto del azar se desvíen de las expectativas en la magnitud observada si la solución a un problema es correcta.

Para realizar la prueba el primer paso es calcular el valor del Chi-cuadrado el cual responde a la siguiente fórmula:

$$X^2 = \sum \frac{(O-E)^2}{E}$$

Donde:

O = el número observado de una clase particular.

E = el número esperado de esta clase.

El siguiente paso es determinar los grados de libertad, que son el número de categorías o clases que existe. Generalmente esto es igual a uno menos el número total de clases o indicadores. El paso final en la aplicación de la prueba del Chi-cuadrado es buscar el valor de Chi-cuadrado calculado y los grados de

libertad en una tabla o gráfica que se presenta en el Anexo 37 y determinar el valor de la probabilidad. Este valor es la probabilidad de que el azar por sí mismo pudiera ser responsable de una desviación tan grande o mayor que la observado, si la hipótesis es correcta. Si la probabilidad es alta se considera que los datos están de acuerdo con la solución, lo cual no prueba que la solución sea correcta, sino que simplemente no se puede demostrar que sea incorrecta. Si la probabilidad es baja, se considera que los datos no respaldan a la propuesta de solución.

Generalmente el nivel de confiabilidad es de 5%, si la probabilidad es menor de 0.05, la diferencia es significativa y si es menor a 0.01 esta es considerada altamente significativa. Las probabilidades en estos intervalos generalmente causan el rechazo de una propuesta.

Utilizando la prueba del Chi-cuadrado en nuestra investigación se construye la tabla IV.22, utilizando los valores de los indicadores de la variable independiente los cuales fueron obtenidos en los ambientes realizados en la muestra especificada, esto es en la red de simulación.

CLASES	F. Obs.	F.Esp.	(E-O)^2	(E-O)^2/F
Paquetes transmitidos	15.64	21,92	39,44	1,8
Velocidad en la transmisión	10,74	17,04	39,69	2,32
Tiempo de Transmisión	28,03	38,03	100	2,63
			Chi-cuadrado:	6,75

TABLA IV.23. Prueba de la Hipótesis, valores del test de Chi-cuadrado

Donde tenemos que él **Chi-Cuadrado = 6,75**

Para los grados de libertad tenemos:

$$gl= (fila-1)(columna-1)$$

$$gl= (3-1)\ (2-1)$$

gl = 2

El siguiente paso es fijar un nivel de significación, que como se mencionó es de 0.05 y construir el valor crítico $X^2$1-α.

Entonces tenemos que el valor crítico del chi-cuadrado para un nivel de significación de 0,05 y con 2grados de libertad es se denota $\chi^2_{0.05}(2) = 5{,}99$.

Para α =0.005 es de 10,6. Como quiera que en el cálculo del χ 2 en nuestro estudio obtuvimos un valor de 6,75, que supera al valor para α=0.005, podremos concluir que las dos variables no son independientes, sino que están asociadas.

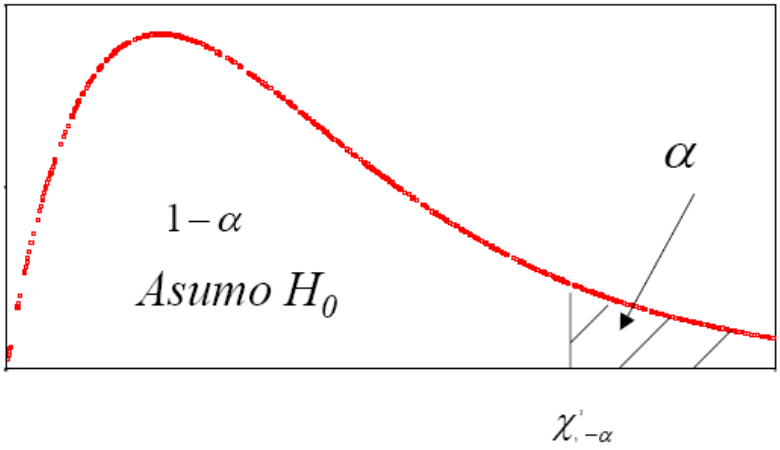


Figura. IV.16. Diagrama de fijación del nivel de significación

Por lo tanto, a la vista de los resultados, rechazamos la hipótesis nula (H_0) y aceptamos la hipótesis alternativa (H_α), en este caso nuestra hipótesis planteada como probablemente cierta.

CAPITULO V

MARCO PROPOSITIVO

5.1. ALTERNATIVAS DE SOLUCIÓN

Dado que distintas aplicaciones como, por ejemplo, teléfono, correo electrónico y video vigilancia, pueden utilizar la misma red IP, es necesario controlar el uso compartido de los recursos de la red para satisfacer los requisitos de cada servicio. Una solución es hacer que los enrutadores y los conmutadores de red funcionen de maneras distintas para cada tipo de servicio (voz, datos y vídeo) del tráfico de la red. Al utilizar la Calidad de servicio (QoS), distintas aplicaciones de red pueden coexistir en la misma red sin consumir cada una el ancho de banda de las otras.

El término Calidad de servicio hace referencia a una cantidad de tecnologías, como DSCP (Differentiated Service Codepoint), que pueden identificar el tipo de

datos que contiene un paquete y dividir los paquetes en clases de tráfico para priorizar su reenvío. Las ventajas principales de una red sensible a la QoS son la priorización del tráfico para permitir que flujos importantes se gestionen antes que flujos con menor prioridad, y una mayor fiabilidad de la red, ya que se controla la cantidad de ancho de banda que puede utilizar cada aplicación y, por lo tanto, la competencia entre aplicaciones en el uso del ancho de banda. El tráfico, que se considera crítico y requiere una latencia baja, es un caso típico en el que la QoS puede garantizar respuestas rápidas a solicitudes de movimiento.

- **SERVICIO DE MEJOR ESFUERZO.**

Se le llama servicio de mejor esfuerzo al que la red provee cuando hace todo lo posible para intentar entregar el paquete a su destino, donde no hay garantía de que esto ocurra. Una aplicación enviará datos en cualquier cantidad, cuando lo necesite, sin pedir permiso o notificar a la red. Éste es el modelo utilizado por las aplicaciones de Ftp y Http. Obviamente, no es el modelo apropiado para aplicaciones sensibles al retardo o variaciones de ancho de banda, las cuales necesitan de un tratamiento especial.

- **SERVICIOS INTEGRADOS: INTSERV**

IntServ es una estructura para definir servicios, por lo que contiene un conjunto de mecanismos de control de tráfico subyacentes. Los servicios IntServ se suelen aplicar por conversación individual. Generalmente, se asocia con el Protocolo de Reserva de Recursos (RSVP, Resource ReServation Protocol)

Con este modelo de trabajo se pretende ofrecer soporte para un funcionamiento adecuado de aplicaciones con requisitos de tiempo real.

Como ya hemos descrito el modelo Intserv implica una reserva individual de recursos por cada flujo de información. La gran cantidad de usuarios que componen una red, así como el elevado número de flujos que puede generar cada usuario provoca que existan graves problemas de escalabilidad en el núcleo de la red. Estos factores provocan que el modelo Intserv sea difícilmente implementable en una red de dimensiones considerables.

Por otro lado las propiedades intrínsecas de las redes inalámbricas, caracterizadas principalmente por la dependencia de un medio especialmente

variable, provocan que un modelo como el propuesto por servicios integrados no resulte adecuado.

- **SERVICIOS DIFERENCIADOS: DIFFSERV**

Es un mecanismo de tratamiento de tráfico por acumulación, adecuado para redes enrutadas. Define el campo DSCP (DiffServ Codepoint) en los encabezados IP, los dispositivos que envían tráfico a una red Diffserv marcan con el mismo valor DSCP a los paquetes de flujos con similares requisitos de QoS, al agregar el flujo a una cola común o al programar el comportamiento. Los routeadores utilizan DSCP para clasificar paquetes y aplicar un comportamiento de cola específico según los resultados de la clasificación.

El modelo de servicios diferenciados propone una solución para el soporte de calidad de servicio basado en la priorización de clases de tráfico. Al igual que el modelo de servicios integrados, la provisión de calidad de servicio se realiza a través de una reserva de recursos en los nodos intermedios, pero en este caso las pre-reservas se realizan por agregados de tráfico, en lugar de por flujos.

Esta pre-reserva de recursos es una labor de la administración de la red, es decir, las aplicaciones no realizan ninguna petición de recursos. Simplemente deberán marcar el tráfico que generen adecuadamente para que reciba un tratamiento específico en función de la clase a la que pertenezca.

5.2. EVALUACIÓN DE LAS ALTERNATIVAS

Concluido el estudio en el que se analizo las alternativas, se recogió datos se estudio de cada una de las alternativas de solución; se decidió implementar para nuestro estudio la alternativa de servicios diferenciados o priorización de tráfico.

Tomando en cuenta que IntServ los resultados obtenidos en el estudio que muestra un claro mejor desempeño de DiffServ frente a la mejora de la calidad en la transmisión de Video IP. A mas de esto se considero que IntServ no presenta la suficiente escalabilidad para la red, ya que al reservar un ancho de banda determinado para uno u otro proceso implica que frente a un crecimiento de nuestro sistema de seguridad IntServ dividirá el ancho de banda reservado para

este proceso para el numero de cámaras existente. Lo que conlleva a una degradación de la calidad en el servicio.

Por las razones expuestas con anterioridad se escogió como la mejor arquitectura de calidad de servicio para la trasmisión de video IP al modelo DiffServ el cual se implemento en los routers como se indica en el siguiente punto del presente trabajo de tesis.

5.3. IMPLEMENTACIÓN DE LA SOLUCIÓN

A continuación procederemos a describir uno a uno los pasos necesarios para la implementación de la arquitectura que obtuvo el mejor rendimiento en el estudio.

5.3.1 DISEÑO DEL ESCENARIO

El diseño se considera como un enlace punto punto de una red WAN.

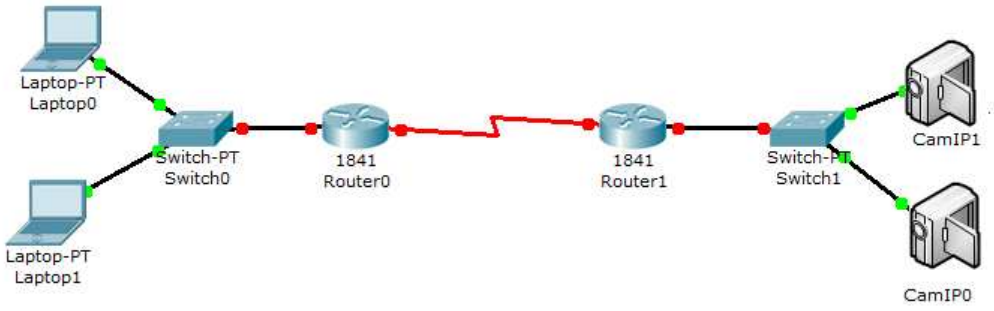


FIGURA V.1. Diseño del escenario

DIRECIONAMIETO IP ROUTERS				
	Interface Serial 0/0/0		Interface FastEthernet	
	IP Address	SubNet Mask	IP Address	SubNet Mask
Router 1	192.168.1.2	255.255.255.0	192.168.2.1	255.255.255.0
Router 2	192.168.1.3	255.255.255.0	192.168.3.1	255.255.255.0

TABLA V.1 Direccionamiento de las dispositivos capa 3

DIRECCIONAMIENTO IP PERIFERICOS FINALES			
	Interface FastEthernet		Default GateWay
	IP Address	SubNet Mask	IP Address
Pc 1	192.168.2.3	255.255.255.0	192.168.2.1
Pc 2	192.168.2.4	255.255.255.0	192.168.2.1
Cam IP1	192.168.3.3	255.255.255.1	192.168.3.1
Cam IP2	192.168.3.4	255.255.255.2	192.168.3.1

TABLA V.2 Direccionamiento dispositivos finales

5.3.2. COMANDOS DE CONFIGURACIÓN

CONFIGURACIÓN DE LAS INTERFACES

a. Configuración del Router1

Router> enable
Router# configure terminal
Router(config)# hostname R1
R1(config-if)# interface fast-ethernet 0/0
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ip address 192.168.1.2 255.255.255.0
R1(config-if)# clock rate 36000
R1(config-if)# no shutdown
R1(config-if)# exit

b. Configuración del Router1

Router> enable
Router# configure terminal
Router(config)# hostname R2
R2(config-if)# interface fast-ethernet 0/0
R2(config-if)# ip address 192.168.3.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# interface serial 0/0/0
R2(config-if)# ip address 192.168.1.3 255.255.255.0

R2(config-if)# no shutdown

R2(config-if)# exit

CONFIGURACIÓN DEL PARÁMETRO DE RUTEO

a. Configuración R1

R1#configure terminal

R1(config)# router rip

R1(config-router)# network 192.168.1.0

R1(config-router)# network 192.168.2.0

R1(config-router)# CTRL+Z

b. Configuración R2

R2#configure terminal

R2(config)# router rip

R2(config-router)# network 192.168.1.0

R2(config-router)# network 192.168.3.0

R2(config-router)# CTRL+Z

CONFIGURACIÓN DIFFSERV

Configuración R1

R1(config)#interface serial 0/0

R1(config-if)#random-detect

R1(config)#interface serial 0/0

R1(config-if)#random-detect exponential-weighting-constant 10

CONCLUSIONES

Al momento de realizar un tipo de proceso en el que se requiera una trasmisión a tiempo real, como puede ser la trasmisión de de video IP, la calidad en el servicio es el parámetro más importante a tomar en cuenta.

Si bien es cierto un gran ancho de banda puede garantizar una trasmisión de calidad. Pero al saturarse este, se necesitara un ancho de banda mayor, lo que implicaría una necesidad de alguna Arquitectura que brinde a la red la calidad en el servicio requerida.

La arquitectura de calidad de servicio DiffServ presenta mayor escalabilidad que IntServ puesto que la reserva en el ancho de banda puede brindar una buena calidad en la trasmisión para un número determinado de procesos, ya que al saturar el ancho de banda reservado se tendrá problemas de calidad incluso mayores a los que existía previo a la implementación de la solución.

La convergencia de la tecnología a las redes, produce un incremento importante en la necesidad de anchos de banda capases de otorgar las condiciones necesarias para todos los requerimientos, lo que ha producido que cada vez se vuelva más importante y primordial la implementación de arquitecturas de calidad de servicio.

IntServ es una excelente opción para las redes que no esperen un crecimiento abrupto del tráfico de las mismas. Ya que al delimitar ancho de banda para un determinado tráfico o porción de la red garantiza el un comunicación con calidad.

RECOMENDACIONES

Se debe realizar una correcta valoración de dispositivos y software necesario para la implementación de los escenarios de prueba, ya que de ellos dependerá la fiabilidad de los resultados obtenidos en los estudios.

Al momento de seleccionar el dispositivo de ruteo para la implementación se debe tomar en cuenta el tipo de IOS que soporta ya que existen IOS que no soportan implementaciones de Calidad de Servicio.

Se recomienda la utilización de herramientas comunes de análisis de tráfico tal como Wireshark ya que permite analizar en detalle los campos de los paquetes y presenta una interface grafica amigable con el usuario.

Previo a la implementación de una arquitectura QoS, definir claramente el tipo de tráfico al que se desea dar prioridad, el tipo de priorización sin llegar a desvalorizar el resto del tráfico en la red.

Tomar muy en cuenta el crecimiento esperado de la red para la implementación de una arquitectura QoS, puesto que un cambio de arquitectura en una etapa avanzada de la vida útil de la red, podría inquirir en gastos innecesarios.

RESUMEN

El presente trabajo titulado “ANALISIS COMPARATIVO DE PROTOCOLOS QoS USADOS EN LA IMPLEMENTACIÓN DE SISTEMAS DE SEGURIDAD Y VIGILANCIA BASADOS EN TECNOLOGIAS IP: CASO PRACTICO DESITEL” esta enfocado a valorar los rendimientos de las arquitecturas IntServ y DiffServ usados para la mejora de la calidad en la trasmisión de video originado por sistemas de seguridad y vigilancia vasados en tecnologías IP.

Para el desarrollo de la investigación se desarrollo el método experimental y correlacional. Se implementó un escenario de prueba de una red WAN que muestre la interacción punto a punto entre el sistema de seguridad y el usuario final. Para la parte de ruteo del escenario se usaron dos Routers Cisco 2800 para, dos Switch Cisco 2950 usados para cada intranet, dos Cámaras IP D-Link CSD-920 que proveen el Video IP para el escenario y dos ordenadores que hicieron la parte de los clientes.

Se configuró cada arquitectura en dicho escenario y se valoró su rendimiento por medio de la utilización del Software de análisis de red Wireshark. Posteriormente se obtuvo la variabilidad de los escenarios con relación a una trasmisión de video IP en un medio BestEfort, obteniendo así el porcentaje de mejora de cada uno de las arquitecturas supuestas a estudio.

Al finalizar el estudio IntServ mejoro en un 17,7% la calidad de la transmisión mientras que DiffServ lo hizo en un 22,58%. En la obtención de los datos se observo que DiffServ obtuvo mejores resultados para la perdida de paquetes y mejoro el ancho de banda disponible para la transmisión de video.

DiffServ mostro mejor tratamiento en el envío de los paquetes de video, mientras que IntServ mejoro los tiempos en el envió de los mismos. Lo que indica que DiffServ provee mejor escalabilidad y rendimiento para la red.

Se recomienda el uso de DiffServ para la mejora del servicio de transmisión de video a tiempo real en servidores centrales de redes que manejan grandes flujos de datos como es el caso de DESITEL que es el proveedor de internet para la Intranet de la ESPOCH.

SUMMARY

GLOSARIO

Algoritmo de gestión de recursos (scheduling) - Especifica el instante en el que un usuario que ya ha ganado acceso al sistema a través del MAC puede comenzar la transmisión de su información. También indica qué cantidad de recursos puede utilizar en esta transmisión.

Beacon - Trama de gestión que contiene información relacionada con el CSMA/CA.

CSMA/CA (Evasión múltiple del sentido Access/Collision del portador).- Método de transferencia de datos que se utiliza para prevenir pérdida de los datos en una red.

DHCP.- Protocolo que deja un dispositivo en una red local, conocida como servidor de DHCP, asigna direcciones temporales del IP a los otros dispositivos de la red, típicamente computadoras.

DNS.- El IP ADDRESS del servidor del ISP, que traduce los nombres de website a direcciones del IP.

DSCP (Differentiated Services Code Point) .- Seis bits del byte ToS se reasignan para ser usados como campo DSCP. Cada DSCP especifica el comportamiento particular por salto que se ha de aplicar a cada paquete. No es compatible con IP Predence y su presencia todavía es limitada en los equipos de red.

Dominio.- Nombre específico para una red de computadoras.

Encolamiento de prioridades - Generalmente, soporta hasta ocho colas, a las que se les da servicio por orden estricto de prioridad. La cola de mayor tamaño siempre es atendida en primer lugar, y así sucesivamente. Si una cola está siendo atendida y un paquete entra en una cola mayor, se le da servicio a ésta inmediatamente.

Explorador.- Es un programa de uso que proporciona una manera de mirar y de obrar recíprocamente con toda la información sobre el World Wide Web.

Ftp (File Transfer Protocol).- Protocolo estándar para enviar archivos entre las computadoras sobre una red de TCP/IP y el Internet.

Hardware.- Aspecto físico de computadoras, de telecomunicaciones, y de otros dispositivos de la tecnología de información.

HTTP (protocolo del transporte del hypertext).- Protocolo de comunicaciones conectada a los servidores en el World Wide Web.

IEEE (Instituto de los ingenieros electrónicos eléctricos).- Instituto independiente que desarrolla estándares del establecimiento de una red.

IP (Internet Protocol).- Protocolo que envía datos sobre una red.

IP ADDRESS - Dirección que identifica a una computadora o un dispositivo en una red.

ISP (Internet Service Provider).- Compañía que proporciona el acceso al Internet.

MAC (Media Access Control).- Dirección única que un fabricante asigna a cada dispositivo del establecimiento de una red.

Mbps (Megabites por segundo).- Un millón de bits por segundo, unidad de medida para la transmisión de datos.

Paquete.- Unidad de los datos enviados sobre una red.

Pérdida de paquetes.- Si una cola alcanza su longitud máxima, se pueden producir pérdidas de paquetes. Cuando sucede, los protocolos orientados a la conexión, como TCP, disminuyen la velocidad de la transmisión para dar servicio a los paquetes de la cola y permitir que ésta se vacíe.

Red.- Varias computadoras o dispositivos conectados con el fin de compartir, almacenar, y/o transmitir datos entre los usuarios.

Servidor.- Cualquier computadora que su función en una red sea la de proporcionar el acceso de los usuarios a los archivos, a la impresión, a comunicaciones, y a otros servicios.

Software.- Una serie de instrucciones que realiza una tarea particular, también se la llama "programa".

Subnet mask.- Es un código de la dirección que determina el tamaño de la red.

TCP/IP (Protocolo del control Protocol/Internet de la transmisión).- Sistema de protocolos que hacen posibles servicios Telnet, FTP, E-mail, y otros entre ordenadores que no pertenecen a la misma red.

UDP (User Datagram Protocol).- Es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción.

ToS (Type-Of-Service) - Campo de ocho bits de la cabecera de IP. Lo utilizan IP Precedence, Differentiated Services Code Point y ToS.

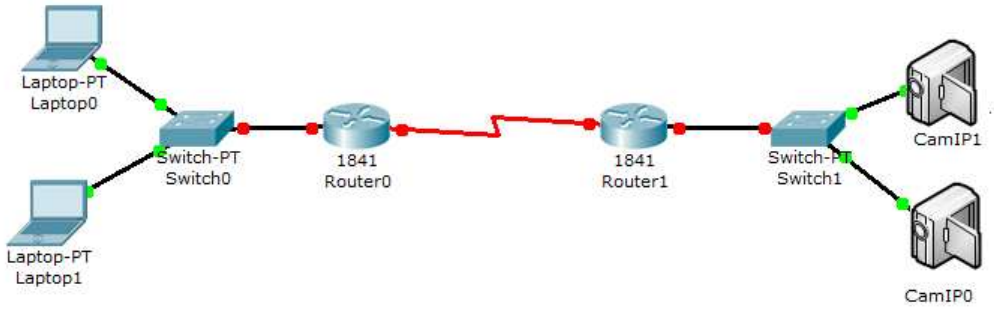
QoS (Calidad de Servicio).- Son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado. Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz. Es la capacidad de una red para proveer diferentes niveles de servicio a los distintos tipos de tráfico.

IntServ.- El modelo de servicios integrados propone una solución para el soporte de calidad de servicio extremo a extremo basado en la pre-reserva de recursos en los diferentes equipos de conmutación que componen el trayecto que seguirá información en la comunicación.

Diffserv.- El modelo de servicios diferenciados propone una solución para el soporte de calidad de servicio basado en la priorización de clases de tráfico.

ANEXOS

ESQUEMA ESCENARIO DE PRUEBA



DIRECCIONAMIENTO IP DEL ESCENARIO

DIRECCIONAMIENTO IP ROUTERS				
	Interface Serial 0/0/0		Interface FastEthernet	
	IP Address	SubNet Mask	IP Address	SubNet Mask
Router 1	192.168.1.2	255.255.255.0	192.168.2.1	255.255.255.0
Router 2	192.168.1.3	255.255.255.0	192.168.3.1	255.255.255.0

DIRECCIONAMIENTO IP PERIFÉRICOS FINALES			
	Interface FastEthernet		Default GateWay
	IP Address	SubNet Mask	IP Address
Pc 1	192.168.2.3	255.255.255.0	192.168.2.1
Pc 2	192.168.2.4	255.255.255.0	192.168.2.1
Cam IP1	192.168.3.3	255.255.255.1	192.168.3.1
Cam IP2	192.168.3.4	255.255.255.2	192.168.3.1

LÍNEAS DE CÓDIGO AMBIENTE DE SIMULACIÓN BESTEFORT

CONFIGURACIÓN DE LAS INTERFACES

a. **Configuración del Router1**

Router> enable
Router# configure terminal
Router(config)# hostname R1
R1(config-if)# interface fast-ethernet 0/0
R1(config-if)# ip address 192.168.2.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
R1(config)# interface serial 0/0/0
R1(config-if)# ip address 192.168.1.2 255.255.255.0
R1(config-if)# clock rate 36000
R1(config-if)# no shutdown
R1(config-if)# exit

b. **Configuración del Router1**

Router> enable
Router# configure terminal
Router(config)# hostname R2
R2(config-if)# interface fast-ethernet 0/0
R2(config-if)# ip address 192.168.3.1 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit
R2(config)# interface serial 0/0/0
R2(config-if)# ip address 192.168.1.3 255.255.255.0
R2(config-if)# no shutdown
R2(config-if)# exit

CONFIGURACIÓN DEL PARÁMETRO DE RUTEO

a. **Configuración R1**

R1#configure terminal
R1(config)# router rip
R1(config-router)# network 192.168.1.0
R1(config-router)# network 192.168.2.0
R1(config-router)# CTRL+Z

b. Configuración R2

R2#configure terminal

R2(config)# router rip

R2(config-router)# network 192.168.1.0

R2(config-router)# network 192.168.3.0

R2(config-router)# CTRL+Z

LÍNEAS DE CÓDIGO AMBIENTE DE SIMULACIÓN INTSERV

CONFIGURACIÓN DE LAS INTERFACES

c. Configuración del Router1

Router> enable

Router# configure terminal

Router(config)# hostname R1

R1(config-if)# interface fast-ethernet 0/0

R1(config-if)# ip address 192.168.2.1 255.255.255.0

R1(config-if)# no shutdown

R1(config-if)# exit

R1(config)# interface serial 0/0/0

R1(config-if)# ip address 192.168.1.2 255.255.255.0

R1(config-if)# clock rate 36000

R1(config-if)# no shutdown

R1(config-if)# exit

d. Configuración del Router1

Router> enable

Router# configure terminal

Router(config)# hostname R2

R2(config-if)# interface fast-ethernet 0/0

R2(config-if)# ip address 192.168.3.1 255.255.255.0

R2(config-if)# no shutdown

R2(config-if)# exit

R2(config)# interface serial 0/0/0

R2(config-if)# ip address 192.168.1.3 255.255.255.0

R2(config-if)# no shutdown

R2(config-if)# exit

CONFIGURACIÓN DEL PARÁMETRO DE RUTEO

c. Configuración R1

R1#configure terminal

R1(config)# router rip

R1(config-router)# network 192.168.1.0

R1(config-router)# network 192.168.2.0

R1(config-router)# CTRL+Z

d. Configuración R2

R2#configure terminal

R2(config)# router rip

R2(config-router)# network 192.168.1.0

R2(config-router)# network 192.168.3.0

R2(config-router)# CTRL+Z

CONFIGURACIÓN INTSERV

a. Configuración R1

<Define class map>

R1#configure terminal

R1(config)#class-map Gold

R1(config-cmap)# match acces-group name Gold

R1(config)# ip access-list extended Gold

R1(config-ext-nacl)# permit tcp 192.168.3.3 0.0.0.255 any

R1(config-ext-nacl)# permit tcp 192.168.3.4 0.0.0.255 any

R1(config-ext-nacl)# deny ip any any

<Creating policies >

R1(config)# policy-map JPG

R1(config)# class Gold

R1(config-pmac-c)# bandwidth 1536

<Attaching policies to interfaces>
R1(config)# interface serial 0/0/0
R1(config)# service-policy output JPG

b. Configuración R2

<Define class map>

R2#configure terminal

R2(config)#class-map Gold

R2(config-cmap)# match acces-group name Gold

R2(config)# ip access-list extended Gold

R2(config-ext-nacl)# permit tcp 192.168.3.3 0.0.0.255 any

R2(config-ext-nacl)# permit tcp 192.168.3.4 0.0.0.255 any

R2(config-ext-nacl)# deny ip any any

<Creating policies >

R2(config)# policy-map JPG
R2(config)# class Gold
R2(config-pmac-c)# bandwidth 1536

<Attaching policies to interfaces>
R2(config)# interface serial 0/0/0
R2(config)# service-policy input JPG

LÍNEAS DE CÓDIGO AMBIENTE DE SIMULACIÓN DIFFSERV

CONFIGURACIÓN DE LAS INTERFACES

e. Configuración del Router1

Router> enable

Router# configure terminal

Router(config)# hostname R1

R1(config-if)# interface fast-ethernet 0/0

R1(config-if)# ip address 192.168.2.1 255.255.255.0

R1(config-if)# no shutdown

R1(config-if)# exit

R1(config)# interface serial 0/0/0

R1(config-if)# ip address 192.168.1.2 255.255.255.0

R1(config-if)# clock rate 36000

R1(config-if)# no shutdown

R1(config-if)# exit

f. Configuración del Router1

Router> enable

Router# configure terminal

Router(config)# hostname R2

R2(config-if)# interface fast-ethernet 0/0

R2(config-if)# ip address 192.168.3.1 255.255.255.0

R2(config-if)# no shutdown

R2(config-if)# exit

R2(config)# interface serial 0/0/0

R2(config-if)# ip address 192.168.1.3 255.255.255.0

R2(config-if)# no shutdown

R2(config-if)# exit

CONFIGURACIÓN DEL PARÁMETRO DE RUTEO

e. Configuración R1

R1#configure terminal

R1(config)# router rip

R1(config-router)# network 192.168.1.0

R1(config-router)# network 192.168.2.0

R1(config-router)# CTRL+Z

f. Configuración R2

R2#configure terminal

R2(config)# router rip

R2(config-router)# network 192.168.1.0

R2(config-router)# network 192.168.3.0

R2(config-router)# CTRL+Z

CONFIGURACIÓN DIFFSERV

Configuración R1

R1(config)#interface serial 0/0

R1(config-if)#random-detect

R1(config)#interface serial 0/0

R1(config-if)#random-detect exponential-weighting-constant 10

CAPTURA DE LAS PANTALLAS DE RESULTADOS OBTENIDOS

BESTEFOR SIN TRÁFICO

Paquetes Capturados

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
2	0.149365	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic
4	0.378874	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
5	0.534386	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic
7	0.541030	192.168.3.4	192.168.2.3	TCP	[TCP Dup ACK 5#1] http > 49326 [ACK] Seq=4923 Ack=1 Win=5840 Len=0
8	0.763100	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
9	0.918134	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic
11	1.147809	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
12	1.301897	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic
14	1.530630	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
15	1.684885	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic
17	1.914845	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
18	2.077283	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic
21	2.307204	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
22	2.470291	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic
24	2.701220	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
25	2.859338	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic
27	3.088377	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
28	3.241221	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic

Sumatoria Tráfico Capturado

Display filter: ip.dst == 192.168.2.3

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	636	100,00 %	790325	0,054	0	0	0,000
Ethernet	100,00 %	636	100,00 %	790325	0,054	0	0	0,000
Internet Protocol	100,00 %	636	100,00 %	790325	0,054	0	0	0,000
Transmission Control Protocol	100,00 %	636	100,00 %	790325	0,054	24	1440	0,000
Hypertext Transfer Protocol	96,23 %	612	99,82 %	788885	0,054	306	325601	0,022
JPEG File Interchange Format	48,11 %	306	58,62 %	463284	0,032	306	463284	0,032

BESTEFORT CON TRÁFICO

Paquetes Capturados

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic
3	0.219705	192.168.3.5	192.168.2.3	TCP	49278 > 51880 [ACK] Seq=1 Ack=1 Win=32768 Len=1460
5	0.439084	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
8	0.660928	192.168.3.5	192.168.2.3	TCP	49278 > 51880 [ACK] Seq=1461 Ack=1 Win=32768 Len=1460
9	0.810597	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic
10	0.817257	192.168.3.3	192.168.2.3	TCP	[TCP Dup ACK 9#1] http > 51851 [ACK] Seq=2446 Ack=1 Win=5840 Len=0
13	1.036696	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
15	1.258023	192.168.3.5	192.168.2.3	TCP	49278 > 51880 [ACK] Seq=2921 Ack=1 Win=32768 Len=1460
16	1.359515	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic
19	1.578804	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
21	1.800308	192.168.3.5	192.168.2.3	TCP	49278 > 51880 [ACK] Seq=4381 Ack=1 Win=32768 Len=1460
22	1.946920	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic
25	2.166364	192.168.3.4	192.168.2.3	HTTP	[TCP Retransmission] Continuation or non-HTTP traffic (JPEG JFIF image)
27	2.267813	192.168.3.4	192.168.2.3	HTTP	[TCP Retransmission] Continuation or non-HTTP traffic
30	2.488896	192.168.3.5	192.168.2.3	TCP	49278 > 51880 [ACK] Seq=5841 Ack=1 Win=32768 Len=1460
32	2.708136	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
34	2.927147	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
36	3.147032	192.168.3.5	192.168.2.3	TCP	49278 > 51880 [ACK] Seq=7301 Ack=1 Win=32768 Len=1460

Sumatoria Tráfico Capturado

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	840	100,00 %	863211	0,055	0	0	0,000
Ethernet	100,00 %	840	100,00 %	863211	0,055	0	0	0,000
Internet Protocol	100,00 %	840	100,00 %	863211	0,055	0	0	0,000
Transmission Control Protocol	100,00 %	840	100,00 %	863211	0,055	129	7842	0,001
Hypertext Transfer Protocol	47,50 %	399	52,47 %	452515	0,029	199	149715	0,010
JPEG File Interchange Format	23,81 %	200	35,08 %	302800	0,019	200	302800	0,019
Data	6,31 %	53	9,30 %	80242	0,005	53	80242	0,005
File Transfer Protocol (FTP)	5,71 %	48	0,37 %	3158	0,000	48	3158	0,000
FTP Data	25,12 %	211	37,01 %	319454	0,021	211	319454	0,021

INTSERV

Paquetes Capturados

No.	Time	Source	Destination	Protocol	Info
2	0.019342	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
4	0.238412	192.168.3.5	192.168.2.3	TCP	49531 > 52043 [ACK] Seq=1 Ack=1 Win=32768 Len=1460
6	0.338033	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic
8	0.557543	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
9	0.564217	192.168.3.3	192.168.2.3	TCP	[TCP Dup ACK 8#1] http > 51851 [ACK] Seq=1461 Ack=1 Win=5840 Len=0
11	0.783465	192.168.3.5	192.168.2.3	TCP	49531 > 52043 [ACK] Seq=1461 Ack=1 Win=32768 Len=1460
13	0.928360	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic
15	1.147610	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
17	1.366625	192.168.3.5	192.168.2.3	TCP	49531 > 52043 [ACK] Seq=2921 Ack=1 Win=32768 Len=1460
19	1.463174	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic
21	1.682456	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
25	1.900335	192.168.3.5	192.168.2.3	TCP	49531 > 52043 [ACK] Seq=4381 Ack=1 Win=32768 Len=1460
28	2.041632	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic
31	2.260946	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
33	2.479966	192.168.3.5	192.168.2.3	TCP	49531 > 52043 [ACK] Seq=5841 Ack=1 Win=32768 Len=1460
35	2.576458	192.168.3.4	192.168.2.3	HTTP	Continuation or non-HTTP traffic
37	2.795658	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
39	3.018252	192.168.3.5	192.168.2.3	TCP	49531 > 52043 [ACK] Seq=7301 Ack=1 Win=32768 Len=1460
41	3.162384	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic

Sumatoria Tráfico Capturado

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	825	100,00 %	838999	0,056	0	0	0,000
Ethernet	100,00 %	825	100,00 %	838999	0,056	0	0	0,000
Internet Protocol	100,00 %	825	100,00 %	838999	0,056	0	0	0,000
Transmission Control Protocol	100,00 %	825	100,00 %	838999	0,056	129	7844	0,001
Hypertext Transfer Protocol	51,27 %	423	57,57 %	483013	0,032	218	172643	0,011
JPEG File Interchange Format	24,85 %	205	36,99 %	310370	0,021	205	310370	0,021
Data	1,70 %	14	2,53 %	21196	0,001	14	21196	0,001
File Transfer Protocol (FTP)	5,45 %	45	0,35 %	2950	0,000	45	2950	0,000
FTP Data	25,94 %	214	38,62 %	323996	0,021	214	323996	0,021

DIFFSERV

Paquetes Capturados

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.3.5	192.168.2.3	TCP	49196 > 54818 [ACK] Seq=1 Ack=1 Win=32768 Len=1460
3	0.219181	192.168.3.5	192.168.2.3	TCP	49196 > 54818 [ACK] Seq=1461 Ack=1 Win=32768 Len=1460
6	0.439020	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
7	0.541822	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic
10	0.629581	192.168.2.1	192.168.2.3	ICMP	Destination unreachable (Host unreachable)
12	0.761505	192.168.3.5	192.168.2.3	TCP	49196 > 54818 [ACK] Seq=2921 Ack=1 Win=32768 Len=1460
19	0.980128	192.168.3.5	192.168.2.3	TCP	49196 > 54818 [ACK] Seq=4381 Ack=1 Win=32768 Len=1460
21	1.199748	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
22	1.300032	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic
24	1.523291	192.168.3.5	192.168.2.3	TCP	49196 > 54818 [ACK] Seq=5841 Ack=1 Win=32768 Len=1460
25	1.529840	192.168.3.3	192.168.2.3	TCP	[TCP Dup ACK 22#1] http > 54787 [ACK] Seq=4231 Ack=1 Win=5840 Len=0
27	1.748817	192.168.3.5	192.168.2.3	TCP	49196 > 54818 [ACK] Seq=7301 Ack=1 Win=32768 Len=1460
29	1.968682	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
30	2.069000	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic
34	2.250685	192.168.2.1	192.168.2.3	ICMP	Destination unreachable (Host unreachable)
35	2.287811	192.168.3.5	192.168.2.3	TCP	49196 > 54818 [ACK] Seq=8761 Ack=1 Win=32768 Len=1460
37	2.506907	192.168.3.5	192.168.2.3	TCP	49196 > 54818 [ACK] Seq=10221 Ack=1 Win=32768 Len=1460
39	2.726716	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic (JPEG JFIF image)
40	2.824501	192.168.3.3	192.168.2.3	HTTP	Continuation or non-HTTP traffic

Sumatoria Tráfico Capturado

Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00 %	293	100,00 %	319050	0,056	0	0	0,000
Ethernet	100,00 %	293	100,00 %	319050	0,056	0	0	0,000
Internet Protocol	100,00 %	293	100,00 %	319050	0,056	0	0	0,000
Transmission Control Protocol	84,98 %	249	99,03 %	315970	0,055	9	540	0,000
Data	41,30 %	121	57,32 %	182866	0,032	121	182866	0,032
Hypertext Transfer Protocol	40,61 %	119	41,55 %	132564	0,023	59	41724	0,007
JPEG File Interchange Format	20,48 %	60	28,47 %	90840	0,016	60	90840	0,016
Internet Control Message Protocol	15,02 %	44	0,97 %	3080	0,001	44	3080	0,001

TABLA DEL CHI CUADRADO

P = Probabilidad de encontrar un valor mayor o igual que el chi cuadrado tabulado, ν = Grados de Libertad

ν/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15	0,2	0,25	0,3	0,35	0,4	0,45	0,5
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722	1,6424	1,3233	1,0742	0,8735	0,7083	0,5707	0,4549
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942	3,2189	2,7726	2,4079	2,0996	1,8326	1,5970	1,3863
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170	4,6416	4,1083	3,6649	3,2831	2,9462	2,6430	2,3660
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449	5,9886	5,3853	4,8784	4,4377	4,0446	3,6871	3,3567
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152	7,2893	6,6257	6,0644	5,5731	5,1319	4,7278	4,3515
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461	8,5581	7,8408	7,2311	6,6948	6,2108	5,7652	5,3481
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479	9,8032	9,0371	8,3834	7,8061	7,2832	6,8000	6,3458
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271	11,0301	10,2189	9,5245	8,9094	8,3505	7,8325	7,3441
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880	12,2421	11,3887	10,6564	10,0060	9,4136	8,8632	8,3428
10	29,5879	27,1119	25,1881	23,2093	20,4832	18,3070	15,9872	14,5339	13,4420	12,5489	11,7807	11,0971	10,4732	9,8922	9,3418
11	31,2635	28,7291	26,7569	24,7250	21,9200	19,6752	17,2750	15,7671	14,6314	13,7007	12,8987	12,1836	11,5298	10,9199	10,3410
12	32,9092	30,3182	28,2997	26,2170	23,3367	21,0261	18,5493	16,9893	15,8120	14,8454	14,0111	13,2661	12,5838	11,9463	11,3403
13	34,5274	31,8830	29,8193	27,6882	24,7356	22,3620	19,8119	18,2020	16,9848	15,9839	15,1187	14,3451	13,6356	12,9717	12,3398
14	36,1239	33,4262	31,3194	29,1412	26,1189	23,6848	21,0641	19,4062	18,1508	17,1169	16,2221	15,4209	14,6853	13,9961	13,3393
15	37,6978	34,9494	32,8015	30,5780	27,4884	24,9958	22,3071	20,6030	19,3107	18,2451	17,3217	16,4940	15,7332	15,0197	14,3389
16	39,2518	36,4555	34,2671	31,9999	28,8453	26,2962	23,5418	21,7931	20,4651	19,3689	18,4179	17,5646	16,7795	16,0425	15,3385
17	40,7911	37,9462	35,7184	33,4087	30,1910	27,5871	24,7690	22,9770	21,6146	20,4887	19,5110	18,6330	17,8244	17,0646	16,3382
18	42,3119	39,4220	37,1564	34,8052	31,5264	28,8693	25,9894	24,1555	22,7595	21,6049	20,6014	19,6993	18,8679	18,0860	17,3379
19	43,8194	40,8847	38,5821	36,1908	32,8523	30,1435	27,2036	25,3289	23,9004	22,7178	21,6891	20,7638	19,9102	19,1069	18,3376
20	45,3142	42,3358	39,9969	37,5663	34,1696	31,4104	28,4120	26,4976	25,0375	23,8277	22,7745	21,8265	20,9514	20,1272	19,3374
21	46,7963	43,7749	41,4009	38,9322	35,4789	32,6706	29,6151	27,6620	26,1711	24,9348	23,8578	22,8876	21,9915	21,1470	20,3372
22	48,2676	45,2041	42,7957	40,2894	36,7807	33,9245	30,8133	28,8224	27,3015	26,0393	24,9390	23,9473	23,0307	22,1663	21,3370
23	49,7276	46,6231	44,1814	41,6383	38,0756	35,1725	32,0069	29,9792	28,4288	27,1413	26,0184	25,0055	24,0689	23,1852	22,3369
24	51,1790	48,0336	45,5584	42,9798	39,3641	36,4150	33,1962	31,1325	29,5533	28,2412	27,0960	26,0625	25,1064	24,2037	23,3367
25	52,6187	49,4351	46,9280	44,3140	40,6465	37,6525	34,3816	32,2825	30,6752	29,3388	28,1719	27,1183	26,1430	25,2218	24,3366
26	54,0511	50,8291	48,2898	45,6416	41,9231	38,8851	35,5632	33,4295	31,7946	30,4346	29,2463	28,1730	27,1789	26,2395	25,3365
27	55,4751	52,2152	49,6450	46,9628	43,1945	40,1133	36,7412	34,5736	32,9117	31,5284	30,3193	29,2266	28,2141	27,2569	26,3363
28	56,8918	53,5939	50,9936	48,2782	44,4608	41,3372	37,9159	35,7150	34,0266	32,6205	31,3909	30,2791	29,2486	28,2740	27,3362
29	58,3006	54,9662	52,3355	49,5878	45,7223	42,5569	39,0875	36,8538	35,1394	33,7109	32,4612	31,3308	30,2825	29,2908	28,3361

BIBLIOGRAFÍA

1. Cisco,Sistems. Student Guide. Huston EEUU 2006/06/28 pp 170-240

   2010/08/23

2. Ferguson, Paul Quality of Service Huston EEUU 1998. pp 140-183

   2010/09/02

3. Flannagan, Michael. Administering Cisco. Syngress. QoS Pag. 124 - 135, 143 - 146, 218 - 227

   2010/11/23

4. CAMARAS IP: DESCRIPCIÓN, VENTAJAS, USO COMUN

   http://es.wikipedia.org/wiki/C%C3%A1mara_IP

   2010/03/14

5. INTSERV: CONCEPTOS BÁSICOS (17/09/2010)

   http://jpadilla.docentes.upbbga.edu.co/QoS/IntServ1%20conceptos%20basicos.pdf

   2010/09/03

6. INTSERV: MODELO DE SERVICIO

   http://jpadilla.docentes.upbbga.edu.co/QoS/IntServ2%20Modelos%20de%20Servicio.pdf

   2009/11/17

7. MEDIOS DE TRANSMISIÓN: TIPOS, CARACTERISTICAS

   http://es.wikipedia.org/wiki/Medio_de_transmisi%C3%B3n

   2010/04/22

8. QOS: DESCRIPCION, VENTAJAS

   http://www.axis.com/es/products/video/about_networkvideo/qos.htm

   2010/07/14