UNIVERSIDAD PRIVADA ANTENOR ORREGO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE TELECOMUNICACIONES Y REDES

ANÁLISIS DE LOS FACTORES QUE INFLUYE CON EL RENDIMIENTO DE LA RED DE DATOS DE LA CORTE SUPERIOR DE JUSTICIA DE LA LIBERTAD BASADOS EN LOS PARÁMETROS DE QoS – 2017

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE TELECOMUNICACIONES Y REDES

LÍNEA DE INVESTIGACIÓN: DISEÑO, INTERCONEXIÓN Y GESTIÓN DE REDES DE COMUNICACIÓN

AUTOR: PALOMINO SUAREZ, TELMO GABRIEL

ASESOR: RAMOS ROJAS OVIDIO HILDEBRANDO

TRUJILLO - PERÚ

2017

ACREDITACIONES

ANÁLISIS DE LOS FACTORES QUE INFLUYE CON EL RENDIMIENTO DE LA RED DE LA CORTE SUPERIOR DE JUSTICIA DE LA LIBERTAD BASADOS EN LOS PARÁMETROS DE QoS - 2017

AUTOR: PALOMINO SUAREZ TELMO GABRIEL

APROBADO POR:

Ing. Filiberto Melchor, Azabache Fernández
PRESIDENTE
N° CIP 97916

Ing. Eduardo Elmer, Cerna Sánchez
SECRETARIO
N° CIP 80252

Ing. Luis Enrique, Alvarado Rodríguez
VOCAL
N° CIP 149200

Ing. Ovidio Hildebrando Ramos Rojas
ASESOR
N° CIP 92622

PRESENTACIÓN

Señores Miembros del Jurado:

Dando cumplimiento y conforme a las normas establecidas en el Reglamento de Grados y Títulos y Reglamento de la Facultad de Ingeniería de la Universidad Privada Antenor Orrego, para obtener el título profesional de Ingeniero de Telecomunicaciones y Redes, se pone a vuestra consideración el Informe del Trabajo de Investigación Titulado **"**ANÁLISIS DE LOS FACTORES QUE INFLUYE CON EL RENDIMIENTO DE LA RED DE DATOS DE LA CORTE SUPERIOR DE JUSTICIA DE LA LIBERTAD, BASADOS EN LOS PARÁMETROS DE QoS - 2017**"**, con la convicción de alcanzar una justa evaluación y dictamen, excusándome de antemano de los posibles errores involuntarios cometidos en el desarrollo del mismo.

Trujillo, 12 de diciembre del 2017.

Palomino Suarez Telmo Gabriel

DEDICATORIA

A mis padres, **Telmo Palomino Cabanillas** y **Violeta Suarez Moncada**, por su dedicación y sacrificio, ya que ambos son mi motor y motivo para superarme y ser un mejor profesional y persona día a día.

A mis amigos, por el constante apoyo que día a día me brindaron y a los cuales considero muchísimo; orientándome y aconsejándome para ser mejor una persona.

A mis hermanos, **Danny, Enemecio y Lucy** por su apoyo en muchas de las etapas de mi vida, mi formación académica, guiándome y demostrándome el verdadero apoyo que solo la familia nos puede dar.

AGRADECIMIENTOS

A Dios, por ser la guía de mi vida y haberme permitido vencer los obstáculos que se pusieron en mi camino.

Al ingeniero Ovidio Ramos Rojas por la orientación profesional que me brindó durante el desarrollo de este proyecto.

A la Universidad Privada Antenor Orrego por ser la casa de estudios que permitió mi formación académica y haberme demostrado, que un buen profesional, no solo es un cúmulo de conocimientos sino también de valores.

RESUMEN

El presente trabajo de investigación se desarrolló en la línea de investigación Diseño, Interconexión y Redes de Comunicación de la Carrera de Ingeniería de Telecomunicaciones y Redes de la Universidad Privada Antenor Orrego; el objetivo principal fue determinar los factores basados en los parámetros de QoS que influyen en el rendimiento de la red de la Corte Superior de Justicia de La Libertad para el periodo 2017. La metodología se basó en una investigación de tipo aplicada y de campo, descriptiva por su alcance, estudiando los procedimientos necesarios para el tratamiento de incidencias dentro de la red. Se utilizó la herramienta de análisis "Wireshark" para recolectar la información relacionada con el tráfico de red las cuales fueron capturadas en 3 días de la semana en horarios de funcionamiento normal en la red de la corte. Los resultados obtenidos se procesaron utilizando el análisis ANOVA disponible dentro del programa estadístico "statgraphics". Al concluir el estudio se pudo determinar que los factores relacionados con el parámetro del Jitter influyen significativamente en el rendimiento de la red.

Palabras Clave: Jitter, Wireshark, Parámetros de QoS

ABSTRACT

The present research work is in the line of research design, interconnection and communication networks of the network and Telecommunications Engineering of the Universidad Privada Antenor Orrego; the main objective was to determine the factors based on the QoS parameters that influence the performance of the network of the Corte Superior de Justicia de La Libertad for the period 2017. The methodology was based on an applied research and field, descriptive in its scope, studying the procedures necessary for the treatment of incidents within the network. We used the tool analyzer "Wireshark" to collect information related to the network traffic which were captured in 3 days a week in times of normal operation in the network of the court. The results obtained were processed using the ANOVA, available in the statistical program called "statgraphics". The conclusion of the study was able to determine that the factors related to the parameter of the Jitter have a significant influence on the performance of the network.

Keywords: Jitter, Wireshark, QoS Parameters

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

CAPÍTULO
I
INTRODUCCION

1 INTRODUCCIÓN

1.1. REALIDAD PROBLEMÁTICA

La función principal del poder judicial es administrar Justicia a través de sus órganos jurisdiccionales, con arreglo a la Constitución y a las leyes, garantizando la seguridad jurídica y la tutela jurisdiccional, para contribuir al estado de derecho, al mantenimiento de la paz social y al desarrollo nacional.

La Corte Superior de Justicia de La Libertad es un Órgano Jurisdiccional del Poder Judicial encargado de administrar justicia en el Distrito Judicial de La Libertad, a nombre de la Nación y a través de las Salas Especializadas o Mixtas, Juzgados Especializados o Mixtos y de Paz Letrado, de acuerdo a los principios establecidos en la Constitución Política del Perú, y a lo normado por la Ley Orgánica del Poder Judicial, los códigos y leyes que correspondan. Funcionalmente depende de la Sala Plena de la Corte Suprema y administrativamente del Consejo Ejecutivo del Poder Judicial. Actualmente la red que da soporte a los servicios de la jurisdicción de la corte superior de justicia de la Libertad se encuentra centralizado en la sede judicial de Natasha Alta la cual se muestra en la gráfica siguiente:

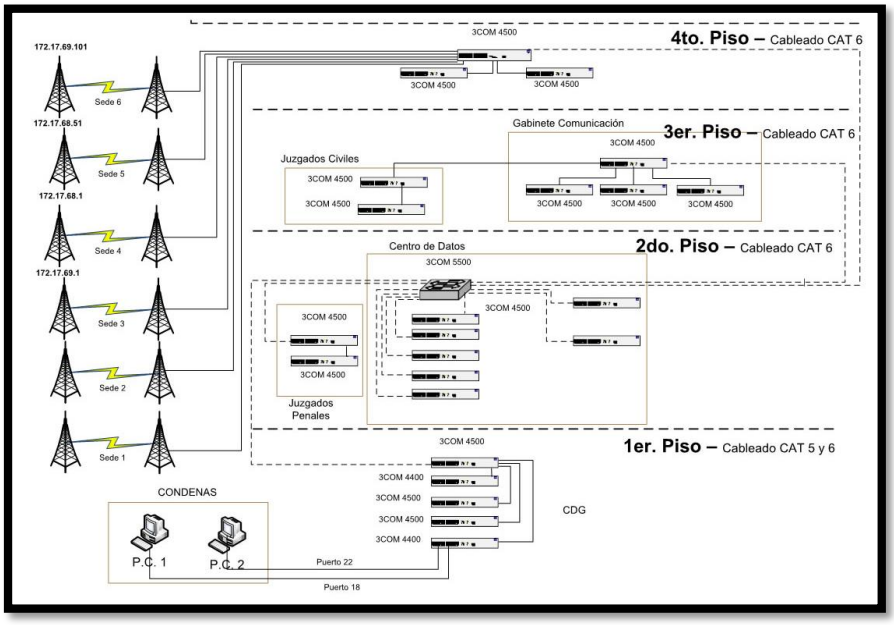


Figura 1: **Topología Actual de la Red de la Corte Superior de Justicia de La Libertad.**
Fuente: **Diagrama actual del Poder Judicial**

Las gestiones actuales de los servicios de la red se realizan desde la data center por el administrador de la red del departamento de informática que en ella se encuentra una serie de dispositivos que facilitan a las distintas áreas y sedes la interconexión e interacción con los servicios de voz, datos y video.

Estos servicios tanto locales como descentralizados actualmente se han incrementado y no se han dispuesto de mecanismos para el mejor funcionamiento de la red, los actuales servicios con los que actualmente dentro de la red son:

- Sistema de Expedientes Judiciales
- Siga (Sistema de Gestión Administrativa)
- Sistema de Peritos Judiciales
- Sistema de Condenas
- Sistemas de la Nueva ley Laboral
- Jurisdiccionales y Administrativos

Todos estos sistemas se han ido acoplando al sistema base original, el cual puede generar un tráfico mayor a la hora de su uso, debido a gran mayoría de transacciones que se pueden realizar al mismo tiempo esto puede generar gran consumo de recursos de red debido a que no solo los trabajadores del poder judicial pueden realizar consultas, sino también el público en general mediante la página web.

1.2. DELIMITACIÓN DEL PROBLEMA

La delimitación de esta investigación se basa en determinar cuáles son los factores basados en los parámetros de QoS que influyen con el rendimiento de la red de la Corte Superior de Justicia de la Libertad para el periodo 2017.

1.3. CARACTERÍSTICAS Y ANÁLISIS DEL PROBLEMA

- **El malestar de los usuarios frente a las interrupciones en el acceso a los servicios que ofrece la red de datos.**

  En la red de red de datos de la Corte Superior de Justicia de la Libertad existen más de 1610 personas distribuidas en las diferentes oficinas como se muestra en la siguiente tabla.

ÁREAS	N° TRABAJADORES POR ÁREAS
Secretaría General y Mesa de Partes	40
Coordinación de Capacitación	30
Oficina de Apoyo a la Justicia de Paz	50
Odicma - Codigma - Imagen Institucional	50
Asesoría	40
Sala Civil	30
Sala Mixta	30
Sala Penal de Aplicaciones	30
Sala Penal Transitoria	30
Juzgado Penal de Liquidación	30
Juzgados Penales Según el N.C.P.P. - Colegiado - Unipersonal - Investigación Preparatoria	250
Juzgados Civiles	50
Juzgados de Familia	50
Juzgados Mixtos	50
Juzgados de Paz Letrado	50

Juzgados de Paz	50

Oficina de Administración
- Tesorería
- Logística
  - Unidad de Control Patrimonial
  - Unidad de Almacén Periférico
- Informática
- Personal
  - Unidad de Bienestar Social
- Estadística
- Servicios Judiciales y Recaudación
  - Unidad Archivo Modular
  - Unidad Secretaria de Multas
- Administrador Modulo Penal
  - Especialista de Salas
  - Asistente Jurisdiccional
  - Especialista de Audiencias
  - Especialista de Juzgados
  - Asistente Jurisdiccional
  - Especialista de Audiencias
  - Unidad Informática
  - Unidad Custodia de Grab. y Exp.
  - Unidad Sala de Lectura
	750

TOTAL	**1610**

Tabla 1: **Nº de Trabajadores por área de la Corte Superior de Justicia de La Libertad.**
Fuente: **Elaboración Propia**

De estos usuarios el 60% hace uso diariamente de los servicios brindados por la red como el sistema de expedientes judiciales, el sistema de gestión administrativa, sistema de peritos judiciales, entre otros; en una encuesta realizada al administrador del departamento de informática de la corte superior de justicia de la libertad manifiesta que existe un gran números de quejas por los usuarios al momento de usar alguno de esto servicios de la red la mayoría de las quejas son por la lentitud del acceso a los servicios de adjuntar información o de consulta misma hasta en algunos de los casos cortes de conectividad.

- **Mala planificación de los servicios que ofrece la red de datos.**

  Frente a los diferentes tipos de servicios que se ofrecen dentro de la red obligan a definir diferentes grados de importancia o prioridad según diferentes tipos de tráfico, de manera que un tipo resulte privilegiado en perjuicio de otro tipo. De acuerdo a las entrevistas programadas con el administrador de la red de la corte nos dice que por este se transmiten el servicio de expedientes judiciales (SEJ), sistema de peritos, sistema de intereses legales, servicio de correo electrónico, servicio de internet, el SIGA (Sistema de Gestión Administrativa), etc; todos estos sistemas se han ido acoplando al sistema base original, el cual genera un tráfico mayor a la hora de su uso, debido a gran mayoría de transacciones que se realizan al mismo tiempo.

  Actualmente se desconoce los diferentes parámetros y el elevado número de protocolos predeterminados ya que posee una red plana en su diseño lo cual dificulta la administración del tráfico de la red, debido a la ausencia de estándares de calidad en gestión de tráfico LAN, políticas de seguridad no alineadas a las necesidades de la empresa.

  Los servicios de mayor incidencia son las audiencias a través de las videoconferencias y que son alrededor de 75 audiencias a la semana (lunes a viernes) que hacen un promedio de 15 audiencias por día, lo cual se usa un equipo por audiencia, un equipo en la sede local y un equipo en la sede remota, estos equipos crean 5 salas multipunto virtuales, eso quiere decir que en una audiencia se puede tener hasta 5 sedes conectadas al mismo tiempo participando en simultaneo, la duración de cada audiencia depende mucho de los involucrados si por algún motivo un abogado de alguna de las partes no llegase a tiempo el otro

abogado puede reprogramar dicha audiencia, se han reportado casos de lentitud al momento de utilizar este equipo en las audiencias.

Al analizar el tráfico dentro de la red a través de un analizador se evidencia un alto grado de errores a nivel de Ethernet entre otros protocolos que podrían estar generando el alto índice de la mala planificación de servicios.

Severity	Group	Protocol	Count
Error	Checksum	Ethernet	1274
Error	Malformed	CDP	172
Error	Malformed	PNG	1
Error	Malformed	LLMNR	2
Warn	Sequence	TCP	57
Warn	Protocol	XML	1
Warn	Sequence	ICMP	2
Note	Sequence	TCP	985
Note	Sequence	IPv4	287
Note	Protocol	TCP	17
Chat	Sequence	TCP	1775
Chat	Sequence	HTTP	5743

Figura 2: **Análisis de Información del tráfico de la red de la Corte Superior de Justicia de La Libertad**
Fuente: **Elaboración propia.**

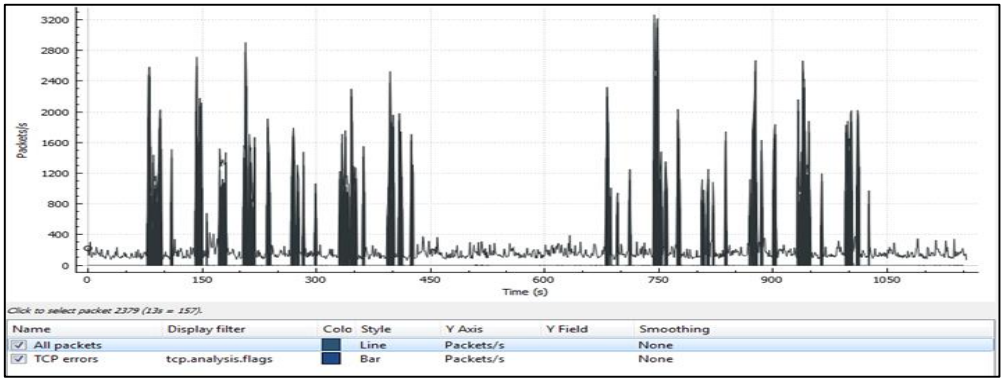


Figura 3: **Estadística gráfica de los paquetes de información del tráfico de red de la Corte Superior de Justicia de La Libertad.**
Fuente: **Elaboración propia.**

1.4. FORMULACIÓN DEL PROBLEMA

¿Cómo los factores basados en los parámetros de QoS influyen en el rendimiento de la red de la Corte Superior de Justicia de la Libertad?

1.5. FORMULACIÓN DE LA HIPÓTESIS

Los factores basados en los parámetros de QoS influyen significativamente en el rendimiento de la red de la Corte Superior de Justicia de la Libertad.

1.6. OBJETIVOS DEL ESTUDIO

1.6.1. GENERAL

Determinar los factores basados en los parámetros de QoS que influyen en el rendimiento de la red de la Corte Superior de Justicia de la Libertad.

1.6.2. ESPECÍFICOS

- Caracterizar los factores basados en los parámetros de QoS que regulan la red de datos.
- Analizar el tráfico de la red.
- Identificar los factores de mayor influencia en el rendimiento de la red

1.7. JUSTIFICACIÓN DEL ESTUDIO

1.7.1. IMPORTANCIA DE LA INVESTIGACIÓN

La importancia del presente estudio es de tipo académica y tecnológica. Académica porque permitirá a los investigadores entender sobre los tipos de factores que influyen en el rendimiento de una red. Tecnológica porque al realizar esta investigación podremos identificar, describir y determinar el nivel de influencia de los parámetros de calidad servicio que afectan el rendimiento de la red de la Corte Superior de Justicia de la Libertad.

1.7.2. VIABILIDAD DE LA INVESTIGACIÓN

En esta investigación es factible contar con el permiso y aprobación para acceder a la información que el jefe del departamento de informática de la corte superior de justicia de la libertad nos brinde, así como el acceso a la red a través de puntos en un router o switch local para su análisis.

Así mismo se cuenta con el aporte y disposición de los recursos humanos y operatividad, prestos a realizar pruebas, encuestas o entrevistas necesarias para el análisis de la investigación.

1.8. LIMITACIONES DEL ESTUDIO

El análisis y evaluación de los parámetros de calidad de servicio QoS de la Corte Superior de Justicia de La Libertad está limitada a las distintas restricciones y usos de algunos dispositivos de red como router que se encuentra en la sala del servidor, un área totalmente restringida a cualquier persona que no pertenezca al departamento de informática, también al tiempo y uso de la red para realizar las pruebas, que fueron efectuadas en tres fases con periodos de tiempo moderados, debido a que las personas del departamento de informática siempre se encuentran ocupados debido a las distintas audiencias programadas y los distintos problemas existentes a nivel tanto de hardware como software en las muchas áreas en la sede judicial de Natasha, el limitado tiempo del encargado del departamento de informática ya que para en constante movimiento entre las sedes de la libertas y aledaños, y su permiso para poder utilizar las instalaciones para realizar las pruebas.

CAPÍTULO
II
MARCO TEÓRICO

2 MARCO TEÓRICO

2.1. ANTECEDENTES

Molina (2012), en su investigación "PROPUESTA DE SEGMENTACIÓN CON REDES VIRTUALES Y PRIORIZACIÓN DEL ANCHO DE BANDA CON QOS PARA LA MEJORA DEL RENDIMIENTO Y SEGURIDAD DE LA RED LAN EN LA EMPRESA EDITORA EL COMERCIO PLANTA NORTE.", se propuso como objetivos: Identificar que la velocidad o tasa de transferencia de datos en horas pico denotaba 3 Mbps frente a 8.5 Mbps como indicador actual de la red. Para así poder determinar que el ancho de banda disponible en horas críticas no era suficiente para soportar el flujo masivo de información en tiempo real (400 Mbps) por lo que la implementación de estrategias QoS ha permitido la mejora sustancial de la velocidad en la red LAN. Su estudio concluyo que la proyección de crecimiento de la Planta Norte es de 16% anual, donde actualmente se cuenta con 50 terminales. Se implementó y configuró la red para soportar este promedio de crecimiento sin afectar el rendimiento de la Lan, gracias a los lineamientos de la metodología adoptada. Con lo que es posible conectar otros switch Cisco de 48 puertos hacia el swicth Core y responder a la tasa de crecimiento, con una velocidad de 100/1000 Gbps en cada troncal. Con ello concluimos que el objetivo de la Escalabilidad fue posible.

La velocidad o tasa de transferencia de datos está operando dentro de los rangos esperados, gracias a la implementación de técnicas de balanceo y priorización de tráfico con QoS, el cual se configuró en los dispositivos que consumen mayor ancho de banda (Teléfonos IP, Pc's periodistas y prensa),identificándose tipos de paquetes (Voz, Datos y Video) para reservar un ancho de banda de origen a destino donde los equipos detectan el tráfico de datos relevantes y lo gestionan con mayor prioridad

(Video y Voz). Asimismo, se implementó mejoras físicas para reforzar la implementación lógica, como es el uso de LACP (Enlaces agregados) entre los switch principales y secundarios, multiplicando el ancho de banda en una proporción de 1 a 4, logrando de esta manera cumplir con el objetivo deseado.

Gonzales y Correa (2010) en su investigación "ESTUDIO DEL TRÁFICO DE RED Y ANCHO DE BANDA EN DIVERSOS PUNTOS CRITICOS DE LA RED DEL CAMPUS DE LA UNIVERSIDAD CENTROAMERICANA MANAGUA-NICARAGUA ENTRE SEPTIEMBRE A NOVIEMBRE DE 2010", se propusieron como objetivos: Analizar el estado actual del cableado estructurado de los IDF del campus para determinar el grado de cumplimiento en relación a las normas ANSI / TIA / EIA568 B y ANSI / TIA / EIA 569 A.

Identificar los problemas que se presentan en el tráfico de la red a nivel de las capas 2 y 3 del modelo OSI, empleando herramientas de análisis de tráfico y de protocolos.

Señalar las posibles anomalías referentes al ancho de banda a nivel de capa de aplicación del modelo OSI con el fin de proponer soluciones que contribuyan a optimizar el ancho de banda y mejorar la calidad de los servicios. Su estudio concluyo que en algunos IDF el nivel de cumplimiento de las normas ANSI/TIA/EIA 568 B y 569 A es alto. En contraste en otros es necesario mejorar la protección del cableado horizontal y de los equipos de comunicación al igual que la organización, etiquetado de los cables y espacios mínimos. Existe gran diversidad de protocolos presente en la red entre los cuales se pueden mencionar ARP, AARP, IPX, NetBios/NetBEU, SPX, SAP, Molp, entre otros. Algunos protocolos como IPX y SPX no son necesarios en los equipos clientes.

La principal anomalía referente al tráfico de red a nivel de capa 2 y 3 el modelo OSI es el excesivo broadcast ocasionado por la poca segmentación lógica de la red. Las cámaras de video vigilancia IP al igual que varias impresoras generan gran cantidad de tormentas de difusión en la red, lo que se traduce en la generación de gran cantidad de tráfico, la degradación del rendimiento en la red y la calidad de los servicios. No existen políticas y normas referentes al ancho de banda internacional, lo cual se traduce en una inadecuada gestión de este valioso recurso.

Torres (2003), en su investigación "ANÁLISIS Y PROPUESTA DE UN ESQUEMA DE CALIDAD DE SERVICIO (QoS) PARA LA RED DE LA UNIVERSIDAD DE COLIMA", se propuso como objetivos: Proponer un esquema de Calidad de Servicio para la red de la Universidad de Colima, mediante el análisis de las arquitecturas de QoS factibles para aplicarse a este entorno y el estudio de las prestaciones de los equipos de red de la dorsal. Realizar estudio de los antecedentes de la Red de la Universidad de Colima. Realizar estudio de las arquitecturas de Calidad de Servicio (QoS). Realizar estudio de los diferentes equipos de comunicación de la dorsal Universitaria. Llegar a la propuesta de esquema de Calidad de Servicio (QoS). Implementación de la propuesta. Analizar resultados. Su estudio concluyo que, como parte del análisis, se concluye que los enrutadores de la dorsal Universitaria tienen soporte total para Servicios diferenciados (DiffServ), lo que hace factible la aplicación de Calidad de Servicio dentro de la dorsal de la Universidad de Colima: lo que no garantiza tener Calidad de Servicio es fuera de su dorsal Universitaria, debido a que Telmex no se compromete a proveer algún esquema de Calidad de Servicio en particular.

Los equipos de PacketShaper por su capacidad de capa 7, lo hace más accesible para manejar capacidades de ancho de banda de hasta lOOMbps. actualmente empleado para el enlace de 34 Mbps hacia Internet, y cuya configuración proporciona calidad de servicios a aplicaciones críticas.

La arquitectura de servicios integrados, a pesar de ser soportados en los equipos SSR 8000 y SSR 8600. no se encuentra disponible al 100% en la versión de firmware de los equipos. Además, es necesario que la totalidad de equipos de la dorsal cumplan con esta arquitectura para tomarla en cuenta como opción.

Prado (2009), en su investigación "IMPLANTACIÓN DE CALIDAD DE SERVICIO (QoS) EN REDES INALÁMBRICAS", se propuso como objetivo central hacer un estudio de la manera en que se gestiona el rendimiento de los servicios que brindan las redes inalámbricas basadas en la tecnología Wi-Fi, a través de la implantación de Calidad de Servicio (QoS) en una red empresarial: asimismo su necesidad, las variables que habitualmente se usan para definirla, las técnicas y herramientas usadas para evaluarla y cómo se aplica este conocimiento a dichas redes. Particularmente, y bajo los mismos términos, se hará un estudio del estándar 802.1 le. de las razones y ventajas de utilizar la funcionalidad WMM en los dispositivos Wi-Fi. y de igual modo una comparación del impacto que tiene QoS sobre Wi-Fi con una red cableada. Su investigación concluyo que varias son las causas que explican la proliferación imparable de las redes Wi-Fi: su versatilidad y economía, la existencia de hardware comercial accesible, la distribución masiva de routers Wi-Fi con accesos a Internet. ADSL. etc. En el momento presente asistimos también a la aparición de nuevos modelos de negocio - muchos de ellos aún sin consolidar que tratan de ofrecer una alternativa de servicio al operador tradicional de redes celulares.

No obstante, la adopción de estas tecnologías, como siempre, no ha sido fácil y esto se debe a la situación de nuestro entorno, donde sabemos bien que existe un rezago tecnológico y sumado a que no somos fabricantes sino sólo consumidores, pero el paso del tiempo y la coyuntura tecnológica que se va teniendo, hace que este tipo de redes se estén implementando. ahora sí. en muchos lugares. Con el avance tecnológico cada vez mayor, se presentan nuevos desafíos, la mejora continua de múltiples servicios que actualmente ya se disponen en todo el mundo a nivel telecomunicaciones es impresionante, no es simplemente el hecho de dar un servicio, sino que éste sea de una calidad confiable y no tenga limitantes o defectos en el uso del mismo.

2.2. BASES TEÓRICAS

A) PROTOCOLOS DE RED

Los protocolos con más presencia y su efecto a la hora de realizar las pruebas son:

- ARP (Address Resolution Protocol).
- DHCPv6 (Dynamic Host Configuration Protocol for IPv6).
- HSRP (Cisco Hot Standby Router Protocol).
- ICMP (Internet Control Message Protocol).
- ICMPv6 (Internet Control Message Protocol for IPv6).
- LLMNR (Link-Local Multicast Name Resolution).
- TCP (Transmission Control Protocol).
- UDP (User Datagram Protocol).

a. PROTOCOLO ARP

El “protocolo de resolución de direcciones” es responsable de convertir las direcciones de protocolo de alto nivel (direcciones IP) a direcciones de red físicas. Para hacer esto, ha de estar estrechamente relacionado con el manejador de dispositivo de red. Si una aplicación desea enviar datos a una determinado dirección IP de destino, el mecanismo de encaminamiento IP determina primero la dirección IP del siguiente salto del paquete (que puede ser el propio host de destino o un "router") y el dispositivo hardware al que se debería enviar. (RFC 826).

b. PROTOCOLO DHCPv6

El funcionamiento del DHCPv6 empieza en el momento en el que el cliente escucha en el puerto 546 y los transmisores escuchan en el puerto 547, estos se comunican por medio de una liga local y direcciones multicast, entonces se puede decir que básicamente como se trabaja en este protocolo en un caso simple es de la siguiente manera:

- Un cliente envía una solicitud (SOLICIT) para encontrar servidores y dichos servidores están enviando mensajes indicando que están disponibles para el servicio (ADVERTISE),
- Luego un cliente envía una solicitud para pedir los parámetros de configuración, (por ejemplo, direcciones IPv6, prefijos IPv6, DNS, NIS, etc.…) a los servidores con prioridad (REQUEST), dichos servidores son asignados según el administrador, para luego el servidor envíe una respuesta (REPLAY) con los permisos a las direcciones y a la información de

configuración, si no responde, sigue buscando por orden de valoración hasta que se quede sin solicitudes, es cuando reinicia su búsqueda. (RFC 3315).

c. PROTOCOLO HSRP

El Hot Standby Router Protocol es un protocolo propiedad de CISCO que permite el despliegue de routers redundantes tolerantes a fallos en una red. Este protocolo evita la existencia de puntos de fallo únicos en la red mediante técnicas de redundancia y comprobación del estado de los routers. Es un protocolo muy similar a VRRP, que no es propietario. Es por ello que CISCO reclama que VRRP viola una serie de patentes que le pertenecen. (RFC 2281).

d. PROTOCOLO ICMP

El protocolo ICMP permite administrar información relacionada con errores de los equipos en red. Si se tienen en cuenta los escasos controles que lleva a cabo el protocolo IP, ICMP no permite corregir los errores, sino que los notifica a los protocolos de capas cercanas. Por lo tanto, el protocolo ICMP es usado por todos los routers para indicar un error (llamado un problema de entrega). (RFC 0792).

e. PROTOCOLO ICMPv6

ICMPv6 es un protocolo de propósito múltiple y está diseñado para realizar funciones tales como detectar errores encontrados en la interpretación de paquetes, realizar diagnósticos, realizar funciones como Neighbor Discovery y detectar direcciones IPv6 multicast. Por esta razón, los mensajes ICMPv6 están subdivididos en dos clases: mensajes de error y mensajes informativos. Los

mensajes ICMPv6 son enviados dentro de paquetes IPv6 los cuales a su vez pueden llevar las extensiones de cabecera de IPv6.

El protocolo ICMPv6 es utilizado por los nodos IPv6 para detectar errores encontrados en la interpretación de paquetes y para realizar otras funciones de la capa de internet como el diagnóstico (ICMPv6 ping) (RFC 2463).

f. PROTOCOLO LLMNR

El protocolo Link-Local Multicast Name Resolution (LLMNR) resuelve los nombres de los sistemas informáticos cercanos, si la red no tiene un servidor de Sistema de nombres de dominio (DNS). La función LLMNR Responder funciona en el entorno IPv4 o IPv6 cuando se utiliza un sistema que tiene la función Emisor LLMNR como Windows. (RFC 4795).

g. PROTOCOLO TCP

Durante una comunicación usando el protocolo TCP, las dos máquinas deben establecer una conexión. La máquina emisora (la que solicita la conexión) se llama cliente, y la máquina receptora se llama servidor. Por eso es que decimos que estamos en un entorno Cliente-Servidor. Las máquinas de dicho entorno se comunican en modo en línea, es decir, que la comunicación se realiza en ambas direcciones. Para posibilitar la comunicación y que funcionen bien todos los controles que la acompañan, los datos se agrupan; es decir, que se agrega un encabezado a los paquetes de datos que permitirán sincronizar las transmisiones y garantizar su recepción.

Otra función del TCP es la capacidad de controlar la velocidad de los datos usando su capacidad para emitir mensajes de tamaño variable. Estos mensajes se llaman segmentos. (RFC 793).

h. PROTOCOLO UDP

User Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 o de Transporte del Modelo OSI). 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. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos. (RFC 768).

i. PROTOCOLO SSDP

SSDP es un protocolo basado en texto basado en HTTPU. Utiliza el protocolo de datagramas de usuario (UDP) como el protocolo de transporte subyacente. Los servicios son anunciados por el sistema de alojamiento con dirección de multidifusión a una dirección de multidifusión IP específicamente designada en el puerto UDP número 1900. En IPv4, la dirección de multidifusión es

239.255.255.250 [4] y SSDP en IPv6 utiliza la dirección establecida ff0X:: c para todos rangos de alcance indicado por X .

Esto da como resultado las siguientes direcciones de multidifusión prácticas conocidas para SSDP:

- 239.255.255.250 (dirección local del sitio IPv4)
- [FF02 :: C] (IPv6 link-local)
- [FF05 :: C] (IPv6 site-local)
- [FF08 :: C] (organización IPv6 local)
- [FF0E :: C] (IPv6 global)

SSDP usa el método HTTP NOTIFY para anunciar el establecimiento o retiro de información de servicios (presencia) al grupo de multidifusión. Un cliente que desea descubrir servicios disponibles en una red utiliza el método M-SEARCH. Las respuestas a tales solicitudes de búsqueda se envían a través del direccionamiento de unidifusión a la dirección de origen y al número de puerto de la solicitud de multidifusión. (RFC 2119).

B) RED LAN

Definición: Las redes de área local, generalmente llamadas LAN (Local Area Networks), son redes de propiedad privada que operan dentro de un solo edificio, como una casa, oficina o fábrica. Las redes LAN se utilizan ampliamente para conectar computadoras personales y electrodomésticos con el fin de compartir recursos (por ejemplo, impresoras) e intercambiar información. Cuando las empresas utilizan redes LAN se les conoce como redes empresariales.

Las redes LAN son muy populares en la actualidad, en especial en los hogares, los edificios de oficinas antiguos, las cafeterías y demás sitios en donde es muy problemático instalar cables. En estos sistemas, cada computadora tiene un módem y una antena que utiliza para comunicarse con otras computadoras.

En la mayoría de los casos, cada computadora se comunica con un dispositivo en el techo, este dispositivo se le denomina AP (Punto de Acceso, del inglés Access Point), enrutador inalámbrico o estación base; transmite paquetes entre las computadoras inalámbricas y también entre éstas e Internet. El AP es como el niño popular de la escuela, ya que todos quieren hablar con él. Pero si hay otras computadoras que estén lo bastante cerca una de otra, se pueden comunicar directamente entre sí en una configuración de igual a igual. (Tanenbaum 5ªE, 2012, p. 17)

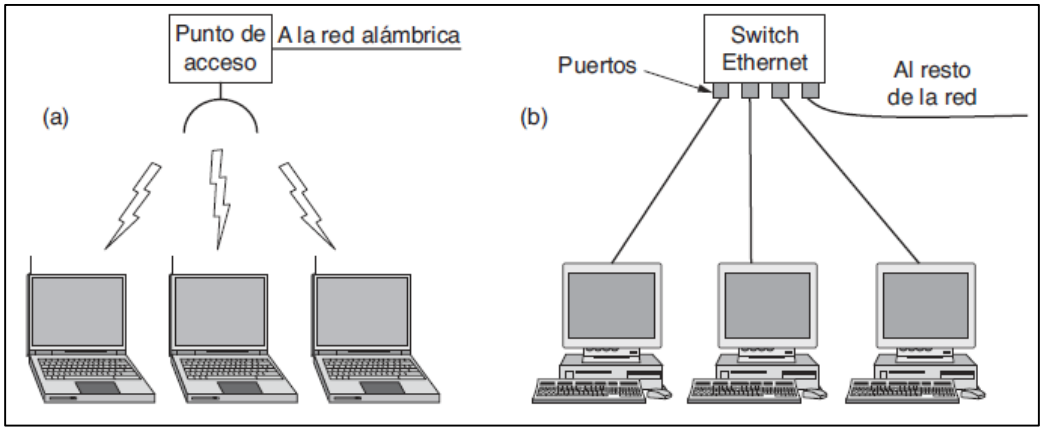


Figura 4: **Redes inalámbrica y alámbrica. (a) 802.11. (b) Ethernet conmutada.**
Fuente: **Tanenbaum, 5ª Edición 2012, p17**

Estándares: La topología de muchas redes LAN alámbricas está basada en los enlaces de punto a punto. El estándar IEEE 802.3, comúnmente conocido como Ethernet, es hasta ahora el tipo más común de LAN alámbrica. Cada computadora se comunica mediante el protocolo Ethernet y se conecta a una caja conocida como switch con un enlace de punto a punto. Un switch tiene varios

puertos, cada uno de los cuales se puede conectar a una computadora. El trabajo del switch es transmitir paquetes entre las computadoras conectadas a él, y utiliza la dirección en cada paquete para determinar a qué computadora se lo debe enviar. (Tanenbaum 5ªE, 2012, p. 18)

Beneficios: También es posible dividir una gran LAN física en dos redes LAN lógicas más pequeñas. Tal vez se pregunte por qué sería esto útil. En ocasiones la distribución del equipo de red no coincide con la estructura de la organización. Por ejemplo, los departamentos de ingeniería y finanzas de una empresa podrían tener computadoras en la misma LAN física debido a que se encuentran en la misma ala del edificio, pero podría ser más sencillo administrar el sistema si cada departamento tuviera su propia red lógica, denominada LAN virtual o VLAN. En este diseño cada puerto se identifica con un "color"; por ejemplo, verde para ingeniería y rojo para finanzas. Después el switch reenvía los paquetes de manera que las computadoras conectadas a los puertos verdes estén separadas de las que están conectadas a los puertos rojos. Por ejemplo, los paquetes de difusión que se envíen por un puerto rojo no se recibirán en un puerto verde, tal como si hubiera dos redes LAN distintas. (Tanenbaum 5ªE, 2012, p. 18)

Componentes: Estos dispositivos son conectados físicamente a la red usando una Network Interface Card (NIC) que tiene su propio código o dirección MAC. La segunda clasificación son los dispositivos de red.

Los dispositivos de red proveen la comunicación entre dispositivos de usuario final. Como, por ejemplo: (Molina, 2012, p. 18).

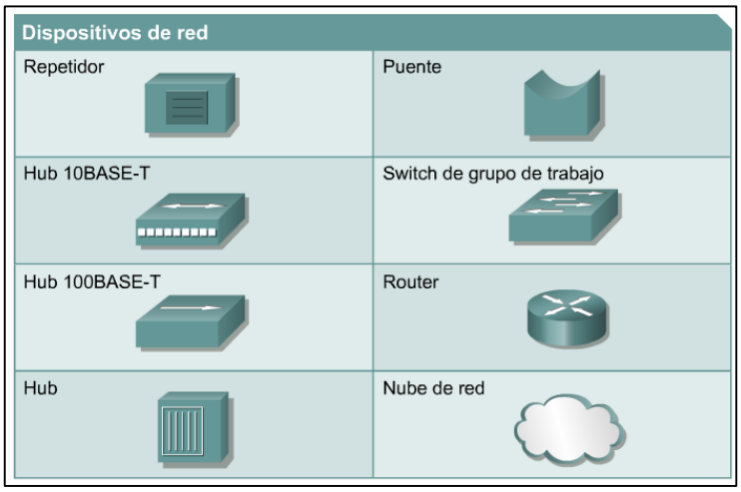


Figura 5: **Dispositivos De Red**
Fuente: **Cisco CCNA 1 - Modulo 2**

a). **Repetidor:** Es un dispositivo de red usado para regenerar una señal. Regeneran señales analógicas o digitales distorsionadas por la pérdida de transmisión debido a la atenuación. Es un dispositivo de capa 1. (Molina, 2012, p. 18)

b). **Hub:** Dispositivo de capa 1 que permite la concentración de varios dispositivos dentro de un solo dominio de colisión o segmento. Regenera y amplifica las señales de datos para todos los dispositivos conectados, excepto para el dispositivo que originalmente envió la señal. También es conocido como un repetidor multipuerto, que extiende los dominios de colisión. (Molina, 2012, p. 18)

c). **Bridge:** Es un dispositivo de capa 2 que separa dominios de colisión, porque analiza las direcciones MAC para determinar si las tramas de datos pueden o no cruzar entre dos segmentos de red. Para lograr esto, el bridge aprende las direcciones MAC de los dispositivos en cada segmento conectado. Además, este dispositivo puede convertir formatos de transmisión de datos, lo cual no puede realizar un switch de capa 2. (Molina, 2012, p. 18)

d). **Switch:** Andrew s. Tanenbaum- 4ta. Ed. (2003). Menciona que es un dispositivo de capa 2 y puede ser referido como un bridge multipuerto. Los switches toman las decisiones de envío basadas en las direcciones MAC contenidas dentro de la trama de datos transmitidas.

Los switches aprenden las direcciones MAC de los dispositivos conectados a cada puerto, a través de la lectura de las direcciones MAC origen que se encuentran en las tramas que ingresan al switch, luego esta información es ingresada dentro de la tabla de conmutación que es almacenada en la CAM. Los switches crean un circuito virtual entre dos dispositivos conectados que quieren comunicarse. Cuando este circuito virtual ha sido creado, un camino de comunicación dedicado es establecido entre los dos dispositivos. Esto crea un ambiente libre de colisiones entre el origen y el destino lo cual implica la máxima utilización del ancho de banda disponible.

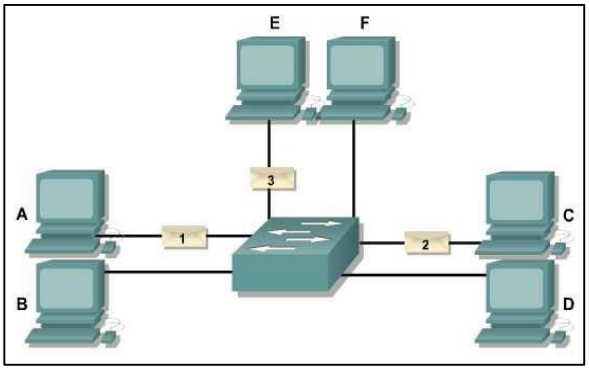


Figura 6: **Transmisiones Simultáneas en un Switch**
Fuente: **http://www.cisco.com/web/learning/netacad**

Cada puerto del switch representa un solo dominio de colisión, lo cual se conoce como microsegmentación. La desventaja de todos los dispositivos de capa 2, es que ellos envían tramas broadcast a todos los dispositivos conectados a sus puertos. (Molina, 2012, p. 19)

e). **Router:** Cisco Networkers Solutions Forum (2006). Se define como dispositivo de capa 3 que toma decisiones basadas en direcciones de red. Estos utilizan tablas de enrutamiento para almacenar estas direcciones de capa 3. Los routers se encargan de elegir el mejor camino para enviar los datos a su destino y conmutar o enrutar los paquetes al puerto de salida adecuado.

Los routers dividen tanto dominios de broadcast como dominios de colisión. Además, son los dispositivos de mayor importancia para regular el tráfico, porque proveen políticas adicionales para la administración de la red con filtrado de paquetes para la seguridad. También dan acceso a redes de área amplia (Wan), las cuales están destinadas a comunicar o enlazar redes de área local (Lan's) que se encuentran separadas por grandes distancias. (Molina, 2012, p. 19,20).

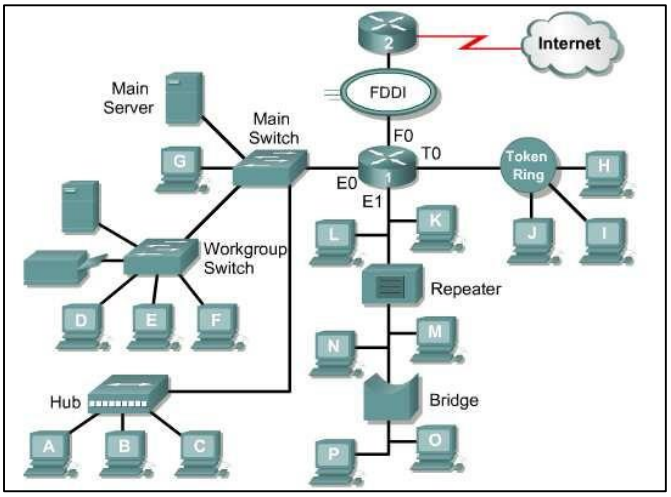


Figura 7: **Ejemplo de la Interconexión de Dispositivos de Red**
Fuente: **Cisco CCNA 1 - Modulo 2**

f). **Red Plana:** Unisys, en una investigación realizada junto al Ponemon Institute, descubrió que casi el 70% de las organizaciones de infraestructura crítica encuestadas informaron haber sufrido al menos una violación de seguridad debido a que contaban con una red plana lo que provocó la pérdida de información confidencial o la interrupción de operaciones durante los últimos 12 meses.

Los ciber-criminales colocan cada vez más su atención en las redes de los bancos – en datos en movimiento – para aprovecharse de los tesoros lucrativos de información que circulan dentro del banco (entre sucursales y centros de datos, entre empleados) y fuera del banco (hacia y desde proveedores, Reserva Federal, clientes, bancos beneficiarios, comerciantes, reguladores, y más).

Ventajas:

- Reduce la complejidad de la configuración y el número de dispositivos que deben ser gestionados.
- Disminuye el costo de mantenimiento.
- Aceleran su capacidad de realizar cambios (lo que no es una ventaja despreciable en el mercado competitivo de hoy en día).
- Reducido la latencia al hacer más eficiente el tráfico entre fuente y destino.

Desventajas:

- Vulnerable a ataques y visibilidad de la información que de otra manera los usuarios legítimos no tendrían derecho a ver.
- Estas redes planas comúnmente fallan a la hora de segregar la información, de manera que los atacantes pueden ver todos los puntos finales de los datos en movimiento y potencialmente acceder a cada sistema involucrado, causando mucho daño. (http://www.emb.cl/gerencia/articulo.mvc?xid=3692&sec=3)

g). Dominio de Colisión. - Un dominio de colisión en ethernet, el área de la red dentro del cual las tramas que ha sufrido colisiones se propagan los repetidores y los hubs propagan las colisiones; los switches Lan, los puentes y los routers no.

El área de red donde se originan las tramas y se producen las colisiones se denomina dominio de colisiones. Todos los entornos de los medios compartidos, como aquellos creados mediante el uso de hubs, son dominios de colisión. Cuando un host se conecta a un puerto de switch, el switch crea una conexión dedicada. Esta conexión se considera como un dominio de colisiones individual, dado que el tráfico se mantiene separado de cualquier otro y, por consiguiente, se eliminan las posibilidades de colisión.

Los switches reducen las colisiones y permiten una mejor utilización del ancho de banda en los segmentos de red, ya que ofrecen un ancho de banda dedicado para cada segmento de red. (CISCO_CCNA/Exploration3intSpanish)

h). Dominio de Broadcast: Es un conjunto de todos los dispositivos que reciben tramas de broadcast que se originan en cualquier dispositivo del conjunto. Los conjuntos de broadcast generalmente están limitados por routers dado que los router no envían tramas de broadcast. Si bien los switches filtran la mayoría de las tramas según las direcciones MAC, no hacen lo mismo con las tramas de broadcast. Para que otros switches de la LAN obtengan tramas de broadcast, éstas deben ser reenviadas por switches. Una serie de switches interconectados forma un dominio de broadcast simple. Sólo una entidad de Capa 3, como un router o una LAN virtual (VLAN), puede detener un dominio de broadcast de Capa 3. Los routers y las VLAN se utilizan para segmentar los dominios de colisión y de broadcast. Cuando un switch recibe una trama de broadcast la reenvía a cada uno de sus puertos excepto al puerto entrante en el que el switch recibió esa trama. Cada dispositivo conectado reconoce la trama de broadcast y la procesa. Esto provoca una disminución en la eficacia de la red dado que el ancho de banda se utiliza para

propagar el tráfico de broadcast. Cuando se conectan dos switches, el dominio de broadcast aumenta. (CISCO_CCNA/Exploration3intSpanish)

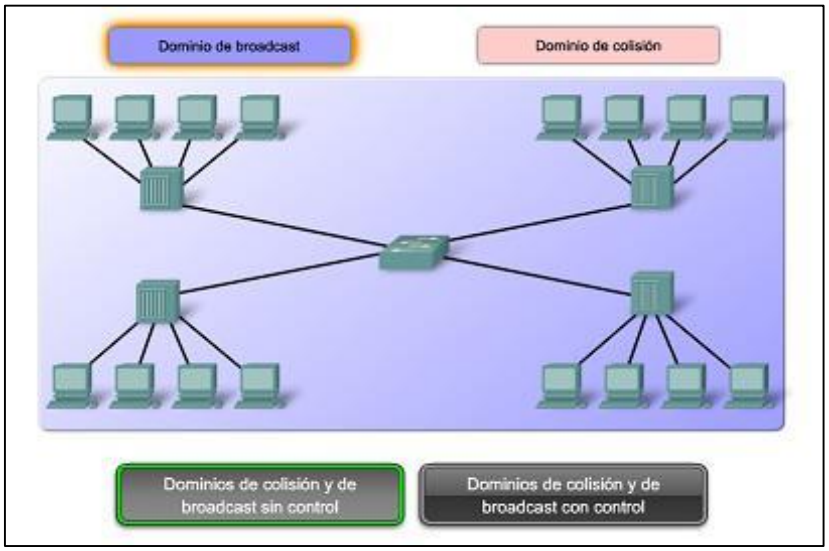


Figura 8: **Dominio de Broadcast sin control**
Fuente: **CISCO_CCNA/Exploration3intSpanish**

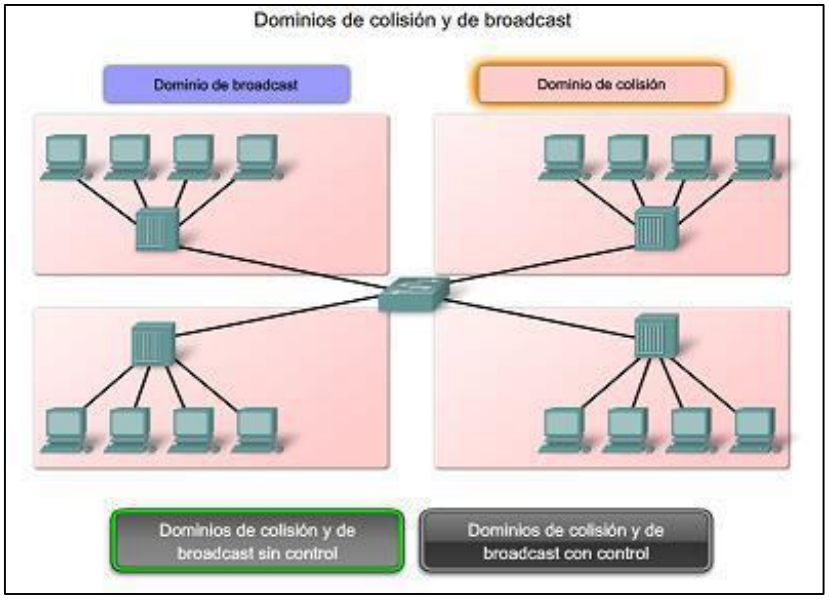


Figura 9: **Dominio de Broadcast sin control**
Fuente: **CISCO_CCNA/Exploration3intSpanish**

i). Segmentación de Red: La segmentación de la red consiste en separar una red en varias redes diferentes, apoyándonos en las propiedades que tienen las redes privadas y mediante la utilización de dispositivos físicos o lógicos que se tienen

desarrollados para este fin. (Segmentación de la red de la biblioteca central de la UNAM, 2010, p.59)

j). Congestión de Red: Cuando hay demasiados paquetes presentes en una red (o en una parte de ella), hay retardo o pérdida en los paquetes y se degrada el desempeño. Esta situación se llama congestión. Las capas de red y de transporte comparten la responsabilidad de manejar la congestión. Como ésta ocurre dentro de la red, la capa de red es quien la experimenta en forma directa y en última instancia debe determinar qué hacer con los paquetes sobrantes. Sin embargo, la manera más efectiva de controlar la congestión es reducir la carga que la capa de transporte coloca en la red. Para ello se requiere que las capas de red y de transporte trabajen en conjunto.

Cuando la cantidad de paquetes que el host envía a la red está muy por debajo de su capacidad de transporte, la cantidad entregada es proporcional a la cantidad enviada. Si se envía el doble de paquetes, se entrega el doble de ellos. Sin embargo, a medida que la carga ofrecida se acerca a la capacidad de transporte, las ráfagas de tráfico llenan ocasionalmente los búferes dentro de los enrutadores y se pierden algunos paquetes. Estos paquetes perdidos consumen una parte de la capacidad, por lo que la cantidad de paquetes entregados cae por debajo de la curva ideal. Ahora la red está congestionada. (Tanenbaun 5° Edición, 2012, p. 337)

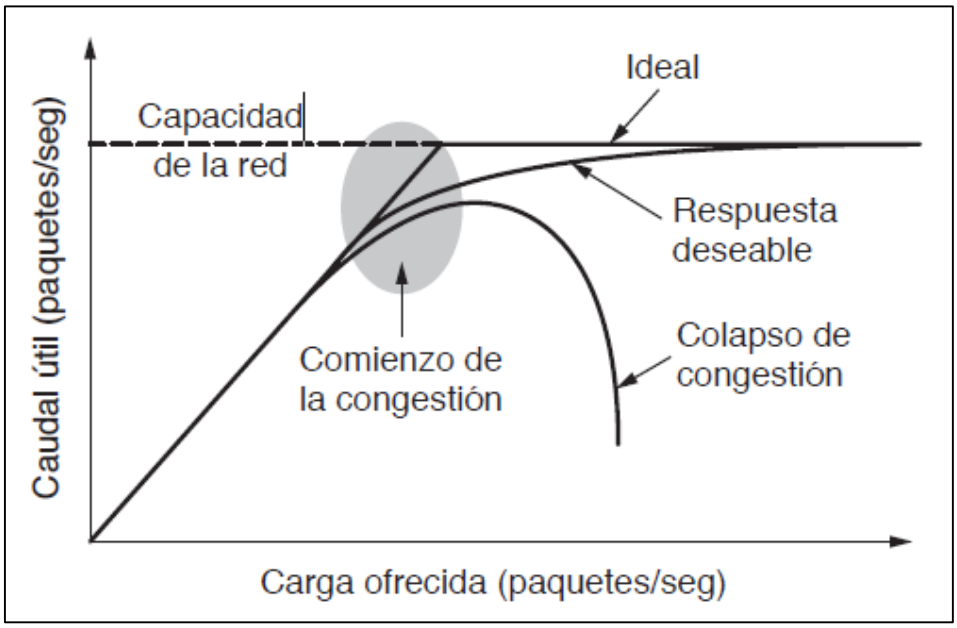


Figura 10: **Comienzo de la congestión**
Fuente: **Tanenbaun 5° Edición**

k). Rede Ethernet: Ethernet o su estándar equivalente IEEE 802.3, es básicamente una tecnología de transmisión Broadcast, donde los dispositivos como computadoras, impresoras, servidores de archivos, etc.; se comunican sobre un medio de transmisión compartido, lo que quiere decir que ellos se encuentran en una continua competencia por el ancho de banda disponible. Por lo tanto, las colisiones son una natural ocurrencia en redes Ethernet y pueden llegar a ser un gran problema.

La entrega de tramas de datos Ethernet es de naturaleza Broadcast. Ethernet usa el método CSMA/CD (Acceso Múltiple Sensible a Portadora con Detección de Colisión), que le permite a una sola estación transmitir, y puede soportar tasas de transmisión de alta Carrier Sense Multiple Access / Collision Detection velocidad, como: Ethernet: 10 Mbps, Fast Ethernet: 100 Mbps, Gigabit Ethernet: 1000 Mbps y 10-Gigabit Ethernet: 10,000 Mbps.

El desempeño de un medio compartido ethernet/802.3 puede ser negativamente afectado por factores como: las aplicaciones multimedia con alta demanda de

ancho de banda tales como video e Internet, que junto con la naturaleza broadcast de Ethernet, pueden crear congestión en la red; y la latencia normal que adquieren las tramas por viajar a través de los medios de red, atravesar dispositivos de red y los propios retardos de las NICs. (Molina, 2012, p. 22).

l). Broadcast Y Multicast: Para comunicarse con todos los dominios de colisión, los protocolos usan tramas broadcast y multicast en la capa 2 del modelo OSI. Por lo tanto, si un nodo necesita comunicarse con todos los hosts en la red, éste envía una trama broadcast con una dirección MAC de destino 0xFFFFFFFFFFFF. Esta es una dirección a la cual todas las tarjetas NIC deben responder.

La acumulación de tráfico broadcast y multicast de cada dispositivo de la red es referido como: radiación de broadcast, cuya circulación puede saturar la red, es decir que no hay ancho de banda disponible para aplicaciones de datos, resultando en la caída de estas conexiones, situación conocida como una tormenta de broadcast. (Molina, 2012, p. 22).

m). Causas de Broadcast y Multicast: Existen varias fuentes de broadcast y multicast en redes IP, estas pueden ser: las estaciones de trabajo, los routers, las aplicaciones multicast, el protocolo DHCP, etc. Las estaciones de trabajo envían broadcast de pedidos ARP (Protocolo de Resolución de Direcciones), cada vez que ellos necesitan localizar una dirección MAC que no está en su tabla ARP. Las tormentas de broadcast pueden ser causadas por el pedido de información de un dispositivo dentro de una red que ha crecido mucho. Las aplicaciones multicast, particularmente las aplicaciones de paquetes de video pueden generar una cadena

de siete megabytes de datos multicast, que en una red conmutada podría ser enviada a cada segmento, resultando en una severa congestión.

Otra fuente generadora de broadcast es el protocolo DHCP cuando un cliente DHCP usa un pedido de broadcast para localizar el servidor DHCP. Además, estos clientes por lo general repiten este pedido después de un relativo corto "timeout", posiblemente debido a una respuesta lenta del servidor, lo que producen las conocidas tormentas de broadcast; que a su vez producen retardos anormales de otros tráficos cliente / servidor, los cuales también pueden empezar a retransmitir. (Molina, 2012, p. 23).

n). DEFINICIÓN DE CALIDAD DE SERVICIO (QOS): QoS hace referencia a la capacidad de una red para proporcionar diferentes niveles de servicio al tráfico de red en diversas tecnologías. Los objetivos principales de QoS es el ancho de banda dedicado, controlar el jitter y la latencia (requerido por algunos servicios en tiempo real y el tráfico interactivo) y la pérdida de características mejoradas.

Las técnicas de trabajo en la congestión de una red se utilizan para administrar y priorizar el tráfico en una Lan donde las aplicaciones solicitan más ancho de banda y que la red no es capaz de proporcionar. Al dar prioridad a ciertas clases de tráfico, estas técnicas permiten a las empresas retrasar las aplicaciones sensibles para que funcionen correctamente en una red congestionada.

o). QoS: Se puede dividir en tres niveles diferentes. Estos modelos de servicio se pueden describir en un conjunto de capacidades QoS de extremo a extremo.

- **QoS extremo a extremo,** es la habilidad de la red para proporcionar un nivel específico de servicio de tráfico de un extremo a otro de la red. Los tres niveles

de servicio son: El de mejor esfuerzo de servicio, servicio integrado y servicio diferenciado.

- Mejor esfuerzo de servicio, como su nombre lo indica, es cuando la red hará todo lo posible para entregar el paquete del servicio a su destino. Con el mejor esfuerzo no hay garantías de que el paquete alcance su rumbo.
- Modelo de servicio integrado, permite a las aplicaciones tener un nivel de servicio garantizado mediante la negociación de parámetros de red de extremo a extremo. Las aplicaciones pueden solicitar un nivel de servicio necesario para que funcionen correctamente y confiar en el mecanismo de calidad de servicio para reservar los recursos de red necesarios antes de que se inicie la transmisión de los paquetes de la aplicación. Es importante señalar que la aplicación no envía algún tipo de tráfico hasta que reciba una señal de la red la cual le indica que la red puede manejar la carga y entregar a su destino un QoS.
- **Modelo de servicios diferenciados**. El cual incluye un conjunto de herramientas de clasificación y gestión de colas para la prestación de algunos protocolos o aplicaciones con una cierta prioridad sobre el tráfico de la red. Los servicios diferenciados se basan en los routers de extremo para realizar la clasificación de los diferentes tipos de paquetes que pasan por una red.

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 manera distinta 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. El tráfico PTZ, que a menudo 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. (Molina, 2012, p. 35).

QoS	Prioridad	Descripción de las clases de servicios
Voz	Real Time	Tráfico Multimedia Voz sobre IP
Video	Video	Tráfico Video: Video Conferencia, Video sobre demanda, Vidoe "Broadcast"
Datos	Platino	Tráfico Datos Alta Prioridad: SNA, SAP, Aplicaciones muy Criticas
	Oro	Tráfico Datos Media Prioridad: Aplicaciones críticas, LAN to LAN, e-mail
	Plata	Tráfico de Datos baja prioridad: Intranet
	Bronce	Tráfico de Datos Best Effort: Internet

Tabla 2: **Priorización de QoS**
Fuente: **https://en.wikipedia.org/wiki/Main_Page**

p). RED SIN QoS: En este ejemplo, PC1 está reproduciendo dos secuencias de vídeo de las cámaras 1 y 2. Cada cámara transmite a 2,5 Mbit/s. De repente, PC2 inicia una transferencia de archivos desde PC3.

En este escenario, la transferencia de archivos intentará utilizar la capacidad total de 10 Mbit/s entre los enrutadores 1 y 2, mientras que las secuencias de vídeo intentarán mantener su total de 5 Mbit/s. Así, ya no se puede garantizar la cantidad de ancho de banda destinada al sistema de vigilancia y probablemente se reducirá la frecuencia de imagen de vídeo. En el peor de los casos, el tráfico del FTP consumirá todo el ancho de banda disponible. (Molina, 2012, p. 37).

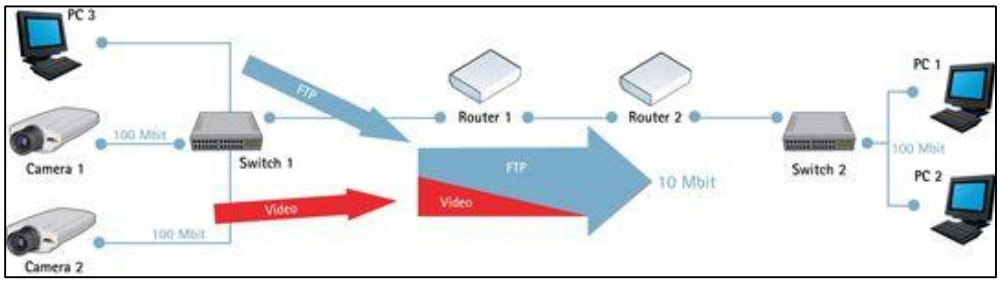


Figura 11: **Gráfica Sin Aplicación De QoS**
Fuente: **http://www.axis.com/**

q). RED CON QoS: En este escenario, se ha configurado el enrutador 1 para dedicar hasta 5 Mbit/s de los 10 disponibles a la transmisión de vídeo. El tráfico del FTP puede utilizar un máximo de 2 Mbit/s, y HTTP, junto con el resto del tráfico, pueden utilizar un máximo de 3Mbit/s. Con esta división, las transmisiones de vídeo siempre tendrán disponible el ancho de banda que necesitan. (Molina, 2012, p. 37)

Las transferencias de archivos se consideran menos importantes y, por lo tanto, obtienen menor ancho de banda; sin embargo, aún quedará ancho de banda disponible para la navegación web y el resto del tráfico. Hay que tener en cuenta que estos valores máximos sólo se aplican en caso de congestión en la red. El ancho de banda disponible que no se use se podrá utilizar por cualquier tipo de tráfico. (Molina, 2012, p. 37).

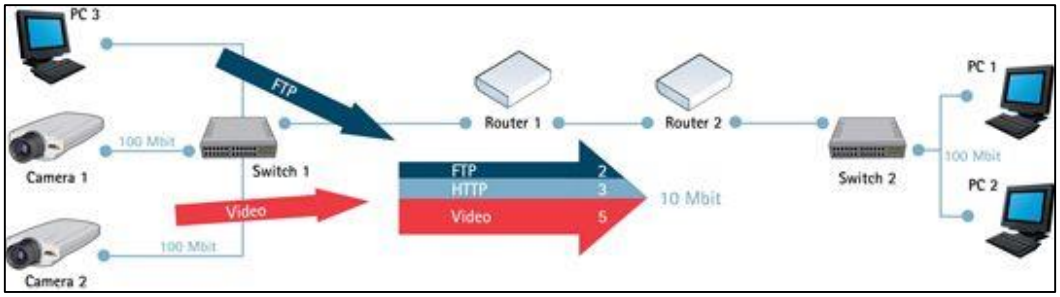


Figura 12: **Gráfica Con Aplicación De QoS**
Fuente: **http://www.axis.com/**

C) TIPOS DE SERVICIOS OFRECIDOS EN UNA RED LAN

a). SERVICIO DE VOZ (VOIP)

Voz sobre protocolo de internet o Voz por protocolo de internet, también llamado voz sobre IP, voz IP, vozIP o VoIP (por sus siglas en inglés de voice over IP: 'voz por IP'), es un conjunto de recursos que hacen posible que la señal de voz viaje a través de Internet empleando el protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional, como las redes PSTN (siglas de Public Switched Telephone Network, red telefónica pública conmutada).

Los protocolos de internet que se usan para enviar las señales de voz sobre la red IP se conocen como protocolos de voz sobre IP o protocolos IP. El tráfico de voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo las LAN (local area network: redes de área local).

Es muy importante diferenciar entre voz sobre IP (VoIP) y telefonía sobre IP.

- VoIP es el conjunto de normas, dispositivos, protocolos (en definitiva, la tecnología) que permite transmitir voz sobre el protocolo IP.
- La telefonía sobre IP es el servicio telefónico disponible al público, con numeración E.164(es una recomendación de la UIT que asigna a cada país un código numérico (código de país) usado para las llamadas internacionales), realizado con tecnología de VoIP. (https://es.wikipedia.org/wiki/Voz_sobre_protocolo_de_internet)

Para que la VoIP sea un reemplazo realista para los servicios de telefonía de redes de telefonía pública conmutada estándar (PSTN), los clientes deben recibir

la misma calidad de transmisión de voz que reciben con los servicios de telefonía básica, es decir, transmisiones de voz de alta calidad sistemáticamente. Al igual que otras aplicaciones de tiempo real, VoIP es extremadamente sensible al ancho de banda y al retraso. Para que las transmisiones de VoIP sean inteligibles para el receptor, los paquetes de voz no se deben perder ni retrasar excesivamente ni sufrir distintos retrasos (también conocido como "fluctuación"). Por ejemplo, se deben cumplir las siguientes normas:

- El códec G.729 predeterminado necesita que haya una pérdida de paquetes bastante inferior al 1 por ciento para evitar errores audibles. Lo mejor sería que no se perdieran paquetes para VoIP.
- La especificación ITU G.114 recomienda un retraso de extremo a extremo unidireccional inferior a 150 milisegundos (ms) para el tráfico en tiempo real de alta calidad como la voz. (Para las llamadas internacionales, se acepta un retraso unidireccional de hasta 300 ms, en especial para las trasmisiones por satélite. Este retraso unidireccional tiene en cuenta el retraso de propagación; es decir, el tiempo necesario para que la señal recorra la distancia).
- Las memorias intermedias para fluctuación (utilizadas para compensar los diferentes retrasos) se agregan posteriormente al retraso de extremo a extremo y normalmente sólo son efectivas en las variaciones de retraso inferiores a 100 ms. Por tanto, se debe minimizar la fluctuación.

VoIP sólo puede garantizar una transmisión de voz de alta calidad si los paquetes de voz, tanto para el canal de audio como para el de señal, tienen prioridad sobre otros tipos de tráfico de red. Para que VoIP se implemente de forma que los usuarios reciban un nivel aceptable de calidad de voz, el tráfico de VoIP debe tener garantizados ciertos requisitos de fluctuación, latencia y

ancho de banda de compensación. QoS garantiza que los paquetes de voz VoIP reciban el trato preferente que requieren. En general, QoS proporciona un servicio de red mejor (y más predecible) al proporcionar las siguientes características:

- Soporte de ancho de banda dedicado.
- Mejora de las características de pérdida.
- Impedimento y administración de la congestión de red.
- Modelado del tráfico de red.
- Configuración de las prioridades del tráfico a través de la red. (Cisco-Calidad de servicio para Voz sobre IP, 2008, p. 2,3)

b). SERVICIO DE VIDEO

La implementación de sistemas de videoconferencia IP resulta más sencilla que la de los sistemas convencionales basados en IP. Sin embargo, los responsables de redes se han de asegurar de que cuentan con toda la infraestructura necesaria para soportar la comunicación. Al igual que los sistemas de videoconferencia RDSI, la videoconferencia basada en IP ofrece voz, vídeo y datos multimedia en tiempo real, con la única diferencia de que para ello se apoya en redes IP de conmutación de paquetes. Pero para que todos los participantes en una sesión puedan comunicarse a través de una red de IP, todos los dispositivos y equipos han de ser interpretativos; es decir, han de basarse en estándares.

H.323 fue la primera norma de videoconferencia IP desarrollada por la Unión Internacional de Telecomunicaciones (UTI) para permitir la comunicación en tiempo real sobre redes IP basadas en paquetes, y actualmente es la más desplegada en el mercado.

H.323 es el estándar con la aceptación global de conferencias multimedia en una red del IP. Este documento describe las herramientas para implementar la Calidad de Servicio (QoS) para las video conferencias H.323 sobre una WAN de empresa con links de velocidad relativamente baja. (http://www.networkworld.es/archive/videoconferencia-basada-en-ip)

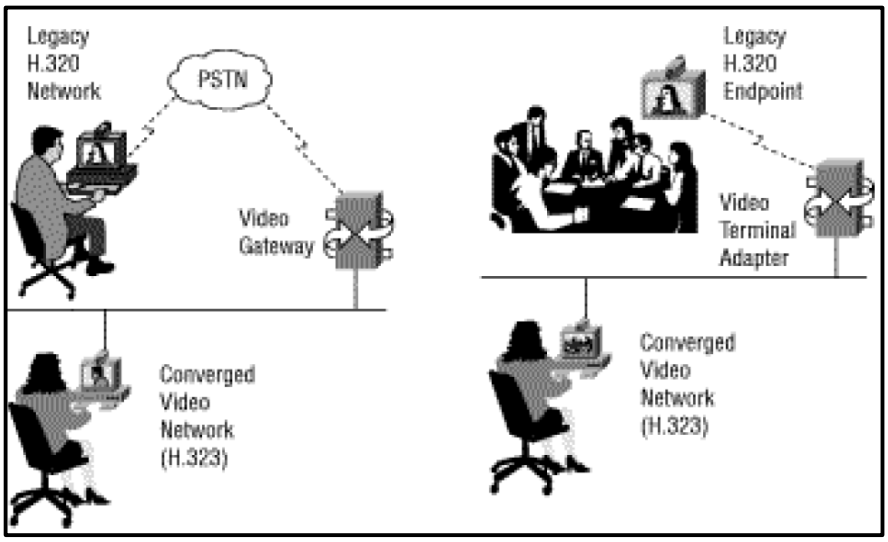


Figura 13: **Tipos de Servicio de video**
Fuente: **Cisco: Implementación de Soluciones QoS para Videoconferencia H.323 sobre IP**

TIPO DE VIDEO	CARACTERÍSTICAS DEL TRÁFICO
Video conferencia	Ancho de banda vivo, bidireccional, pequeño de los grupos: Una o más secuencias por el usuario.
Video on Demand	Una forma, (ancho de banda de punto a punto del modelo de la extracción), una secuencia por el usuario.
Video de broadcast (programado)	Una forma, uno-a-muchos (ancho de banda del modelo del empuje), Una secuencia a los usuarios ilimitados (Multicast)

Tabla 3: **Tipos de Trafico de Video**
Fuente: **Cisco: Implementación de soluciones QoS para video conferencia**

- **Consumo de Ancho de banda por llamada**

  Con la planificación de capacidad, uno de la mayoría de los conceptos críticos a entender es cuánto utiliza el ancho de banda usted para cada llamada. Esta sección enumera el ancho de banda que cada decodificador del codificador (codificador-decodificador) utiliza. Refiera a la voz sobre IP - Por el consumo de ancho de banda de la llamada para más información

- **H.323 Audio:** Las señales de audio contienen digitalizado, sonido comprimido (generalmente discurso). Algoritmos de códec de audio probados soportes del estándar de ITU de H.323. Los algoritmos con el soporte incluyen:
  - G.711 — 3.1 kilociclos (kHz) en 48, 56, y 64 kbps (telefonía normal)
  - G.722 — 7 kHz en 48, 56, y 64 kbps
  - G.728 — 3.1 kHz en 16 kbps
  - G.723 — 5.3 y 6.3 modos del kbps

- **H.323 Video:** Según el estándar de H.323, la capacidad de video en los Terminales H.323 son opcionales. Sin embargo, cuando usted implementa los Terminales H.323, las terminales deben soportar el codificador-decodificador H.261, con el soporte opcional para el estándar H.263.
- **H.261 -** Códec de video para los servicios audiovisuales en los múltiplos de 64 kbps. Los dispositivos H.261-compliant codifican completamente las tramas iniciales. Los dispositivos entonces cifran solamente las diferencias entre las tramas iniciales y subsiguientes para las transmisiones de paquetes

mínimas. La compensación de movimiento opcional mejora la calidad de la imagen.

- **H.263 -** Códec de video para el Servicio telefónico sencillo antiguo (POTS) video. El estándar H.263 es una actualización compatible con versiones anteriores al estándar H.261. El H.263 aumenta perceptiblemente la calidad de la imagen con una técnica de la valoración del movimiento de la mitad-pixel, que es un requisito. Las mejoras también vienen de las tramas previstas y de una Tabla de códigos de Huffman, con la optimización para las transmisiones del Low Bit Rate. (Cisco - Implementación de Soluciones QoS para Videoconferencia H.323 sobre IP, 2016, p. 3,4)

c). SERVICIO DE DATOS

Los servicios de red más comunes son:

- **Protocolo de Configuración Dinámica de Host (DHCP)**

  El Protocolo de Configuración Dinámica de Host (DHCP) es un estándar del Grupo de Trabajo de Ingeniería de Internet (IETF), diseñado para reducir la carga administrativa y la complejidad de la configuración de hosts en un Protocolo de Control de Transmisión / Protocolo de Internet (TCP/IP) basado en red, como una organización privada intranet.

  El proceso de configuración TCP/IP en los equipos clientes DHCP es automático al:

  - Gestionar centralmente direcciones IP y otros parámetros de configuración relacionados.
  - Utilizar equipos clientes para solicitar y aceptar información de configuración TCP/IP de los servidores DHCP.

- Utilizar agentes de retransmisión DHCP para pasar información entre clientes y servidores DHCP. (https://es.wikipedia.org/wiki/Servicio_de_red)

- **Protocolo Simple de Administración de Red (SNMP)**

  El Protocolo Simple de Administración de Red o SNMP, es el estándar utilizado para la gestión de redes TCP/IP. Actualmente es el estándar de gestión de red más popular, debido a su simplicidad de implementación y lo moderado en el consumo del tiempo del procesador y recursos de red. La versión más avanzada SNMPv2, también es compatible para redes basadas en el Modelo OSI.

  SNMP funciona enviando mensajes, conocidos como Protocolos de Unidad de Datos o PDUs a diferentes partes de la red y está compuesto por dos elementos básicos: estaciones de trabajo y agentes.

  Una estación de trabajo o gestor se refiere a los elementos activos encargados de monitorear la red, los elementos activos. Es un software que recoge y monitoriza los diferentes agentes que se encuentran en los nodos de la red, los datos que estos han ido obteniendo, además del funcionamiento de los equipos de enrutamiento y direccionamiento de la red. (Molina, 2012, p. 48)

- **Correo electrónico**

Los sistemas de correo electrónico consisten en dos sub sistemas: los agentes de usuario y los agentes de transferencia de mensajes.

Un agente de usuario (MUA) normalmente es un programa (a veces llamado lector de correo) que acepta una variedad de comandos para componer, recibir y contestar los mensajes, así como para manipular los buzones de correo. Algunos agentes de usuario tienen una interfaz elegante operada por menús o por iconos que requiere un ratón, mientras que otros esperan comandos de un carácter desde el teclado. Funcionalmente, ambos son iguales.

Un agente de transferencia de mensaje (MTA) transfiere mensajes de correo electrónico entre hosts usando el Protocolo para la Transferencia Simple de Correo Electrónico o SMTP. Un mensaje puede pasar por muchos MTAs a medida que este se mueve hasta llegar a su destino. (https://es.wikipedia.org/wiki/Servicio_de_red)

- **Domain Name System (DNS)**

  El DNS es el servicio de Internet que permite traducir el nombre de un sitio Web u otros dominios en una dirección IP, ya que es alfabético, de modo que así se le hace más fácil al propietario o al usuario de recordar. El servidor DNS ejecuta una aplicación de red la cual procesa la cadena URL o dirección Web y en conjunto con la base de datos realiza la acción de conversión en una dirección IP. (https://es.wikipedia.org/wiki/Servicio_de_red).

- **Protocolo de transferencia de Archivos (FTP)**

FTP es la forma más fácil de transferir archivos entre ordenadores a través de Internet y utiliza TCP, el protocolo de control de transmisión, y la IP, protocolos, sistemas de Internet para realizar tareas de carga y descarga.

TCP/IP son los dos protocolos más importantes que mantienen al internet sin problemas. TCP gestiona la transferencia de datos, mientras que IP dirige el tráfico a direcciones de Internet. FTP es un subordinado de lanzaderas archivos de ida y vuelta entre el servidor FTP y un cliente FTP/TCP. Debido a FTP requiere que los dos puertos estén abiertos el servidor y de los clientes facilita el intercambio de grandes archivos de información. Utilizando el modo activo de FTP estándar, el ordenador se comunica el número de puerto en el que estará a su lado para recibir la información del controlador y la dirección IP, ubicación de Internet de la cual o al cual desea transferir archivos. (Molina, 2012, p. 49)

- Servicio de directorio
- Servicio de impresión
- Network File System (NFS)

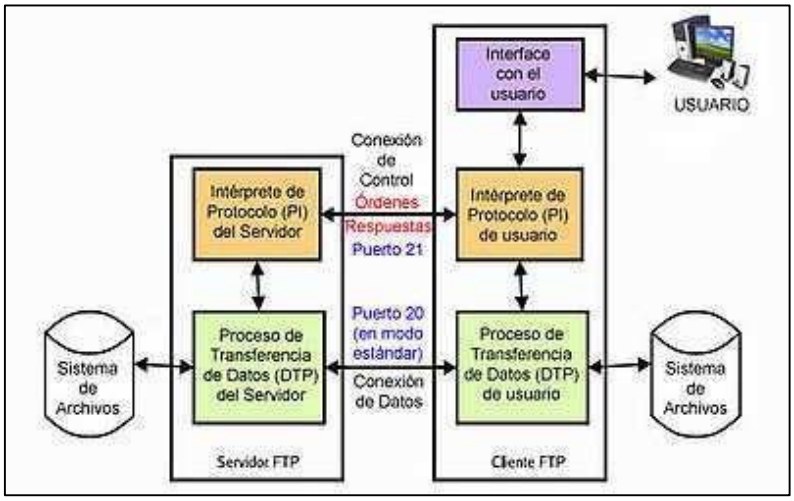


Figura 14: **Diagrama Servicio FTP**
Fuente: http://es.wikipedia.org/wiki/File_Transfer_Protocol

D) RENDIMIENTO DE RED

Hay muchas formas diferentes de medir el rendimiento de una red, ya que cada red es diferente en su naturaleza y diseño. El rendimiento también puede ser modelado en lugar de medir; un ejemplo de esto es usar diagramas de transición de estados para modelar el rendimiento de colas en una red de conmutación de circuitos. Estos diagramas permiten que el planificador de la red analice cómo la red se comportará en cada estado, asegurando que la red se diseñe de manera óptima.

➢ MEDIDA DE RENDIMIENTO

Las siguientes medidas son a menudo consideradas importantes:

- **ANCHO DE BANDA** medido en bits/segundo es la velocidad máxima en la que la información puede ser transferida.
- **THROUGHPUT** es la tasa real de que la información es transferida.
- **LATENCIA** es la demora entre el envío desde el emisor y el descifrado por el receptor, esto es principalmente una función del tiempo de viaje de las señales, y el tiempo de procesamiento en los nodos que la información atraviesa.
- **JITTER** es la variación en el tiempo de llegada al receptor de la información.
- **LA TASA DE ERROR** es el número de bits corruptos expresado como fracción del total enviado.

Un malentendido común es pensar que tener un mayor throughput significa una conexión 'más rápida'. Sin embargo, throughput, latencia, el tipo de información transmitida, y la forma en que la información se aplica afectan a la velocidad percibida de una conexión. (https://es.wikipedia.org/wiki/Rendimiento_de_red).

1. **ANCHO DE BANDA:** En computación de redes y en biotecnologia, ancho de banda digital, ancho de banda de red o simplemente ancho de banda es la medida de datos y recursos de comunicación disponible o consumida expresados en bit/s o múltiplos de él como serían los Kbit/s,Mbit/s y Gigabit/s.

   Ancho de banda puede también referirse a ancho de banda consumido (consumo de ancho de banda), que corresponde al throughput o goodput conseguido; esto es, la tasa media de transferencia de datos exitosa a través de una vía de comunicación.

   (https://es.wikipedia.org/wiki/Ancho_de_banda_(inform%C3%A1tica).

2. **TRHOUGHPUT:** Throughput es denominado como el número de mensajes que fueron recibidos de manera exitosa, por unidad de tiempo. Es controlado por el ancho de banda disponible, la señal a radio (decibeles) disponible y las limitaciones del hardware. Para propósitos de este artículo, Throughput, será tomado en cuenta desde el primer bit de información que llega al receptor; esto con el fin de separar el concepto, con el de latencia, ya que generalmente son usados como sinónimos. (https://es.wikipedia.org/wiki/Throughput).

3. **LATENCIA:** La velocidad de la luz, impone un tiempo mínimo de propagación de todas las señales electromagnéticas. No es posible disminuir la latencia debajo de:

$$t = s / c_m$$

Donde: **S = distancia**, **C = velocidad de la luz, en la mitad**.

Otros retrasos surgen en nodos intermedios. En una red de paquetes conmutados retrasos pueden surgir debido a la espera puesta en cola.
(https://es.wikipedia.org/wiki/Latencia).

4. **JITTER:** es la desviación no deseada de la periodicidad verdadera de una señal asumida como periódica, en electrónica y telecomunicaciones, muchas veces relacionada en referencia a una señal de reloj. Jitter puede encontrarse presente en características como la frecuencia de sucesivas pulsaciones, la amplitud de señal o fase de señales periódicas. Jitter es un factor importante y usualmente no deseado, en el diseño de casi todas las ligas de comunicación (e.g., USB, PCI-e, SATA, OC-48). En aplicaciones de recuperación de reloj es denominado como timing jitter. (https://es.wikipedia.org/wiki/Jitter).

5. **TASA DE ERROR:** En transmisiones digitales el número de errores binarios son el número de bits recibidos de una corriente de datos sobre un canal de comunicación que ha sido alterado debido a ruido, interferencia, distorsión o errores de sincronización bit.

   El rango de error binario o tasa de error binario es el número de errores bit, divididos por el número total de bits transferidos durante el intervalo de tiempo estudiado. El rango de error binario es la medición de tiempo sin medida, que es usualmente expresada como el porcentaje.

   La probabilidad de error bit p, es el valor esperado de la tasa de error binario. Puede ser considerado como una aproximación estimada de la probabilidad de error binario. En intervalos de larga duración y alto número de errores binarios la estimación es acertada. (https://es.wikipedia.org/wiki/Tasa_de_error_binario).

2.3. DEFINICIÓN DE TÉRMINOS

- **CALIDAD:** La totalidad de las características de una entidad que determinan su capacidad para satisfacer las necesidades explícitas e implícitas.

  NOTA – Las características deben ser observables y/o mensurables. Cuando las características se definen, se convierten en parámetros y se expresan en unidades de medida. (Recomendación UIT-T E.800, 2008, p. 3).

- **CALIDAD DE SERVICIO (QoS):** La totalidad de las características de un servicio de telecomunicaciones que determinan su capacidad para satisfacer las necesidades explícitas e implícitas del usuario del servicio. (Recomendación UIT-T E.800, 2008, p. 3).

- **REQUISITOS DE QoS DEL USUARIO/CLIENTE (QoSR):** Declaración de los requisitos de QoS de un cliente/usuario, o de uno o varios segmentos de la clientela/los usuarios con requisitos o necesidades de calidad de funcionamiento exclusivos.

  NOTA – Las necesidades de los clientes/usuarios puede expresarse en términos descriptivos (criterios) en orden de prioridad, con un valor de calidad de funcionamiento preferida para cada criterio. El proveedor de servicio se encarga de traducir los criterios en parámetros y unidades de medida aplicables al servicio [UIT-T E.802]. (Recomendación UIT-T E.800, 2008, p.3).

- **QoS OFRECIDA/PLANIFICADA POR EL PROVEEDOR DE SERVICIOS (QoSO):** Declaración del nivel de calidad planificada y, por ende, ofrecida al cliente por el proveedor de servicios.

NOTA – Nivel de QoS que el proveedor de servicios prevé alcanzar (y, por tanto, ofrece) al cliente/usuario se expresa en valores objetivo (o gamas de valores) mensurables de los parámetros pertinentes para un servicio específico. (Recomendación UIT-T E.800, 2008, p. 3).

- **QoS PROPORCIONADA/LOGRADA POR EL PROVEEDOR DE SERVICIO (QoSD):** Declaración del nivel de QoS lograda o proporcionada al cliente.

  NOTA – La QoS lograda o proporcionada se expresa en unidades de medida para los parámetros pertinentes del servicio. (Recomendación UIT-T E.800, 2008, p. 3).

- **QoS EXPERIMENTADA/PERCIBIDA POR EL CLIENTE/USUARIO (QoSE)**

  Declaración del nivel de calidad que los clientes/usuarios consideran haber experimentado.

  NOTA 1 – El nivel de QoS experimentada y/o percibida por el cliente/usuario puede expresarse utilizando notas de opinión.

  NOTA 2 – La QoSE tiene dos principales componentes humanos: el cuantitativo y el cualitativo. El componente cuantitativo puede estar influido por todos los efectos del sistema de extremo a extremo (infraestructura de red).

  NOTA 3 – El componente cualitativo puede estar influido por las expectativas del usuario, las condiciones ambientales, factores psicológicos, el contexto de aplicación, etc.

NOTA 4 – La QoSE también puede considerarse como la QoSD recibida e interpretada por un usuario con los factores cualitativos pertinentes que influyen en su percepción del servicio. (Recomendación UIT-T E.800, 2008, p. 3).

- **SERVICIO:** El conjunto de funciones ofrecidas al usuario por una organización constituye un servicio. (Recomendación UIT-T E.800, 2008, p. 4).

- **USUARIO:** Entidad que utiliza una entidad de comunicación (por ejemplo, inicia o responde una llamada) [UIT-T Q.1300] o Persona o entidad externa a la red que utiliza para la comunicación conexiones a través de la red.

  NOTA – Se utiliza conexión en el contexto del establecimiento de una comunicación entre dos puntos de una red. Conexión es el "trayecto portador, trayecto conmutado con etiqueta, circuito virtual y/o trayecto virtual establecidos por el encaminamiento de la llamada y el encaminamiento de la conexión" [UIT-T E.360.1) y [UIT-T E.361]. (Recomendación UIT-T E.800, 2008, p. 5)

- **CLIENTE:** Usuario que paga por los servicios recibidos. (Recomendación UIT-T E.800, 2008, p. 5).

- **CALIDAD DE FUNCIONAMIENTO DE LA RED:** Aptitud de una red o parte de la red para ofrecer las funciones correspondientes a las comunicaciones entre usuarios.

  NOTA 1 – La calidad de funcionamiento de la red se aplica a la planificación, desarrollo, operaciones y mantenimiento por el proveedor de la red, y es la parte técnica detallada de la QoSO.

NOTA 2 – Los parámetros de calidad de funcionamiento de la red son significativas para los proveedores de la red y cuantificables en la parte de la red a la que se aplican. (Recomendación UIT-T E.800, 2008, p. 5).

- **PROVEEDOR DE RED:** Organización que posee una red de telecomunicaciones para transportar portadoras de servicios de telecomunicaciones. (Recomendación UIT-T E.800, 2008, p. 5).

- **PROVEEDOR DE SERVICIOS:** Organización que presta servicios a los usuarios y los clientes. (Recomendación UIT-T E.800, 2008, p. 5).

- **VARIABLE DE QoS:** Toda variable de funcionamiento (tal como congestión, retardo, etc.) que es perceptible por un usuario ([UIT-T E.360.1]). (Recomendación UIT-T E.800, 2008, p. 7).

- **QoS RELATIVA:** Cuando el tráfico tiene valores límites para los parámetros de QoS como el retardo, etc., que no se expresan en términos absolutos. Se refiere a aquellos casos en los que el procesamiento de ciertas clases de tráfico es diferente del de otras, y cada clase obtiene un nivel distinto de QoS [UIT-T Y.2111]. (Recomendación UIT-T E.800, 2008, p. 7).

- **VELOCIDAD:** Criterio de calidad de funcionamiento que describe el intervalo de tiempo que se utiliza para realizar la función o la velocidad a la que se realiza la función. (La función puede o no realizarse con la precisión deseada.) [UIT-T I.350]. (Recomendación UIT-T E.800, 2008, p. 7).

- **CERTIDUMBRE:** La certidumbre es el criterio de calidad de funcionamiento que describe el grado de certeza (o seguridad) con que se realiza la función, Independientemente de la velocidad o precisión, pero dentro de un determinado intervalo de observación ([UIT-T I.350]). (Recomendación UIT-T E.800, 2008, p. 7).

- **DISPONIBILIDAD:** Disponibilidad de un elemento para hallarse en estado de realizar una función requerida en un instante determinado o en cualquier instante de un intervalo de tiempo dado, suponiendo que se facilitan, si es necesario, los recursos externos ([UIT-T E.802]). (Recomendación UIT-T E.800, 2008, p. 7).

- **FIABILIDAD:** Probabilidad de que una entidad realice la función requerida en las condiciones impuestas en un intervalo de tiempo dado. (Recomendación UIT-T E.800, 2008, p. 7).

- **CALIDAD DE EXTREMO A EXTREMO:** Calidad relacionada con el funcionamiento de un sistema de comunicaciones, incluidos todos los equipos terminales.

  NOTA – Para los servicios vocales, es equivalente a la calidad boca-oído ([UIT-T P.10]). (Recomendación UIT-T E.800, 2008, p. 8).
- **CALIDAD DE LA CONVERSACIÓN:** Calidad con la que un participante de la comunicación percibe una conversación bidireccional o multidireccional. ([UIT-T P.10]). (Recomendación UIT-T E.800, 2008, p. 9).

- **CALIDAD DE TRANSMISIÓN VOCAL UNIDIRECCIONAL:** Calidad vocal relacionada con las señales transmitidas a través de un sistema de comunicación, experimentada por un usuario de ese sistema en una situación de escucha solamente. Se refiere únicamente a las características de transmisión unidireccionales ([UIT-T P.10]). (Recomendación UIT-T E.800, 2008, p. 9).

- **DESCARGA:** Transferencia de datos o programas de un servidor o computador anfitrión al computador o dispositivo del usuario. (Recomendación UIT-T E.800, 2008, p. 10).

- **SEGURIDAD:** El término "seguridad" se utiliza en el sentido de minimizar las vulnerabilidades de los bienes y recursos. Un "bien" es todo elemento de valor. Vulnerabilidad es toda debilidad que pudiera explotarse para violar un sistema o las informaciones que éste contiene ([UIT-T X.800]). (Recomendación UIT-T E.800, 2008, p. 10).

- **SEGURIDAD DE LA INFORMACIÓN:** Preservación segura de la confidencialidad, integridad y disponibilidad de la información ([UIT-T X.1051]). (Recomendación UIT-T E.800, 2008, p. 10).

- **SEGURIDAD DE LOS DATOS:** Preservación segura de la integridad y la disponibilidad de los datos. (Recomendación UIT-T E.800, 2008, p. 10)

- **PRIVACIDAD:** Derecho de las personas a controlar o influir sobre la información relacionada con ellos que puede recogerse o almacenarse y las personas a las cuales o por las cuales esta información puede ser revelada.

  NOTA – Como este término se relaciona con el derecho de las personas, no puede ser muy preciso y su uso debe evitarse, salvo como un motivo para exigir seguridad ([UIT-T X.800]). (Recomendación UIT-T E.800, 2008, p. 10).

- **CONTRASEÑA:** Información de autenticación confidencial, usualmente compuesta por una cadena de caracteres. ([UIT-T X.800]). (Recomendación UIT-T E.800, 2008, p. 10).

- **CONFIDENCIALIDAD:** Propiedad de una información que no está disponible ni es divulgada a personas, entidades o procesos no autorizados ([UIT-T X.800]). (Recomendación UIT-T E.800, 2008, p. 10).

- **CONFIDENCIALIDAD DE LOS DATOS:** Un servicio que se puede utilizar para obtener la protección de los datos frente a buscadores no autorizados. El servicio de confidencialidad de datos está soportado por un marco de autentificación. Se puede utilizar para la protección contra la intercepción de datos ([UIT-T X.509]). (Recomendación UIT-T E.800, 2008, p. 10).

- **INTEGRIDAD:** Propiedad de que los datos no han sido alterados de una manera no autorizada ([UIT-TH.235.0]). (Recomendación UIT-T E.800, 2008, p. 10).

- **INTEGRIDAD DE LOS DATOS:** Propiedad que garantiza que los datos no han sido alterados o destruidos de una manera no autorizada ([UIT-T X.800]). (Recomendación UIT-T E.800, 2008, p. 11).

- **INTERFAZ RED/USUARIO:** La interfaz red/usuario es la interfaz física entre la red del proveedor de servicios y el equipo en los locales del cliente del usuario o cliente.

  NOTA – En algunos casos, será el proveedor de servicios quien facilite el equipo en los locales del cliente. La definición anterior es también válida para estos casos. (Recomendación UIT-T E.800, 2008, p. 13).

- **INTERCONEXIÓN:** "Interconexión" es la vinculación física y lógica de las redes públicas de comunicaciones utilizadas por un mismo o por distintos proveedores de servicios para que los usuarios de un proveedor de servicios puedan comunicarse con los usuarios de otro proveedor de servicios, o acceder a los servicios prestados por otro proveedor de servicios. (Recomendación UIT-T E.800, 2008, p. 13).

- **ACCESIBILIDAD DE LA RED:** Probabilidad de que el usuario de un servicio, tras haberla solicitado (a una red), reciba la señal "proceda a la selección" dentro de determinadas condiciones.

  NOTA – La señal "proceda a la selección" es la señal que invita al usuario a seleccionar el destino deseado. (Recomendación UIT-T E.800, 2008, p. 13).

- **ACCESIBILIDAD DE LA CONEXIÓN:** Probabilidad de que pueda establecerse una conexión dentro de las tolerancias especificadas y otras condiciones dadas tras la recepción de un código válido en la central. (Recomendación UIT-T E.800, 2008, p. 13).

- **TRANSPARENCIA DE BITS:** Capacidad de un sistema de telecomunicaciones para transportar la señal que se le presenta al punto de ingreso y reproducirla sin modificaciones en un punto de egreso en un periodo de tiempo dado. (Recomendación UIT-T E.800, 2008, p. 14).

- **TASA DE ERRORES EN LOS BITS (BER, BIT ERROR RATIO):** Relación entre el número de bits erróneos y el número total de bits transmitidos durante un intervalo determinado. (Recomendación UIT-T E.800, 2008, p. 14).

- **TASA DE SEGUNDOS SIN ERRORES:** Relación entre el número de intervalos de un segundo durante los cuales no se reciben bits con errores y el número total de intervalos de un segundo dentro de un intervalo determinado. (Recomendación UIT-T E.800, 2008, p. 14).

- **RED IP DE EXTREMO A EXTREMO:** Conjunto de EL (enlaces de intercambio) y NS (secciones de red) que procuran el transporte de paquetes IP transmitidos del SRC al DST. Los MP (puntos de medición) que unen la red IP de extremo a extremo son los que se encuentran en el SRC (anfitrión origen) y el DST (anfitrión destino) ([UIT-T Y.1540]). (Recomendación UIT-T E.800, 2008, p. 14).

- **CALIDAD DE FUNCIONAMIENTO DE RED IP DE EXTREMO A EXTREMO:** Relación mensurable entre cualquier servicio IP de extremo a extremo unidireccional dado. ([UIT-T Y.1540]). (Recomendación UIT-T E.800, 2008, p. 14).

- **PORCENTAJE DE DISPONIBILIDAD DE SERVICIO IP (PIA, PERCENT IP SERVICE AVAILABILITY):** Porcentaje del tiempo de servicio IP planificado total (porcentaje de intervalos T_{av}) que se categoriza como disponible utilizando la función de disponibilidad de servicio IP ([UIT-TY.1540]). (Recomendación UIT-T E.800, 2008, p. 14).

- **CLASE DE SERVICIO:** El conjunto de valores de calidad de funcionamiento de extremo a extremo (o gama) para un servicio se denomina "clase de servicio". Una oferta de servicio puede tener entre tres y cinco clases de servicio con límites de calidad de funcionamiento especificados para distintos parámetros. Estas clases de servicio se suelen utilizar para ofrecer diversas tarifas al cliente. (Recomendación UIT-T E.800, 2008, p. 15).

- **DURACIÓN DE LA INTERRUPCIÓN:** Tiempo que dura una interrupción. (Recomendación UIT-T E.800, 2008, p. 16).

- **COBERTURA DE FALLOS:** Proporción de fallos de una entidad que pueden reconocerse en determinadas condiciones. (Recomendación UIT-T E.800, 2008, p. 16).

- **COBERTURA DE REPARACIÓN:** Capacidad de una organización de mantenimiento para, en determinadas condiciones, facilitar, previa petición, los recursos necesarios para el mantenimiento de una entidad, en el marco de una política de mantenimiento dada.

NOTA – Las condiciones determinadas están relacionadas con la entidad misma y con las condiciones en que se utiliza y mantiene. (Recomendación UIT-T E.800, 2008, p. 16).

- **CALIDAD DE FIABILIDAD:** Capacidad de una entidad para realizar la función que se le requiere en determinadas condiciones durante un intervalo de tiempo dado. (Recomendación UIT-T E.800, 2008, p. 17).

CAPÍTULO

III

MATERIALES Y MÉTODOS

3 MATERIAL Y MÉTODOS

3.1. MATERIAL

3.1.1. POBLACIÓN Y MUESTRA

La población y muestra está conformada por la recolección de 3 capturas de tráfico realizados en distintos días de la semana en horarios de funcionamiento normal en la red de la corte.

3.1.2. UNIDAD DE ANÁLISIS

Trafico de la red.

3.2. MÉTODO

3.2.1. NIVEL DE INVESTIGACIÓN

El presente proyecto se basó en una investigación de tipo aplicada en su propósito y descriptiva por su alcance, ya que se estudiaron los procedimientos necesarios para el tratamiento de incidencias.

3.2.2. DISEÑO DE INVESTIGACIÓN

El nivel de investigación propuesto en el presente proyecto es de tipo investigación de campo.

Se utilizó la herramienta de análisis “Wireshark” para recolectar la información relacionada con el tráfico de red las cuales fueron capturadas en 3 días de la semana en horarios de funcionamiento normal en la red de la corte.

3.2.3. VARIABLES DE ESTUDIO Y OPERACIONALIZACIÓN

3.2.3.1. VARIABLE INDEPENDIENTE

FACTORES BASADOS EN LOS PARAMETROS DE QoS.

DEFINICIÓN CONCEPTUAL: El tráfico de red se basa habitualmente en la utilización de sondas con interfaz Ethernet conectadas a un bus. Dichas sondas, con su interfaz Ethernet funcionando en modo promiscuo, capturan el tráfico a analizar y constituyen la plataforma en la que se ejecutaran, de forma continua, aplicaciones propietarias o de dominio público, con las que se podrá determinar el tipo de información que circula por la red y el impacto que pudiera llegar a tener sobre la misma también se mide como la cantidad de información promedio que se transfiere a través del canal de comunicación, y a la velocidad que se transfiere por ello la importancia, del conocimiento sobre la "Teoría de la información" y sus diferentes elementos para poder evaluar en formas más eficiente y eficaz el tráfico en la red. (Análisis del tráfico de una red local universitaria, 2009, pag. 21).

DEFINICIÓN OPERACIONAL:

Indicadores

- Ancho de Banda.
  - Capacidad del Canal
  - Utilización del Canal
  - Protocolos de Conexión.
  - Aplicaciones.

- Perdida de Paquetes.
  - Capacidad de procesamiento de equipos.
  - Mecanismos de acceso al medio.
  - Congestión de red.

- Jitter.
  - Tamaños de paquetes transmitidos por la red.
  - Números de Host conectados.
  - Distancia entre Pc y Servidor.

3.2.3.2. VARIABLE DEPENDIENTE

RENDIMIENTO DE LA RED.

DEFINICIÓN CONCEPTUAL: Normalmente, los parámetros de QoS de un servicio de telecomunicación se especifican de manera que se puedan aplicar a numerosas ofertas de servicio de diferentes proveedores y así poder compararlos.

Por consiguiente, es necesario que las definiciones y los métodos de medición abarquen diferentes tecnologías, aplicaciones técnicas y modelos comerciales, por lo que se formulan de una manera más generalizada. Ello deberá tenerse presente cuando se determinen y se utilicen conjuntos de parámetros de QoS para establecer estadísticas de calidad que abarquen a una serie de redes o servicios. (UIT-T E.802, 2007, pag. 15).

DEFINICIÓN OPERACIONAL:

Indicadores

- Ancho de Banda.
- Perdida de paquetes.
- Variación de retardo (Jitter).

Variable Independiente	Indicadores	Unidad de Medida	Instrumento de Investigación
Factores basados en los parámetros de QoS.	Tamaños de paquetes transmitidos por la red	Porcentaje (%) significancia	ANOVA
	Numero de host conectados		
	Distancia entre PC y Servidor		

Tabla 4: **Variable Independiente**
Fuente: **Elaboración Propia**

Variable Independiente	Indicadores	Unidad de Medida	Instrumento de Investigación
Rendimiento de RED	Ancho de banda	Kbps	Objetivos de calidad de funcionamiento para aplicaciones de audio y video (Cuadro I.1/G.1010)
	Perdida de paquetes	Porcentaje (%)	
	Variación de retardo (Jitter)	Porcentaje (%) de significancia	Objetivos de calidad de funcionamiento para aplicaciones de datos (Cuadro I.2/G.1010)

Tabla 5: **Variable Dependiente**
Fuente: **Elaboración Propia**

3.2.4. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS

A) Caracterizar los parámetros de QoS que regulan la red de datos

Se caracterizó los factores basados en los parámetros de QoS según la ITU-T G.1010 "Transmission Systems And Media, Digital Systems And Networks" los cuales establece que:

Voz:

- Latencia <= 150 ms
- Jitter <= 30 ms
- Loss <= 1%
- Bandwidth (30 – 128 Kbps+)

Video:

- Latencia <= 200 - 400 ms
- Jitter <= 30 - 50 ms
- Loss <= 0.1 – 1 %
- Bandwidth (384 kbps – 20Mbps+)

Datos:

- Latencia <= 2 - 15 ms
- Jitter <= 200 ms – 60 s
- Loss = 0 %
- Bandwidth (1 Kb – 1Mb+)

Medio	Aplicación	Grado de simetría	Velocidades de datos típicas	Parámetros clave y valores de objetivo para la calidad de funcionamiento			
				Tiempo de transmisión en un sentido	Variación de retardos	Pérdida de información (Nota 2)	Otros
Audio	Voz en conversación	Dos sentidos	4-64 kbit/s	Preferido < 150 ms (Nota 1) Límite < 400 ms (Nota 1)	< 1 ms	Relación de pérdida de paquete (PLR) < 3%	
Audio	Mensajería vocal	Principalmente en un sentido	4-32 kbit/s	< 1 s para reproducción < 2 s para grabación	< 1 ms	PLR < 3%	
Audio	Audio en tiempo real de gran calidad	Principalmente en un sentido	16-128 kbit/s (Nota 3)	< 10 s	<< 1 ms	PLR < 1%	
Vídeo	Videoteléfono	Dos sentidos	16-384 kbit/s	Preferido < 150 ms (Nota 4) Límite < 400 ms		PLR < 1%	Sinc. labios: < 80 ms
Vídeo	Un sentido	Un sentido	16-384 kbit/s	< 10 s		PLR < 1%	

NOTA 1 – Se supone el control de eco adecuado.

NOTA 2 – Los valores exactos dependen del códec específico, pero se supone el uso de un algoritmo de ocultación de pérdida de paquete para minimizar el efecto de esa pérdida.

NOTA 3 – La calidad depende mucho del tipo de códec y de la velocidad binaria.

NOTA 4 – Estos valores se consideran valores de objetivo a largo plazo y es probable que la tecnología actual no los satisfaga.

Tabla 6: **Objetivos de cumplimiento para aplicaciones de datos**
***Fuente*: ITU-T I.1 G.1010 – Objetivos de calidad de funcionamiento para aplicaciones de audio y video**

Medio	Aplicación	Grado de simetría	Velocidades de datos típicas	Parámetros clave y valores de objetivo para la calidad de funcionamiento		
				Tiempo de transmisión en un sentido (Nota)	Variación de retardos	Pérdida de información
Datos	Navegación en la web – HTML	Principalmente un sentido	~10 KB	Preferido < 2 s/página Aceptable < 4 s/página	No disponible	Nula
Datos	Transferencia/ recuperación de gran volumen de datos	Principalmente un sentido	10 KB-10 MB	Preferido < 15 s Aceptable < 60 s	No disponible	Nula
Datos	Servicios de transacciones de alta prioridad, como comercio electrónico, ATM	Dos sentidos	< 10 KB	Preferido < 2 s Aceptable < 4 s	No disponible	Nula
Datos	Medio dirigido/ control	Dos sentidos	~ 1 KB	< 250 ms	No disponible	Nula
Datos	Imagen fija	Un sentido	< 100 KB	Preferido < 15 s Aceptable < 60 s	No disponible	Nula
Datos	Juegos interactivos	Dos sentidos	< 1 KB	< 200 ms	No disponible	Nula
Datos	Telnet	Dos sentidos (asimétrico)	< 1 KB	< 200 ms	No disponible	Nula
Datos	Correo electrónico (acceso a servidor)	Principalmente un sentido	< 10 KB	Preferido < 2 s Aceptable < 4 s	No disponible	Nula
Datos	Correo electrónico (transferencia de servidor a servidor)	Principalmente un sentido	< 10 KB	Puede ser varios minutos	No disponible	Nula
Datos	Fax ("tiempo real")	Principalmente un sentido	~ 10 KB	< 30 s/página	No disponible	$<10^{-6}$ BER
Datos	Fax (almacenamiento y retransmisión)	Principalmente un sentido	~ 10 KB	Pueden ser varios minutos	No disponible	$<10^{-6}$ BER
Datos	Transacciones de baja prioridad	Principalmente un sentido	< 10 KB	< 30 s	No disponible	Nula
Datos	Usenet	Principalmente un sentido	Puede ser 1 MB o más	Pueden ser varios minutos	No disponible	Nula
KB kbit/s MB Mbit/s NOTA – En algunos casos, puede ser más apropiado considerar estos valores como tiempos de respuesta.						

Tabla 7: **Objetivos de cumplimiento para aplicaciones de datos**
Fuente**: ITU-T I.2 G.1010 – Objetivos de funcionamiento para aplicaciones de datos**

B) Captura del tráfico de la información de la red

Se utilizó la herramienta de análisis "Wireshark" open-source diseñado por Gerald Combs y está disponible para plataformas Windows y Unix. La cual permite recolectar información relacionados con el tráfico de red, implementando una amplia gama de filtros que facilitan el criterio de búsqueda para los más de 1100 protocolos soportados; y todo ello por medio de una interfaz sencilla e intuitiva que permite desglosar por capas cada uno de los paquetes capturados. (Análisis de Trafico de Wireshark, INTECO, pag.4)

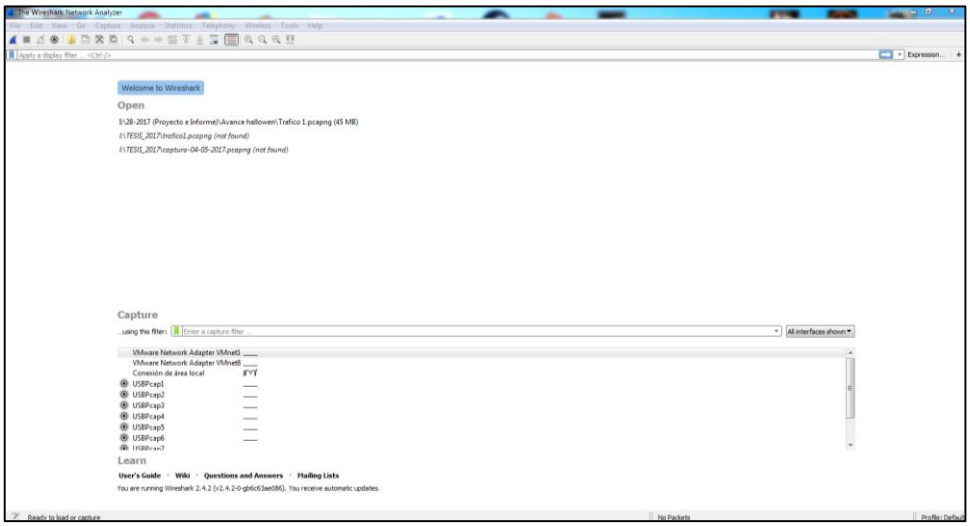


Figura 15: **Analizador de Tráfico Wireshark**
Fuente: **Captura de pantalla propia**

Los protocolos con más presencia y su efecto a la hora de realizar las pruebas son:

- ARP (Address Resolution Protocol).
- DHCPv6 (Dynamic Host Configuration Protocol for IPv6).
- HSRP (Cisco Hot Standby Router Protocol).
- ICMP (Internet Control Message Protocol).
- ICMPv6 (Internet Control Message Protocol for IPv6).
- LLMNR (Link-Local Multicast Name Resolution).
- TCP (Transmission Control Protocol).
- UDP (User Datagram Protocol).

PROTOCOLO ARP:

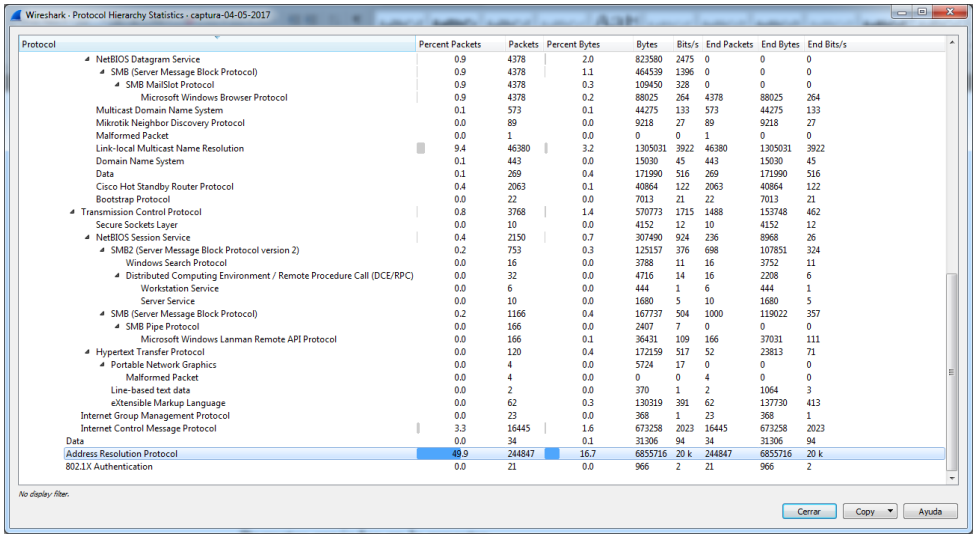


Figura 16: **Presencia del Protocolo ARP en la muestra realizada a la red de la CSJLL con el programa Wireshark**
Fuente: **Elaboración Propia**

El protocolo ARP tiene una presencia del 49.9%, con más de 244847 paquetes enviados en el periodo de muestra tomada.

PROTOCOLO DHCPv6:

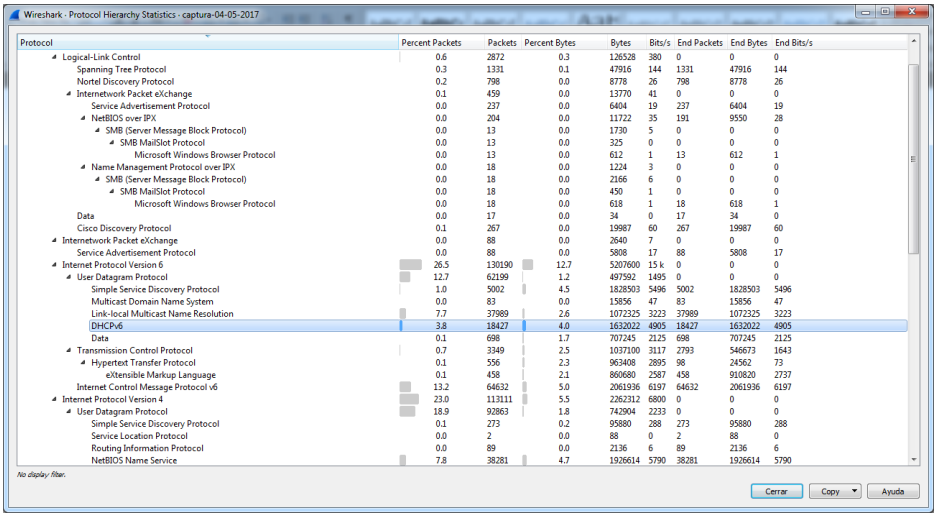


Figura 17: **Presencia del Protocolo DHCPv6 en la muestra realizada a la red de la CSJLL con el programa Wireshark**
Fuente: **Elaboración Propia**

El protocolo DHCPv6 tiene una presencia del 3.8%, con más de 18427 paquetes enviados en el periodo de muestra tomada.

PROTOCOLO HSRP:

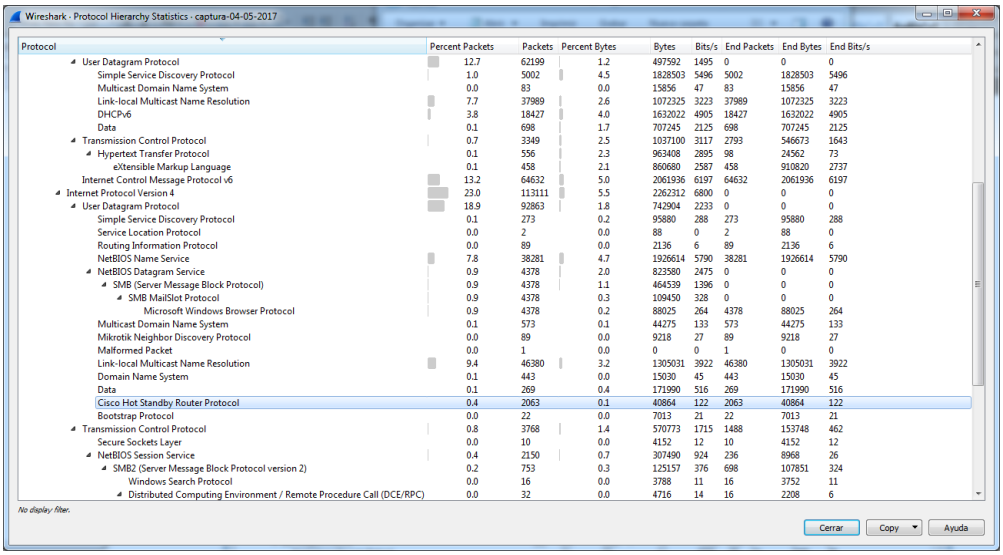


Figura 18: **Presencia del Protocolo HSRP en la muestra realizada a la red de la CSJLL con el programa Wireshark**
Fuente: **Elaboración Propia**

El protocolo HSRP tiene una presencia del 0.4%, con más de 2063 paquetes enviados en el periodo de muestra tomada.

PROTOCOLO ICMP:

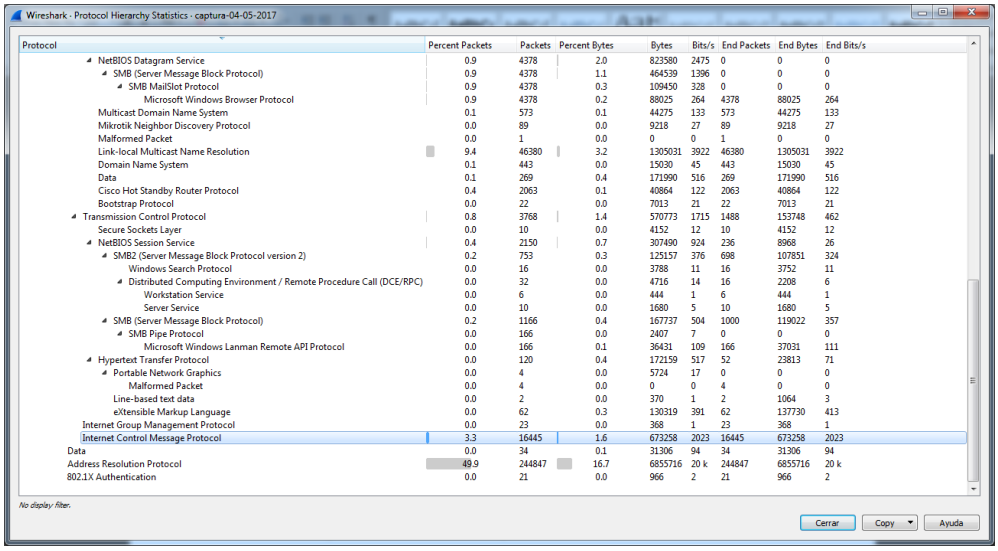


Figura 19: **Presencia del Protocolo ICMP en la muestra realizada a la red de la CSJLL con el programa Wireshark**
Fuente: **Elaboración Propia**

El protocolo ICMP tiene una presencia del 3.3%, con más de 16445 paquetes enviados en el periodo de muestra tomada.

PROTOCOLO ICMPv6:

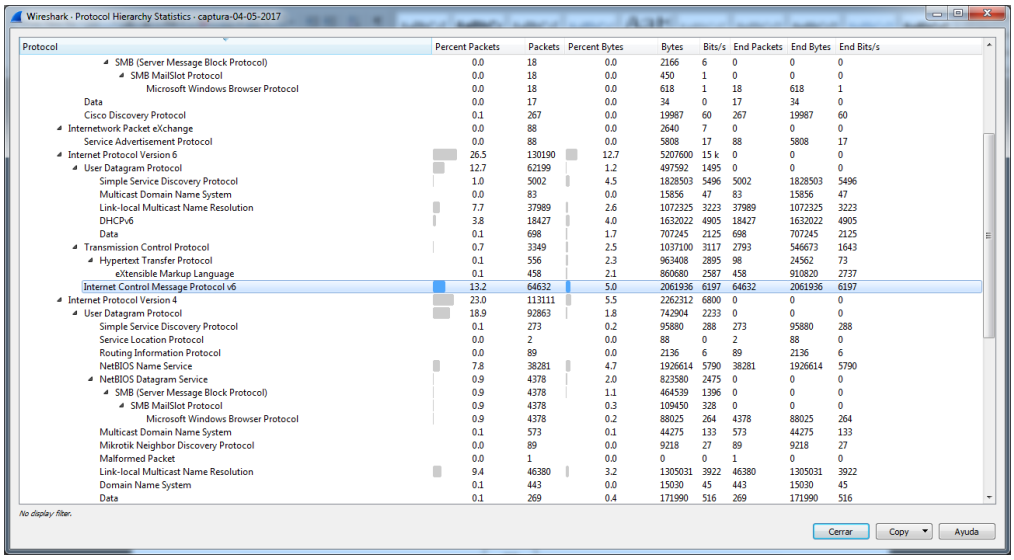
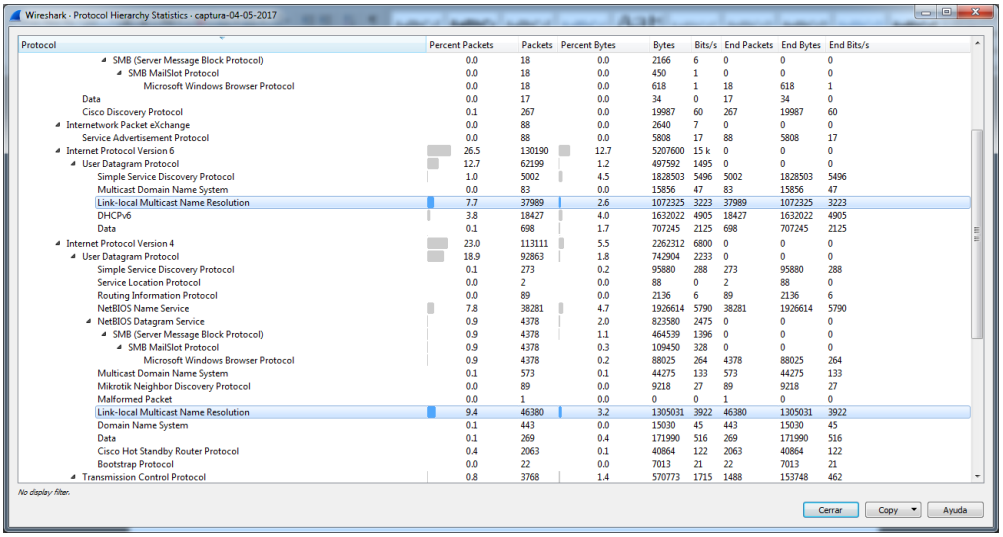


Figura 20: **Presencia del Protocolo ICMPv6 en la muestra realizada a la red de la CSJLL con el programa Wireshark**
Fuente: **Elaboración Propia**

El protocolo ICMPv6 tiene una presencia del 13.2%, con más de 64632 paquetes enviados en el periodo de muestra tomada.

PROTOCOLO LLMNR:



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
SMB (Server Message Block Protocol)	0.0	18	0.0	2166	6	0	0	0
SMB MailSlot Protocol	0.0	18	0.0	450	1	0	0	0
Microsoft Windows Browser Protocol	0.0	18	0.0	618	1	18	618	1
Data	0.0	17	0.0	34	0	17	34	0
Cisco Discovery Protocol	0.1	267	0.0	19987	60	267	19987	60
Internetwork Packet eXchange	0.0	88	0.0	2640	7	0	0	0
Service Advertisement Protocol	0.0	88	0.0	5808	17	88	5808	17
Internet Protocol Version 6	26.5	130190	12.7	5207600	15 k	0	0	0
User Datagram Protocol	12.7	62199	1.2	497592	1495	0	0	0
Simple Service Discovery Protocol	1.0	5002	4.5	1828503	5496	5002	1828503	5496
Multicast Domain Name System	0.0	83	0.0	15856	47	83	15856	47
Link-local Multicast Name Resolution	7.7	37989	2.6	1072325	3223	37989	1072325	3223
DHCPv6	3.8	18427	4.0	1632022	4905	18427	1632022	4905
Data	0.1	698	1.7	707245	2125	698	707245	2125
Internet Protocol Version 4	23.0	113111	5.5	2262312	6800	0	0	0
User Datagram Protocol	18.9	92863	1.8	742904	2233	0	0	0
Simple Service Discovery Protocol	0.1	273	0.2	95880	288	273	95880	288
Service Location Protocol	0.0	2	0.0	88	0	2	88	0
Routing Information Protocol	0.0	89	0.0	2136	6	89	2136	6
NetBIOS Name Service	7.8	38281	4.7	1926614	5790	38281	1926614	5790
NetBIOS Datagram Service	0.9	4378	2.0	823580	2475	0	0	0
SMB (Server Message Block Protocol)	0.9	4378	1.1	464539	1396	0	0	0
SMB MailSlot Protocol	0.9	4378	0.3	109450	328	0	0	0
Microsoft Windows Browser Protocol	0.9	4378	0.2	88025	264	4378	88025	264
Multicast Domain Name System	0.1	573	0.1	44275	133	573	44275	133
Mikrotik Neighbor Discovery Protocol	0.0	89	0.0	9218	27	89	9218	27
Malformed Packet	0.0	1	0.0	0	0	1	0	0
Link-local Multicast Name Resolution	9.4	46380	3.2	1305031	3922	46380	1305031	3922
Domain Name System	0.1	443	0.0	15030	45	443	15030	45
Data	0.1	269	0.4	171990	516	269	171990	516
Cisco Hot Standby Router Protocol	0.4	2063	0.1	40864	122	2063	40864	122
Bootstrap Protocol	0.0	22	0.0	7013	21	22	7013	21
Transmission Control Protocol	0.8	3768	1.4	570773	1715	1488	153748	462

No display filter.

Figura 21: **Presencia del Protocolo LLMNR en la muestra realizada a la red de la CSJLL con el programa Wireshark**
Fuente: **Elaboración Propia**

El protocolo LLMNR tanto como para IPv4 con 7.7% de presencia con más de 37989 de paquetes enviados así mismo el protocolo IPv6 con un 9.4% de presencia y más de 46380 de paquetes enviados cada uno en el periodo de muestra tomada.

PROTOCOLO TCP:

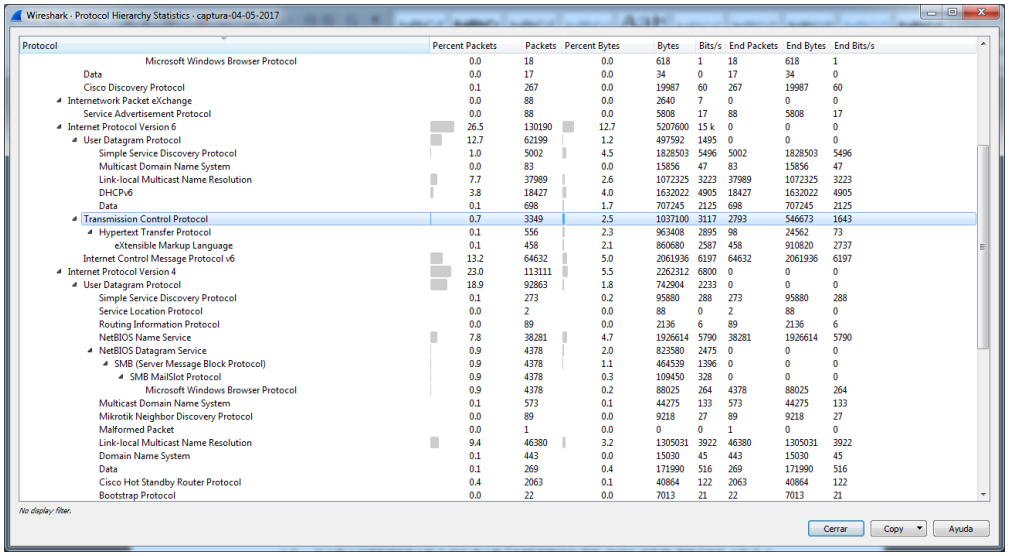


Figura 22: **Presencia del Protocolo TCP en la muestra realizada a la red de la CSJLL con el programa Wireshark**
Fuente: **Elaboración Propia**

El protocolo TCP con un 0.7% de presencia y más de 3349 paquetes enviados en el periodo de muestra tomada.

PROTOCOLO UDP:

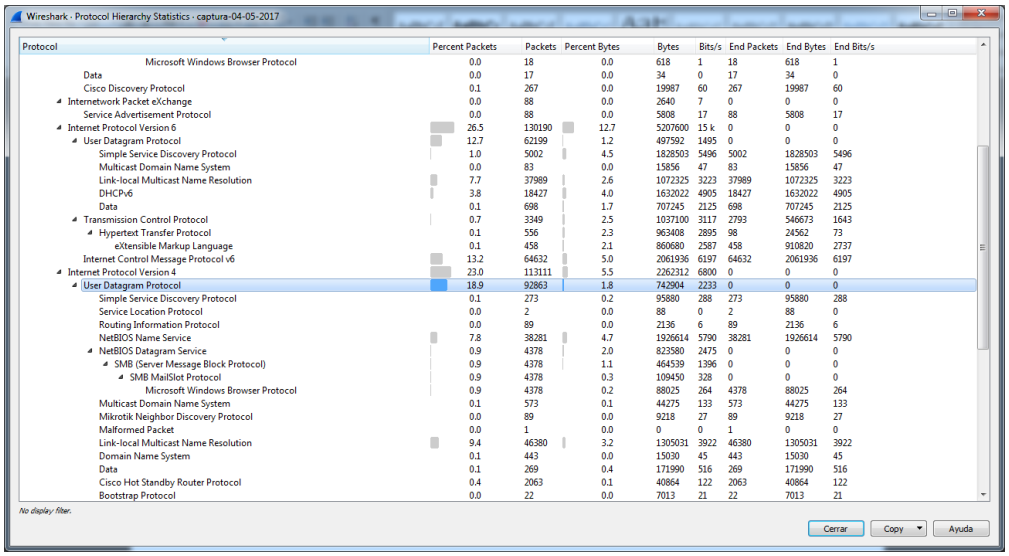


Figura 23: **Presencia del Protocolo UDP en la muestra realizada a la red de la CSJLL con el programa Wireshark**
Fuente: **Elaboración Propia**

El protocolo UDP con un 18.9% de presencia y más de 92863 paquetes enviados en el periodo de muestra tomada.

C) Caracterizar el tráfico de la información de la red

La plataforma informática de la sede judicial de Natasha de la corte superior de justicia de la libertad cuenta con un ISP (Movistar), que es una línea dedicada a la que todos los usuarios conectados llámese, trabajadores que laboran actualmente dentro de esta sede, tenga un ancho de banda adecuado para realizar su trabajo o cualquier otro tipo de tramites, consulta etc., a través del mismo esta sede cuenta con una línea dedicada con un **ancho de banda** de 20Mb.

Este ancho de banda brindado por el ISP llega a un router "CISCO" ubicado en la sala de servidor a lado del departamento de informática, el cual se reparte a los gabinetes los cuales cuentan con un Switch (3COM - 24 puertos) ubicados en cada piso, con una distancia que no supera los 50-60 metros de la corte superior de justicia de la libertad.

El ancho de banda se distribuye por los switches de cada piso para llegar a los equipos por medio de cable UTP CAT6 – PANDUIT, las PC's utilizan una conexión de red 10/100 gigabit ethernet integradas en las computadoras DELL en su gran mayoría.

El servidor HP con capacidad de virtualización es donde se conectan todos los usuarios a realizar las consultas, de una u otra manera dentro de un determinado tiempo todos los días debido a que la gran mayoría trata de conectarse al mismo tiempo para utilizar estas aplicaciones:

- Sistema de intereses legales.

- Servicio de correo electrónico.
- SEJ (Servicio de Expedientes Judiciales).
- Sistema de peritos.
- SIGA (Sistema de Gestión Administrativa).
- SIJ (Sistema Integrado Judicial).
- Notificación electrónica.
- Notificación de audiencias.

Como muestran las Figuras (25, 26 y 27) sobre Wireshark IO Graphs – Red LAN de la CSJLL Error/Protocol con respecto a la congestión y a la perdida de paquetes se muestran un total de perdida cuantificable realizadas en 3 muestras de tráfico en distintas fechas a distintas horas obteniendo así en cada una, un promedio cuantificable en perdida de paquetes con respecto al tiempo haciendo así más fácil su interpretación.

Tomando como referencia el último análisis de tráfico realizado se obtiene un resumen con todos los protocolos existentes y su presencia en la red.

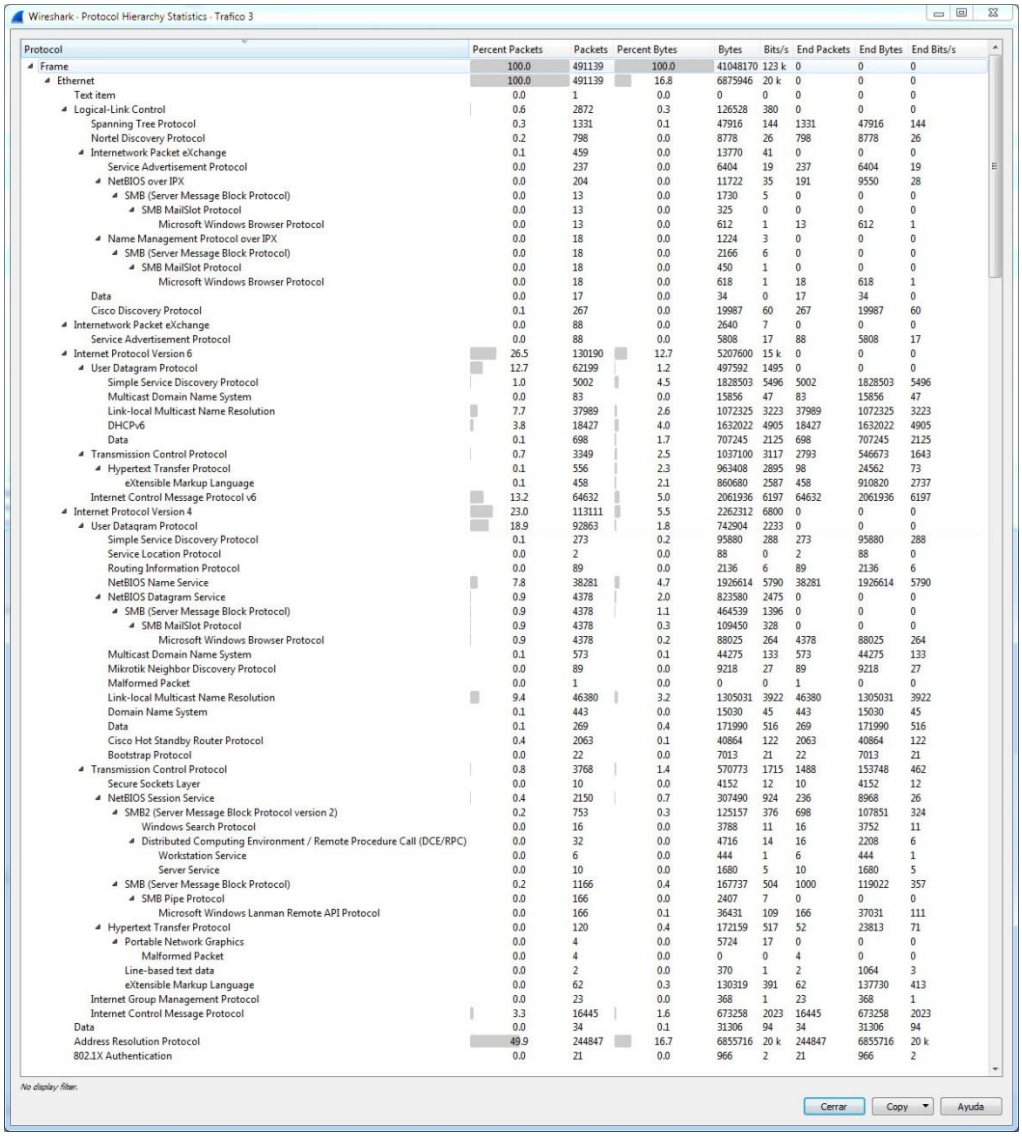


Figura 24: **Wireshark Protocol Hierarchy Statistics**
Fuente: **Elaboración Propia**

3.2.5. TÉCNICAS DE ANÁLISIS DE DATOS

3.2.5.1. Se utilizó las opciones de la herramienta "Wireshark" para analizar el tráfico de la información y determinar que parámetro(s) está significativamente influenciado sobre el rendimiento de la red de datos de la corte superior de justicia de la libertad.

a). El **ancho de banda** es medido por la velocidad máxima en que la información es transferida en una red LAN y que esta es proporcionada por un ISP, con un total de 20Mb dedicada para la corte superior de justicia de la libertad, teniendo así que ser distribuida por los 4 pisos que actualmente cuenta la corte, encaminándose por los 4 gabinetes de distribución que se encuentran en cada piso y llegando a todas las áreas en donde los usuarios con acceso a internet se conectan al mismo tiempo.

b). El **retardo de extremo a extremo o Latencia** es la demora que existe entre el envío de una consulta desde el emisor y el descifrado de la misma por el receptor y esta principalmente en función del tiempo, en la red de la corte, este parámetro se encuentra principalmente a la hora de realizar un consulta en el Sistema de Expedientes Judiciales ya sea al servidor local o al servidor principal (lima) generándose un retardo en las horas de 9:00am - 11:00am momento en el cual se realizan un mayor número de consultas al mismo tiempo queriendo acceder todos al mismo tiempo al servidor y ocasionando un cuello de botella percibida por el usuario que realiza la consulta y generando las molestias de la misma.

c). **Perdida de paquetes o Throughput** denominado como la tasa real de información transferida e una red LAN y el número de mensajes enviados y recibidos de manera exitosa, asociado en su mayoría al ancho de banda disponible en un red LAN también existen distintos factores que pueden afectar este parámetro, en la corte superior de

justicia de la libertad se cuenta con una red de 20 Mb dedicadas el cual puede parecer mucho pero en realidad al momento de realizar la prueba se observó que efectivamente algunos bits en la trasmisión de la misma se pierden, los switchs de todos los gabinetes distribuidos en los 4 pisos son de la marca 3com con un total de 42 puertos cada uno y utilizados solamente la mitad en cada uno con una posibilidad de expansión más adelante se observa que no todos están a su máxima capacidad de puertos, pero no solo debemos atribuirle dicha perdida a los switchs ya que en visitas posteriores y pudiendo constatar con fotos que los gabinetes en algunos pisos se encuentra descuidados, sin mantenimiento, con polvo y en algunos casos sin refrigeración y cables quebrados podemos decir que esto es un grave problema por el cual afecta hoy por hoy a la corte superior de Justicia de La Libertad.

Tomando muestra de cada una de ellas en tres periodos de prueba distintos los cuales fueron denominados:

- Tráfico 1
- Tráfico 2
- Tráfico 3

TRÁFICO 1

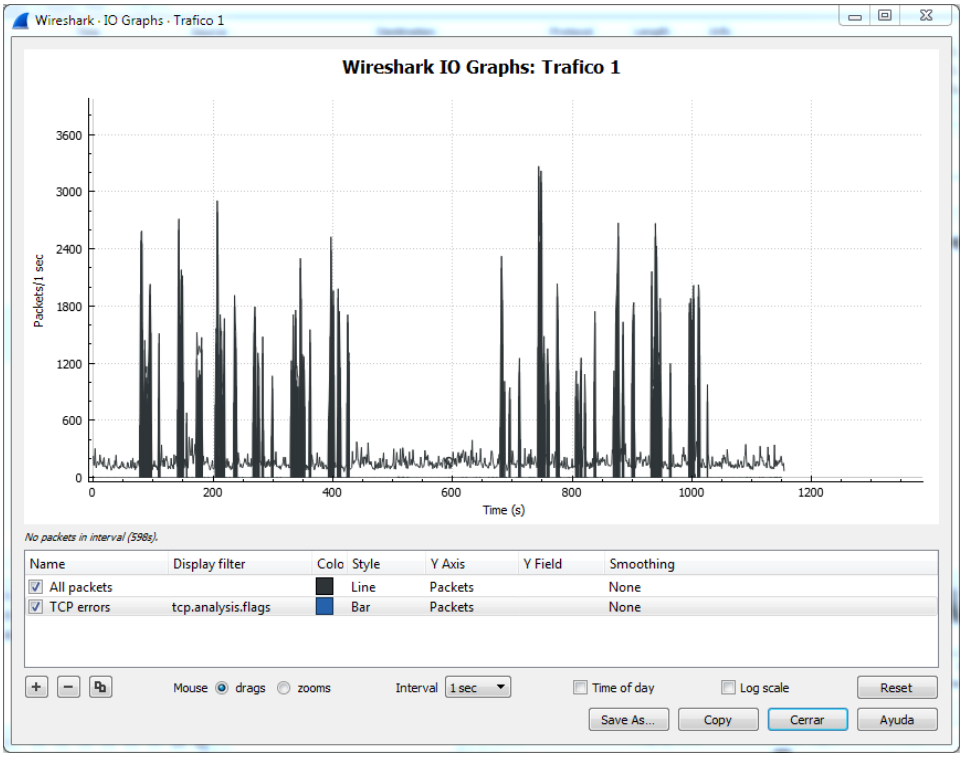


Figura 25: **Wireshark IO Graphs – Tráfico 1 Red LAN de la CSJLL Error/Protocol**
Fuente: **Elaboración Propia**

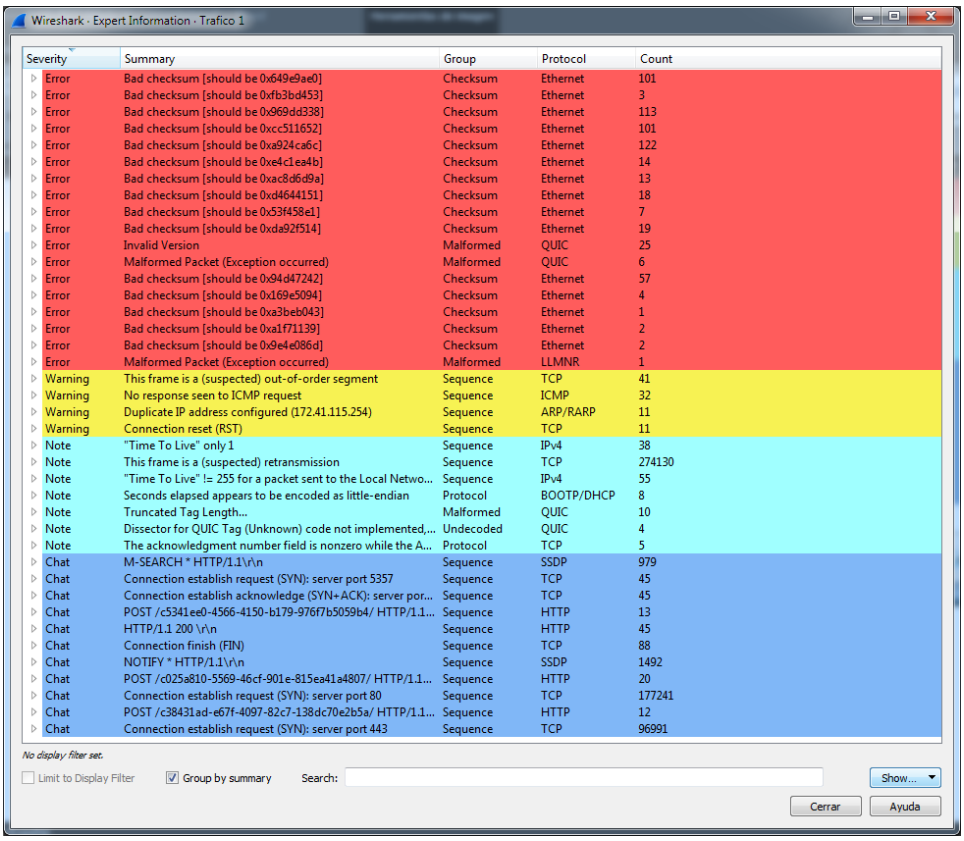


Figura 26: **Expert Information – Tráfico 1 Red LAN de la CSJLL Summary**
Fuente: **Elaboración Propia**

El presente gráfico muestra la tasa de error en un periodo de tiempo de 20 minutos donde en escala máxima de perdida es de casi 3300 pack/seg y los protocolos con más problemas en la red son (Ethernet, TCP, ICMP y ARP/RARP).

TRÁFICO 2

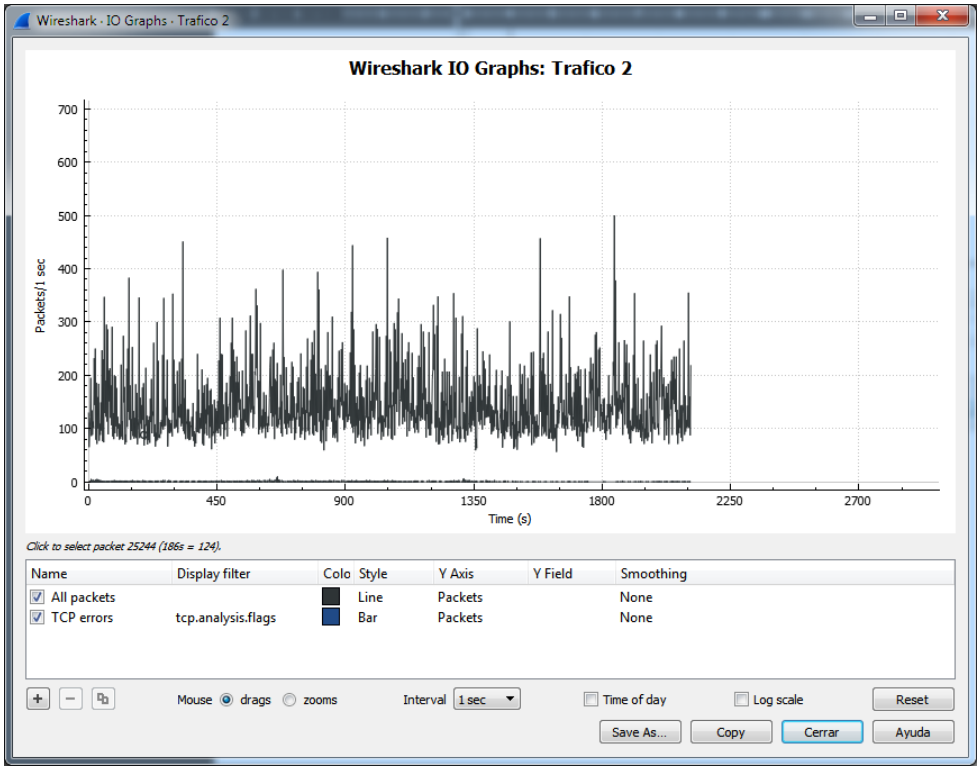


Figura 27: **Wireshark IO Graphs – Tráfico 2 Red LAN de la CSJLL Error/Protocol**
Fuente: **Elaboración Propia**

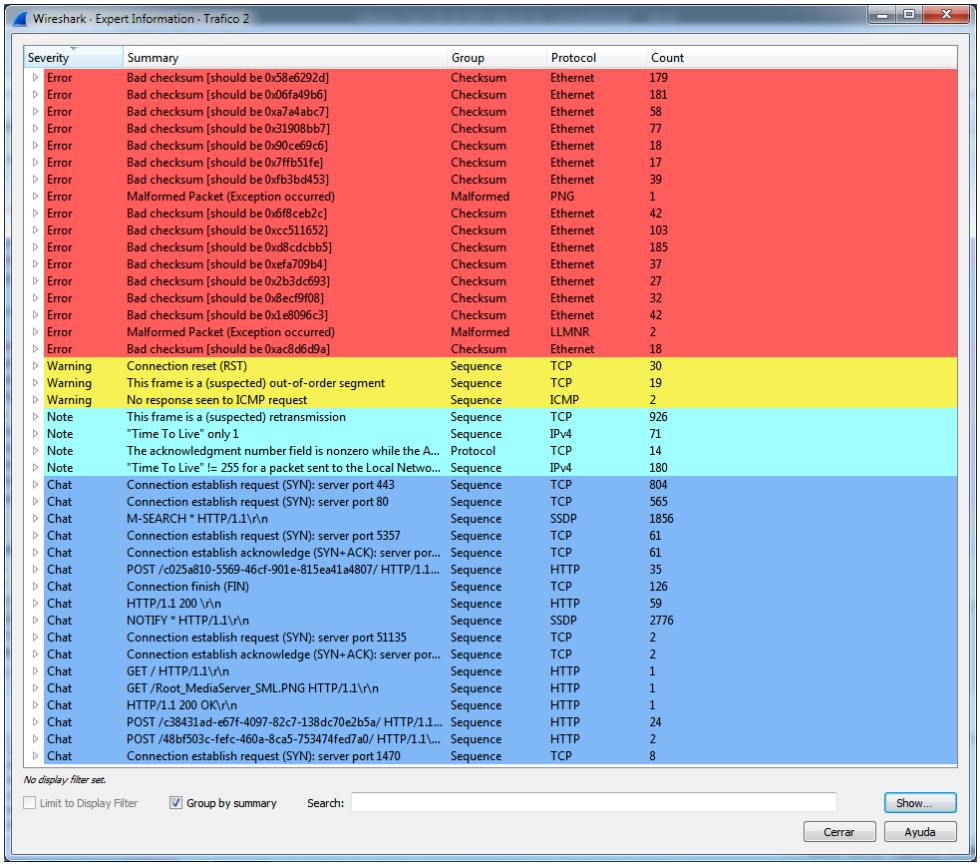


Figura 28: **Expert Information – Tráfico 2 Red LAN de la CSJLL Summary**
Fuente: **Elaboración Propia**

El presente gráfico muestra la tasa de error en un periodo de tiempo de 30 minutos donde en escala máxima de perdida es de casi 500 pack/seg y los protocolos con más problemas en la red son (Ethernet, LLMNR, TCP, ICMP).

TRÁFICO 3

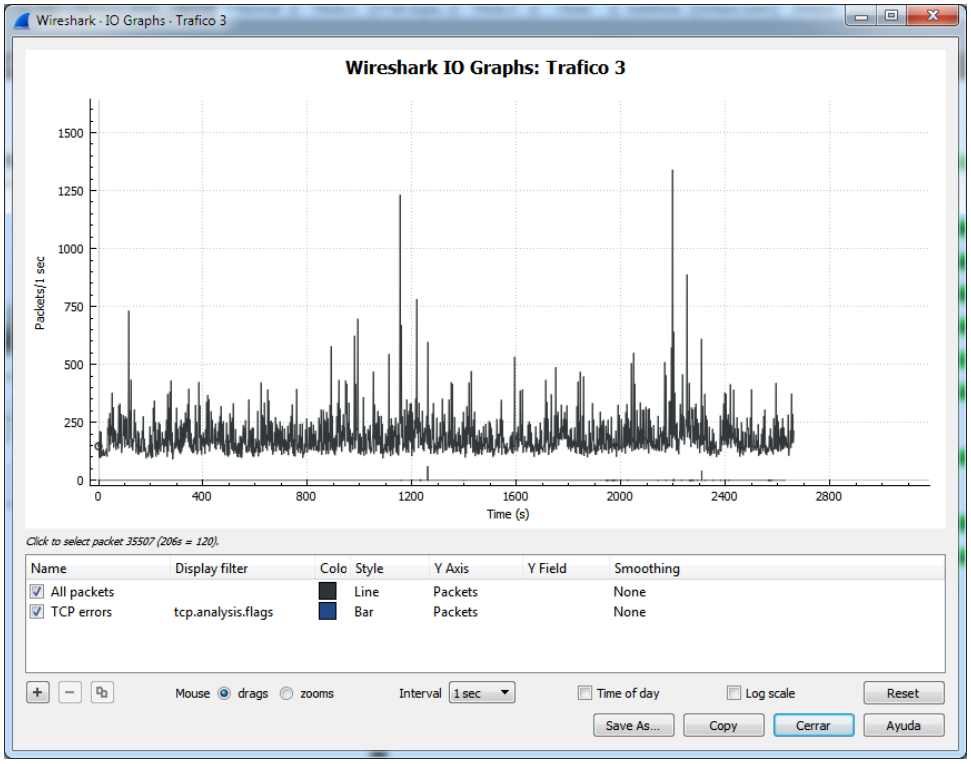


Figura 29: **Wireshark IO Graphs – Tráfico 3 Red LAN de la CSJLL Error/Protocol**
Fuente: **Elaboración Propia**

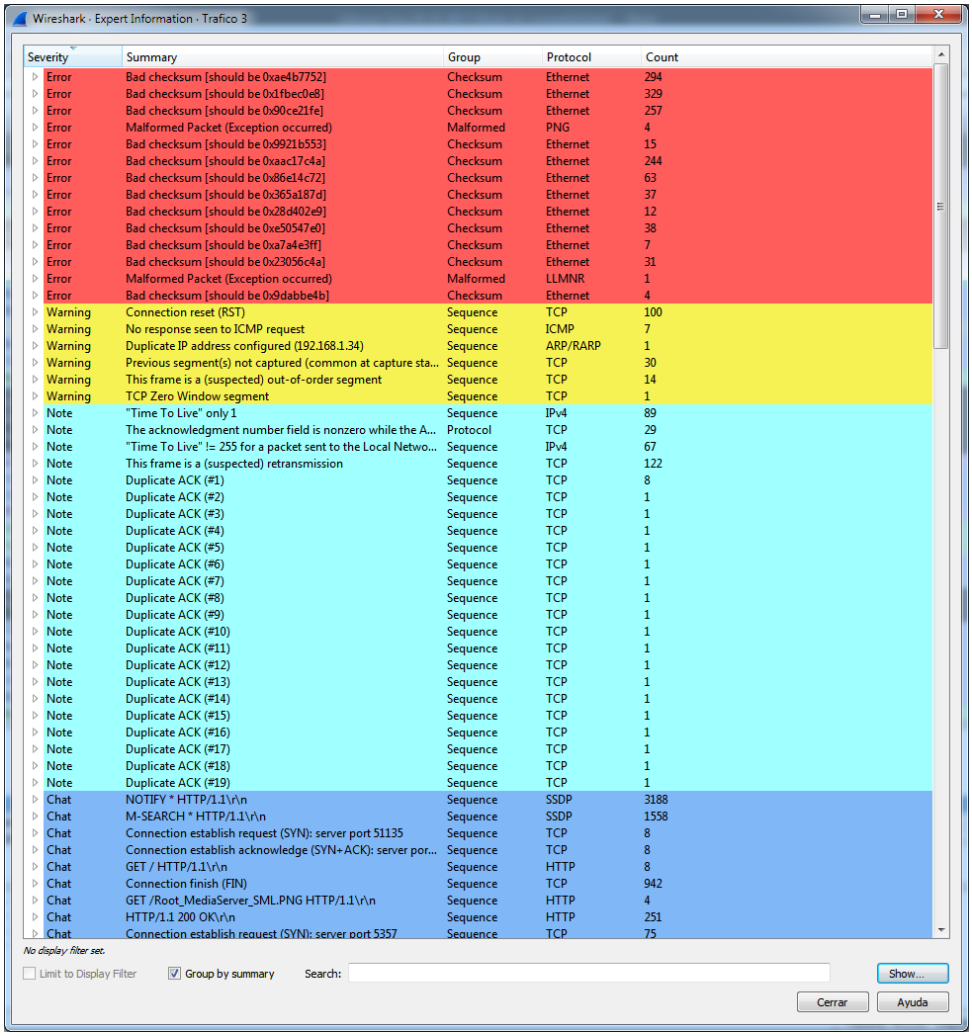


Figura 30: **Expert Information – Tráfico 3 Red LAN de la CSJLL Summary**
Fuente: **Elaboración Propia**

El presente gráfico muestra la tasa de error en un periodo de tiempo de 40 minutos donde en escala máxima de perdida es de casi 1300 pack/seg y los protocolos con más problemas en la red son (Ethernet, LLMNR, TCP, ICMP).

d). La **variación de retardo o Jitter** ligada a la perdida de paquetes o Throughput- se define técnicamente como la variación o el tiempo de llegada de los paquetes causada por la congestión de la red con una pequeña diferencia, esta tiene que ver con la perdida de sincronización o por las diferentes rutas seguidas por los paquetes para llegar a su destino.

Unos de los mayores problemas presentados en la plataforma informática de la corte superior de justicia de la libertad es en reiteradas ocasiones la interrupción inesperadas al momento de descargar un archivo, subir un archivo y/o tratar de conectarse, claro no se da habitualmente pero si en algunas oportunidades se logró constatar por medio del encargado de informática que recibían llamadas quejándose de que su petición no se realizó de manera exitosa, existen muchos algunos factores que podrían estar ocasionando dicha interrupción con respecto al jitter, una de ellas seria la congestión de la red misma ya que en ocasiones se realizan audiencias consecutivas o a la misma hora en distintos auditorios o salas las cuales dan prioridad para realizar una videoconferencia a distintos puntos del país el cual genera un cuellos de botella en la misma, una pérdida de sincronización con el servidor donde se encuentra almacenado dicho documento o las distintas rutas y saltos que realiza la petición hecha por el usuario para llegar a su destino el cual hace que en un momento dado la conexión se pierda.

3.2.5.2. Para evaluar los niveles de influencia se utilizó la herramienta estadística ANOVA.

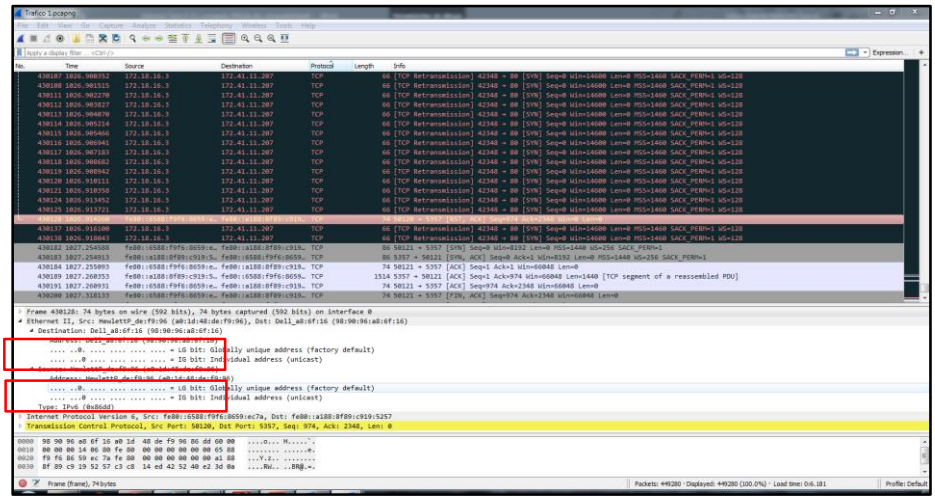


Figura 31: **Wireshark – Tráfico 1 Red LAN de la Corte Superior de Justicia de La Libertad Error Conexión al Cliente**
Fuente: **Elaboración Propia**

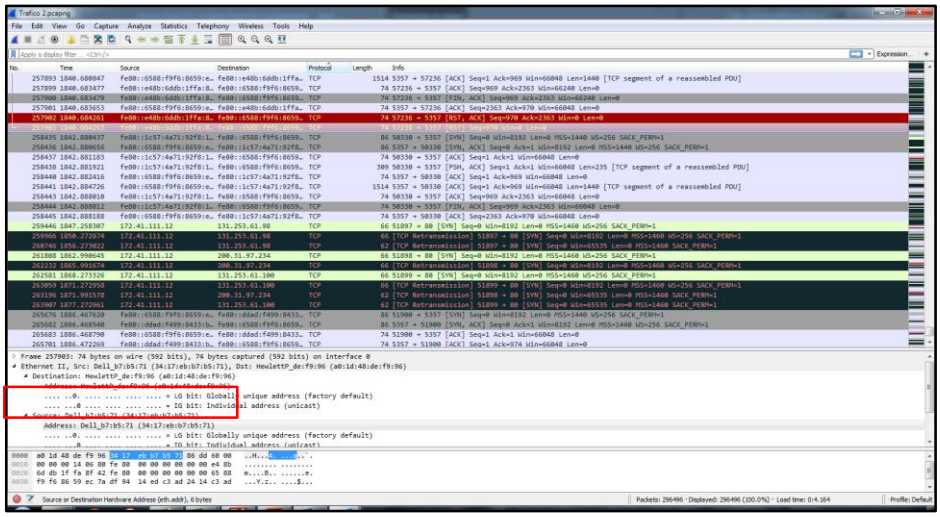


Figura 32: **Wireshark – Tráfico 2 Red LAN de la Corte Superior de Justicia de La Libertad Error Conexión al Servidor**
Fuente: **Elaboración Propia**

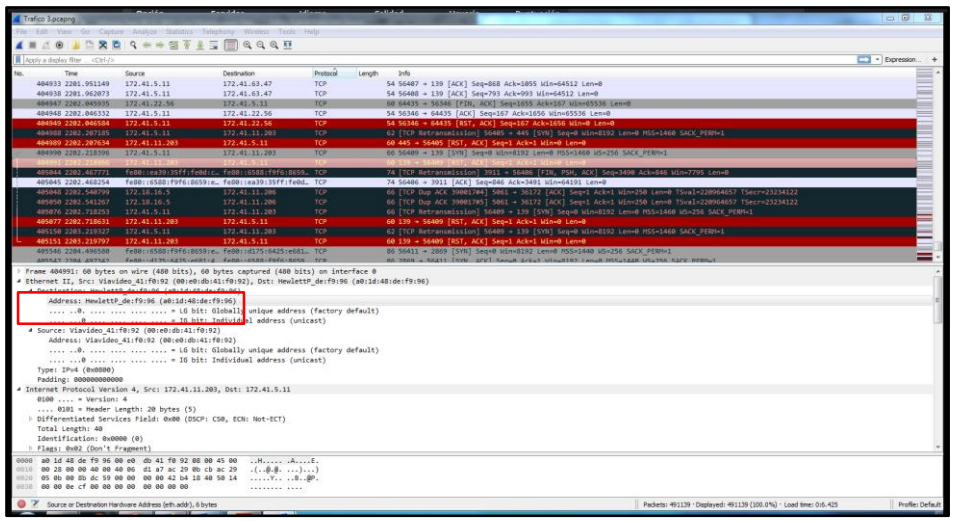


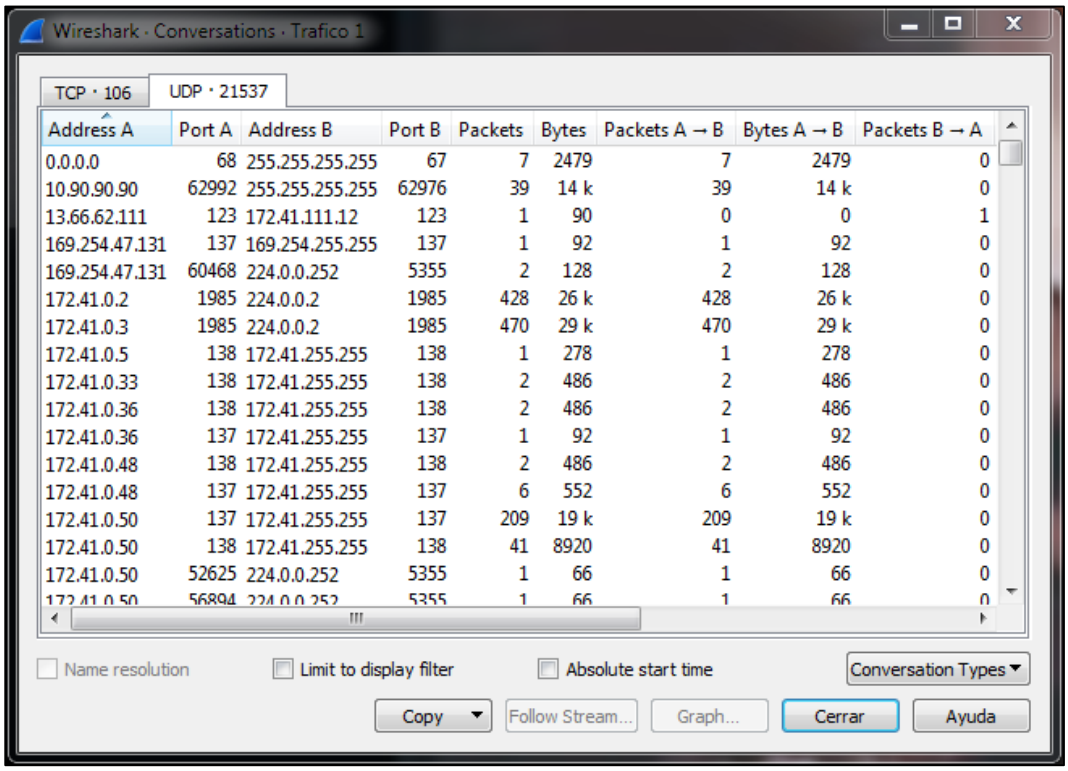
Figura 33: **Wireshark – Tráfico 3 Red LAN de la Corte Superior de Justicia de La Libertad Error Conexión al Servidor**
Fuente: **Elaboración Propia**

CAPÍTULO IV

RESULTADOS

4 RESULTADOS

Se determinó que muchas de las aplicaciones presentes según el analizador de tráfico utilizan el protocolo TCP o UDP ya que estos son protocolos orientado a la conexión lo cual asegura una entrega de paquetes más confiable.



Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A
0.0.0.0	68	255.255.255.255	67	7	2479	7	2479	0
10.90.90.90	62992	255.255.255.255	62976	39	14 k	39	14 k	0
13.66.62.111	123	172.41.111.12	123	1	90	0	0	1
169.254.47.131	137	169.254.255.255	137	1	92	1	92	0
169.254.47.131	60468	224.0.0.252	5355	2	128	2	128	0
172.41.0.2	1985	224.0.0.2	1985	428	26 k	428	26 k	0
172.41.0.3	1985	224.0.0.2	1985	470	29 k	470	29 k	0
172.41.0.5	138	172.41.255.255	138	1	278	1	278	0
172.41.0.33	138	172.41.255.255	138	2	486	2	486	0
172.41.0.36	138	172.41.255.255	138	2	486	2	486	0
172.41.0.36	137	172.41.255.255	137	1	92	1	92	0
172.41.0.48	138	172.41.255.255	138	2	486	2	486	0
172.41.0.48	137	172.41.255.255	137	6	552	6	552	0
172.41.0.50	137	172.41.255.255	137	209	19 k	209	19 k	0
172.41.0.50	138	172.41.255.255	138	41	8920	41	8920	0
172.41.0.50	52625	224.0.0.252	5355	1	66	1	66	0
172.41.0.50	56894	224.0.0.252	5355	1	66	1	66	0

Figura 34: **Wireshark – Tráfico 1 – Conversaciones Totales TCP - UDP**
Fuente: **Elaboración Propia**

Como se observa en el análisis del tráfico existen muchas aplicaciones TCP las cuales son muy expansivas y consumen una gran porción de la capacidad de la red y tienen un grado de significancia en la red en función del tiempo y numero de muestras hechas, según las tablas de (IO Graphs – Error/Protocol del Trafico 1,2 y 3).

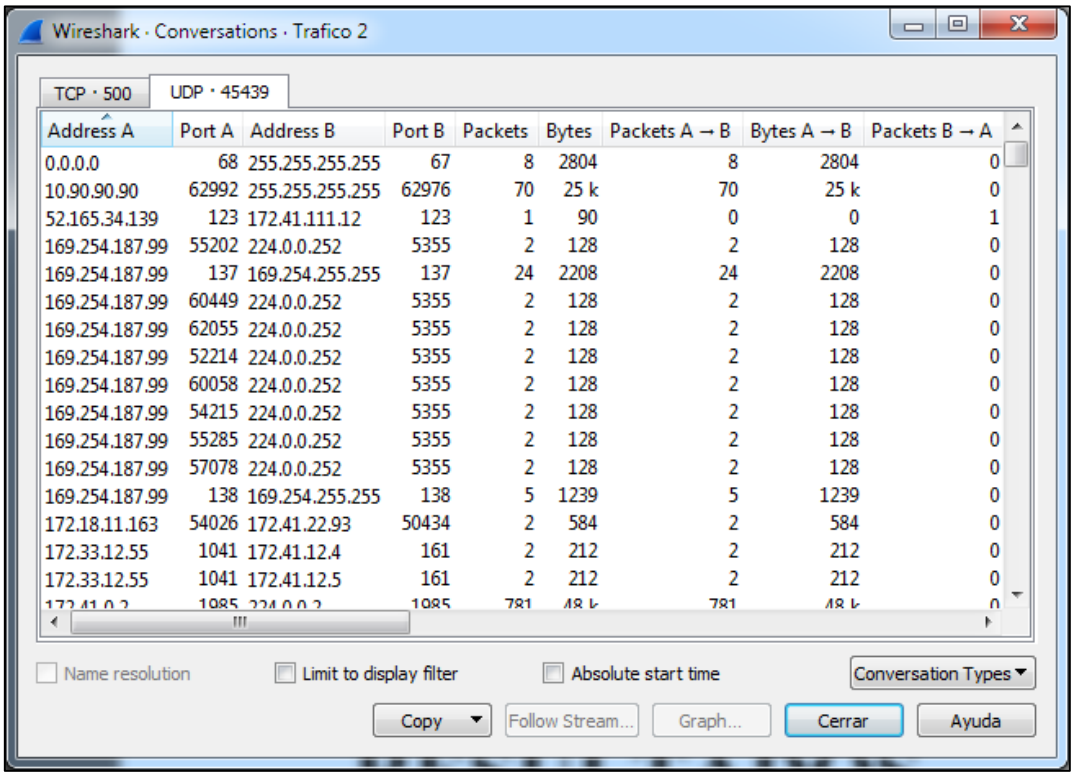


Figura 35: **Wireshark – Tráfico 2 – Conversaciones Totales TCP - UDP**
Fuente: **Elaboración Propia**

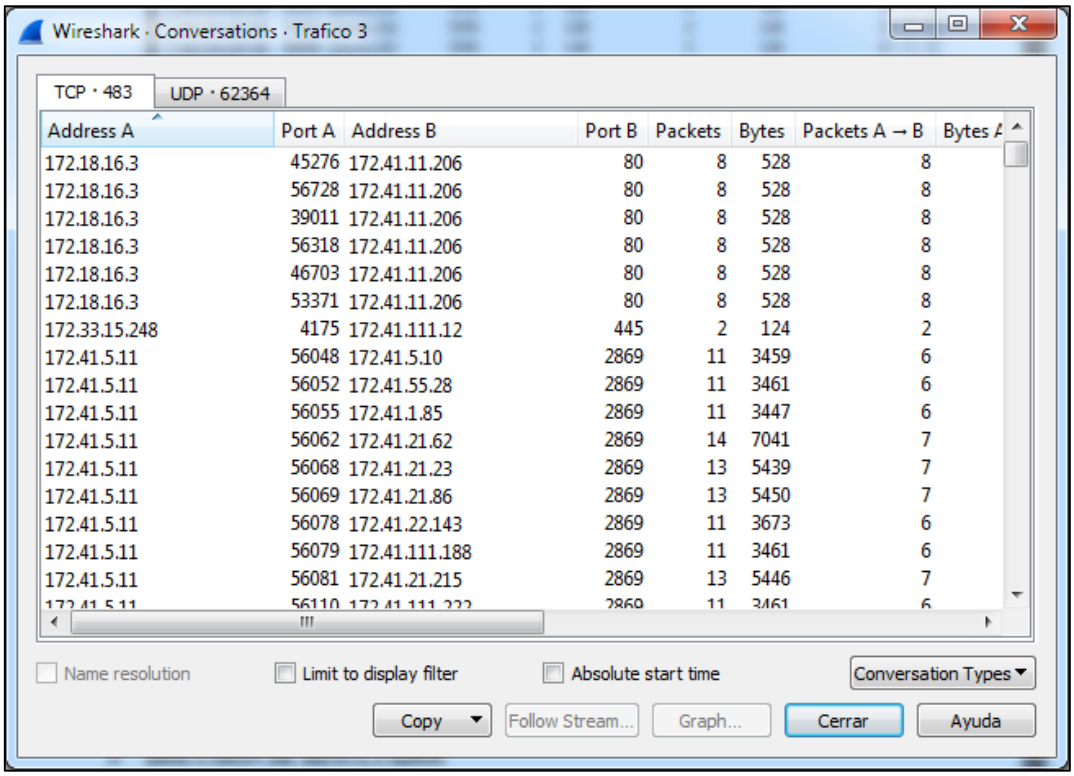


Figura 36: **Wireshark – Tráfico 3 – Conversaciones Totales TCP - UDP**
Fuente: **Elaboración Propia**

Mediante la herramienta de análisis Wireshark se determinó los factores predominantes relacionados con el parámetro del Jitter las cuales son la cantidad mínima y máximo de paquetes presentes según las aplicaciones y su relación con los protocolos, estas que son generadas por la el total de host conectados en la red:

name	Count	Average	Min-val	Max-val	Rate--ms-	Percent	Burst-rate	Burst-start	name2	isrange	Count3	Average4	Min-val5	Max-val6	Rate--ms-7	Percent8	Burst-rate9	Burst-start10
Packet Lengths	449280	73.09	42	1514	0.3892	100%	4.51	207.74	0-19	VERDADERO	0	-	-	-	0	0.00%	-	-
Packet Lengths	449280	73.09	42	1514	0.3892	100%	4.51	207.74	20-39	VERDADERO	0	-	-	-	0	0.00%	-	-
Packet Lengths	449280	73.09	42	1514	0.3892	100%	4.51	207.74	40-79	VERDADERO	380286	64.98	42	78	0.3294	84.64%	4.4400	207.740
Packet Lengths	449280	73.09	42	1514	0.3892	100%	4.51	207.74	80-159	VERDADERO	63433	95.95	81	159	0.055	14.12%	2.3500	277.286
Packet Lengths	449280	73.09	42	1514	0.3892	100%	4.51	207.74	160-319	VERDADERO	3579	216.10	160	309	0.0031	0.80%	0.0900	508.716
Packet Lengths	449280	73.09	42	1514	0.3892	100%	4.51	207.74	320-639	VERDADERO	1597	532.82	342	590	0.0014	0.36%	0.2000	209.441
Packet Lengths	449280	73.09	42	1514	0.3892	100%	4.51	207.74	640-1279	VERDADERO	268	949.54	686	1159	0.0002	0.06%	0.0600	756.311
Packet Lengths	449280	73.09	42	1514	0.3892	100%	4.51	207.74	1280-2559	VERDADERO	117	1389.93	1302	1514	0.0001	0.03%	0.0800	756.667
Packet Lengths	449280	73.09	42	1514	0.3892	100%	4.51	207.74	2560-5119	VERDADERO	0	-	-	-	0	0.00%	-	-
Packet Lengths	449280	73.09	42	1514	0.3892	100%	4.51	207.74	5120 and greater	VERDADERO	0	-	-	-	0	0.00%	-	-

***Tabla 8*: Longitud mínima y máxima de los paquetes presentes en la 1° muestra realizada**
Fuente: Elaboración Propia

name	Count	Average	Min-val	Max-val	Rate--ms-	Percent	Burst-rate	Burst-start	name2	isrange	Count3	Average4	Min-val5	Max-val6	Rate--ms-7	Percent8	Burst-rate9	Burst-start10
Packet Lengths	296496	86.65	42	1514	0.1405	100%	3.55	330.446	0-19	VERDADERO	0	-	-	-	0	0.00%	-	-
Packet Lengths	296496	86.65	42	1514	0.1405	100%	3.55	330.446	20-39	VERDADERO	0	-	-	-	0	0.00%	-	-
Packet Lengths	296496	86.65	42	1514	0.1405	100%	3.55	330.446	40-79	VERDADERO	164245	63.28	42	79	0.0778	55.40%	0.7800	83.699
Packet Lengths	296496	86.65	42	1514	0.1405	100%	3.55	330.446	80-159	VERDADERO	122510	95.72	81	159	0.0581	41.32%	3.1100	330.406
Packet Lengths	296496	86.65	42	1514	0.1405	100%	3.55	330.446	160-319	VERDADERO	6141	214.07	160	314	0.0029	2.07%	0.1100	1590.113
Packet Lengths	296496	86.65	42	1514	0.1405	100%	3.55	330.446	320-639	VERDADERO	2857	537.46	340	586	0.0014	0.96%	0.1300	641.429
Packet Lengths	296496	86.65	42	1514	0.1405	100%	3.55	330.446	640-1279	VERDADERO	564	837.26	686	1157	0.0003	0.19%	0.2000	1079.675
Packet Lengths	296496	86.65	42	1514	0.1405	100%	3.55	330.446	1280-2559	VERDADERO	179	1384.09	1306	1514	0.0001	0.06%	0.0600	1161.164
Packet Lengths	296496	86.65	42	1514	0.1405	100%	3.55	330.446	2560-5119	VERDADERO	0	-	-	-	0	0.00%	-	-
Packet Lengths	296496	86.65	42	1514	0.1405	100%	3.55	330.446	5120 and greater	VERDADERO	0	-	-	-	0	0.00%	-	-

***Tabla 9*: Longitud mínima y máxima de los paquetes presentes en la 2° muestra realizada**
Fuente: Elaboración Propia

name	Count	Average	Min-val	Max-val	Rate--ms-	Percent	Burst-rate	Burst-start	name2	isrange	Count3	Average4	Min-val5	Max-val6	Rate--ms-7	Percent8	Burst-rate9	Burst-start10
Packet Lengths	491139	83.58	42	1514	0.1845	100%	8.41	2197.236	0-19	VERDADERO	0	-	-	-	0	0.00%	-	-
Packet Lengths	491139	83.58	42	1514	0.1845	100%	8.41	2197.236	20-39	VERDADERO	0	-	-	-	0	0.00%	-	-
Packet Lengths	491139	83.58	42	1514	0.1845	100%	8.41	2197.236	40-79	VERDADERO	315057	62.18	42	79	0.1184	64.15%	2.4100	1259.723
Packet Lengths	491139	83.58	42	1514	0.1845	100%	8.41	2197.236	80-159	VERDADERO	162677	96.17	80	159	0.0611	33.12%	4.5900	2251.998
Packet Lengths	491139	83.58	42	1514	0.1845	100%	8.41	2197.236	160-319	VERDADERO	7453	216.16	160	314	0.0028	1.52%	0.7100	2197.272
Packet Lengths	491139	83.58	42	1514	0.1845	100%	8.41	2197.236	320-639	VERDADERO	4207	511.71	322	633	0.0016	0.86%	0.4700	2197.266
Packet Lengths	491139	83.58	42	1514	0.1845	100%	8.41	2197.236	640-1279	VERDADERO	1051	991.57	655	1271	0.0004	0.21%	1.2900	2197.273
Packet Lengths	491139	83.58	42	1514	0.1845	100%	8.41	2197.236	1280-2559	VERDADERO	694	1453.55	1297	1514	0.0003	0.14%	0.7000	2197.272
Packet Lengths	491139	83.58	42	1514	0.1845	100%	8.41	2197.236	2560-5119	VERDADERO	0	-	-	-	0	0.00%	-	-
Packet Lengths	491139	83.58	42	1514	0.1845	100%	8.41	2197.236	5120 and greater	VERDADERO	0	-	-	-	0	0.00%	-	-

***Tabla 10*: longitud mínima y máxima de los paquetes presentes en la 3° muestra realizada**
Fuente: Elaboración Propia

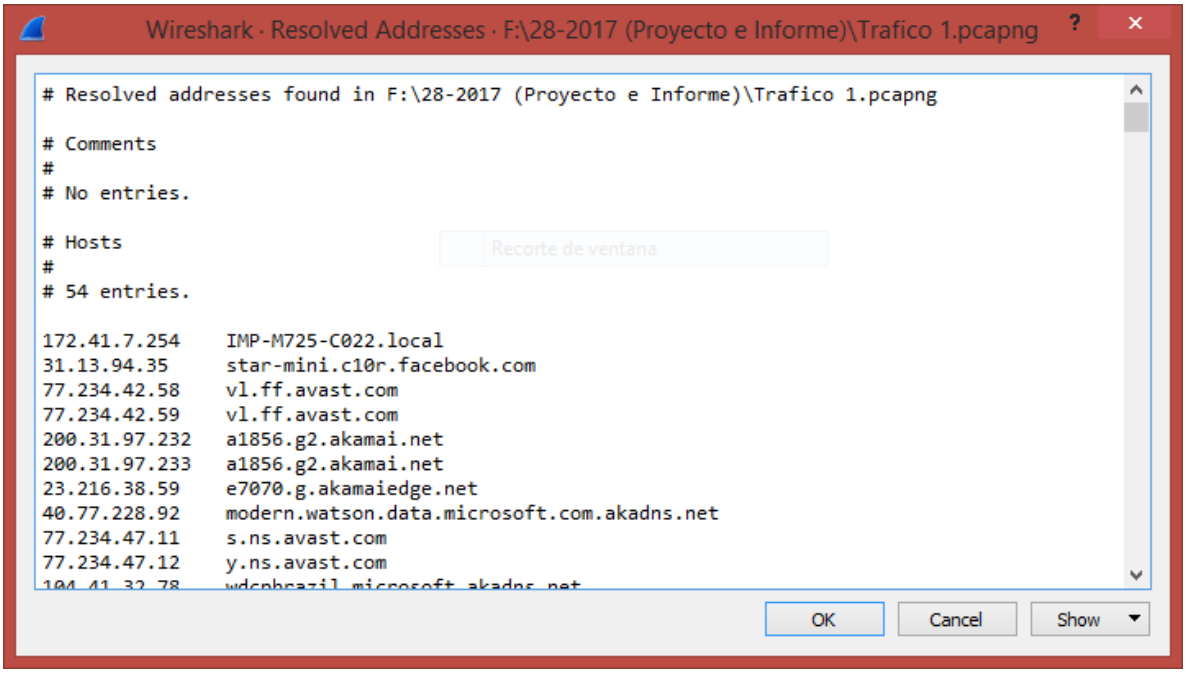


***Figura 37*: N° Total de Host conectados en la 1° muestra realizada**
Fuente: Elaboración Propia

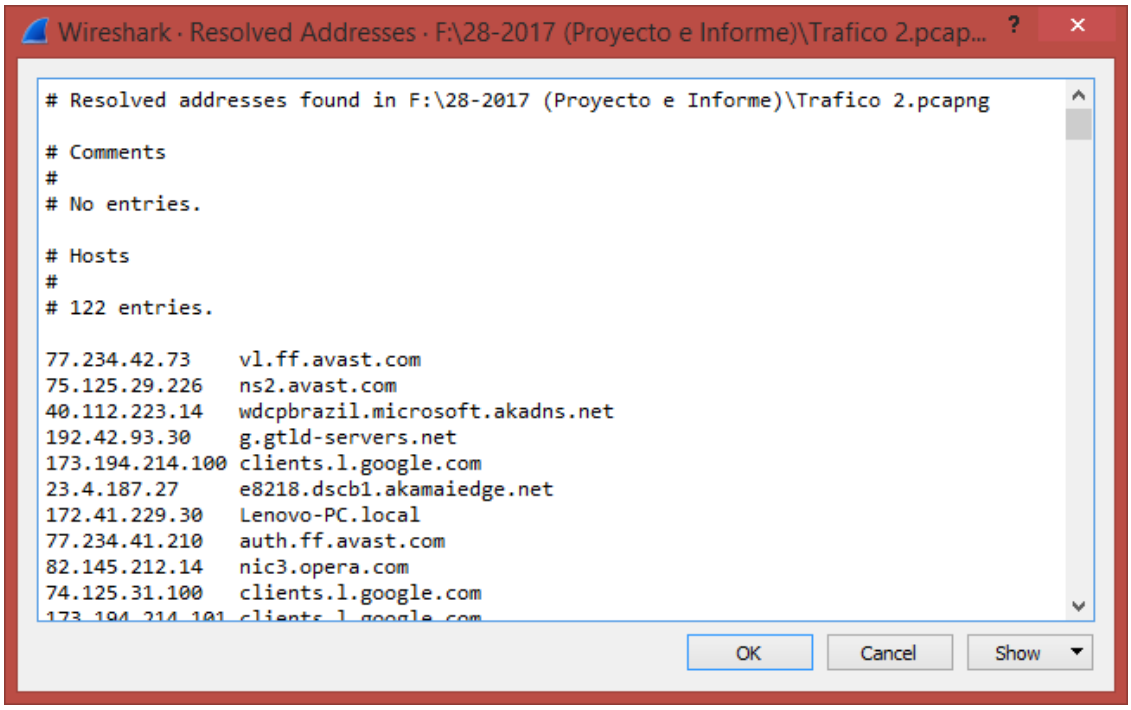


***Figura 38*: N° Total de Host conectados en la 2° muestra realizada**
Fuente: Elaboración Propia

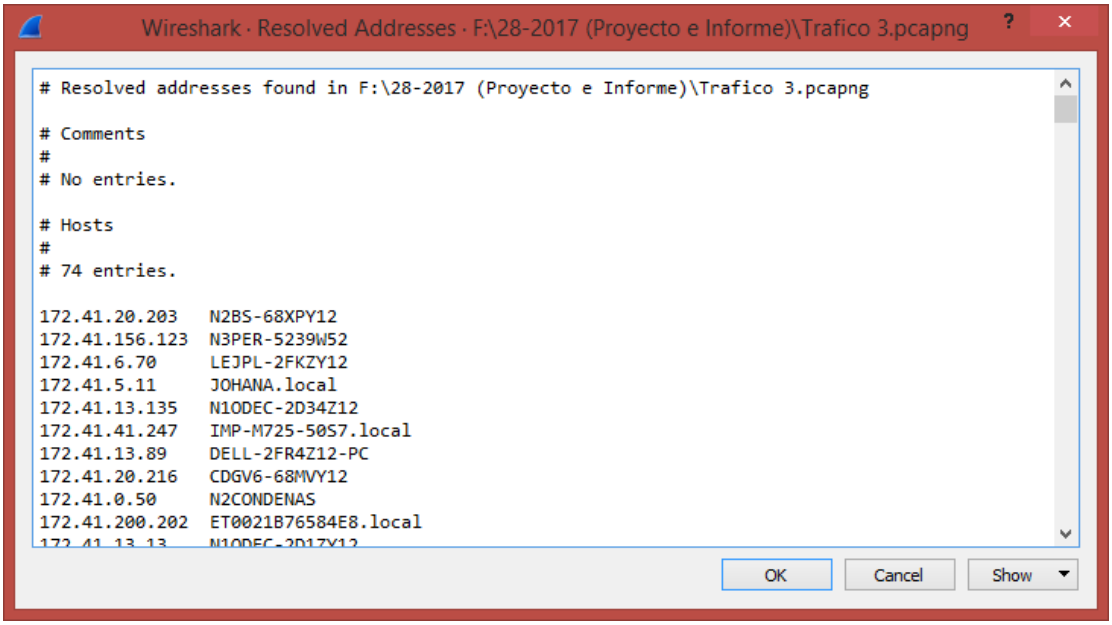


***Figura 39*: N° Total de Host conectados en la 3° muestra realizada**
Fuente: Elaboración Propia

Por lo tanto, se considera los factores: Tamaño del paquete, Número de PCs activas en la red de los totales realizadas la 3 muestras realizadas y distancia entre el PC (Cliente) y el Servidor. Cada factor presenta un número específico de niveles cuantitativos acorde con el siguiente Tabla.

Factor	Descripción	N° Niveles
1	Tamaño de paquetes transmitidos por la red	12
2	Numero de Host conectados	3
3	Distancia del Pc y Servidor	6

***Tabla 11:* Factores vs Niveles**
***Fuente*: Elaboración propia**

Corresponde a un diseño factorial de 12x3x6=216 combinaciones de tratamientos o puntos experimentales.

Los valores establecidos para cada uno de los factores son:

- Tamaño de paquetes trasmitidos por la red: 42, 79, 80, 159, 160, 314, 322, 633, 655, 1271, 1297, 1514 (Kb)
- Números de Host conectados: 54, 122, 74
- Distancia entre PC-Cliente y Servidor: 10, 20, 30, 40,50, 60 (m)

Quedando nuestra matriz de la siguiente manera:

Tamaños de paquete transmitidos por la red	Numero de Host conectados 54 Distancia entre PC-Cliente y Servidor						Numero de Host conectados 122 Distancia entre PC-Cliente y Servidor						Numero de Host conectados 72 Distancia entre PC-Cliente y Servidor					
	10	20	30	40	50	60	10	20	30	40	50	60	10	20	30	40	50	60
42	0,40	0,43	0,46	0,48	0,51	0,54	0,42	0,44	0,46	0,51	0,59	0,56	0,46	0,50	0,53	0,52	0,53	0,55
79	0,73	0,76	0,79	0,81	0,84	0,87	0,80	0,77	0,82	0,82	0,89	0,94	0,78	0,81	0,82	0,89	0,92	0,94
80	0,74	0,77	0,79	0,82	0,85	0,88	0,75	0,80	0,86	0,90	0,91	0,92	0,74	0,80	0,84	0,83	0,89	0,96
159	1,44	1,47	1,50	1,52	1,55	1,58	1,49	1,54	1,51	1,55	1,63	1,59	1,49	1,47	1,52	1,55	1,56	1,62
160	1,45	1,48	1,50	1,53	1,56	1,59	1,53	1,50	1,52	1,59	1,60	1,60	1,50	1,48	1,58	1,58	1,62	1,65
314	2,82	2,85	2,87	2,90	2,93	2,96	2,88	2,85	2,95	2,98	2,93	3,01	2,89	2,85	2,94	2,93	2,99	2,98
322	2,89	2,92	2,94	2,97	3,00	3,03	2,92	3,00	3,02	2,99	3,06	3,04	2,91	2,95	3,01	3,01	3,06	3,09
633	5,65	5,68	5,71	5,73	5,76	5,79	5,71	5,74	5,75	5,78	5,81	5,84	5,66	5,69	5,79	5,74	5,79	5,82
655	5,85	5,87	5,90	5,93	5,96	5,99	5,92	5,88	5,94	5,99	5,99	6,06	5,89	5,89	5,96	5,97	5,99	6,04
1271	11,32	11,35	11,37	11,40	11,43	11,46	11,40	11,36	11,45	11,47	11,51	11,49	11,34	11,40	11,42	11,41	11,50	11,46
1297	11,55	11,58	11,61	11,63	11,66	11,69	11,61	11,61	11,64	11,64	11,68	11,72	11,59	11,64	11,63	11,70	11,73	11,70
1514	13,48	13,51	13,53	13,56	13,59	13,62	13,53	13,56	13,56	13,56	13,60	13,68	13,53	13,56	13,55	13,56	13,64	13,64

Tabla 12: **Matriz (Tamaño de Paquete transmitidos por la red, Numero de Hosts conectados y Distancias entre Pc-Cliente y Servidor)**
***Fuente*: Elaboración propia**

A través del uso del software estadístico Statgraphics, se realizó un análisis multifactorial de la varianza para Jitter, el cual realiza varios tests para determinar qué factores tienen un efecto estadísticamente significativo en el Jitter como variable de salida.

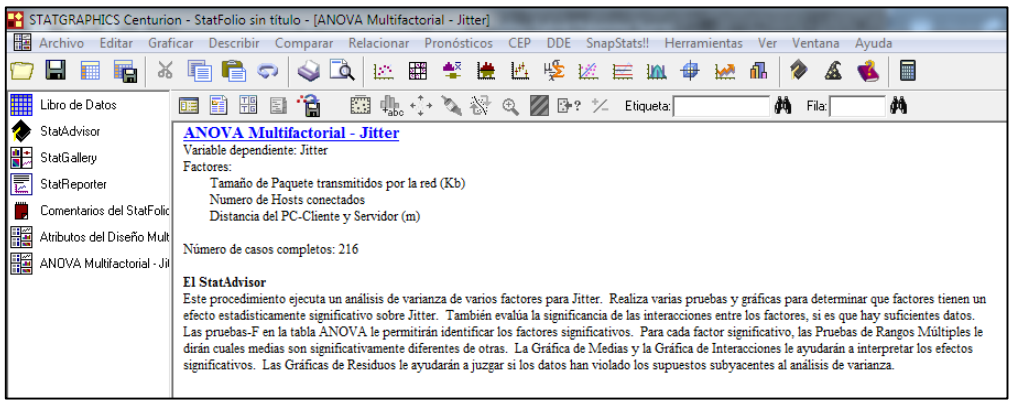


Figura 40 **STATGRAPHICS Centurion – ANOVA Multifactorial Jitter**
Fuente: **Elaboración Propia**

Análisis de Varianza para Jitter - Suma de Cuadrados Tipo III

Fuente	*Suma de Cuadrados*	*Gl*	*Cuadrado Medio*	*Razón-F*	*Valor-P*
EFECTOS PRINCIPALES					
A:Tamaño de Paquetes (kb)	4458,48	11	405,317	985764,23	0,0000
B:Numero de Hosts conectados	0,0778731	2	0,0389366	94,70	0,0000
C:Distancia del PC y Servidor (m)	0,496448	5	0,0992896	241,48	0,0000
INTERACCIONES					
AB	0,0081713	22	0,000371423	0,90	0,5906
AC	0,0223963	55	0,000407205	0,99	0,5061
BC	0,00172685	10	0,000172685	0,42	0,9344
RESIDUOS	0,0452287	110	0,00041117		
TOTAL (CORREGIDO)	4459,14	215			

Todas las razones-F se basan en el cuadrado medio del error residual

Tabla 13: **Tabla ANOVA completa para Jitter**
***Fuente*: Elaboración propia**

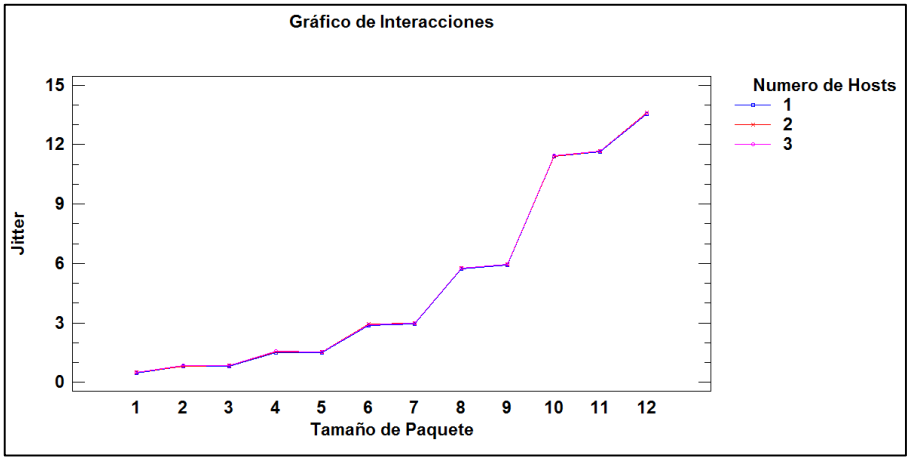


Figura 41: **Interacción Tamaño del Paquete - Host**
***Fuente:* Elaboración Propia**

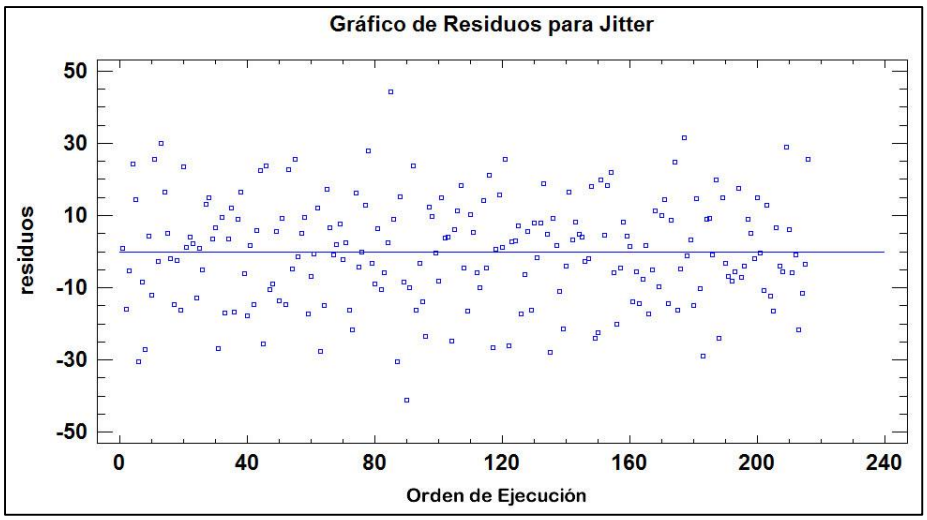


Figura 42: **Residuos según el orden en la toma de los datos**
***Fuente:* Elaboración Propia**

5 DISCUSIÓN DE RESULTADOS

- Según la caracterización de los parámetros basados en la normativa ITU-T G.1010 "Transmission Systems And Media, Digital Systems And Networks" se puede observar que el Jitter es el parámetro con mayor tolerancia respecto al tráfico de datos dentro de la red en un rango de 200ms a 60s, respecto a los otros parámetros como son la latencia 2 y 15 ms, pérdida de paquetes de 0% y ancho de banda entre 1Kb y mayores de 1Mb.

- Mediante la herramienta de análisis Wireshark se determinaron los valores de 42Kb y 1514Kb como cantidad mínima y máxima de paquetes presentes en cada una de las muestras realizadas; así mismo se determinó el total de 54, 122 y 74 host conectados en cada una de las muestras capturadas.

- El estudio factorial de los tres factores como: el tamaño de paquetes trasmitidos por la red, el número de Host conectados, y la distancia entre PC-Cliente – Servidor (A, B, C) permitió investigar los efectos de las combinaciones entre ellos: A, B, C, AB, AC, BC y ABC; la tabla ANOVA descompone la variabilidad del parámetro JITTER en las contribuciones debidas a los 3 factores. Se ha medido la contribución de cada factor eliminando los efectos del resto de los factores. Según el análisis de varianza, los 6 $p-values$ son inferiores a 0,05, lo cual indica que estos factores tienen un efecto estadísticamente significativo en el Jitter, para un 95,0% de confianza.

6 CONCLUSIONES

- Según la caracterización de los parámetros basados en la normativa ITU-T G.1010 "Transmission Systems And Media, Digital Systems And Networks" se determinó que el Jitter es el parámetro con mayor relevancia dentro de la red, respecto a los otros parámetros como la latencia, pérdida de paquetes y el ancho de banda.

- Después de analizar el tráfico de la red se determinó el tamaño de paquetes, el número de host, distancias pc-cliente y servidor como factores predominantes relacionados con el parámetro de mayor relevancia (Jitter).

- Se determinó la importancia de tener en cuenta que las interacciones entre estos factores arrojaron efectos estadísticamente significativos relacionados al Jitter y son aquellas que tienen en común el factor de número de host conectados a la red.

7 RECOMENDACIONES

- En esta investigación se delimito a hacer el análisis específicamente con los factores relacionados con el Jitter sin embargo se recomienda hacer el estudio y análisis de otros factores relacionados con otros parámetros de calidad de servicio, aplicando las técnicas utilizadas en esta investigación.

- Los resultados obtenidos en la presente investigación se obtuvieron a partir del análisis de los datos proporcionados por el programa Wireshark, sin embargo, se recomienda hacer una comparativa de otras herramientas analizadoras de tráfico de red.

- En esta investigación se obtuvieron datos utilizando herramientas a nivel de software sin embargo se recomienda realizar una comparativa de estos resultados con datos obtenidos a través de herramientas físicas.

8 REFERENCIAS BIBLIOGRÁFICAS

MATERIAL DIDACTICO (LIBROS).

- CISCO. Networkers Solutions Forum Routed Fast Converence and High Availability, 2006.
- COMER, Douglas. Redes Globales de Información con Internet y TCP/IP. México: Prentice–Hall, 1996.
- REGIS, Joseph. Comunicaciones Inalámbricas de Banda Ancha. McGraw-Hill, 2003.
- STALLINGS, William. Comunicación y redes de computadoras. Pearson-Education, 2000.
- STALLINGS, William. Organización y arquitectura de computadoras. Great Prentice-Hall, 2006.
- STALLINGS, William. Redes de internet de alta velocidad. Pearson-Educación, 2003.
- TANENBAUM, Andrew. Redes de Computadoras. México: Prentice–Hall, 2003.
- JENSEN Bente, SLAVENSKY Henning KJAERSGAARD Soren. Benchmarking and QoS of House Powerline Equipment for AV-Streaming Application. IEEE Proceedings of ISPLC2006, Orlando, 2006.
- MARTINEZ B., Ciro. Estadística y Muestreo. 9 Edición México: Ecoe ediciones, 2006.
- LEE M. K., NEWMAN R., LATCHMAN H. A., KATAR S., YONGE L. HomePlug 1.0 Powerline Communication LANs Protocol Description and Comparative Performance Results. Accepted for publication in the Special Issue of the International Journal on Communicaction Systems on Powerline Communicacions, 2003.

RECURSOS BIBLIOGRÁFICOS EN LÍNEA.

- "Redes Virtuales VLANs." (2011 [citado el 16 de Marzo de 2011]) disponible en http://www.textoscientificos.com/redes/redes-virtuales
- Calle, Ingrid. "Configuración: Tecnología DSL." (2007 [citado el 25 de Junio de 2011]) disponible en http://www.uninorte.edu.co/divisiones/ingenierias/Dpto_Sistemas/lab_redes/upload/file/Configuracion_de_Tecnologia_%20ADSL.pdf
- Castañeda, Luis. "Simuladores de Redes Cisco." (2010 [citado el 23 de Junio de 2011]) disponible en http://www.slideshare.net/aaron12/simuladores-de-redes-cisco
- Della, Jorge. "Modelo de Referencia OSI." (2005 [citado el 28 de Abril del 2011]) editado por Mario Navarro: disponible en http://www.frm.utn.edu.ar/comunicaciones/modelo_osi.html
  http://www.dte.us.es/personal/mcromero/masredes/docs/SMARD.0910.qos.pdf
  http://www.redescisco.net/archivos/clases_online/Clase1_ACL.pdf
  http://www.redescisco.net/v2/art/la-encapsulacion-de-datos-unconcepto-critico/
- Medina, Luis. "Diseño de Redes, Modelo Jerárquico." (2011 [citado el 06 de Junio de 2011]) disponible en http://www.redesymas.org/2011/05/diseno-de-redes-modelojerarquico.html
- Millán, Ramón. "La tecnología de acceso ADSL." (1999 [citado el 24 de Junio de 2011]) disponible en http://www.ramonmillan.com/tutoriales/adsl.php
- Redes CISCO. "La encapsulación de datos, un concepto crítico." (2010 [citado el 29 de Abril de 2011]) editado por Paulo Colomés
- Romero, María. "Calidad de servicios QoS en redes." (2010 [citado el 21 de Junio de 2011])

- Spichiger, Juan Carlos. “Listas de control de acceso·” (2010 [citado el 27 de Mayo del 2011])
- TICOM. “Como usar ftp paso a paso.” (2010 citado el 16 de Julio de 2011) disponible en http://www.ticomperu.com/manualdeftppasoapaso.html
- Cisco, “Implementación de Soluciones QoS para Videoconferencia H.323 sobre IP” (Citado el 17 de octubre del 2016) disponible en http://www.cisco.com/cisco/web/support/LA/102/1026/1026685_video-qos.html
- Cisco, “Calidad de servicio para Voz sobre IP” (Citado el 14 de abril del 2008) disponible en http://www.cisco.com/cisco/web/support/LA/8/81/81646_tech_tk652_tk698_tech_white_paper09186a00800d6b73.html

9 ANEXOS:

INTERNATIONAL TELECOMMUNICATION UNION

ITU-T G.1010

(11/2001)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Quality of service and performance

End-user multimedia QoS categories

ITU-T Recommendation G.1010

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TESTING EQUIPMENTS	G.500–G.599
TRANSMISSION MEDIA CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
QUALITY OF SERVICE AND PERFORMANCE	**G.1000–G.1999**
TRANSMISSION MEDIA CHARACTERISCTICS	G.6000–G.6999
DIGITAL TERMINAL EQUIPMENTS	G.7000–G.7999

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation G.1010

End-user multimedia QoS categories

Summary

This Recommendation defines a model for multimedia Quality of Service (QoS) categories from an end-user viewpoint. By considering user expectations for a range of multimedia applications, eight distinct categories are identified, based on tolerance to information loss and delay. It is intended that these categories form the basis for defining realistic QoS classes for underlying transport networks, and associated QoS control mechanisms.

Source

ITU-T Recommendation G.1010 was prepared by ITU-T Study Group 12 (2001-2004) and approved under the WTSA Resolution 1 procedure on 29 November 2001.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation G.1010

End-user multimedia QoS categories

1 Scope

The intent of this Recommendation is to provide guidance on the key factors that influence Quality of Service (QoS) from the perspective of the end-user. By considering a range of applications involving the media of voice, video, image and text, and the parameters that govern end-user satisfaction for these applications, a broad classification of end-user QoS categories is determined. It is intended that these categories be used as the basis for deriving realistic QoS classes and associated QoS control mechanisms for the underlying transport networks.

2 References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

NOTE – The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[1] ITU-T Recommendation F.700 (2000), *Framework Recommendation for multimedia services*.

[2] ITU-T Recommendation G.131 (1996), *Control of talker echo*.

[3] ITU-T Recommendation G.114 (2000), *One-way transmission time*.

[4] ETSI TS 101329-2 (2002), *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 3; End-to-end Quality of Service in TIPHON Systems; Part 2: Definition of speech Quality of Service (QoS) classes*.

3 User-driven performance requirements

A major challenge for emerging wireline and wireless IP-based networks is to provide adequate Quality of Service (QoS) for different services. To do this requires a detailed knowledge of the performance requirements for particular services and applications. The starting point for deriving these performance requirements must be the user.

A typical user is not concerned with how a particular service is implemented. However, the user is interested in comparing the same service offered by different providers in terms of universal, user-oriented performance parameters. This implies that performance should be expressed by parameters that:

- Take into account all aspects of the service from the user's point of view;
- Focus on user-perceivable effects, rather than their causes within the network;
- Are independent of the specific network architecture or technology;
- Can be objectively or subjectively measured at the service access point;
- Can be easily related to network performance parameters;

- Can be assured to a user by the service providers(s).

4 Key parameters impacting the user

4.1 Delay

Delay manifests itself in a number of ways, including the time taken to establish a particular service from the initial user request and the time to receive specific information once the service is established. Delay has a very direct impact on user satisfaction depending on the application, and includes delays in the terminal, network, and any servers. Note that from a user point of view, delay also takes into account the effect of other network parameters such as throughput.

4.2 Delay variation

Delay variation is generally included as a performance parameter since it is very important at the transport layer in packetised data systems due to the inherent variability in arrival times of individual packets. However, services that are highly intolerant of delay variation will usually take steps to remove (or at least significantly reduce) the delay variation by means of buffering, effectively eliminating delay variation as perceived at the user level (although at the expense of adding additional fixed delay).

4.3 Information loss

Information loss has a very direct effect on the quality of the information finally presented to the user, whether it be voice, image, video or data. In this context, information loss is not limited to the effects of bit errors or packet loss during transmission, but also includes the effects of any degradation introduced by media coding for more efficient transmission (e.g. the use of low bit-rate speech codecs for voice).

5 Performance considerations for different applications

5.1 Audio

A general classification of audio into five levels of quality, and a mapping to various services, is given in [1]. More specific details are given below.

5.1.1 Conversational voice

Requirements for conversational voice are heavily influenced by one-way delay. In fact, there are two distinct effects of delay. The first is the creation of echo in conjunction with two-wire to 4-wire conversions or even acoustic coupling in a terminal. This begins to cause increasing degradation to voice quality for delays of the order of tens of milliseconds, and echo control measures must be taken at this point (provision of echo cancellers etc [2]). The second effect occurs when the delay increases to a point where it begins to impact conversational dynamics, i.e. the delay in the other party responding becomes noticeable. This occurs for delays of the order of several hundred milliseconds [3].

However, the human ear is highly intolerant of short-term delay variation (jitter). As a practical matter, for all voice services, delay variation due to variability in incoming packet arrival times must be removed with a de-jitterizing buffer.

Requirements for information loss are influenced by the fact that the human ear is tolerant to a certain amount of distortion of a speech signal. In IP-based transmission systems a prime source of voice quality degradation is due to the use of low bit-rate speech compression codecs and their performance under conditions of packet loss.

5.1.2 Voice messaging

Requirements for information loss are essentially the same as for conversational voice (i.e. dependent on the speech coder), but a key difference here is that there is more tolerance for delay since there is no direct conversation involved. The main issue, therefore becomes one of how much delay can be tolerated between the user issuing a command to replay a voice message and the actual start of the audio. There is no precise data on this, but based on studies related to the acceptability of stimulus-response delay for telecommunications services, a delay of the order of a few seconds seems reasonable for this application. In fact, a distinction is possible between recording and playback, in that user reaction to playback is likely to be the more stringent requirement.

5.1.3 Streaming audio

Streaming audio is expected to provide better quality than conventional telephony, and requirements for information loss in terms of packet loss will be correspondingly tighter. However, as with voice messaging, there is no conversational element involved and delay requirements for the audio stream itself can be relaxed, even more so than for voice-messaging, although control commands must be dealt with appropriately (see 5.3.4).

5.2 Video

A general classification of video into six levels of quality, and a mapping to various services, is given in [1]. More specific details are given below.

5.2.1 Videophone

Videophone as used here implies a full-duplex system, carrying both video and audio and intended for use in a conversational environment. As such, in principle the same delay requirements as for conversational voice will apply, i.e. no echo and minimal effect on conversational dynamics, with the added requirement that the audio and video must be synchronised within certain limits to provide "lip-synch".

Once again, the human eye is tolerant to some loss of information, so that some degree of packet loss is acceptable depending on the specific video coder and amount of error protection used. It is expected that the latest MPEG-4 video codecs will provide acceptable video quality with frame erasure rates up to about 1%.

5.2.2 One-way video

The main distinguishing feature of one-way video is that there is no conversational element involved, meaning that the delay requirement will not be so stringent, and can follow that of streaming audio.

Taking into account the above considerations, performance targets for audio and video applications are shown in Table I.1.

5.3 Data

From a user point of view, a prime requirement for any data transfer application is to guarantee essentially zero loss of information. At the same time, delay variation is not generally noticeable to the user, although there needs to be a limit on synchronisation between media streams in a multimedia session (e.g. audio in conjunction with a white-board presentation). The different applications therefore tend to distinguish themselves on the basis of the delay which can be tolerated by the end-user from the time the source content is requested until it is presented to the user.

5.3.1 Web-browsing

In this category we refer to retrieving and viewing the HTML component of a Web page, other components e.g. images, audio/video clips are dealt with under their separate categories. From the user point of view, the main performance factor is how quickly a page appears after it has been requested. Delays of several seconds are acceptable, but not more than about 10 seconds.

5.3.2 Bulk data

This category includes file transfers, and is clearly influenced by the size of the file. As long as there is an indication that the file transfer is proceeding, it is reasonable to assume somewhat longer tolerance to delay than for a single Web-page.

5.3.3 High-priority transaction services (E-commerce)

The main performance requirement here is to provide a sense of immediacy to the user that the transaction is proceeding smoothly, and a delay of no more than a few seconds is desirable.

5.3.4 Command/control

Clearly, command/control implies very tight limits on allowable delay, much less than a second. Note that a key differentiator from conversational voice and video services with similar low delay requirements is the zero tolerance for information loss.

5.3.5 Still image

This category includes a variety of encoding formats, some of which may be tolerant to information loss since they will be viewed by a human eye. However, given that even single bit errors can cause large disturbances in other still image formats, it is argued that this category should in general have zero information loss. However, delay requirements for still image transfer are not stringent and may be comparable to that for bulk data transfer, given that the image tends to be built up as it is being received, which provides an indication that data transfer is proceeding.

5.3.6 Interactive games

Requirements for interactive games are obviously very dependent on the specific game, but it is clear that demanding applications will require very short delays of the order of a fraction of a second, consistent with demanding interactive applications.

5.3.7 Telnet

Telnet is included here with a requirement for a short delay of a fraction of a second in order to provide essentially instantaneous character echo-back.

5.3.8 E-mail (server access)

E-mail is generally thought to be a store and forward service which, in principle, can tolerate delays of several minutes or even hours. However, it is important to differentiate between communications between the user and the local email server and server, to server transfer. When the user communicates with the local mail server, there is an expectation that the mail will be transferred within a few seconds.

5.3.9 Instant messaging

Instant messaging primarily relates to text, but can also include audio, video and image. In any case, despite the name, it is not a real-time communication in the sense of conversational voice, and delays of several seconds are acceptable.

5.4 Background applications

In principle, the only requirement for applications in this category is that information should be delivered to the user essentially error free. However, there is still a delay constraint, since data is effectively useless if it is received too late for any practical purpose.

5.4.1 Fax

Fax is included in this category since it is not normally intended to be an accompaniment to highly interactive real-time communication. Nevertheless, for so-called "real-time" fax there is an expectation in most business scenarios that a fax will be received within about 30 seconds. Delay for store and forward fax can be much higher. Note that fax does not require zero information loss.

5.4.2 Low priority transaction services

An example in this category is Short Message Service (SMS). 10s of seconds are an acceptable delivery delay value.

5.4.3 Email (server-to-server)

This category is included for completeness, since as mentioned earlier, the prime interest in email is in the access time.

5.4.4 Usenet

Usenet is a world-wide distributed discussion system. It consists of a set of "newsgroups" with names that are classified hierarchically by subject. "Articles" or "messages" are "posted" to these newsgroups by people on computers with the appropriate software. These articles are then broadcast to other interconnected computer systems via a wide variety of networks. This is a very low priority service, with corresponding relaxed delay requirements. However, it is desirable that messages are received by the user in the order that they are posted, to avoid seeing a reply prior to the original message.

Taking into account the above considerations, performance targets for data applications are summarised in Table I.2.

6 Classification of performance requirements into end-user Quality of Service categories

Based on the target performance requirements identified in Appendix I, the various applications can be mapped onto axes of packet loss and one-way delay as shown in Figure 1. The size and shape of the boxes provide a general indication of the limit of delay and information loss tolerable for each application class.

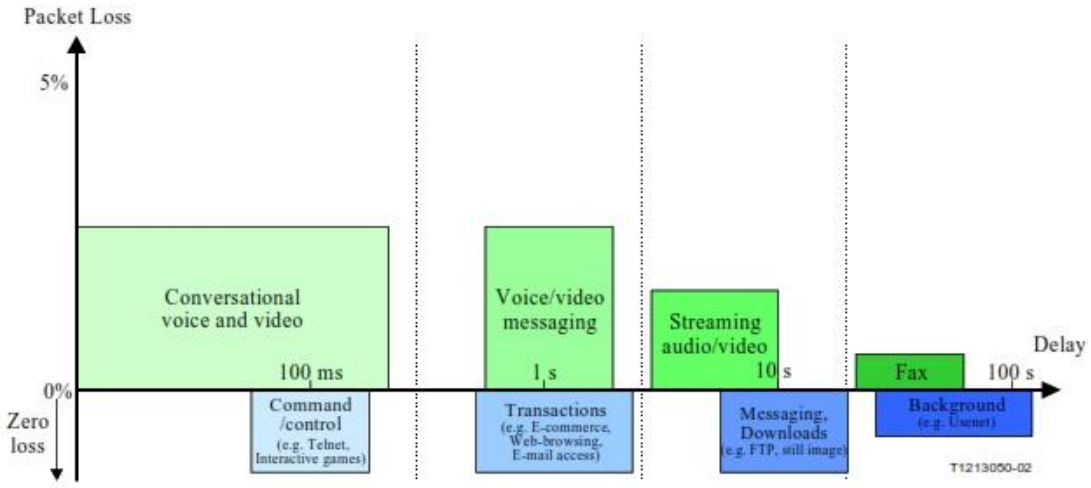


Figure 1/G.1010 – Mapping of user-centric QoS requirements

It can be seen that there are eight distinct groupings which encompass the range of applications identified. Within these eight groupings there is a primary segregation between applications that can tolerate some information loss and those that can not tolerate any information loss at all, and four general areas of delay tolerance.

This mapping can be formalised in Figure 2, to provide a recommended model for end-user QoS categories, where the four areas of delay are given names chosen to illustrate the type of user interaction involved. Of course, it is possible that each category could be subdivided into further categories to provide a range of quality levels for a specific service, as has been done for conversational voice in ETSI TS 101329-2 [4].

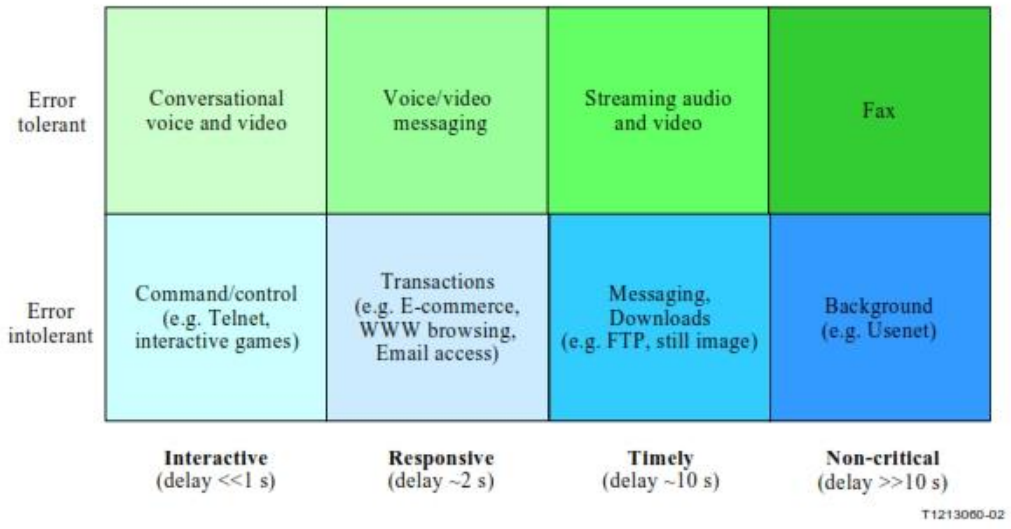


Figure 2/G.1010 – Model for user-centric QoS categories

Several useful features of this model are:

1) The model is based on end-to-end user perception of impairments and is therefore not dependent on any specific technology for its validity. This feature means that the model can be applied regardless of the underlying transport technology (IP, ATM, wireline, wireless etc).

2) The model provides an indication of the upper and lower boundaries for applications to be perceived as essentially acceptable to the user. Exceed an upper boundary (in loss or delay) and the service will be considered unsatisfactory; exceed a lower boundary, and the service will still be considered acceptable but may be wasteful from a network resource point of view because the service is using unnecessary resources.

3) The model provides a simple means of determining whether a bearer channel qualifies to carry a given application's data. For example, a channel with one-way delay of 1 second cannot support effective, natural real-time communication such as voice and Telnet. Furthermore, even if the one-way delay were reduced to 100 ms, Telnet would still be compromised if there were any information loss: loss of a single character would be conspicuous.

4) The model shows how the underlying impairments of information loss and delay can be grouped appropriately, without implying that one class is "better" than another (as in categorisations that use Gold, Silver, etc.). This can be used as the basis for deriving realistic and meaningful network QoS classes for differentiating service performance.

5) Note that the particular applications cited are exemplars rather than exhaustive. Other applications can be located in the schema by their similarity to these exemplars.

APPENDIX I

Performance targets

Based on information in the Bibliography (Appendix II), Table I.1 provides an indication of suitable performance targets for audio and video applications.

Table I.1/G.1010 – Performance targets for audio and video applications

Medium	Application	Degree of symmetry	Typical data rates	Key performance parameters and target values			
				One-way delay	Delay variation	Information loss (Note 2)	Other
Audio	Conversational voice	Two-way	4-64 kbit/s	<150 ms preferred (Note 1) <400 ms limit (Note 1)	< 1 ms	< 3% packet loss ratio (PLR)	
Audio	Voice messaging	Primarily one-way	4-32 kbit/s	< 1 s for playback < 2 s for record	< 1 ms	< 3% PLR	
Audio	High quality streaming audio	Primarily one-way	16-128 kbit/s (Note 3)	< 10 s	<< 1 ms	< 1% PLR	
Video	Videophone	Two-way	16-384 kbit/s	< 150 ms preferred (Note 4) <400 ms limit		< 1% PLR	Lip-synch: < 80 ms
Video	One-way	One-way	16-384 kbit/s	< 10 s		< 1% PLR	

NOTE 1 – Assumes adequate echo control.

NOTE 2 – Exact values depend on specific codec, but assumes use of a packet loss concealment algorithm to minimise effect of packet loss.

NOTE 3 – Quality is very dependent on codec type and bit-rate.

NOTE 4 – These values are to be considered as long-term target values which may not be met by current technology.

Based on information in the Bibliography (Appendix II), Table I.2 provides an indication of suitable performance targets for data applications.

Table I.2/G.1010 – Performance targets for data applications

Medium	Application	Degree of symmetry	Typical amount of data	Key performance parameters and target values		
				One-way delay (Note)	**Delay variation**	**Information loss**
Data	Web-browsing – HTML	Primarily one-way	~10 KB	Preferred < 2 s /page Acceptable < 4 s /page	N.A.	Zero
Data	Bulk data transfer/retrieval	Primarily one-way	10 KB-10 MB	Preferred < 15 s Acceptable < 60 s	N.A.	Zero
Data	Transaction services – high priority e.g. e-commerce, ATM	Two-way	< 10 KB	Preferred < 2 s Acceptable < 4 s	N.A.	Zero
Data	Command/control	Two-way	~ 1 KB	< 250 ms	N.A.	Zero
Data	Still image	One-way	< 100 KB	Preferred < 15 s Acceptable < 60 s	N.A.	Zero
Data	Interactive games	Two-way	< 1 KB	< 200 ms	N.A.	Zero
Data	Telnet	Two-way (asymmetric)	< 1 KB	< 200 ms	N.A.	Zero
Data	E-mail (server access)	Primarily one-way	< 10 KB	Preferred < 2 s Acceptable < 4 s	N.A.	Zero
Data	E-mail (server to server transfer)	Primarily one-way	< 10 KB	Can be several minutes	N.A.	Zero
Data	Fax ("real-time")	Primarily one-way	~ 10 KB	< 30 s/page	N.A.	$<10^{-6}$ BER
Data	Fax (store & forward)	Primarily one-way	~ 10 KB	Can be several minutes	N.A.	$<10^{-6}$ BER
Data	Low priority transactions	Primarily one-way	< 10 KB	< 30 s	N.A.	Zero
Data	Usenet	Primarily one-way	Can be 1 MB or more	Can be several minutes	N.A.	Zero

NOTE – In some cases, it may be more appropriate to consider these values as response times.

APPENDIX II

Bibliography

- KWOK (T.): Residential broadband Internet services and application requirements, *IEEE Communications Magazine*, June 1997.
- STEINMETZ (R.): Human Perception of Jitter and Media Synchronisation, *IEEE J-SAC*, Vol. 14, Issue 1, January 1996.
- SHNEIDERMAN (B.): Response Time and Display Rate in Human Performance with Computers, *ACM-Computing Surveys*, Vol. 16, No. 3, September 1984.
- MACDONALD (D.M.), ARCHAMBAULT (S.): Using customer perception in setting objectives for Intelligent Network services, *ITC-14*, 1994 .
- GALLAWAY (Glen R.): Response time to user activities in Interactive Man/Machine computer systems, *Proceedings of the Human Factors Society*, 25th Annual meeting, 1981.
- ETSI ETR 160, 1995, *Human factors aspects of multimedia telecommunications*.
- SHUR and MORTON, Performance of character-echo oriented applications on X.25 packet networks, *Globecom'92*.
- DANESHMAND (M.F.), ROY (R.R.) and SAVOLAINE (C.G.): Framework and requirements of Quality of Service for multimedia applications, *IIS'97*.
- GOLICK (Jerry): Catching the Multimedia Wave, *Data Communications Tech Tutorials*, 21st March 1999.
- WANG (S.Y.), MEYER (S.E.) and MY LAI: Quality of Service for Residential Broadband Video Service, *Globecom'96*.
- ANSI T1.522-2000, *Quality of Service for Business Multimedia Conferencing*.
- ZANETTIN (Alberto): Applications Prioritization: Giving the Green Light to Business Apps., *Data Communications Tech Tutorials*, March 1999.
- ISO-IEC/JTC 1/SC 29/WG 11 Report N2604, *Report of the formal verification tests on MPEG-4 video error resilience*, December 1998.

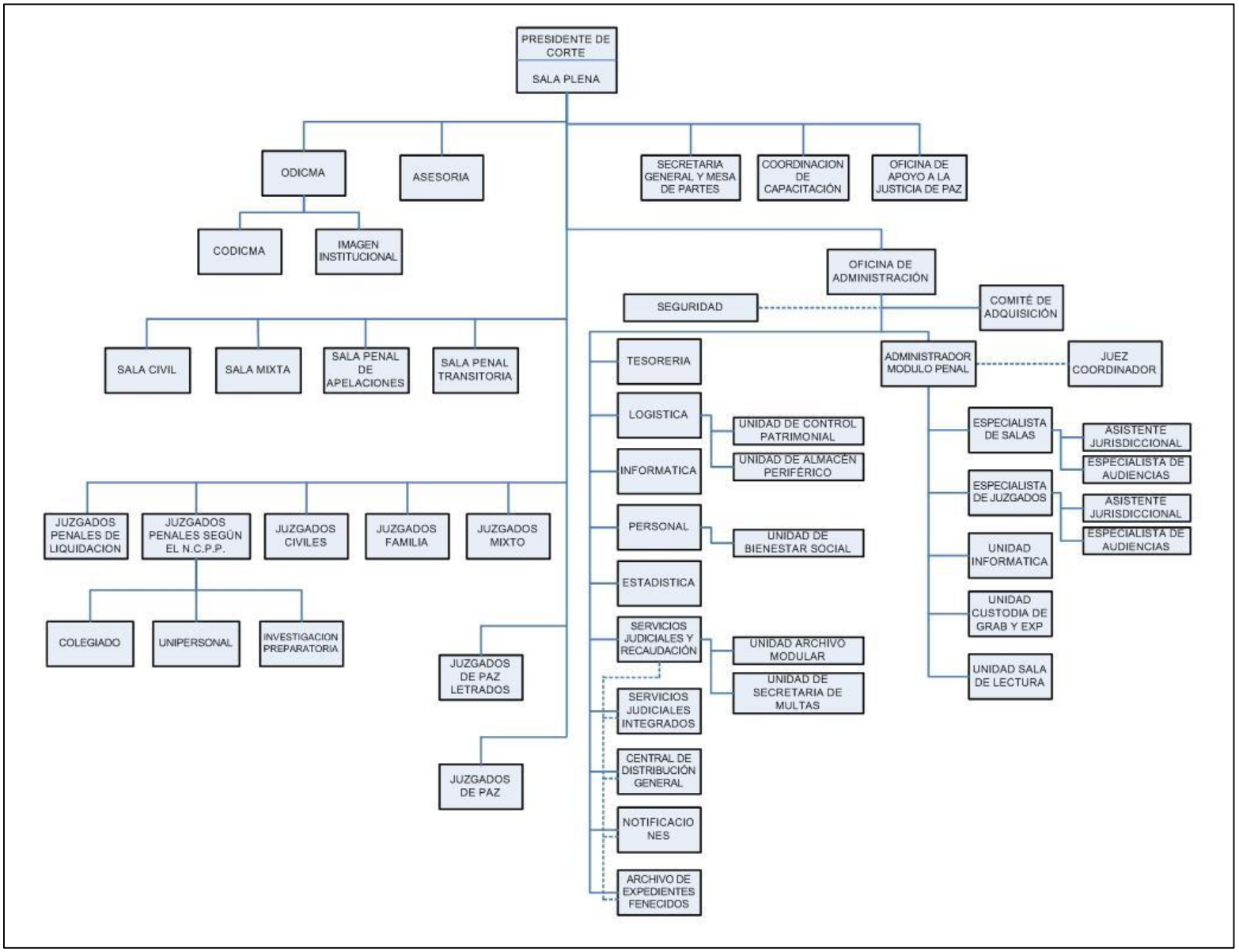
SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series B	Means of expression: definitions, symbols, classification
Series C	General telecommunication statistics
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	TMN and network maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks and open system communications
Series Y	Global information infrastructure and Internet protocol aspects
Series Z	Languages and general software aspects for telecommunication systems

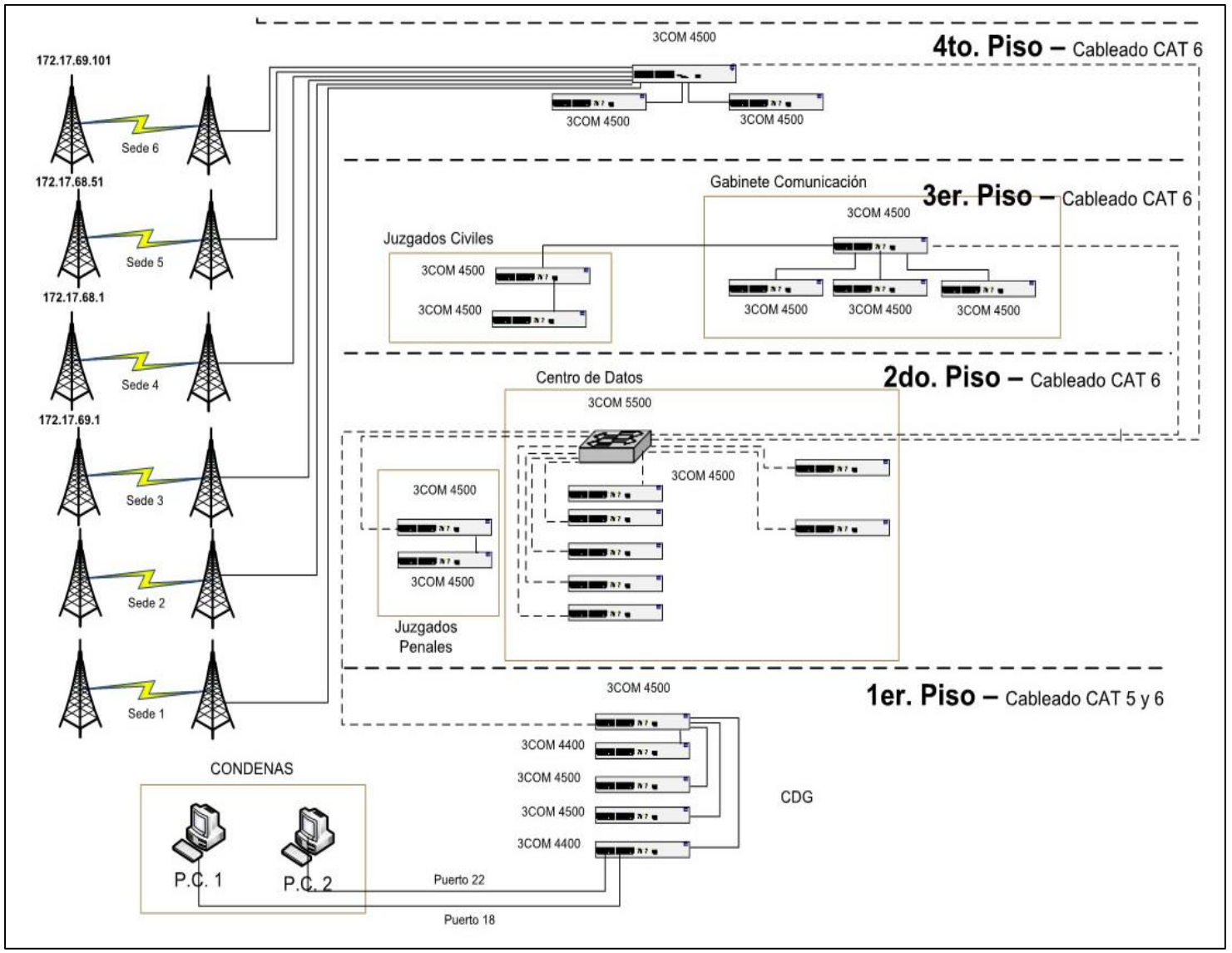
21883

Printed in Switzerland
Geneva, 2002

ORGANIGRAMA DE LA CORTE SUPERIOR DE JUSTICA DE LA LIBERTAD

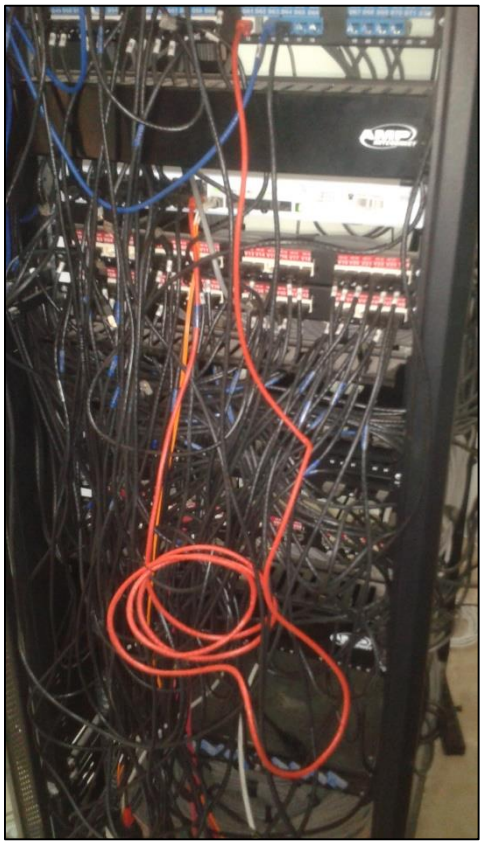


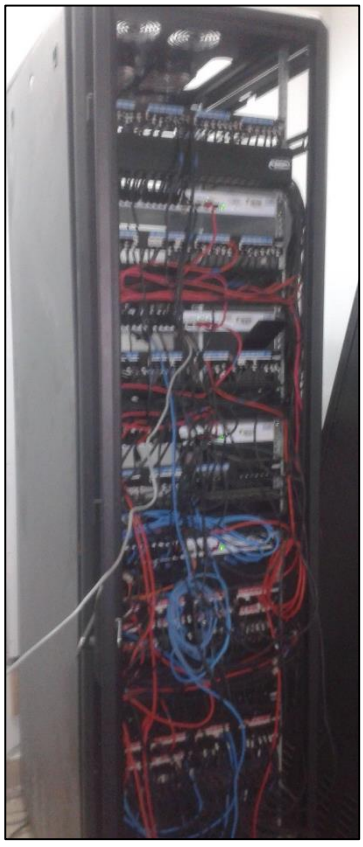
TOPOLOGÍA ACTUAL DE LA RED DE LA CORTE

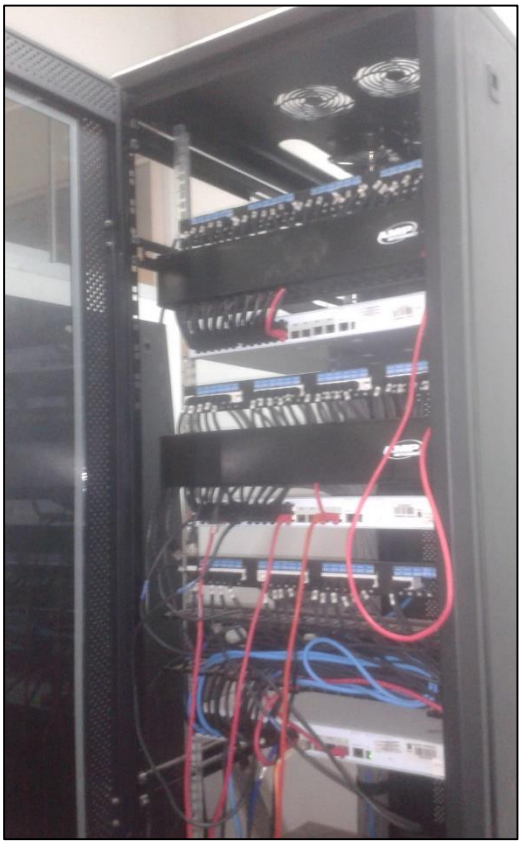


SALAS DE GABINETES UBICADOS EN LA RED

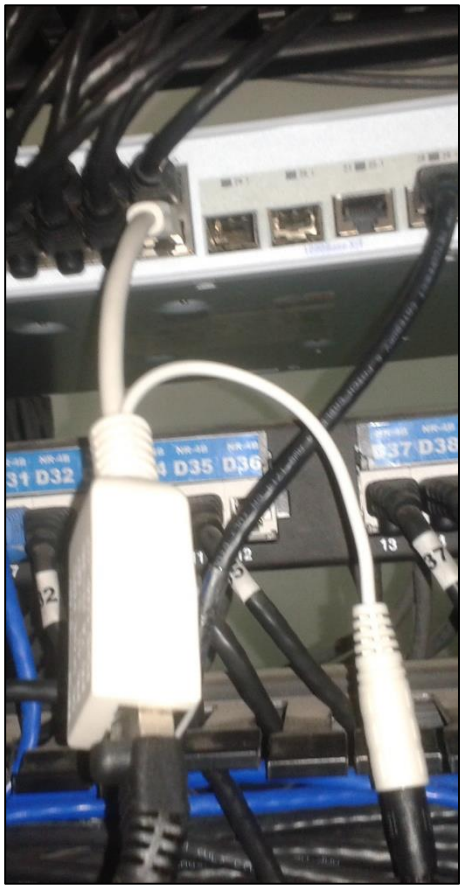
GABIENTES Y DISPOSITIVOS DE RED

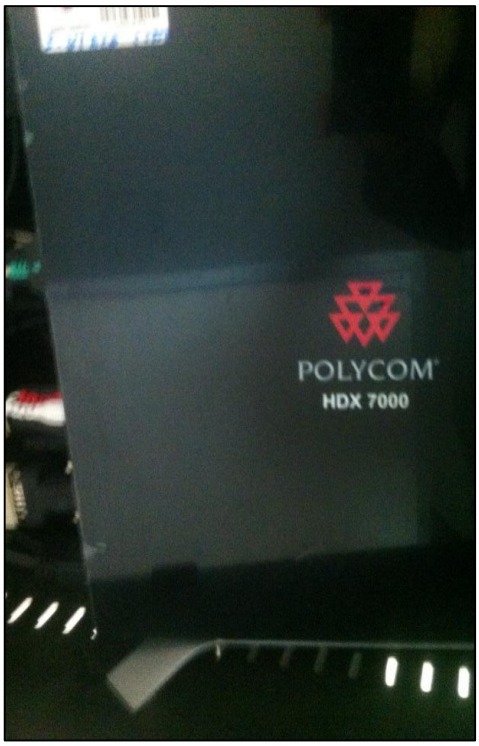






EQUIPO POLYCOM - VIDEOCONFERENCIAS





AUDIENCIAS REALIZADAS