INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA

MAESTRÍA EN CIENCIAS EN INGENIERÍA DE TELECOMUNICACIONES

"MODELO DE LA INFRAESTRUCTURA PARA QoS APLICADO EN AMBIENTES EDUCATIVOS"

TESIS QUE PARA OBTENER EL GRADO DE **MAESTRO EN CIENCIAS EN INGENIERÍA DE TELECOMUNICACIONES**

PRESENTA **L.S.C. NÉSTOR GUILLERMO MARTÍNEZ ALVARADO.**

Asesores:
Dr. Salvador Álvarez Ballesteros.
M. en C. Chadwick Carreto Arellano.

México, D.F. Diciembre 2009.

INSTITUTO POLITÉCNICO NACIONAL

SIP-14

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESIS

En la Ciudad de México, D. F. siendo las 11:00 horas del día 26 del mes de Noviembre del 2009 se reunieron los miembros de la Comisión Revisora de Tesis designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de E. S. I. M. E. para examinar la tesis de titulada:

"MODELO DE LA INFRAESTRUCTURA PARA QoS APLICADO EN AMBIENTES EDUCATIVOS"

Presentada por el alumno:

MARTÍNEZ	ALVARADO	NESTOR GUILLERMO
Apellido paterno	Apellido materno	Nombre(s)

Con registro:

A	0	8	0	2	7	5

aspirante de:

MAESTRO EN CIENCIAS EN INGENIERÍA DE TELECOMUNICACIONES

Después de intercambiar opiniones los miembros de la Comisión manifestaron ***SU APROBACIÓN DE LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISION REVISORA

Director de tesis

DR. SALVADOR ALVAREZ BALLESTEROS

Presidente

DR. HÉCTOR OVIEDO GALDEANO

Segundo Vocal

M. EN C. CHADWICK CARRETO ARELLANO

Tercer Vocal

DR. ROLANDO MENCHACA GARCÍA

Secretario

M. EN C. MIGUEL SÁNCHEZ MERAZ

EL PRESIDENTE DEL COLEGIO

DR. JAIME ROBLES GARCIA

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
ESTADOS UNIDOS MEXICANOS
I. P. N.
SECCION DE ESTUDIOS DE POSGRADO E INVESTIGACION

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA CESIÓN DE DERECHOS

En la ciudad de **México, D.F.** el día **08** del mes de **diciembre** del año **2009**, el que suscribe **Néstor Guillermo Martínez Alvarado** alumno del Programa de **Maestría en ingeniería de telecomunicaciones** con número de registro **A080275**, adscrito a **la sección de de estudios de posgrado e investigación de a la Escuela Superior de Ingeniería Mecánica y Eléctrica unidad Zacatenco**, manifiesta que es autor intelectual del presente trabajo de Tesis bajo la dirección del **Dr. Salvador Álvarez Ballesteros y M. en C. Chadwick Carreto Arellano** y cede los derechos del trabajo intitulado **Modelo de la infraestructura para QoS aplicado en ambientes educativos**, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección **powernma@gmail.com**. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

NAA

NESTOR GUILLERMO MARTINEZ ALVARADO

Nombre y firma

Resumen.

En el presente trabajo se propone, describe e implementa un modelo que asegura calidad de los servicios desplegados sobre una red convergente, el caso de estudio se realiza en un ambiente educativo, ya que cuenta con usuarios y equipos heterogéneos que permiten tener una gama amplia en cuanto a estudios y resultados se refiere.

A lo largo del trabajo se detallan las fases de implementación del modelo, además se especifican las características del estudio y las herramientas que se han empleado para hacer una correcta implementación dando pauta a una arquitectura funcional, estable, flexible y robusta

El caso práctico fue puesto en marcha en la red del Centro de Formación e Innovación Educativa (CFIE). Una red que a su vez es un segmento de la red institucional del Instituto Politécnico Nacional (IPN). La red del centro es una red convergente que contempla servicios de video, voz y datos. Además de múltiples usuarios a los que se les deben prestar servicios.

Se hace la puntualización de los objetivos que pretenden alcanzarse al tener la arquitectura en estado operativo. Además se describen las ventajas y desventajas con las que cuenta el modelo.

Abstract.

In this thesis the proposal is made the description and implementation of a model that ensures quality service deployed on a converged network, the case study is done in an educational environment.

Throughout the research thesis detailing the implementation phases of the model also shows the characteristics of the study and the tools have been used to make a successful deployment pattern giving a functional architecture, stable, flexible and robust

The case study was implemented in the network of Centro de Formacion e Innovación educative (CFIE - the Center for Training and Educational Innovation). A network that in turn is a segment of the institutional network of the Instituto Politécnico Nacional (IPN - National Polytechnic Institute).

It is the clarification of the objectives to be achieved by having the operating state architecture. Also discusses the advantages and disadvantages with which the model accounts.

Agradecimientos.

Gracias a Dios.

Gracias a Dios por el proyecto de vida que ha tenido para mí. Por protegerme siempre como a la niña de sus ojos, cubrirme con su sangre poderosa y resguardarme en el hueco de su mano. Gracias por hacerme saber que caerán a mi lado mil y diez mil a mi diestra mas a mi no llegaran. Ningún arma forjada contra mí prosperará y se condenara toda lengua que se levante contra mí en juicio**.** Gracias por todas las promesas de vida que tiene para mi, quiero un día seguir sus planes divinos.

La ciencia ni la tecnología están peleadas con la fe, con Dios. Sin embargo, están peleadas con la religión, los religiosos y fanáticos. De igual manera deberían estar peleadas con la política, politiqueros y estorbos.

Gracias a mis padres.

Por ser siempre inagotable fuente de amor y apoyo. Gracias a mi padre, Ing. Justino Martínez Juárez. Quien por ser mi héroe personal y querer seguir sus pasos he venido a parar al Glorioso Instituto Politécnico Nacional. A mi madre Ing. Herminia Alvarado Martínez, que siempre ha tenido lo mejor que dar para mí, limpiado mis heridas y me ha impulsado a seguir siempre adelante, haciendo más fácil el mundo con un abrazo. Espero no decepcionarlos nunca y disfrutar juntos logros como este que también son suyos.

Gracias a mis hermanos.

Gracias por estar siempre ahí aunque no digamos nada, por jugar siempre. Por apoyarme, gracias a Juanita por ser un buen ejemplo a seguir, centrada y cariñosa hermana, sabia para dar consejo. Te quiero mucho hermanita. Gracias también a Brian por ser lo que es y no lo que yo quiera, por competir algunas veces conmigo y ganar siempre, dueño de la eterna juventud y todos los méritos. Te quiero mucho también.

A mi familia.

A mi abuelita Virginia, por ser una abuelita muy consentidora, querendona y apapachable. Por estar siempre al pendiente y alegrarse hasta las lagrimas con los logros que le podemos compartir.

A mi abuelo, por que ha jugado un papel importante en mi formación humana, siempre me ha respetado mucho, siempre me ha querido mucho y yo lo quiero mucho a él.

A todos mis tíos y tías con los que he tenido trato siempre, esa gran familia que hay en casa que siempre está ahí para cuando se necesita. Son grandes personas y yo los quiero mucho. A mis primos por crecer juntos todos jugando siempre, por superarnos todos y por lo buenos que somos! –jaja-.

A Evelyn.

Gracias amor por estar conmigo estos últimos 3 años 9 meses 12 días y contando, gracias por apoyarme tanto por no dejarme ir cuando quise tirar todo y salir huyendo, gracias por esa sonrisa maravillosa que me da ánimos de continuar. Gracias por querer envejecer a mi lado. Gracias por todo. ¿Sabes algo? ¡TE AMO!

A mis amigos.

A mis pequeños saltamontes porque siempre estuvieron pendientes de la superación de su sensei, gracias a todos los amigos que me hacían el día diciendo que paso mai ya pa'cuando? Gracias a todos los que de alguna manera me ayudaron a no sentirme solo en la ciudad de la furia. Gracias a todos los que recibieron mis escritos científicos y me dijeron que estaba muy bien, aun sin siquiera leerlo. Gracias a todos por su contribución para terminar esto. Y pues como dicen por ahí arrieros somos y en el camino andamos! Chida la banda!

A mis Asesores.

Gracias por todo el tiempo que invirtieron en ayudarme a terminar este trabajo, el tiempo es algo muy valioso y por eso espero que este trabajo sea de provecho.

Gracias al Dr. Salvador Álvarez Ballesteros por creer en mí y darme la oportunidad de demostrar que puedo. Le estaré por siempre agradecido pues fue parte crucial para lograr la meta que tenia de estudiar en esta institución. Gracias por su apoyo y sabios consejos no solo del trabajo sino de vida. Creo que aparte del grado gane un amigo.

Gracias al M. en C. Chadwick Carreto Arellano. Porque involuntariamente y sin enseñanza le he aprendido la calidad humana y buen humor, además del trabajo de calidad. Gracias por brindarme su apoyo, también sus consejos y la seguridad de que las cosas siempre salen bien cuando se trabaja duro. Literalmente, este trabajo no hubiera podido ver la luz sin usted, sin su colaboración. De igual manera creo que además del grado gane un amigo al conocerlo.

Todos son importantes y el orden de los en que se encuentran no afecta que les agradezca más o menos, o que los estime más o menos. Pero he querido dejar para el final al pasado y al futuro.

Gracias a ti que te has ido.

Sin tantas explicaciones, gracias por la huella que dejaste, te has ido para bien o para mal hoy ya no estás. A tu paso, al encontrarnos en esta vida algo tuve que aprender, es por eso que agradezco.

Gracias a ti que aun no has llegado.

Solo tengo en mente a alguien cierto para agradecer en este apartado, **Gracias a ti pollito bebe** que aun no has llegado, espero que cuando leas esto se siembre en ti la semillita de ser mejor cada vez, de superarte, de superarme. De caminar por la vida intentando siempre lo mejor. Toma lo bueno de las personas, deja pasar lo malo. Siempre tendrás mucho amor de mi parte. Siempre estaré para ti. Aun ahora que solo te imagino siento que te amo. Aun antes de escribir esto, aun antes de comenzar este proyecto ya te esperaba con ansia.

Y si es más de un pollito bebe. Los querré inmensamente no importa el orden en que lleguen para mi serán el numero uno. Los consejos, agradecimientos y esta dedicatoria es especialmente para ustedes.

ÍNDICE GENERAL.

CAPITULO II. ESTADO DEL ARTE Y PROPUESTA DE NUEVO MODELO.

CAPITULO III. ARQUITECTURA DE CALIDAD.

CAPITULO IV. PRUEBAS Y RESULTADOS

CONCUSIONES Y TRABAJO FUTURO.

ANEXOS.

GLOSARIO.

A

ACL. *Access Control List. Lista de Control de Acceso.* Es una lista específica donde se les concede los usuarios acceso a los recursos, así como las operaciones que están autorizados a llevar a cabo en sistemas específicos.

ACTIVEX. Arquitectura de sistemas desarrollado por Microsoft como una alternativa al lenguaje Java, orientado al desarrollo de programas para la Internet.

Consiste en tres elementos principales:
-Controles ActiveX. Función parecida a los controles convencionales OLE.
-Documentos ActiveX. Permite ver los documentos activos semejantes a las páginas HTML
-Guiones ActiveX. Los guiones (scripting), permiten coordinar los controles ActiveX en el sitio Web usando su lenguaje de guiones preferido.

ANONYMAIZER. *Proxy anónimo.* Es una herramienta que intenta hacer la actividad en el Internet imposible de rastrear. Se accede a Internet con un nombre del usuario, protegiendo la información personal por ocultar información de identificación del equipo de origen.

APPLETS. Es un componente de una aplicación que se ejecuta en el contexto (dentro) de otro programa, por ejemplo un navegador web.

ARP. *Address Resolution Protocol. Protocolo de resolución de direcciones.* Es un protocolo de nivel de red responsable de encontrar la dirección hardware (MAC Address) que corresponde a una determinada dirección IP.

ARQ. *Automatic Repeat-reQuest. Solicitud de repetición automática* es un protocolo utilizado para el control de errores en la transmisión de datos, garantizando la integridad de los mismos.

***AT&T**. American Telephone and Telegraph. Teléfonos y telégrafos Americanos.* Compañía Estadounidense de telecomunicaciones. Una división de esta compañía, la Bells Lab, creó el primer sistema operativo Unix.

ATM. *Asynchronous Transfer Mode. Modo de Transferencia Asíncrona.* Es una tecnología de telecomunicaciones desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones desarrollada en la década de los 60.

B

BADCHECKSUM. Son los parámetro erróneos que son devueltos después de la verificación de los datos a través de las tramas TCP/IP.

BB. *Bandwidth Broker.* Es un agente que gestiona el uso de la red. Mediante los informes de uso del ancho de banda que le envían periódicamente los ruteadores y conociendo los recurso de la red y los usuarios registrados, su algoritmo de control adaptativo permite reestructurar todos los flujos de usuarios mediante el control de las colas en los ruteador.

C

CFIE. *Centro de Formación e Innovación Educativa.* Fue creado en abril de 2004 y se destaca por su fortaleza cualitativa en cuanto a oportunidad, suficiencia y equidad hacia el desarrollo del personal del Instituto Politécnico Nacional, lo cual se traduce en la formación, innovación e investigación educativa, pilares para mejorar el desempeño del capital humano del Instituto, así como de los procesos administrativos y de gestión.

CHECKSUM. Es el parámetro que permite la verificación de los datos a través de las tramas TCP/IP.

COOKIES. Es un fragmento de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página. Esta información puede ser luego recuperada por el servidor en posteriores visitas

CRC. *Código de Redundancia Cíclica.* Es un código de comprobación que se suele añadir a los datos transmitidos en muchas comunicaciones, y que permiten detectar si se ha producido algún error en la transmisión.

CSF6N. *Class of Service Full IPv6 Network. Clase de servicio completa de red IPv6.* El trafico esta conmutado como en una red Diffserv. Cada ruteador CSF6N necesita compartir definiciones comunes de las clases de tráfico con los otros ruteadores de la misma red. Es necesario establecer una definición común en la etiqueta de flujo de 20 bits disponibles para ello y teóricamente 220 clases de tráfico. Las tablas de asignación de ruteadores serán similares a las tablas de aplicación diffserv.

CSMA/CD. *Carrier Sense Multiple Access with Collision Detection. Acceso múltiple por detección de portadora con detección de colisiones.* Sistema de acceso a una red local, por el cual los nodos se aseguran de que la red no está en uso antes de enviar un paquete. La detección de colisiones significa que la red puede determinar cuándo se producen colisiones y proporciona medidas correctoras.

D

DDOS. *Denial of Service. Ataque de denegación de servicio.* Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

DNS. *Domain Name System. Sistema de nombres de dominio*. Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado al internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

E

ENMH. *Escuela Nacional de Medicina y homeopatía del Instituto Politécnico Nacional.*

ESFM. *Escuela Superior de Física y Matemáticas del Instituto Politécnico Nacional.*

ESIA*. Escuela Superior de Ingeniería y Arquitectura del Instituto Politécnico Nacional.*

ESIME. *Escuela Superior de Ingeniería Mecánica Y Eléctrica del Instituto Politécnico Nacional.*

ETSI. *European Telecommunications Standards Institute. Instituto Europeo de Normas de Telecomunicaciones.* Es una organización de estandarización de la industria de las telecomunicaciones (fabricantes de equipos y operadores de redes) de Europa, con proyección mundial. El ETSI ha tenido gran éxito al estandarizar el sistema de telefonía móvil GSM. Cuerpos de estandarización significativos dependientes del ETSI son 3GPP (para redes UMTS) o TISPAN (para redes fijas y convergencia con Internet).

F

F6SN. *Full IPv.6 Switched Network. Redes completamente conmutadas IP.v6.*

FDDI. *Fiber Distributed Data Interface. Interfaz de datos distribuida por fibra.* Es un conjunto de estándares ISO y ANSI para la transmisión de datos en redes de computadoras de área extendida o local (LAN) mediante cable de fibra óptica. Se basa en la arquitectura token ring y permite una comunicación tipo Full Duplex.

Dado que puede abastecer a miles de usuarios, una LAN FDDI suele ser empleada como backbone para una red de área amplia (WAN).

FEC. *Forward Error Correction. Corrección de errores hacia adelante.* Es un tipo de mecanismo de corrección de errores que permite su corrección en el receptor sin retransmisión de la información original. Se utiliza en sistemas sin retorno o sistemas en tiempo real donde no se puede esperar a la retransmisión para mostrar los datos.

FTP. *File Transfer Protocol. Protocolo de Transferencia de Archivos.* Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP, basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

H

HOAXES. *Noticia falsa* es un intento de hacer creer a un grupo de personas que algo falso es real.[1] En el idioma español el término se popularizó principalmente al referirse a engaños masivos por medios electrónicos especialmente Internet.

HTTP. *HyperText Transfer Protocol. Protocolo de Transferencia de Hipertexto.* Define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.

I

ICMP. *Internet Control Message Protocol. Protocolo de Mensajes de Control de Internet.* Es el sub protocolo de control y notificación de errores del Protocolo IP. Como tal, se usa para enviar mensajes de error, indicando que un servicio determinado no está disponible o que un router o host no puede ser localizado.

IEEE. *Institute of Electrical and Electronics Engineers. Instituto de Ingenieros Electricistas y Electrónicos.* Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros electricistas, ingenieros en electrónica, científicos de la computación, ingenieros en informática, ingenieros en biomédica , ingenieros en telecomunicación e Ingenieros en Mecatrónica. Dedicada principalmente a la difusión de los avances de las tecnologías recientes y estandarización de las mismas.

IP. *Internet Protocol. Protocolo de Internet.* Es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados. Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas.

IPN. *Instituto Politécnico Nacional.*

ISO. *International Organization for Standardization.Organización Internacional para la Estandarización.* Es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

ITU. *International Telecommunication Union. Unión Internacional de Telecomunicaciones.* Es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas administraciones y empresas operadoras.

N

NAS. *Network Attached Storage. Almacenamiento Compartido en red.* Son dispositivos de almacenamiento específicos a los que se accede desde los equipos a través de protocolos de red.

NETBIOS. *Network Basic Input/Output System. Sistema básico de red Entrada/Salida.* Es una capa de software desarrollado para enlazar un sistema operativo de red con hardware específico.

NETFLOW*.* Es un protocolo de red desarrollado por Cisco Systems para correr sistemas con soporte en Cisco IOS para recolectar información de tráfico IP. Es un protocolo propietario y compatible con otras plataformas de IOS, tales como Juniper, Linux o FreeBSD y OpenBSD.

P

P2P. *Peer to Peer. Red de pares.* Es una red de computadoras en la que todos o algunos aspectos de esta funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Los nodos actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red.

PCN-DIFFSERV. *Pre Congestion Notification. Notificación de antes de una congestión basado en una solución Diffserv.*

PING. Un comando usado para comprobar las conexiones a uno o más hosts remotos. La utilidad ping emplea paquetes ICMP de petición de eco y respuesta de eco para determinar si un sistema IP concreto de una red es funcional. La utilidad ping es útil para diagnosticar fallos IP de la red o del enrutador (Packet INternet Groper).

PRN. *Private Relay Node. Nodo Privado de retardo.*

Q

QoS. *Quiality of Service. Calidad en el servicio.*

R

RARP. *Reverse Address Resolution Protocol. Protocolo de resolución de direcciones inverso.* Es un protocolo utilizado para resolver la dirección IP de una dirección hardware dado.

RFC. *Request For Comments. Petición De Comentarios.* Son una serie de notas sobre Internet que comenzaron a publicarse en 1969. Se abrevian como RFC. Cada una de ellas individualmente es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet, que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.

RIP. *Routing Information Protocol. Protocolo de encaminamiento de información.* Es un protocolo de puerta de enlace interna utilizado por los ruteadores, aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.

RMON. *Remote Network Monitoring. Monitoreo Remoto de Red.* Fue desarrollado por la IETF para apoyar el monitoreo y análisis de protocolo de redes de área local.

RSVP. *Resource Reservation Protocol. Protocolo de Reserva de Recursos.*

RTT. *Round-Trip delay Time. Tiempo de viaje Redondo.* Es tiempo que tarda un paquete enviado desde un emisor en volver a este mismo emisor habiendo pasado por el receptor de destino.

S

SFLOW. Describe un mecanismo para capturar datos del tráfico en redes cambiadas o encaminadas. Utiliza una tecnología del muestreo para recoger estadística del dispositivo y está por esta razón aplicable a las redes de alta velocidad.

SIP. *Session Initation Protocol. Protocolo de Inicio de Sesiones.* Es un protocolo desarrollado por el IETF con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos en línea y realidad virtual.

SLA. *Service Level Agreement. Acuerdo de Nivel de Servicio*. Es un contrato escrito entre un proveedor de servicio y su cliente con objeto de fijar el nivel acordado para la calidad de dicho servicio. El SLA es una herramienta que ayuda a ambas partes a llegar a un consenso en términos del nivel de calidad del servicio, en aspectos tales como tiempo de respuesta, disponibilidad horaria, documentación disponible, personal asignado al servicio, etc. Básicamente el SLA define la relación entre ambas partes: proveedor y cliente. Un SLA identifica y define las necesidades del cliente a la vez que controla sus expectativas de servicio en relación a la capacidad del proveedor, proporciona un marco de entendimiento, simplifica asuntos complicados, reduce las áreas de conflicto y favorece el diálogo ante la disputa.

SNMP. *Simple Network Managemen Protocol. Protocolo Simple de Administración de Red.* Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

SPAM. Se denomina *correo basura* a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.

SSH. *Secure Shell. Interprete de órdenes segura.* Es un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si hay un Servidor X (en sistemas Unix y Windows) corriendo.

T

T1. Es un estándar de entramado y señalización para transmisión digital de voz y datos basado en PCM ampliamente usado en telecomunicaciones en Norteamérica, Corea del Sur y Japón. La tasa de transmisión original (1,544 Mbps).

TCP. *Transmission Control Protocol. Protocolo de Control de Transmisiones.* Es un protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto.

THROUGHPUT. Se define como el volumen de trabajo o de información que fluye a través de un sistema. Así también se le llama al volumen de información que fluye en las redes de datos. Particularmente significativo en almacenamiento de información y sistemas de recuperación de información, en los cuales el

rendimiento es medido en unidades como accesos por hora.

TMN. *Telecommunications Management Network. Red de gestión de telecomunicaciones.* Es una red que presenta un modelo real , orientado a objetos, actualizado y ampliamente aplicable , definido por un número de estándares y basado sobre el modelo de comunicaciones de siete capas OSI.

TOKEN-BUCKET. Es un algoritmo de control de congestión basado en el captado de tráfico. Es de tipo bucle abierto, lo que significa que previene la congestión (no reacciona cuando ya se ha producido, sino que previene que no se produzca), y lo hace captando el tráfico que entra a la red para que ésta lo pueda diferenciar.

U

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

UPALM. *Unidad Profesional Adolfo López Mateos del Instituto Politécnico nacional.*

UPIICSA*. Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias Sociales y Administrativas del Instituto Politécnico Nacional.*

UPIITA. *Unidad Profesional Interdisciplinaria de Ingeniería y Tecnología Avanzadas del instituto Politécnico Nacional.*

V

VoIP. *Voz sobre Protocolo de Internet.* Es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP . Esto significa que se envía la señal de voz en forma digital en paquetes en lugar de enviarla (en forma digital o analógica) a través de circuitos utilizables sólo para telefonía como una compañía telefónica convencional.

ÍNDICE DE TABLAS Y FIGURAS.

NOMBRE. **PAGINA.**

CAPITULO I.

NOMBRE. **PAGINA.**

CAPITULO I.

CAPITULO II.

CAPITULO III.

CAPITULO IV.

COMCLUSIONES.

Introducción.

En el trabajo se realiza una investigación detallada acerca de lo que es la calidad de los servicio (QoS), desde su definición, la normatividad sobre la que está sustentada emitidas por organismos reguladores internacionales como la IEEE y la ITU además de otros organismos como el foro de investigaciones de internet. Se mencionan los factores sobre los cuales se mide la calidad en el servicio. Las acepciones que esta tiene entre diferentes espectadores como, usuarios, los prestadores y administradores de servicios.

Se hace un repaso sobre el estado del arte, en donde ha estado ubicada la calidad del servicio a través de las diferentes tecnologías implementadas al correr de los años y sobre diferentes sistemas de red.

Se describen diferentes soluciones modelos que han sido implementados tal como IntServ, DiffServ y MPLS, de igual manera una pequeña comparativa entre estas soluciones. Haciendo alusión también al modelo de mejor esfuerzo que más bien en realidad no ofrece garantía alguna en la entrega y calidad de los servicios.

El trabajo se centra en presentar una propuesta de modelo de calidad de los servicios, detallando las características para lograr su implementación en una red convergente.

Se definen los objetivos y tareas, así como el análisis y los resultados que se han obtenido a través de la implementación del estudio logrando deducir la realización de los objetivos.

Finalmente es interesante el análisis de los resultados, conclusiones y recomendaciones a las que llega el modelo, después del proceso de implantación dando lugar a una arquitectura en estado funcional.

Justificación.

Actualmente las redes de comunicaciones son muy bastas, se integran de elementos heterogéneos entre cada sistema de red. Lo mismo se integra de servicios diferentes que despliegan a usuarios con múltiples necesidades.

Es importante hacer una correcta planeación de red tomando en cuenta entre otras cosas las características que se han mencionado ya que de ello dependerá el correcto funcionamiento del sistema. Se puede elaborar un sistema tan complejo como las necesidades de comunicación lo demanden.

Lo que queda para las redes que ya están establecidas es hacer una reingeniería, reinventarse.

Al comienzo de las tecnologías de red no tenían la regulación estricta, los antecedentes históricos se ven desde la incompatibilidad entre soluciones de fabricantes diferentes, así pues menos se aseguraba la conectividad con lo que solo se asegura que se hace el mejor esfuerzo por integrar la comunicación.

Así pues han evolucionado desde las capacidades de conexión hasta las formas y motivos de comunicación. Y la exigencia de asegurarse que los servicios estarán disponibles cuando se les requiera. Que la información que viaje por cualquier medio de comunicación establecido llegara en tiempo y forma adecuados.

Hoy en día se ha expuesto la necesidad explícita de asegurar esa calidad. Organismos especializados se han dado a la tarea de normar un tema tan importante como asegurar calidad de los servicios.

La importancia es dada a que ante el crecimiento desmesurado y sin planeación la manera de contrarrestar es asegurando que al menos los servicios necesarios estarán disponibles. Bajo cualquier circunstancia o contingencia.

La solución que se ofrece es un modelo que tras su implantación en la red dará como resultado una arquitectura sencilla, gradual, basada en mejora continua que puede asegurar la calidad de los servicios sobre la red que se implanta, normalmente una red convergente, las redes de actualidad.

Objetivos.

En general cubriendo los objetivos de cada etapa de implementación de la propuesta de solución del modelo de calidad, se obtendrá una arquitectura (implementación funcional del modelo) capaz de recolectar información del sistema de red, procesarla y tomar decisiones acerca de mejoras que se pueden realizar para el desempeño optimo de la red.

Los objetivos de este trabajo de investigación y desarrollo tecnológico son:

- Emitir recomendaciones ante la implementación del modelo de calidad propuesto para que la arquitectura (implementación funcional del modelo) sea capaz de ofrecer mejora continua.

- Proponer métodos de mejora en el proceso de las comunicaciones.

CAPÍTULO I.

INTRODUCCIÓN A LA CALIDAD DE LOS SERVICIOS (QoS).

RESUMEN:

En este capítulo se presentan las generalidades en cuanto a calidad de servicio. Conceptos básicos e introductorios para la comprensión en el desarrollo del trabajo además de una primera muestra de soluciones QoS existentes.

OBJETIVOS DEL CAPITULO:

- Definir que es calidad en los servicios.
- Definir los parámetros de medición QoS.
- Presentar un panorama general de las soluciones QoS existentes.

1.1 Introducción.

La constante modernización de equipo tecnológico en la era digital y de la información, el abaratamiento de la tecnología, y por consiguiente la demanda de servicios, ha propiciado que se dispare el uso de las redes y las telecomunicaciones como medios cotidianos de comunicación entre las sociedades.

El creciente número de usuarios de algunos servicios que han apoyado sobre internet, las redes de comunicaciones o alguna rama de telecomunicaciones ha desembocado en la necesidad de proceso de enormes volúmenes de información. Es por eso que ha surgido la iniciativa de estandarizar los procesos inherentes a las comunicaciones y telecomunicaciones por parte de organismos reguladores internacionales. Así como también la especialización de los administradores de sistemas de red, prestadores de servicios y tecnologías de información.

Se exponen a continuación una serie de tablas y gráfica estadísticas [1], en ellas se puede observar cómo ha crecido sustancialmente el uso de internet a nivel mundial, también se han sub clasificado por regiones. Lo anterior da una idea de la importancia que ha cobrado internet no solo como servicio, también como base para desplegar muchos servicios mas como video conferencia, tele vigilancia, telecontrol, VoIP, etc. Resaltando el desarrollo tecnológico que debe haber detrás de estos servicios que hoy en día son comunes en la redes convergentes.

Uso de Internet a nivel mundial y estadísticas de población.						
Regiones del mundo	Población (Estadísticas 2009)	Usuarios de internet (30-12- 2000)	Últimos datos de Usuarios de Internet	Penetración (% de la población)	Crecimiento de usuarios (2000-2009)	Usuarios Totales (% del total de la tabla)
África	991,002,342	4,514,400	**65,903,900**	6.7 %	1,359.9 %	3.9 %
América del Norte	340,831,831	108,096,800	**251,735,500**	73.9 %	132.9 %	15.1 %
América latina y El Caribe	586,662,468	18,068,919	**175,834,439**	30.0 %	873.1 %	10.5 %
Asia	3,808,070,503	114,304,000	**704,213,930**	18.5 %	516.1 %	42.2 %
Europa	803,850,858	105,096,093	**402,380,474**	50.1 %	282.9 %	24.2 %
Medio Oriente	202,687,005	3,284,800	**47,964,146**	23.7 %	1,360.2 %	2.9 %
Oceanía/Australia	34,700,201	7,620,480	**20,838,019**	60.1 %	173.4 %	1.2 %
Total mundial	6,767,805,208	360,985,492	**1,668,870,408**	**24.7 %**	362.3 %	100.0 %

Tabla 1.1. Crecimiento y distribución de usuarios de internet.

La tabla 1.1. Muestra como ha crecido el uso de internet entre la población a nivel mundial, Internet es un servicio más de las redes de telecomunicaciones, a finales de esta década ha cobrado un valor agregado junto con muchos servicios más, gracias a que se ha vuelto de uso común entre los usuarios finales, usuarios domésticos, como un medio de comunicación e información de uso cotidiano a todos niveles.

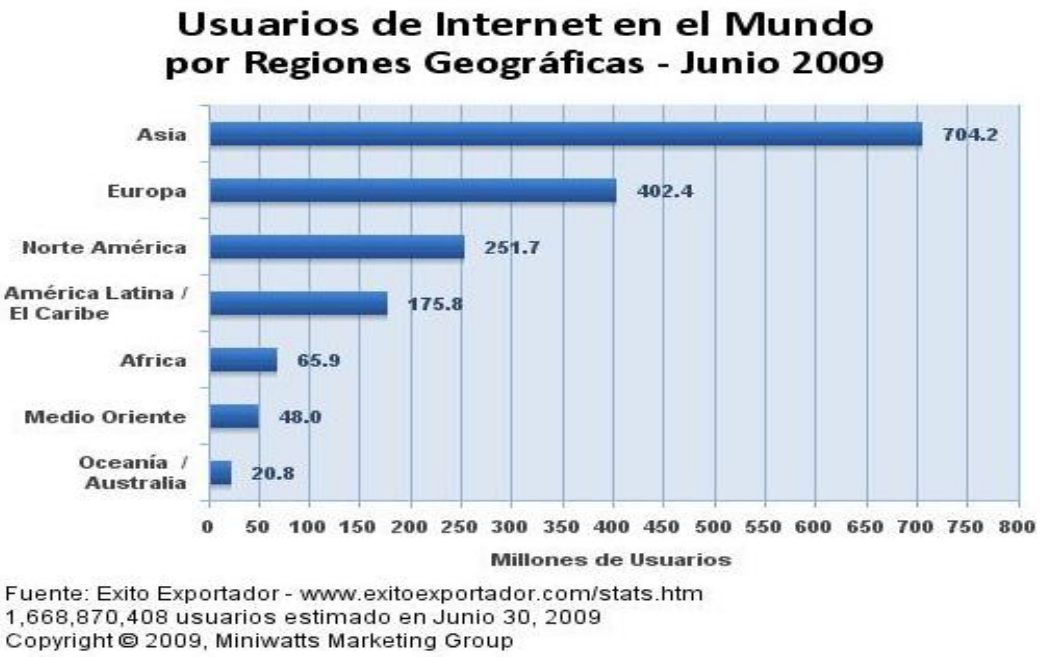


Figura 1.1. Crecimiento y distribución de usuarios de internet en el mundo.

La Figura 1.1. Muestra la distribución por millones de usuarios que tienen acceso a la red de internet, se muestra la división entre diferentes regiones del mundo, la región a la que se le puede dedicar especial interés es Latinoamérica pues México se encuentra contemplado en esta región.

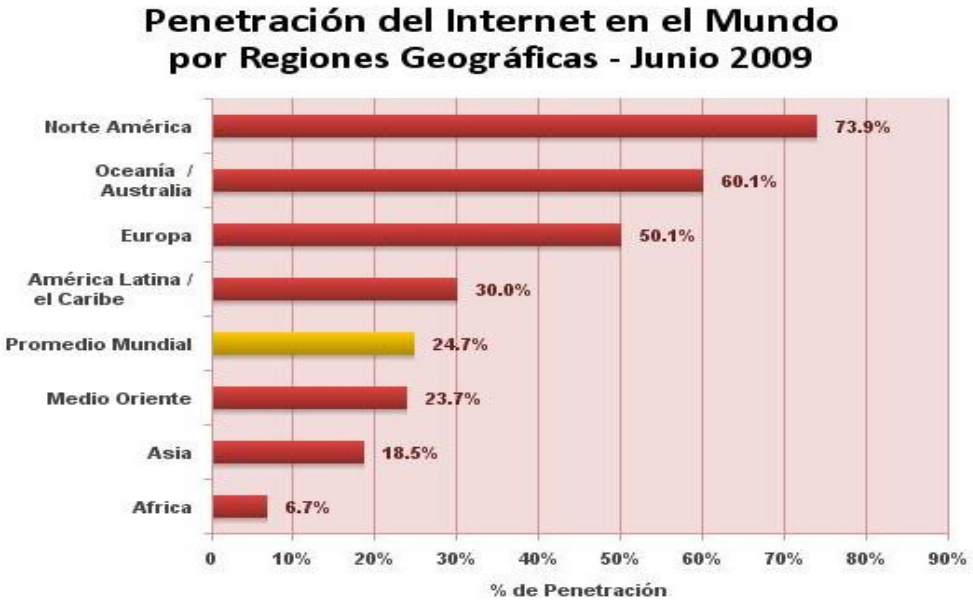


Figura 1.2. Penetración de internet en el mundo.

La Figura 1.2. Muestra el alcance que ha tenido internet, el porcentaje de la poblacion que ahora tiene un uso comun de ese servicio. Es interesante el dato de crecimiento promedio mundial y que la region latinoamerica, supera ese promedio.

En la segunda serie de figuras y gráficas se muestra la información de manera específica, exponiendo los detalles acerca de América latina en comparación con el resto del mundo que es lo que interesa ver. Y continuando después con la información que se ha recabado sobre México y el impacto que ha tenido en el continente.

Uso de Internet a nivel América Latina y estadísticas de población.						
Regiones	Población (Estadísticas 2009)	% Población del mundo	Últimos datos de Usuarios de Internet	Penetración (% de la población)	Crecimiento de usuarios (2000-2009)	Usuarios Totales (% del total de la tabla)
América Latina	569,212,811	8.4 %	**171,833,339**	30.2 %	865.7 %	10.3 %
Resto del Mundo	6,198,592,397	91.6 %	**1,497,037,069**	24.2 %	336.2 %	89.7 %
Total	6,767,805,208	100.0 %	**1,668,870,408**	24.7 %	362.3 %	100.0 %

Tabla 1.2. Crecimiento y distribución de usuarios de internet en América Latina.

De lo general a lo específico en la Tabla 1.2. Se ven las estadísticas que para América latina se han generado, siendo internet un escenario de negocio y comunicación de uso común entre diferentes sectores de la población mundial. Hay ya diferentes servicios que se apoyan de Internet, y se basan en su

correcto funcionamiento para que estos servicios puedan tener un optimo desempeño.

Uso de Internet a nivel América Latina y estadísticas de población.					
Regiones	Población (Estadísticas 2009)	Últimos datos de Usuarios de Internet	Penetración (% de la población)	Crecimiento de usuarios (2000-2009)	Usuarios Totales (% del total de la tabla)
Argentina	40,913,584	**20,000,000**	48.9 %	700.0 %	11.6 %
Bolivia	9,775,246	**1,000,000**	10.2 %	733.3 %	0.6 %
Brasil	198,739,269	**67,510,400**	34.0 %	1,250.2 %	39.3 %
Chile	16,601,707	**8,368,719**	50.4 %	376.2 %	4.9 %
Colombia	43,677,372	**18,234,822**	41.7 %	1,976.9 %	10.6 %
Costa Rica	4,253,877	**1,500,000**	35.3 %	500.0 %	0.9 %
Cuba	11,451,652	**1,450,000**	12.7 %	2,316.7 %	0.8 %
República Dominicana	9,650,054	**3,000,000**	31.1 %	5,354.5 %	1.7 %
Ecuador	14,573,101	**1,634,828**	11.2 %	808.2 %	1.0 %
El Salvador	7,185,218	**763,000**	10.6 %	1,807.5 %	0.4 %
Guatemala	13,276,517	**1,320,000**	9.9 %	1,930.8 %	0.8 %
Honduras	7,833,696	**658,500**	8.4 %	1.546.3 %	0.4 %
México	**111,211,789**	**27,400,000**	**24.6 %**	**910.2 %**	**15.9 %**
Nicaragua	5,891,199	**155,000**	2.6 %	210.0 %	0.1 %
Panamá	3,360,474	**778,800**	23.2 %	1,630.7 %	0.5 %
Paraguay	6,995,655	**530,300**	7.6 %	2,551.5 %	0.3 %
Perú	29,546,963	**7,636,400**	25.8 %	205.5 %	0.6 %
Puerto Rico	3,966,213	**1,000,000**	25.2 %	400.0 %	0.6 %
Uruguay	3,494,382	**1,340,000**	38.3 %	262.2 %	0.8 %
Venezuela	26,814,843	**7,552,570**	28.2 %	695.0 %	4.4 %
Total	569,212,811	**171,833,339**	30.2 %	865.7 %	100.0

Tabla 1.3. Crecimiento y distribución de usuarios de internet en América Latina (desglosado por países).

En la tabla 1.3. Se muestra el desglose, bajo los mismos factores de las tablas anteriores, dentro de esta se observa el desempeño que tiene México y se observan matices interesantes tal como el crecimiento de usuarios.

México, tiene el segundo lugar en mayor número de usuarios que se han contabilizado para generar las estadísticas cuenta con un 15.9 %. Esta justo debajo de Brasil que cuenta con 39.3%.

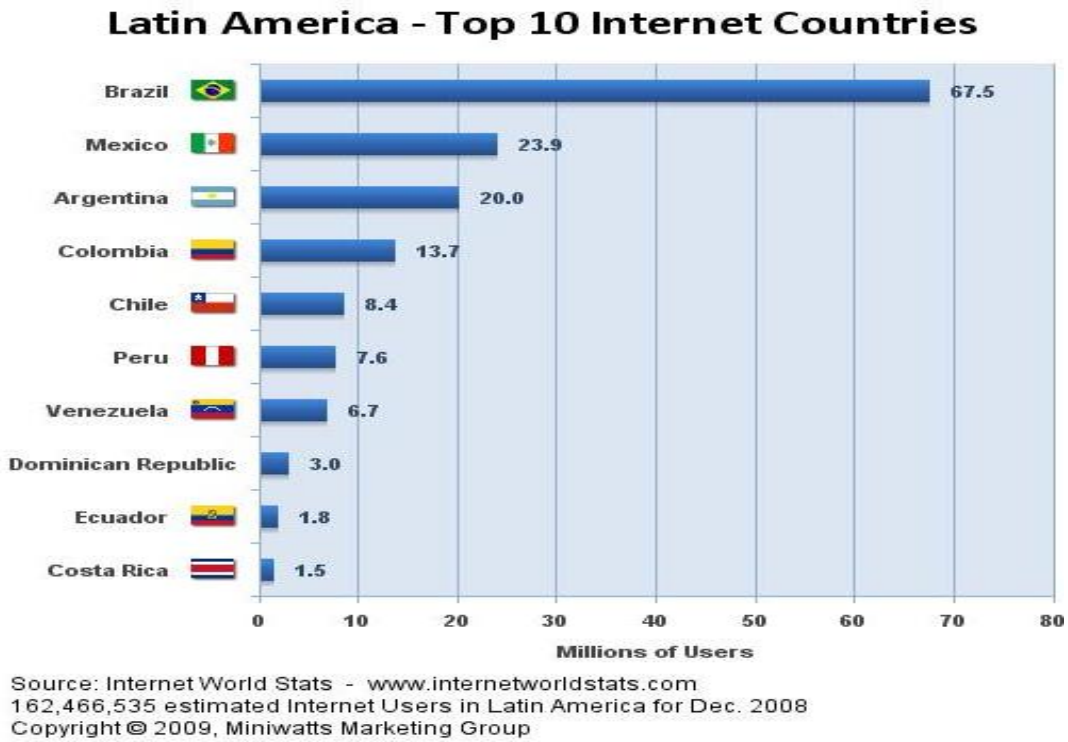


Figura 1.3. Distribución de usuarios de internet en América latina.

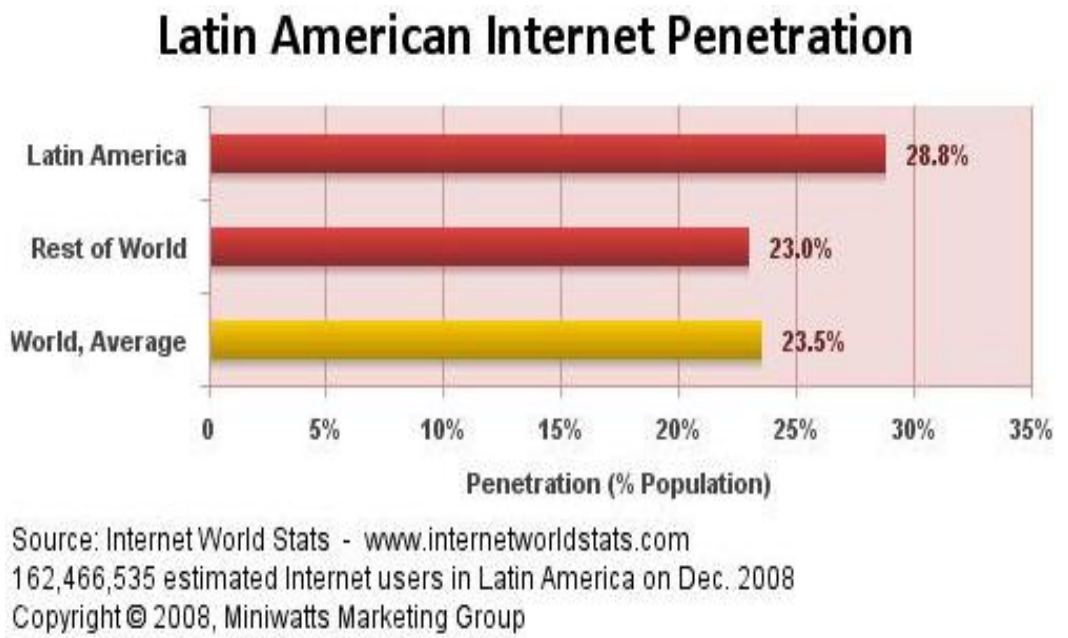


Figura 1.4. Penetración de internet en población de América Latina.

La Figura 1.3. Se hace notar el alcance que ha tenido internet entre los 10 países que tienen más usuarios. México se encuentra en segundo lugar debajo de Brasil, pero arriba de países que también han tenido despliegue tecnológico como argentina y Colombia.

En la figura 1.4 Se muestran los puntos porcentuales del alcance de internet a los usuarios, comparando la penetración que este servicio ha tenido en America latina y el resto del mundo es muy interesante notar que, Latinoamérica tiene un crecimiento de 5.8% por arriba del resto del mundo, y 5.3% del promedio mundial.

NOTAS:

(1) Las Estadísticas de Usuarios Mundiales Internet fueron actualizadas a Junio 30, 2009.
(2) Los datos de población se basan en cifras para 2009 del US Census Bureau.
(3) Los datos de usuarios provienen de información publicada por Nielsen Online, **ITU** y de Internet World Stats.
(4) Estas estadísticas son propiedad intelectual de Miniwatts Marketing Group, se pueden citar, siempre manifestando el debido crédito y estableciendo un enlace activo a www.exitoexportador.com.

1.2. Calidad de los servicio (QoS Quality of Service).

Como se ha mencionado hasta este momento el desarrollo de la tecnología tanto hardware como software ha propiciado la evolución de muchos servicios. Sin duda el más característico y de mayor uso es internet, la red de redes.

Dentro del modelo de usuarios y servicios intervienen muchas definiciones y actores, ahora se definirán algunos conceptos básicos.

Según el "**TelemaManagement Fórum [2]**" define los servicios de telecomunicaciones como:

"Un conjunto de funciones independientes que son parte integral de uno o más procesos de negocio. Éste conjunto funcional está formado por componentes hardware y software formando los medios de comunicación."

Se define calidad de los servicios bajo la perspectiva de diferentes organizaciones **[3]**.

De acuerdo con la **norma ISO 8402** Calidad se define como "La totalidad de características que conforman una entidad y que influyen en su capacidad para satisfacer necesidades expresadas o implícitas"

En la recomendación **E.800 [ITU-TE.800] ETSI [ETSI-ETR003]** define la calidad en el servicio como "el efecto colectivo del desempeño de los servicios que determinan el grado de satisfacción del usuario de dicho servicio"

Ejemplos de servicio pueden ser:

- ✓ En una Red Convergente.
  - ✓ VoIP (Voz sobre IP).
  - ✓ Internet.
  - ✓ Servicios de video: vigilancia, conferencia, almacenamiento etc.
- ✓ En telefonía.
  - ✓ Buzón de Voz.
  - ✓ Identificador de llamadas.
  - ✓ Desvío de llamadas.
- ✓ En Internet.
  - ✓ Navegación web.
  - ✓ Servicio de e-mail.
  - ✓ e-educación.
  - ✓ e-comercio.

1.2.1. Clasificación de QoS.

En primera instancia se puede hacer una reclasificación de la calidad de Servicio en 3 grupos principales.

- ✓ QoS Intrínseca:
  Hace alusión a las expectativas de las personas que diseñan y operan los equipos que brindan servicios de Telecomunicaciones. (Grupos reguladores, fabricantes de equipo, Etc.).

El objetivo es tener la capacidad de competir entre diferentes servicios de telecomunicaciones, con calidad a la par del mercado destino. Este tipo de QoS suele ser medido en comparación a los resultados emitidos por rigurosas métricas estandarizadas y propuestas por organismos especializados.

- ✓ QoS Percibida:
  Es relativa a las expectativas que tienen las personas que usan el servicio. (Usuario final, Domestico, Empresarial, etc.).

  Es el resultado, o la noción de calidad que se tiene después de haber utilizado el servicio realmente, después de que el usuario ha experimentado sus actividades de comunicación, o poder emitir un juicio al completar sus necesidades de comunicación o conectividad.

  Normalmente, el resultado o juicio de calidad que aporta el usuario dependerá de manera proporcional a que tan experto sea en el uso de los sistemas de telecomunicaciones, o incluso influido por las campañas de presentación de los proveedores de los servicios.

- ✓ QoS Evaluada:
  Incluye las expectativas de las personas que deben tratar con los operadores y proveedores de servicios (Administradores de QoS, Administradores de red, etc.).

  En este apartado se toma en cuenta el criterio de evaluación de calidad de un administrador especializado, si es que se está realizando algún tipo de pago o intercambio por el servicio se considera una verdadera necesidad su uso cotidiano o se puede prescindir del servicio o en su defecto hacer aportes a los fabricantes o proveedores para hacer mejoras en sus servicios.

Es importante, después de que se han definido con claridad los servicios requeridos, tener en cuenta con que calidad van a ser dotados y entregados. También tener la conciencia y capacidad para medir los servicios.

Por otra parte, se debe considerar que cada aplicación probablemente tendrá parámetros especiales de calidad de los servicios por satisfacer. Y que se pueden generalizar en esquemas donde se acoplen de una manera eficaz.

1.2.2. Clasificación de aplicaciones que requieren QoS[4].

Algunos esquemas de clasificación para aplicaciones que necesitan niveles de QoS pueden ser presentados como sigue:

1. Aplicaciones elásticas:
   Son las que pueden adaptar su funcionamiento y parámetros de calidad de los servicios sobre el esquema de "el mejor esfuerzo". En estas aplicaciones no se ve una interacción humana muy enlazada a la comunicación. Ejemplo de ellas son la transferencia de archivos, o envío de correo. Tecnológicamente estas aplicaciones no requieren que se les garantice, parámetros especiales como pudiera ser un ancho de banda específico, O limite de retardos. Ya que en el caso de que tengan un ancho de banda pequeño, solo tardaran más tiempo en ser enviados, el tiempo de transferencia será más largo o inclusive existen mecanismos de recuperación de datos y paquetes perdidos, corrección de errores que son características (pero insuficientes para otros servicios) propias de las redes.

2. Aplicaciones No elásticas:
   En contraste con las aplicaciones anteriores estas aplicaciones si requieren que se les garanticen algunos parámetros de calidad de los servicios. Aplicaciones en tiempo real por ejemplo, necesitan ancho de banda y un nivel mínimo de retardos para tener estabilidad en transmisión. Aunque algunas de estas aplicaciones muestran cierta habilidad de adaptarse a los cambios en parámetros de calidad de los servicios. (Sin dejar de asegurarse la misma). Se Mencionan como ejemplos de este apartado como las videoconferencias pueden realizar una transmisión de calidad con poco ancho de banda pero con una codificación eficiente (la solución optima puede obtenerse el software o hardware un recurso también valido, que puede hacer un trabajo de mejor eficiencia al usar otro estándar de digitalización). En ambos casos, con gran ancho de banda o con una codificación eficiente, los límites de retardo deberán ser pequeños para que la videoconferencia sea bien lograda.

3. Aplicaciones interactivas.
   Típicamente un humano interactúa en este esquema de comunicación, normalmente en un dispositivo de extremo que requiere una respuesta rápida para que otro usuario, dispositivo o nodo host logre un buen desempeño. Los parámetros que se requieren en general para garantizar una alta calidad de los servicios son límites estrictos para un

bajo tiempo de retardo, minimizar la tasa de error etc. Ejemplos de estas aplicaciones son: Voz sobre IP (VoIP), videoconferencia, aplicaciones colaborativas en línea, juegos en línea etc.

4. Aplicaciones no interactivas.
   Aquí no necesariamente se requiere de la colaboración directa humana para realizar la transmisión exitosa. Ni se requieren parámetros estrictos de calidad en el servicio. Por ejemplo se puede minimizar el poco ancho de banda con almacenamiento previo de los archivos o componentes. Si se requiere hacer una precarga (streaming) de audio o video puede hacerse con un ligero retardo (propio del almacenamiento) sin que eso signifique un problema significativo. Ejemplo de estas aplicaciones son: Navegación WEB, transferencia de archivos, chats o precarga de contenido de audio o video (streaming).

Ahora se ha definido el concepto básico “servicio” pero se requiere de asegurar que este (Servicio) llegará de manera eficaz y oportuna con “Calidad” para que se pueda trabajar y lograr conectividad, transferencia de información y buen término de lo que persiguen los servicios, ahora se da paso a algunas recomendaciones previas como:

1. Necesidad de entender los requerimientos inherentes a la calidad de los servicios. Si se tiene en mente por ejemplo un servicio VoIP, se ha mencionado que es un tema crítico en cuanto a la necesidad de un retardo mínimo, tolera solo una poca pérdida de paquetes, y necesita una reserva elevada de ancho de banda total, en comparación de otros servicios como la navegación web.

2. Estimar el volumen de cada necesidad de servicio. Hacer una calendarización y horarios a fin de minimizar las fallas en horas pico, incluso identificar cuáles son las horas pico y reducir sus consecuencias negativas. Armando un plan de contingencia.

3. Definir el nivel de aceptación por parte del usuario final para cada servicio. Para servicios en los que se requiere la participación directa de los sentidos por ejemplo (y uno de los mayores retos a vencer) asegurar calidad en VoIP o videoconferencias. Donde el usuario final puede darse cuenta de las fallas muy fácilmente y calificando de manera negativa el desempeño de la red. (pues al ser un modelo de comunicación transparente para él, no sabe lo que hay detrás o los esfuerzos tecnológicos que hay que hacer para obtener esta calidad) no considerando los parámetros estipulados en las normas, o desconociendo las fallas técnicas en la red e imponiendo parámetros propios como “se escucha mal, ruidoso, entrecortado, o simplemente no

escucho o no entiendo” por el lado de la videoconferencia, que el video no va a acorde con la voz. Etc. Detalles inherentes a una mala calidad de la red.

4. Definir las características y necesidades de flujo. Referido acerca de que tan grande puede ser el nivel de tráfico para cada servicio.

5. Concretar el Acuerdo de Nivel de Servicio (SLA - *Service Level Agreement*). Un SLA es un protocolo plasmado normalmente en un documento de carácter legal por el que una compañía que presta un servicio a otra se compromete a prestar el mismo bajo unas determinadas condiciones y con unas prestaciones mínimas.

6. Uso de mecanismos apropiados entre el operador de red y el proveedor de servicios para cumplir con el SLA.

7. Mediciones del usuario final. En este caso, lo que evalúa es la sensación de satisfacción ante lo estipulado en el SLA por parte de los usuarios de los servicios.

1.3. Como se mide QoS.

Existen en efecto, algunos parámetros específicos de medición, que básicamente arrojan información fiable de cómo se encuentra funcionando la red, de acuerdo a la calidad que puede ofertar para los servicios, que puede asegurarse y que estos puedan funcionar de manera correcta.

Aunque estos parámetros están al alcance de todos, usuarios, fabricantes y administradores. Puesto que las normas, recomendaciones y estándares son internacionales, no todas deberán aplicar a todos los servicios, de manera que solo tomando en cuenta algunos parámetros de acuerdo al orden del servicio, sus características y necesidades, afectaran de manera positiva al desempeño de ellos sobre la red.

1.3.1. Mediciones a puntos singulares (nodos en la red).

Remite información estadística de usuarios extremo a extremo, donde se puede medir el RTT (round trip time), que es el tiempo que tardan en inicializar los servicios después de que se piden al sistema.

Algunos parámetros para medir el desempeño de la red y la calidad en los servicios son:

- **Retardo.**

Este parámetro de medición en general se refiere al tiempo que tarda la aplicación destino en obtener los paquetes generados por la aplicación fuente, al viajar de extremo a extremo en la red.

Una subdivisión más especifica del retardo que atiende a la forma o proceso en que es generado.

- ✓ Retardo de procesamiento.
  Es el tiempo que necesitan los elementos de la red para procesar el paquete. Depende de la velocidad de procesamiento y complejidad de cada dispositivo en la red. Un ejemplo de ello es el tiempo que tardan en procesarse las colas de paquetes y ruteo, procesar las tablas de búsqueda, etc.

- ✓ Retardo en cola.
  Es el tiempo que espera el paquete en las colas que existen en los componentes de entrada/salida de la red. Las colas se hacen grandes (y el tiempo en cola por supuesto aumenta) cuando las redes se congestionan.

- ✓ Retardo de transmisión.
  Es el tiempo necesario para transmitir un paquete a una tasa de transmisión determinada. Puede significar un retardo grande si el volumen de información es demasiado grande para la capacidad de la red o en su defecto una velocidad baja de una red, Es calculado como:

$$Retardo\ de\ transmisión = \frac{número\ de\ bits\ a\ transmitir}{tasa\ de\ transmisión}$$

- ✓ Retardo de propagación.
  Es el tiempo que necesitan las señales para viajar a través del medio. Ejemplo de ello es cuando la red tiene entre sus medios la fibra óptica o el par trenzado de cobre, no tendrán la misma velocidad de propagación las señales y menos la misma velocidad de viaje en los datos. Ni sería la misma velocidad al viajar por el vacio. Puede calcularse como:

$$Retardo\ de\ propagación = \frac{Distancia\ física}{Velocidad\ de\ propagación}$$

- **Jitter.**

Son las perturbaciones de caída y realzo de la señal de transmisión (señal que oscila no constantemente) y dificulta la transmisión de información. Se calcula con la diferencia entre el retardo y paquetes secuenciales.

El jitter o variación de retardo puede ser causado por diferentes factores tales como:

- ✓ Diferentes paquetes pueden tener diferente plazo en las colas en el mismo dispositivo de red.

- ✓ Diferentes paquetes pueden tener diferentes tiempo de procesamiento en un mismo dispositivo de red agregándose así, diferentes tiempos de retardo. Hay por ejemplo una diferencia notable entre las tecnologías actuales que usan los dispositivos de red tal como el hardware de reenvío de paquetes y el software tecnológicamente más antiguos de reenvío de paquetes basados en web.

- ✓ Diferentes paquetes pueden viajar por diferentes rutas de red y los retardos se acumularían en diferentes tiempos de cola y retardos mismos de la propagación.

Desde la perspectiva del usuario, el jitter o la falta de él, repercute en la coherencia o consistencia de las aplicaciones. Mientras sea un nivel bajo y constante las aplicaciones pueden resultar adaptativas.

Según InterQoS [5] para obtener mediciones relacionadas con el estudio del jitter se propone que sea bajo el siguiente método:

- ✓ Intervalo máximo de medición de 5 minutos

- ✓ Separación en el intervalo de envío y recepción de paquetes 200 ms (la medida mínima se redondea a 1 ms).

- ✓ Normalmente se reporta al menos un lapso de variación en el retardo, en el 99% de los casos dentro de los periodos de medición.

Pérdida de paquetes:

Es la medida de los paquetes que no se han transmitido con éxito sobre la red en relación con todos los paquetes enviados sobre la misma. Usualmente detectados vía métodos ARQ (Automatic Repeat-reQuest), y medidos en bits sobre segundo (bps). Principalmente existen cuatro causas principales de perder paquetes en la red.

- ✓ Debido a la mala calidad del medio ya sea por interferencias físicas o electromagnéticas (esto se da muy frecuentemente en medios inalámbricos).
- ✓ Debido a la congestión de enlaces, causando desbordamiento de buffer en los dispositivos de red usados.
- ✓ Fallos en los dispositivos de la red.
- ✓ Cambios en el esquema de enrutamiento o protocolos de red, causando pérdida o daños en los paquetes

La pérdida de paquetes se puede calcular como:

$$Relación\ de\ perdida\ de\ paquetes = \frac{Paquetes\ enviados - Paquetes\ recibidos}{Paquetes\ enviados}$$

Desde la perspectiva del usuario, la pérdida de paquetes se ve reflejada en la calidad de presentación de las aplicaciones por ejemplo un buen sonido en un audio, o nitidez en la imagen de video.

Para medir la tasa de pérdida de paquetes, InterQoS recomienda que sea bajo el siguiente método:

- ✓ Intervalo máximo de medición de 5 minutos
- ✓ La métrica de medida para la tasa de pérdida de paquetes es mostrada como un porcentaje con precisión de 0.1%
- ✓ Normalmente se reporta un valor de tasa de pérdida de paquete en cada intervalo de medición

Throughput:

Es el caudal eficaz de tráfico enviado y recibido con éxito a través de la red en un tiempo determinado.

Estrictamente hablando, las métricas arriba mencionadas son suficientes para determinar el desempeño de las aplicaciones de usuario dentro de la red, así como también su apreciación de calidad de los servicios que tengan desde la perspectiva del usuario.

De tal manera que el ancho de banda no es un factor específico como tal, más bien a veces se ocupa el ancho de banda eficaz o un ancho de banda reservado especial para garantía de algunos servicios.

Desde las recomendaciones de la **ITU**-T (Unión Internacional de Telecomunicaciones) serie Y [1541]**[6]**, la siguiente tabla resume los objetivos para el buen desempeño de las redes IP convergentes. Los objetivos de esta recomendación buscan proponer un estándar en el manejo del tráfico, basado en parámetros de algunos factores que se puedan presentar sobre el sistema de red.

Parámetro de desempeño de la red	Clase 0	Clase1	Clase 2	Clase 3	Clase 4	Clase 5
Retardo	100 ms	400 ms	100 ms	400 ms	1 s	N/E
Jitter	50 ms	50 ms	N/E	N/E	N/E	N/E
Tasa de pérdida de paquetes	$1X10^{-3}$	$1X10^{-3}$	$1X10^{-3}$	$1X10^{-3}$	$1X10^{-3}$	N/E
Tasa de error						N/E
Dirigido a Aplicaciones	Altamente Sensibles a variación del retardo, aplicaciones interactivas como VoIP, Video Conferencia.	Sensibles a variación del retardo, VoIP, Video Conferencia.	Intercambio muy interactivo de datos de datos (señalización)	De envío interactivo de datos	De baja pérdida envíos de corta distancia, datos en grandes cantidades o flujos de video.	Aplicaciones tradicionales sobre redes IP con parámetros default

Tabla 1.4. Resumen de la recomendación Y.1541 [ITU]. Clases de QoS y objetivos de desempeño de red.

Los objetivos Y [1541] son generalizados para diversos tipos de aplicaciones. Por ejemplo, Clase 0 se puede utilizar para voz interactiva y el vídeo. Ellos sólo se preocupan de la parte del sistema de red.

1.3.2. Mediciones Multipunto.

Mediciones bidireccionales en la red, con usuarios de extremo a extremo y de redes o segmentos de redes separadas o heterogéneas. Para lograr eso se deben conocer ciertos factores claves, tales como la sincronización de reloj, en el sistema de red, así como el flujo de tráfico. Para el segundo caso comentado que es el flujo de tráfico, específicamente se deben conocer los paquetes individuales para después lograr medir parámetros característicos (mencionados anteriormente). Para identificar el flujo de tráfico usualmente se usan cabeceras de paquete (direcciones, puerto, números de identificación de paquete). Por tanto para obtener los factores que se requieren en la medición se hace uso del monitoreo para después hacerlo medir en un punto singular.

1.3.3. Métodos de medición de QoS.

1. Analizadores de Red.

Capturan paquetes que viajan a través de la red, y los analizan para concluir que es lo que pasa en ella, son usados para decodificar los protocolos de uso común y muestra el tráfico en forma que pueda ser leída por el administrador de red. Se componen en general de cinco partes principales.

- Hardware. Aunque normalmente toda la configuración y el trabajo de monitoreo, recabado, análisis y proceso de la información se hace a nivel software. La parte hardware se usa para checar que no hay errores de redundancia cíclica (CRC), problemas de voltaje, problemas de negociación entre host etc.

- Driver de captura. Es el núcleo del analizador, se encarga de hacer el proceso de captura y análisis de paquetes sobre la red.

- Buffer. Es la unidad de almacenamiento de los paquetes capturados.

- Analizador en tiempo real. Es usado para analizar el tráfico de paquetes tal cual como salen del cable de red.

- Presentador. Ya que cada protocolo tiene su propio codificar y decodificador su función es hacer que la información obtenida y procesada sea presentada en forma entendible al administrador de red.

2. Herramientas de monitoreo QoS en tiempo real.

Con estas herramientas es posible monitorear la conectividad e intercambio de flujos e información entre dos aplicaciones, así como la calidad que hay en la transmisión y entrega de los paquetes que viajan sobre la red.

El software debe estar instalado en ambos equipos, tiene posibilidades de capturar todo el tráfico o en su defecto en modo monitor, solo los paquetes enviados. El software usa información de paquetes IP y de protocolos de red de capas superiores.

3. MOSFET. (Mobile service testing and measurement tool).

Diseñado para medir factores como retardo, entre un punto específico y el servidor de la red. Recolecta información HTTP, peticiones de usuarios celulares (3G, EDGE, GPRS), el sistema consiste en un servidor de prueba, y una aplicación que soporte el usuario móvil que ejecutaría las mediciones actuales.

Algunas características de este tipo de herramienta son:

- Servicio de tiempo de conexión. Promedio, máximo, mínimo etc.

- Servicio de tiempo de carga de contenido. Promedio, máximo, mínimo etc.

- Total de bytes transferidos en cada petición.

- Total de servicios fallidos en cada petición.

- Tiempo total en que se desarrolla la prueba.

- Total de archivos transmitidos cuando se desarrolla la prueba.

- Promedio de datos transferidos cuando se desarrolla la prueba medida en Kbps.

4. Métodos de medición diseñados por medio de aplicación de capa y monitoreo.

- RMON. Es posible monitorear y decodificar algunos protocolos que operan en capas más altas de red, puede leer aun paquetes de esas capas con cabeceras encapsuladas, provee de un monitor de nivel de aplicación.

- RTFM. Es una arquitectura de flujo de tráfico en tiempo real, diseñado como monitor de flujos de red, identificado a través de recursos o destinos de tráfico en varios mecanismos de monitoreo.

- RTCP. Siendo posible implementar QoS mediante mensajes de protocolos de control en tiempo real, que son usados para calcular QoS y garantizarla a usuarios de extremo a extremo.

1.4 Soluciones QoS.

Existen ya algunas soluciones circulando en los sistemas de red dentro del ambiente de las telecomunicaciones, se describirán a continuación las características principales de tres de ellos. Tabla 1.5 [7]. Se exponen DiffServ, MPLS e IPv6 por ser los más difundidos y usados sobre los sistemas de red actualmente.

Soluciones QoS existentes	DiffServ IP QoS	MPLS QoS	IPv6 QoS (CSF6N, F6SN) CSF6N supone el uso de una arquitectura con manejador de ancho de banda.

Tabla 1.5. Algunas soluciones QoS existentes.

En la siguiente Tabla 1.6., se muestra en general como hace el manejo de tráfico desde la perspectiva de cada solución tecnológica QoS. Se describen características como, si es que la el modelo de solución agrega información extra en el manejo y procesamiento del trafico del sistema de red, si el modelo contempla un agente que haga el manejo del ancho de banda o si tiene integrado un SLA, etc.

Manejo de tráfico	Diffserv	MPLS	IPv6
Encabezados adicionales para la pila IP	NO	SI, con encabezado de 32 bits MPLS	SI, el encabezado IPv6 si el host implementa IPv4 No, para IPv4 QoS-PRN si el host implementa IPV6
Etiqueta de conmutación	No, no está implementado para IntServ	Sí, pero únicamente para porciones de MPLS integradas. Si, para MPLS completo.	No, Para CSF6N Si, Para F6SN
Potencia agregada y escalabilidad	No se requiere por qué no se tiene control. Si, para todas las soluciones DiffServ. No para IntServ.	Si, para MPLS integrados en cada porción. Si, para MPLS completo	Si
Concurrencia para accesar a recursos	No, porque no existe control Si, para PCN DiffServ Si, para BB Si, para IntServ	Si, para MPLS integrados en cada porción. Si, para MPLS completo	Si
Clasificación SLS/SLA	Limitada Distinción de tráfico particular para IntServ	Limitada para MPLS integrado. Ilimitado para MPLS completo	Ilimitado para CSF6N Ilimitado para F6SN completo
Manejador de ancho de banda dinámico	No, porque no hay control. No para PCN DiffServ. Si, para BB Si, para IntServ	Si, para MPLS integrados en cada porción. Si, para MPLS completo	SI
Procedimiento de asignación de Recursos	No, porque no hay control. Manual/automático para PCN DiffServ. Automático para BB. Automático para IntServ	Automático para MPLS integrado, con cada porción concentrando el total de red IPv4 QoS-PRN. Automático para MPLS completo.	Automático.

Tabla 1.6. Manejo de Tráfico.

En la tabla 1.7. Se muestran las características que tienen las soluciones QoS existentes, características importantes pues se trata de cómo deciden hacer el manejo de ancho de banda, así como el control y asignación que se hace para los recursos del sistema de red.

Optimización de ancho de banda	Diffserv	MPLS	IPv6
Sondeo	No usado si no hay control. Necesario para PCN DiffServ. No usado para IntServ	No usado para MPLS integrado. No usado para MPLS completo.	No usado
Esquema de asignación de ancho de banda	No implementado si no hay control. Estático para PCN DiffServ. Dinámico para BB. Dinámico para IntServ.	Dinámico para MPLS integrado. Dinámico para MPLS completo	Dinámico
Control de asignación de recursos	No implementado si no hay control. Nivel de planeación para PCN DiffServ. Nivel de llamada para BB. Nivel de llamada para IntServ	Nivel de llamada para MPLS integrado. Nivel de llamada para MPLS completo	Nivel de llamada
Aprovechamiento de ancho de banda cuando se agrega SLA heterogéneo	No considerado si no hay control. Desaprovechamiento medio para PCN DiffServ. Desaprovechamiento medio para BB Sin desaprovechamiento para IntServ	Desaprovechamiento medio para MPLS integrado. Sin desaprovechamiento para MPLS completo	Sin desaprovechar

Tabla 1.7. Aprovechamiento del ancho de banda.

La tabla 1.8. Muestra el manejo que se hace ante la admisión de control llamada. Un método usado para impedir el libre acceso a la red, ya que esto provoca congestiones, en cambio con el CAC. Se puede complementar con el protocolo RSVP y ofrecer una solución para dar prioridades, espaciamiento y control sobre los usuarios que soliciten acceder al sistema de red.

Control de Admisión de llamada (CAC)	Diffserv	MPLS	IPv6
Control de admisión de llamada	NO si no hay control. Si para PCN DiffServ. Si para BB. Si para IntServ	Si para MPLS integrado. Si para MPLS completo	Si
Precisión para procesar el ancho de banda durante el CAC	No se aplica si no hay control. Limitado para PNC DiffServ. Alto para BB Muy alto para IntServ	Muy alto para MPLS integrado. Muy alto para MPLS completo	Muy alto para CSF6N. Muy alto para SF6N.
Apropiación durante CAC	No se aplica si no hay control. Implementable para PNC DiffServ. implementable BB implementable para IntServ	Implementable MPLS integrado. Implementable MPLS completo.	Implementable

Tabla 1.8. Control de Admisión de llamada.

Algo muy importante dentro de las redes de telecomunicaciones son los protocolos de señalización, las soluciones que se proponen a través del uso de estos y el trato que hacen hacia tráfico, la tabla 1.9. Se muestran las opciones de señalización que ofrecen los modelos QoS.

Protocolos de señalización	DiffServ	MPLS	IPv6
Protocolos de interdominio	No señalización si no hay control. QBGP/modificado RSVP para PCN (estandarizado). NSIS/protocolo QoS dedicado Protocolo BB no estandarizado	qBGP/RSVP-TE para MPLS completo (no estandarizado)	NSIS/Protocolo QoS Dedicado (no estandarizado)

Tabla 1.9. Protocolos y señalización.

Por último en esta sección se muestra la tabla 1.10. Donde se puede ver cómo es que ocurre la planeación del sistema de red y como cada tecnología aporta la solución que se adapta a sus necesidades.

Planeación de red	DiffServ	MPLS	IPv6
Necesidad a priori sobre-provisión	Si, (si un mínimo de calidad es requerida) para no control Parcial par PCN DiffServ. Parcial para BB. No, Para IntServ	Parcial para MPLS integrado. No, para MPLS completo	Parcial para CFF6N. No para F6SN
Diseño de planeación de fase.	No requerido/trivial si no hay control. Dificultad promedio para PCN Diffserv. Difícil para BB. Difícil para IntServ.	Difícil	difícil

Tabla 1.10. Planeación de red.

En Internet:

[1] www.exitoexportador.com/stats.htm

[2] http://www.tmforum.org/browse.aspx?type=4&SearchString=QoS

[6] http://www.itu.int/rec/T-REC-Y.1541/es

Referencias bibliográficas:

[3] Deploying QoS for cisco ip and next generation networks. Vinod Joseph / Brett Chapman. Morgan Kaufmann. ISBN 978-0-12-374461-6. Año de publicación 2009.

[4] Deploying IP and MPLS QoS for multiservice networks. Jhon Evans / Clarence Filsfils. Editorial Morgan Kaufmann. ISBN 13: 978-0-12-370549-5. Año de publicación 2007.

[5] S. Amante et al, "Inter-provider Quality of Service", Quality of Service Working Group, MIT Communications Futures Program (CFP), Nov. 2006

[7] QoS over heterogeneous networks. Mario Marchase. Editorial Wiley. ISBN 978-0-470-01752-4. Año de publicación 2007.

CAPÍTULO II.

Estado del arte y propuesta del nuevo modelo.

RESUMEN:

En este capítulo se presentan y se hace detalle acerca de las soluciones existentes que hay para asegurar QoS. Además se hace la propuesta y caracterización de un modelo nuevo modelo de calidad.

OBJETIVOS DEL CAPITULO:

- Mostrar el estado del arte de las soluciones QoS.
- Mostrar el panorama general de la propuesta de solución ante la falta de calidad en los servicios en base del nuevo modelo.

2.1 Tecnología de soluciones QoS.

A lo largo de la historia de las telecomunicaciones se ha dado la rápida evolución de las redes de computadoras, han surgido tecnologías y técnicas para hacer más eficiente el uso de los servicios que se despliegan sobre los propios sistemas de red. En la actualidad estas son redes convergentes que corren sobre si muchos servicios y si el administrador o el ingeniero de red se preocupan por asegurar calidad en los servicios las redes tendrán un funcionamiento óptimo en desempeño de sus servicios.

Un sistema de red convergente está dotado de tecnologías capaces de unificar el tráfico de voz, video y datos, sobre un solo canal de comunicaciones. Anexando además al entorno los servicios y aplicaciones que integran las propias tecnologías dándole un extra de utilidad y beneficios. Tal como telefonía IP, video conferencias, Tráfico de grandes volúmenes de información a velocidades altas (Redes de alta velocidad).

Algunos beneficios de implementar este tipo de red son:

- óptimo aprovechamiento del ancho de banda debido a la capacidad de subdividir canales de acuerdo al uso, planeación o requerimiento de cada segmento o servicio de la red.
- Redes más seguras debido a la mejor señalización, además del buen manejo de tráficos y flujos que existan sobre la red.
- Simplicidad en cuanto al uso de aplicaciones y compartir información ya que al viajar los diferentes tipos de información por el mismo canal, hay compatibilidad en las aplicaciones integradas a los mismo sistemas de comunicación.
- Reducción en las la latencia y caídas de la red que originan pérdidas en de información y mala conectividad

Si es necesario hacer una reingeniería de red, no es forzoso adquirir todo el equipo tecnológico de una sola vez para hacer la migración a los sistemas de red convergente, podría ser gradual comenzando con el equipo inservible u obsoleto.

Existen algunas preguntas [1] que sientan las bases al realizar una planeación de red, responder a ellas es un buen camino para el aseguramiento QoS.

¿Cómo saber cuándo es considerable desplegar QoS como solución en una red?

Las posibles respuestas son:

- Cuando hay exigencia por parte de los servicios para tener prioridades de aplicaciones con necesidades críticas de la red.
- Cuando se requiere maximizar el uso de la infraestructura de red actual.
- Obtener mejor desempeño para sensibilidad de retardo en aplicaciones, tales como voz o video.
- Cuando ha habido cambios en el sistema de red, y se implementa como un plan para responder a dichos cambios por ejemplo flujos o volumen de tráfico.

Un ejemplo de ello se muestra a continuación, con un ejercicio de análisis, donde de manera gradual se van obteniendo y descartando posibles respuestas de solución.

> ¿Se asumen recursos sobrados de red?

Bien, esta pregunta resulta hasta cierto sentido hipotético o utópico al darle el enfoque de, ¿Si se tienen los suficientes recursos de red, para que hacer planeación QoS?

Podría pensarse que hay un buen sentido de certeza. Pero; es innegable que, aunque haya suficiente equipo tecnológico y recursos la red no estará disponible en esa abundancia en todo momento en todos los escenarios posibles. Es por ello que debe tenerse una planeación y asignación de recursos y escenarios, ya que de no hacerse la red por sí misma no ofrece ninguna garantía de buena ejecución o calidad más allá del mejor esfuerzo.

> No se tienen recursos tecnológicos sobrados para la red, solo los suficientes ¿Se podría equilibrar con la reserva de recursos y/o control de admisión?

En efecto teniendo un esquema que asegure los recursos para cuando sean necesitados por los servicios y de esa noción de calidad a los usuarios mediante calendarización, arbitraje, políticas o planes.

Ejemplo de estas decisiones podrían ser, el recurso exclusivo (no compartir en ningún momento, usado solamente por algún servicio o grupo particular); compartir recursos en desuso. En cualquiera de los casos hay un nivel de garantía y una planeación para algún escenario distintivo.

> ¿Cómo será la asignación de los recursos entre quien los pida?

En el entendido de que se está manejando una red convergente, donde finalmente viajarán sobre el mismo canal datos provenientes de servicios de video, voz, o datos. Hay que idear la manera correcta en que se va a hacer la asignación, para que resulte más adecuada conforme los recursos que están desplegados sobre la red.

Hay que ser capaz de separar o clasificar tráfico de diferentes grupos de servicios, para tomar decisiones acerca de que o cuanto será lo que cada grupo de tráfico merece para un óptimo desempeño. En consecuencia, hacer la ejecución según los planes o políticas que hayan sido asignados.

Para esto se han creado modelos tecnológicos, que a lo largo de la historia de desarrollo han tenido gran importancia y evolución hasta llegar a lo que tenemos hoy en día.

2.2. Antecedente histórico de las soluciones QoS [1].

QoS referido como modelo de servicio, es un conjunto dotado de capacidades para proveer un nivel específico de calidad extremo a extremo de la red.

Es así que se comenzará a describir los avances para asegurar QoS a través del tiempo, también se abordará en primer lugar la red telefónica pública conmutada, hasta ampliar el panorama a la actualidad sobre los métodos y modelos de QoS.

2.2.1 Soluciones sobre la red telefónica publica conmutada (PSTN).

Al ser de las primeras redes de comunicaciones denominadas mundiales, esta red tenía entre su tecnología la reserva de tiempo de acción, por medio de periodos de reserva de recursos para que los usuarios pudiesen realizar la comunicación.

Esto podría hacerse de dos maneras, manual o automática mediante protocolos de desempeño, señalización y comunicación.

Si se realizaba de manera automática era solo bajo la plena seguridad que el acceso a los medios estaba soportado para el o los clientes que lo solicitaron, de otra manera, se haría una rutina de control de acceso (negando el acceso) si es que la red está al límite o por demás saturada.

La manera manual obedecía al desempeño que la red tenia y una reserva no automatizada de recurso para permitir o negar el acceso de manera manual.

Las soluciones QoS que despliega este tipo de red son básicamente:

- Apoyarse en los recursos de reserva y control de admisión.
- Asignación de recursos de manera exclusiva.

2.2.2 QoS sobre redes en modo de transferencia asíncrona (ATM).

La tecnología ATM fue pensada para construir y sustentar las bases de la infraestructura para redes de banda ancha, basándose en la conmutación de paquetes y no en la conmutación de circuitos. Originalmente fue ideada en la década de los 60 en los laboratorios AT&T.

A diferencia de la tecnología de red telefónica conmutada, en ATM la información no es transmitida sobre canales asignados previamente bajo permanencia de estado de reserva sino en paquetes o tramas individuales (bajo su propio formato ATM), y que pueden ser enrutadas usando los canales o rutas virtuales (VC). Tecnicismos propios del funcionamiento la tecnología de comunicación ATM.

Ante lo cual, la solución de QoS para ATM se caracterizaba por dos propiedades básicas.

- Reserva de recursos de apoyo y control de admisión. Aunque se haga dicha reserva no se tiene acceso al uso exclusivo a los recursos de red.
- Usando alguna política o basándose en la interfaz de cliente se hacia algún tipo de asignación, reserva o clasificación, de tráficos, además ATM también contaba con mecanismos de gestión de tráfico por eso sería indispensable confiar en la separación de colas y la programación sofisticada para garantizar el desempeño al tiempo que permitía el intercambio de recursos.

ATM ofrecía una solución muy sofisticada QoS. Se podía garantizar el rendimiento y al mismo tiempo permitía el uso compartido de recursos. Pero a expensas de la alta complejidad, lo que llevó a alto costo y la falta de interfaz de alta velocidad.

2.2.3 QoS sobre redes con reenvío de tramas (Frame relay).

Frame relay es una técnica de aprovechamiento de red, normalmente ligada a ATM, inclusive hay autores que lo manejan como su extensión o complemento.

Frame relay fue propuesta por la **ITU**, consiste en la conmutación de paquetes enviados de forma encapsulada en un marco o frame de tamaño variable haciendo su envío de manera ordenada por el mismo camino de comunicación, proporciona conexiones entre usuarios de manera permanente o conmutada.

Este tipo de tecnología tiene una reserva de recursos (acceso a los servicios, por tiempo delimitado. Tipo lapso de uso). Además de ser una tecnología muy adaptativa a las demandas de red, no obstante cuando se supera la reserva de recursos los paquetes excedentes se enviarán “marcados como de mejor esfuerzo (Best Effort)”.

Un segundo mecanismo de QoS puede ser la llamada notificación de tráfico ya sea por bits o en la cabecera del marco enviado para así, disminuir la velocidad o continuidad del flujo y evitar pérdidas de información o caídas en los servicios.

Bien al ser considerado la mayoría de las veces como un conjunto de ATM (más bien muchas veces esta tecnología recae o esta cimentada en ATM) se pueden usar los mismos criterios QoS que para ATM.

2.2.4 QoS sobre Ethernet.

Ethernet es una tecnología que se caracteriza por su simplicidad de uso e implementación a un bajo costo, que le ha valido la sobrevivencia a través de los años y diferentes tecnologías. Incluso se sigue estudiando para que pueda ser mas explotada (se sigue mejorando y estudiando su uso, para que sea una tecnología más eficiente).

Creada a finales de la década de los 70, en el centro de investigaciones de Palo Alto California. Ha sufrido bastantes modificaciones hasta llegar a los que es hoy en día. A principios de los 80 se crea la versión de 10Mb y es estandarizada por la **IEEE**. Pero es hasta el año de 1998 cuando se comienzan a observar las nociones de QoS y se extiende el uso de las redes IP. Es en esa época donde se mancuerna Ethernet con el protocolo TCP y el protocolo IP.

Sin embargo, la brecha que hay que cubrir es grande, en cuanto a la señalización y control de las comunicaciones. La solución que ocupa la tecnología Ethernet para transmitir en cierto sentido de QoS es el acceso múltiple por detección de portadora con detección de errores (CSMA/CD), que en sus inicios se le pronosticaba poca utilidad ya que en general la tecnología; se decía no proponía nada nuevo e incluso no aseguraba el envío ni la entrega de datos.

La tecnología Ethernet proponía QoS basada en implementación de prioridades:

- Prioridad 0: por defecto, que se supone mejor esfuerzo.
- Prioridad 1: Reservado, "menos que" el mejor esfuerzo.
- Prioridad 2-3: Reservado.
- Prioridad 4: Sensible al retardo, no obligado.
- Prioridad 5: Sensible retado, 100 ms. Soluciones QoS.
- Prioridad 6: Sensible al retardo, 10.
- Prioridad 7: Control de red.

Pero en realidad, esta propuesta de prioridades nunca se llevo a cabo como tal.

La gran mayoría del tráfico se envía etiquetado como mejor esfuerzo sin ninguna garantía.

2.2.5 Servicios de Mejor esfuerzo (Best-Effort service):

Es el primer modelo utilizado, desde los inicios de las redes, y en realidad la calidad que pueda ofrecer no tiene ninguna garantía más que el potencial de la misma red. Ciertas aplicaciones pueden funcionar sin mayor problema en este modelo, estas son FTP y HTTP. Como se puede ver, son aplicaciones de bajo nivel de consumo de recursos y exigencias de red, además que no requieren mayor demanda de calidad por parte del usuario.

2.3 Estado del arte de las soluciones QoS [3].

2.3.1 Servicios Diferenciados (DiffServ).

Este modelo provee los parámetros de calidad por medio de negociación de características en las redes extremo a extremo. Optimiza el nivel necesario por estas aplicaciones para operar satisfactoriamente; se apoya en los mecanismos QoS para reservar los recursos necesarios de la red, dando prioridad a la aplicación para comenzar su correcta transmisión.

A manera de apoyo, la red usa el proceso de control de admisión, que es un mecanismo de prevención de sobrecarga. Para que las aplicaciones comiencen la transmisión de datos debe haber antes una señal de liberación por parte del modelo QoS. Después de ello, la comunicación comienza la transmisión sobre los recursos reservados, hasta que termina o rebasa el nivel reservado de ancho de banda y otorgándosele un estado de nueva reservación por flujo, política, clasificación y/o almacenado en una cola inteligente administrada bajo el modelo QoS.

Las dos maneras principales de brindar la carga controlada de los servicios son por medio de un manejo inteligente de colas y RSVP (Resource Reservation Protocol) en conjunto con los protocolos de ruteo para determinar el mejor camino de asegurar el nivel requerido de QoS. RSVP es un protocolo que habilita una lista dinámica de acceso en los ruteadores, asignando parámetros de un nivel mínimo en el modelo de QoS.

2.3.2 Servicios Integrados (IntServ).

Este modelo proporciona un conjunto de reglas y mecanismos de clasificación, así como de encolamiento, además de trabajar en conjunto con protocolos y aplicaciones que otorgan un nivel de prioridad sobre otro tipo de tráfico que no requiera niveles específicos de QoS.

El modelo DiffServ confía en la configuración de la topología de ruteadores de borde para realizar la clasificación de tráfico de paquetes que atraviesan la red, cabe la posibilidad de hacer clasificación bajo diferentes criterios como son:

- Direcciones red.
- Protocolos y puertos.
- Interfaces de ingreso.

O cualquier otra que pueda satisfacer alguna necesidad específica, tomando en cuenta los datos compilados por la lista de acceso a la red. El marcado o clasificación de paquetes es en una sola dirección de flujo.

2.3.3 Conmutación de paquetes mediante etiquetas (MPLS).

MPLS es capaz de ser transportado sobre cualquier capa de enlace de protocolo, incluyendo IP, ATM, Frame Relay y Ethernet, en MPLS la primer entrada al ruteador clasifica los paquetes en un FEC (Forward Error Correction - sistema de corrección de errores) tomando en cuenta la información de cabecera de paquete y a continuación, los mapas a la FEC deciden el siguiente salto basado en el algoritmo de enrutamiento.

Sobre el modelo MPLS, los paquetes viajan de un ruteador a otro y cada ruteador toma la decisión independiente de los otros ruteadores para el reenvío de los paquetes. Cada ruteador analiza la cabecera de paquetes y elige el próximo salto para el paquete sobre la base de la cabecera y el algoritmo de enrutamiento de paquetes. El ruteador periódicamente ejecuta un algoritmo de enrutamiento de capa de red, y los resultados son almacenados en la tabla de ruteo para una revisión rápida. Por ejemplo, en el envío convencional de paquetes IP el ruteador podría hacer un mapa con prefijos de direcciones X en su tabla de ruteo, basados en su camino más largo para cada destino de dirección paquetes. Este paquete atraviesa la red y en cada salto se le reasigna el salto siguiente. La integración de la capa tres (capa de red en el modelo OSI) y el envío de datagramas y la capa dos (capa de enlace en el modelo OSI) Switcheo y transporte utiliza la etiqueta para permitir búsquedas más eficientes de clasificación de paquetes. Los Paquetes MPLS son capaces de llevar una serie de etiquetas, organizadas en una pila LIFO (Last-In/First-Out).

Hay dos enfoques para el etiquetado del control de rutas.

1. Control independiente significa dispositivos que son capaces de crear y distribuir conjuntos de etiquetas hacia otros dispositivos independientes.

2. Pedido o reserva de camino de control, que se utiliza para garantizar que una clase particular, el tráfico sigue un camino con una serie de propiedades QoS, algunas ventajas que esto presenta son:

    - Los paquetes pueden ser etiquetados de manera diferente en función del ruteador por donde entre, y las decisiones de transmisión depender también del ruteador de entrada.

- El paquete puede ser obligado a seguir un camino de modo explícito en lugar de ser elegido por el algoritmo de enrutamiento para apoyar la ingeniería de tráfico.

La clase de servicio puede deducirse de la etiqueta, y los ruteadores pueden después aplicar diferente programación de disciplinas o descartar a paquetes.

Hasta ahora se ha presentado un panorama general de lo que puede entenderse como la historia y estado del arte de los modelos utilizados para asegurar QoS, a continuación se caracteriza, detalla y presenta un modelo capaz de asegurar QoS sobre redes convergentes, basado en métodos y técnicas que proponen realizar una descripción total de la infraestructura tecnológica y los servicios con que cuenta. Para lograr esto, el modelo se basa en un estudio detallado de la red donde se va a aplicar dicho modelo para así garantizar un buen nivel de calidad. El modelo busca ser flexible, adaptable y robusto, para así al llegar a una etapa de implementación se convierta en una buena alternativa de solución y arquitectura de calidad.

2.4 Propuesta de modelo de calidad en los servicios para una red convergente.

En este apartado se describirá la propuesta de solución para asegurar calidad en una red convergente, este modelo es una idea original concebida después de hacer un análisis a la problemática detectada en un segmento de red del instituto politécnico nacional, dicha red corresponde al segmento del Centro de Formación e Innovación educativa y la necesidad de garantizar los servicios desplegados sobre ella. Se definen las etapas del modelo propuesto que consta de seis capas y permiten garantizar servicios de conectividad, reconocimiento y monitoreo de una red de voz, video y datos servicios y tráficos típicos en una red convergente y de uso en un sistema educativo.

La solución propuesta a través del modelo Figura 2.1 pretende estar dotada de un carácter estándar para diferentes tipos de red, en cuanto a su composición tecnológica de hardware y topología lógica, dando paso después de la implantación (del modelo presentado) sobre el sistema de red a una arquitectura.

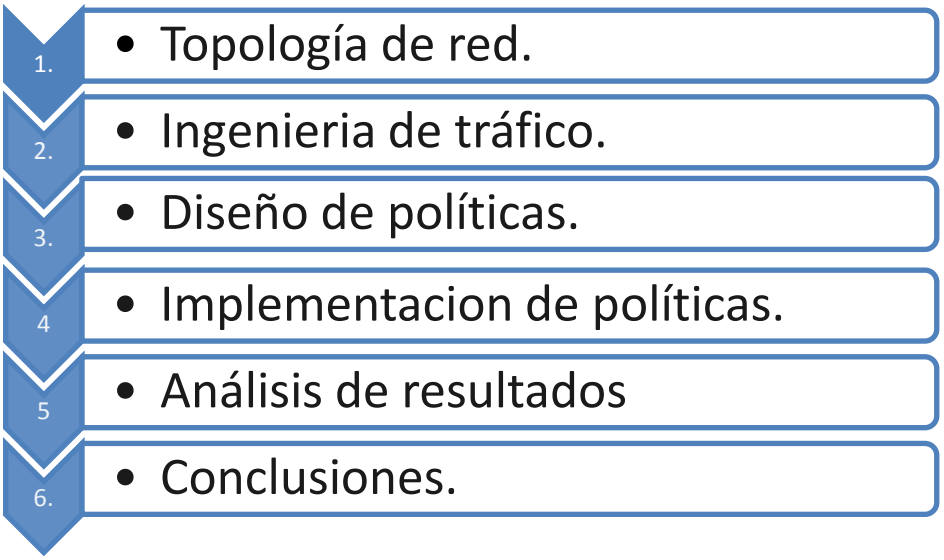


Figura 2.1. Modelo de calidad.

Al implementar este tipo de tecnología, métodos y técnicas se asegura que aquellas aplicaciones o servicios que requieren utilizar determinados parámetros o alguna característica específica de la red, para su buen funcionamiento tengan reservado y disponible ese recurso en el momento que se le solicite.

Para tal fin uno de los principales conceptos acompañados a la tecnología QoS es la priorización, esto es darle de alguna manera más importancia a algunas conexiones que a otras.

Veamos algunos beneficios que podemos encontrar al implementar QoS en redes convergentes:

- Control sobre los recursos: podemos limitar el ancho de banda utilizado por aquellas aplicaciones con este tipo de conexión en sus comunicaciones.
- Permite usar más eficientemente los recursos de la red: al poder establecer prioridades sobre los diferentes tipos de servicios.
- Menor latencia: este es el caso en el que por ejemplo una aplicación de tráfico interactivo como es el protocolo SSH, telnet, etc. requieren un menor tiempo de respuesta que otras aplicaciones.

Existen varias formas de aplicar esta tecnología de calidad de servicio ya sea en software como en hardware, existen las aplicaciones comerciales y por supuesto las alternativas libres y de código abierto.

Este tipo de tecnología es importante tenerla presente en los ambientes laborales y empresariales, debido a que muchas veces la red es mal utilizada por los usuarios, para transmitir, descargar, o navegar entre información

muchas veces innecesaria. Implementando el servicio QoS podemos llevar un mejor control no solamente del contenido sino también de las terminales que tendrán un mejor acceso que otras.

2.4.1 Etapa de Análisis de la topología de red.

Aquí es donde se hace un estudio detallado de la red en cuestión, intentando conocer diversos factores operacionales responder preguntas claves como:

- ¿Con que equipo tecnológico se cuenta? (topología de red)

Aunque en el momento del estudio, los equipos puedan mostrarse aun en estado funcional, se tiene que considerar una renovación tecnológica si acaso la vida útil de los equipos ha terminado puesto que, para aplicar y asegurar tecnologías de calidad es necesario características denominadas especiales que el equipo actual brinda de manera implícita dentro de sus configuraciones.

El objetivo de hacer el reconocimiento de la topología de red tiene dos propósitos fundamentales, el primero relacionado estrechamente con el manejo de la red y principalmente tomar en cuenta los puntos donde se llevara a cabo la recolección de información y datos acerca del equipo que es usado en la red tal como serían ruteadores, conmutadores (switches), sistemas de transmisión, sistemas de conexión (eléctrica), cableado estructurado que exista entre dichos equipos.

Con esto también estamos cubriendo la necesidad de conocer la forma en que se encuentran configurados los equipos, hacer el rastreo del estatus de funcionamiento actual, capacidad de procesamiento y en algunos casos los informes de alarma que se puedan generar o haber generado a causa de los dispositivos componentes de la red.

La manera en que se actúa para hacer lograr lo arriba mencionado es a través del uso de Protocolos de red por ejemplo SNMP (protocolo Simple de Manejo de Red - Simple Network Management Protocol) bajo un fallo conocido (exploit), otra opción sería el Protocolo de Manejo de Redes de Telecomunicaciones (Telecommunications Management Network TMN).

El principio básico del método de reconocimiento de topología de red se basa en la elección y monitoreo periódico de dispositivos y procesar sus notificaciones generadas, se menciona como factor importante en reportes y en el manejo de plataformas de marcas especializadas.

El segundo objetivo que queda cubierto es el reconocimiento lógico de la topología, y que está estrechamente relacionado con las características de ruteo y el reconocimiento de las matrices de tráfico, permite al administrador de red tener bases solidas para la toma de decisiones acerca de la optimización y el buen desempeño de la red. Dicho reconocimiento de las características de ruteo puede hacerse con monitoreo específico, lo cual es solamente una recolección de datos que necesitaran un análisis posterior, en esta encomienda es muy usado software que se apoya en el protocolo de información de ruteo (Routing Information Protocol. RIP). Y el estudio de cada configuración guardada y desempeñada por el dispositivo.

- ¿Quién usa la red? (Servicios ofrecidos).

Al momento de llegar a esta etapa se necesita hacer un estudio detallado de los usuarios que usan la red, los servicios que necesitan, los servicios ofrecidos por la red, y saber si se están aprovechando recursos como el ancho de banda incluso hacer el estudio para cada nodo de manera óptima, si cada servicio consume el ancho de banda que necesita y genera solo el tráfico que le es permitido o si es el caso, cual usuario o servicio genera más tráfico del que pudiese requerir, entonces se podría decidir cómo solucionar ese aspecto.

- ¿Cuál es el uso que se le da a la red? (Servicios requeridos).

Cuál es el tipo de usuarios que comúnmente acceden a los servicios que brinda la red. (Para el caso de estudio se tendrá en cuenta una red educativa, universitaria). Para luego entonces comenzar a caracterizar ciertos factores claves como son el nivel de uso mantenido por el tráfico, flujo de tráfico, volumen de tráfico etc. Una calendarización que nos permitirá saber si se encuentran horas pico, congestiones regulares, y poder darle una solución adecuada.

Toda vez que se tienen resultados de las mediciones entonces se puede realizar un análisis para proponer la forma de atacar el problema, entonces se puede dar paso a una etapa más.

2.4.2 Ingeniería de Tráfico.

La ingeniería de tráfico obtiene soporte de las bases de la red, la asignación o reasignación de los parámetros de transporte de la red, para lograr la optimización de su comportamiento. Cumple también con diferentes objetivos, como son previsión, planeación, dimensionamiento, control, y desempeño a través de una caracterización y monitoreo de la red, este proceso es manejado

normalmente usando diferentes perfiles de recolección, podríamos clasificarlo de primera instancia como diario (poniendo atención puntual en horas), semanal, mensual, e inclusive llegando a reportes anuales, logrando así un compilado histórico acumulativo. Los beneficios de hacer la implementación de Ingeniería de tráfico es la posibilidad de hacer una comparación detallada entre caracterizaciones de los tipos de servicio entrantes y los servicios a los que se les ha agregado el soporte de calidad. El proceso de estudio de ingeniería de tráfico junto con algunas propuestas para separar las clases de flujos reconocidas dentro del sistema de red podría ser:

- Caracterización de tráfico.

Tiene como objetivo identificar patrones de variación del tráfico transportado, usando el análisis estadístico de los datos recopilados sobre la red, poniendo atención sobre el enfoque granular ya que podemos hacer la separación y puntualización en perfiles de flujos de tráfico, interfaces, nodos, rutas o caminos, fuentes, destinos, etc.

Por supuesto, hacer la estimación de la carga de tráfico de acuerdo a los servicios, perfiles de uso y usuario o rutas seguidas. Y observar la tendencia de crecimiento para obtener la previsión y respuesta adecuada a la demanda que surja a causa del tráfico.

- Monitoreo de red.

Los objetivos fuertemente identificados para este punto son conocer el estado operacional de la red, incluso aunque esté pasando por un periodo funcionalmente malo, obtener el reconocimiento continuo de la calidad brindada en los servicios desplegados por la red y el adecuado funcionamiento de políticas aplicadas a dichos servicios, y por último, verificar los contratos establecidos entre el proveedor de servicios y el desempeño de la red a través de las mediciones que arroja el monitoreo de los segmentos intercomunicados por intranet LAN y la salida a conexiones de internet WAN.

Ya que las redes tienden a ser convergentes y deberán soportar flujos de tráfico multimedia y datos a la vez, lo que debemos tener en cuenta en este tipo de mediciones y monitoreo son las métricas que regulan una buena o mala calidad. Tal como retardo, variación de retardo, jitter, latencia, ancho de banda, disponibilidad de red y servicios, pérdida de paquetes etc. Antes de hacer un despliegue a favor de la implementación de mejoras o normas se debe de tener probado el rendimiento de los servicios y la red bajo esos parámetros.

Una métrica es una unidad de medida que coincide con un método específico o análisis específico, son valores cuantitativos acerca de cualquier aspecto de red que nos permita estudiarla, dependiendo de cómo y dónde se calculen, u

obtengan las métricas nos permitirán estudiar diferentes aspectos de un mismo dato o información.

Hay dos grupos principales que se encargan de la investigación y estandarización de las métricas de calidad. La **ITU** (International Telecommunication Union – Unión Internacional de Telecomunicaciones) y la **IPPM** (IP Performance Metrics – Métricas de desempeño IP). Estos dos grupos se encargan de definir un criterio sólido para poder documentar un conjunto de métricas que den la posibilidad de medir la calidad, el desempeño y la disponibilidad de las comunicaciones por medio de internet. Deberán proporcionar resultados objetivos basados en mediciones.

- Control de tráfico.

Las funciones que cumple el control de tráfico sobre el desempeño de la red son primordiales e importantes, los objetivos que debe alcanzar son, entre otros, un desempeño adaptativo en la optimización de red que pueda responder ante cambios, contingencias o demandas específicas a la misma. Por ejemplo, hacer un re-enrutamiento en caso de alguna falla o punto sobrecargado de la red, llevando el tráfico por puntos alternos y que la comunicación no se vea afectada, esto según la estructuración del modelo y topología física lo permita. Diseñar un mecanismo de respuesta ante posibles cambios en el flujo de tráfico de la red, haciendo señalización y disponibilidad de la misma. Tener un soporte de la admisión de tráfico generado, de entrada y salida. Un medio para lograr esto sería la reconfiguración del modelo calidad aplicado, las políticas usadas, etc. Dentro de la estructuración del control de tráfico, hay que tomar en cuenta el modelado de niveles tal como comportamiento, accesibilidad, servicio, prioridad, etc.

- Nivel de ocupación de red.

Se Propone realizar un monitoreo general de las funciones de red y sus servicios desplegados, se pueden utilizar para este fin diferentes técnicas e instancias como son:

- ✓ Marcado de paquetes.
- ✓ Marcado de servicios.
- ✓ Marcado de usuarios.
- ✓ Marcado de rutinas.

- Control de acceso.

Es necesario definir quién puede entrar al entorno de red y a que servicios o a que partes de la red, dependiendo la aplicación o los datos que manejen o necesite cada usuario.

Y después dar paso a las consideraciones puntuales, de cada ente que genera tráfico en la red, tomando en consideración la posición que poseen dentro del ambiente estudiado.

Ya que se ha realizado el monitoreo general y particular, obtenemos resultados tangibles que podrán ser comparados con las métricas y políticas propuestas en secciones posteriores. Ese compilado de resultados deberá hacerse en forma frecuente y gradual integrándose a una bitácora de consulta al alcance de los administradores para decidir las acciones a tomar.

2.4.3. Diseño de políticas.

Basándose en lo que ahora se conoce de la red, se puede hacer un reporte, seguido de los puntos que se puedan optimizar, implantar, y de los que sea necesario remover. En conjunto se realizara un plan de escalabilidad para que la red pueda mantenerse actualizada.

En esta etapa se busca poder hacer ciertas distinciones nada triviales ya que es un factor angular, entre más específicas lleguen a ser esas distinciones mejor desempeño tendrá la arquitectura calidad. Comprendido lo anterior entonces, se tiene que clasificar el tráfico generado (aunque algunos de esos generadores de tráfico pueden quedar en una o más categorías no se deben considerar como redundantes, en cambio deberán tomarse en cuenta bajo la perspectiva de que más adelante brindará un elemento de decisión).

Al realizar el análisis, se puede entonces identificar perfectamente lo que resultará en la caracterización de políticas.

Las políticas suelen definirse como un conjunto de reglas, y ello responde a que ciertamente es un ciclo de planeación causa – efecto – reacción.

Al idearse una política atiende a esperar un suceso, si ello pasa (ya sea favorable o negativo), basándose en el proceso de análisis se tiene una reacción, y ejecuta la acción que se le ha asociado.

En esta sección ya es sabido cuales son las amenazas a las que se enfrenta el sistema de red y que acciones deberá tomar para protegerse de ellas, inclusive

es recomendable un plan de acción en caso de desastre. El estudio de estas amenazas y debilidades dará forma a políticas que se desempeñen para mejorar el entorno. Un punto muy importante es la implantación de estas políticas. Ya que solo funcionan si están siendo implementadas.

Entre otras cosas se puede realizar:

- Clasificación.

  Esto lo puede hacer un hardware especializado o algún otro elemento software de red, para identificar los paquetes que correspondan a un flujo, servicio o grupo en particular. Hacer una distinción y trato especial de ellos de acuerdo a las políticas elaboradas.

  Haciendo distinción entre el tipo de servicios que requieren los usuarios de red, tipo de usuario. Una vez teniendo ello, podemos hacer uso de teoría de colas, tablas y protocolos de ruteo.

- Jerarquización

  Una vez que se han clasificado los servicios a usar, los usuarios etc., se deben formar jerarquías que mostrarán quien tiene prioridad (basándose en todos los puntos anteriores.) para formarse y salir de la cola, dar menos saltos en entre ruteadores etc. Hacer clases de tráfico para que sean enviados con prioridades, y que nivel de garantía se le otorgara frente a las demás clasificaciones y frente a la red para un mejor desempeño.

- Control de flujo.

  Para tener vigilancia del sentido del flujo de tráfico, saltos que surjan entre peticiones etc.

- Sectorización.

  Entendida bajo el contexto, de que se encontrarán zonas (por ejemplo zona de jefes, zona de empleados medios etc.) donde los servicios que se utilizan no deberán tener la misma prioridad, puesto que el nivel de jerarquía de los usuarios no es el mismo. Se tiene que atender entonces los de nivel más alto, e ir incrementando gradualmente.

- Control de acceso

  Es aquí en donde se decide si el flujo entrante puede acceder al sistema de red, una de las primeras bases para la toma de decisión es saber si el recurso no se está utilizado ya o cual es la forma en que se decidirá un nuevo acceso. En este sentido actualmente hay una gran variedad de

modalidades de aplicación de control de acceso entre ellas un gestor de políticas.

En conjunto se definirán ciertas políticas, solucionando un grupo de objetivos y desarrollando los planes a seguir por parte de los administradores y usuarios para que el desempeño de la red y sus servicios sea óptimo. Hay diferentes tipos de políticas que darán como valor agregado las mejoras que se persiguen para que la red trabaje mejor y sea aprovechada al máximo, algunos puntos pueden ser seguridad física en las instalaciones, seguridad de sistemas, políticas de acceso, etc.

Hay ciertos puntos que hacen fuertes a las políticas, incluso muchas deben basarse aparte de las necesidades de la red, en normas y estándares que han estipulado organismos especializados tanto nacionales como internacionales, algunas características a considerar para solidificar estas propuestas son, por ejemplo:

- Delimitar el alcance, metas y objetivos de las políticas.

  Hay que ser claro hasta donde es competente la política cual es su nivel de acción, definir puntualmente que se quiere lograr con cada una de ellas, desde cada perspectiva por ejemplo: uso de herramientas, acciones, estado normal, estado de reacción etc.

- Descripción clara y concisa de sus requerimientos, sanciones y difusión entre los competentes a las mismas.

  Definir quienes serán los afectados o protegidos por la política o conjunto de políticas dependiendo el nivel de acción.

- Delimitar las responsabilidades de cada servicio y recurso hacia todos los niveles de competencia de la red.

  Definir hasta donde un actor o integrante de la política es responsable del entorno. Incluso ir creciendo de manera gradual es conveniente por ejemplo individual, por entorno, por grupo o departamento según sea requerido.

- Personal de contacto y responsable, manejo de riesgos y respuesta ante contingencias.

  Ya que hay improvistos bajo cualquier escenario, se debe contar con un plan de acción inmediata ante alguna contingencia o anomalía, para evitar pérdidas de cualquier tipo, hardware o datos, a continuación se describen algunas consideraciones a seguir:

- ✓ Las políticas ante este tipo de situaciones garantizarán que el sistema funcione adecuadamente ante algún suceso inesperado.

- ✓ Las políticas deben ya estar implementadas, planeadas.

- ✓ Debe haber un monitoreo constante ante las debilidades de la empresa que pueda adelantarse y el suceso no llegue a presentarse. O en su defecto que no pase desapercibido y se pueda actuar.

- ✓ Acción inmediata para mitigar efectos negativos.

- ✓ Comunicación. Para dar difusión del estado de alarma y los involucrados tomen su papel de acuerdo con las políticas.

- ✓ Análisis detallado de la situación. Proporcionara las respuestas y bases para que esta acción no sea tan fuerte o no pase.

- ✓ Recuperación. Si es que hubo alguna pérdida ante la contingencia.

- ✓ Reacción y aprendizaje. Es el punto de documentación. Así entrara en la política de contingencia y será mitigada de forma precisa y segura.

- Seguridad física de la red.

  Las medidas de seguridad física deben proporcionar la protección y el acceso a los activos físicos de la empresa (por ejemplo, servidores y aplicaciones). El documento sobre seguridad física debe describir cómo deben ser protegidos los distintos activos (tales como cuartos cerrados de servidor, lectores de tarjetas de acceso limitado, o sistemas de registro para rastrear quién tiene acceso a cada tipo de servidor).

Las políticas que puedan crearse al igual que en las etapas anteriores necesitan ser de manera granular, no dar por general todo porque dentro del sistema de red, hay diferentes expectativas y necesidades por ello, hay políticas para usuarios, para tecnologías de información, para externos, etc. Este proceso es dinámico, no se puede dejar sin actualizar, menos sin monitoreo que arroja los resultados de las implementaciones

2.4.4. Implementación de políticas.

Los tipos de políticas que se han ideado ahora, deben ser implementadas para que las mejoras no queden solo en planeación y entren en un plan de acción, en esta etapa que hay cierto tipo de políticas que son inherentes a los modelos específicos de calidad. Y siguiendo lo ideado en la etapa anterior, se implementará una solución del tipo token-bucket (bote de fichas), que es un algoritmo de control de congestión basado en el captado de tráfico. Es de tipo bucle abierto, lo que significa que previene la congestión (no reacciona cuando ya se ha producido, sino que previene que no se produzca), y lo hace captando el tráfico que entra a la red para que ésta lo pueda diferenciar. Otra solución podría ser la implementación de un agente tipo un bandwidth broker este agente gestiona el uso de la red. Mediante los informes de uso del ancho de banda que le envían periódicamente los ruteadores y conociendo los recurso de la red y los usuarios registrados, su algoritmo de control adaptativo permite reestructurar todos los flujos de usuarios mediante el control de las colas en los ruteadores. Muy aparte de las demás planes de políticas que se han ideado.

Hablando de estas últimas, hay diferentes aspectos que se deben considerar como puntos en contra en la implementación, se puede hablar de que no deben usarse demasiados tecnicismos para que puedan entenderlos los involucrados, y por otro lado, las soluciones primero mencionadas tienen sus propios inconvenientes, si es que no hay una estrategia adecuada en la muestra de beneficios de la aplicación y adquisición de tecnología.

Las políticas que se pretenden implementar deben contar con un nivel conciso de restricción, deben tener la capacidad de ser adaptativas y en la medida de lo posible inteligentes para que a partir de ellas se puedan tomar decisiones. Incluso sería lo ideal contaran con un nivel alto de heurística.

La propuesta de aspectos en los que se deben formular políticas son:

- Políticas de calidad de los servicios.

  Las políticas de calidad de los servicios son aquellas que basadas en los requerimientos específicos actúan para brindarle a cada servicio los recursos que necesitan. Toman en cuenta las métricas y el diseño del modelo a cumplir. Entonces este tipo de política le asegurara a cada usuario que podrá usar un servicio en un momento específico. Preferentemente cuando lo solicite y sino gestionará los dispositivos para que pueda acceder y hacer uso de la red.

- Políticas de acceso.

Las políticas de acceso responden perfectamente a la necesidad de control, bajo muchos sentidos los usuarios estarán monitoreados y en base a estas políticas se pude dar autorización para que sean manipulados muchos servicios, o tiempos de acceso etc.

La manera más fácil es autenticar al usuario por medio de credenciales, ponerlos en listas negras o blancas. Credenciales que los usuarios conocen o que son datos inherentes a ellos.

Cuando un usuario ya esta autenticado el sistema de red, se puede hacer un registro de lo que hace dentro del sistema, historial de navegación, correos, uso de red etc.

- Políticas de seguridad.

  Las políticas de seguridad por lo general no son solo pocas líneas, son un conjunto conglomerado acerca de diferentes áreas del sistema de red. Uso de las componentes que lo integran formas en que los usuarios se identifican en la red, políticas de navegación web por ejemplo. Si hay usuarios locales internos o externos. Etc.

  De igual manera que todas las políticas deben ser viables, sostenibles y con facilidad en su implementación.

2.4.5. Análisis de resultados.

Una vez en esta etapa del modelo prácticamente se tiene realizado todo el proceso de implantación, un reconocimiento puntual de los componentes y usos de la red. Sus servicios brindados, una ingeniería de tráfico hecho a la medida del sistema etc.

Se conocen también las métricas, recomendaciones y normas de los organismos internacionales ejemplos de estas se han mencionado las recomendaciones de la serie Y emitida por la **ITU**.

Por último las políticas que se han generado, tomando en cuenta puntos y factores clave a lo largo del estudio de red. Que están basadas en recomendaciones de los organismos reguladores internacionales, y que tienen adaptaciones a lo que al caso concreto conviene más, después de la evaluación y resultados obtenidos a través de las pruebas e implementaciones.

El punto fuerte de esta etapa se centra precisamente en hacer una comparación entre estas caracterizaciones. Estudiarlas a fondo para concluir el mejor resultado a arrojar. Ya sea un veredicto de que todo resulto de manera positiva. Que hay que reestructurar alguna etapa para llegar a la optimización, o que hay que dar vuelta atrás.

En cualquiera de los casos será una decisión basada y fundamentada en lineamientos, mediciones y estudios de calidad.

2.4.6. Conclusiones.

Lo que se pueda decir sobre resultados finales será basado en el análisis de todas las etapas anteriores, en los resultados de todas las mediciones y estudios realizados. Se podrá concluir que se asegura la calidad en los servicios bajo circunstancias específicas, que hacer para evitar contingencias y congestiones, las jerarquías y niveles de cada perfil de servicio y usuario, y en su forma más básica de flujo de tráfico de paquetes. Se podrán dar los parámetros a seguir para implementar el modelo que ya en funcionamiento se convertirá en una arquitectura robusta de calidad.

Algunas consideraciones finales se pueden dar sabiendo y redundando en el entendido que la arquitectura final es un conjunto de técnicas y estudios basados en medios y equipos físicos de la red equipo tecnológico usado para interconexión y comunicación de la misma, tal como cables, switches, ruteadores, nodos, terminales de usuario final etc.

Medios y métodos lógicos basados en software, tal como mecanismos de medición, y procesamiento de datos, monitoreo de red, de protocolos etc.

En este punto es cuando salta a la vista el concepto entre modelo, que es la solución echa en base a los estudios y pruebas sobre la red. Y una arquitectura que es la parte de implantación del modelo en un caso de estudio particular para probar y corroborar los resultados obtenidos y los supuestos hechos en el modelo. Normalmente la arquitectura se deja funcionando por tiempo indefinido mientras siga haciendo aportes y dando beneficios a la red. Aunque requira de ajustes siempre y cuando cumpla los objetivos no hay necesidad de recurrir a un nuevo modelo.

Y por ultimo una hibridación entre los dos más básicos que podría ser un agente dotado de algoritmos de decisión, inteligencia artificial y heurística. Que se capaz de interactuar con el hardware de red, el software y en base a todos

los datos recolectados pueda tomar decisiones, incluso adelantarse a problemas que puedan surgir e implementar mecanismos para que estos sean amortizados de manera automática, temprana y eficaz.

De igual manera se deben saber y tomar en cuenta otros aspectos de la red tal como su tecnología de interconexión, topología, metodología y algoritmos de comunicación y complejidad. En el caso que tenga detección de errores, de colisiones, de pérdida de datos etc.

Referencias:

[1] Implementing service quality in ip networks. Vilho Raisamen. Editorial Wiley. ISBN 0-470-84793-X. Año de publicación 2003.

[2] Technical, commercial and regulatory challenges of QoS an internet service model perspective. Xipeng Xiao. Editorial Morgan Kauffman. ISBN: 978-0-12-373693-2. Año de publicación 2008.

[3] Network Quality of Service Know It All. *Volume Editor: Adrian Farrel. Editorial Morgan Kauffam. ISBN 978-0-12-374597-2. Año de publicación 2009.*

CAPÍTULO III.

Capitulo 3. Arquitectura de Calidad.

RESUMEN:

En este capítulo se hace la descripción general de cómo está integrado el sistema de red institucional. Comenzando desde lo general a lo puntual en la red donde se hace la implementación del modelo. Se hace la caracterización del modelo en dos fases describiendo en este capítulo la primera que abarca las capas de topología de red e ingeniería de tráfico pertenecientes a la propuesta de solución del modelo de calidad.

OBJETIVOS DEL CAPITULO:

- Mostrar el estado de la red en donde se va a implementar el modelo.
- Mostrar el detalle de la propuesta del nuevo modelo de calidad, implementándolo en un segmento real del sistema de red.

En el capitulo anterior se ha descrito la propuesta de solución a la necesidad de calidad de los servicios sobre una red convergente desplegada en un ambiente educativo en base de un modelo, lo que ha quedado descrito es el panorama general y en algunos cosas el ideal en la toma de decisiones, algunas ideas de lo que se propone considera para fortalecer la implementación del modelo de calidad. en este capítulo se describirá el proceso de implantación sobre el segmento de red real donde fue implementado el modelo para poder probar sus características y así definir su funcionalidad y operación, la red utilizada para tal fin, fue la red del Centro de Formación e Innovación Educativa del IPN (CFIE-IPN).

3.1 Implementación del modelo en la red de CFIE.

En la actualidad existe gran demanda de servicios educativos, para los catedráticos se requiere una actualización y para los alumnos una mayor oferta. En conjunto el sistema debe ofrece un despliegue tecnológico de punta.

El Instituto Politécnico Nacional atreves del CFIE está ofreciendo distintos programas de actualización para toda la comunidad docente que pertenece al IPN, se oferta actualización docente en línea y presencial para la comunidad local, nacional e internacional.

Cuenta además con la versatilidad de un ambiente educativo, tiene componentes heterogéneos, ya que dentro del edificio donde se localiza el CFIE se realizan múltiples actividades que hacen uso y demandan servicios.

Hay usuarios de personal administrativo, se encuentran también profesores investigadores y hay usuarios esporádicos a los que se les debe brindar conectividad. Por ejemplo los usuarios que asisten a algunas actividades como son foros, congresos o diplomados, ferias y exposiciones etc.

Se ha decidido implementar este modelo en el segmento de red del CFIE, ya que el centro cuenta con un amplio despliegue tecnológico, una red convergente y múltiples servicios ofrecidos en ella.

Es interesante la implementación del modelo para probar su flexibilidad ya que en el CFIE hay diferentes servicios desplegados, diferentes necesidades de servicio y diferentes equipos tecnológicos, haciendo esto notorio en la arquitectura de los nodos desde los que acceden los usuarios, mencionando arquitectura física, los sistemas operativos y firmware de los equipos, protocolos de todo el modelo de comunicaciones, software de aplicación etc.

Es por eso que el ambiente educativo es ideal para el estudio, en especial este segmento por los servicios que maneja su red convergente, video vigilancia, video conferencia, VoIP, navegación WEB, correo electrónico etc.

3.2. Descripción de la Red.

El sistema de red institucional que está desplegado para darle servicio a los diferentes usuarios dentro del Instituto Politécnico Nacional, tiene contemplados a mas de 18,000 equipos de cómputo conectados al sistema de red, el backbone está integrado por tres nodos principales: Zacatenco, Santo Tomás y UPIICSA; por medio de enlaces de fibra óptica monomodo con ancho de banda de 12 Gbps entre cada uno de ellos y conexiones a Internet e Internet2 con un ancho de banda de E3 (34 Mbps) (figura 3.1).

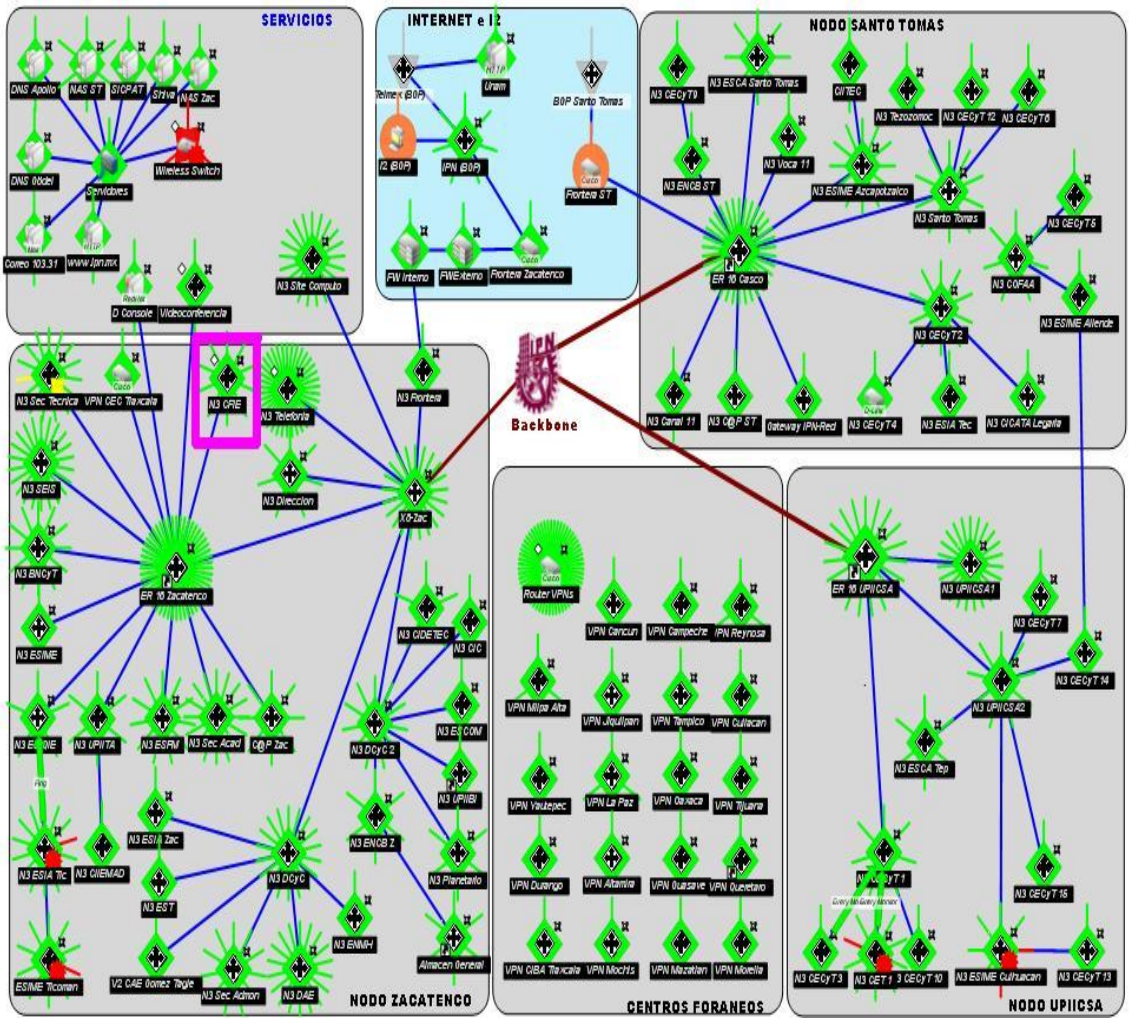


Figura 3.1 Red Institucional IPN.

El nodo de interés para este trabajo es el nodo zacatenco ya que es el que sirve de conexión al Centro de Formación e Innovación Educativa (CFIE), dicho nodo es considerado el más importante del backbone, abarca la Unidad Profesional “Adolfo López Mateos” (UPALM) y la Unidad Profesional Ticomán (UPT), a través del nodo zacatenco se logra la conexión a Internet e Internet 2, así como a los servidores de correo electrónico, los servidores DNS’s (Domain Name Service), los servidores de almacenaje (NAS), entre otros. Ahí se encuentran los enlaces satelitales, que se encargan de servirle conexión de red a los 16 centros foráneos que tiene el IPN; los enlaces de fibra óptica y cables de cobre a 40 diferentes centros cercanos a éste nodo; también se encuentran enlaces por microondas hacia UPIICSA, Santo Tomás y UPIITA. En este nodo se encuentra uno de los anillos FDDI que actualmente operan en la red del IPN, a este anillo están conectados directamente: el Centro de Investigación en Computación, la Biblioteca Nacional de Ciencia y Tecnología, ESIME Zacatenco, ESFM, ENMH y ESIA Ticomán. Figura 3.2

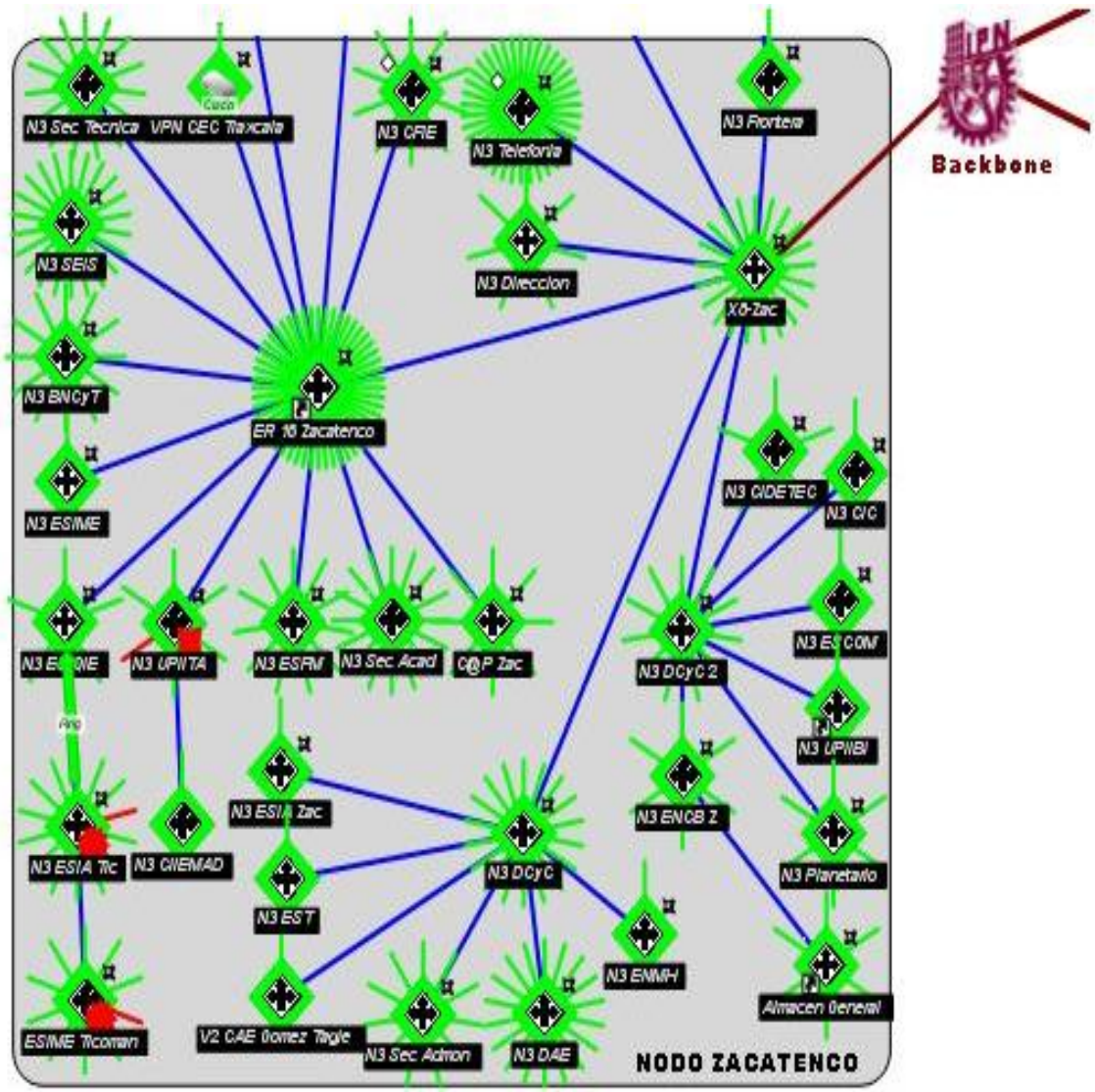


Figura 3.2 Nodo Zacatenco. Red Institucional IPN.

La red del Centro de Formación e Innovación Educativa (CFIE), depende directamente del centro de cómputo y comunicaciones del instituto politécnico nacional. Dado que el nodo ER 16 zacatenco del que recibe conexión, se encuentra físicamente dentro del edificio del centro de cómputo y comunicaciones. Figura 3.3

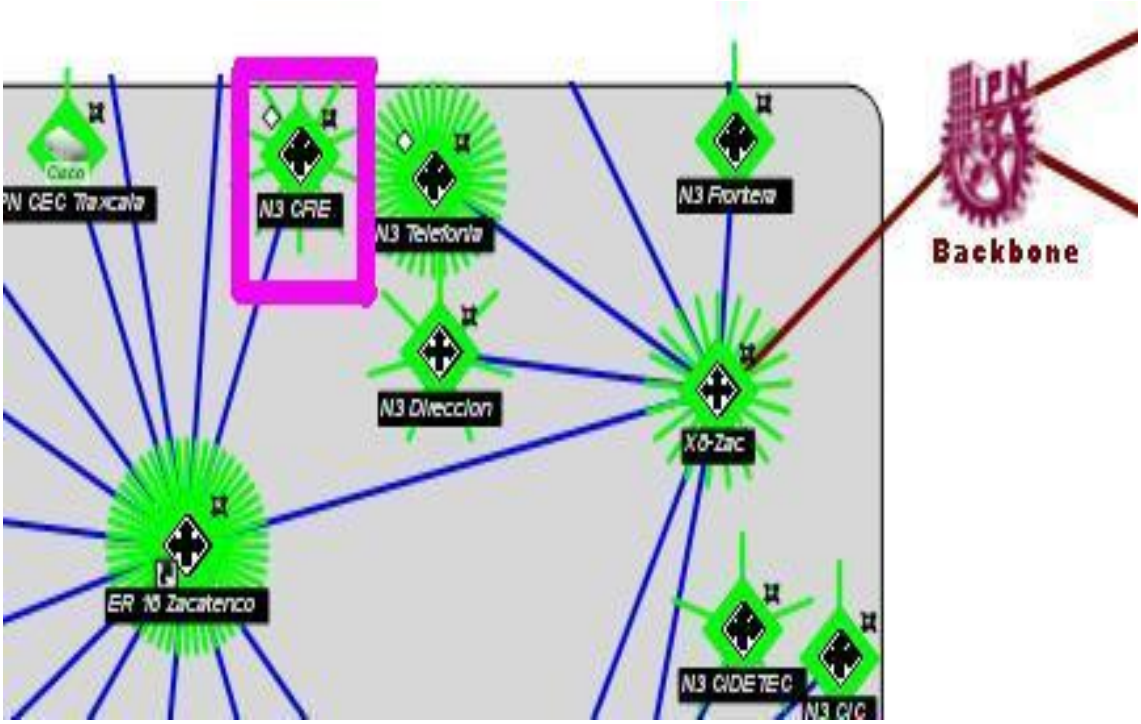


Figura 3.3. CFIE, dentro del nodo Zacatenco. Red Institucional IPN.

Cuenta con una conexión de ancho de banda T1. El enlace desde el centro de cómputo y telecomunicaciones se hace mediante fibra óptica. El site principal que tiene el centro consta de 5 switches Enterays serie A modelo 2H124 de 24 puertos cada uno. Un servidor unificado de mensajes Avaya modelo S8300, un Enterasys N3 y un Enterasys Matrix 1G modelo 582-09. El centro cuenta con otros 2 pequeños servidores espejo y de distribución como se puede observar en la figura 3.4.

Dentro del mismo site principal se encuentran los enlaces puente de red hacia la Unidad Politécnica de Desarrollo y Competitividad Empresarial, Unidad Politécnica de Educación Virtual, Centro de Lenguas Extranjeras. Todos ellos dependientes del Politécnico Nacional.

Al interior del CFIE se encuentran los equipos de cómputo tal como se enlistan a continuación.

- 39 computadoras basadas en arquitectura X-86 con procesadores core 2 duo E4500, 160 Gb en HD, memoria ram de 1Gb DDR2.

- 59 computadoras basadas en arquitectura X-86 con procesadores Pentium 4 a una velocidad de 800GHz, 1Mb de cache, 80Gb en HD, memoria ram desde los 256 Mb hasta 2Gb DDR2.

- 14 computadoras basadas en arquitectura X-86 con procesadores Pentium Dual Core E2200, 160 Gb en HD, memoria ram de 2Gb DDR2.

- 5 computadoras basadas en arquitectura powerPC con procesadores powerMAC G5, 160Gb en HD, memoria RAM de 1Gb SDRAM DDR2.

Los sistemas de impresión con los que cuenta el centro son los siguientes equipos:

- 3 impresoras Xerox de la serie Phaser dos de ellas conectadas en red.

- 3 impresoras Dell modelo 1720dn, una de ellas conectada en red.

- 4 impresoras Epson modelo stylus 2200.

- 14 impresoras HP modelos diferentes, cuatro de ellas conectadas en red.

Los equipos que integran el sistema de seguridad y video conferencia son los que se mencionan a continuación:

- 13 cámaras de seguridad marca Axis. Todas ellas conectadas en red.

- 3 cámaras de video conferencia marca Axis conectadas en red.

- 2 módulos de audio marca Axis.

El sistema de telecomunicaciones está conformado por los siguientes equipos:

- 20 switches de la marca enterasys modelo V2H124-24.

La conexión telefónica es por medio de Telefonía IP y los equipos que componen este sistema son:

- 86 teléfonos IP Avaya modelos 4602 sw + IP. Y 4610 SW IP.

En total se cuentan con 262 nodos de red que componen todo el sistema de CFIE interactuando diariamente entre ellos. Como nota adicional este centro atiende algunos cursos y congresos los cuales requieren de servicios de

conexión y en estas ocasiones puede elevarse el número de usuarios registrados, el consumo habitual de ancho de banda y el uso de los servicios que el sistema de red ofrece a sus usuarios.

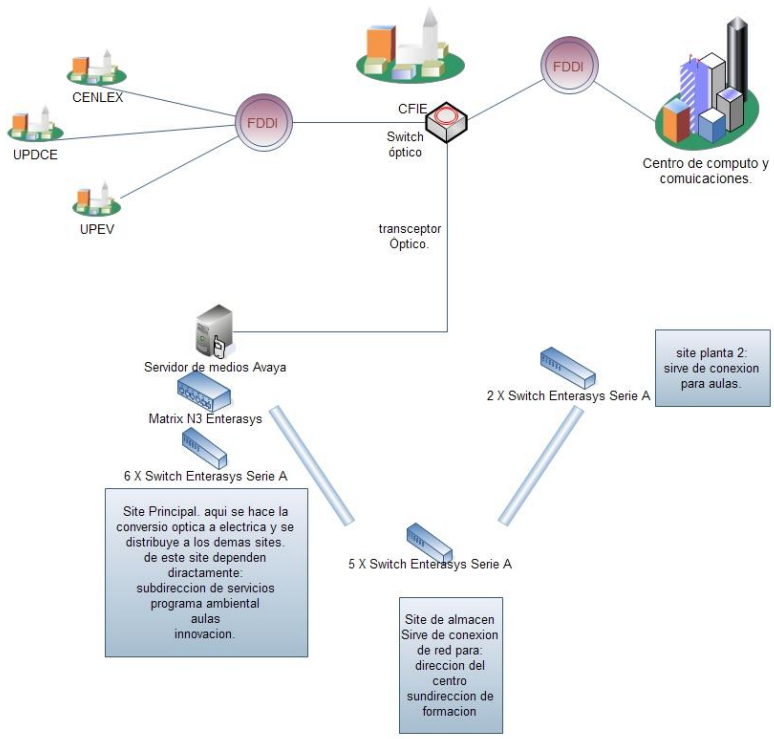


Figura 3.4. Sistema de Red CFIE.

A continuación se hace una descripción general de las capacidades tecnológicas de los principales equipos que conforman el sistema de red.

1. Switch Enterasys N3.

   Flexible para redes Voz, vídeo y datos (Redes Convergentes). Soporta servicios como Voz sobre IP (VoIP), alimentación eléctrica sobre Ethernet (Power-over-Ethernet), servicios broadcast y multicast de video.

   Proporciona seguridad avanzada mediante la prioridad de flujos y mecanismos de control de ancho de banda. Esto sin comprometer el rendimiento de la red. Tiene capacidad de manejar políticas avanzadas basada en el control de flujo y acceso.

   - Políticas de autenticación multi usuario.
   - Clasificación dinámica de paquetes basados en flujo.
   - Capacidades para asegurar QoS

- ✓ Mapeo de prioridad de colas (802.1p & IP ToS/ DSCP) con arriba de 16 colas por puerto.

- ✓ Limitación de tráfico por puerto o por usuario.

- ✓ Tasa QoS controlable jerarquización

Compatible con estándares y protocolos importantes como son:

- Servicios de conmutación y Vlan: soporta protocolo802.1p, VLAN 802.1Q, soporta puentes MAC 802.1D, Ethernet 802.3, Gigabit Ethernet 802.3ab, Control de flujo 802.3x, Gigabit Ethernet (fibra) 802.3z, Multicast IP (IGMP v1, v2, por VLAN), GVRP (Generic VLAN Registration Protocol).

- Ruteo IP.: Ruteo General RFC 1812, RFC 792 ICMP, Protocolo de descubrimiento de rutas RFC 1256 ICMP, RFC 826 ARP, RFC 1027 Proxy ARP, Rutas Estaticas, RFC 1058 RIPv1, RFC 1723 RIPv2 con balanceo de cargas de igual volumen, RFC 1812 RIP, RFC 1519 CIDR, Protocolo de redundancia virtual de ruteo RFC 2338 VRRP, Estándar ACL, Servidor DHCP RFC 1541/ Retardo RFC 2131.

- Seguridad de red y Manejo de políticas: Autenticación basada en puertos 802.1X, Múltiples tipos de autenticación por puerto (simultáneamente) (802.1x, MAC, PWA+), Múltiples usuarios autenticados por puertos, con políticas únicas por usuario y sistema (Asociación independiente por cada VLAN), RADIUS RFC 3580 **IEEE** 802.1, con políticas VLAN hacia Mapeo de políticas y Asignación de VLAN vía autenticación.

- Clasificación de servicios: Trato estricto en la prioridad de colas, Transmisión de 4 colas por puerto (10/100/1000), Contador de paquetes o limitaciones de ancho de banda basado en tasas de transmisión, Marcado y remarcado IP ToS/DSCP, Mapeo para transmitir alguna cola con prioridad 802.1D.

- Manejo control y análisis: SNMP v1/v2c/v3, manejo Web basado en interfaz, servidor y cliente Telnet, Shell segura (SSHv2), Protocolo de descubrimiento Cabletron, Protocolo de descubrimiento Cisco v1/v2, **IEEE** 802.1AB LLDP, TIA/ANSI 1057 LLDP-MED, Syslog, cliente FTP, Protocolo simple de tiempo de red (Simple Network Time Protocol-SNTP), Netflow versión 5 y versión 9, Autorizacion VLAN RFC 3580, RFC 2865 RADIUS.

- Protección contra ataques de negación de servicio. (DDoS): Escaneo de puertos TCP/UDP, Ataques de árbol de navidad (Christmas Tree Attack), ataque Fraggle, Fragmentación y alargamiento ICMP, inundación ICMP, ataques de invalidación ICMP, ataque de redireccionamiento ICMP, ataques LANd.

Entre una serie de características más, que lo hace un equipo potente y versátil para el manejo del tráfico que se genera dentro del CFIE.

	N3
DFE Module Slots	3
Switching Throughput	40.5 Mpps
Total Backplane Capacity	240 Gbps
10/100 ports per system	216
100 Base-FX ports per system	162
10/100/1000 ports per system	216
10/100/1000 PoE ports per system	144
1000 Base-X ports per system	72
10 Gigabit ports per system	12

Figura 3.5 Tabla de características generales de Switch Enterasys N3.

Figura 3.6 Switch Enterasys N3.

En la Figura 3.7. Siguiente, se puede apreciar el detalle de la configuración lógica del equipo principal que reparte los servicios de conexión al interior del centro.

Figura 3.7. Vista de configuración N3 CFIE.

2. Los switches de la serie A con los que cuenta el centro, al ser de la misma compañía tecnológica son 100% compatibles con los equipos anteriormente descritos, estos switches proporcionan características similares y apoyo completo en el aseguramiento de calidad sobre la red. Se Basan en la diferenciación de hasta 8 colas por cada puerto Ethernet con múltiples niveles de prioridades diferentes.

   Según se ha visto en las visitas al site de comunicaciones, el monitoreo y pruebas realizadas en el segmento de red, el enlace desde el centro de computo y comunicaciones llega directamente al switch N3, y los diferentes switches de la serie A se encargan de distribuir las conexiones dentro del sistema de red de CFIE.

   Tiene mucha similitud en cuanto a la compatibilidad de protocolos y servicios que ofrece el Enterasys N3.

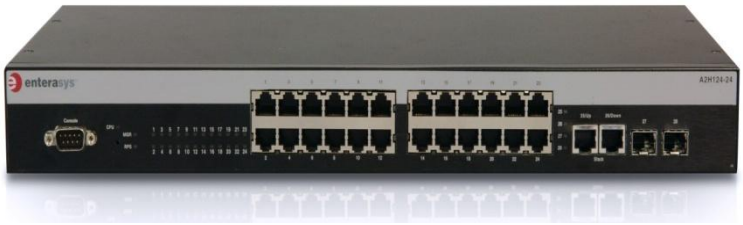


Figura 3.8. Switch Enterasys Serie A.

3. Enterasys Matrix 1G 582-09.

   Manejo de calidad sobre la capa dos (capa de enlace del modelo OSI), puede asignar clases de tráfico basado en el estándar 802. Diferenciando cada puerto y la mayoría de los parámetros contenidos en las capas 2 - 4, incluyendo la dirección IP de la subred y el número de socket TCP o UDP.

   Puede hacer el manejo y administración de ancho de banda, para que el administrador pueda cumplir con los requisitos básicos de los servicios.

   - Soporte para el estándar 802.1p.
   - 4 colas por Puerto.
   - Soporta DiffServ.
   - Limita la tasa de transferencia basado en hardware.

Al igual que los dos anteriores es de la marca Enterasys. Y tiene compatibilidad con ellos, con casi todos los estándares que los anteriores.

Figura 3.9. Matrix 1G582-09 Enterasys.

4. Servidor de medios Avaya S8300.

En complemento con los equipos anteriores, la red la compone también un servidor de medios Avaya S8300. Es el que da servicio a toda la comunicación de VoIP. Tiene capacidad para 450 host.

Puede manejarse como estación para servicio local o conexión remota.

- Integración con VBX.
- Servicio de correo de voz.
- Tiene soporte a estándares como: TAPIA, ISAPI, ETAPA, CAPI, ASIA, LDA., H.323, PSIG, H.450 y H.248.
- Usa cableado Ethernet CAT 5. Esta configuración permite aprovechar los beneficios de la arquitectura distribuida del concepto de pasarela de medios y ofrece una capacidad de supervivencia, basada en estándares, infraestructura de comunicaciones IP, sin comprometer las aplicaciones, confiabilidad, y la creación de redes multiservicio. La solución es escalable, modular, cuenta arquitecturas redundantes.
- Capacidad de escalabilidad.

- Mensajería integrada.

Figura 3.10. Avaya servidor de medios.

3.3. Descripción del proceso de implantación del modelo.

La implantación del modelo Figura 3.11. Que se ha hecho sobre la red del CFIE, después de implementar al menos un ciclo ha dado como resultado una arquitectura, realizar el estudio para saber cómo se comportará, si gana eficiencia o si asegura calidad en el desempeño de la red se hace en base a todos los análisis y se vierte en el apartado de conclusiones.

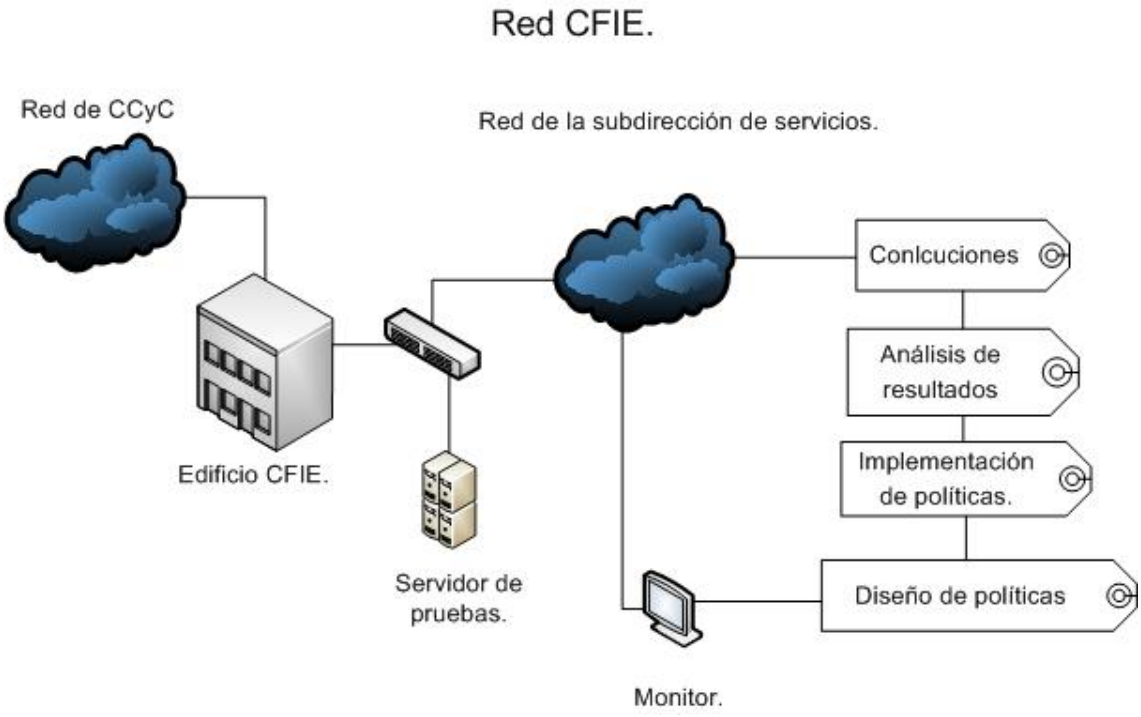


Figura 3.11. Estado de la arquitectura después de implementar el modelo calidad en la red.

En la Figura 3.11 se puede observar como quedo implantado el modelo (Después de implantarlo un ciclo, es una arquitectura). Se nota como llega la conexión desde el Centro de Cómputo y Comunicaciones, entra al edificio de CFIE. En esta sección es donde se comienza a distribuir la conexión a los segmentos entre ellos la subdirección de servicios lugar específico donde se ha implementado el modelo. Justo en el switch que da servicio al segmento, se ha colocado el servidor de pruebas PFsense, después, se ha colocado un monitor dedicado desde ahí se monitorea el segmento de la red de servicios, una vez teniendo las herramientas se procede con el diagrama de flujo que abarca:

- Diseño de políticas.
- Implantación de políticas.
- Análisis de resultados.
- Conclusiones.

Una vez realizado el primer ciclo hay que continuar con el modelo, si se han hecho cambios en la topología, se continuara corroborando desde la primer etapa de reconocimiento de topología, si no se han hecho modificaciones a la topología se podrá avanzar desde la etapa dos que es la ingeniería de tráfico y así sucesivamente.

3.3.1. Topología de red.

La primera etapa se cubrió utilizando el programa de SolarWinds. LAN Surveyor. El cual hace un descubrimiento y mapeo del sistema de red, haciendo uso de la familia de protocolos TCP y UDP.

- SNMP: por defecto en el puerto UDP 161.
- Ping: por defecto en el puerto ICMP.
- Respuestas de Clientes: por defecto en el puerto UDP 4347.
- Clientes NetBIOS: por defecto en el puerto UDP 137.
- Nodos SIP (VoIP): por defecto en el puerto UDP 5060.

- Clientes en Retrospectiva (historial de re conexión): por defecto apagado en el puerto UDP 497.

Esta herramienta se basa en las recomendaciones:

- RFC 1213.
- RFC 1493.
- RFC 2108.
- RFC 2674.

Durante el descubrimiento de la topología del sistema de red, **LANsurveyor** utiliza una cantidad muy pequeña del ancho de banda de red. Para cada tipo de método de descubrimiento (ICMP Ping, NetBIOS, SIP, etc.), **LANsurveyor** envía una pequeña cantidad de paquetes UDP por dirección IP (<300 bytes). Además, **LANsurveyor** divide grandes rangos de direcciones IP en bloques de 10 direcciones y espera unos segundos para las respuestas de las 10 direcciones. Buscando en la red de esta forma, **LANsurveyor** no debe tener ningún efecto negativo notable en el ancho de banda de red o dispositivos.

Estas son las generalidades de la herramienta usada, además tiene otras características que la hacen una buena opción. Tal como la exportación del diagrama a un documento PDF o Microsoft Visio.

Aunque el programa tiene el uso con pago de licencia, la versión demo sirve muy bien si solo se quiere hacer un primer descubrimiento y no depender de él para hacer un inventario.

A continuación se muestra el mapa que arrojo tras el descubrimiento de la red Figura 3.12. En el rango 148.204.73.0 a 148.204.73.255 perteneciente al rango de red asignado a CFIE.

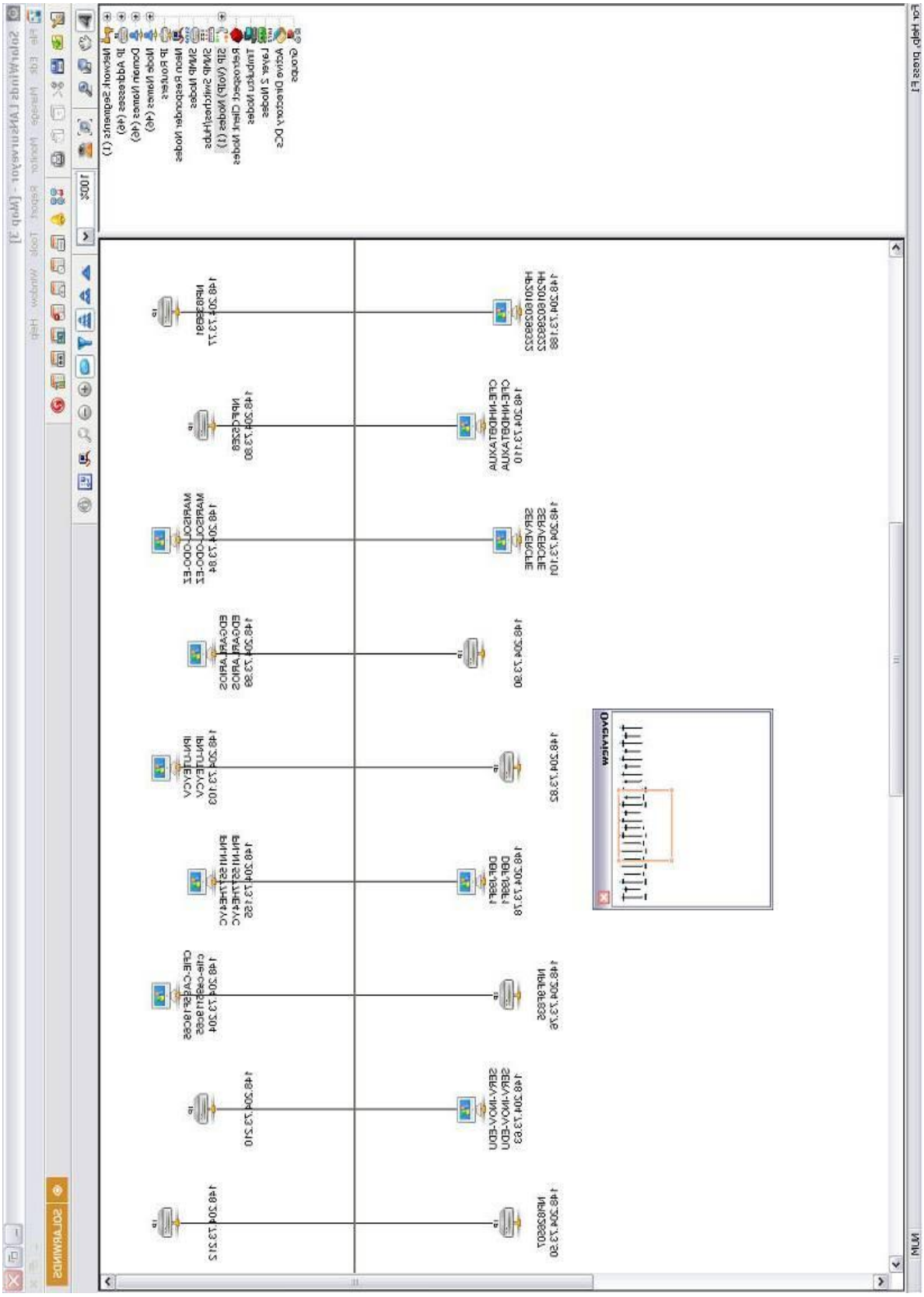
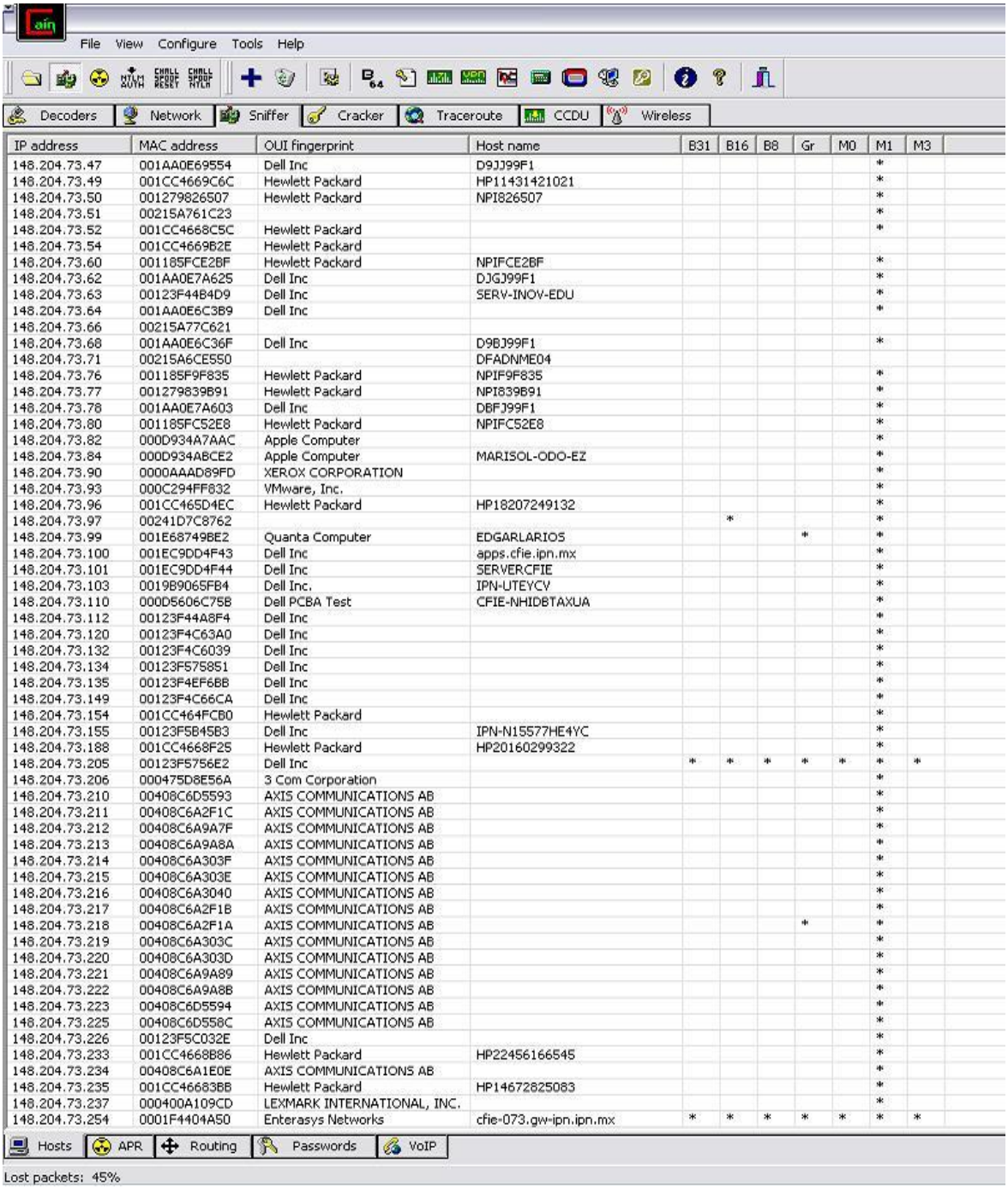


Figura 3.12 Descubrimiento de red con SolarWinds.

La herramienta utilizada para descubrir los nombres asociados a la direcciones de cada host fue **Caín & Abel** de oixit software una opción de software libre, aunque no presenta resultados tan gráficos ni compatibles con otros software comerciales arroja resultados de mas índole y capaz de ser exportado a texto plano.

A manera de confirmación y complemento de la herramienta anterior se ha usado esta, con el siguiente resultado:



IP address	MAC address	OUI fingerprint	Host name	B31	B16	B8	Gr	M0	M1	M3
148.204.73.47	001AA0E69554	Dell Inc	D9JJ99F1						*	
148.204.73.49	001CC4669C6C	Hewlett Packard	HP11431421021						*	
148.204.73.50	001279826507	Hewlett Packard	NPI826507						*	
148.204.73.51	00215A761C23								*	
148.204.73.52	001CC4668C5C	Hewlett Packard							*	
148.204.73.54	001CC4669B2E	Hewlett Packard								
148.204.73.60	001185FCE2BF	Hewlett Packard	NPIFCE2BF						*	
148.204.73.62	001AA0E7A625	Dell Inc	DJGJ99F1						*	
148.204.73.63	00123F44B4D9	Dell Inc	SERV-INOV-EDU						*	
148.204.73.64	001AA0E6C3B9	Dell Inc							*	
148.204.73.66	00215A77C621									
148.204.73.68	001AA0E6C36F	Dell Inc	D9BJ99F1						*	
148.204.73.71	00215A6CE550		DFADNME04							
148.204.73.76	001185F9F835	Hewlett Packard	NPIF9F835						*	
148.204.73.77	001279839B91	Hewlett Packard	NPI839B91						*	
148.204.73.78	001AA0E7A603	Dell Inc	DBFJ99F1						*	
148.204.73.80	001185FC52E8	Hewlett Packard	NPIFC52E8						*	
148.204.73.82	000D934A7AAC	Apple Computer							*	
148.204.73.84	000D934ABCE2	Apple Computer	MARISOL-ODO-EZ						*	
148.204.73.90	0000AAAD89FD	XEROX CORPORATION							*	
148.204.73.93	000C294FF832	VMware, Inc.							*	
148.204.73.96	001CC465D4EC	Hewlett Packard	HP18207249132						*	
148.204.73.97	00241D7C8762				*				*	
148.204.73.99	001E68749BE2	Quanta Computer	EDGARLARIOS				*		*	
148.204.73.100	001EC9DD4F43	Dell Inc	apps.cfie.ipn.mx						*	
148.204.73.101	001EC9DD4F44	Dell Inc	SERVERCFIE						*	
148.204.73.103	0019B9065FB4	Dell Inc.	IPN-UTEYCV						*	
148.204.73.110	000D5606C75B	Dell PCBA Test	CFIE-NHIDBTAXUA						*	
148.204.73.112	00123F44A8F4	Dell Inc							*	
148.204.73.120	00123F4C63A0	Dell Inc							*	
148.204.73.132	00123F4C6039	Dell Inc							*	
148.204.73.134	00123F575851	Dell Inc							*	
148.204.73.135	00123F4EF6BB	Dell Inc							*	
148.204.73.149	00123F4C66CA	Dell Inc							*	
148.204.73.154	001CC464FCB0	Hewlett Packard							*	
148.204.73.155	00123F5B45B3	Dell Inc	IPN-N15577HE4YC						*	
148.204.73.188	001CC4668F25	Hewlett Packard	HP20160299322						*	
148.204.73.205	00123F5756E2	Dell Inc		*	*	*	*	*	*	*
148.204.73.206	000475D8E56A	3 Com Corporation							*	
148.204.73.210	00408C6D5593	AXIS COMMUNICATIONS AB							*	
148.204.73.211	00408C6A2F1C	AXIS COMMUNICATIONS AB							*	
148.204.73.212	00408C6A9A7F	AXIS COMMUNICATIONS AB							*	
148.204.73.213	00408C6A9A8A	AXIS COMMUNICATIONS AB							*	
148.204.73.214	00408C6A303F	AXIS COMMUNICATIONS AB							*	
148.204.73.215	00408C6A303E	AXIS COMMUNICATIONS AB							*	
148.204.73.216	00408C6A3040	AXIS COMMUNICATIONS AB							*	
148.204.73.217	00408C6A2F1B	AXIS COMMUNICATIONS AB							*	
148.204.73.218	00408C6A2F1A	AXIS COMMUNICATIONS AB					*		*	
148.204.73.219	00408C6A303C	AXIS COMMUNICATIONS AB							*	
148.204.73.220	00408C6A303D	AXIS COMMUNICATIONS AB							*	
148.204.73.221	00408C6A9A89	AXIS COMMUNICATIONS AB							*	
148.204.73.222	00408C6A9A8B	AXIS COMMUNICATIONS AB							*	
148.204.73.223	00408C6D5594	AXIS COMMUNICATIONS AB							*	
148.204.73.225	00408C6D558C	AXIS COMMUNICATIONS AB							*	
148.204.73.226	00123F5C032E	Dell Inc							*	
148.204.73.233	001CC4668B86	Hewlett Packard	HP22456166545						*	
148.204.73.234	00408C6A1E0E	AXIS COMMUNICATIONS AB							*	
148.204.73.235	001CC46683BB	Hewlett Packard	HP14672825083						*	
148.204.73.237	000400A109CD	LEXMARK INTERNATIONAL, INC.							*	
148.204.73.254	0001F4404A50	Enterasys Networks	cfie-073.gw-ipn.ipn.mx	*	*	*	*	*	*	*

Figura 3.13 Descubrimiento de red con cain & Abel.

3.3.2 Ingeniería de tráfico.

En la etapa de ingeniería de tráfico se implementó el uso de la herramienta **Ntop** de Luca Deri para hacer la recolección de datos importantes sobre la red.

Ntop muestra el uso en tiempo real del sistema de red. Se enlista la totalidad de los hosts que están utilizando la red y la información relativa a los informes tanto para tráfico IP y tráfico no IP, así como el tráfico generado y recibido por cada host. **Ntop** puede operar como colector de datos final y en tiempo real (Front - End) usando algunos complementos (plug-in) o como un recolector histórico (stand-alone). Se requiere de un navegador web para acceder a la información capturada por el programa de **ntop**.

Ntop es una herramienta de capa híbrida, ya que es capaz de trabajar en la capa 2 / Capa 3 como un monitor de red, es decir, por defecto se usa la capa 2, Media Access Control (MAC) y la capa de 3 direcciones TCP / IP. **Ntop** es capaz de asociar a los dos, de modo que el tráfico IP y el tráfico no IP (por ejemplo, ARP, RARP) se combinan para obtener un reporte detallado y completo de la actividad que hay sobre la red.

Para comprobar y como complemento de los datos que arroja la herramienta **Ntop**. Se ha ocupado también el sistema **Pfsense**, que es un sistema sistema corta fuegos (firewall), basado en en el sistema operativo **Freebsd**. Con todas las características y potencia que este sistema de software libre puede ofrecer.

3.3.2.1 Análisis de de tráfico.

En este apartado se muestran las gráficas desglosadas de acuerdo a diferentes criterios pero todos sobre datos que circulan sobre la red se muestran la información graficando según el parámetro y su forma de medición (b/s, Paquetes/segundo, etc.), conforme del tiempo (en contraste con el tiempo en el que ocurrió el registro).

Adicionalmente cada gráfica define la cantidad máxima, el promedio y la medición actual, de acuerdo con el parámetro estudiado o mostrado en cada caso.

1. Clasificación por tamaño de paquetes.

   La clasificación que se hace en el tamaño de paquetes va desde los 256 paquetes hasta los 1518 paquetes. Son los paquetes que van viajando

sobre el sistema de red, se monitorea en tiempo real y se puede ir haciendo un archivo histórico. Se puede apreciar el calendario de medición caracterizado desde diferentes periodos en el tiempo, se presenta a continuación el análisis diario (distribuido en horas), la distribución semanal y por último la anual. Las gráficas vistas en paquetes/segundos y el contraste con el tiempo de medición.

- Vista Anual.

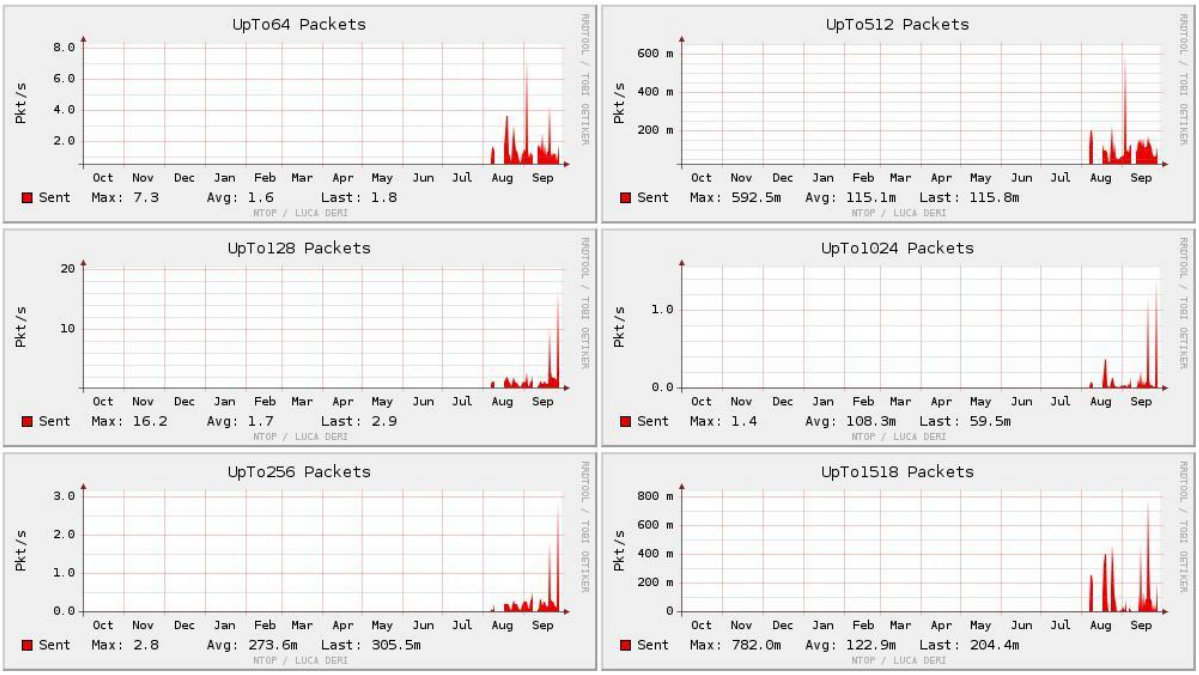


Figura 3.14 Clasificación de paquetes según su tamaño. Vista anual.

2. Clasificación por BroadCast y MultiCast.

   El Broadcast atiende al envío de paquetes que hace un nodo emisor hacia múltiples nodos receptores sobre el sistema de red, y “en un solo camino o canal”, si hacer duplicado de información.

   Multicast es bajo el mismo concepto un envío de paquetes por parte de un nodo emisor hacia múltiples nodos receptores, con la diferencia de que si hay más de un camino o canal en la comunicación realiza duplicidad de datos para enviarlo al canal adicional.

   La gráfica se muestra midiendo paquetes/ segundo y el contraste con el tiempo de medición.

- Vista Anual.

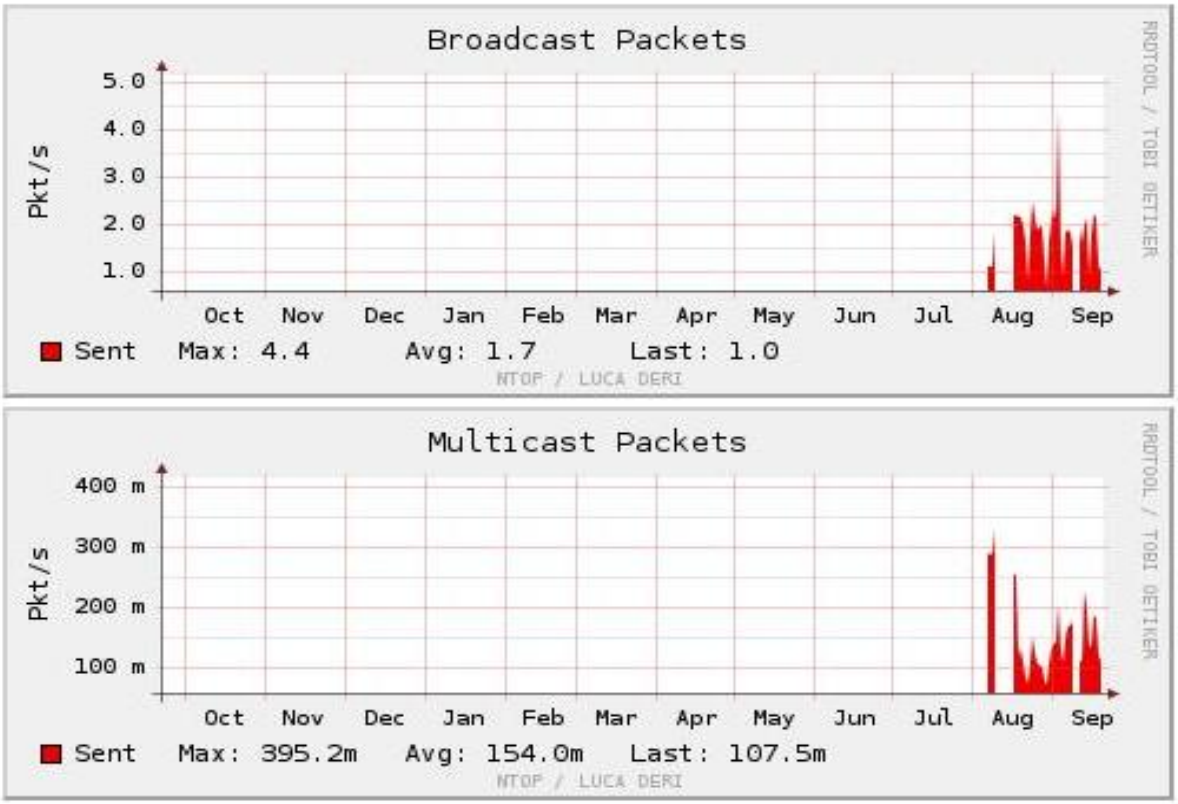


Figura 3.15 Clasificación de paquetes Broadcast/Multicast. Vista anual.

3. Tipos de flujo.

   Este apartado tiene una gran importancia ya que con él se observa el desglose de los flujos que transitan en la red, flujos HTTP, SNMP, etc. Atendiendo a los diferentes servicios que despliega la red, y que generan tráfico sobre ella.

   Haciendo el análisis pertinente se puede dar solución a algunos problemas de tráfico, incluso priorizar algún tipo de flujo etc.

   Las gráficas mostradas en flujos/ segundo y el contraste con el tiempo de medición.

- Vista Anual.

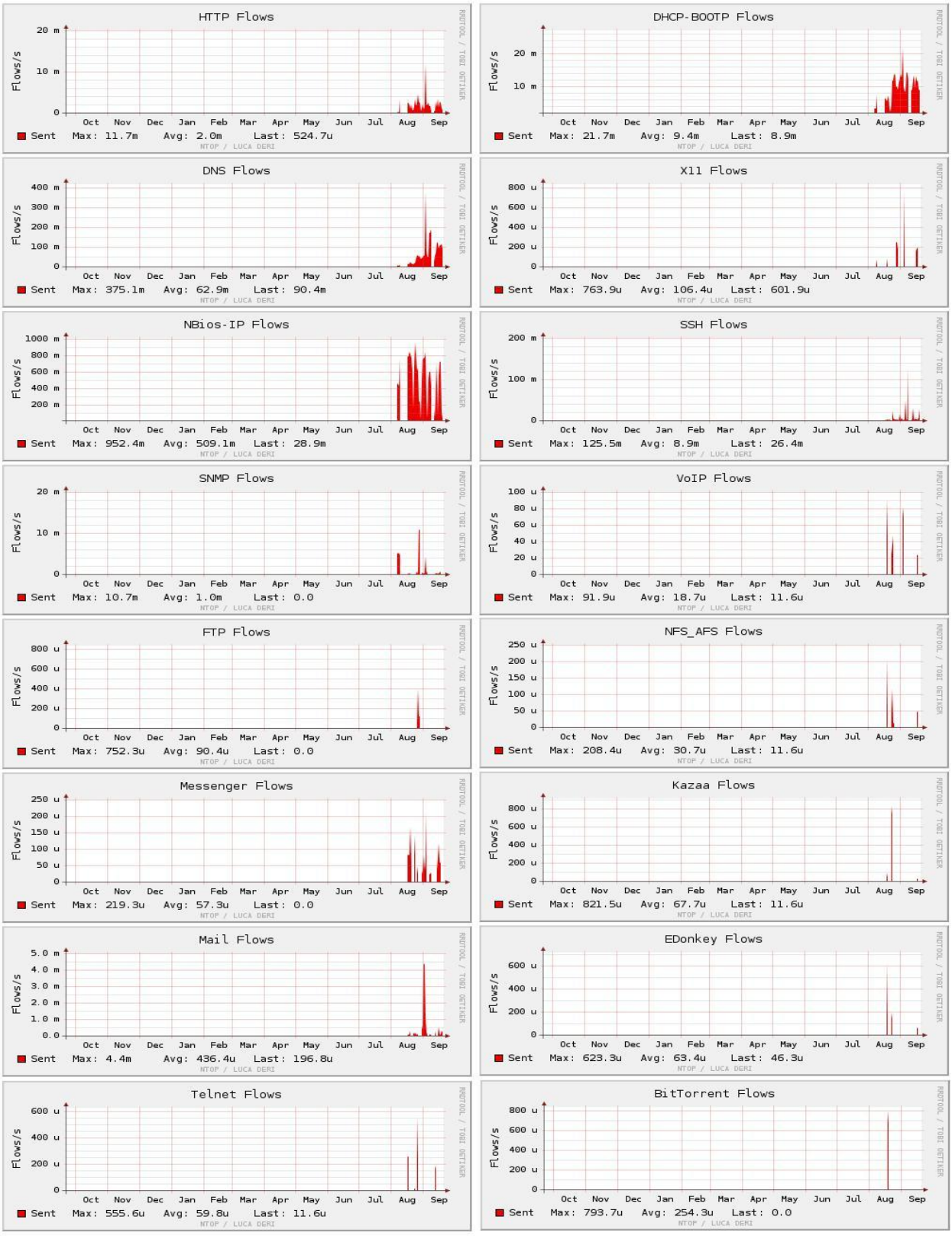


Figura 3.16 Clasificación flujos. Vista anual.

4. Volumen de tráfico.

   En este apartado hay puntos interesantes también, expuestos al análisis puntual. Por ejemplo se muestra el tráfico Ethernet (*estándar **IEEE 802.3***) y algunos otros enfoques como son el del volumen de tráfico generado por el servicio HTTP, ahora medidos en bits/segundo.

   También se nota la dirección del flujo, si es local – local, Remoto – local etc.

   Las gráficas se presentan en bits/segundo y el contraste el tiempo en que se realizo la medición.

- Vista Anual.

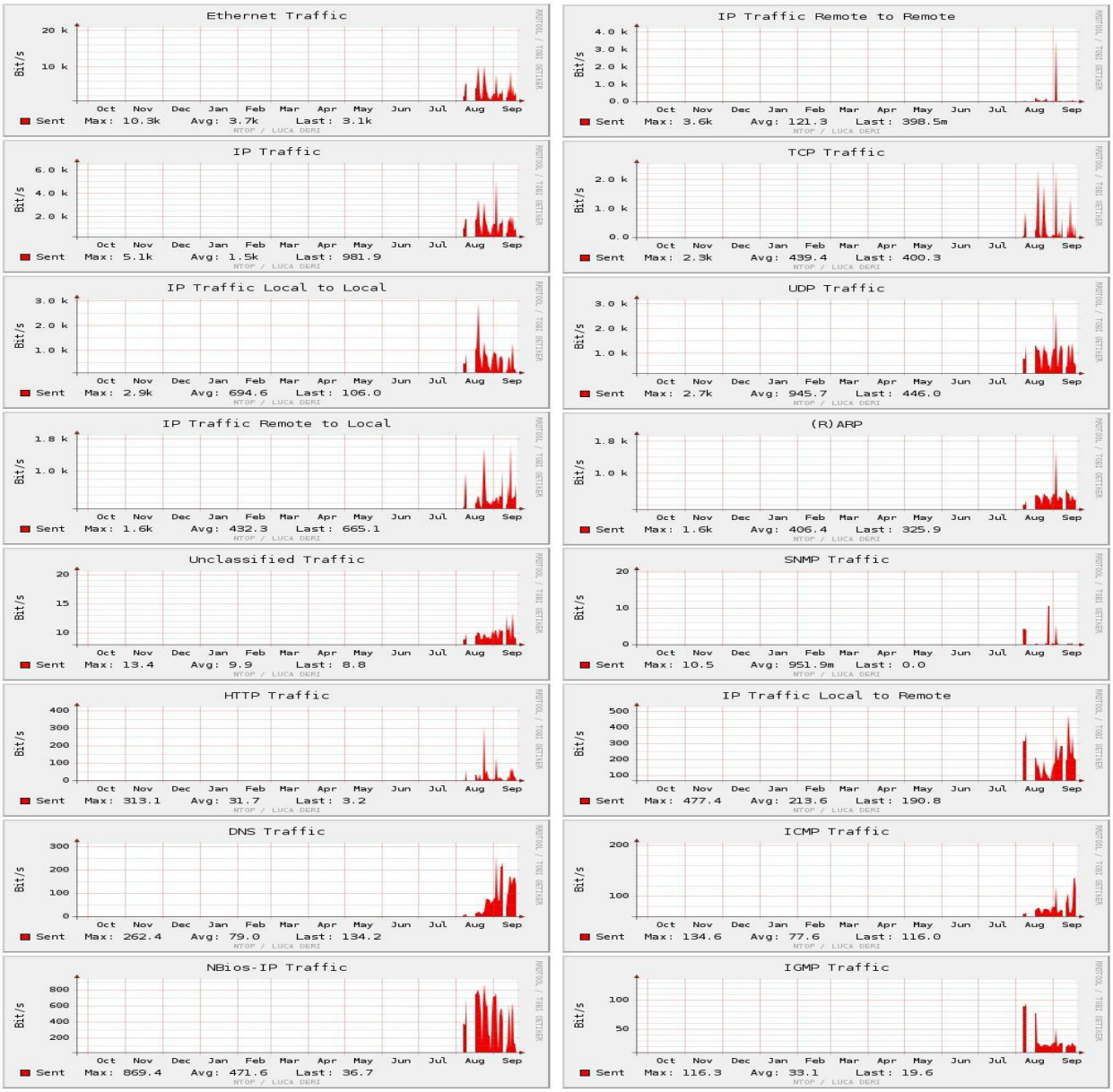


Figura 3.17. Clasificación flujos volumen de tráfico. Vista anual.

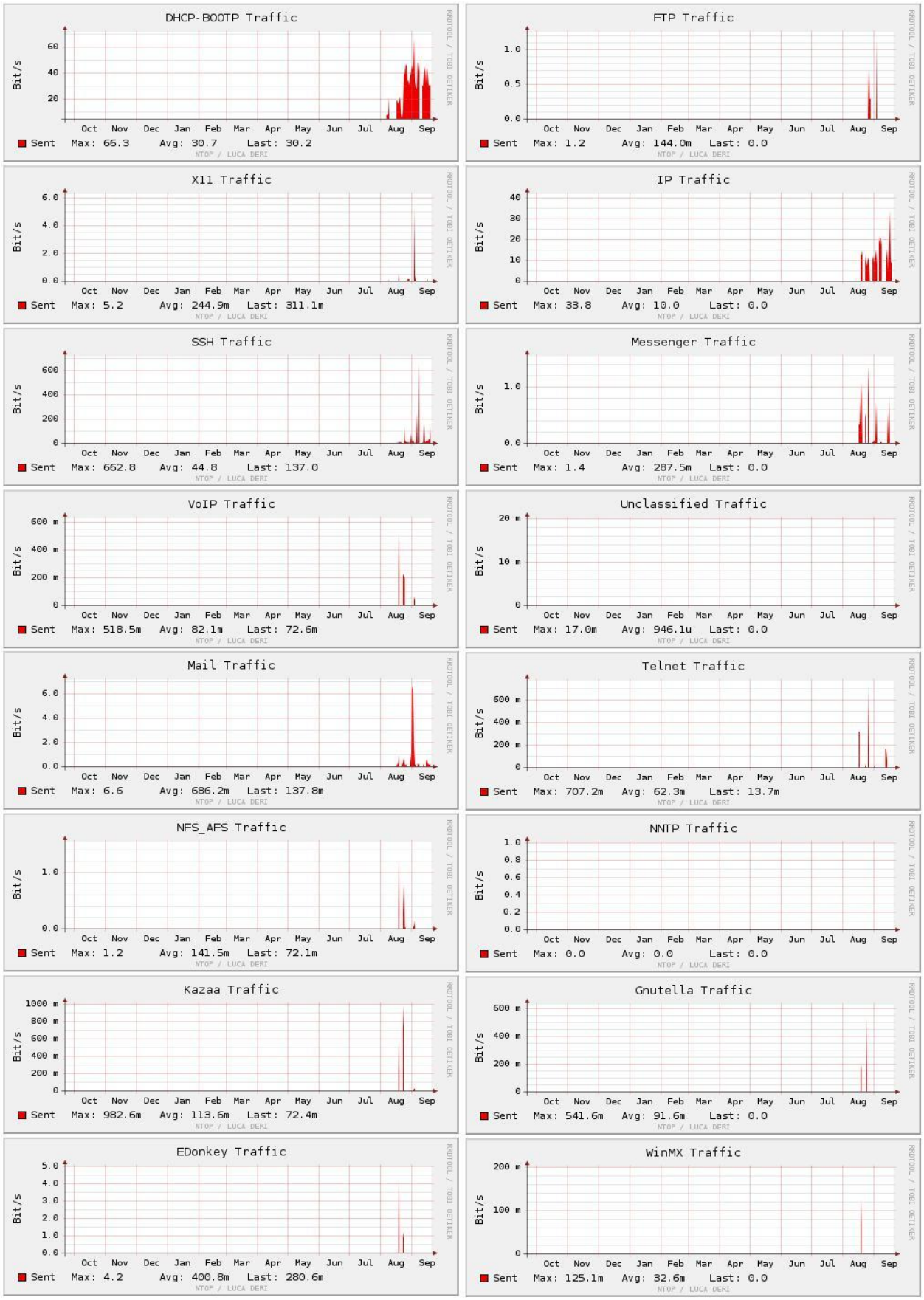


Figura 3.18. Clasificación flujos volumen de tráfico. Vista anual. (Continuación).

5. Volumen de Paquetes.

   En esta sección se muestran los parámetros de Volumen que transitan por la red, pero medidos sobre los paquetes que han sido enviados en ella.

   Añadiendo algunos parámetros de medición como los Badchecksums. Checksum es el parámetro que permite la verificación de los datos a través de las tramas TCP/IP.

   La gráfica se presenta en paquetes/segundo y el contraste con el tiempo en que se realizo la medición.

- Vista Anual.

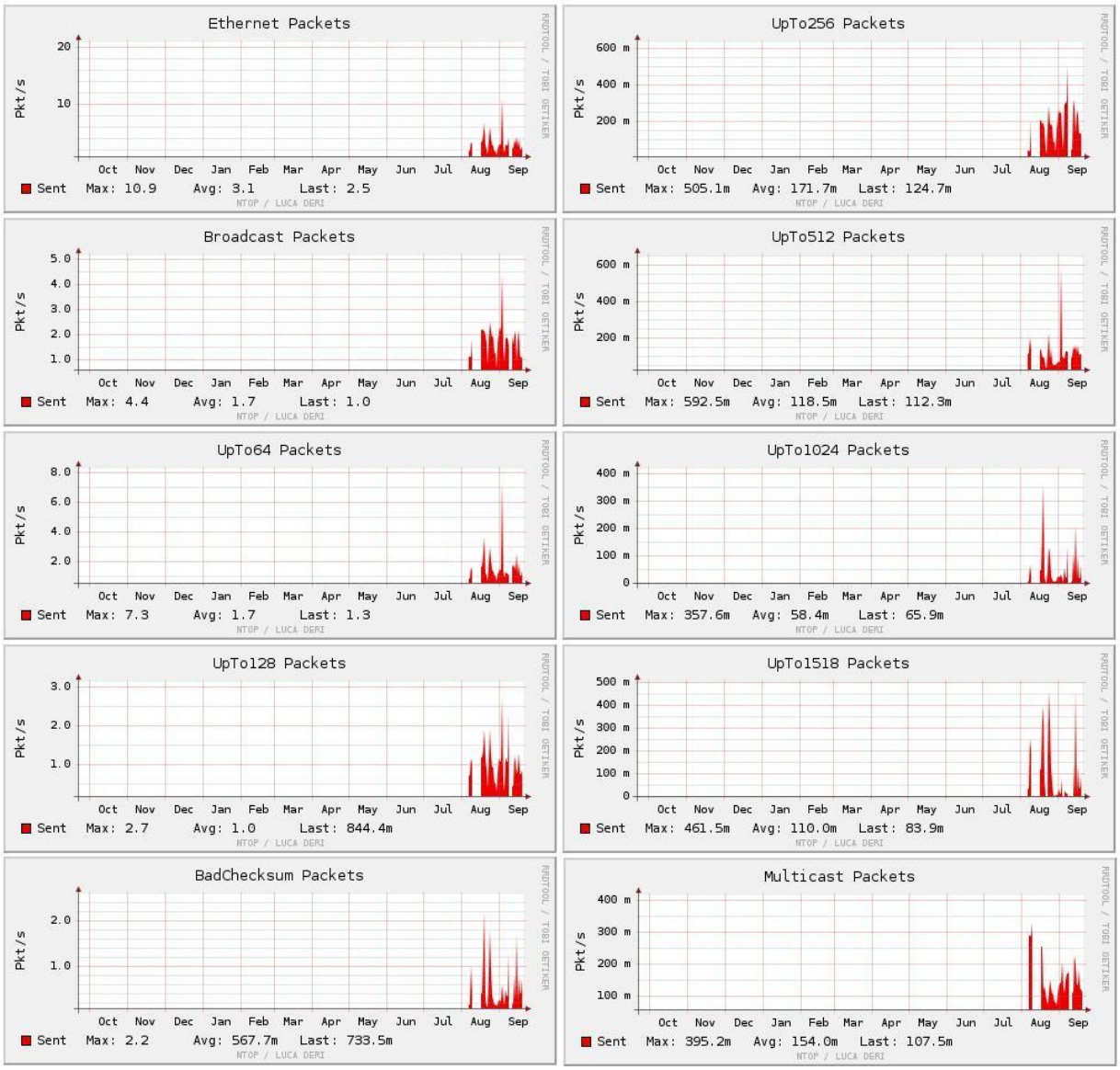


Figura 3.19. Clasificación flujos volumen de paquetes, verificación de datos. Vista anual.

6. Distribución del uso de ancho de banda.

   En esta sección se puede apreciar cómo es usado el ancho de banda por los diferentes servicios desplegados por la red los datos y flujos que están enviando a la red y el nivel de ocupación mantiene.

   En la vista diaria se puede apreciar de mejor manera el uso, incluso las etapas de anomalía (espacios en donde se caen los servicios y/o la red.) por diminutos o corto espacio que ocupe.

- Vista Diaria.

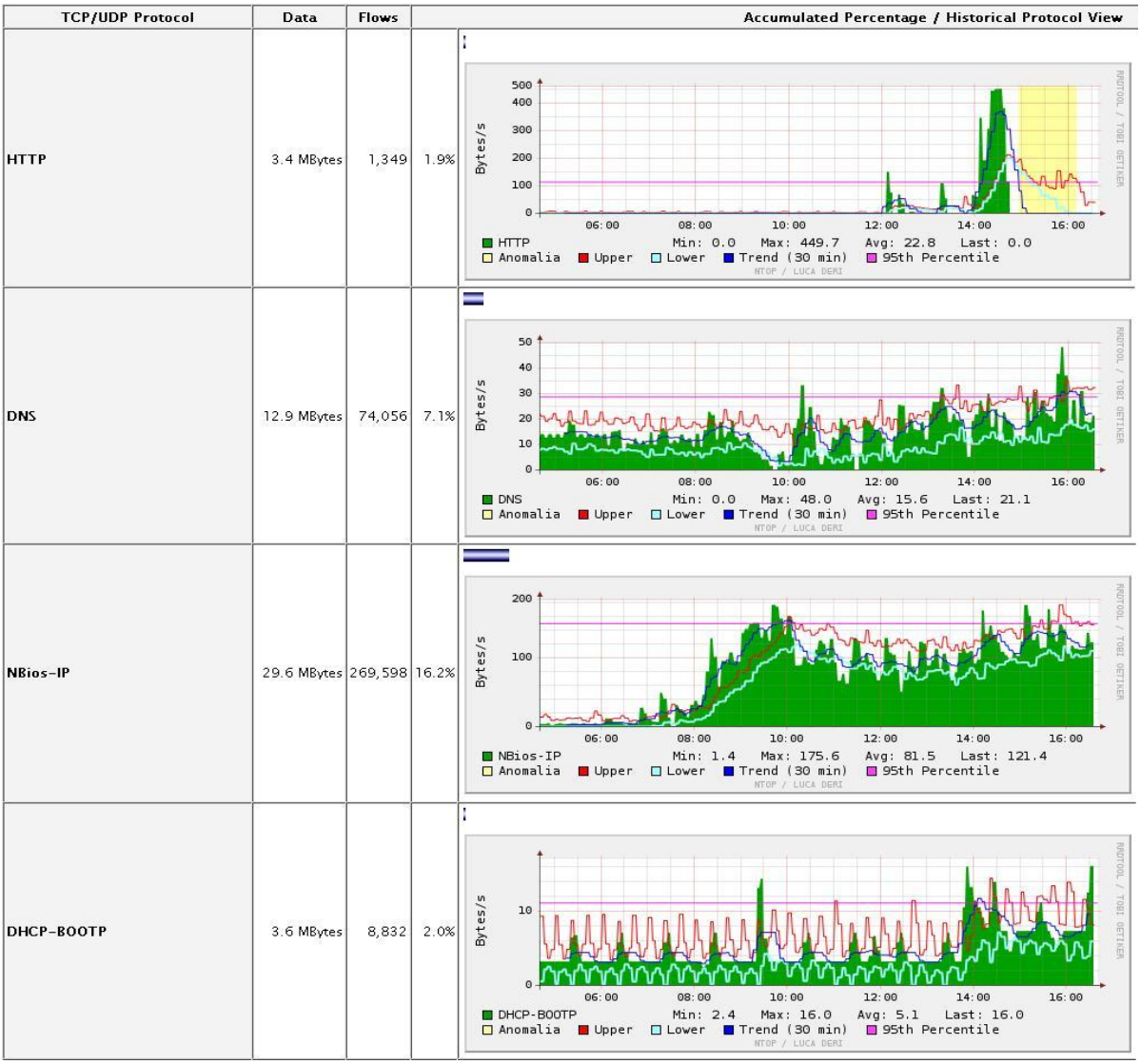


Figura 3.20. Clasificación flujos, uso del ancho de banda. Vista diaria.

- Vista histórica de los diferentes tipos de tráfico.

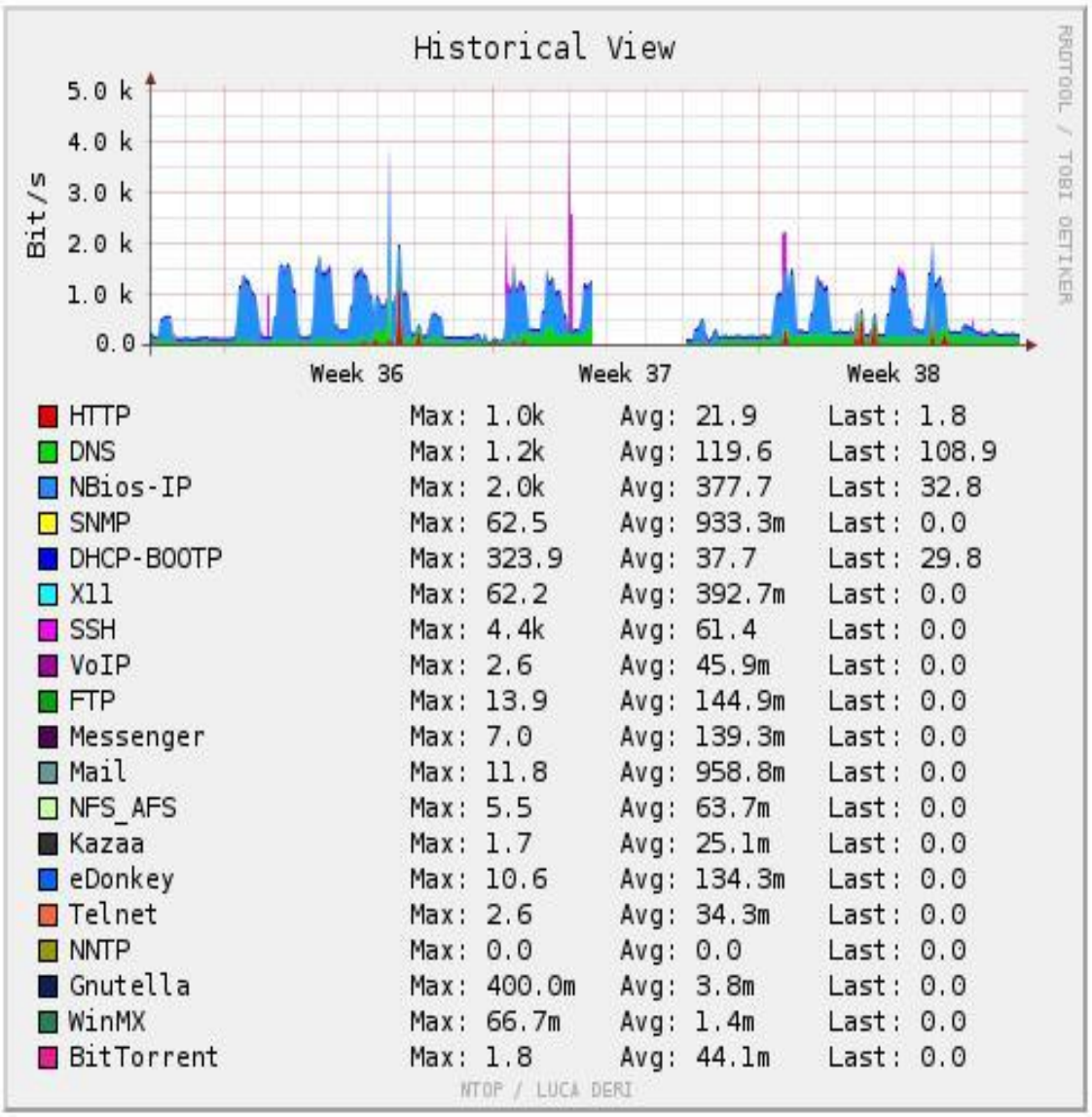


Figura 3.21. Concentrado histórico de la calcificación de tráfico.

7. Nivel de Ocupación de la red.

   El nivel de ocupación se puede ver por los nodos que han sido conectados satisfactoriamente a la red. En el caso de estudio ha habido ciertos disparos de equipos puesto que dentro de los servicios que despliega esta red es brindar conectividad (con tecnología inalámbrica) aun a los usuarios no comunes (considerando que ha habido congresos, diplomados y otros eventos como ferias del libro etc.) dentro de las instalaciones donde esta tendida la red.

   La gráfica muestra el número de nodos y el tiempo en que se realizo la medición.

- Vista Semanal.

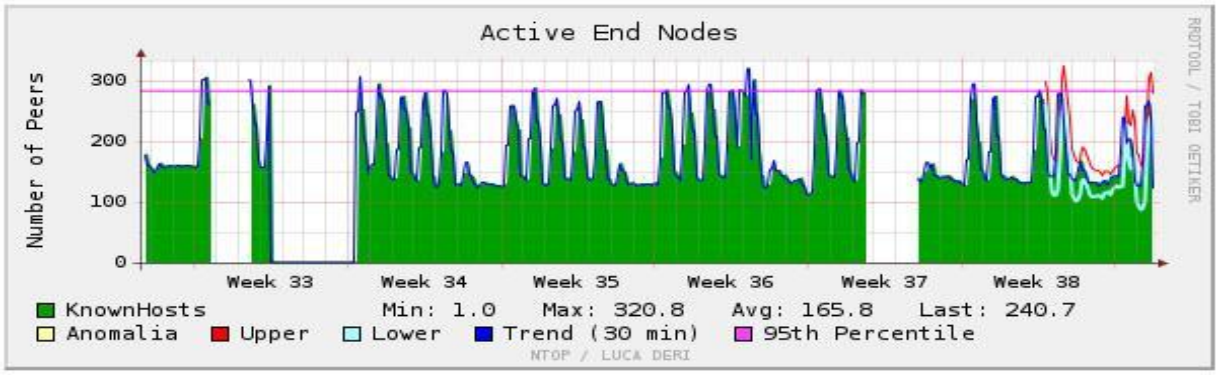


Figura 3.22. Nivel de Ocupación de la red. Vista semanal.

8. Rendimiento de la red (throughput).

   Es la cantidad real de datos que han sido transmitidos en la red, (desde un punto hasta otro). En esta sección se muestra que ha habido caídas en la red, con un mínimo de rendimiento del sistema de red (throughput) de cero.

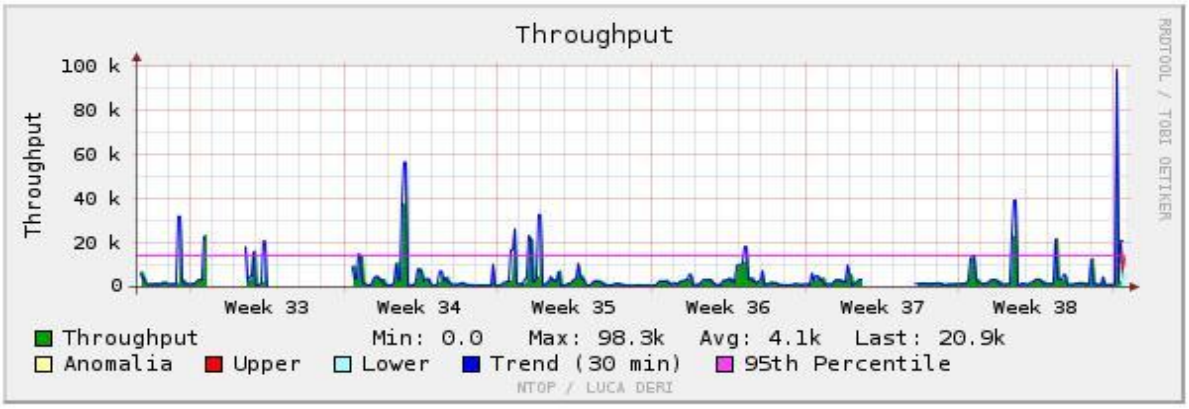


Figura 3.23. Caudal eficaz de transporte de red. Vista semanal.

9. Calidad de la red.

   En esta sección se muestra el tiempo en que tardan los datos en viajar por la red, traducidos en calidad que desempeña la red. Nuevamente se hacen notorios los lapsos en que se ha caído la red, se pierde la conexión y por ende hay una pérdida de paquetes del 100% conectividad nula.

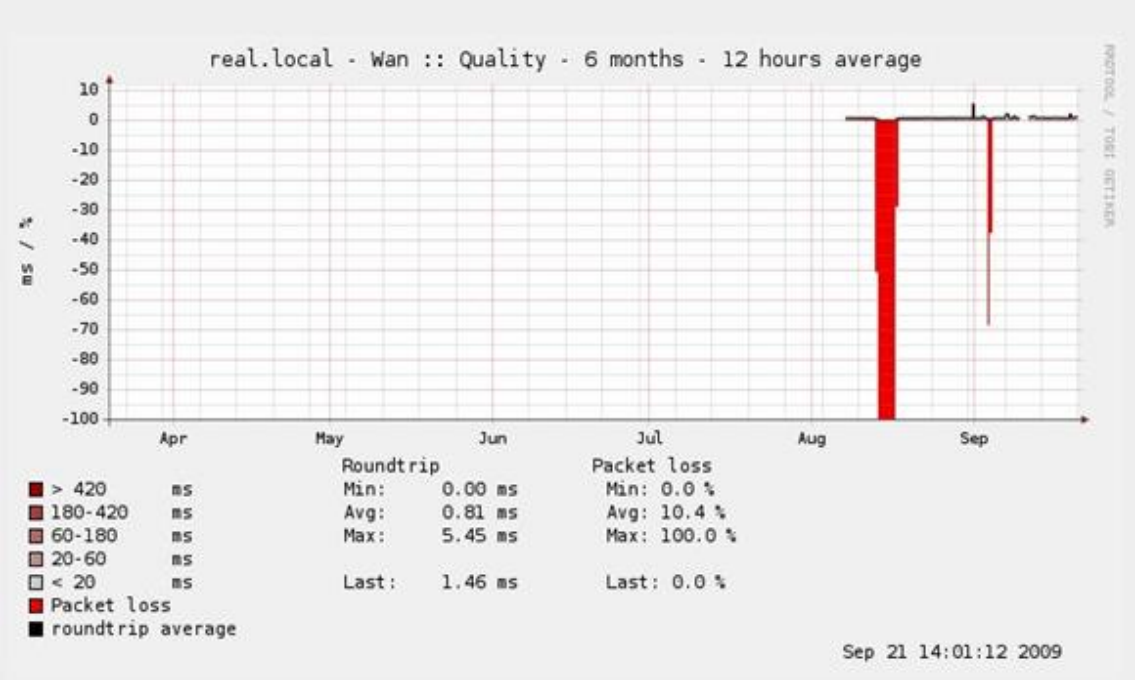


Figura 3.24. Análisis de calidad en la red con PFsense.

10. Paquetes WAN – LAN en la red.

A continuación se muestra el tráfico que hay sobre el sistema de red, clasificado de acuerdo a si pertenece al tráfico generado por el dispositivo WAN o LAN, si es tráfico de entrada o tráfico de salida de datos. Graficado en bits/segundo y en contraste el tiempo en que fue monitoreado.

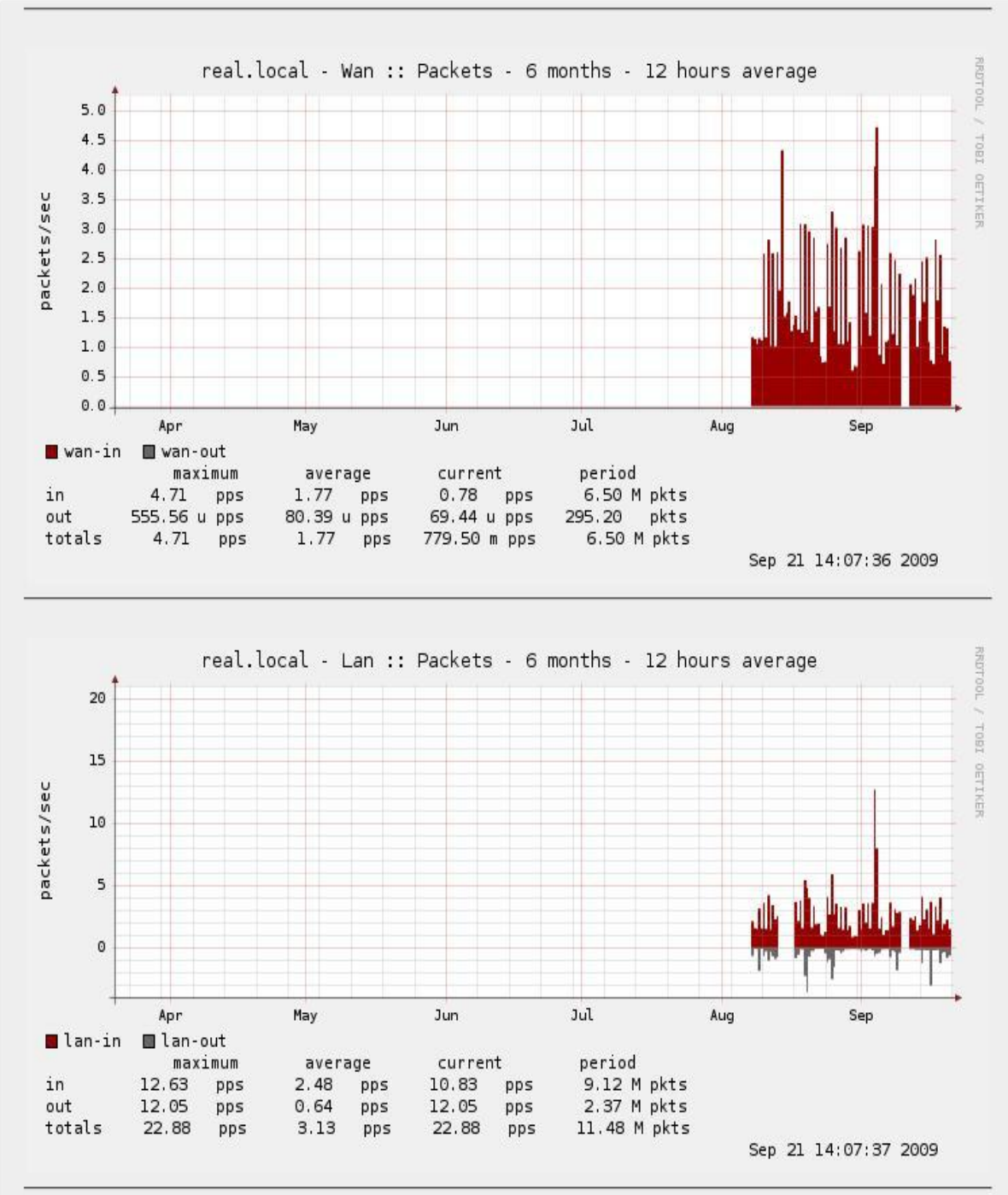


Figura 3.25. Tráfico de paquetes WAN/LAN en la red con PFsense. Vista de anual con énfasis de paquetes/segundo.

11. Conteo de las 20 máquinas que más acceden al sistema de red y uso que hacen del sistema de red.

Para hacer esta medición se ha usado la herramienta bandwidth que en este caso se ha podido instalar como un complemento al sistema **pfsense**. Esta herramienta muestra información muy relevante, como el uso que hacen las maquinas clasificadas en las 20 que mas acceden a los servicios de la red, de igual manera se puede mostrar la red completa. Y entre la información que arroja puede verse el uso de los servidores DNS, el uso que hace también cada nodo en la red. Etc.

- Vista Mensual.

Top 20 IPs by Traffic - Monthly

Ip and Name	Total	Total Sent	Total Received	FTP	HTTP	P2P	TCP	UDP	ICMP
Total	920.9M	573.2M	347.6M	50.6K	83.8M	382.4K	564.2M	295.5M	58.6M
148.204.73.205	516.5M	386.4M	130.2M	34.6K	53.6M	272.9K	444.8M	42.1M	29.6M
148.204.73.255	98.9M	0	98.9M	0	0	0	0	98.9M	32
148.204.73.204	88.3M	13.3M	74.9M	15.3K	17.8M	101.3K	87.7M	471.7K	30.6K
148.204.73.95	30.3M	4.1M	26.3M	0	11.6M	0	29.2M	1.1M	1.6K
148.204.73.254	27.6M	13.7M	13.9M	0	0	0	0	0	27.6M
148.204.73.96	10.4M	10.3M	10.8K	0	136	0	23.1K	10.3M	8.6K
148.204.73.92	9.1M	9.1M	12.1K	0	48	0	4.1K	9.1M	9.2K
148.204.73.99	8.4M	8.4M	21.1K	0	12.2K	0	18.1K	8.3M	3.1K
148.204.73.38	5.4M	5.4M	7.8K	0	148	0	2.4K	5.4M	5.5K
148.204.73.101	5.4M	5.3M	56.6K	0	0	576	401.9K	4.5M	424
148.204.73.73	4.7M	4.7M	13.7K	0	120	0	13.7K	4.7M	7.0K
148.204.73.79	3.3M	3.3M	4.5K	0	0	0	4.3K	3.3M	3.8K
148.204.73.217	3.3M	3.3M	3.9K	120	17.8K	0	18.5K	3.3M	2.8K
148.204.73.213	3.3M	3.3M	7.7K	0	412	0	1.9K	3.3M	5.6K
148.204.73.234	3.3M	3.3M	9.5K	0	13.7K	0	15.0K	3.3M	7.8K
148.204.73.212	3.3M	3.3M	10.5K	0	156	0	1.7K	3.3M	8.7K
148.204.73.218	3.3M	3.3M	6.9K	0	14.8K	0	15.8K	3.3M	5.6K
148.204.73.103	3.0M	3.0M	464	0	2.1K	0	2.2K	2.3M	384
148.204.73.32	3.0M	3.0M	6.2K	0	104	52	864	3.0M	4.8K
148.204.73.84	2.4M	2.4M	11.9K	0	88	0	2.8K	2.4M	10.0K

Figura 3.26. Tráfico sobre la red LAN. Vista mensual. Bandwidth.

Para fines demostrativos de este trabajo, se explica la implementación de este modelo dividido en 2 fases:

La primera fase contiene las capas de topología de red, Ingeniería de tráfico.

La segunda fase contiene las capas de diseño de políticas, implementación de políticas, análisis de resultados y conclusiones.

3.4. Análisis de resultados de la primera fase de implementación.

Resultado del monitoreo anterior, en esta sección se plantea (tomando en cuenta el modelo propuesto) la implementación de varios esquemas de mejora de calidad y basándose en los resultados obtenidos, los cuales se describen a continuación:

3.4.1. Resultados de la etapa de implementacion.

Al principio de la implementación del modelo haciendo **el reconocimiento de la red**, se ha llegado a la conclusión de que la red está subdividida en redes LAN virtuales (VLAN) Figura 3.43. Que por medio de ellas se despliega el servicio de telefonía (VoIP).

Figura 3.27. detalle de la segmentación de la red con VLAN's

Hay muchas ventajas de la red subdividida bajo este tipo de esquema, algunas de las más destacables se mencionan las siguientes:

- Hace a la red más confiable.
- Se tiene una mejor validación de los usuarios, equipos y servicios de red.
- Amplia las capacidades de seguridad y control de los datos que viajan sobre la red.
- Se hace una red extendida, no es físicamente local sino local “en configuración lógica” aunque este geográficamente separada.

Las principales desventajas captadas y que son atribuibles a la configuración del esquema VPN al que está sometida la red son las siguientes:

- Se obtiene un monitoreo parcial de la red. Puede decirse que es incompleto ya que al estar ciertos canales o flujos de datos transportados bajo la VPN, únicamente las mediciones de los flujos o canales de índole general ya que están sin un método de cifrado general.

  En este caso la solución apropiada será enmascarar la dirección IP de navegación o grupo de red. Lo cual implica añadir configuraciones y usuarios personalizados para adquirir el acceso en los servidores. Abrir puertos e implementar seguridad al usuario monitor.

  O inclusive un puente usando el protocolo SSH como medio de comunicación asegurándose que está bien configurado y asegurado puede hacer la conectividad en lugar de VPN.

  Pero esto se debe pedir directamente al Centro de Computo y Comunicaciones del Instituto Politécnico Nacional ya que se ha mencionado que este departamento es el encargado y superior jerárquico (en todo lo relacionado con conectividad) del CFIE.

3.4.2. Corroborando los resultados obtenidos.

Para cubrir este objetivo se uso el software Caín y Abel, dicho software permitió cumplir con el objetivo de **comprobar la veracidad** entre resultados, a

la vez que se identificaron algunos **problemas** como que la seguridad es muy débil ya que la red puede ser monitoreada por agentes o personas que son externos al sistema de red, o inclusive si alguien consiguiera acceso a la red desde fuera (Ya sea con técnicas de DDOS (negación de servicio), el hombre de en medio (man in the middle), virus y puertas traseras por mencionar algunos) Se podrá obtener mucha información por ejemplo las direcciones IP de los servidores asociados con su dirección **MAC** (Media Access Control) e incluso su nombre dentro de la red. Ejemplificando los datos arrojados de manera automática sin necesidad de conocimientos bastos en redes o su escaneo. Para después realizar un ataque que podría ser letal a las comunicaciones en el centro incluso poniendo en peligro toda la red institucional y los datos que por ella transitan.

La solución a ello es idear un esquema de ocultamiento de datos, mostrar los mínimos posibles y requeridos para un funcionamiento óptimo, cerrar puertos innecesarios para el cumplimiento de los servicios e implementar políticas de seguridad y conciencia de la información que se muestra a la red.

Hacer una auditoria para saber los datos que se pueden obtener aunque se crea que no están mostrados, verificar los niveles de seguridad, ya que si los datos transitan de manera insegura alguien pude leerlos y sacarle provecho con fines maliciosos, hay que valorar la información que se envía, recibe y procesa. Recordemos que la información es poder.

3.4.3 Características negativas de la red (latencia).

Una mala característica de la red es su **latencia**. La importancia de que la red sea lo más estable posible es porque ésta característica negativa acarrea muchos **problemas** de fondo. Comenzaremos explicando algunos de los más relevantes.

- Ya que hay mucha latencia en la red, los datos no llegan y estando dentro del esquema de Ethernet CSMA/CD, por sus siglas en ingles que significan Carrier Sense Multiple Access with Collision Detection (en español, "Acceso Múltiple por Detección de Portadora con Detección de Colisiones"). Por esta mala característica de la red se crea un circulo vicioso que afecta a la comunicación ya que se hace reenvió constante de paquetes, provocando colisiones en la red y saturación de la misma. Incrementado otros factores negativos como son retardos. En el peor de los casos esto se ve reflejado en los periodos en los que la red se cae y no hay comunicación. En el mejor de ellos la red notablemente lenta haciéndose un fenómeno notorio.

Se incrementa el tráfico broadcast, consumo significativo de ancho de banda que podría considerarse desaprovechamiento por alguna mala configuración.

La **solución** propuesta a este problema es revisar el buen funcionamiento de los equipos en este caso los switches y routers ya que estos elementos de red son fundamentales en la decisión y encaminamiento de todo el tráfico de la red. Ya corroborado que el hardware se encuentra completamente funcional hay que pasar a la revisión de una configuración adecuada. Ya que comúnmente hay muchas fallas en este tipo de secciones al hacer una actualización en la red o cambios físicos o lógicos la configuración no es debidamente actualizada. Además es muy importante actualizar al último firmware estable publicado por los fabricantes y por defecto instalar también los parches de seguridad o extensiones adecuadas a las necesidades de los equipos.

- Se pudo observar que los flujos de algunos servicios clave son constantes. Estrictamente hablando de los flujos VoIP que viajan sobre la red.

  Entonces surge una pregunta ¿Por qué si se está induciendo hacia la conclusión de que la red está mal hay flujos constantes?

  Bien la explicación es la siguiente, ya que la red cuenta con un ancho de banda T1, y los servicios como VoIP necesitan un ancho de banda relativamente bajo (a comparación de lo que se tiene disponible) hay un funcionamiento que se podría describir como bueno o constante. Pero ante las mediciones esto es solo una ilusión ya que los demás datos o los servicios que requieren un ancho de banda considerablemente mayor no están sobrados y trabajan de manera forzada o limitada aun teniendo la capacidad de una red T1. Por tanto es una conclusión que los servicios trabajan por que hay recursos buenos pero no trabajan de manera óptima, no están bien configurados ni hay una buena planeación, en base a las pruebas realizadas y los resultados obtenidos se nota el desperdicio de capacidades tecnológicas y de red, además de una mala administración general del sistema de red.

  Nuevamente la solución propuesta es que sea una prioridad la estabilización de la red, como ya se menciono aplicando mejoras en la configuración, actualización de equipos etc.

- El tráfico generado es mayor que el necesario, el throughput es demasiado bajo de acuerdo al ancho de banda que se tiene disponible. Ya que dentro de la red hay mucho tráfico basura broadcast o en el mejor de los casos multicast. Hay que intentar a toda costa elevar el tipo de tráfico unicast benévolo para las comunicaciones y tránsito de la red.

- Evitar también las colisiones, por reenvío de tráfico y cuellos de botella, esto generara a la larga pérdida de información saturación de la red y caída de los servicios y comunicaciones.

  En esta sección la propuesta de solución es un estudio eficaz para encontrar un equilibrio en el nivel apropiado que los servicios y usuarios requieren.

- Acerca de la distribución del ancho de banda. El esquema en que está distribuido el ancho de banda disponible para esta red deja mucho que desear, se han notado factores negativos que se enlistan a continuación.

  1. El ancho de banda con el que se cuenta no tiene una distribución equitativa.

  2. La red no está debidamente multiplexada. Las redes convergentes de nueva generación brinda la posibilidad de hacer la división de canales. Para voz video y datos, aunque viajen por el mismo medio físico hay una clara tendencia a separarlos y así asegurar los servicios para brindarle a la red y usuarios, basado en diferentes necesidades.

  3. No hay un canal de reserva para los servicios que así lo requieran. Por ejemplo las comunicaciones VoIP, o en un caso de mayor exigencia videoconferencia.

  La solución propuesta, ahora es hacer las configuraciones pertinentes además de la reserva de características necesarias para el óptimo funcionamiento de la red.

- Nivel de ocupación de la red. Sin dudas este es un punto a considerar siendo estrictamente necesario darle servicios de conexión a todos los usuarios que así lo requieren. Se ha dicho que

el ancho de banda que se maneja es aparentemente sobrado, de igual manera se ha demostrado que la red está trabajando de manera normal, por ello y como está refiriéndose a que si en algún momento se anexa un servicio nuevo o usuarios más, la red podría colapsar. Ya que volviendo al tema de la inestabilidad y la mala planeación en que se encuentra la red. Se han detectado problemas como los siguientes:

1. Problemas de conectividad.

2. Mala planeación y organización de la red, pocas expectativas de crecimiento y adaptabilidad ante ello.

La solución propuesta consiste en la implementación de políticas de seguridad, de usuario, de uso de la red etc.

En general se concluye que la red tiene grandes deficiencias que a la larga pueden desencadenar inoperatividad de la red, si estas situaciones no se atienden se está comprometiendo toda la información que viaja sobre la red, ya que la calidad que ofrece para los servicios es ineficiente.

Para corroborar estos resultados se han hecho mediciones desde diferentes perspectivas mencionando el caso particular del software **ntop** montado sobre el sistema **PFsnese[1]** basado en el S.O **freebsd** actualizado los tres a su última versión 3.3.8 para **ntop[2]**, 7.1 para **freebsd** y 1.2.3 para **PFsense**. Liberados en el año 2008 en sus versiones estables, nombrado para análisis ahora **ntop**1.

El comentario surge a partir del análisis que se ha realizado sobre las mediciones obtenidas con un servidor Ubuntu Linux, 8.10 y **ntop** 3.2 esta versión de **ntop** liberada en su versión estable en el año 2005. Nombrada ahora **ntop**2.

Bien las diferentes perspectivas que se muestran dado que en cuestión de análisis los volúmenes son idénticos pero no las fuentes. Por ejemplo para el reporte de **ntop**1 el dispositivo que hace mayor uso de ancho de banda es el propio servidor y es comprensible ya que al hacer las mediciones está inmerso en todo el tráfico que circula por la red.

En cambio en el reporte **ntop**2 enlista como uno de los dispositivos con mayor uso de ancho de banda los propios DNS y que aun aquí está distribuido el tráfico de manera desigual.

Considerando los dos enfoques correctos ya que de alguna manera el total de volumen de tráfico recorre invariablemente sobre estos dispositivos en la red, y las mediciones (como ya se ha mencionado) de volumen son idénticos. Aunque las fuentes se muestren un poco variable.

En Internet.

[1] http://www.pfsense.com/

[2] http://www.ntop.org/ntop-man.html

CAPÍTULO IV.

Pruebas y resultados (implementación del modelo).

RESUMEN:

En este capítulo se hace el análisis de los resultados, tras implementar las primeras etapas del modelo (ahora ya es una arquitectura). Se compara el desempeño de la red antes de implementar el modelo y después de su implementación.

OBJETIVOS DEL CAPITULO:

- Mostrar que el modelo es ya una arquitectura implementada.
- Mostrar los resultados tras implementar el modelo.
- Hacer el análisis de resultados y proponer mejoras.
- Comparar el desempeño antes y después de la implementación del modelo.

4.1 Resultados de la segunda etapa de implementación del modelo sobre la red de CFIE.

Ya que se ha hecho el análisis del monitoreo y se han detectado algunas fallas, se ha procedido a emitir las soluciones y las políticas adecuadas para mejorar la calidad de la red.

4.1.1. Gestión de recomendaciones para mejora de calidad.

De acuerdo con los resultados obtenidos por las mediciones realizadas a continuación se proponen una serie de recomendaciones y posibles mejoras basadas en el modelo propuesto, las cuales se han dividido en recomendaciones de tipo administrativo y de infraestructura, así como las concernientes a la parte de seguridad y disponibilidad de la red principalmente definiendo políticas para este fin.

Desde sus inicios la informática y telecomunicaciones han sido una materia compleja en sus aplicaciones y desarrollos tecnológicos, por lo que es necesario el uso de metodologías en cada uno de sus componentes. Desde su diseño básico hasta su más complejo mecanismo. Las metodologías que se usan en un sistema de red reflejan la capacidad con que se maneja el sistema al desembocar en políticas robustas.

Las políticas que se logran implementar tiene la finalidad de englobar los conocimientos de los profesionales que están dando soporte al sistema de red, tal como si lo hiciera uno solo.

4.2. Diseño de políticas.

El acceso a la infraestructura de red y los servicios que sobre esta se despliegan son para uso de las personas que laboran dentro del *Centro de Formación e Innovación Educativa* (*CFIE*). (Administrativos, diseñadores, cuerpo de soporte etc.)
Cada persona que labora en el (CFIE) y tiene necesidades para el buen cumplimiento de su trabajo tiene a su disposición unos equipos conectados a la infraestructura tecnológica de la red, con los respectivos servicios de los que dispone el sistema y la red misma.

Para este aspecto se contemplan las siguientes políticas aplicables a la red institucional y al CFIE:

USUARIO:

Políticas de acceso:

- Usar Claves de Acceso que no estén asociadas a datos comunes del usuario, tales como su fecha de nacimiento, apelativos, nombres de familiares, etc.

- Los nombres de usuario y contraseñas no deben ser compartidos por los usuarios, tampoco se deben tener respaldados o ser manipulados por escrito.

- Cambiar de Clave de Acceso por lo menos cada 3 meses. Aunque lo ideal es hacerlo mensualmente. O ante la sospecha de amenaza.

- Las claves de acceso deben tener una longitud de al menos 8 caracteres, y deben ser alfanuméricos e incluso signos permitidos (puntuación).

- Los usuarios no deberán repetir las contraseñas que ya han sido utilizadas anteriormente.

- Al introducir el nombre de usuario o contraseña incorrecta al paso de X intentos incorrectos la cuenta deberá bloquearse por seguridad (normalmente se bloquea el sistema tras 3 o 5 intentos).

- Si el servidor no reconoce su nombre y clave de acceso o servicio de correo, podría ser que ya esté siendo utilizado por un intruso. A menos que haya un error en la configuración, la cual deberá ser verificada.

Políticas de seguridad.

- El usuario del sistema será responsable de la mantener la integridad de sus datos.

- Los usuarios deben bloquear sus sesiones siempre que estén lejos de sus equipos por muy corto que sea el tiempo en que pierdan de vista el equipo.

- Los usuarios deberán apagar sus terminales de trabajo después de terminar día de labores.

- Los usuarios de estaciones de trabajo internos y usuarios externos deberán actualizar en forma permanente los últimos parches de los sistemas operativos.

- Es de suma importancia tener instalado un software antivirus, sin importar la marca o lenguaje de instalación, y actualizar su registro de virus diariamente. Además de realizar un escaneo a los dispositivos regularmente o ante cada conexión de dispositivos externos.
- No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, así ofrezca en él atractivos premios o temas provocativos. Mucho menos si estos archivos tienen doble extensión.

- No instalar copias de software pirata. Además de transgredir la Ley, pueden contener virus, spyware o archivos de sistema incompatibles con el del usuario, lo cual provocará su inestabilidad.

- No copiar, distribuir o instalar ningún software no permitido, incluyendo (aunque no solamente) salvapantallas, temas de escritorio, juegos, demos etc.

- Tomar precauciones con los contenidos de applets de Java, JavaScripts y Controles ActiveX, durante la navegación, así como los Certificados de Seguridad. Es recomendable configurar el navegador desactivando la ejecución automática de estos contenidos.

- Instalar un Firewall de software o cualquier sistema seguro para controlar los puertos de su sistema. No dejar puertos abiertos más que los estrictamente necesarios.

- No almacenar información importante en su sistema. (Si un intruso la captura, puede borrar esos archivos y eliminar toda prueba, para posteriormente usar los datos obtenidos). Es recomendable mantener esta información en unidades de cinta o memorias extraíbles, almacenados en un lugar seguro.

- No se debe confiar en los archivos gratuitos que se descargan de sitios web desconocidos, ya que son una potencial vía de propagación de virus.

- Configurar el sistema para que muestre las extensiones de todos los archivos.

- No contestar los mensajes SPAM, ya que al hacerlo se re-confirmará su dirección IP, ni prestar atención a los mensajes con falsos contenidos (Hoaxes), tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, advertencia de virus de fuentes desconocidas, etc.

- No se deben descargar archivos con títulos atractivos pero sospechosos, desde canales de Chat, Grupos de noticias (Newsgroups), redes P2P como **KaZaa, Morpheus, BearShare, Ares** o servidores de archivos **torrent**, etc. Tampoco vía servidores FTP desconocidos.

- La aparición y desaparición de archivos, incluso temporales injustificadamente, lentitud del sistema, bloqueos o reinicios continuos, desconexiones del modem, inicialización o finalización de programas o procesos sin justificación, la bandeja del CD/DVD se abre y cierra sin motivo alguno, el teclado, mouse u otro periférico dejan de funcionar, entre algunas otras, esas son evidencias de que el equipo está siendo controlado por un agente externo que ha ingresado al sistema por medio de alguna técnica que podría ser un troyano/puerta trasera (backdoor). Informe al cuerpo de soporte o al administrador de red de forma inmediata.

- Borrar constantemente los cookies, archivos temporales e historial, en la opción Herramientas, Opciones de Internet, de su navegador.

- Es preferible navegar a través de un Proxy anónimo que no revele la identidad o dirección IP real del usuario o adquirir un software de navegación segura como **Anonymizer, Freedom WebSecure**, etc. que emplean sistemas de túneles con IPs de intercambio aleatorio.

- Corroborar que la información a la cual se tiene acceso o con la que se está tratando es precisa, está completa y esta actualizada.

- Dar aviso al departamento de soporte ante cualquier anomalía por mínima que sea.

- No descargar información que contenga algún tipo o carácter inapropiado tal como pornografía, ideas contrarias la moral como racismo etc. O que fomente la violencia.

Políticas de uso:

- El servicio es por tiempo limitado y coincide con los periodos escolares, esto para llevar bitácora de servicios, rendimiento y periodos de mantenimiento.

- Los servicios proporcionados serán basados en redes IP, acceso a Internet y acceso a servicios locales basados en Web como es el correo electrónico y explotación de bancos de información Bibliotecaria. Confiando en el buen criterio del usuario para no usarlo a deshoras o haciendo mal uso dentro de horas de trabajo incluso nada no relacionado con el mismo.

- Es responsabilidad del usuario el tipo de información de la que hace uso, ya que esta puede ser de contenido inapropiado. Y tiene sanciones.

- Algunos recursos y servicios de la red Internet son privados y existen derechos sobre ellos ya sea de autor o comerciales, por lo que el acceso no autorizado a estos es responsabilidad única del usuario. Al igual que el almacenaje de publicaciones, música o video sin el conveniente pago de derechos. Infringir con las leyes también tiene sanciones.

- Los usuarios del sistema de red son monitoreados constantemente para evitar que se hace un uso inapropiado de los servicios. Se considera uso inapropiado actividades como: piratería, envío de propaganda subversiva, propagación de virus informáticos, uso delictivo, etc.

- En caso de infringir en algo que vaya en contra del buen uso del sistema Se generará un reporte que irá directamente al expediente del usuario, con sanciones por ello.

ADMINISTRADORES:

Políticas de acceso:

- Solo los administradores de la red y cuerpo de soporte tendrán acceso a los servidores y tendrán llave del sitio de red.

- Usar Claves de Acceso que no estén asociadas a datos comunes del usuario, tales como su fecha de nacimiento, apelativos, nombres de familiares, etc.

- Nombres de usuario y contraseñas no deben ser compartidos por los usuarios, tampoco se deben tener respaldados o ser manipulados por escrito.

- Cambiar de Clave de Acceso por lo menos cada 3 meses. Aunque lo ideal es hacerlo mensualmente. O ante la sospecha de amenaza.

- Las carpetas compartidas, dentro de una Red, deben tener una Clave de Acceso, la misma que deberá ser cambiada periódicamente.

- Las claves de acceso deben tener una longitud de al menos 8 caracteres, y deben ser alfanuméricos e incluso signos permitidos (puntuación).

- Los usuarios no deberán repetir las contraseñas que ya han sido utilizadas anteriormente

- Al introducir el nombre de usuario o contraseña incorrecta al paso de X intentos incorrectos la cuenta deberá bloquearse por seguridad.

Políticas de seguridad:

- Una copia de seguridad, de las copias importantes del sistema (contraseñas, datos importantes, configuraciones) deberán ser guardadas en un lugar seguro donde no puedan ser alcanzados por un desastre o incluso un robo. también es recomendable tenerlos en un lugar aparte alejado de los demás respaldos de seguridad.

- Deberá llevarse el control y auditoría en todos los sistemas que hagan uso de autenticación por usuario y contraseña con todos los registros de

intentos de entrada / fracasos, los inicios de sesión con éxito y los cambios realizados en todos los sistemas.

- Los administradores de red deberán actualizar en forma permanente los últimos parches de los sistemas operativos.

- Mantener al mínimo el uso de la autenticación como administrador en los sistemas. Siempre que sea posible resolver problemas con privilegios de usuario común.

- Es de suma importancia tener instalado un software antivirus, sin importar la marca o lenguaje y actualizar su registro de virus diariamente. Además de realizar un escaneo a los dispositivos regularmente o ante cada conexión de dispositivos externos.

- No ejecutar ningún archivo contenido en un mensaje de correo no solicitado o enviado por un remitente desconocido, así ofrezca en él atractivos premios o temas provocativos. Mucho menos si estos archivos tienen doble extensión.

- No instalar copias de software pirata. Además de transgredir la Ley, pueden contener virus, spyware o archivos de sistema incompatibles con el del usuario, lo cual provocará su inestabilidad.

- Verificar cualquier software que haya sido instalado, asegurándose que provenga de fuentes conocidas y seguras.

- No copiar, distribuir o instalar ningún software no permitido, incluyendo (aunque no solamente) salvapantallas, temas de escritorio, juegos, demos etc.

- Tomar precauciones con los contenidos de applets de Java, JavaScripts y Controles ActiveX, durante la navegación, así como los Certificados de Seguridad. Es recomendable configurar el navegador desactivando la ejecución automática de estos contenidos.

- Instalar un Firewall de software o cualquier sistema seguro para controlar los puertos de su sistema. No dejar puertos abiertos más que los estrictamente necesarios.

- No emplear los máximos privilegios en tareas para las que no sean estrictamente necesarias.

- No almacenar información importante en su sistema. (Si un intruso la captura, puede borrar esos archivos y eliminar toda prueba, para posteriormente usar los datos obtenidos). Es recomendable mantener esta información en unidades de cinta o memorias extraíbles, almacenados en un lugar seguro.

- No se debe confiar en los archivos gratuitos que se descargan de sitios web desconocidos, ya que son una potencial vía de propagación de virus.

- Configurar el sistema para que muestre las extensiones de todos los archivos.

- No contestar los mensajes SPAM, ya que al hacerlo se re-confirmará su dirección IP, ni prestar atención a los mensajes con falsos contenidos (Hoaxes), tales como ofertas de premios, dinero, solicitudes de ayuda caritativa, advertencia de virus de fuentes desconocidas, etc.

- Si el servidor no reconoce su nombre y clave de acceso o servicio de correo, podría ser que ya esté siendo utilizado por un intruso. A menos que haya un error en la configuración, la cual deberá ser verificada.

- Tampoco se deben descargar archivos con títulos atractivos pero sospechosos, desde canales de Chat, Newsgroups, redes P2P como **KaZaa, Morpheus, BearShare, Ares** o servidores de archivos **torrent**, etc. Tampoco vía servidores FTP desconocidos.

- La aparición y desaparición de archivos, incluso temporales injustificadamente, lentitud del sistema, bloqueos o reinicios continuos, desconexiones del modem, inicialización o finalización de programas o procesos sin justificación, la bandeja del CD/DVD se abre y cierra sin motivo alguno, el teclado, mouse u otro periférico dejan de funcionar, entre algunas otras, esas son evidencias de que el equipo está siendo controlado por un agente externo que ha ingresado al sistema por medio de alguna técnica que podría ser un troyano/puerta trasera (backdoor). Informe al cuerpo de soporte o al administrador de red de forma inmediata.

- Borrar constantemente archivos temporales y archivos innecesarios del sistema.

- Es preferible navegar a través de un Proxy anónimo que no revele la identidad o dirección IP real del usuario o adquirir un software de navegación segura como **Anonymizer, Freedom WebSecure**, etc. que emplean sistemas de túneles con IPs de intercambio aleatorio.

- Todos los servidores deben estar configurados con el mínimo de servicios para realizar sus funciones designadas.

- Mantener los servicios desplegados sobre la red, al nivel mínimo posible. No saturar su uso si no es estrictamente necesario.

- Corroborar que la información a la cual se tiene acceso o está tratando es precisa, está completa y esta actualizada.

- No descargar información que contenga algún tipo o carácter inapropiado tal como pornografía, ideas contrarias la moral como racismo etc. O que fomente la violencia.

SISTEMAS:

Políticas de acceso.

- Para mejor control los datos de los equipos en red deben estar asociados al usuario de entre los cuales destacan los siguientes:
    - Marca y modelo del dispositivo.
    - Sistema Operativo (o versión de firmware según aplique)
    - Tipo y versión del antivirus. (Si aplica).
    - Dirección MAC (identificador asociado a la tarjeta de red).
    - Dirección IP.

- No deberán hacerse cambios entre componentes del equipo (hardware) de conexión, tampoco configuración de conexión tal como:

    - dirección IP.
    - dirección MAC.
    - Nombre del equipo.
    - Grupo de red o de trabajo.

- Alguno de estos cambios solo se puede hacer por el personal indicado (cuerpo de soporte técnico) previo análisis del problema detectado por el usuario.

- Los servicios proporcionados serán basados en redes IP, acceso a Internet y acceso a servicios locales basados en Web como es el correo electrónico y explotación de bancos de información Bibliotecaria. Confiando en el buen criterio del usuario para no usarlo a deshoras o haciendo mal uso dentro de horas de trabajo incluso nada no relacionado con el mismo.

Políticas de seguridad.

- Los usuarios sólo tendrán suficientes derechos para todos los sistemas que les permitan realizar su función de trabajo. Los derechos de los usuarios se mantendrá en un mínimo en todo momento.

- Siempre que sea posible ninguna persona tendrá acceso total a ningún sistema particular. El Departamento de control de red / servidor de contraseñas y contraseñas del sistema serán asignados por el administrador del sistema en el departamento de soporte técnico.

- Es de suma importancia tener instalado un software antivirus, sin importar la marca o lenguaje y actualizar su registro de virus diariamente. Además de realizar un escaneo a los dispositivos regularmente o ante cada conexión de dispositivos externos.

- Los usuarios del sistema de red son monitoreados constantemente para evitar que se haga un uso inapropiado de los servicios. Se considera uso inapropiado actividades como: molestar a los usuarios con mensajes y charlas electrónicas, piratería, envío de propaganda subversiva, propagación de virus informáticos, uso delictivo, etc.

Políticas de uso.

- Toda la red debe estar debidamente documentada, planos de red cableada. O alcance de las redes inalámbricas.

- Se debe de hacer un escaneo constante y periódico de los medios de red ya sea guiados o no guiados en conjunto con el equipo de red del que hagan uso para corroborar su buen funcionamiento.

- Deberá eliminarse a toda costa la redundancia de conexiones a excepción que así lo indique la planeación de la red.

- Todos los servidores y equipo de funcionamiento crítico para la red deberán estar equipadas con el UPS para asegurar el suministro de energía eléctrica ante cualquier falla.

- Configurar el sistema para que muestre las extensiones de todos los archivos.

- Todos los servidores deben estar configurados con el mínimo de servicios para realizar sus funciones designadas.

- Mantener los servicios desplegados sobre la red, al nivel mínimo posible. No saturar su uso si no es estrictamente necesario.

Una vez implementadas las recomendaciones se describirán los resultados obtenidos en las mediciones tomadas.

4.3 Implementación de políticas:

Tras el análisis de los resultados después de la implementación del modelo en la red del CFIE, resultados que fueron mayoritariamente negativos, se hace una serie de propuestas y en esta sección se comenzara a hacer una descripción más detallada de dichas soluciones. Ya que el cambio más pequeño y sin planeación puede generar un gran impacto en el desempeño de la red.

- Ya que se ha encontrado información desactualizada en cuanto a los responsables operativos y ha habido cambios en la topología y cableado estructurado de la red. Se propone hacer un análisis de manera minuciosa acerca del estado funcional y configuraciones de los equipos.

- Checar configuración de VLAN'S. ya que está comprobado que estas se usan para brindar seguridad a la información, segmentar positivamente a los nodos de la red, e incluso agrupar usuarios de un mismo dominio sin importar su lugar físico (en caso de encontrarse en pisos separados o cuartos diferentes). Toda la configuración y esquema lógico recae un solo puerto del switch.

- La herramienta actualmente usada puede dar un monitoreo completo si es que se puede tener acceso a la configuración de los switch bajo los tres o alguno de los tres conceptos siguientes:

- Encaminar el tráfico Sflow hacia el monitor **ntop** para que este se encargue de hacer el análisis, dicho monitor deberá estar conectado directamente a la red asociada al tráfico (segmento de red).

- Encaminar el tráfico Netflow hacia el monitor **ntop** para que este se encargue de hacer el análisis, dicho monitor deberá estar conectado directamente a la red asociada al tráfico (segmento de red).

- Asignar y configurar un puerto de monitoreo, al cual se conectara directamente el servidor **ntop** para que se haga el análisis de tráfico en la red.

- Reasignar las listas de acceso (ACL –Access Control List) en los equipos ruteadores con la configuración adecuada a las necesidades de la red. Ya que las listas de acceso sirven para identificar el tráfico, y en un momento dado filtrarlo y así conseguir una mejor administración en el tráfico general de la red.

  Ya que de primera instancia las listas de acceso son controladas por el ruteador y están asignadas a sus interfaces, de igual manera debe checarse el buen funcionamiento operativo de los equipos y la correcta configuración de acuerdo a las necesidades lógicas y físicas de la red, pues con ello se ganara flexibilidad en los flujos de datos que salen y entran de estos dispositivos.

  Las listas de acceso no son más que políticas y reglas de aceptación o prohibición de flujos originados por los protocolos o direcciones IP de la red.

  Cuando un paquete llega a la interfaz, el dispositivo comprueba si hay ligado a él una ruta dentro de sus tablas de enrutamiento, si no la hay el paquete queda descartado. En caso de que se comience la gestión de envío.

- Reacondicionamiento de las rutas IP. Los ruteadores son un punto crucial, sobre este dispositivo se pueden hacer diferentes configuraciones, ya se hablo de las listas de acceso. Y su alcance no solo abarca negar o permitir flujos de tráfico, sino encaminar el tráfico priorizándolo según su destino o fuente. Asignándole un nivel o número de clase. Las rutas IP a las que tiene acceso y de las que tiene

conocimiento este tipo de dispositivos fungen como mapa y son de suma importancia en el buen funcionamiento y administración del tráfico general de la red. El administrador de red debe tener una visión amplia de las características que ocurren sobre su red, poniendo las rutas IP de manera estática (el administrador suministra la información de los caminos y la toma de decisiones. El mismo debe realizar la reasignación ante cualquier cambio o actualización de la configuración lógica y/o física de la red) o bien de manera dinámica que son las rutas que el dispositivo “aprende” a través de su interacción en el despliegue de la red y con otros dispositivos. Previamente por supuesto debe estar configurado el protocolo de enrutamiento y debidamente asegurado.

- Otra solución propuesta es, la conmutación de tráfico desde los switches[1]. Ya mencionamos que la red está distribuida en Vlans para telefonía IP. Esta medida no es para nada exagerada pues tiene beneficios aunque desgraciadamente desventajas. Dejando de lado esta configuración se puede anotar que en este tipo de dispositivos se puede hacer el monitoreo con un puerto dedicado y configurado para dicho propósito, es de gran importancia además corroborar la configuración y el buen funcionamiento de la red ya que el switch puede repartir el ancho de banda en cada segmento o en cada puerto o en cada usuario de ser necesario. Así que si se hiciera ese tipo de “conmutación” (con un buen aseguramiento, planeación y QoS) se podría eliminar la necesidad absoluta de una VLAN. Ya que los switches trabajan con el hardware desplegado en las redes, pueden ser tan rápidos como el medio lo sea. De esta manera se puede eliminar las colisiones redundantes en el reenvío de tráficos o el broadcast y por consiguiente liberar ancho de banda y eliminar retardos y latencia en la red por este tipo de problemas. Algunas ventajas de este esquema pueden ser:

    - ✓ Las comunicaciones dedicadas entre los host de la red, por medio de un dominio de colisión dedicado (libre de colisiones) incrementando la velocidad y fluidez en las transmisiones.

    - ✓ Adaptación a la velocidad que maneje el medio, respondiendo los dispositivos tan rápido como el medio lo permita.

    - ✓ Este tipo de dispositivos brinda la posibilidad de hacer la comunicación de manera full dúplex.

    - ✓ Los switch tienen circuitos virtuales que dan la capacidad de comunicación entre hosts aunque se encuentren bajo segmentos diferentes.

Después de emitir las recomendaciones, para la mejora continua a la red se presenta en este apartado las soluciones que se implantaron en el segmento de red.

Una vez hecha la investigación de topología, ingeniería de tráfico y otras características de la red, se ha notado que el centro de Formación e Innovación Educativa no cuenta con los elementos básicos de una buena administración de red. se ha optado por de características fundamentales como:

- Manuales de red. donde se concentra el estado operacional de la red, topología lógica, topología física o distribución física en el espacio del edificio, configuración de los equipos del sistema de red (clientes y servidores), capacidad de procesamiento etc.

- Bitácora de monitoreo. En donde se concentra toda la información recabada, a partir de ahí se podrá analizar, para después hacer la toma de decisiones. Puede ser en formato electrónico y con la información relevante hacer un concentrado impreso.

- Políticas generales de:

  - ✓ Seguridad.

  - ✓ Acceso.

  - ✓ Uso.

  Para todos los equipos que están contemplados dentro de este segmento de red, estas políticas a su vez han sido desglosadas para:

    - ✓ Usuarios.

    - ✓ Administradores.

    - ✓ Sistemas.

- Actualización de software y firmware. Actualización del sistema operativo y firmware de los equipos (si corresponde) se ha hecho también la actualización de software para los nodos que acceden a la red.

- Actualización de configuraciones en equipos de red como switch y ruteador, también de configuraciones en los nodos que acceden al sistema de red.

- Actualización física (reacomodo) de los nodos.

- Reasignación de las direcciones IP de los nodos que acceden a la red.

- Reasignación en el numeral que da servicio a la red telefónica IP que sirve al centro.

4.4. Análisis de resultados.

Despues de haber implantando el modelo con todas sus capas sobre la red del CFIE, se han hecho nuevas mediciones entre ellas de los flujos de tráfico que hay sobre la red LAN, WAN, mediciones de la calidad de la red y througput. Los mismos que reflejan una mejoria. La red se ha mantenido mas estable dando asi oportunidad de hacer un despliegue de calidad de los servicios ofrecidos por la red.

A continuacion se muestran los resultados desglozados por categorías.

4.4.1. Medición de calidad [2].

En la gráfica siguiente Figura 4.1 se puede observar que la red ha permanecido mas constante, lo cual ha podido asegurar que diferentes servicios funcionen sin retardos ni latencia. En este periodo de mediciones, despues de haber aplicado el modelo ya no se han experimentado pérdidas de paquetes asi que la red ha tenido un desempeño superior comparado con los resultados preliminares antes de la implementación de dicho modelo.

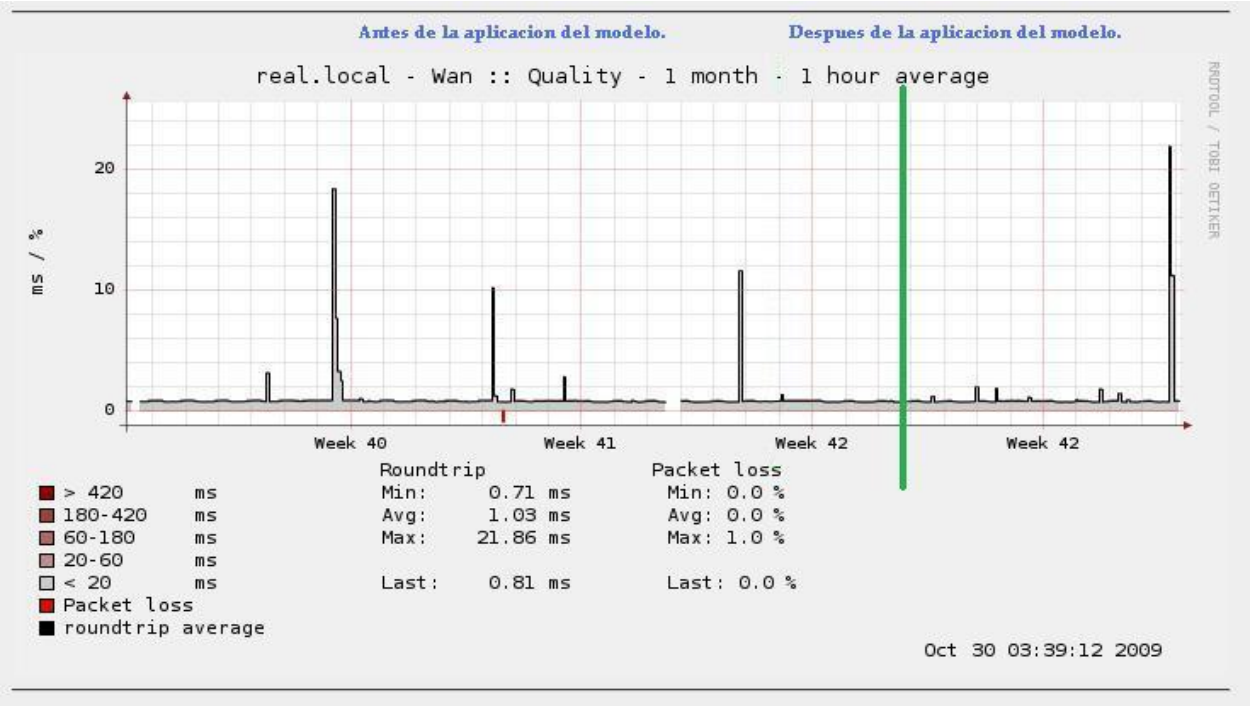


Figura 4.1 Resultado de mediciones de calidad.

4.4.2 Mediciones de Throughput.

Después de haber implementado el modelo y analizando la figura 4.2 se observa que el throuhput ahora tiene un nivel que puede denominarse constante, los flujos de datos a la salida se han visto beneficiados teniendo una mejoria en la transferencia de datos. En este periodo es donde se ha registrado el mejor pico a la salida que es de 58.01kb/s. además de permitir a la entrada picos significativamente buenos.

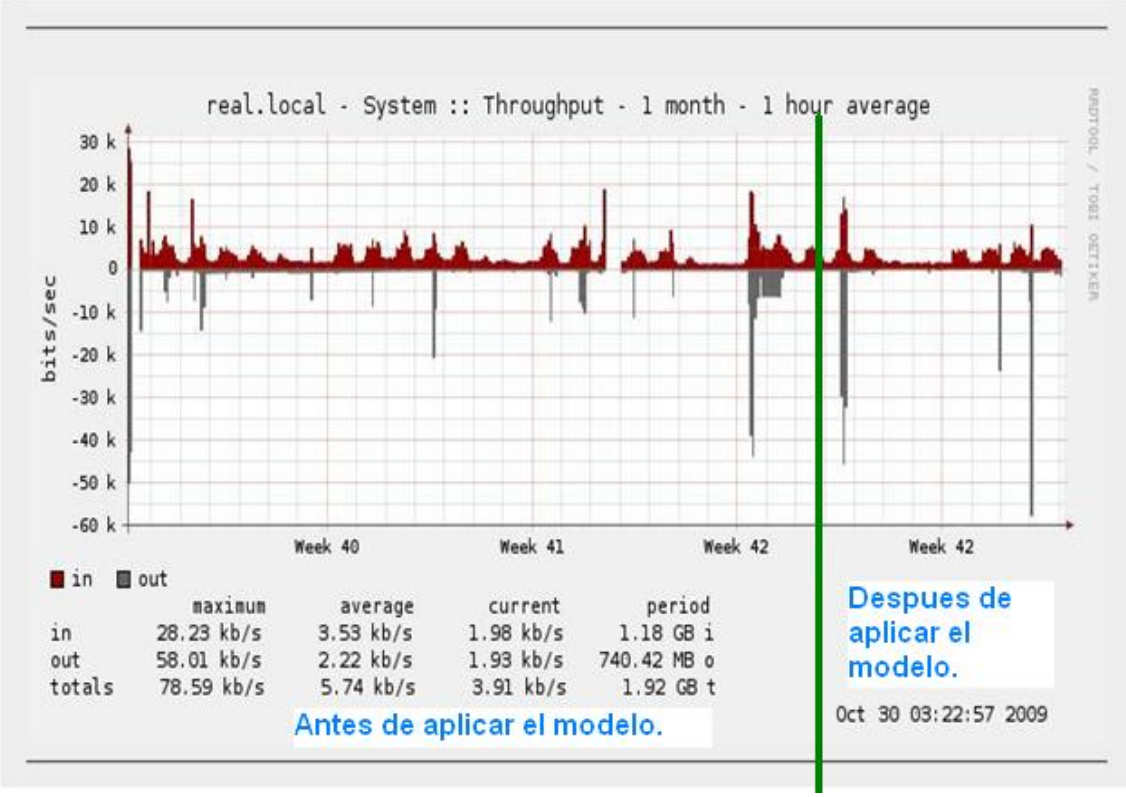


Figura 4.2. Medición de Throughput en la red.

4.4.3 Medición de tráfico de la red LAN.

Lo que se muestra a continuación en la figura 4.3 es el resultado de las mediciones sobre el segmento de la red LAN (interna) y su desempeño general. Se puede apreciar que la red tiene un comportamiento más estable y los picos que se muestran del lado de la salida de flujos son los máximos en el periodo de medición, lo cual indica una mejor transferencia de datos al exterior de la red lo cual desemboca en mejores comunicaciones.

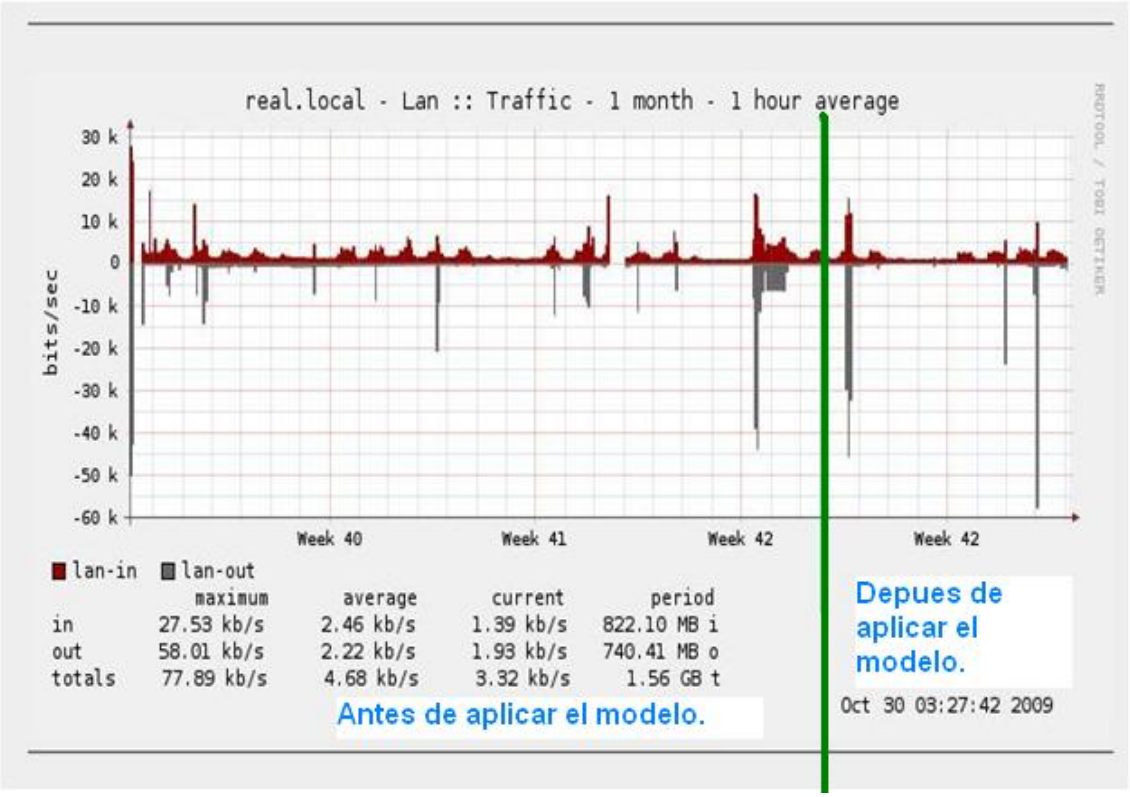


Figura 4.3. Medición de tráfico sobre la red LAN.

4.4.4. Medición de tráfico sobre la red WAN.

Los resultados obtenidos después de analizar el tráfico generado a través de la interface de servicio WAN. Se ve reflejado que hay una buena conectividad una probabilidad grande de realizar las conexiones desde internet hacia los servicios que presta la red, por mencionar algunos servicios que hacen uso de este flujo y servicios de red son los foros que tiene a su cargo el CFIE. Y algunos cursos en línea.

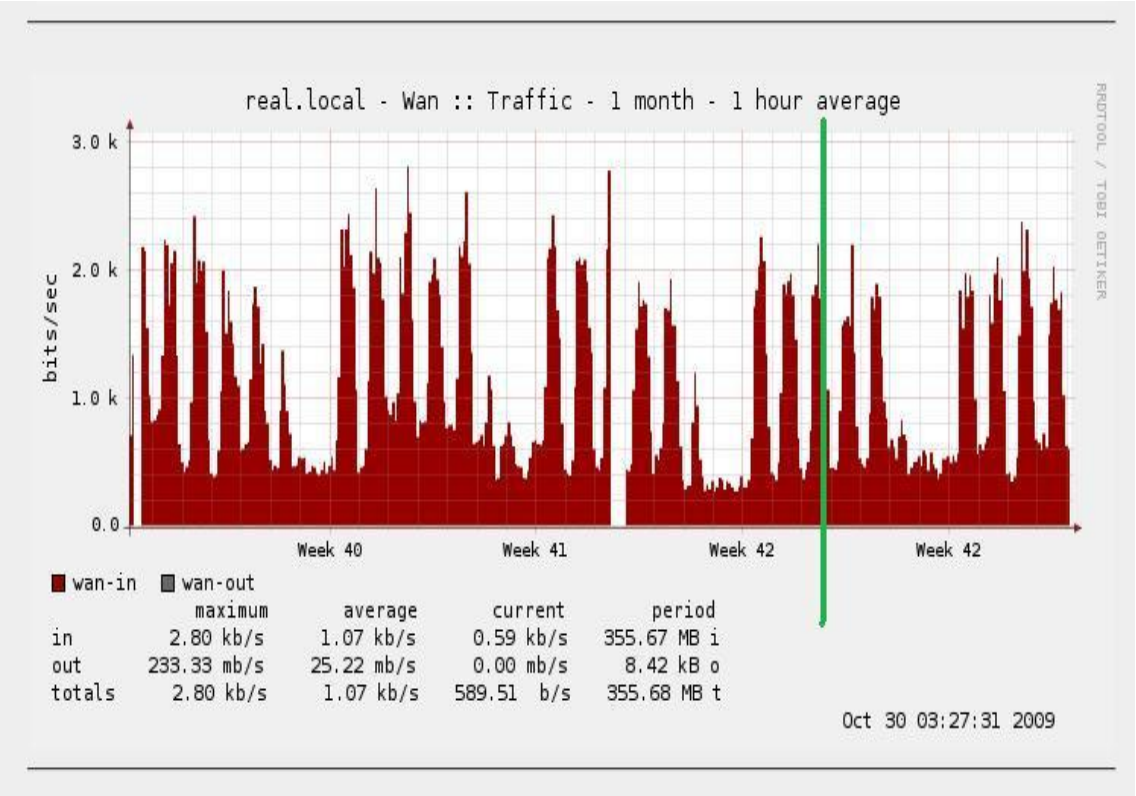


Figura 4.4 Medición de tráfico en la red WAN.

4.4.5. Medición de ocupación de la red por flujos y datos originados por protocolos [3].

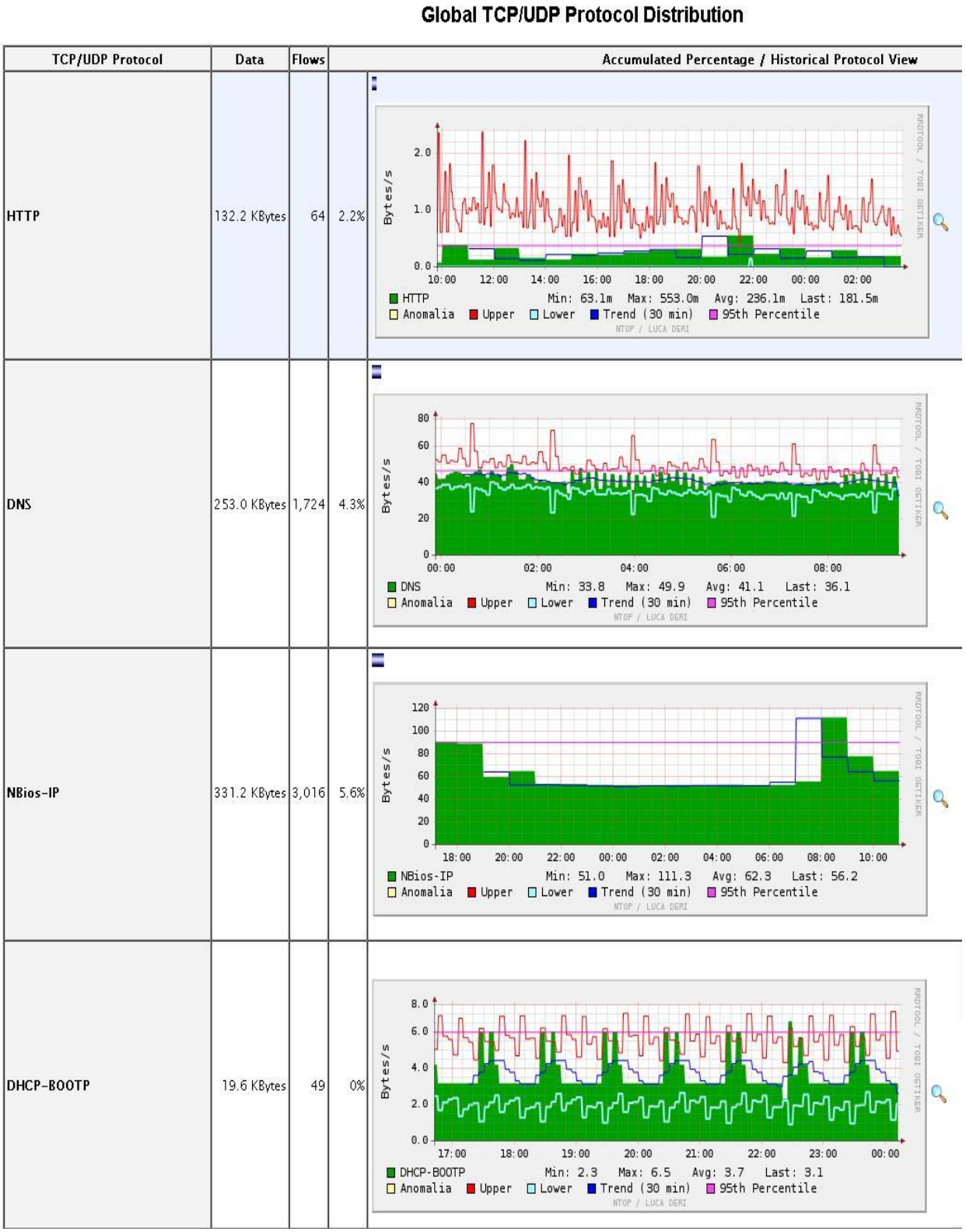


Figura 4.5. Resultados después de la implementación del modelo. Protocolos y flujos de datos.

4.5. Comparativa con mediciones anteriores.

En este apartado se muestran las comparativas de los resultados obtenidos después de implementar el modelo contra los resultados antes de la implementación.

La única simbología que hay nueva en las gráficas es una línea que hace la función de distinguir entre los resultados del proceso de monitoreo antes y después del modelo.

1. Comenzando con el throughput. Figura 4.6. Donde se muestran características como:

- Se ha mantenido un nivel constante de throughput después de la implementación del modelo.
- El pico más alto se registro dentro de este periodo.

La importancia de haber aumentado el promedio de throughput y mantenerlo constante se refleja en que el nivel de volumen de información que ha transitado por la red ha sido procesada de manera oportuna. Haciendo que los servicios y red en general presenten un mejor funcionamiento

Figura 4.6. Comparativa de throughput antes y después de la arquitectura QoS.

2. Paquetes Ethernet.

La comunicación por medio de la tecnología Ethernet de igual forma se ha estabilizado, esto se interpreta como que los flujos que transitan en la red han viajado de manera ordenada permitiendo que las comunicaciones y servicios tengan una mejor fluidez. Si bien antes del modelo se registraron los picos más altos. También antes estaba presente la latencia comunicación y ello propiciaba la pérdida de paquetes además del envío y reenvío de tráfico nocivo a la red. Ver figura 4.7 y 4.8.

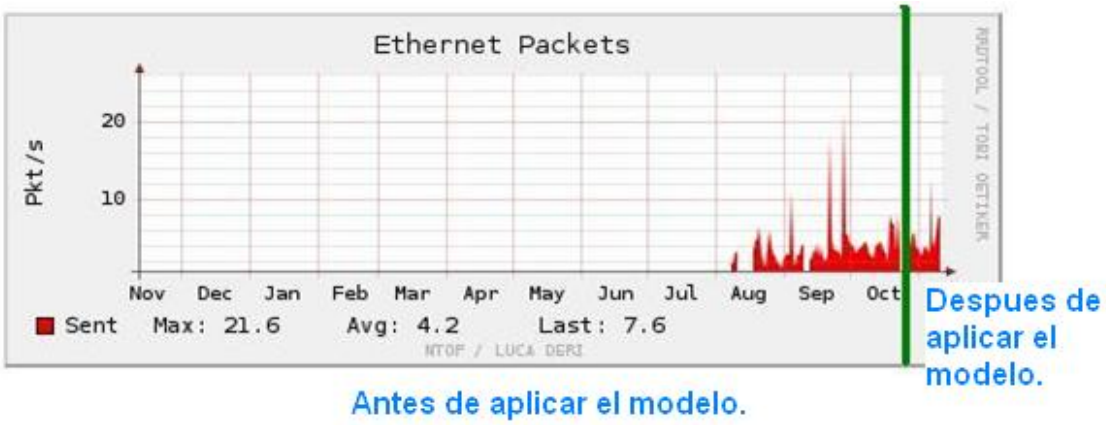


Figura 4.7. Comparativa de paquetes Ethernet antes y después de la arquitectura QoS.

En la siguiente gráfica 4.8 se muestra el desglose que de los diferentes tamaños de flujo detectados en tránsito sobre la red, se puede ver que han permanecido constantes, en algunos casos como el de paquetes mayores a 1518 los picos son mayores después de implementar el modelo. Lo cual habla de que el tráfico es tratado de mejor forma permitiendo una mejor comunicación y fluidez en la red.

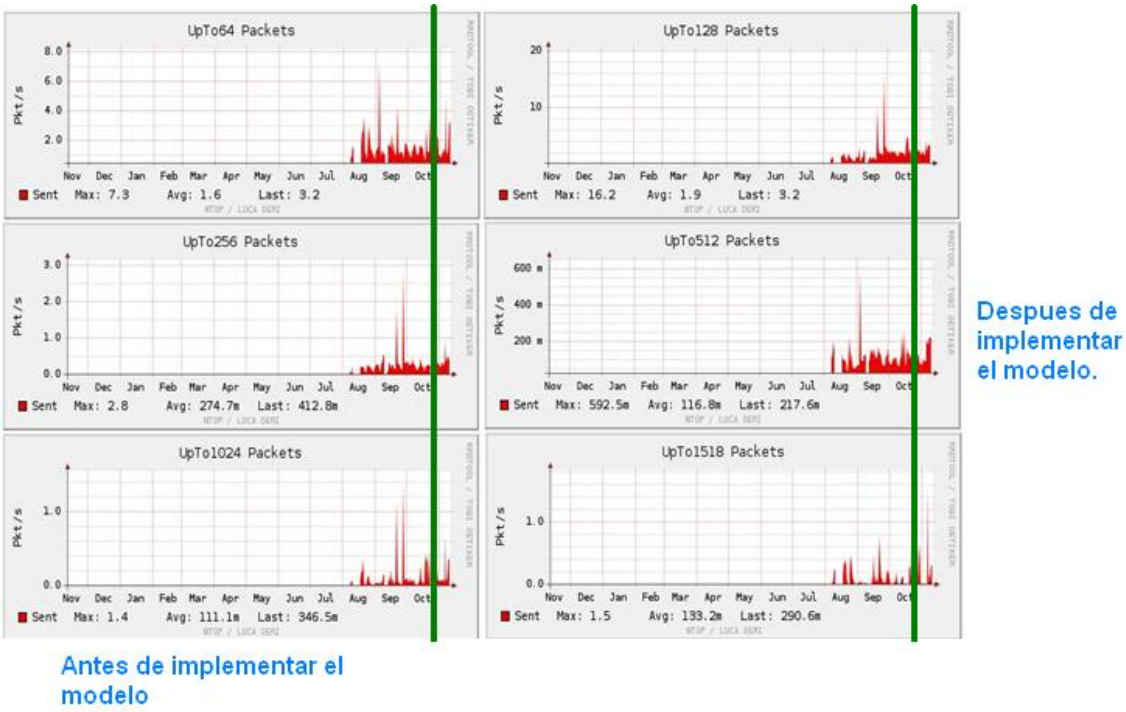


Figura 4.8. Comparativa de paquetes Ethernet (desglose de tamaño de flujos) antes y después de la arquitectura QoS.

3. Paquetes broadcast.

Los paquetes broadcast han disminuido y se han mantenido, como en los ejemplos anteriores. La disminución los paquetes broadcast refleja que la resolución la búsqueda interna de equipos para la comunicación se ha mejorado.

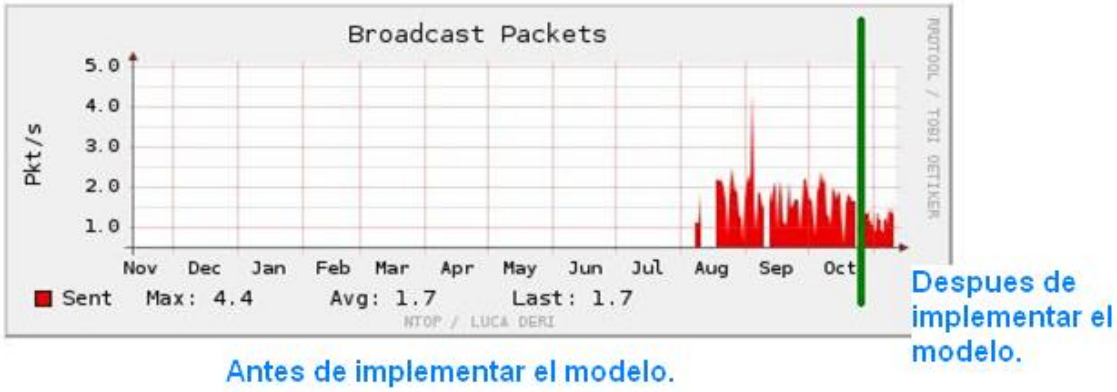


Figura 4.9. Comparativa de paquetes Broadcast antes y después de la arquitectura QoS.

4. Ocupación de la red.

El sistema de red que se encuentra desplegado dentro del CFIE, tiene los picos que se observan en la figura 4.9 debido a que presta servicio a usuarios esporádicos ya que llegan a congresos. Por tanto se puede observar un poco variable pero los usuarios que laboran en sus instalaciones y son constantes la mantienen en un nivel promedio constante, esto indica que las mediciones son correctas pues en general se tiene la misma ocupación de red, y no están arrojando resultados alentadores debido al menor uso o a que se ha discriminado a usuarios esporádicos.

Figura 4.10. Comparativa del nivel de ocupación de la red antes y después de la arquitectura QoS.

5. Tráfico IP.

El tráfico IP estudiado en esta sección ha disminuido, esto garantiza que las comunicaciones han tenido un mejor desempeño y no ha sido necesario inyectar tráfico redundante, se puede agregar que el tráfico ha sido únicamente el indispensable para cumplir con la sana comunicación de paquetes. Se puede ver en la gráfica 4.10 que es más estable respecto a las mediciones anteriores y que los picos de uso de este tipo de tráfico son más pequeños.

Figura 4.11. Comparativa del nivel de tráfico IP en la red antes y después de la arquitectura QoS.

Se hace un desglose en las dirección que fluye el tráfico figura 4.12, local – local, local – remoto, remoto – remoto. Estos se ven claramente beneficiados ya que el tráfico ha disminuido, lo cual permite que se tenga una mayor ocupación de la red. Se puede interpretar además como que las comunicaciones están funcionando de manera oportuna, fluida y concreta.

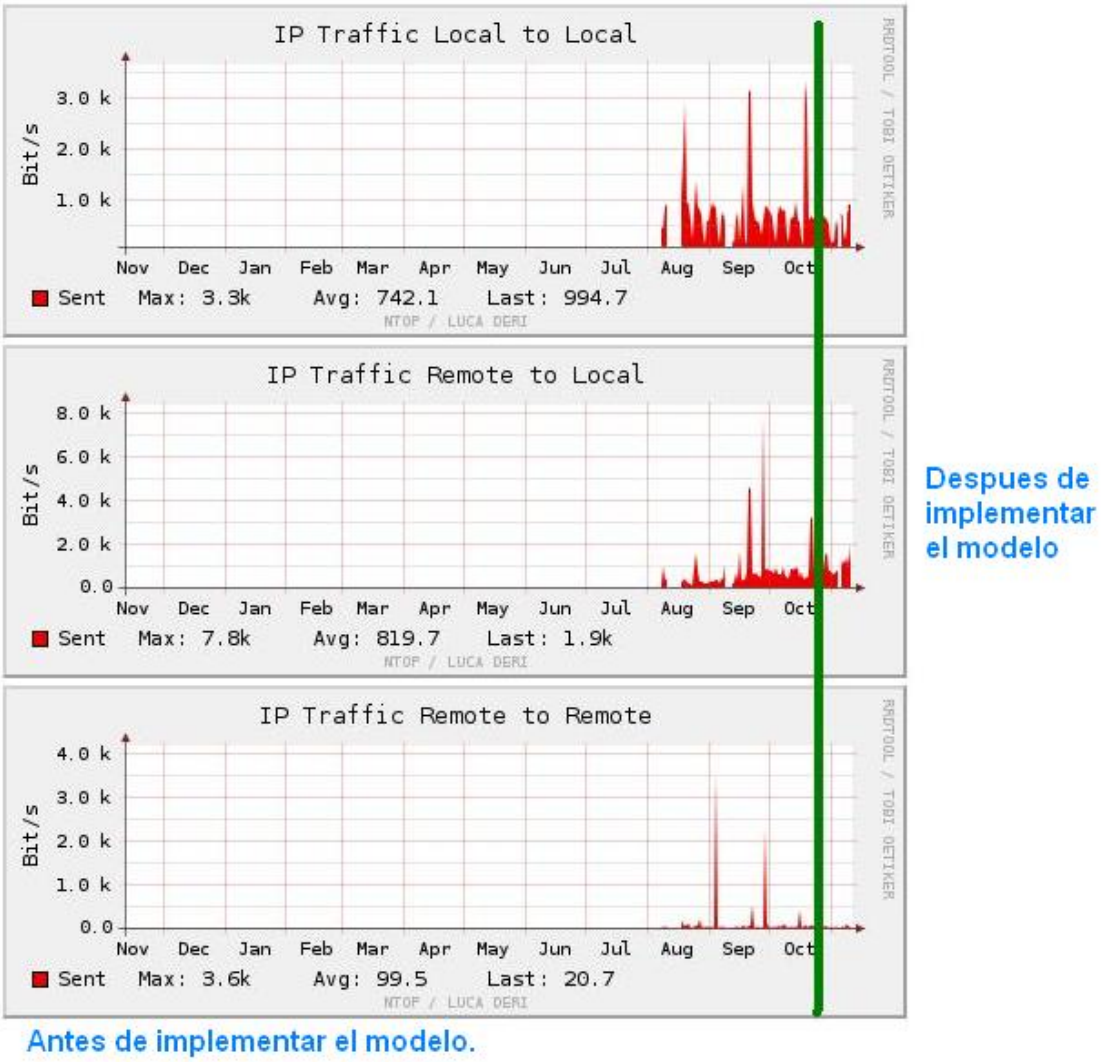


Figura 4.12. Comparativa del nivel de tráfico IP (desglose de dirección de flujos) en la red antes y después del modelo de calidad.

6. Clasificación de flujos de paquetes.

Se ha encontrado que al implementar la el modelo de calidad se ha podido realizar una mejor clasificación en los flujos que viajan sobre la red. Haciendo distinción en los paquetes con los flujos de tráfico TCP, UDP y dejando una menor cantidad de flujos sin clasificar. Como se muestra en la figura 4.12. la distinción entre flujos de tráfico orientados a conexión (TCP) y los no orientados a conexión (UDP) se han mantenido sobre un promedio. En contraste la tasa de flujos ARP ha disminuido, lo que concuerda con las conclusiones de que esto beneficia a la comunicación y la conectividad de la red realzando el desempeño general de la red.

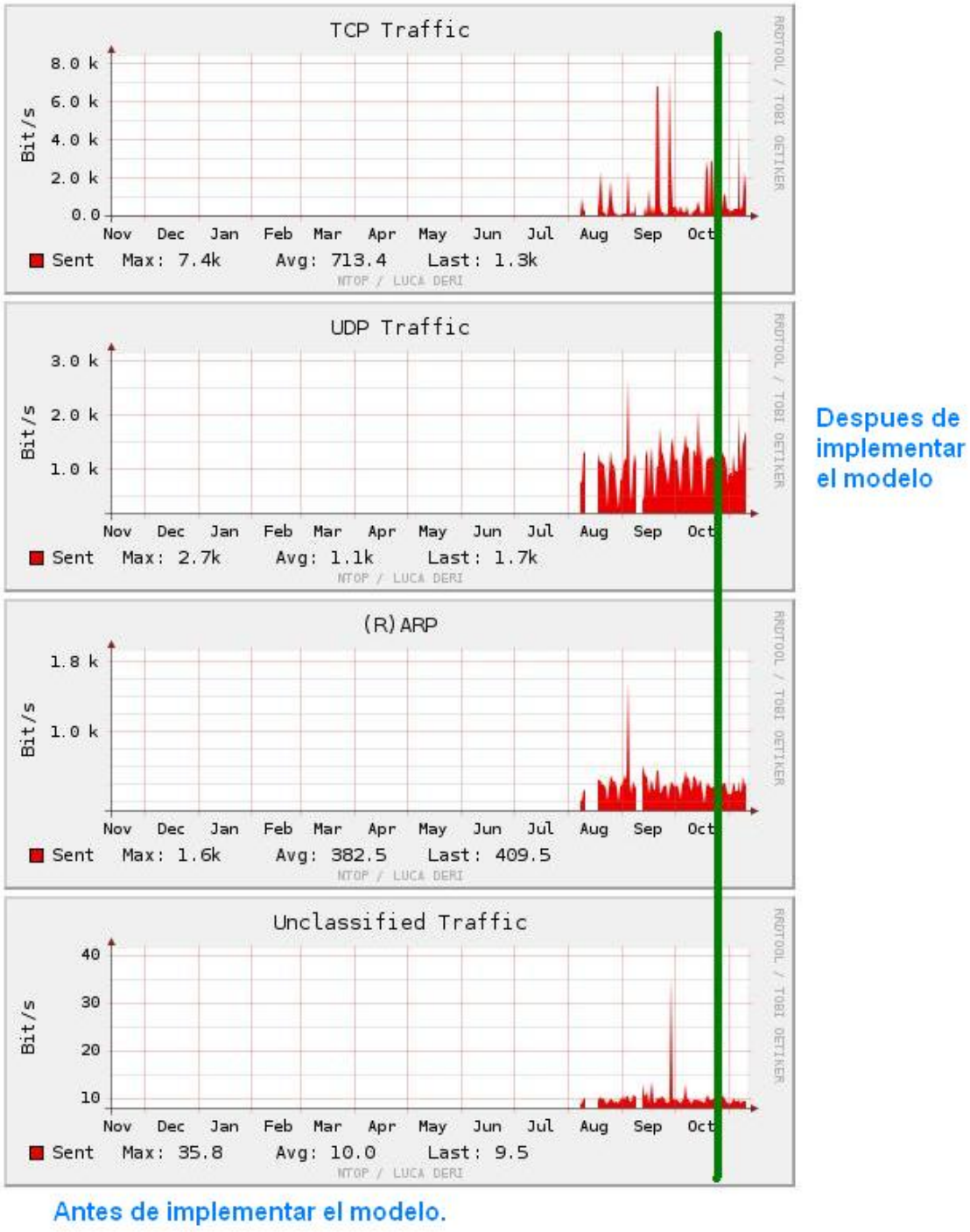


Figura 4.13. Comparativa de clasificación de flujos de tráfico en la red antes y después implementar el modelo de calidad.

7. Servicios.

Los servicios se han visto beneficiados con la implementación del modelo de calidad. Figura 4.14 Por mencionar algunos, los flujos HTTP (o navegación web) han sido realzados, y mantenidos constantes. Otros servicios importantes como la comunicación mail han heredado la misma suerte gracias a la implantación de del modelo que ha dejado tras de sí arquitectura que se comporta de manera funcional. Y los flujos de VoIP se han podido notar con mayor frecuencia y dentro de un promedio. Hay que agregar que los flujos dañinos se han disminuido y algunos desaparecido casi por completo, tal es el caso de los flujos de servicios que absorben gran ancho de banda y que institucionalmente están prohibidos como son las descargas P2P como **Kazaa** o redes basadas en **torrents**.

El SSH (secure Shell o Shell segura) es flujo de origen remoto y de entrada hacia los sistemas. Este tipo de flujo se utiliza para hacer un túnel seguro y prácticamente se puede obtener control total del sistema en cuestión, si puede ser vulnerado, normalmente los atacantes buscan autenticarse para poder desestabilizar la seguridad completa del sistema de red. Obtener privilegios sobre las configuraciones o tirar los servicios. En los servidores de pruebas el tráfico SSH se puede entender como ataques explícitos hacia los servidores. Debido a esto, se ha reforzado la seguridad para prevenir dichos ataques, y por lo tanto los flujos SSH han disminuido notoriamente. No se han eliminado puesto que es un servicio necesario y desplegado para algunos usuarios de la red, ante esto no se puede ser tajante y cerrar puertos (por defecto el protocolo SSH corre sobre el puerto 22). Así que por esto no se puede controlar el flujo entrante de manera directa.

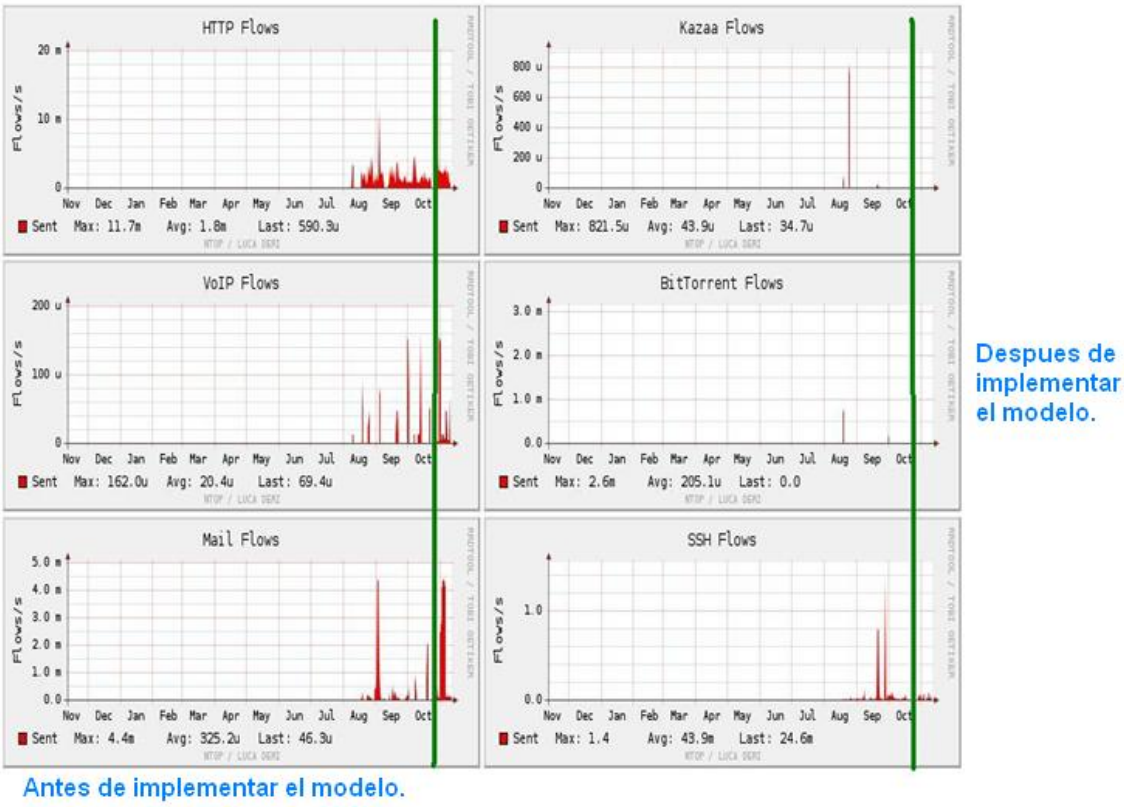


Figura 4.14. Comparativa entre el desempeño de servicios antes y después implementar el modelo de calidad.

4.5 Conclusiones.

Después de la implantación del modelo sobre el sistema de red en el segmento de CFIE, se ha concluido que el sistema de red tenia aproximadamente a un 60% de estabilidad antes de la implementación del modelo, después de la implementación se ha ganado aproximadamente un 15% extra. Las cifras anteriores son hechas en base a la apreciación del administrador del segmento de la red, en conjunto con la de los autores de este trabajo. Tomando en consideración los estudios, las pruebas y la interpretación de los resultados obtenidos.

En las mediciones realizadas después de la implantación del Modelo se notó mejoría pero se requiere tomar otras acciones de mejora continua lo cual es parte del modelo.

Monitoreo constante y la realización de una bitácora donde se almacenan las graficas y los datos recopilados, para hacer el trazado de los planes y verificar que se han cumplido los objetivos propuestos en las fases previas del modelo.

Es además importante el monitoreo ya que si es detectada alguna anomalía ya sea en el monitoreo en tiempo real o a través del histórico, se podrán tomar acciones de manera inmediata y de forma regular hasta componer este hecho.

De acuerdo a los resultados obtenidos por el modelo, se puede prever que se puede incrementar la tasa de mejora en la calidad de los servicios entre más tiempo se encuentre implantado el Modelo, ya que hay muestras claras de la mejora de la red y un aumento favorable pero gradual en cuestiones de servicios. Incluso un factor muy relativo como lo es la percepción de los usuarios ha sido mejorado con comentarios buenos acerca del desempeño actual de la red de CFIE.

Referencias.

[1] Redes cisco guía de estudio para certificación CCNA 640-802. Ernesto Ariganello. Editorial Alfaomega. ISBN 978-970-15-1546-6.

En Internet.

[2] http://www.pfsense.com/

[3] http://www.ntop.org/ntop-man.html

Conclusiones y trabajo futuro.

RESUMEN:

En este capítulo se hace el análisis de los resultados, tras implementar las primeras etapas del modelo (ahora ya es una arquitectura), así como la caracterización y propuesta de las etapas siguientes del modelo, las cuales son desarrollo e implementación de mejoras, comparación de resultados etc.

OBJETIVOS DEL CAPITULO:

- Mostrar que el modelo es ya una arquitectura implementada.
- Mostrar los resultados tras implementar el modelo.
- Hacer el análisis de resultados y proponer mejoras.
- Proponer trabajos futuros.

5.1 Conclusiones.

La calidad en el servicio no es solo una técnica de restricción de ancho de banda, involucra la planeación y estudio de la red.

La calidad en el servicio y su aseguramiento significa cosas diferentes para personas diferentes, según el modelo y capacidades del sistema de red, por ello es importante que los modelos a implementar sean adaptativos, flexibles y robustos. No obstante hay parámetros preestablecidos por los organismos reguladores internacionales especializados en la materia.

El modelo propuesto en el presente trabajo como se pudo apreciar consta de seis capas de estructuradas para dar continuidad una después de la otra, lo que significa que se deben implementar de manera gradual y la anterior le dará información de inicio a la capa subsecuente. De esta manera surge el concepto de sistema cíclico, la capa número seis de nueva cuenta proporcionará información a la capa uno, el proceso de mejora continua volverla a su fase inicial para sí poder optimizar la red aun mas y corregir imperfecciones que hayan surgido en el proceso anterior, o inclusive aplicar cambios que beneficien el desempeño general de la red.

5.1.1. Ventajas.

Las ventajas de este modelo sobre los modelos ya existentes se comentan a continuación:

- **Modelo de lo General a lo Específico:**
  Mencionar esta parte de lo general hasta lo específico, dado que se está proponiendo hacer estudios de la red hasta lograr que dicho estudio sea puntual, debido a que se hacen estudios y caracterizaciones de los componentes importantes de la red. Y se conozcan sus fortalezas y debilidades.

- **Aseguramiento de la calidad en base a su funcionalidad:**
  Al final, y como se pudo demostrar será posible asegurar QoS comprobando la funcionalidad del modelo y de la red, siempre que sea implementado de la manera sugerida. Cumpliendo el objetivo de hacer una arquitectura robusta.

- **Basado en estándares:**
  Otra ventaja es que se han tomado de algunos conceptos clave de modelos ya existentes como son DiffServ, IntServ, o MPLS y que aportan características que enriquecen a la funcionalidad de este modelo y que son compatibles entre sí. Se habla de características como la clasificación de garantías, el marcado de paquetes, o inclusive la sectorización y jerarquía de flujos, servicios y usuarios. A su vez esos modelos están basados en diferentes estándares emitidos por organismos reguladores internacionales.

- El equipo físico es capaz de soportarlo.
  Para este caso de estudio particular se tuvo la ventaja extra de que el hardware y en general el sistema de red estaba preparado para soportar todas las fases del modelo. Se puede apreciar en las características del equipo físico que incluso tiene soporte ya específico para QoS.

- Sencillo de implantar.
  En términos generales este es un modelo tecnológicamente sencillo. Y por lo mismo es muy fácil implementar ya que viene integrado en pocas etapas y es estructurado porque cada etapa da pauta a la siguiente, haciendo posible así su implementación final.

- Adaptable a diferentes entornos.
  Este modelo puede implementarse no solo en sistemas de red parecidos al caso de estudio en cuestión sino en estudios por demás diferentes incluso si el hardware no tiene soporte explicito para QoS.

- Mejora continua por etapas, procesos de planeación y evaluación.
  El modelo puede ofrecer un proceso de mejora continua, y después de hacer la implantación sobre el sistema de red, se puede seguir mejorando el desempeño ya que permite gradualmente aumentar hasta obtener niveles realmente altos en relación a los beneficios que el sistema puede ofrecer.

5.1.2. Desventajas.

- Algunas de las desventajas encontradas en el modelo, son que la implementación requiere de cierto nivel de especialidad en el administrador de red pues hacer los análisis e interpretaciones de los resultados no es sencillo.

- Hacer todo el proceso de caracterización de red; lo que refiere al reconocimiento de la red, caracterización de servicios, o una planeación de las necesidades y oportunidades que hay en el sistema de red, hacer la optimización de recursos y el desarrollo de mejoras. Caracterización de flujo o lo correspondiente a la ingeniería de tráfico.

- Hacer la implementación de la estructura completa del modelo lleva tiempo, al final no es desperdicio o pérdida pues se ha comprobado que el modelo es funcional pero, no es un modelo que arroje resultados contundentes a corto plazo.

- El modelo es cíclico y no es autónomo, siempre se va a requerir de alguien que haga el análisis de resultados, la administración del modelo, sus capas, se haga cargo de la red, toma de decisiones, planeación e implementación de mejoras.

5.1.3. Trabajo a Futuro.

El modelo presentado a lo largo de este trabajo de investigación aun es perfectible. Aunque se han obtenido resultados favorables hay cosas que pasan por encima de las capas y estructuras que este modelo propone tal como un superior jerárquico al que se tenga que pedir autorización para hacer implementaciones pensadas y diseñadas a través de estudios y caracterizaciones fuertes tal como la ingeniería de tráfico.

Lo ideal sería hacer un hibrido entre hardware y software especializado en el aseguramiento de la calidad en los servicios. Como propuesta se puede emitir un agente dotado de inteligencia y toma de decisiones capaz de amortizar los efectos negativos de la red. Caídas o contingencias de consumo de ancho de banda y tráfico. Dicho agente deberá negociar con el hardware las mejores políticas de decisión para que la red sea funcional. Aun con todo esto, no escapa del monitoreo pues como se ha expuesto anteriormente, un sistema de

red no es un sistema sin ley, o sin reglas. Mucho menos si el objetivo es implementar y asegurar QoS. Agregando que es una recomendación ya que la arquitectura ha funcionado, siendo una opción viable.

Desarrollar un sistema autónomo es un trabajo que llevara mucho tiempo pero es alcanzable, y es una mezcla de diferentes campos de la ingeniería integrando disciplinas como la ingeniería de software, ingeniería de sistemas, inteligencia artificial etc. Haciendo la interconexión hasta fundirla en un solo producto que finalmente será capaz de hacer la toma de decisiones y mantener la red en un estado optimo. En el mejor de los casos un proyecto donde el resultado sea libre de mantenimiento y supervisión o el menor posible.

Hasta ahora se ha propuesto que el modelo cuente con cierto grado de flexibilidad ante cambios inesperados, y plantea también basarse en los estándares y recomendaciones de organismos reguladores, aun con esas características falta que el modelo tenga de algún modo capacidad de adaptarse a los estándares de calidad que vayan surgiendo con el paso del tiempo, pues la tecnología avanza de manera constante y con una mirada atrás podemos darnos cuenta que los cambios han sido radicales en muy poco tiempo.

5.1.4. Comparativa con otras soluciones de calidad.

	IntServ	MPLS	Solución – Calidad
Fácil implementación	medio	no	medio
Fácil mantenimiento	si	no	medio
Desempeño	medio	Alto	Alto
costoso	No	Si	No
Automático	Medio	si	no
Necesidades tecnológicas	si	si	no
Especialización de administrador	si	Si	si

Figura 5.1. Comparativa con otros modelos calidad.

La propuesta de solución a base del modelo para asegurar calidad, tiene un nivel de complejidad de implementación medio, ya que lleva tiempo y en base al estado del sistema de red en donde se implemente depende el tiempo que tomara para asegurar calidad, así como el número de ciclos antes de ver resultados. De acuerdo al análisis de los demás modelos, empata el nivel de complejidad en la implementación con una solución basada en Diffserv, pero tiene una menor complejidad de implementación que MPLS.

Tiene un nivel de mantenimiento calificado como medio, ya que se necesitan hacer iteraciones en la implementación, colecta y análisis de información y toma de decisiones. En este punto es superado pro Diffserv ya que este tipo de solución una vez configurada es casi libre de mantenimiento salvo actualizaciones y fallas no contempladas. En comparación con una solución MPLS que requiere una configuración exhaustiva y mantenimiento cada vez que se reconocen nuevas directrices en el manejo del trafico o usuarios.

El modelo de calidad propuesto, tiene un alto desempeño, aunque es a largo plazo. Después de implementarlo cíclicamente y con la mejora continua ofrecida, se pueden corregir diversas clases de errores detectados en los sistemas de red, desde mala administración hasta errores técnicos. El modelo diffserv, en cambio ofrece un desempeño medio ya que necesita combinarse con otras técnicas y métodos para garantizar una optima manera de obtener calidad. El modelo MPLS también tiene un desempeño elevado, pero requiere de características específicas para poder funcionar de manera óptima y entregar mejores resultados.

Este modelo de calidad, no es costoso ya que trabaja con el equipo que existe sobre el sistema de red, se basa más bien en técnicas y métodos para que el desempeño de red, y no en harware o software especifico. El modelo Difsserv, no es costoso ya que los equipos necesarios no son tan caros, de cierta manera combina el hardware y con algunas técnicas de QoS para asegurar el desempeño de la red. Sin embargo el modelo MPLS si es caro, es una tecnología de punta basado en configuraciones y hardware especifico, de ahí su elevado costo.

Lamentablemente este modelo no es automático, necesita de un administrador que dirija los análisis, interprete los resultados y tome decisiones, no asi el modelo Diffserv aunque no es completamente automático tiene un nivel medio pues no requiere de tanta atención por parte del administrador del sistema. Una ventaja que presenta MPLS sobre las dos soluciones de calidad anteriores, es que MPLS si es automático, salvo la primera configuración y las actualizaciones en la mismas.

Otra ventaja que presenta este modelo de calidad sobre diffserv y MPLS es que no tiene necesidades tecnológicas específicas, de ahí la importancia de que sea flexible y estándar.

El nivel de especialización del administrador de la red para este modelo debe ser alto, pues debe enfrentarse a problemas propios de los sistemas de red. o la configuración de los equipos, debe tener noción y conocimiento del funcionamiento de los equipos y nodos que existen sobre el sistema de red. de igual manera para administrar las soluciones basadas en Diffserv y MPLS se requiere de un nivel de especialización alto para estos modelos de solución de calidad, ya que trabajan con señalización, configuración y equipos específicos.

5.1.5. Consideraciones finales.

El desarrollo del presente trabajo permitió poner en práctica los conocimientos adquiridos dentro de las aulas de clases bajo la tutela de experimentados catedráticos. En especial en los tópicos de redes de computadoras, planeación de redes de computadoras, administración de las redes etc.

Así como también permitió desarrollar y profundizar en las capacidades de investigación y redacción de proyectos tecnológicos y científicos.

Sobre la etapa final de redacción de este trabajo, se ha notado la similitud con otro tipo de modelo de calidad como es ITIL, ya que de primera instancia en los objetivos de este trabajo estaba contemplado asegurar calidad en los servicios en una red convergente, tomando como objetivo de investigación y desarrollo de pruebas un ambiente educativo, no se ha podido profundizar en comprar con este tipo de modelo pero se agrega en el apartado de anexos una breve reseña de lo que es ITIL, así pretendiendo dejar un antecedente para que sea un posible teoría u objetivo de comparación.

Anexos.

RESUMEN:

En la sección de anexos se presentan algunos documentos complementarios a este trabajo.

OBJETIVOS DEL CAPITULO:

- Complementar la información expuesta a lo largo del trabajo de tesis.
- Mostrar algunos productos derivados de este trabajo.

Anexo 1. Recomendación Y.1540 de la ITU.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T Y.1540

(12/2002)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN Y ASPECTOS DEL PROTOCOLO INTERNET

Aspectos del protocolo Internet – Calidad de servicio y características de red

Servicio de comunicación de datos con protocolo Internet – Parámetros de calidad de funcionamiento relativos a la disponibilidad y la transferencia de paquetes del protocolo Internet

Recomendación UIT-T Y.1540

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN Y ASPECTOS DEL PROTOCOLO INTERNET

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	**Y.1500–Y.1599**
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T Y.1540

Servicio de comunicación de datos con protocolo Internet – Parámetros de calidad de funcionamiento relativos a la disponibilidad y la transferencia de paquetes del protocolo Internet

Resumen

Esta Recomendación define parámetros que se pueden utilizar para especificar y evaluar la calidad de funcionamiento en cuanto a velocidad, exactitud, seguridad de funcionamiento y disponibilidad de la transferencia de paquetes IP del servicio de comunicación de datos con protocolo Internet (IP). Los parámetros definidos se aplican al servicio IP de extremo a extremo, punto a punto, y a tramos de la red que proporcionan, o contribuyen, a la prestación de ese servicio de conformidad con las referencias normativas especificadas en la cláusula 2. El transporte sin conexión es un aspecto diferenciador del servicio IP que se considera en la presente Recomendación.

Orígenes

La Recomendación UIT-T Y.1540, preparada por la Comisión de Estudio 13 (2001-2004) del UIT-T, fue aprobada por el procedimiento de la Resolución 1 de la AMNT el 14 de diciembre de 2002.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB.

ÍNDICE

Página

Anexo 2. Recomendación Y.1541 emitida por la ITU.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T Y.1541

(05/2002)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN Y ASPECTOS DEL PROTOCOLO INTERNET

Aspectos del protocolo Internet – Calidad de servicio y características de red

Objetivos de calidad de funcionamiento de red para servicios basados en el protocolo Internet

Recomendación UIT-T Y.1541

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN Y ASPECTOS DEL PROTOCOLO INTERNET

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	**Y.1500–Y.1599**
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T Y.1541

Objetivos de calidad de funcionamiento de red para servicios basados en el protocolo Internet

Resumen

En esta Recomendación se definen las clases de calidad de servicio de la red (QoS), y se especifican unos objetivos provisionales para los parámetros de calidad de funcionamiento de redes con protocolo Internet. Estas clases tienen por objetivo establecer las bases para los acuerdos entre los proveedores de servicios de red, y entre los usuarios de extremo y sus proveedores de servicios de red.

En el apéndice I se indica cómo podría el ATM soportar la calidad de funcionamiento en la capa IP. En el apéndice II se discuten alternativas para definir la variación del retardo IP. El contenido del apéndice II se incorporará probablemente a la Rec. UIT-T Y.1540. En el apéndice III se presentan los trayectos de referencia ficticios con los que se probó la factibilidad de los objetivos de QoS Y.1541. En el apéndice IV se dan ejemplos de cálculo de la variación del retardo de los paquetes. En el apéndice V se discuten los temas que se deben considerar siempre que se efectúen mediciones de IP. En el apéndice VI se describe la relación entre esta Recomendación y el mecanismo definido por el IETF para la gestión de QoS. En el apéndice VII se discute el objetivo del retardo de transferencia de los paquetes y su relación con otras Recomendaciones. En el apéndice VIII se presenta una bibliografía. En el apéndice IX se discuten las aplicaciones potenciales de las redes IP.

Orígenes

La Recomendación UIT-T Y.1541, preparada por la Comisión de Estudio 13 (2001-2004) del UIT-T, fue aprobada por el procedimiento de la Resolución 1 de la AMNT el 7 de mayo de 2002.

ÍNDICE

Página

Anexo 3. Reseña del modelo ITIL.

ITIL. Information Technology Infrastructure Library. Infraestructura de Librerías de Tecnologías de Información. Es la organización internacional que gestiona el marco que describe las "buenas prácticas" para la gestión de servicios IT. El compendio de ITIL evolucionó a partir de los esfuerzos del gobierno Inglés durante la década de 1980 para documentar el éxito que se acercó a las organizaciones de gestión de servicios. En la década de 1990 se había producido una gran colección de libros de documentación de las "mejores prácticas" para la gestión de servicios IT. Esta biblioteca fue la que finalmente se denominó la IT Infrastructure Library. La Oficina de Comercio del Gobierno Inglés sigue funcionando como el propietario de la marca de ITIL ®.

ITIL ® ha pasado por varias evoluciones y se ha renovado con el lanzamiento de la versión 3 en 2007. A través de estas evoluciones del ámbito de aplicación de prácticas documentadas ha aumentado con el fin de mantenerse al día con la madurez continua de la industria de TI y satisfacer las necesidades y exigencias de la comunidad de profesionales que manejan TI. ITSM (IT Service Management)

ITIL ® es sólo una de muchas fuentes para las mejores prácticas, incluyendo las que están documentadas por:

• Marcos Pública (ITIL ®, COBIT, CMMI, etc.)

• Normas (ISO 20000, BS 15000).

• El conocimiento de propiedad de organizaciones e individuos.

En general, las mejores prácticas son las que formaliza como consecuencia de su éxito en la amplia utilización de la industria.

El modelo ITIL toma como base la de definición de servicio como:

"un medio de entregar valor a los clientes, facilitando los resultados que quieren obtener sin los adjudicarle costos o riesgos específicos".

Tomando en cuenta una perspectiva orientada a servicios, se deberá tomar en cuenta:

• La comunicación con clientes y usuarios finales se debe mantener de manera eficaz.

• Se deben mantener tiempos de resolución adecuados para el usuario final y las consultas de los clientes.

• Se debe mantener la transparencia en la organización, así como el gasto de recursos económicos.

• La organización de TI debe trabajar de forma proactiva para identificar los problemas potenciales que se deben corregir o acciones de mejora que se podrían implementar.

A través de cinco los volúmenes se componente la propuesta del modelo ITIL. (Version 3):

• Service Strategy. Estrategia de servicios.
Se refiere fundamentalmente al desarrollo de capacidades para la Gestión de Servicios, estas prácticas permiten (junto con la organización de TI en general) convertirse en un activo estratégico de la organización. Se puede resumir como:

- ✓ Se deben comprender los principios de la Estrategia del Servicio.
- ✓ Desarrollar la Estrategia de Gestión del Servicio.
- ✓ Estrategia y Servicio de Economía.
- ✓ ¿Cómo afecta a la estrategia de ciclo de vida de servicio?
- ✓ Estrategia y diseño de la cultura organizacional y el diseño.

Contar con una estrategia es crucial para tener éxito en el mercado para las organizaciones de TI que consideran la provisión de los servicios de TI como su principal negocio. Estas organizaciones necesitan enfocarse en la estrategia de entrega de los servicios, diferenciando un servicio de las alternativas de la competencia.

Estrategia de Servicios trata sobre la definición del mercado, desarrollo de ofertas, desarrollo de activos estratégicos y preparación para la ejecución. Los procesos que se incluyen en esta fase son:

- ✓ Administración del Portafolio de Servicios.
- ✓ Administración de la Demanda.
- ✓ Administración Financiera

•Service Design. Diseño de Servicios.

La fase de diseño del servicio se refiere principalmente con el diseño de servicios de TI, así como los asociados o requerido:

- ✓ Procesos.
- ✓ Sistemas de gestión de servicios y herramientas.
- ✓ Soluciones de servicio.
- ✓ Tecnología de arquitecturas.
- ✓ Sistemas de medición.

El factor determinante en el diseño de nuevos servicios o modificar servios es apoyar las necesidades cambiantes que tienen las empresas. Cada vez que se produce una nueva solución de servicio, se debe verificar contra el resto de la cartera de servicios para garantizar que se integrará y habrá una interacción con todos los otros servicios existentes.

Principales Metas y Objetivos del Diseño de Servicio:

- ✓ Contribuir a los objetivos del negocio.
- ✓ Contribuir a ahorra tiempo y dinero.
- ✓ Minimizar o prevenir riesgos.
- ✓ Contribuir a satisfacer necesidades presentes y futuras del mercado.
- ✓ Evaluar y mejorar la eficacia y eficiencia de los servicios de TI.
- ✓ Apoyar el desarrollo de políticas y estándares para los servicios de TI.
- ✓ Contribuir a mejorar la calidad de los servicios de TI.

Hay 5 aspectos individuales del Diseño de Servicios:

- ✓ Cambio o nueva solución de servicio.
- ✓ Sistema de administración de servicio y herramientas, especialmente el Portafolio de Servicios.
- ✓ Arquitectura tecnológica y administración de sistemas.
- ✓ Procesos, roles y capacidades.
- ✓ Métodos de medición y métricas.

• Service Transition. Transición de servicios.
El propósito de esta etapa es coordinar y llevar a cabo las actividades y procesos requeridos para entregar y administrar los servicios de acuerdo a los niveles de servicio acordados con los clientes y usuarios del negocio. Así también, es responsable de administrar la tecnología que se utiliza para entregar y soportar estos servicios.

Se centra en las vulnerabilidades que hay entre la fase diseño y la fase de operación de un servicio. Es especialmente crítico sobre errores funcionales y técnicos que no se encuentran en esta fase dará lugar a niveles de impacto significativamente mayor a la empresa y / o infraestructura de TI ya que por lo general cuesta mucho más que corregir esos errores una vez que el servicio está en funcionamiento.

Es importante un balance en metas opuestas:

- ✓ Vista interna de TI contra vista externa de negocio.
- ✓ Estabilidad contra responsivas.
- ✓ Calidad de Servicio contra costo de servicio.
- ✓ Reacción contra actividades proactivas

Alcance:

- ✓ Servicios.
- ✓ Procesos.
- ✓ Tecnología.
- ✓ Personas

• Service Operation. Operación de servicios.
Se centra principalmente en la gestión de servicios de TI, asegura la efectividad y eficiencia en la entrega y el soporte.

Requiere coordinación y ejecución de actividades y procesos necesarios para entregar y administrar servicios en los niveles acordados para los usuarios y clientes de de negocio.

La Transición del Servicio se enfoca en implementar todo el aspecto del servicio, no solo su aplicación y como es usado en circunstancias normales. Es

necesario asegurar que el servicio puede operar bajo extremos previstos o circunstancias anormales y que el soporte por fallas o errores está disponible.

La transición del servicio consta generalmente de seis pasos:

- ✓ Planificación y preparación.
- ✓ Construcción y pruebas.
- ✓ Pilotos.
- ✓ Planificación y preparación y desarrollo.
- ✓ Desarrollo y transición.
- ✓ Revisión y cierre de la transición del servicio

• Continual Service Improvement. Modelo de mejora continúa del servicio.

Es la fase que une los demás elementos del modelo, asegura que tanto los servicios y las capacidades de proporcionarlos tendrán una mejora continua y de forma madura.

Objetivos:

- ✓ Revisar, analizar y hacer recomendaciones de mejora para cada etapa.
- ✓ Revisar y analizar el cumplimiento de los acuerdos de servicio (SLAs).
- ✓ Identificar e implementar actividades para mejorar la calidad de los servicios de TI.
- ✓ Mejorar el costo-beneficio de la entrega de los servicios de TI.
- ✓ Asegurar que se utilicen métodos de calidad que soporten las actividades de mejora continua.

Fuente:

http://www.itil.com.mx

The art of service. ITIL V3 Foundation. Complete Certification Kit: 2009 edition. Study guide book and online course.

Anexo 4. Artículos derivados de este trabajo.

Anexo 4.1. Articulo presentado en 4° congreso mexicano de ingeniería en comunicaciones y electrónica.

Modelo y Arquitectura de Calidad en el Servicio QoS para redes Convergentes

Chadwick Carreto Arellano
Centro de Formación e Innovación Educativa
Escuela Superior de Cómputo
ccarretoa@ipn.mx

Rolando Menchaca García
Centro de Investigación en Computación
fmenchac@ipn.mx

Salvador Álvarez Ballesteros
Nestor Martínez Alvarado
Escuela Superior de Ingeniería Mecánica y Eléctrica
salvarez@ipn.mx
san_nestor@hotmail.com

RESUMEN

En el presente artículo se definen las etapas de un modelo para implementar Calidad de Servicio (QoS) en redes convergentes, el modelo propuesto consta de seis etapas y permiten garantizar servicios de conectividad, reconocimiento y monitoreo de una red de voz, video y datos típicos en una red convergente.

Se pretende llegar a un Modelo estándar para diferentes tipos de red, dando paso después aun arquitectura que sea eficaz.

Palabras clave: Calidad de Servicio, QoS, Modelo, Arquitectura.

I. INTRODUCCIÓN

En primer lugar definamos que es QoS (Quality of Service o Calidad de Servicio): es un conjunto de protocolos y tecnologías que garantizan tanto la transmisión de datos como la entrega de los mismos en un momento dado (throughput). Al implementar este tipo de tecnología aseguramos que aquellas aplicaciones que requieren de la utilización de un determinado ancho de banda para su buen funcionamiento tengan reservado y disponible su recurso en el momento que se le solicite.

Para tal fin uno de los principales conceptos acompañados a la tecnología QoS es la priorización, esto es darle de alguna manera más importancia a algunas conexiones que a otras.

Veamos algunos beneficios que podemos encontrar al implementar QoS en redes convergentes:

Control sobre los recursos: podemos limitar el ancho de banda utilizado por aquellas aplicaciones con este tipo de conexión en sus comunicaciones.

Permite usar más eficientemente los recursos de la red: al poder establecer prioridades sobre los diferentes tipos de servicios.

Menor latencia: este es el caso en el que por ejemplo una aplicación de tráfico interactivo como es el SSH, telnet, etc requieren un menor tiempo de respuesta que otras aplicaciones.

Existen varias formas de aplicar esta tecnología de calidad de servicio ya sea en software como en hardware, existen las aplicaciones comerciales y por supuesto las alternativas libres y de código abierto.

Este tipo de tecnología es importante tenerla presente en los ambientes laborales y empresariales, debido a que muchas veces la red es mal utilizada por los usuarios, para transmitir, descargar, o navegar entre información muchas veces innecesaria. Implementando el servicio QoS podemos llevar un mejor control no solamente del contenido sino también de las terminales que tendrán un mejor acceso que otras.

II.- MODELO DE CALIDAD DE SERVICIO QOS

La propuesta de modelo que presentamos a continuación consta de 6 etapas, cada una cuenta con sus respectivas subestructuras. Y llevan una estrecha relación para que la propuesta final (una arquitectura que asegure QoS) sea implementable, funcional, medible etc.

Una descripción general de las etapas de nuestro modelo se pude mencionar como sigue.

1. Etapa de reconocimiento de red.

Aquí es donde hacemos un estudio detallado de la red en cuestión, intentando conocer diversos factores operacionales responder preguntas claves como:

> ¿Con que equipo tecnológico se cuenta? Aunque en el momento del estudio, los equipos puedan mostrarse aun en estado operacional, se tiene que considerar una renovación tecnológica si acaso la vida útil ha terminado puesto que, para aplicar y

asegurar tecnologías QoS es necesario características "especiales" que el equipo actual brinda de manera implícita dentro de sus configuraciones.

¿Quién usa la red? Al momento de llegar a esta etapa necesitamos hacer un estudio detallado de los usuarios que usan la red, los servicios que necesitan, los servicios ofrecidos por la red, y saber si se está aprovechando el ancho de banda para cada nodo de manera optima, si cada servicio consume el ancho de banda que necesita y genera solo el trafico que le es permitido o si es el caso cual usuario o servicio genera más tráfico del que pudiese requerir, entonces se podría decidir cómo solucionar ese aspecto.

¿Cuál es el uso que se le da a la red? Cuál es el tipo de usuarios que comúnmente acceden a los servicios que brinda la red. (Para el caso de estudio taremos en cuenta una red educativa, universitaria). Para luego entonces comenzar a caracterizar ciertos factores claves como son el nivel de uso mantenido por el tráfico, flujo de tráfico, volumen de tráfico etc. Una calendarización que nos permitirá saber si se encuentran horas pico, congestiones regulares, y poder darle una solución adecuada.

Toda vez que tenemos resultados de las mediciones entonces podemos realizar un análisis para proponer la forma de atacar el problema (¡claro, tenemos identificado el problema!) entonces podemos dar paso a una etapa más.

2. Planeación y desarrollo de mejoras.

Basados en lo que ahora se conoce de la red, podemos hacer un reporte, seguido de los puntos que se puedan optimizar, implantar, y de los que sea necesario remover. En conjunto se realizara un plan de escalabilidad para que la red pueda mantenerse actualizada.

En esta etapa se busca poder hacer ciertas distinciones nada triviales ya que es un factor angular, Entre más específicas lleguen a ser esas distinciones mejor desempeño tendrá la arquitectura QoS. Comprendido lo anterior entonces tenemos que clasificar el trafico generado (aunque algunos de esos generadores de trafico puedan quedar en una o más categorías no deben considerarse como redundantes, en cambio deberán tomarse en cuenta bajo la perspectiva de que mas a delante brindaran un elemento de decisión).

Clasificación: haciendo distinción entre el tipo de servicios que requieren los usuarios de red, tipo de usuario. Una vez teniendo ello, podemos hacer uso de teoría de colas, tablas y protocolos de ruteo.

Jerarquización: una vez que se han clasificado los servicios a usar los usuarios etc., debemos formarles una jerarquía que mostrara quien tiene prioridad (basado en todos los puntos anteriores.) para formarse y salir de la cola, dar menos saltos en entre enrutadores etc. Hacer clases de tráfico para que sean enviados con prioridades, y que

nivel de garantía se le otorgara frente a las demás clasificaciones y frente a la red para un mejor desempeño.

Control de flujo. Para tener vigilancia del sentido del flujo de tráfico. Saltos que surjan entre peticiones etc.

Sectorización. Entendida bajo el contexto, de que encontraremos zonas (por ejemplo zona de jefes, zona de empleados medios etc) donde los servicios que se utilizan no deberán tener la misma prioridad, puesto que el nivel de jerarquía de los usuarios no es el mismo. Se tiene que atender entonces los de nivel mas alto.

3. Monitoreo. Proponemos realizar un monitoreo general de las funciones de red y sus servicios desplegados, podemos echar mano de diferentes técnicas e instancias como son:

- Marcado de paquetes
- Marcado de servicios
- Marcado de usuarios
- Marcado de rutinas

Y después dar paso a las consideraciones puntuales, de cada ente que genera tráfico en la red, tomando en consideración la posición que poseen dentro del ambiente estudiado.

Ya que se ha realizado el monitoreo general y particular, obtenemos resultados tangibles que podrán ser comparados con las métricas y políticas propuestas en secciones posteriores. Ese compilado de resultados deberá hacerse en forma frecuente y gradual integrándose a una bitácora de consulta al alcance de los administradores para decidir las acciones a tomar.

4. Implementación de políticas. Las políticas que se pretenden implementar deben contar con un nivel conciso de restricción, deben tener la capacidad de ser adaptativas y en la medida de lo posible inteligentes para que a partir de ellas se puedan tomar decisiones. Incluso contar con un nivel de heurística.

La propuesta de aspectos en los que se deben formular políticas son:

- Políticas de calidad en el servicio.
- Políticas de acceso.
- Políticas de seguridad.

5. Comparación. Llegados a esta etapa del modelo prácticamente lo tenemos todo, un reconocimiento puntual de los componentes y usos de la red. Sus servicios brindados, una ingeniería de tráfico hecho a la medida.

Se conocen también las métricas y recomendaciones de los organismos internacionales ejemplos de las cuales tenemos la normatividad emitida por la Unión Internacional de Telecomunicaciones (International Telecommunication Unión –ITU), Instituto de Ingenieros en Electricidad y Electrónica (Institute of Electrical and Electronics Engineers -IEEE) o grupos nacionales que surgen a través de la orbe y desarrollan ideas y aportaciones interesantes.

Y por último las políticas que hemos generado, tomando en cuenta puntos y factores clave a lo largo del estudio de red. Que si bien están basadas en recomendaciones de los arriba mencionados organismos internacionales, tienes adaptaciones a lo que a nosotros en el caso práctico de estudio (o aplicación, según corresponda.) nos conviene más.

El punto fuerte de esta etapa se centra precisamente en hacer una comparación entre estas caracterizaciones. Estudiarlas a fondo para concluir el mejor resultado a arrojar. Ya sea un veredicto de que todo resulto de manera positiva. Que hay que reestructurar alguna etapa para llegar a la optimización, o que hay que dar vuelta atrás.

En cualquiera de los casos será una decisión basada y fundamentada en lineamientos, mediciones y estudios de calidad.

6. Reporte, Conclusiones y Recomendaciones. Lo que se pueda decir sobre resultados finales será basado en el análisis de todas las etapas anteriores, en los resultados de todas las mediciones y estudios realizados. Se podrá concluir que se asegura la calidad en los servicios bajo circunstancias específicas, que hacer para evitar contingencias y congestiones, las jerarquías y niveles de cada perfil de servicio y usuario, y en su forma mas básica de flujo de trafico de paquetes. Se podrán dar los parámetros a seguir para implementar el modelo que ya en funcionamiento se convertirá en una arquitectura robusta de QoS.

III.- CONCLUSIONES

Algunas consideraciones finales podemos darlas sabiendo y redundando en el entendido que la arquitectura final es un conjunto de técnicas y estudios basados en medios y equipos físicos de la red equipo tecnológico usado para interconectividad y comunicación de la misma, tal como cables, switches, ruteadores, nodos, terminales de usuario final etc.

Medios y métodos lógicos basados en software, tal como mecanismos de medición, y procesamiento de datos, monitoreo de red, de protocolos etc.

Y por ultimo una hibridación entre los dos más básicos que podría ser un agente dotado de algoritmos de decisión, inteligencia artificial y heurística. Que se capaz de interactuar con el hardware de red, el software y en base a todos los datos recolectados pueda tomar decisiones, incluso adelantarse a problemas que puedan surgir e implementar mecanismos para que estos sean amortizados de manera automática, temprana y eficaz.

De igual manera debemos saber y tomar en cuenta otros aspectos de la red tal como su tecnología de interconexión, topología, metodología y algoritmos de comunicación y complejidad. En el caso que tenga detección de errores, de choques, de perdida de datos etc.

REFERENCIAS

1. OYAMA, Cybelle Suemi Oda e DE LUCENA, Sidney Cunha. **Considerações acerca do estabelecimento de QoS no RNP2.** NewsGeneration, v.6 nº 3, 21 de maio de 2002. http://www.rnp.br/newsgen/0205/qos_rnp.shtml

2. BATISTA, Daniel Macêdo; FIGUEIREDO, Gustavo Bittencourt; e FIGUEIREDO, Mercia Eliane Bittencourt. **Estudo de QoS IP sobre redes ATM.** NewsGeneration, v. 5 nº 4, 25 de julho de 2001. http://www.rnp.br/newsgen/0107/qos.shtml

3. GRANVILLE, Lisandro Zambenedetti et alii. **NetPlus - um ambiente para gerência de QoS baseado na web.** NewsGeneration, v. 5 nº 4, 25 de julho de 2001. http://www.rnp.br/newsgen/0107/netplus.shtml

4. SANTOS, Ana Paula Silva dos. **Qualidade de Serviço na Internet.** NewsGeneration, v. 3 nº 6, 12 de novembro de 1999. http://www.rnp.br/newsgen/9911/qos.shtml

5. VIANA, Aline C. et alii. Perspectivas sobre **Qualidade de Serviço nos Protocolos da Internet - Estudo de Caso: Aplicações de Vídeo Sob Demanda.** NewsGeneration, v. 4 nº 4, 28 de julho de 2000. http://www.rnp.br/newsgen/0007/art1.shtml

Anexo 4.2. Articulo presentado en XI Congreso Nacional de Ingeniería Electromecánica y de Sistemas.

Propuesta de Modelo de QoS para una red convergente.

L.S.C. Néstor Guillermo Martínez Alvarado[1] M. en C. chadwick Carreto Arellano[2], Dr. Salvador Álvarez ballesteros[3]
1, 3 Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Profesional Adolfo López Mateos Av. Instituto Politécnico Nacional s/n. Edificio Z-4, 3er. Piso. 57296000 Ext. 54755, 54756, 54757.
2 Centro de Formación e Innovación Educativa, Av. Wilfrido Massieu s/n Esq. Luis Enrique Erro, Unidad Profesional "Adolfo López Mateos", Zacatenco, Ciudad de México, D. F., C.P. 07738. Teléfonos: +52 (55) 5729 6000 extensiones 57166 y 57167, México, D.F.
E-mail: san_nestor@hotmail.com, ccarretoa@ipn.mx, salvarez@ipn.mx

Resumen — **Este trabajo tiene la función de difundir una propuesta de modelo para asegurar QoS sobre una red convergente y heterogénea en tecnología y usuarios. Se usan algunas de las características Principales de diferentes Arquitecturas existentes para proponer una nueva que arroje resultados integrales.**

Palabras Clave – **Arquitectura, Calidad en el Servicio (QoS), Modelo**

Abstract — **This short paper was done for the purpose of disseminating a model proposal to ensure QoS on a converged network and heterogeneous in technology and users. He used some of the main features of various existing architectures to propose a new integral that yields results.**

Keywords — **Architecture, Model , Quality of Service (QoS)**

I. Introducción

La Calidad en el servicio se ha vuelto un factor importante gracias a tres cualidades surgidas de las redes en los últimos años. Crecimiento desmesurado y sin planeación, Aplicaciones tecnológicas, Convergencia de las mismas. En la actualidad hay organismos reguladores para casi cualquier parámetro existente, con tal de asegurar QoS.

II. Metodología

El modelo propuesto se desarrolla de manera estructurada, consta de 6 capas. Tras su implementación se pretende obtener una arquitectura de QoS que sea robusta, flexible, e integral.

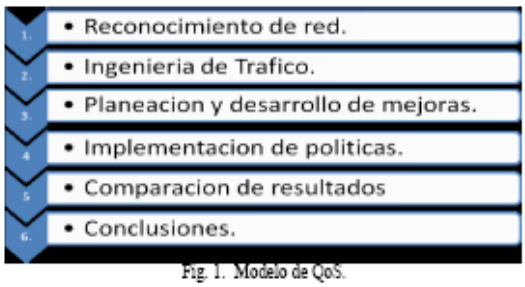


Fig. 1. Modelo de QoS.

A. *Reconocimiento de la red.*

La importancia de hacer un reconocimiento de red es dual por un lado está apegado estrechamente al reconocimiento del equipo que conforma el sistema de transmisión de comunicaciones (routers, switches, nodos finales ya sean pc's, impresoras, teléfonos), Sistemas de conexión eléctrica, cableado estructurado, etc. Para determinar el criterio de análisis después de la recolección de datos identificando así puntos clave de monitoreo. De esta manera cubrimos además la necesidad de conocer la forma en que se encuentran configurados los equipos, rastreo de estatus de funcionamiento actual, capacidad general de procesamiento y en algunos casos estatus de alarma arrojados por algunos equipos o componentes en mal funcionamiento.

Aunque hay diferentes maneras de identificar los datos y realizar el proceso arriba mencionado. Para este caso de estudio se uso un software llamado LanSourveyor de la marca Orión solar winds. (Explicaremos más adelante en el apartado de resultados).

El segundo objetivo es el reconocimiento lógico de la estructura de la red. En este caso una red convergente IP. Que de manera natural nos proporcionará muchas características específicas del ruteo y matrices de tráfico. Dicho sea de paso nos comenzaremos a armar de una buena bitácora para optimizar el desempeño de la red

El principio básico del método de reconocimiento de red es el monitoreo, el cual se realiza de manera selectiva y continua entre los dispositivos que conforman la red.

B. *Ingeniería de tráfico.*

La ingeniería de tráfico se entiende como el conjunto de procesos de medición, modelado y control del tráfico. Normalmente usada para canalizar la ocupación de ancho de banda excedente hacia ligas, caminos o rutas que estén más despejadas y desahoguen el tráfico de red, se basa estrictamente en los protocolos y estándares de enrutamiento y aunque tiene ciertos criterios de decisión (camino más corto, camino menos transitado, etc.) no toma consideración del estado de la red, ya sea nivel de ocupación, congestión, ancho de banda disponible e incluso retrasos. Todo este

conjunto permite a los proveedores de servicio satisfacer las necesidades de servicio acordados en el nivel de servicio (SLA).

- Caracterización de tráfico.

Tiene como objetivo identificar patrones de variación del trafico transportado, usando el análisis estadístico de los datos recopilados sobre la red, poniendo atención sobre el enfoque granular ya que podemos hacer la separación y puntualización en perfiles de flujos de tráfico, interfaces, nodos, rutas o caminos, fuentes, destinos, etc.
Por supuesto, hacer la estimación de la carga de tráfico de acuerdo a los servicios, perfiles de uso y usuario o rutas seguidas. Y observar la tendencia de crecimiento para obtener la previsión y respuesta adecuada a la demanda que surja a causa del tráfico.

- Monitoreo de red.

Los objetivos fuertemente identificados para este punto son conocer el estado operacional de la red, incluso aunque esté pasando por un periodo funcionalmente malo, obtener el reconocimiento continuo de la calidad brindada en los servicios desplegados por la red y el adecuado funcionamiento de políticas aplicadas a dichos servicios, y por último, verificar los contratos establecidos entre el proveedor de servicios y el desempeño de la red a través de las mediciones que arroja el monitoreo de los segmentos intercomunicados por intranet y WAN.

- Control de tráfico.

Las funciones que cumple el control de tráfico sobre el desempeño de la red son primordiales e importantes, los objetivos que debe alcanzar son, entre otros, un desempeño adaptativo en la optimización de red que pueda responder ante cambios, contingencias o demandas específicas a la misma. Por ejemplo, hacer un re-enrutamiento en caso de alguna falla o punto sobrecargado de la red, llevando el tráfico por puntos alternos y que la comunicación no se vea afectada, esto según la estructuración del modelo y topología física lo permita. Diseñar un mecanismo de respuesta ante posibles cambios en el flujo de tráfico de la red, haciendo señalización y disponibilidad de la misma. Tener un soporte de la admisión de tráfico generado, de entrada y salida. Un medio para lograr esto sería la reconfiguración del modelo QoS aplicado, las políticas usadas, etc. Dentro de la estructuración del control de tráfico, hay que tomar en cuenta el modelado de niveles tal como comportamiento, accesibilidad, servicio, prioridad, etc.

C. Planeación y Desarrollo de mejoras.

En este punto, tenemos mucha información acerca de la red. El trabajo ahora es analizar el total de la información realizar una discriminación de lo que sirve y es relevante y desechar lo que no.

Al realizar el análisis, podremos entonces identificar perfectamente lo que resultara en la caracterización de políticas. Entre otras cosas podemos realizar:

Clasificación de usurarios, servicios requeridos. Desembocando en un análisis completo de matriz de tráfico, teoría de colas y tablas de ruteo.

Jerarquización: de entre los tipos de servicio, de entre los usuarios que tendrán privilegios en la red, de entre las clases de tráfico. Lo cual nos dará la ventaja en la toma de decisiones de grupo de datos o tráfico dará menos saltos para establecer comunicación, saldrá o tendrá prioridad en colas etc.

Control de flujo. Para tener monitoreado en su caso hacia donde hay congestiones por ejemplo. O la mayor ocupación de la red etc.

Sectorización. En caso de tener un sistema de red grande, (o si la necesidad así lo implica o amerita) dividir por secciones a los usuarios y su tráfico. No necesariamente de manera física, pudiendo ser de manera lógica e integrarlos a la jerarquización previa.

Políticas. Son el condensado de los planes y objetivos a cumplir toman en cuenta las características arriba mencionadas, se adecuan a la jerarquización, sectorización tipo de servicio etc. O en su defecto los usuarios se adecuaran a ellas. (No es un sistema sin ley). Estas políticas deberán estar sustentadas en las recomendaciones que emiten organismos especializados por ejemplo la ITU. IEEE. Algunas características que es importante mencionar para que sean más robustas pueden ser:

Descripción de la política (alcance, requerimientos, sanciones)

Delimitar responsabilidades de cada actor participante en ella.

Difusión de la política

Hay que asegurarse que todos sepan que existen las políticas, que las entiendan y que sepan que en caso de incumplimiento hay sanciones pues es una cuestión delicada para tener un desempeño de la red.

Otra cosa importante a resaltar es que existen políticas para usuarios internos, invitados o externos. Para seguridad, contingencias etc. Entre más granular sea la identificación de ellas tendremos menos sorpresas si algo ocurre mal y mejor referencia de las cosas buenas y puntos fuertes de la red. Este proceso es dinámico, y no pude dejarse sin actualización puede estar en constante movimiento según resultados de los objetivos.

D. Implementación de políticas.

En esta sección solo diremos que todo el desarrollo y planeación del apartado anterior debe de ponerse en práctica. Hacer que sea un plan de acción y realizar el monitoreo constante del cumplimiento de objetivos esto a manera de estándar para saber si esta todo funcionando o deberán hacerse cambios y reestructuras

Como nota final hay que decir que hay cierta ambigüedad en esto que llamamos políticas pues algunas características inherentes a las arquitecturas de calidad en el servicio (diffserv, intserv, MPLS) tales como token buchet. Leaky-bucket o incluso un bandwidth bróker que son muy aparte de las políticas que se han descrito e ideado para el desarrollo de este modelo

E. Comparación de políticas.

La importancia de comparar entre los antes y después de cómo se encontraba la red, y comparar las políticas ideadas y los parámetros dictados por los organismos especializados en la materia. Al realizar esta etapa del modelo con un criterio analítico, realista objetivo.

Una vez realizado esto, podemos hacer el acumulativo de la información que nos dará paso a la etapa final. Un resultado estudiado probado y cimentado en la realidad por la cual pasa el sistema de red.

El objetivo es saber si todo resulto bien, hay que hacer una reestructuración parcial o en definitiva comenzar de nuevo.

F. Resultados y Conclusiones.

Lo que se pueda decir sobre resultados finales será basado en el análisis de todas las etapas anteriores, en los resultados de todas las mediciones y estudios realizados. Se podrá concluir que se asegura la calidad en los servicios bajo circunstancias específicas o diferentes perfiles, qué hacer para evitar contingencias y congestiones, las jerarquías y niveles de cada perfil de servicio y usuario, y en su forma más básica de flujo de tráfico de paquetes. Se podrán dar los parámetros a seguir para implementar el modelo que ya en funcionamiento se convertirá en una arquitectura robusta de QoS.

III. RESULTADOS

Hasta ahora se tienen resultados, algunos de ellos contundentes que de alguna forma han logrado ayudar al mejor funcionamiento de la red en donde se prueba. Dicha red es un segmento de la red del IPN. A continuación se presentan imágenes de pruebas y resultados.

Fig. 2. Etapa de Reconocimiento de Red con NTOP.

Usando la Herramienta NTOP podemos obtener bastante información, de entrada nos muestra el nombre del host, el dominio al que se está asociando, su dirección IP, MAC Address, consumo de ancho de banda, Nombre del fabricante, Numero de brincos hasta el dominio, Tiempo de actividad etc. Para hacer un simple reconocimiento da información muy detallada. Esta herramienta es usada en otras etapas más dentro del modelo.

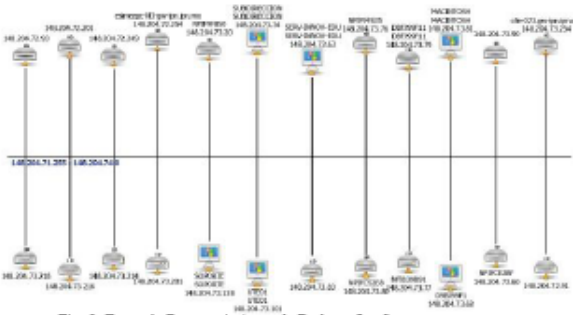


Fig. 2. Etapa de Reconocimiento de Red con LanSurveyor.

Una segunda opinión la muestra LanSurveyor de Orión Solar Winds, la cual nos entrega una idea clara de la topología en la cual se encuentra la red. Junto con una breve descripción de los nodos y equipos conectados a ella.

Esto podría ser corroborado si esque hay tiempo con los manuales de red (que deberían existir en las organizaciones) y una auditoria física para verificar la autenticidad de esta información.

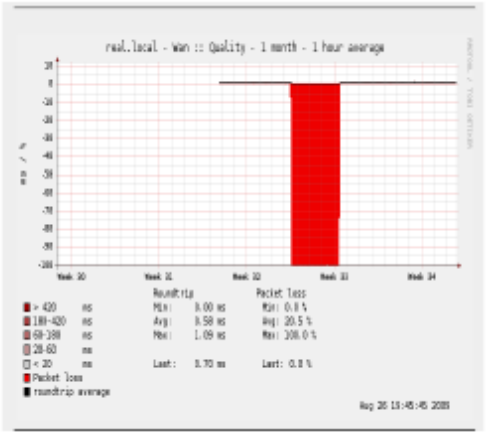


Fig. 3. Monitoreo de QoS con PFsense.

La imagen anterior nos muestra las estadísticas que arrojan el monitoreo de 4 semanas sobre la red del caso de practico de estudio, la grafica muestra un promedio de viaje de datos a una velocidad de .58ms un máximo de .84ms que está dentro del aceptable (refiriéndonos a la transmisión de paquetes VoIP establecido en la norma del protocolo de comunicaciones H.323) y una muy notoria perdida de paquetes (una caida de red).

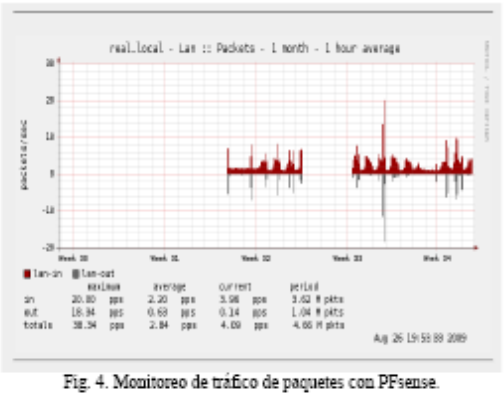


Fig. 4. Monitoreo de tráfico de paquetes con PFsense.

La grafica 4.muestra las estadisticas del trafico de paquetes en la interface LAN. De color rojo a la entrada y de color gris a la salida. Nos marca de igual manera un máximo un mínimo y un promedio del tráfico que ha pasado por la red con una métrica de paquetes por segundo.

Fig. 5. Monitoreo de tráfico con PFsense.

La figura 5 muestra el tráfico de datos en bits sobre segundo, en un histórico mensual, de igual manera el rojo es la entrada, gris a la salida y arroja datos del promedio, máximo y mínimo de paquetes de datos enviados sobre la red.

IV. Discusión

El trabajo se encuentra en la etapa de Ingeniería de tráfico, se sigue avanzando paralelamente en la etapa de documentación de políticas y recomendaciones de organismos especializados. Para que en la etapa siguiente se puedan hacer sugerencias integrales par el mejor desempeño de la red. Si bien estamos dentro de un entorno centralizado (la unidad de cómputo y comunicaciones del IPN) es la encargada de autorizar la mayoría de los estudios y políticas oficiales que serán parte del sistema de red. Se hace lo posible por que las emitidas en este trabajo de investigación sean tomadas en cuenta.

V. Conclusiones

La calidad en el servicio no es solo un plan de contingencia, debe ser tomada en cuenta desde la planeación de la red o en su defecto como pilar fundamental en la reestructuración. Asegurar calidad en el servicio no es trivial, y no se debe pecar de confianza solo porque el equipo tecnológico este aparentemente sobrado.

Hay que tomar en cuenta que, la verdadera red es la de datos y aunque se hable de convergencia, el internet, la Voz sobre IP, videoconferencia y demás son solo servicios. Que en efecto deben tener un cierto nivel de garantía por ende considerar de manera oportuna QoS.

De cierta manera la QoS no depende o más bien no está ligada solo con marcas de fabricante de equipo tecnológico,

o sistemas software. Pude combinarse y hacerse un sistema flexible.

AGRADECIMIENTOS

A las personas involucradas en este proyecto.

REFERENCIAS

[1] Vilho Raisanen. Implementing Service Quality in IP Networks. Soluciones Avanzadas. John Wiley & Sons Inc. 2003 ISBN 0-470-84793-X

[2] Mike Flannagan. Administering Cisco QOS for IP Networks. Syngress; 1 edition (March 15, 2001). ISBN-10: 1928994210.

[3] Xiao, XiPeng. Technical, commercial, and regulatory challenges of QoS. Morgan Kaufmann. 2008 ISBN: 978-0-12-373693-2

[4] *Volume Editor: Adrian Farrel, Old Dog Consulting, UK.* Network Quality of Service Know It All. Morgan Kaufmann 2008.

Anexo 4.3. Articulo presentado en Vigésima Reunión de Otoño de Comunicaciones, Computación, Electrónica y Exposición Industrial

Aplicación de Políticas al Modelo de QoS sobre una red convergente.

L.S.C. Néstor Guillermo Martínez Alvarado[1] M. en C. Chadwick Carreto Arellano[2], Dr. Salvador Álvarez Ballesteros[3]

1, 3 Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Profesional Adolfo López Mateos Av. Instituto Politécnico Nacional s/n. Edificio Z-4, 3er. Piso. 57296000 Ext. 54755, 54756, 54757.
2 Centro de Formación e Innovación Educativa, Av. Wilfrido Massieu s/n Esq. Luis Enrique Erro, Unidad Profesional "Adolfo López Mateos", Zacatenco, Ciudad de México, D. F., C.P. 07738. Teléfonos: +52 (55) 5729 6000 extensiones 57166 y 57167, México, D.F.
E-mail: san_nestor@hotmail.com, ccarretoa@ipn.mx, salvarez@ipn.mx

Resumen — **En el presente trabajo se muestra una propuesta de modelo para asegurar QoS sobre una red convergente y heterogénea en tecnología y usuarios. Se usan algunas de las características principales de diferentes arquitecturas existentes para proponer una nueva que arroje resultados integrales y genere recomendaciones para garantizar QoS.**

Palabras Clave – **Arquitectura, Calidad en el Servicio (QoS), Modelo**

Abstract — **In this short paper we present the purpose of disseminating a model proposal to ensure QoS on a converged network and heterogeneous in technology and users. We used some of the main features of various existing architectures to propose a new integral that yields results and generate recommendations for guarantee QoS.**

Keywords — **Architecture, Model, Quality of Service (QoS)**

INTRODUCCIÓN

La Calidad en el servicio se ha vuelto un factor importante gracias a tres cualidades surgidas de las redes en los últimos años. Crecimiento desmesurado y sin planeación, Aplicaciones tecnológicas, Convergencia de las mismas. En la actualidad hay organismos reguladores para casi cualquier parámetro existente, con tal de asegurar QoS.

Existen tres modelos predominantes o que tienen la mayor difusión.

IntServ. Básicamente hace una modificación al modelo de servicio IP para soportar el trafico de aplicaciones en tiempo real y "de mejor esfuerzo", donde el flujo de datos puede ser host- host o aplicación – aplicación. Usa el conjunto de protocolos de reserva de recursos. RSVP (Resource Reservation Protocol). Tomando de la señalización de red para reservar los recursos que aseguren calidad de servicio en para ciertas aplicaciones. Mantiene una señalización por flujo en el múcleo de la red aunque la escalabilidad en esta arquitectura representa algunos cambios es posible realizar.

A manera de ejemplo se presenta que en la arquitectura IntServ se usan 3 clases para diferenciar uso del ancho de banda por el tráfico, desde la perspectiva de una aplicación que tiene cierto nivel de requerimientos en retardo.

1. Clase de garantía de servicio. Es el nivel más alto permisible de retardos en donde aun se garantiza una correcta trasmisión de la información.
2. Clase de carga controlada de servicio. Es una estadística de retardo según el servicio y aplicación y que no debe ser violado aun más allá de cuando no allá carga en la red.
3. Servicio "Del mejor esfuerzo". Nuevamente clasificado: en Ráfaga interactiva (Navegación WEB), Volumen interactivo (FTP), y Asíncrono (e-mail).

DiffServ. Usa el método de marcado de paquetes basado en extremos. El comportamiento de reenvío de paquetes locales por clase y el manejo de los recursos para dar soporte múltiples niveles de servicio sobre una red de servicio basada en IP.

La terminología usada en DiffServ es la siguiente:

1. Comportamiento por salto (PHB). Es el trato de que hace la arquitectura a los paquetes, el encargado de aplicarlo es el router. Se aplica a todos los paquetes que referidos por los servicios que tenga la arquitectura.

2. Código de punto de servicios diferenciados (DSCP). El valor que resalta en la cabecea del paquete, es quien se encargara de aplicar el PHB.
3. Comportamiento Agregado (BA). Conjunto de paquetes con la misma DSCP.
4. Orden Agregado (OA). Conjunto de BA's. puede ser llevado a la misma cola.
5. PHB programación de clases (PSC). El conjunto de PHB aplicado a un criterio OA, usan la misma cola.

MPLS. Capa de switcheo multi protocolo (MultiProtocol Label Switching). Diseñado par enviar paquetes a través de la red, con un excelente desempeño y agregando etiquetas a los paquetes que es como ellos entran a la arquitectura de routers de frontera (o extremos). Normalmente los routers según el camino de paquetes miran hacia la cabecera de cada IP individual. MPLS ocupa una limpieza simple etiquetas para cada cabecera de paquete incluyendo la información de la ruta que se encontraba en el. El desbordamiento provocado por cada router en la vista de los paquetes es muy compactado y el envío de los paquetes por parte de los routers es acrecentado.

Al ser MPLS una tecnología relativamente nueva, aun se estudian más bondades que le puedan ser atribuidas tal como la compatibilidad y uso de RSVP.

Como resultado del análisis de los modelos anteriores se propone el desarrollo de un nuevo modelo, tomando en cuanta las ventajas de los modelos anteriormente descritos.

En la sección II se describirá la metodología, se define el modelo propuesto y sus ventajas, para en la sección III describir los resultado obtenidos del modelo propuesto aplicado a una red real, para en la sección IV definir los puntos de discusión y el trabajo a futuro. Finalmente en la sección V se describen las conclusiones obtenidas del presente trabajo.

METODOLOGÍA

El modelo propuesto se desarrolla de manera estructurada, consta de 6 capas. Tras su implementación se pretende obtener una arquitectura de QoS que sea robusta, flexible, e integral.

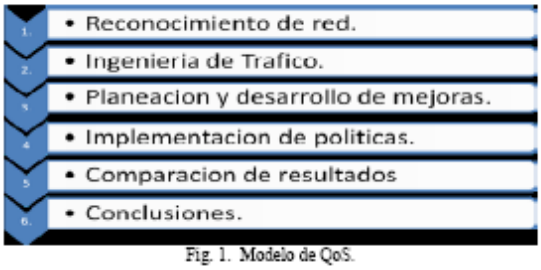


Fig. 1. Modelo de QoS.

A. Reconocimiento de la red.

La importancia de hacer un reconocimiento de red es dual por un lado está apegado estrechamente al reconocimiento del equipo que conforma el sistema de transmisión de comunicaciones (routers, switches, nodos finales ya sean pc's, impresoras, teléfonos), Sistemas de conexión eléctrica, cableado estructurado, etc. Para determinar el criterio de análisis después de la recolección de datos identificando así puntos clave de monitoreo. De esta manera cubrimos además la necesidad de conocer la forma en que se encuentran configurados los equipos, rastreo de estatus de funcionamiento actual, capacidad general de procesamiento y en algunos casos estatus de alarma arrojados por algunos equipos o componentes en mal funcionamiento.

Aunque hay diferentes maneras de identificar los datos y realizar el proceso arriba mencionado. Para este caso de estudio se uso un software llamado LanSourveyor de la marca Orión solar winds. (Explicaremos más adelante en el apartado de resultados).

El segundo objetivo es el reconocimiento lógico de la estructura de la red. En este caso una red convergente IP. Que de manera natural nos proporcionará muchas características específicas del ruteo y matrices de tráfico. Dicho sea de paso nos comenzaremos a armar de una buena bitácora para optimizar el desempeño de la red

El principio básico del método de reconocimiento de red es el monitoreo, el cual se realiza de manera selectiva y continua entre los dispositivos que conforman la red.

B. Ingeniería de tráfico.

La ingeniería de tráfico se entiende como el conjunto de procesos de medición, modelado y control del tráfico. Normalmente usada para canalizar la ocupación de ancho de banda excedente hacia ligas, caminos o rutas que estén más despejadas y desahoguen el tráfico de red, se basa estrictamente en los protocolos y estándares de enrutamiento y aunque tiene ciertos criterios de decisión (camino más corto, camino menos transitado, etc.) no toma consideración del estado de la red, ya sea nivel de ocupación, congestión, ancho de banda disponible e incluso retrasos. Todo este conjunto permite a los proveedores de servicio satisfacer las necesidades de servicio acordados en el nivel de servicio (SLA).

- Caracterización de tráfico.

Tiene como objetivo identificar patrones de variación del trafico transportado, usando el análisis estadístico de los datos recopilados sobre la red, poniendo atención sobre el

enfoque granular ya que podemos hacer la separación y puntualización en perfiles de flujos de tráfico, interfaces, nodos, rutas o caminos, fuentes, destinos, etc.
Por supuesto, hacer la estimación de la carga de tráfico de acuerdo a los servicios, perfiles de uso y usuario o rutas seguidas. Y observar la tendencia de crecimiento para obtener la previsión y respuesta adecuada a la demanda que surja a causa del tráfico.

- Monitoreo de red.

Los objetivos fuertemente identificados para este punto son conocer el estado operacional de la red, incluso aunque esté pasando por un periodo funcionalmente malo, obtener el reconocimiento continuo de la calidad brindada en los servicios desplegados por la red y el adecuado funcionamiento de políticas aplicadas a dichos servicios, y por último, verificar los contratos establecidos entre el proveedor de servicios y el desempeño de la red a través de las mediciones que arroja el monitoreo de los segmentos intercomunicados por intranet y WAN.

- Control de tráfico.

Las funciones que cumple el control de tráfico sobre el desempeño de la red son primordiales e importantes, los objetivos que debe alcanzar son, entre otros, un desempeño adaptativo en la optimización de red que pueda responder ante cambios, contingencias o demandas específicas a la misma. Por ejemplo, hacer un re-enrutamiento en caso de alguna falla o punto sobrecargado de la red, llevando el tráfico por puntos alternos y que la comunicación no se vea afectada, esto según la estructuración del modelo y topología física lo permita. Diseñar un mecanismo de respuesta ante posibles cambios en el flujo de tráfico de la red, haciendo señalización y disponibilidad de la misma. Tener un soporte de la admisión de tráfico generado, de entrada y salida. Un medio para lograr esto sería la reconfiguración del modelo QoS aplicado, las políticas usadas, etc. Dentro de la estructuración del control de tráfico, hay que tomar en cuenta el modelado de niveles tal como comportamiento, accesibilidad, servicio, prioridad, etc.

C. Planeación y Desarrollo de mejoras.

En este punto, se ha recabado bastante información acerca de la red. El trabajo ahora es analizar el total de la información realizar una discriminación de lo que sirve y es relevante y desechar lo que no.

Al realizar el análisis, existe la posibilidad de identificar perfectamente lo que resultara en la caracterización de políticas. Entre otras cosas podemos realizar:

Clasificación de usurarios, servicios requeridos. Desembocando en un análisis completo de matriz de tráfico, teoría de colas y tablas de ruteo.

Jerarquización: de entre los tipos de servicio, de entre los usuarios que tendrán privilegios en la red, de entre las clases de tráfico. Lo cual nos dará la ventaja en la toma de decisiones de grupo de datos o tráfico dará menos saltos para establecer comunicación, saldrá o tendrá prioridad en colas etc.

Control de flujo. Para tener monitoreado en su caso hacia donde hay congestiones por ejemplo. O la mayor ocupación de la red etc.

Sectorización. En caso de tener un sistema de red grande, (o si la necesidad así lo implica o amerita) dividir por secciones a los usuarios y su tráfico. No necesariamente de manera física, pudiendo ser de manera lógica e integrarlos a la jerarquización previa.

Políticas. Son el condensado de los planes y objetivos a cumplir toman en cuenta las características arriba mencionadas, se adecuan a la jerarquización, sectorización tipo de servicio etc. O en su defecto los usuarios se adecuaran a ellas. (No es un sistema sin ley). Estas políticas deberán estar sustentadas en las recomendaciones que emiten organismos especializados por ejemplo la ITU. IEEE. Algunas características que es importante mencionar para que sean más robustas pueden ser:

Descripción de la política (alcance, requerimientos, sanciones)

Delimitar responsabilidades de cada actor participante en ella.

Difusión de la política

Hay que asegurarse que todos sepan que existen las políticas, que las entiendan y que sepan que en caso de incumplimiento hay sanciones pues es una cuestión delicada para tener un desempeño de la red.

Otra cosa importante a resaltar es que existen políticas para usuarios internos, invitados o externos. Para seguridad, contingencias etc. Entre más granular sea la identificación de ellas tendremos menos sorpresas si algo ocurre mal y mejor referencia de las cosas buenas y puntos fuertes de la red. Este proceso es dinámico, y no pude dejarse sin actualización puede estar en constante movimiento según resultados de los objetivos.

D. Implementación de políticas.

La calidad en el servicio representa cosas diferentes para personas diferentes, dependiendo el papel en donde se encuentren dentro del modelo su apreciación y exigencias cambiara, en efecto no solo es incrementar o restringir el ancho de banda a la red. Es hacer diferencias en el trato entre diferentes componentes y métricas de la red ya sea una sola o en conjunto varias de ellas, y estos criterios de diferenciación están completamente ligados con las aplicaciones a las que sirven y que tienen un criterio de calidad en el servicio diseñado para ellas. Normalmente los servicios de voz, tienen criterios muy diferentes (y necesidades) en comparación con el envío de datos de información.

Estas políticas configuran el método y medio de acción de los dispositivos que conforman la red, en conjunto con las reglas que serán usadas para las decisiones y buen manejo de los recursos y los datos que componen el sistema.
En el panorama más alentador (respecto a las políticas que aseguren QoS) son los sistemas especializados y basados en el binomio hardware y software. Sistemas como los llamados PBNM por sus siglas en ingles Manejo de red basado en políticas, (Policy Based Network Management). Donde se concentran dispositivos con políticas precargadas de uso activando un buen funcionamiento del modelo de negocio y de red.
Otra solución puede darse, según el modelo de aprovisionamiento de QoS (DiffServ, IntServ, MPLS) por ejemplo usando un ente llamado Bandwidth Broker. El cual se encarga de hacer las negociaciones con los diferentes componentes del sistema o modelo. Tales como el proveedor de servicio. Podría desempeñar algunas tareas como el control de admisión a la red, manejo de recursos, y el manejo de los dispositivos y configuraciones del conjunto de políticas para dar soporte QoS. El Bandwidth Broker es un ente lógico.
En el caso concreto de este estudio se están haciendo esfuerzos pos caracterizar y proponer una serie de políticas tales como

- Uso/Usabilidad. Que en general es toda la entrada de flujo de tráfico hacia la red. Contempla mecanismo de control de acceso etc.

- Usuario/Usabilidad/Disponibilidad. Donde se hacen propuestas de manejo de tráfico en todo el sistema de red, la disponibilidad de los dispositivos y servicios y con qué calidad pueden ser utilizados por los usuarios de la red. Aquí está concentrado todo el procesamiento y el trabajo rudo de la red.

- Tráfico. Que es propiamente la salida de todo el procesamiento de la información después del recorrido del sistema. La presentación a los sistemas y dispositivos que integraran la información y hacen la presentación final. O la que lo envía a otros segmentos o redes de "fuera". Control de todo el flujo de salida.

- Seguridad. Es primordial tener control de la seguridad de los sistemas, basado en políticas se facilita bastante el trabajo. Y puede ser muy granular e incluso se integran planes de contingencia.

E. Comparación de Resultados.

La importancia de comparar entre los antes y después de cómo se encontraba la red, y comparar las políticas ideadas y los parámetros dictados por los organismos especializados en la materia. Al realizar esta etapa del modelo con un criterio analítico, realista objetivo.

Una vez realizado esto, podemos hacer el acumulativo de la información que nos dará paso a la etapa final. Un resultado estudiado probado y cimentado en la realidad por la cual pasa el sistema de red.

El objetivo es saber si todo resulto bien, hay que hacer una reestructuración parcial o en definitiva comenzar de nuevo.

F. Resultados y Conclusiones.

Lo que se pueda decir sobre resultados finales será basado en el análisis de todas las etapas anteriores, en los resultados de todas las mediciones y estudios realizados. Se podrá concluir que se asegura la calidad en los servicios bajo circunstancias especificas o diferentes perfiles, qué hacer para evitar contingencias y congestiones, las jerarquías y niveles de cada perfil de servicio y usuario, y en su forma más básica de flujo de tráfico de paquetes. Se podrán dar los parámetros a seguir para implementar el modelo que ya en funcionamiento se convertirá en una arquitectura robusta de QoS.

RESULTADOS

Hasta ahora se tienen resultados, algunos de ellos contundentes que de alguna forma han logrado ayudar al mejor funcionamiento de la red en donde se prueba. Dicha red es un segmento de la red del IPN. A continuación se presentan imágenes de pruebas y resultados.

Fig. 2. Etapa de Reconocimiento de Red con NTOP.

Usando la Herramienta NTOP se puede obtener información valiosa, de entrada nos muestra el nombre del host, el dominio al que se está asociando, su dirección IP, MAC Address, consumo de ancho de banda, Nombre del fabricante, Numero de brincos hasta el dominio, Tiempo de actividad etc. Para hacer un simple reconocimiento da información muy detallada. Esta herramienta es usada en otras etapas más dentro del modelo.

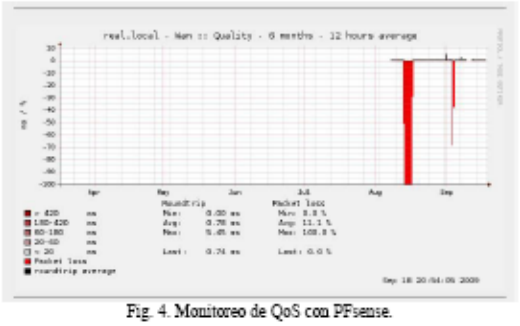


Fig. 4. Monitoreo de QoS con PFsense.

La Figura 4. Muestra las estadísticas que arrojan el monitoreo de 4 semanas sobre la red del caso de practico de estudio, la grafica muestra un promedio de viaje de datos a una velocidad de .58ms un máximo de .84ms que está dentro del aceptable (refiriéndose a la transmisión de paquetes VoIP establecido en la norma del protocolo de comunicaciones H.323) y una muy notoria perdida de paquetes (una caída de red).

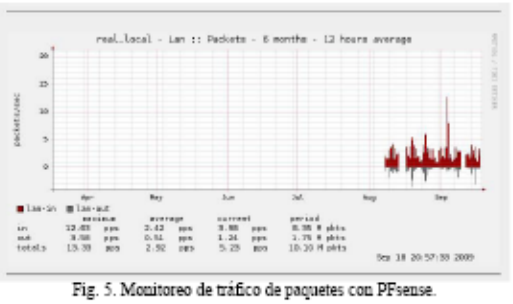


Fig. 5. Monitoreo de tráfico de paquetes con PFsense.

La Figura 5. Muestra las estadísticas del tráfico de paquetes en la interface LAN. De color rojo a la entrada y de color gris a la salida. Nos marca de igual manera un máximo un mínimo y un promedio del tráfico que ha pasado por la red con una métrica de paquetes por segundo.

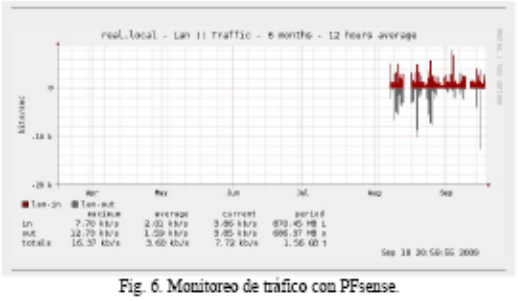


Fig. 6. Monitoreo de tráfico con PFsense.

La figura 6. Muestra el tráfico de datos en bits sobre segundo, en un histórico mensual, de igual manera el rojo es la entrada, gris a la salida y arroja datos del promedio, máximo y mínimo de paquetes de datos enviados sobre la red.

Fig. 7. Registro de sistema (intentos de conexión).

Otro tipo de resultado que se ha obtenido en el desarrollo del trabajo de la investigación es la seguridad. La figura 7 muestra algunos ataques tratando de obtener acceso y

privilegios para al servidor (monitor de pruebas). Aunque pudiera ser que estén navegando tras un proxy anónimo y entregar información errónea, los ataques han sido constantes, con diferentes rangos de red, lo cual nos hace deducir que han sido de diferentes partes del mundo. No han tenido éxito y el trabajo continua su marcha.

Fig. 8. Rastreo de la dirección IP atacante.

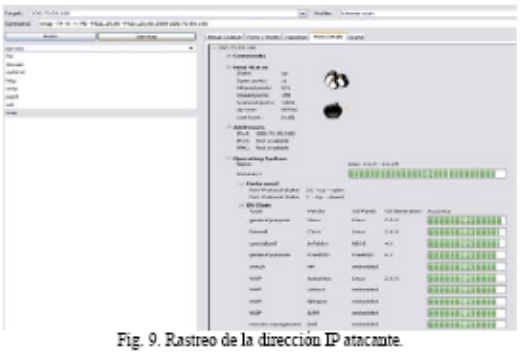


Fig. 9. Rastreo de la dirección IP atacante.

En la Figura 8. Se muestra el rastreo de las direcciones IP atacantes usando el software NeoTrace. El cual entrega abúndate información, como es saltos en la red, ubicación geográfica velocidad de respuesta etc. Solo para archivo estadístico y reforzar la seguridad de contraseñas y demás medios.

Se usa el software NMAP Figura 9., para obtener un poco de información extra para integración de análisis estadísticos, normalmente los ataques provienen de direcciones asiáticas como china pero también las hay rusas, y americanas.

4. CONCLUSIONES

El trabajo se encuentra en la etapa caracterización, implementación y desarrollo de políticas integrales par el mejor desempeño de la red. La unidad de cómputo y comunicaciones del IPN es la encargada de autorizar la mayoría de los estudios y políticas oficiales que serán parte del sistema de red.

El trabajo próximo que se tiene considerado es la implementación del modelo lo cual arrojara finalmente una arquitectura y es ahí el tiempo en donde se va a realizar la comparación para emitir las conclusiones finales. Recomendaciones etc. Del trabajo de investigación en si.

La calidad en el servicio no es solo un plan de contingencia, debe ser tomada en cuenta desde la planeación de la red o en su defecto como pilar fundamental en la reestructuración. Asegurar calidad en el servicio no es trivial, y no se debe pecar de confianza solo porque el equipo tecnológico este aparentemente sobrado.

El aporte de este modelo es su nivel de aplicación, en esta etapa de pruebas es en un segmento de red, la idea es que al final se obtenga un modelo portable flexible y robusto capaz de ser implementado redes de aun escala mayor (macro red) hablando por ejemplo de una red institucional no solo un segmento.

REFERENCES

Vilho Raisanen. Implementing Service Quality in IP Networks. Soluciones Avanzadas. John Wiley & Sons Inc. 2003 ISBN 0-470-84793-X

Mike Flannagan. Administering Cisco QOS for IP Networks. Syngress; 1 edition (March 15, 2001). ISBN-10: 1928994210.

Xiao, XiPeng. Technical, commercial, and regulatory challenges of QoS. Morgan Kaufmann. 2008 ISBN: 978-0-12-373693-2

Volume Editor: Adrian Farrel, Old Dog Consulting, UK Network Quality of Service Know It All. Morgan Kaufmann 2008.

L.S.C Néstor Guillermo Martínez Alvarado.

Estudios:

Maestría en Ciencias en Ingeniería de Telecomunicaciones, Esime Zacatenco, Instituto Politécnico Nacional. Mexico Distrito Federal.

Egresado de la Universidad Autónoma del Estado de Hidalgo. Pachuca de Soto Hidalgo.

Ha escrito artículos para:

4to. Congreso Mexicano de ingeniería en Comunicaciones y Electrónica. Artículo: "**Modelo y Arquitectura de Calidad en el Servicio QoS para redes Convergentes**"

*XXII Congreso Nacional y VIII Congreso Internacional de Informática y Computación Articulo: "**Implantación de un Modelo y Arquitectura de Calidad en el Servicio QoS para redes Convergentes**"*

El 5° Congreso Internacional de Ingeniería Electromecánica y de Sistemas. Artículo: "**Propuesta de Modelo de QoS para una red convergente.**"