UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

ARTICULO CIENTÍFICO

OPTIMIZACIÓN DEL ANCHO DE BANDA DE ACCESO A INTERNET Y CONTROL DE TRÁFICO DE LA UNIVERSIDAD TÉCNICA DEL NORTE APLICANDO CALIDAD DE SERVICIO (QoS)

AUTOR: DIEGO FABIÁN PASPUEL FRAGA

DIRECTOR: ING. CARLOS VÁSQUEZ

IBARRA - ECUADOR

2014

OPTIMIZACIÓN DEL ANCHO DE BANDA DE ACCESO A INTERNET Y CONTROL DE TRÁFICO DE LA UNIVERSIDAD TÉCNICA DEL NORTE APLICANDO CALIDAD DE SERVICIO (QoS)

Diego Fabián Paspuel Fraga

Facultad De Ingeniería En Ciencias Aplicadas, Universidad Técnica del Norte

Ibarra, Ecuador

diegofpf1988@hotmail.es

Tutor: Ing. Carlos Vásquez

cava_6@hotmail.com

***Resumen*- Al implementarse políticas de calidad de servicio en la red de la UTN-FICA se realiza con el objetivo de controlar el flujo de tráfico que cursa por la red. Primeramente se trata los fundamentos teóricos básicos de calidad de servicio como son: concepto y parámetros de calidad de servicio, modelos de calidad de servicio, mecanismos para obtener calidad de servicio dentro de una red, además se describen las herramientas seleccionadas para realizar la auditoria y el monitoreo de la red.**

Luego se realiza el estudio de la situación actual de la red de la Universidad Técnica del Norte tanto para la parte física y lógica de la red, para conocer el funcionamiento y los requerimientos de la misma mediante el uso de herramientas de monitoreo, y diagnosticar la actividad de la red. Seguidamente se procede a plantear las políticas necesarias de calidad de servicio QoS, para proponer un esquema adecuado de optimización del ancho de banda, para lo cual se analizan los datos obtenidos en la auditoria de red, y de esta forma determinar los requerimientos que se requieren para cada uno de los diferentes tráficos que circulan por la red de la UTN.

I. INTRODUCCIÓN

Debido al avance progresivo de las redes, han hecho que estas soporten diferentes tipos de servicios y aplicaciones con requerimientos de performance muy diferentes tales como voz, video y datos sobre una infraestructura común. Cada uno de estos tipos de tráfico tiene varios requerimientos de ancho de banda, retardo y pérdida de paquetes, etc.; las cuales en conjunto representan un gran reto para el personal administrador.

Para poder dar respuesta a los diferentes requerimientos de las aplicaciones y servicios sobre una misma infraestructura de red se requiere implementar calidad de servicio QoS, y así asegurar la entrega de información necesaria, dando preferencia a las aplicaciones críticas sobre las demás aplicaciones de menor importancia.

La QoS permite hacer uso eficiente de los recursos de la red ante una situación de congestión, al seleccionar un tráfico específico de la red y así priorizarlos según su importancia dentro de la red.

II. ANTECEDENTES

Se realizó la auditoría de red tanto de la parte física como lógica para dar un diagnóstico del funcionamiento de la misma y la compatibilidad de los equipos para la implementación de QoS.

A. Análisis de la topología física de la red

Actualmente la red de la UTN dentro de la capa de Core existe un Router 7604 el cual sirve como enlace con su proveedor de servicios de Internet "TELCONET S.A" para la universidad el cual brinda un ancho de banda de 300 Mbps a través de un convenio que mantiene esta institución educativa con CEDIA.

La estructura de la red interna de la Universidad Técnica del Norte se encuentra formada por 2 Switches CISCO 4506-E dentro de la capa de distribución, de los cuales uno se encuentra ubicado en la planta baja del edificio central, dentro del Departamento de Informática ubicado en el cuarto frio, el cual es administrado por el Departamento de Redes. Y el segundo Switch CISCO 4506-E se encuentra ubicado en el primer piso de la Facultad de Ingeniería en Ciencias Aplicadas, a un lado de los Laboratorios de Informática, el cual también es administrador por el Departamento de Informática.

Los servidores y varios equipos de red se encuentran distribuidos dentro de los racks existentes en el Cuarto Frio del Departamento de Informática para las diferentes aplicaciones y servicios para los docentes, estudiantes y personal de la universidad, actualmente este departamento cuenta con dos racks en donde se montan los diferentes dispositivos de red.

En la Dirección de Desarrollo Informático y Tecnológico se realiza la gestión y distribución de todos los equipos para la administración, de telefonía IP. Además dentro del cuarto frio se dispone de un aire acondicionado el cual brinda el ambiente de trabajo más adecuado para todos los equipos regulando la temperatura en caso de existir anomalías que afecten el comportamiento normal de los elementos de hardware, y también existen UPS que sirven como respaldo en caso de existir fallas eléctricas.

1) Backbone de la UTN

El backbone de la UTN es el encargado de interconectar las diferentes dependencias de este campus mediante fibra óptica, que soportan las diversas aplicaciones y servicios que circulan dentro de la infraestructura de red.

Dentro de la infraestructura física, la tecnología que se maneja actualmente a nivel de interfaces FastEthernet y gigabit Ethernet son velocidades de 10/100 Mbps y 1Gbps.

La interconexión que existe entre las diferentes dependencias de la Universidad se lo realiza mediante un cableado vertical o backbone utilizando fibra óptica multimodo de 62,5/125 con cubierta OFNR la cual contiene 8 pares de fibra soporta hasta un ancho de banda de 1 Gbps, cumple con la normativa TIA/TEIA-568-B, la cual define los estándares que permitirán el diseño e implementación de sistemas de cableado estructurado para edificios comerciales y entre edificios en entornos de campus.

Además la red de la UTN cuenta con un cableado de categoría 5E, existen diferentes dependencias donde existe cableado categoría 6 y en el nuevo edificio de postgrados existe cableado categoría 6A, lo que produce un desbalance en el desempeño dentro de la infraestructura de la red.

B. Análisis de la topología lógica de la red

La red interna de la UTN se encuentra divida por varias VLANS administradas por el Switch Catalyst 4506-E, la administración de estas se realizan a través de acceso telnet y SSH, en esta distribución de VLANS se utiliza el modelo Servidor-Cliente, que permiten la creación de dominios de broadcast a través de espacios lógicos de los Switches.

Las VLANs son un mecanismo que permite al administrador de red crear diferentes dominios de broadcast mediante espacios lógicos que pertenecen a un switch o diversos switchs sin tomar a consideración las proximidades físicas, por lo que este mecanismo es útil al momento reducir el tamaño de dominios de broadcast, evitando la necesidad de encontrarse físicamente dentro de un mismo lugar, según el administrador de red las formación de las VLANs se realizó mediante el peso del tráfico que genera un grupo de usuarios dentro del campus universitario.

2) La zona desmilitarizada (DMZ)

Alberga la mayoría de servidores a los que se puede tener acceso desde la WAN. Entre los que se pueden mencionar son: el Servidor WEB, de Aplicaciones, de Base de Datos, de Streaming del Canal y Radio Universitaria, del Campus Virtual, y del Repositorio Digital de la Biblioteca. El objetivo primordial de contar la DMZ es proteger a los servicios de posibles ataques ocasionados por intrusos.

La zona desmilitarizada (DMZ) se conecta directamente al Firewall Cisco ASA 5520 que permite detectar posibles ataques y amenazas, con una capacidad de hasta 450 Mbps y un promedio de 9000 sesiones por segundo. Posee cuatro interfaces Gigabit Ethernet, un puerto FastEthernet y soporta hasta 150 VLAN. Permite funciones de autentificación de identidad, cifrado, y la personalización de las políticas de seguridad de acuerdo a las exigencias específicas de la institución. La tabla I incluye los rangos de direccionamiento lógicos principales de la red UTN.

TABLA I
DIRECCIONAMIENTO LÓGICO PRINCIPAL DE LA RED UTN

RED	MÁSCARA	DESCRIPCIÓN
255.255.0.0	10.24.X.X	ZONA DESMILITARIZADA (DMZ)
255.255.255.0	172.20.X.X	RED INTERNA
255.255.255.224	190.95.X.X	RED EXTERNA

Fuente: Información proporcionada por la Dirección de Desarrollo Tecnológico e Informático

3) Equipamiento de la red de la UTN

El equipamiento se encuentra divido en áreas con sus diferentes componentes respectivamente en sus racks, clasificadas en principales y secundarias debido a la importancia que prestan en la administración y manejo de la red de la UTN.

El equipamiento de red de la UTN se encuentra ubicado en sus diferentes edificios y facultades, los cuales deben ser accesibles y cómodos para realizar cualquier tipo de trabajo o reparación dentro de los mismos.

4) Servidores y Aplicaciones

Los servidores que se encuentran dentro de la red de la UTN proveen los servicios y aplicaciones que transitan dentro de la red.

Servidor DNS, mediante el cual se suministra la traducción y correspondencia de nombres de dominios a direcciones IP que se usan en la redes TCP/IP, como Internet, para localizar servicios y equipos con nombres sencillos que se encuentran alojados en el Internet.

Servidor DHCP, usado dentro de una red para asignar dinámicamente direcciones IP a los diferentes usuarios (estaciones de trabajo).

Servidor de aplicaciones, permite el procesamiento de datos de una aplicación cliente. Entre sus principales ventajas están la centralización y la disminución de la complejidad del desarrollo de aplicaciones

Servidor de bases de datos, encargado de proveer servicios de bases de datos a las aplicaciones que utilizan la arquitectura cliente/servidor, donde un cliente puede buscar información y tener acceso mediante los recursos de red.

Servidor WEB, implementa el uso del protocolo HTTP, el cual pertenece a la capa de aplicación del modelo OSI, se lo usa para transferir páginas web, HTML o hipertextos, las páginas HTML.

Geoportal, usado para la captura, edición, análisis, tratamiento, diseño, publicación e impresión de información geográfica. Es usado por el Laboratorio de Geomática de la Universidad Técnica del Norte (UTN) que se encuentra en el emprendimiento de la IDE Red CEDIA.

Aula virtual, es usado en proceso de enseñanza-aprendizaje mediante el uso de las TIC´s, se lo utiliza para subir tareas e interactuar con los alumnos dentro de un mejor proceso de educación. Forma parte del Repositorio Digital.

Streaming de video de la UTN, utilizado para transmisión de un flujo de datos continúo de video bajo demanda de diferentes contenidos multimedia a través de las redes informáticas.

Repositorio Digital, realiza la publicación y almacenamiento en texto completo de los trabajos de final de carrera, como pueden ser tesis o proyectos, también constan publicación y reglamentaciones de la universidad, dando cumplimiento a la Ley de Educación Superior.

En la tabla II se muestran los puertos de comunicación usados por los servidores dentro de la infraestructura de red de la UTN que fueron obtenidos a través de la auditoría.

TABLA II
PUERTOS USADOS POR LOS SERVIDORES DE LA RED UTN

SERVIDOR	PUERTOS DE COMUNICACIÓN
svrapp2.utn.edu.ec	ssh [22], cycleserv2 [772], vnc [5801], vnc-1 [5901], vnc-2 [5902], vnc-3 [5903], vnc-http-2 [5802]
apex.utn.edu.ec	ssh [22], netbios-ssn [139], microsoft-ds [445], ncube-lm [1521], vnc-1 [5901], vnc-2 [5902], http-alt [8080]
svrapp3.utn.edu.ec	ssh [22], netbios-ssn [139], microsoft-ds [445], vnc [5900], vnc-1 [5901], vnc-3 [5903], kti-icad-srvr [6701], afs3-callback [7001], etlservicemgr [9001], dynamid [9002], ddi-tcp-1 [8888]
svrapp1.utn.edu.ec	ssh [22], ldap [389], ldaps [636], ncube-lm [1521], vnc [5801], vnc-http-2 [5802], vnc-1 [5901], vnc-2 [5902], vnc-3 [5903], x11 [6008], interwise [7778]
repositorio.utn.edu.ec	ftp [21], ssh [22], http [80], https [443], postgresql [5432], vnc [5801], vnc-1 [5901]
geoportal.utn.edu.ec	http [80], netbios-ssn [139], https [443], microsoft-ds [445], mysql [3306], postgresql [5432], vnc [5801], vnc-1 [5901], vnc-2 [5902]
aplicaciones.utn.edu.ec	ftp [21], http [80], netbios-ssn [139], https [443], microsoft-ds [445], mysql [3306], appserv-http [4848], vnc [5800], vnc [5900], afs3-callback [7001], blackice-alerts [8082], ddi-tcp-1 [8888]
encuesta_postgrado.utn.edu.ec	ssh [22], kti-icad-srvr [6701], afs3-callback [7001], ddi-tcp-1 [8888], etlservicemgr [9001], dynamid [9002]
biblioteca.utn.edu.ec	netbios-ssn [139], https [443], microsoft-ds [445], ms-wbt-server [3389], vnc [5800], vnc [5900], blackice-alerts [8082]

eventos.utn.edu.ec	ssh [22], http [80], https [443], mysql [3306], vnc [5900]
online.edu.ec	netbios-ssn [139], microsoft-ds [445], vnc [5800], vnc [5900]
online.edu.ec	http [80], netbios-ssn [139], microsoft-ds [445], lmsocialserver [1111], macromedia-fcs [1935], vnc [5800], vnc [5900]

Fuente: Auditoría de puertos de comunicación con el programa Axence NetTools y Zenmap

5) Ancho de Banda usado por la red UTN-FICA

Para conocer la situación actual del ancho de banda de la red se ha realizado un monitoreo continuo de la red para determinar el comportamiento del ancho de banda en tiempo real, y además obtener la información sobre el tipo, volumen y protocolos más usados en la red interna, para establecer un patrón característico acerca de los recursos de la red.

I. Análisis de tráfico

Para monitorear el tráfico de la red se considera recopilarlo a través de un port mirroring por el cual transcurre el mismo tráfico que circula en el enlace desde el switch de distribución a la FICA, y así conocer el comportamiento del mismo y los diferentes tráficos que circulan por dicho enlace.

II. Port-mirroring

Es una de las maneras más cómoda al momento de capturar el tráfico de red. Dicho modo de trabajo, denominado modo SPAN en entornos Cisco, permite duplicar el tráfico que transcurre por uno o varios puertos del switch y replicarlo al puerto que queramos. Hay que tener en cuenta que el puerto configurado como Mirroring tiene que ser tan rápido como el puerto/puertos a monitorizar para evitar pérdida de tramas.

Para monitorear el tráfico se creará una sesión de SPAN, la cual copia el tráfico proveniente de una o varias interfaces de un switch, hacia una interfaz determinada para su respectivo análisis e interpretación, para su configuración dentro de un switch se requiere especificar la fuente de origen y destino de los datos.

III. Estrategias de monitoreo

Antes de implementar un esquema de monitoreo se deben tomar en cuenta los elementos que se van a monitorear, así como las herramientas que se utilizarán para esta tarea.

Existen muchos aspectos que pueden ser monitoreados, pero los que más se consideraron para el desarrollo del presente proyecto son:

- Utilización de ancho de banda
- Tipo de tráfico.
- Servicios (p.e. Web, correo, Bases de Datos, DHCP, Aplicaciones)

Como se puede observar el figura 1 que los datos que se generan indican que el 99,7 % del total de datos monitoreados por la herramienta de código abierto NTOP corresponden al protocolo de Internet IP, donde el 98,7 % corresponden con el protocolo TCP, 1,3 % a UDP y el porcentaje restante se distribuye entre ICMP, ICMPv6 y varios protocolos no identificados por el software.

IV. Ancho de banda utilizado en la red UTN-FICA

Para medir este parámetro se ha utilizado las herramientas de monitoreo NTOP y PacketShaper, las cuales servirán para verificar el ancho de banda consumido dentro de la red interna, la auditoría de red se realizó mediante el uso de puerto espejo (Port-Mirroring) que duplica el tráfico que circula por las VLANs pertenecientes a la red de la FICA y lo replica a través del puerto FastEthernet 0/46 del switch de distribución CISCO 4506-E conectado al servidor donde se encuentra implementado la herramienta de monitoreo NTOP, y así poder clasificar los diferentes tráficos que circula por la red. La auditoría de red se realizó durante un mes, con lo que se pudo determinar el comportamiento del ancho de banda y el tráfico cursante, debido a la gran cantidad de información obtenida durante este proceso se tomó como referencia algunos días de auditoría.

Una vez finalizada la auditoría se procede a realizar varias tablas comparativas por horas, días y semanas para determinar los picos de utilización y promedio del consumo de ancho de banda de la red UTN-FICA. Además se realizará una comparación por días del comportamiento del ancho de banda dentro de la red.

6) Requerimientos necesarios para las aplicaciones de la red UTN-FICA

Los requerimientos necesarios para cada una de las aplicaciones usadas en la red de la UTN se lo realizarán usando un esquema de distribución de aplicaciones de prioridad crítica, alta, media y baja que se presentan en la tabla III, donde se detalla sus respectivos puertos de comunicación y la asignación del nivel de prioridad.

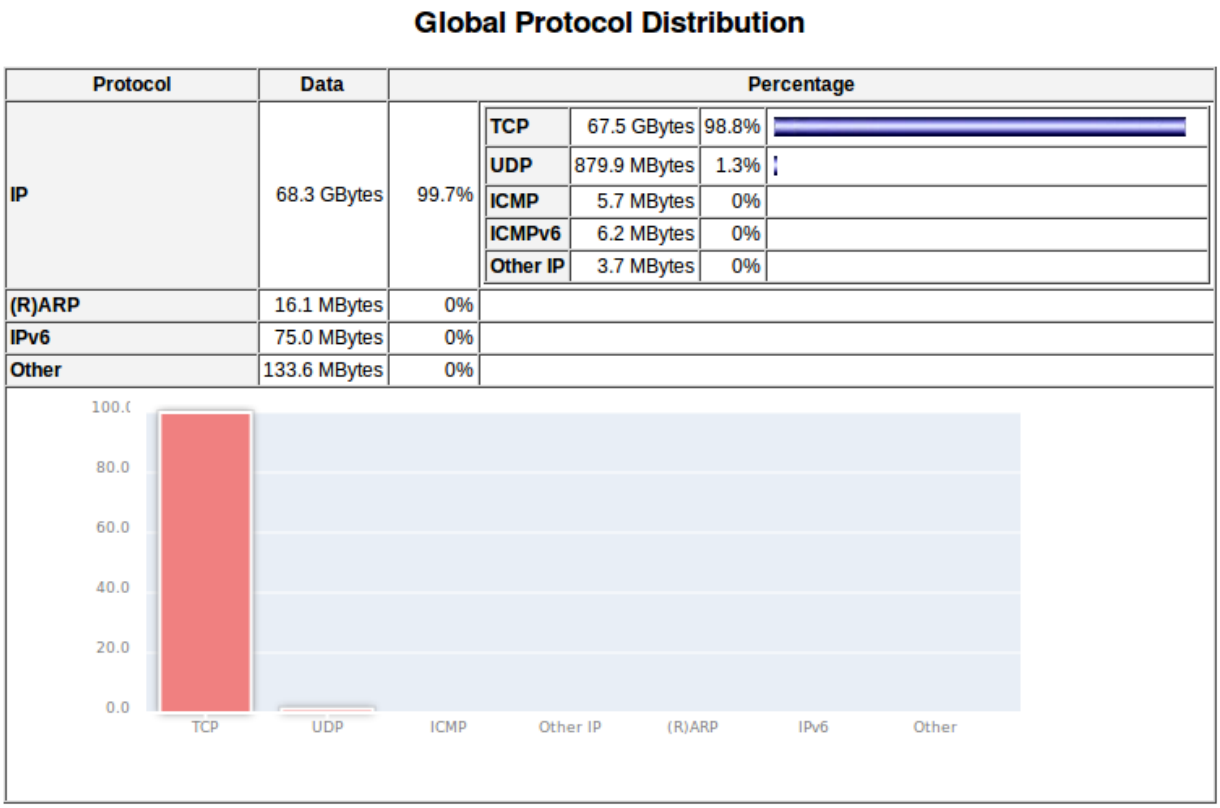

Figura 1: Distribución Global por Protocolos en la red UTN-FICA
Fuente: Resultados obtenidos de la auditoría de red mediante el uso de la herramienta NTOP

TABLA III
PUERTOS Y PRIORIDADES PARA LAS APLICACIONES USADAS EN LA RED UTN

APLICACIÓN	PRIORIDAD	PUERTOS
TELEFONIA IP	CRÍTICA	UDP: [16384-32767] [1720] Señalización
VIDEO	CRÍTICA	[80], [139], [445], [1111], [1935], [5800], [5900].
BASE DE DATOS	ALTA	[22], [139], [445], [1521], [5901], [5902], [8080].
SERVIDORES DE APLICACIONES	ALTA	[21], [22], [80], [139], [389], [443], [445], [636], [772], [1521], [3306], [4848], [5432], [5800], [5801], [5802], [5900], [5901], [5902], [5903], [6008], [6701], [7001], [7778], [8081], [8082], [8443], [8888], [9001], [9002].
DNS	MEDIA	[42], [53], [88], [135], [139], [389], [445], [464], [593], [636], [3268-3269], [5357], [49154-49158].
DHCP	BAJA	[67], [68], [11], [873], [3128], [3306], [5432], [5636], [5900].
CUALQUIER OTRO	DEFAULT	Varios puertos

Fuente: Programa Axence NetTools y Nmap - Zenmap

La clasificación anterior se realizó en base a la importancia que tienen determinadas aplicaciones y servicios más usados por los usuarios finales, y en base a las consideraciones técnicas de la Dirección de Desarrollo Tecnológico e Informático de la UTN, basándose en la línea básica de QoS de CISCO, manual de procedimientos y de acuerdo a la clasificación de aplicaciones.

Por otra parte, se especificó los puertos para la voz en un rango de 16384 a 32767, debido a que este rango de puertos es usado por CISCO para sesiones RTP en aplicaciones de tiempo real, y así asegurarse de que a todo el tráfico de voz se le dé un servicio de prioridad critica.

PROCEDIMIENTO PARA IMPLEMENTAR CALIDAD DE SERVICIO

Para implementar políticas de calidad de servicio QoS dentro de una red de datos, primeramente se debe diseñar y plantear etapas o fases que son: Evaluación y diagnóstico, análisis del tráfico, priorización del tráfico y planeación de

mejoras, implementación de políticas y verificación o resultados.

1) *Fases del proceso de implementación de QoS*

Para implementar adecuadamente las políticas de calidad de servicio QoS como se muestra en la figura 2 se lo debe realizar de forma estructurada con las fases anteriormente descritas, una vez implementadas se podrá contar con un diseño de QoS integral, flexible y robusto.

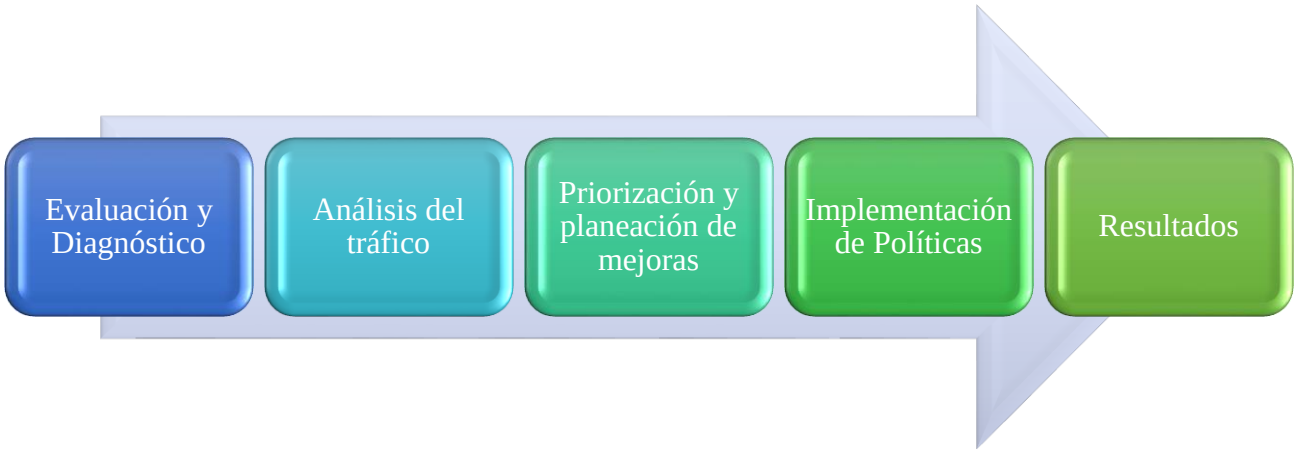

Figura 2: Fases para implementar QoS en una red de datos

I. Evaluación y diagnóstico de la red

Esta fase consiste en el análisis del equipamiento con el que consta una red, y así determinar su estado inicial para constatar que todos soporten la aplicación de calidad de servicio QoS.

Reconocimiento de la parte física de la red

En este paso primeramente se realiza un reconocimiento de la parte física de la red, reconocimiento de los equipos que forman parte de la red (Routers, Switches y Servidores), cableado estructurado y sistema de conexión eléctrica.

Este paso es primordial para conocer la configuración de equipos, funcionamiento actual, estado y características generales.

Reconocimiento de la parte lógica de la red

En este paso se realiza el reconocimiento lógico de la estructura de red, con lo que se podrá conocer la topología lógica, matrices de tráfico, aplicaciones que se usan y características específicas del enrutamiento.

Para reconocer el estado de una red se debe realizar una auditoría, que se la ejecutará de manera continua y selectiva entre los diferentes dispositivos que forman la red de datos.

Para esta fase dentro de la red de la UTN se hizo el levantamiento de datos de los equipos que la conforman, entre los que se pueden mencionar son los switches de distribución los CISCO Catalyst 4506-E y los switch de acceso distribuidos en las diferentes facultades.

El siguiente proceso de esta fase fue el reconocimiento del direccionamiento lógico dentro de la red, donde se pudo constatar la estructura lógica, la distribución de las VLANs dentro de la institución, los servidores, su direccionamiento, su tipo de enrutamiento y el direccionamiento que se maneja.

II. Análisis del tráfico

Esta fase consiste en el proceso de medición, clasificación y determinación del tráfico cursante por la red de datos, con lo que se podrá constatar el ancho de banda, congestión, etcétera.

Auditoría de la red

En este paso se realizará un reconocimiento de estado actual operacional de la red mediante el uso varias técnicas de monitoreo, pero para el presente proyecto se usó el port-mirroring, para conocer el comportamiento de los servicios desplegados por la red, con lo que se constatará si existen o no políticas dentro de la red.

Determinación del tráfico

Este paso del monitoreo del tráfico tiene como objetivo identificar patrones de variación del tráfico cursante de la red, usando un análisis estadístico de los datos recolectados de la red durante el proceso de auditoría de red, determinando así perfiles de tráfico, nodos, rutas, fuentes, destinos, etcétera. Con lo que se podrá clasificar el tráfico para poder brindar niveles de organización de las aplicaciones de la infraestructura de red.

En esta fase se realizó una auditoría de red a través de la técnica de port mirroring, que consiste en replicar el tráfico de una interfaz hacia otro puerto previamente seleccionado, para monitorear el patrón de comportamiento del tráfico cursante, se monitoreo a través de la interfaz FastEthernet 6/42 del switch de distribución 4506-E, cual replicaba todo el tráfico de la red de la UTN-FICA que cursa por la interfaz gigabithernet 2/2.

También se determinó a través de la auditoría los puertos de comunicación que usan los diferentes servidores que forman la UTN, para desarrollar las diferentes actividades cotidianas dentro de la institución, esta información servirá para poder filtrar, clasificar y priorizar las diferentes aplicaciones previas a la implementación de las políticas adecuadas de QoS.

Una vez finalizada la auditoría de la red y de acuerdo a los datos recolectados se podrá determinar las horas picos de uso, los diferentes protocolos usados, puertos de comunicación, los picos de consumos que determinaran el patrón de comportamiento del tráfico, para poder implementar adecuadas políticas de acuerdo a niveles de organización de las aplicaciones de la red.

III. Priorización de aplicaciones y planeación de mejoras

En esta fase se determinará los servicios, aplicaciones y tráfico que tiene mayor prioridad o importancia dentro de una institución, con lo que se podrá determinar las políticas de calidad de servicio QoS, de acuerdo a la información obtenida en fases anteriores.

Por lo que se deberá realizar:

- Clasificación de aplicaciones y servicios para asignar niveles de prioridad.
- Establecimiento de políticas de QoS de acuerdo a los niveles previamente establecidos.
- Determinación del modelo de QoS que se acople de mejor forma para mejorar el rendimiento de la red.

En esta fase se realizará la respectiva priorización de las aplicaciones que maneja la red de la UTN-FICA, que serán clasificadas de acuerdo al manual de procedimientos y varias recomendaciones que da CISCO en su línea base de configuración de calidad de servicio QoS.

Dentro de esta clasificación se definieron las prioridades de las aplicaciones de acuerdo al grado de importancia que desempeñan dentro de la institución basándose en los recursos anteriormente descritos, quedando la clasificación como se muestra en la figura IV.

Una vez clasificadas las diferentes aplicaciones según su prioridad se procedió a implementar las respectivas políticas de acuerdo a su nivel establecido, donde se le garantizará una reserva de ancho de banda, un mecanismo para evasión y control de congestión, una precedencia de descarte existiendo así un nivel de preferencia de descarte de los paquetes con menor valor DSCP.

TABLA IV
CLASIFICACIÓN DE LAS APLICACIONES SEGÚN SU PRIORIDAD

PRIORIDAD	APLICACIÓN
CRÍTICA	TELEFONÍA IP
	SEÑALIZACION
	VIDEO CONFERENCIA
	VIDEO STREAMING
ALTA	BASES DE DATOS
	APLICACIONES WEB
MEDIA	DNS
BAJA	DHCP
DEFAULT	CUALQUIER OTRO

El ancho de banda para cada clase de tráfico será asignado por el administrador de acuerdo a diversos cálculos que se realizarán, dicho ancho de banda puede ser definido en kbps, en porcentaje del ancho de banda disponible de la interfaz o del ancho de banda remanente de la interfaz, en base a estas asignaciones se definirán las políticas adecuadas para los diferentes tráficos que conforman la red.

IV. Implementación de las políticas

Esta fase conlleva la configuración de equipos involucrados en las fronteras de confianzas (ya sea en switch, router, equipos terminales), con lo que se podrá marcar, diferenciar y aplicar políticas para cada uno de los niveles de prioridad de los diferentes tráficos que circulan por la red de datos, ya sea a la entrada o salida de los mismos. En esta fase se tendrá delimitada nuestra frontera de confianza como se muestra en la figura 3, en la cual se respetará las acciones definidas por el administrador para el tratamiento del tráfico, para la implementación de las políticas de calidad de servicio QoS en la red UTN-FICA, se consideró delimitar la frontera de confianza lo más cerca al origen del tráfico, quedando comprendida entre el switch de distribución CISCO Catalyst 4506-E y los switches de acceso CISCO Catalyst 2960. En el switch de distribución CISCO Catalyst 4506-E se realizará el filtrado, clasificación, marcaje e implementación de las políticas para el tráfico cursante de la red y en los switches CISCO Catalyst 2960 se realizará el control y evasión de la congestión, a través de la respectiva configuración de los equipos.

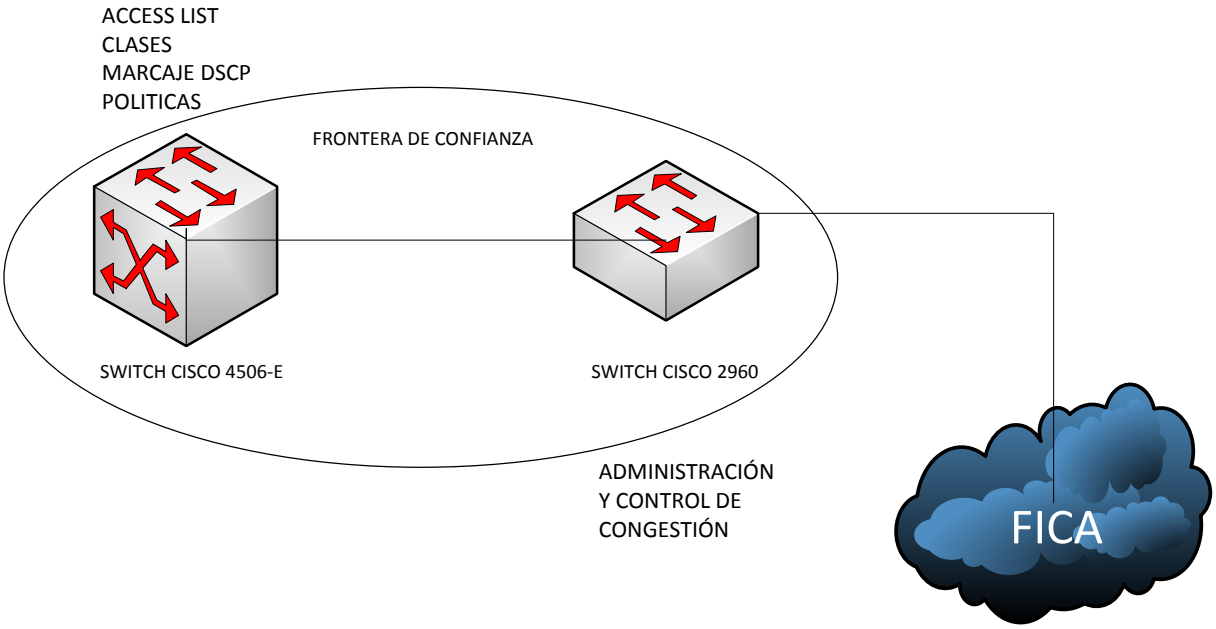

Figura 3: Frontera de confianza dentro la red de la UTN-FICA
Fuente: Dirección de Desarrollo Tecnológico e Informático de la UTN

V. Comparación de resultados

En esta fase se realizará una comparación entre situación precursora de la red y después de las implementación de las políticas de QoS en la red. Con lo que se podrá determinar si el proceso fue el adecuado o no y si cumple o no con los requerimientos determinados. En caso de que el resultado no sea el esperado se tendrá que realizar una reestructuración parcial o en el peor de los casos comenzar nuevamente.

Al implementar políticas de calidad de servicio QoS se debe tomar en consideración varios factores que son evasión de congestión, establecimiento de jerarquías, control de flujo y clasificación del tráfico.

Elección del modelo de calidad de servicio QoS

Como es bien conocido el modelo TCP/IP fue diseñado para brindar un servicio Best-Effort, y por ende no ofrece ningún nivel de garantía para aplicaciones que funcionan en tiempo real, es decir las aplicaciones con voz y video. Existen dos modelos que permiten obtener QoS dentro de una red, diferenciados cada uno en su modo de operación como lo son: servicios integrados (IntServ) y servicios diferenciados (DiffServ), en la tabla V se muestra las ventajas y desventajas entre estos dos modelos.

TABLA V
VENTAJAS Y DESVENTAJAS DE INTSERV-DIFFSERV

MODELO	IntServ (Integrated Services)	DiffServ (Differentiated Services)
Ventajas	Permite que la red mantenga políticas integradas. Permite crear políticas de Calidad de servicio QoS para flujos discretos, conociendo así la disponibilidad de red.	No existe reservación del canal Reduce la carga dentro de la red. Basa en el marcaje de paquetes. Evita los problemas de escalabilidad que plantea IntServ. Clasifica los paquetes por categorías.
Desventajas	Se necesita actualizar periódicamente para mantener la sesión, por consecuente aumenta el tráfico dentro de la red. Se aísla el tráfico de datos por flujos.	No existen reservas, por ende los servicios no están garantizados. Algún equipo intermedio puede cambiar el marcaje previamente definido. Las garantías de QoS no son tan severas.

Referencia: Modelos de QoS "IntServ & DiffServ"
Recuperado de: http://arantxa.ii.uam.es/~ferreiro/sistel2008/anexos/Diff&IntServ.pdf

De las tabla V se puede concluir que DiffServ ofrece mayores ventajas respecto IntServ con respecto escalabilidad, flexibilidad y la distinción para diferentes clases de servicios por medio del marcado de paquetes y

otras técnicas de control de tráfico, siendo esta la alternativa más apta para implementar un esquema adecuado de políticas de calidad de servicio QoS, este modelo se basa en la clasificación de tráfico a través de la diferenciación mediante el uso PHB (Per Hop Behavior).

Al usar DiffServ primero se clasifica el tráfico y seguidamente marcado para un tratamiento diferenciado, de acuerdo a su importancia dentro de una organización, para el marcaje del tráfico en la UTN dentro este modelo se usaran valores DSCP que permite hasta 64 combinaciones de niveles de prioridad, mecanismo de control y evasión de congestión dentro del enlace en donde se implementará las políticas de QoS

Al utilizar este modelo el tráfico en un inicio clasificado y marcado. A medida que fluye en la red va recibiendo distinto trato dependiendo de su marca, dentro de este modelo se debe tomar a consideración los siguientes aspectos: el tráfico es clasificado, las políticas de calidad de servicio son aplicadas dependiendo de la clase y finalmente elegir el nivel de servicio para cada tipo de clase que corresponderá a determinadas necesidades basándose en manuales de procedimientos, recomendaciones para cada una de las diversas aplicaciones dependiendo el nivel de importancia que tiene en la infraestructura de red de la UTN.

En DiffServ, hay cuatro servicios disponibles de PHB`s, que son: Expedited Forwarding (EF) para aplicaciones en tiempo real: VoIP, Assured Forwarding (AF) que asegura que el tráfico sea entregado conforme al perfil contratado por un flujo evitando perdidas, reserva de recursos y ancho de banda garantizado, Best Effort que no ofrece garantía en de ancho de banda asegurado, baja latencia no recomendable para aplicaciones en tiempo real y Class-Selector (CS) que maneja 7 niveles. Las operaciones de clasificación, marcado, política y control de tráfico sólo se realizan dentro de la fronteras de confianza.

I. Elección del método de clasificación del tráfico

Para poder brindar un servicio adecuado a los diferentes tráficos, primeramente hay que identificarlos, por lo que se ha determinado utilizar el método para clasificación de tráfico las Listas de Control de Acceso o ACL`s, que se lo va describir detalladamente a continuación.

Lista de control de acceso ACL`s

Las Listas de Control de Acceso son un mecanismo de seguridad informática usado para clasificar tráficos por separación de privilegios, con lo que se logra determinar los permisos de acceso de equipos en una infraestructura de red. Existen varias ventajas al momento de usar ACL`s son:

- Limitar el tráfico de red y mejorar el rendimiento de la red.
- Brinda control de flujo para cada tipo de tráfico.
- Proporciona un nivel básico de seguridad para el acceso a la red.

Después de implementar las ACL´s se ejecutan en orden secuencial, primeramente se verifica si el paquete cumple con la primera condición, caso contrario se pasan a las siguientes, estas sentencias son las que permiten o niegan un tráfico según su correspondiente caso.

Para implementar las políticas de QoS se realiza ACL`s de tipo permisivas, ya que no se tiene la finalidad de denegar ningún tipo de tráfico, sino el de darle una debida prioridad, pero existe una sentencia implícita que denegará todo tipo de tráfico que no cumpla con las sentencias previamente establecidas.

Para clasificar el tráfico primeramente se lo debe filtrar lo cual se lo realizará mediante la implementación de ACL`s, con lo que se logrará discernir el tráfico que llega a las interfaces del switch CISCO Catalyst 4506-E y de esta forma clasificarlo mediante un traffic class. Se consideró implementar ACL's extendidas ya que permiten elegir origen, destino, puerto y protocolo para el tratamiento de paquetes que entran o salen por una interfaz del equipo. El filtrado de paquetes se realizó en base a la auditoría realizada en donde se obtuvieron los puertos de comunicación que usaban los servidores con los clientes para el intercambio de información.

II. Elección del método de marcaje de tráfico

Para escoger el método para marcar el tráfico, primeramente se tomó a consideración el modelo de QoS escogido el que es DiffServ, determinando así que el marcado del tráfico se lo realizará mediante el DiffServ Code Point (DSCP), que se encuentra especificado dentro de este modelo. El modelo de QoS DiffServ aumenta el número de niveles de prioridad a través de la reasignación de bits de un paquete IP para la identificación de prioridades. Estos bits significativos son tres más conocidos como "IP Precedence".

DSCP permite crear 64 niveles de QoS, sin embargo se utilizan 32 valores. Se debe tomar a consideración que entre más alto sea el valor, el paquete tiene mayor prioridad.

Por lo que se puede concluir que para realizar el marcaje de los paquetes se utilizará DSCP debido a que es la técnica más estandarizada y extendida con diferentes valores de asignación para los diferentes tráficos.

Para el determinar los valores DSCP para cada una de las clases definidas se debe establecer políticas, en las cuales se especificarán el tratamiento que recibe cada una de ellas. Este tratamiento se realizará diversas funciones como son marcado, police, encolamiento o cualquier otra función de DiffServ. El marcado de paquetes se lo realizó en base al manual de procedimientos y también con algunas consideraciones de la línea base de configuración de

calidad de servicio de CISCO quedando el marcaje del tráfico para la red de la UTN de la siguiente forma:

TABLA VI
MARCAJE PARA EL TRÁFICO DE LA RED UTN-FICA

PRIORIDAD	APLICACIÓN	VALOR DSCP
CRÍTICA	TELEFONÍA IP	EF
	SEÑALIZACION	CS3
	VIDEOCONFERENCIA	AF41
	VIDEO STREAMING	AF43
ALTA	BASES DE DATOS	AF31
	APLICACIONES WEB	AF33
MEDIA	DNS	AF21
BAJA	DHCP	AF23
DEFAULT	CUALQUIER OTRO	0

Después de haber definido los valores de marcaje para los diferentes tipos de tráfico que conforman la red, se usará el mecanismo Class-Based Packet Marking, con lo que se proporcionará un marcado eficiente de paquetes, el cual es activado al momento de configurar una política para cada clase definida en la configuración, en este caso se marcará los paquetes usando los bits de IP Precedence, que nos servirán de identificación en la zona de confianza formada por el switch de distribución CISCO Catalyst 4506-E y el switch de acceso CISCO Catalyst 2960.

III. Elección del método de administración de la congestión del tráfico

Para administrar la congestión de red se debe utilizar un mecanismo de encolamiento para controlar situaciones de demanda de ancho de banda elevado y excede el ancho de banda total de la red, controlando la prioridad que se maneja para cada uno de los tráficos dentro de la red.

Se escogió para la implementación de las políticas de QoS al mecanismo de control de congestión mediante el mecanismo de traffic policing, que limitará la tasa de transmisión de una clase de tráfico, basada en criterios definidos por el administrador, permitiendo entre sus funciones la remarcación de paquetes, además realiza diferentes funciones en caso de que el tráfico cursante sobrepase la tasa acordada, permitiendo así a la red un mejor tratamiento de paquetes al momento de presentarse una congestión.

IV. Elección del método de control de congestión y teorías de colas

En este subtema se indicará el mecanismo que tiene la plataforma CISCO Catalyst 2960 para administrar el encolamiento de los paquetes mediante la administración de colas, este mecanismo es SRR (Shaped Round Ribon), que usa para establecer una reserva de ancho de banda de una interfaz que maneja diferentes colas de entrada tanto de entrada como de salida, con lo que se logra que paquetes de baja prioridad hagan uso del recurso del buffer cuando este se encuentre disponible. Al usar este mecanismo se diferencia las clases de tráfico, para evaluar todos los paquetes procesados de acuerdo a umbrales o "thresholds que son asignados a cada cola ya sea de entrada o de salida, que confían en paquetes pre marcados con valores DSCP, y en caso de existir un exceso de estos umbrales los paquetes son descartados.

Dentro de la red de la UTN-FICA se dispone de switch CISCO Catalyst 2960 en la capa de acceso, el cual permite la configuración de 2 colas de entrada y cuatro de salida, con tres umbrales o threshold cada una, teniendo el threshold 3 un porcentaje del 100% por defecto para el uso de los paquetes encolados antes del descarte, las interfaces de este equipo no poseen ningún parámetro de calidad de servicio asignado por lo que se deberá habilitar en modo de configuración global, para que este equipo y todas sus interfaces confíen en los paquetes que viene pre marcados con un valor DSCP del switch de distribución CISCO Catalyst 4506-E.

Delimitación de la frontera de confianza

Una frontera de confianza es el perímetro dentro del cual la red confía y respeta el marcaje que se ha realizado por un equipo sobre o dentro de este perímetro, esta frontera debe ser lo más cercana a la fuente de tráfico.

Por escalabilidad el marcaje y clasificación de tráfico debe hacerse lo más cercano a la fuente de tráfico: en dispositivos terminales, en dispositivos de capa de acceso y distribución.

Para la implementación de las políticas de QoS en la red de la UTN se consideró que la frontera de confianza entre el switch de acceso Catalyst 2960 y switch de distribución Catalyst 4506-E como se muestra en la figura 3.

VI. CONCLUSIONES

Al implementar las políticas de calidad de servicio QoS dentro de la infraestructura de red de la UTN se pudo optimizar el ancho de banda de acceso a internet y control de tráfico para las diferentes aplicaciones que se manejan, mediante el reconocimiento, análisis y control para optimar los recursos, mediante el uso de diferentes políticas para cada tipo de tráfico a través de la clasificación, marcaje, priorización y control de congestión para garantizar un ancho de banda adecuado mediante la segmentación y distribución del mismo.

Existen dos modelos de QoS que son IntServ y DiffServ que realizan diferentes operaciones para priorizar flujos de tráfico, pero para el presente proyecto se escogió el modelo DiffServ ya que ofrece mayores ventajas respecto IntServ en lo referente a escalabilidad, flexibilidad y la distinción para diferentes clases de servicios por medio del marcado de paquetes y otras técnicas de control de tráfico, siendo esta la alternativa más apta para implementar un esquema adecuado de políticas de calidad de servicio QoS.

Al momento de realizar la auditoria de red se pudo determinar la importancia de cada una de las aplicaciones, que fueron agrupados en diferentes prioridades basándose en el manual de procedimiento que podían ser critica, alta, media y baja. Al monitorear constantemente la red se puede llevar un control eficiente del consumo de ancho de banda del tráfico cursante, que ayudarán a determinar el patrón de comportamiento en horas pico o de mayor consumo para determinar las políticas adecuadas de calidad de servicio QoS para el tráfico de la red UTN-FICA.

Al usar un esquema adecuado de políticas de QoS se garantiza a las aplicaciones críticas un ancho de banda adecuado ante aplicaciones de baja prioridad, existiendo descarte de paquetes en clases bajas, de acuerdo a los niveles asignados por el administrador basados en un manual de procedimientos y la tabla de recomendaciones para marcar tráfico de CISCO, que garantizan tener una red basada en niveles o clases de servicio.

Al implementar políticas de calidad de servicio QoS, las aplicaciones en tiempo real se transmiten de forma rápida y eficiente con mejores niveles de servicio que necesitan estas aplicaciones, que serán atendidas primeras ante la presencia de un flujo considerable de datos dentro de una red.

Al implementar calidad de servicio QoS en una red se puede controlar y evadir la congestión, controlando los parámetros como jitter, perdida de paquetes, ancho de anda y retardo, evitando que paquetes importantes o prioritarios tengan que ser descartando causando falencias en las aplicaciones y servicios usados por el usuario.

Dentro de la red de la UTN-FICA al implementar políticas de calidad de servicio QoS se beneficia ya que las aplicaciones no criticas puede ocupar todo el enlace, hasta el momento en que las aplicaciones críticas o con nivel superior soliciten su ancho de banda garantizado, asegurando que las aplicaciones críticas sean las que se transmitan rápidamente y sin eliminar las aplicaciones que cursan en ese momento.

VII. RECOMENDACIONES

Se debe establecer la frontera de confianza ya que es una medida importante en el diseño porque delimitará un perímetro, dentro del cual los diferentes dispositivos respetarán y confiarán en las marcas de QoS realizadas y los dispositivos que la conforman deben estar dentro de nuestro control administrativo y que de acuerdo al dispositivo tendrá la capacidad de realizar unas tareas u otras dependiendo de su nivel.

Se debe contar con políticas de seguridad o un manual de procedimientos adecuado ligados al acceso de los servicios y el uso eficiente de los recursos, y manejar un adecuado nivel de jerarquización de red que facilite la implementación de las políticas de calidad de servicio.

Al realizar una auditoría de red se debe utilizar las herramientas de monitoreo adecuadas que se ajusten a los requerimientos de la red, que consten con diferentes características para monitorear los componentes de la infraestructura, el sistema operativo en el cual se va implementar, vigilar sistemas y aplicaciones, generar diferentes reportes estadísticos del comportamiento de la red, para comprender la situación actual de la red.

Se debe realizar una adecuada clasificación de las aplicaciones dependiendo del grado de importancia o relevancia que tienen dentro de la infraestructura, para mejorar el desempeño y la eficiencia de la red.

Para poder controlar y monitorear adecuadamente la infraestructura tecnológica de red de la UTN, se recomienda obtener herramientas de monitoreo actuales y que se adapten a las necesidades de la red, por lo que es necesario contar con las versiones profesionales ya que éstas permiten tener un grado más amplio en la información del estado de la red de datos a monitorear.

Al adquirir nuevos equipos de conectividad se debe de verificar las versiones de IOS, porque dependiendo de las versiones se podrá establecer si los equipos soportan

calidad de servicio QoS, y por ende poder aplicar las diferentes políticas de QoS.

REFERENCIAS

[1] Adrián Delfino, (2010).Diffserv: Servicios Diferenciados. [Online]. Available: http://iie.fing.edu.uy/ense/asign/perfredes/trabajos/trabajos_2003/diffserv/Trabajo%20Final.pdf

[2] Anónimo, (2012). Arquitecturas de Calidad de servicio (QoS). [Online]. Available: http://es.slideshare.net/c09271/2-2diff-servintserv

[3] Anónimo, (2012). Calidad de servicio (QoS). [Online]. Available:http://technet.microsoft.com/es-s/library/cc757887(v=ws.10).aspx

[4] Ariganello , E., & Barrientos Sevilla, E. (2010). REDES CISCO. CCNP a Fondo. Mexico D.F: Alfaomega.

[5] Carrión, H. (2008) Calidad de servicio. [Online]. Available: http://es.scribd.com/doc/61410997/P-calidad-servicio

[6] CISCO, Comparing Traffic Policing and Traffic Shaping for Bandwidth Limiting [Online]. Available: http://www.cisco.com/en/US/tech/tk543/tk545/technologies_tech_note09186a00800a3a25.shtml

[7] CISCO, Implementación de políticas de Calidad de servicio (QoS) con DSCP [Online]. Available: http://2.bp.blogspot.com

[8] Evans, J., & Filsfils, C. (2007). Deploying IP and MPLS QoS for Multiservice networks Theory and Practice. Estados Unidos: Elsevier.

[9] Hatting, C. (2005). End to End QoS Network Desing. Estados Unidos: Cisco Press.

[10] Marchese, M. (2007). QoS over Heterogeneous Networks. Inglaterra: Wiley.

[11] Rogelio Montaña, (2011). Calidad de servicio (QoS) [Online]. Available: www.uv.es/montanan/ampliacion/amplif_6.ppt

[12] M. Ferreyra. *Advanced Campus QoS Design*. Mayo 2010.

[13] Leonardo Balliache. (2010) Practical QOS. [Online]. Available: http://www.opalsoft.net/qos/WhyQos-2425.htm

[14] T.Sziget y C. Hattingh. *End to End QoS network*. Noviembre. 2004.

[15] CISCO. *Implementing Cisco Quality of Service*. Volumen 1 y 2. 2004

Carlos A. Vásquez A.

Nació en Quito - Ecuador el 19 de Septiembre de 1981. Ingeniero en Electrónica y Telecomunicaciones, Escuela Politécnica Nacional en 2008.

Actualmente es docente de la Carrera de Ingeniería en Electrónica y Redes de Comunicación en la Universidad Técnica del Norte, Ibarra-Ecuador, y es egresado de la Maestría en Redes de Comunicación, Pontificia Universidad Católica del Ecuador, Quito-Ecuador.

Diego F. Paspuel F.

Nació en Ibarra - Ecuador el 1 de junio de 1988. Hijo de Fabián Paspuel y Fátima Fraga. Realizó sus estudios primarios en la Unidad Educativa "La Salle". En el año 2006 obtuvo el título de Bachiller en Físico Matemático en la Unidad Educativa Experimental "Teodoro Gómez de la Torre". Actualmente, es egresado de la Carrera de Ingeniería Electrónica y Redes de Comunicación de la Universidad Técnica del Norte de la ciudad de Ibarra.