UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

ESCUELA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"POLÍTICAS DE QOS DE LA RED LOCAL DE COMUNICACIONES DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA"

AUTOR: MYRIAM ESTEFANÍA MUÑOZ GARCÍA

DIRECTOR: ING. CARLOS VÁSQUEZ

IBARRA, 2016

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA.

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital institucional determina la necesidad de disponer los textos completos de forma digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición el siguiente trabajo:

DATOS DE CONTACTO		
Cédula de Identidad	10033265459	
Apellidos y nombres	Myriam Estefanía Muñoz García	
Dirección	Ibarra, Barrio 1ro de Enero, Antonio Ante 2-41 e Isla Baltra	
Email	migumg@hotmail.com	
Teléfono	Fijo:062601574	Móvil: 0979254047

DATOS DE LA OBRA	
Título	"POLÍTICAS DE QoS DE LA RED LOCAL DE COMUNICACIONES DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA"
Autor	Myriam Estefanía Muñoz García
Fecha	19 de febrero de 2016
Programa	Pregrado
Título por el que opta	Ingeniería en Electrónica y redes en Comunicación
Director	Ing. Carlos Vásquez

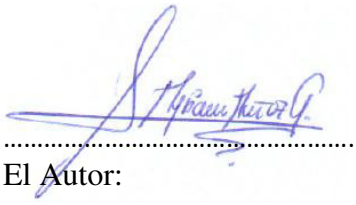
2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Myriam Estefanía Muñoz García, con cédula de identidad Nro. 1003265459, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en Repositorio Digital Institucional y el uso del archivo digital en la biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión, en concordancia con la ley de Educación Superior Artículo 144.

3. CONSTANCIA

El autor manifiesta que la obra objeto de la presente autorización es original y se desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y es titular de los derechos patrimoniales, por lo que se asume la responsabilidad del contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

En la ciudad de Ibarra a los 19 días del mes de febrero de 2016.



.....

El Autor:

Myriam Estefanía Muñoz García

CI: 100326545-9

UNIVERSIDAD TÉCNICA DEL NORTE

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo**, Myriam Estefanía Muñoz García**, con cédula de identidad Nro. 1003265459, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la ley de propiedad intelectual del Ecuador, articulo 4, 5 y 6, en calidad de autora del trabajo de grado denominado: **"POLÍTICAS DE QOS DE LA RED LOCAL DE COMUNICACIONES DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA"**, que ha sido desarrollado para optar por el título de Ingeniería en Electrónica y Redes de Comunicación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En mi condición de autora me reservo los derechos morales de la obra antes mencionada, aclarando que el trabajo aquí descrito es de mi autoría y que no ha sido previamente presentado para una calificación profesional.

En constancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la biblioteca de la Universidad Técnica del Norte.

.....

Firma

Myriam Estefanía Muñoz García

CI: 100326545-9

En la ciudad de Ibarra a los 19 días del mes de febrero de 2016.

DECLARACIÓN

Yo, Myriam Estefanía Muñoz García, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que este no ha sido previamente presentado para ningún grado o calificación profesional.

A través de la presente declaración cedo los derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las leyes de propiedad intelectual, del reglamento y normativa vigente de la Universidad Técnica del Norte.

.....

Myriam Estefanía Muñoz García

CERTIFICACIÓN

Certifico que el presente trabajo de titulación "POLÍTICAS DE QOS DE LA RED LOCAL DE COMUNICACIONES DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA" ha sido realizada en su totalidad por la Srta. Myriam Estefanía Muñoz García portadora de cédula de ciudadanía 100326545-9.

Ing. Carlos Vásquez Ayala

Director del Proyecto

DEDICATORIA

Este trabajo lo dedico en primer lugar a mi mami, Amparito, quien hizo de mi lo que soy con su amor infinito e incansable ejemplo de esfuerzo , trabajo y honestidad; a mis mamis: Coisito, Gladys, Magui, que me han dado su amor y apoyo incondicional; a mi ñaño Alex, a mi papi Byron, a mi padre de corazón Ivancito, a Milton, Gonzalito y Mayto; a mis pequeñas Lety y Kiki, a mis enanos Osquitar, Francis y Nena, a mi precioso Alan a mis hermanos Jane, Maty, Jairi, Ely, Linkito, Ivani, Dome, Yoma, Miriam, Antony, Paula, Keny, Dianita.

AGRADECIMIENTO

Mi agradecimiento a Dios, que me ha acompañado en cada momento, a mi madre y toda a mi familia, el pilar fundamental de mi vida, gracias por su amor incondicional.

Al Ing. Carlos Vásquez, muchas gracias por su guía, paciencia y apoyo desde el inicio de este proyecto, al Ing. Jaime Michilena, gracias por su ayuda y confianza; a mis profesores por sus conocimientos y enseñanzas.

A Javier más que mi compañero, amigo y apoyo incondicional.

A la Dirección de TIC del Gobierno Autónomo Descentralizado de San Miguel de Ibarra, por su apertura y colaboración, un agradecimiento especial al Ing. Manuel Lara.

A esas personas especiales que se convirtieron en entrañables amigos quienes a lo largo de mi vida me han apoyado, demostrando siempre buena voluntad y cariño: Eve, Gaby, Jesy, Taty, Diego A., Diego P., Pabli E., Rodo, Juanis, Edus, Raque, Lau, Majito, Normi, Queiter y Silvano.

Myriam Muñoz García.

RESUMEN GENERAL

El proyecto propuesto consiste en realizar el diseño de políticas de Calidad de Servicio (QoS) para la red local del Gobierno Autónomo Descentralizado de San Miguel de Ibarra, el mismo permitirá mejorar el rendimiento de la red.

Se inició con un análisis del estado inicial de la red y de las aplicaciones de la misma para junto con los administradores definir las condiciones óptimas. A continuación se utilizó herramientas de software libre para realizar un análisis del tráfico cursado y obtener parámetros relevantes para el diseño de las políticas.

Con la información obtenida del análisis anterior se procedió a establecer las políticas de Calidad de Servicio: separando las diferentes clases de tráfico, definiendo prioridades, métodos de encolamientos y anchos de banda para cada una de ellas.

Con las políticas de QoS planteadas, se inició la implementación de un ambiente de prueba, tan similar como sea posible a la red real del Gobierno Autónomo Descentralizado de San Miguel de Ibarra, el cual posibilite configurar políticas mediante los recursos de software o hardware necesarios. Para esto se utiliza el simulador GNS3.

Finalmente en el ambiente de prueba se realizó el análisis del comportamiento de tráfico de la red, para comparar la red sin aplicar QoS y la red aplicando QoS, para determinar los cambios que se han producido y comprobar que el proceso se ha llevado a cabo correctamente.

ABSTRACT

The proposed project consists in design Quality of Service (QoS) policies for the Gobierno Autónomo Descentralizado de San Miguel de Ibarra Local Area Network, it will improve the network a better performance.

It started with an analysis of the initial state of the network and applications in order to define the optimal conditions with administrators. Then with free software tools it made an analysis of traffic carried and got the most important parameters to design the politics.

Using the information obtained from the above analysis it proceeded to establish Quality of Service policies: separating the different classes of traffic, defining priorities, queuing methods and bandwidths for each class.

With the QoS policies established, it started to implement a test environment, as similar as possible to the real Gobierno Autónomo Descentralizado de San Miguel de Ibarra Local Area Network, which enables set policies through necessary software or hardware resources. For this the GNS3 simulator is used.

Finally in the test environment it analyzed the traffic behavior in the LAN in order to compare the network unapplied QoS between the network applying QoS, to determine changes that have occurred and assure that the process was right.

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ECUACIONES

ANTECEDENTES

- **PROBLEMA**

Las redes de comunicaciones, extienden cada día su cantidad de usuarios y los servicios que ofrecen, a menudo se inicia con una infraestructura básica, con equipos para conectividad únicamente, y se van agregando a ésta las nuevas prestaciones de la red, si este proceso no se realiza con el debido dimensionamiento puede causar problemas en el rendimiento y disponibilidad de la red, causando cuellos de botella, perdida de información (descarte de paquetes). La red inicial de Gobierno Autónomo Descentralizado San Miguel de Ibarra, era sencilla y relativamente pequeña, en los últimos años ha crecido, existen nuevos servicios web tanto para usuarios internos como para el resto de la ciudadanía, nuevas prestaciones en el sistema interno del municipio, aplicaciones con mapas de la ciudad para uso de los diferentes departamentos , mayor cantidad de usuarios, interconexiones con redes externas como la red inalámbrica en las parroquias, comunicación con otras entidades públicas.

El Gobierno Autónomo Descentralizado San Miguel de Ibarra, cuenta con una infraestructura de red heterogénea, con miras al crecimiento de servicios; la falta de procesos de administración, provoca que los usuarios indistintamente consuman ancho de banda en exceso y desequilibren la red, cabe mencionar que se ha mantenido el mismo ancho de banda inicial para todas las aplicaciones que la red soporta. Si la red no está optimizada se puede presentar también congestión en la misma, impidiendo que las aplicaciones existentes dentro de la red, no cumplan su objetivo de una manera correcta, actualmente se está implementando VoIP, que es una aplicación en tiempo real y que requiere

un tratamiento adecuado para lograr buen funcionamiento, surge la necesidad de priorizar el tráfico en la red.

Para solucionar los problemas que se puedan presentar en la red, es necesaria la implementación de procesos que permitan mejorar el uso de recursos (ancho de banda), como por ejemplo marcado y priorización de paquetes, además de herramientas de administración con parámetros de calidad de servicio y monitoreo de la red, con el fin de potenciarla, optimizar sus recursos y prevenir fallas.

- **OBJETIVOS**

Objetivo General

Diseñar políticas de QoS en la red local del Gobierno Autónomo Descentralizado de San Miguel de Ibarra, mediante un análisis del comportamiento del tráfico, la situación actual y las necesidades de la entidad que garantice un mejor rendimiento y disponibilidad de la red.

Objetivos Específicos

- Describir los elementos principales de una red con parámetros de calidad de servicio y también las herramientas de software libre para monitoreo del tráfico de la red, que sirvan como fundamento de los procesos de implementación de QoS
- Analizar la situación actual de la red local del Gobierno Autónomo Descentralizado San Miguel de Ibarra, para la definición de los requerimientos de la misma.
- Realizar el monitoreo y análisis estadístico del tráfico cursante en la red, estableciendo el comportamiento de la misma, la clasificación y requerimientos del tráfico.

- Definir las políticas de QoS para cada clase de tráfico, de acuerdo a los requerimientos obtenidos del monitoreo y situación actual.
- Realizar la implementación, en un entorno de prueba, de las políticas QoS previamente analizadas.
- Efectuar el monitoreo de la red después de la implementación de políticas de QoS para la realización de un análisis comparativo con el comportamiento inicial de la red y constatación del mejoramiento de las prestaciones.

- **ALCANCE**

El presente proyecto, comenzará con un estudio de los fundamentos teóricos de los parámetros de calidad de servicio y herramientas de monitoreo de red. Seguidamente se inicia el proceso de QoS, empezando con el análisis de la situación actual de la red local del Gobierno Autónomo Descentralizado San Miguel de Ibarra; describiendo sus recursos, para definir la arquitectura, establecer la función que cumplen los diferentes elementos de la red y determinar en donde se implementará la calidad de servicio, así por ejemplo las fronteras de confianza para el proceso de marcado.

Lo siguiente es analizar el comportamiento del tráfico de la red local, esto se efectuará con herramientas de Software libre y permitirá identificar los tipos de tráfico y sus requerimientos, luego se clasificara el tráfico de la red de acuerdo a los requerimientos identificados. Una vez realizado esto, se debe determinar el mejor modo de separar las clases específicas de tráfico, definir prioridades, métodos de encolamientos, los flujos correctos y anchos de banda para cada una de ellas, es decir se deben plantear políticas de

acuerdo a las necesidades de la institución y a los requerimientos obtenidos en los estudios previos.

Con la información y políticas de QoS planteadas, se procederá a implementar un ambiente de prueba, similar a la red real del municipio, el cual posibilite configurar políticas mediante los recursos de software o hardware necesarios, dentro de estos procesos se pueden mencionar: marcaje, administración de cola, listas de acceso (ACL), que son una herramienta fundamental para el filtrado de los diferentes tipos de tráfico.

En el ambiente de prueba se realizará el análisis del comportamiento de tráfico de la red, para comparar con el estado inicial, determinar los cambios que se han producido y comprobar que el proceso de QoS se ha llevado a cabo correctamente.

- **JUSTIFICACIÓN**

En la red del Gobierno Autónomo Descentralizado San Miguel de Ibarra, se cursa información relevante para la ciudad y sus habitantes, es por eso que esta información merece ser tratada de manera correcta y para que esto ocurra, la infraestructura de red debe funcionar bajo condiciones óptimas. Es clave administrarla apropiadamente, debido a que esta red soporta diversos tipos de tráfico, como voz y datos; es una red convergente por lo cual se debe tomar en cuenta los tipos de aplicaciones y las condiciones para que estas funcionen, la VoIP, por ejemplo es muy sensible al retardo y jitter, por el contario otras aplicaciones como correo, no lo son; es necesario el uso de mecanismos que permitan a estos tipos de tráfico coexistir.

Los diversos servicios que ofrece la red, precisan una correcta administración, que permita: el control sobre los recursos como el ancho de banda, el conocimiento de la manera en que la red está siendo usada, mejorar el rendimiento y disponibilidad; propiciando de esta manera el comportamiento adecuado de la red al momento de cursar aplicaciones críticas, esto se logra mediante la Calidad de Servicio.

La implementación de políticas de Calidad de Servicio en la red del Gobierno Autónomo Descentralizado San Miguel de Ibarra, no solo permitirá tener un control sobre los recursos de la red y el uso más eficiente de los mismos, sino que además garantizará un óptimo funcionamiento de las diversas aplicaciones en la red, ya que se pueden controlar la congestión y las colas, la priorización de tipos de tráfico, disminuyendo el retardo y sus fluctuaciones (jitter), que son problemas que afectan principalmente a aplicaciones en tiempo real, como la VoIP.

CAPÍTULO 1

1 INTRODUCCIÓN: CALIDAD DE SERVICIO Y HERRAMIENTAS DE SOFTWARE LIBRE PARA MONITOREO DE LA RED

1.1 CALIDAD DE SERVICIO EN REDES

1.1.1 INTRODUCCIÓN: DEFINICIÓN DE QoS (QUALITY OF SERVICE, CALIDAD DE SERVICIO) EN UNA RED CONVERGENTE

Hoy en día existe un crecimiento en las redes de comunicaciones, tanto en la tecnología como en las aplicaciones que ofrecen, las redes en la actualidad soportan voz, video y datos en una misma infraestructura. La convergencia de estas aplicaciones se traduce en un reto, pues se debe lograr el funcionamiento óptimo de las mismas; cada aplicación tiene ciertos parámetros a cumplirse para que sea aceptable, debe considerarse la voz y el video como aplicaciones críticas, pues son sensibles al retardo. Para lograr el funcionamiento correcto de las aplicaciones es necesario implementar en la red políticas de QoS (Calidad de Servicio). Sin la implementación adecuada de herramientas de QoS, las aplicaciones que no requieran procesamiento en tiempo real, podrían utilizar la capacidad de transferencia disponible y de esta manera impedir la transferencia de aplicaciones críticas o de tiempo real.

Existen varias definiciones de calidad de servicio:

Calidad de servicio es "un conjunto de requisitos de servicios que han de ser satisfechos por la red mientras transporta una conexión o flujo; el efecto colectivo de la calidad de servicio que determina el grado de satisfacción de un usuario del servicio" (UIT-T , recomendación E.360.1, 2002, p. 6)

Calidad de servicio "es un conjunto de requisitos de servicio que debe cumplir la red durante el transporte de un flujo". (IETF , RFC 2386, 1998, p. 2)

Calidad de servicio "es una medida de la capacidad de las redes y sistemas informáticos para proporcionar diferentes niveles de servicio para seleccionar los flujos de aplicaciones y de red asociados". (Braun, Diaz, Enríquez Gabeiras, & Staub, 2008, pág. 1)

Podría definirse la calidad de servicio como la capacidad de una red que permite garantizar servicios a las aplicaciones, para que se efectúen de manera adecuada, mediante un tratamiento específico para cada una de ellas.

1.1.2 PARÁMETROS DE CALIDAD DE SERVICIO

1.1.2.1 **Ancho de Banda disponible**

En general el ancho de banda se refiere a la capacidad del canal. Habitualmente un paquete fluye por el camino con mejor ancho de banda. "El mejor ancho de banda disponible en la ruta es el del enlace con menor ancho de banda. El ancho de banda disponible es el mayor ancho de banda de una ruta dividido entre el número de flujos." (Ariganello & Barrientos Sevilla, 2010, pág. 792)

La falta de ancho de banda puede provocar problemas en las aplicaciones de la red, los cuales pueden evidenciarse en retardo o pérdida de paquetes. Estos problemas se pueden solucionar de varias formas como: usar técnicas de compresión, incremento de ancho de banda o la aplicación de QoS, en procesos como clasificación, marcado y encolamiento adecuados del tráfico de la red, para poder asegurar que los paquetes fluyan de forma apropiada. Esta última es la opción más recomendable pues las dos primeras utilizan muchos recursos de software y tienen un alto costo económico respectivamente.

1.1.2.2 **Retardo de extremo a extremo**

Al periodo de tiempo que tarda un paquete para llegar desde su origen a su destino, se conoce como retardo o retraso, las aplicaciones en tiempo real (VoIP y video) son sensibles al retardo, existen varios tipos de retardo:

1.1.2.2.1 Retardo de procesamiento:

Es el tiempo que tarda un dispositivo de capa 3 en recibir un paquete por la interfaz de entrada, procesar la información pertinente y ponerlo en la interfaz de salida

1.1.2.2.2 Retardo de encolamiento:

Es el tiempo que un paquete permanece en la cola de una interfaz, esto depende del tipo de cola configurado, de la utilización del enlace y el número de paquetes.

1.1.2.2.3 Retardo de serialización:

"Es el tiempo empleado en poner en el medio físico todos los bits de una trama"

(Ariganello & Barrientos Sevilla, 2010, p. 793)

1.1.2.2.4 Retardo de propagación:

Es el tiempo que tarda la información en viajar por el medio físico, depende principalmente del tipo de medio físico

1.1.2.3 **Jitter**

Es la variación del retardo de los paquetes (Ver Figura 1) que forman parte de un mismo flujo de datos, se produce debido a que el paquete llega al destino a una velocidad distinta a la velocidad de emisión.

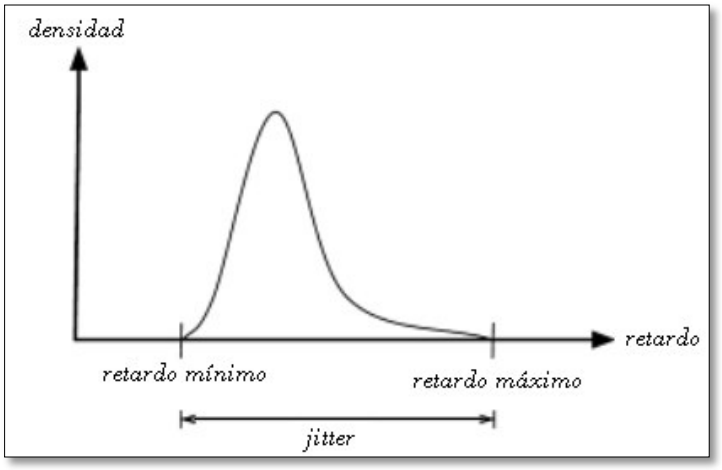


Figura 1. Jitter

Referencia: (Braun, Diaz, Enríquez Gabeiras, & Staub, 2008, p. 3)

En VoIP y video los paquetes deberían llegar al destino en el mismo orden y velocidad con los que fueron emitidos; pero esto no siempre sucede debido a procesos como: espera en cola, cambios de ruta, perdida de sincronización, que hacen que haya variación en el retardo en estas aplicaciones impidiendo su desarrollo adecuado. La implementación de mecanismos de QoS ayuda a mitigar estos efectos.

Para mejorar el jitter se debe hacer uso de un buffer, llamado de-jitter buffer o jitter buffer para almacenar y los paquetes que llegan y de RTP[1], que permite que los paquetes sean entregados en orden.

El uso eficiente de la red acompañado de la correcta administración de tráfico y su ancho de banda también hacen posible mejorar el jitter.

1.1.2.4 **Pérdida de Paquetes**

Se refiere al número de paquetes que no llegan al destino en relación a todos los paquetes enviados. Los dispositivos pueden descartar paquetes por distintas razones por ejemplo si el buffer de su interfaz de salida está lleno, no puede almacenar otros paquetes que llegan por lo tanto debe descartarlos. La Ecuación 1 muestra el cálculo de la tasa de perdida de paquetes (Braun, Diaz, Enríquez Gabeiras, & Staub, 2008, p. 4).

$$tasa\ de\ perdida\ de\ paquetes = \frac{paquetes\ enviados - paquetes\ recibidos}{paquetes\ enviados} \quad \textbf{(1)}$$

[1] RTP Real Time Transport Protocol (Protocolo de Transferencia en Tiempo Real), Este protocolo define un formato de paquete estándar para el envío de audio y video sobre Internet, está definido en el RFC1889.

La pérdida de paquetes se relaciona directamente con el tipo de protocolo utilizado por las aplicaciones pues en el protocolo TCP hay reenvío de paquetes descartados o erróneos mientras que, en el protocolo UDP, que es utilizado para aplicaciones en tiempo real, no se realiza el reenvío debido a que en estas aplicaciones no es posible realizar retransmisiones por los estrictos requisitos de retardo que tienen, además de que se genera más tráfico en la red.

1.1.3 PROCESO DE IMPLEMENTACIÓN DE CALIDAD DE SERVICIO

Para la implementación de calidad de servicio en una red se debe cumplir con un proceso que asegure que las políticas de QoS sean las más apropiadas para la red. Este proceso se debe cumplir los siguientes pasos:

- "Identificar tipos de tráfico y sus requerimientos
- Clasificar el tráfico basándose en los requerimientos especificados
- Definir las políticas para cada clase" (Ariganello & Barrientos, 2010, p.795).

1.1.3.1. Identificación de Tráfico y requerimientos

Es el primer paso a realizarse en una implementación de calidad de servicio, la identificación del tráfico y sus requerimientos incluye:

1.1.3.1.1 Auditoria de la red:

Dentro de esto es importante definir una estructura física de la red que se refiere a su topología y las funciones y características de dispositivos de red principales; y también la estructura lógica, que se obtiene mediante la monitorización del software y aplicaciones

cursadas por la red. Este monitoreo se debe hacer tanto durante las horas pico de utilización de la red como en otros periodos.

1.1.3.1.2 Determinación de la importancia de cada aplicación

Esto dependerá de la empresa en donde se realice la auditoria, pues son las necesidades de la misma las que dan la pauta para determinar la importancia de cada aplicación, aquí también se definen las clases de tráfico.

1.1.3.1.3 Definición de niveles de servicio para cada clase de tráfico

Para las clases de tráfico previamente identificadas, se debe establecer un nivel de servicio en el cual figuran parámetros como ancho de banda garantizado, retardo, etc.

1.1.3.2 **Clasificación del Tráfico**

Las clases de tráfico van a depender de la empresa y sus características, en la mayoría de las redes empresariales suelen haber las siguientes clases de tráfico:

- *Clase de VoIP:* Por los requerimientos de esta clase es la de mayor prioridad.
- *Clase de Misión Crítica:* Son las aplicaciones de alta importancia dentro en la red empresarial
- *Clase de tráfico de señalización:* Es el tráfico de señalización para aplicaciones como video o el tráfico del protocolo SIP para establecimiento de llamadas de VoIP.
- *Clase de Aplicaciones de transacción*: como las bases de datos interactivas u otros servicios similares.

- *Clase Best-Effort*: Es el tráfico que no pertenece a las clases anteriores y se le asigna el ancho de banda sobrante.
- *Clase sin importancia:* Son aplicaciones consideradas inferiores a las de la clase Best-Effort, como: juegos online, aplicaciones P2P, etc.

1.1.3.3 **Definición de Políticas**

Este constituye el paso final del proceso, e incluye tareas como:

- La asignación de un ancho de banda máximo para una clase
- La asignación de un ancho de banda mínimo garantizado para una clase
- Establecer niveles de prioridad de acuerdo a las clases
- Uso de mecanismos adecuado para la congestión, gestionando o eliminando la misma

1.1.4 MODELOS DE CALIDAD DE SERVICIO

1.1.4.1 **Modelo Best-Effort**

Básicamente es un modelo en el cual no se aplica ninguna política de calidad de servicio, lo que significa que el tráfico es enviado y tratado por igual, sin procedimiento específico para ningún flujo de información. No se garantiza fiabilidad, los límites de retardo, o el rendimiento a ninguna aplicación.

Este modelo presenta la ventaja de facilidad pues no requiere mecanismos o configuraciones especiales.

En una red que soporta múltiples clases de aplicaciones simultáneamente, el término Best-Effort se refiere al servicio más bajo contemplado dentro del SLA

1.1.4.2 **Modelo de Servicios Integrados (Intserv)**

Este modelo se basa en la reserva de recursos, que permitan soportar los requerimientos de SLA para cada tipo de aplicación.

Su funcionamiento es el siguiente: de acuerdo al SLA cada aplicación tiene un tipo de servicio el cual comprende parámetros como ancho de banda y requisitos de retardo, la aplicación solicita un tipo específico de servicio a la red antes del envío de los datos. Esta solicitud se realiza mediante señalización explícita, luego la aplicación informa a la red de su perfil de tráfico y solicita el tipo particular de servicio correspondiente de acuerdo al SLA. La señalización explícita se realiza mediante el protocolo RSVP.

1.1.4.2.1 RSVP (Resourse Reservation Protocol)

RSVP es el protocolo usado para la reserva de recursos en la red. Este protocolo puede ser usado en tráfico de multidifusión y unidifusión, y aplicaciones para TCP y UDP, para que funcione, todos los nodos de la red deben soportar RSVP.

Para realizar la reserva, el modelo de Servicios Integrados se basa en descriptores de flujo para caracterizar el tráfico de red; esto consiste en:

FilterSpec es un filtro de especificación que muestra la identificación del origen y el destino del flujo.

FlowSpec es una especificación de flujo con información sobre las características del tráfico y la petición de reserva.

Los dos mensajes más importantes que utiliza RSVP para la creación de la reserva de recursos son PATH y RESV (Ver Figura 2).

PATH: Estos mensajes se envían junto con los paquetes regulares, así cada router puede saber el salto anterior, lo que permite que los mensajes RESV que viajen en dirección contraria vayan por el mismo camino.

RESV: Estos paquetes son los que en realidad llevan la solicitud de reserva.

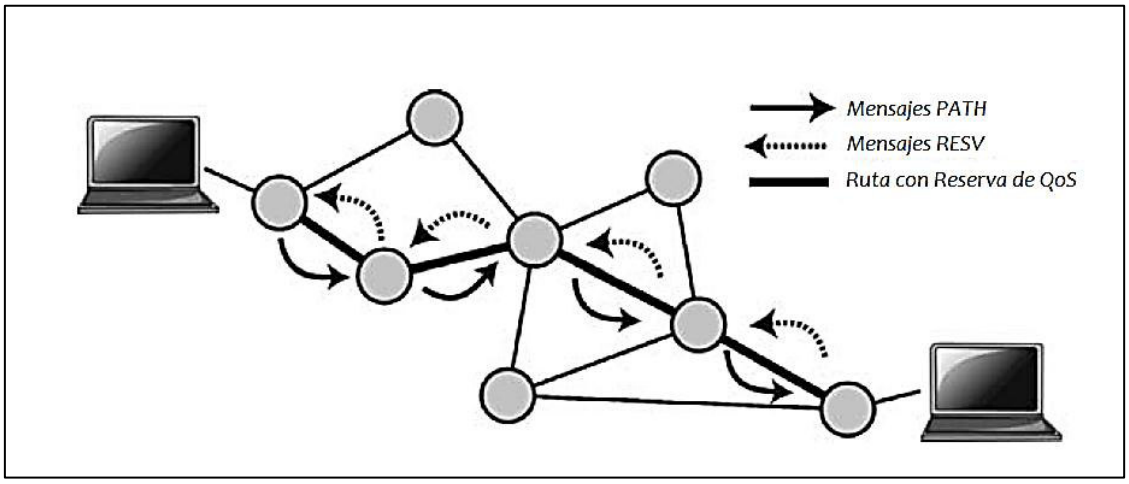


Figura 2. Creación de la reserva mediante mensajes PATH y RESV

Referencia (Braun, Diaz, Enríquez Gabeiras, & Staub, 2008, p. 13)

1.1.4.3 **Modelo de Servicios Diferenciados (Diffserv)**

Trata de superar los problemas de escalabilidad que tiene Intserv, ya que en este modelo este no requiere señalización, resultando en disminución del flujo de tráfico. Diffserv se basa en la clasificación del tráfico y el PHB (Per Hop Behavior, Comportamiento por salto).

En este modelo, el control de admisión no se realiza en el núcleo, evitando procesamiento en los que los equipos que pertenecen al mismo; de hecho una de las mejoras de diffserv es

que las funciones de clasificación y control del tráfico son realizados en el borde, lo que lo hace un modelo escalable.

La clasificación del tráfico en Diffserv se realiza basada en el marcado de paquetes mediante un código único utilizando los 6 bits más significativos del campo de ToS (Type of Service, Tipo de Servicio) de la cabecera IP, denominada DSCP. Este código identifica a todos los flujos con el mismo criterio de clasificación, para los cuales el router debe tener un comportamiento específico. La diferenciación de servicios se obtiene basada en el comportamiento de reenvío asignado a un DSCP denominado PHB. El PHB define si un paquete se reenvía o descarta.

Un dominio DS (Servicios Diferenciados), está formado por los nodos de frontera los mismos que realizan el tratamiento del tráfico basado en especificaciones del SLA, como se muestra en la Figura 3

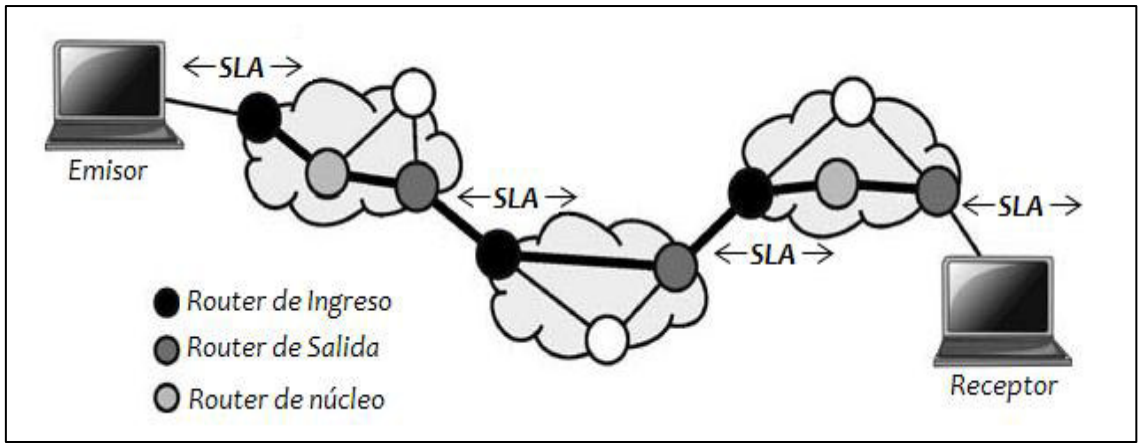


Figura 3. Diffserv en una red

Referencia (Braun, Diaz, Enríquez Gabeiras, & Staub, 2008, p. 15)

1.1.4.4 **Análisis comparativo Intserv vs Diffserv**

Es importante realizar un análisis comparativo entre los dos últimos modelos, para poder utilizarlo más adelante en el diseño de políticas de QoS.

En la Tabla 1, se realiza la comparación de las principales características de Intserv vs Diffserv.

Tabla 1. Comparación entre IntServ y DiffServ

INTSERV	**DIFFSERV**
QoS garantizado por flujos de trafico	QoS garantizado por agregación de trafico
Administración de recursos distribuidos	Administración de recursos centralizados
Este modelo requiere mecanismo de señalización explícita para transmitir información, como RSVP	En este modelo no se requiere de mecanismos de señalización.
Requiere reservar recursos previamente, para lograr calidad de servicio.	Tiene como objetivo marcar los paquetes con prioridad y enviarlo a la red, sin reserva previa de los recursos.
Modelo por flujo de datos.	Es un modelo que es apropiado para los flujos agregados.
Garantía de QoS a corto plazo mientras dura la sesión	Garantía de QoS a largo plazo

Referencia: Between "IntServ vs DiffServ" Recuperado de: http://www.slideshare.net/c09271/2-2diff-servintserv

En la Tabla 2 se presentan las ventajas y desventajas de cada modelo:

Tabla 2. Ventajas y desventajas de IntServ y DiffServ

DiffServ	
VENTAJAS	DESVENTAJAS
Mejora los servicios de mejor esfuerzo proporcionadas por internet, mediante la diferenciación del tráfico.	Si bien es fuerte en la simplicidad, pero muy débil al momento de ofrecer garantías.
DiffServ es altamente escalable y relativamente menos complejo, al no requerir estado por flujo a ser almacenados en los routers, y al no utilizar protocolos de señalización complejos	No se recomienda su uso para usuarios finales.
El modelo DiffServ tiene como objetivo proporcionar clases de servicio.	
IntServ	
VENTAJAS	DESVENTAJAS
IntServ es adecuado para redes privadas más pequeñas, intranets o redes troncales ISP.	Cuando el ancho de banda está reservada para una determinada aplicación, no puede ser reasignado para otra aplicación.
IntServ puede proporcionar garantías por el flujo con límites firmes sobre el ancho de banda y el retardo	No se recomienda este modelo en red como el internet, debido a su poca flexibilidad al crecimiento.
El modelo DiffServ tiene como objetivo proporcionar clases de servicio.	

Referencia: Between “IntServ vs DiffServ” Recuperado de: http://www.slideshare.net/c09271/2-2diff-servintserv

1.1.5 ADMINISTRACIÓN DE TRÁFICO

1.1.5.1 **Clasificación y Marcaje**

El proceso de clasificación se refiere a identificar y categorizar tipos de tráfico en clases, y el marcado en cambio se refiere a etiquetar el tráfico basado en su categoría. (Ariganello & Barrientos, 2010).

El marcado puede ser de Capa 2:

- Clase de Servicio: CoS en la Trama Etehrnet 802.1Q/P
- EXP en MPLS
- DE en Frame Relay

O de Capa 3:

- DSCP
- IP precedence

A continuación se describe cada tipo de marcado.

1.1.5.1.1 Clase de Servicio: CoS en la Trama Ethernet 802.1Q/P

IEE 802.1Q , es un estándar para enlace troncal entre switches, que añade a la cabecera Ethernet original 4 bytes, dentro de los cuales se encuentra el campo CoS de 3 bits, definido en el estándar IEE 802.1P (Ver Figura 4), el mismo que permite establecer 8 niveles de prioridad (Ver tabla 3) como un mecanismo básico para marcar el tráfico, y en consecuencia diferenciarlo y proveer QoS.

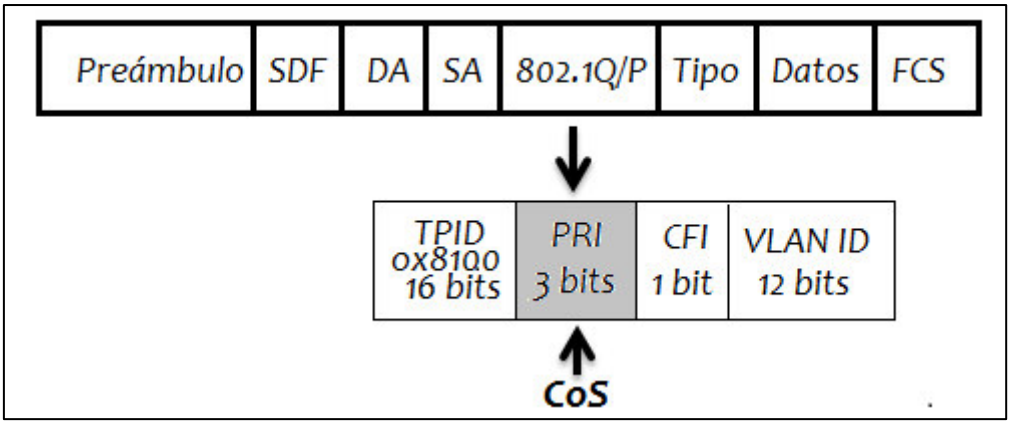


Figura 4. Campo CoS en la cabecera Ethernet

Referencia NetworkLife, ONT - Classification, Marking, NBAR (2010) recuperado de http://www.networklife.net/2010/06/ont-classification-marking-nbar/

Tabla 3. Valores de los bits CoS 802.1p

CoS (bits)	CoS (Decimal)	IETF RFC791	Aplicación
000	0	Routine	Datos
001	1	Priority	Datos de media prioridad
010	2	Inmediate	Datos de alta prioridad
011	3	Flash	Señal de llamada
100	4	Flash-Override	Videoconferencia
101	5	Critical	Voz
110	6	Internet	Reservado (inter-network control)
111	7	Network	Reservado (network control)

Fuente (Ariganello & Barrientos Sevilla, 2010, p. 808)

1.1.5.1.2 EXP en MPLS

En cada etiqueta de un paquete MPLS, se encuentra un campo de 3 bits, llamado EXP (Ver Figura 5), que se utiliza con propósitos de QoS, por ejemplo puede contener información sobre el tratamiento para el reenvío de un paquete, utilizado en el modelo Diffserv. Al tener 3 bits "es compatible con IP precedence y CoS" (Ariganello & Barrientos Sevilla, 2010, pág. 810)

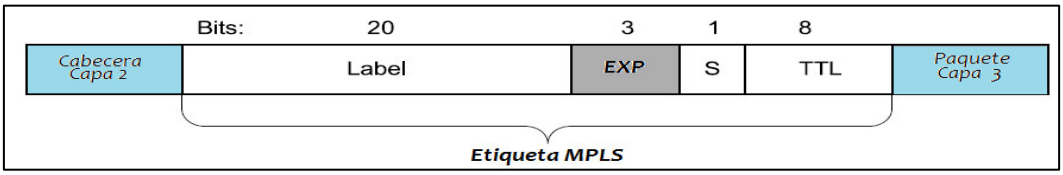


Figura 5. Campo EXP en la etiqueta MPLS

Referencia (Ariganello & Barrientos Sevilla, 2010, p. 810)

1.1.5.1.3 DE (Discard Elegibility) en Frame Relay

Si en una red Frame Relay, hay gran volumen de tráfico, se puede utilizar el bit de DE de la cabecera de Frame Relay (Ver Figura 6), mediante el cual se elige los paquetes que deben ser descartados, Frame relay también proporciona una notificaciones de congestión a través de los campos FECN y BECN.

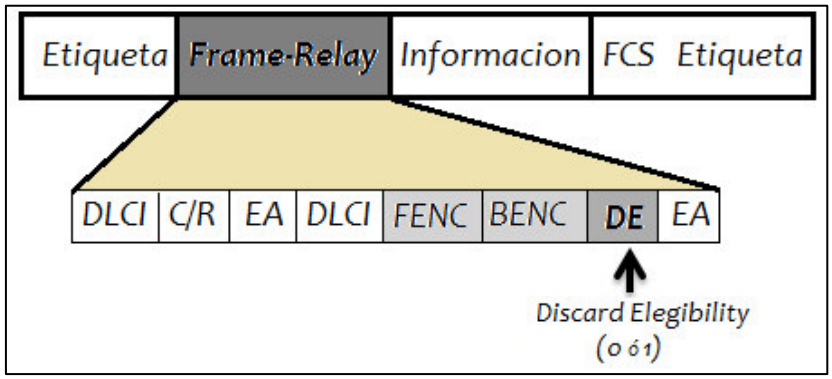


Figura 6. DE (Discard Elegibility) en Frame Relay

Referencia (Ariganello & Barrientos Sevilla, 2010, p. 809)

1.1.5.1.4 DSCP (Differentiated Services Code Point, Punto de Código de Servicios Diferenciados)

De la redefinición del campo ToS de la cabecera IP nace el campo DSCP, mostrado en la Figura 7, el cual como se mencionó en la sección 1.1.4.3 está formado por los 6 bits más significativos del campo ToS.

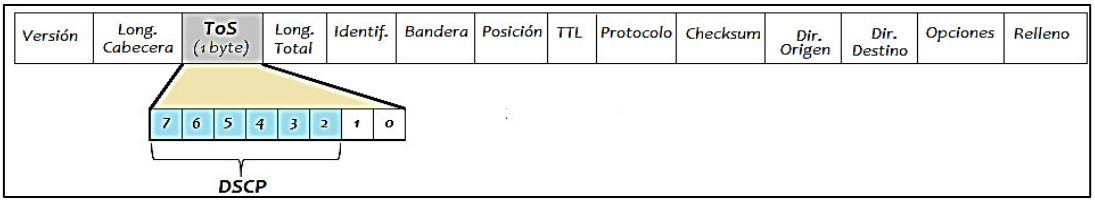


Figura 7. Campo DSCP en la cabecera IP

Referencia: Debian & Comunicación, Quality of Service: ToS, CoS y otros bits (2012) Recuperado de http://debian-comunicacion.blogspot.com/2012_03_01_archive.html

Las combinaciones de estos bits permiten tener 4 tipos de PHB, de acuerdo a los valores de DSCP asignados, los cuales se muestran en la Tabla 4.

Tabla 4. Tipos de PHB de acuerdo a las combinaciones de los bits DSCP

Bits DSCP						**TIPO**
-	-	-	0	0	0	Selector de Clase PHB
0	0	0	-	-	0	PHB por defecto
0	0	1	-	-	0	PHP Assured Forwarding
0	1	0	-	-	0	
0	1	1	-	-	0	
1	0	0	-	-	0	
1	0	1	1	1	0	PHB Expedite Forwarding

Fuente: (Ariganello & Barrientos Sevilla, 2010, p. 812)

Selector de Clase PHB: Se obtiene compatibilidad con IP precedence, al setear en 000 los 3 bits menos significativos del DSCP. (Ariganello & Barrientos, 2010).

PHB por defecto: resulta en Best Efford, utilizando los 3 bits más significativos del DSCP.

PHB Assured Forwarding (AF): Utiliza los 3 bits más significativos del DSCP, en sus diferentes combinaciones, y es usado para garantizar ancho de banda. Proporciona cuatro clases de reenvío diferentes que se pueden asignar a un paquete. Cada clase de reenvío proporciona tres precedencias de descarte. AF permite asignar distintos niveles de servicio a clientes y aplicaciones para priorizar tráfico y servicios, no obstante no asegura ninguna garantía para caudales, retardos.

PHB Expedite Forwarding (EF): usado para servicios de bajo retardo, los 3 bits más significativos del DSCP están seteados en 101. EF, Asegura que tráfico marcado con el valor de DSCP correspondiente tiene la máxima prioridad; no se pone en cola. De esta manera proporciona una pérdida de datos, latencia y demora mínimos. El valor DSCP recomendado para EF es 101110. Se encuentra definido en el RFC 2598.

En la Tabla 5, se muestran todos los valores para DSCP, según se explica en los párrafos anteriores:

Tabla 5. Valores para el campo DSCP

DECIMAL	BINARIO	DETALLE	TIPO
62	111110	Reservado	Control de Red
60	111100	Reservado	
58	111010	Reservado	
56	111000	Precedencia 7 (Routing & Control)	
54	110110	Reservado	Control de Red
52	110100	Reservado	
50	110010	Reservado	
48	110000	Precedencia 6 (Routing & Control)	
46	101110	EF (Premium)	Expedited
44	101100	Configuración de Usuario.	Forwarding
42	101010	Configuración de Usuario.	
40	101000	Precedencia 5	
38	100110	AF43	Assured
36	100100	AF42	Forwarding
34	100010	AF41	Class 4
32	100000	Precedencia 4	
30	011110	AF33	Assured
28	011100	AF32	Forwarding
26	011010	AF31	Class 3
24	011000	Precedencia 3	
22	010110	AF23	Assured
20	010100	AF22	Forwarding
18	010010	AF21	Class 2

16	010000	Precedencia 2	
14	001110	AF13	Assured
12	001100	AF12	Forwarding
10	001010	AF11	Class 1
8	001000	Precedencia 1	
6	000110	Configuración de Usuario	Best Effort
4	000100	Configuración de Usuario	(Default)
2	000010	Configuración de Usuario	
0	000000	Precedencia 0 (Routing & Control)	

Fuente: (Ariganello & Barrientos Sevilla, 2010) pags: 812-813

1.1.5.1.5 IP precedence

El uso de IP precedence está definido en le RFC 291, en el cual se define a precedence como una medida independiente de la importancia de cada paquete IP. IP precedence permite marcar el tráfico de acuerdo a su importancia con los 3 bits más significativos del campo ToS de la cabecera IP (Ver figura 8), es importante mencionar que es compatible con DSCP y CoS.

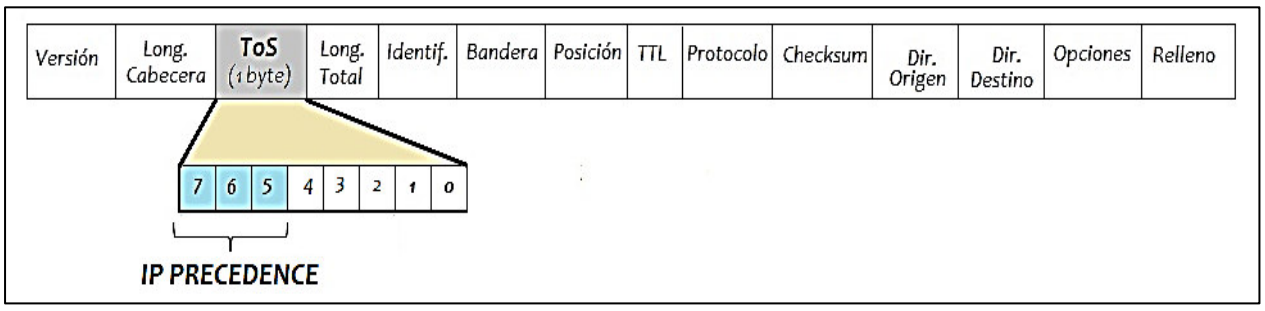


Figura 8. IP precedence en la cabecera IP

Referencia: Debian & Comunicación, Quality of Service: ToS, CoS y otros bits (2012) Recuperado de http://debian-comunicacion.blogspot.com/2012_03_01_archive.html

Al utilizar 3 bits permite ocho niveles de prioridad mientras más importante sea el paquete más alta su prioridad. La Tabla 6 contiene los valores posibles de IP Precedence.

Tabla 6. Valores posibles de IP Precedence.

IP PRECEDENCE		
Decimal	**Binario**	**Nombre**
000	0	Routine
001	1	Priority
010	2	Inmediate
011	3	Flash
100	4	Flash-Override
101	5	Critical
110	6	Internet
111	7	Network

Fuente (Ariganello & Barrientos Sevilla, 2010, p. 811)

"Los valores 6 y 7 son usados por diferentes protocolos en su tráfico de gestión y no está permitido que se configuren para aplicaciones" (Ariganello & Barrientos, 2010, p.811)

1.1.5.2 **Fronteras de confianza**

Es un perímetro formado de equipos que están asignados para realizar el marcaje de paquetes, toda la red confiará y respetará el marcaje que hagan únicamente estos quipos y el marcaje hecho por otros equipos fuera de este perímetro será descartado.

Para determinar la frontera de confianza es importante considerar que los equipos que a los cuales se les asigne esta responsabilidad deben estar dentro de nuestro control

administrativo y deben soportar las características de QoS requeridas; además las fronteras de confianza deben delimitarse lo más cerca posible del origen de tráfico (Ver figura 9), entonces la frontera de confianza podrá estar ubicada en: sistema final, capa acceso o capa de distribución.

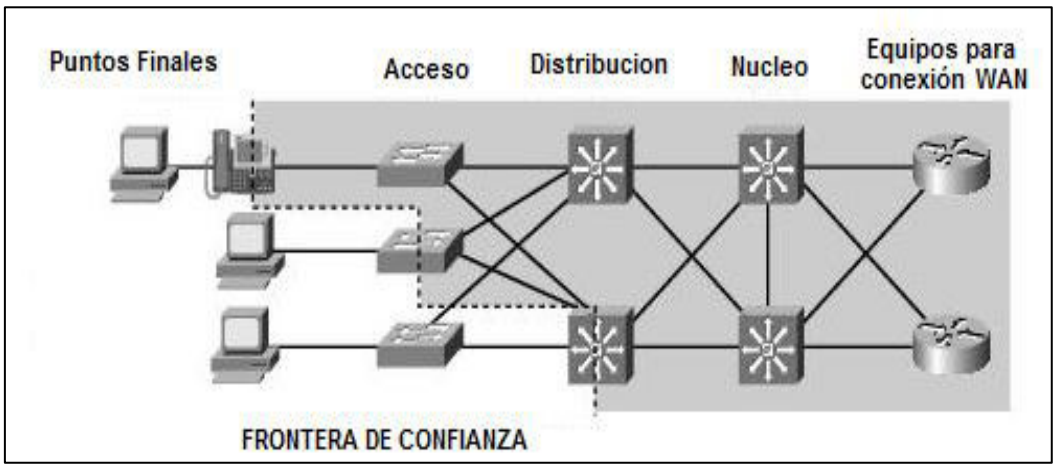


Figura 9. Frontera de confianza

Referencia: CISCO, Campus QoS Design (2012), Recuperado de http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoSDesign.html

1.1.5.3 **Encolamiento: Control de Congestión**

Si el tráfico que llega a un dispositivo requiere un ancho de banda mayor que el disponible en la interfaz, se produce congestión en la red. En redes en las cuales la congestión es temporal se pueden implementar diversas técnicas de encolamiento; de manera general encolamiento es el mecanismo que controla la forma en que los buffers administran los paquetes mientras esperan para ser transmitidos. A continuación los diversos tipos de encolamiento serán descritos.

1.1.5.3.1 FIFO (First IN-First OUT)

El algoritmo FIFO (el primero en entrar es el primero en salir) es el más elemental; los paquetes son enviados en el mismo orden en que llegan, sin tomar en cuenta la clase o prioridad de los paquetes simplemente se considera su orden de llegada. En su forma más simple los paquetes son almacenados si hay congestión en la red y enviados cuando se tiene la posibilidad, la falencia de este mecanismo se evidencia en la limitación de la capacidad de su búfer en momentos de congestión (Ver figura 10) y no es adecuado para Qos, se podría implementar en interfaces rápidas con poca probabilidad de congestión.

Este método puede ocasionar un problema debido a que algunas aplicaciones de descarga como FTP pueden saturar el enlace evitando el paso de paquetes de VoIP, o dejando pasar solamente algunos, causando llamadas entrecortadas.

FIFO, es el método configurado por defecto en la mayoría de las interfaces, excepto en las interfaces de menos de 2,048 Mbps de capacidad.

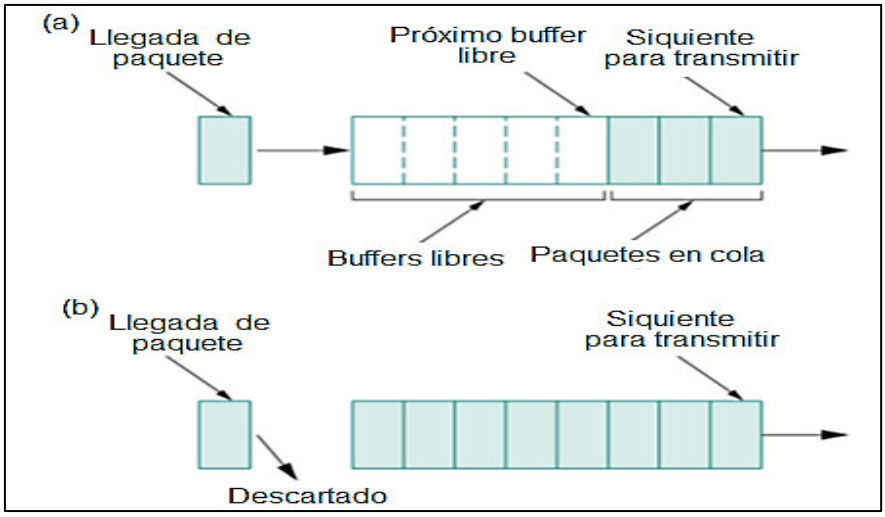


Figura 10. Algoritmo FIFO

Referencia: Chari, G, Clase de Qualtity of Service Capa de red (10/2012) Recuperado de http://www.dc.uba.ar/materias/tc/2012/2c/descargas/clasespracticas/calidaddeservicio

1.1.5.3.2 PQ (Priority Queuing)

Este tipo de encolamiento requiere clasificación del tráfico, determinando que tipo de tráfico pertenece a cada una de las 4 colas de prioridad de las que dispone; estas son:

- Alta
- Media
- Normal
- Baja

Mediante la priorización se asegura que el tráfico importante reciba un servicio más rápido en cada punto de la red, donde este mecanismo este implementado. Las prioridades se definen por filtros en los routers, diferenciadas por parámetros como: el protocolo de red, la interfaz del router por el que llegue el paquete, el tamaño del paquete y la dirección de origen o destino.

Los paquetes que estén en la cola de prioridad alta, se enviarán hasta que esté vacía, luego se envían los de prioridad media, luego vuelve a verificar la prioridad alta, si no hay paquetes, revisa nuevamente la prioridad media, si está vacía, pasa a la prioridad normal y envía solamente un paquete y vuelve a verificar la cola de prioridad alta, y así sucesivamente, como se explica en la Figura 11, PQ siempre prioriza el tráfico perteneciente a la cola de prioridad alta (Ariganello & Barrientos Sevilla, 2010)

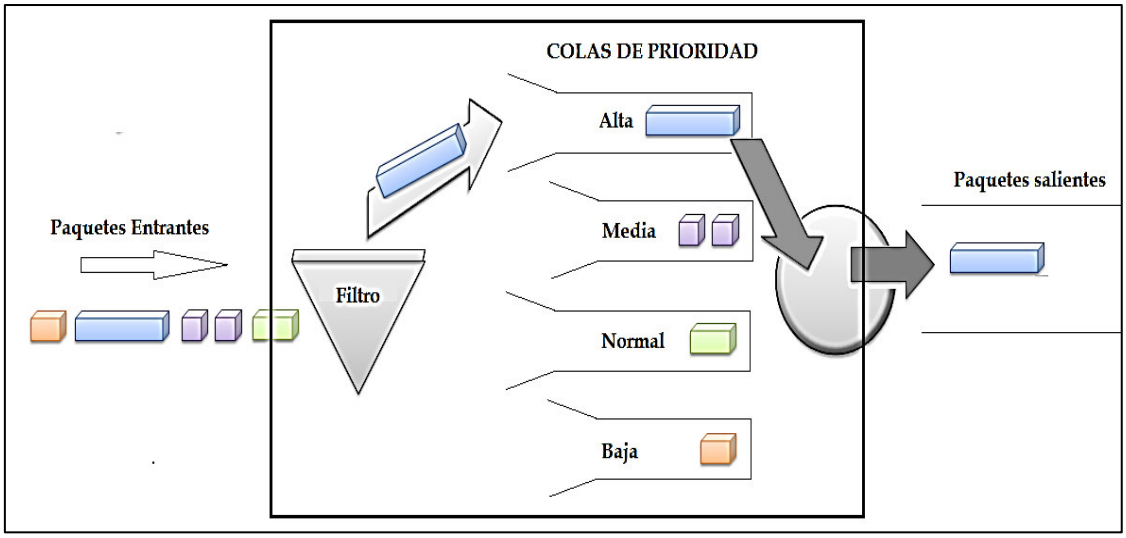


Figura 11. Mecanismo de Priority Queuing

Referencia CISCO,Troubleshooting Output Drops with Priority Queueing (2008) Recuperado de http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a0080103e8a.shtml

1.1.5.3.3 RR (Round Robin)

Round Robin asigna diversas colas de prioridad, a las cuales les da igual trato; es decir un paquete de cada cola es enviado, primero, de la prioridad más alta, luego pasa a la siguiente, y a la siguiente, hasta llegar a la prioridad más baja, y nuevamente regresa a la prioridad más alta y así sucesivamente. Aunque a cada cola se le asigna un tipo de tráfico, no se lo diferencia pues cada cola tiene el mismo trato.

Puede considerarse un método equitativo, aunque si una de las colas tiene paquetes de mayor tamaño estaría gozando de mayor prioridad pues enviaría mayor cantidad de datos en cada turno.

1.1.5.3.4 WRR (Weighted Round Robin)

Este método tiene una cola para cada tipo de tráfico y a cada una se le asigna un peso (Ver Figura 12), el cual corresponde al ancho de banda permitido o dicho de otra forma a la cantidad de tráfico. Los paquetes son enviados de acuerdo al peso de cada cola.

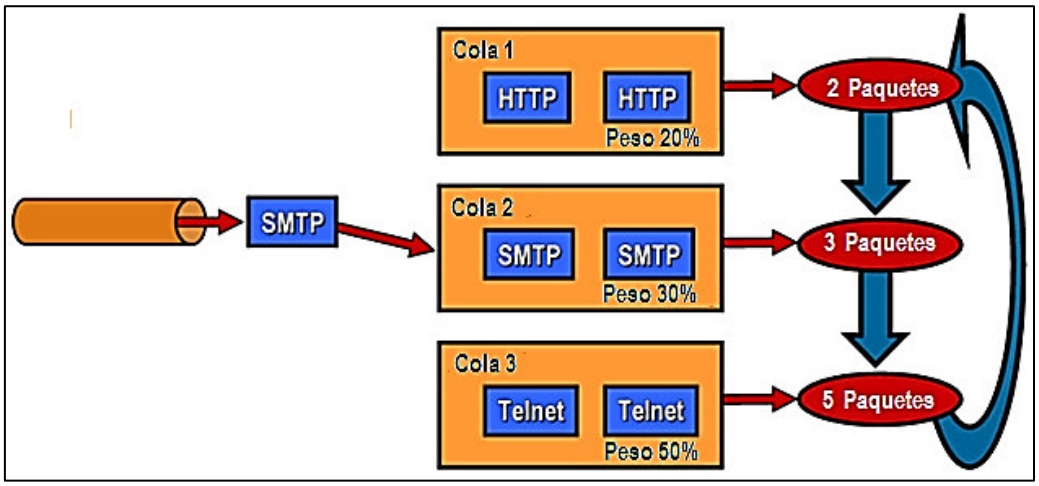


Figura 12. Mecanismo de Weighted Round Robin

Referencia HILL ASOCIATES, Weighted round robin queuing (2007), Recuperado de: http://www.hill2dot0.com/wiki/index.php?title=Weighted_round_robin

1.1.5.3.5 WFQ (Weighted Fair Queuing)

El algoritmo de este método consiste en dividir el tráfico en flujos y, a estos flujos se les asigna un ancho de banda adecuado; los flujos con mayor prioridad tienen mayor ancho de banda y los de poco volumen son despachados mas rapidamente. Este metodo ayuda a eliminar retraso y jitter.

La categorización de flujos se realiza basado en parametros como: direccion IP origen o destino, protocolo, campo ToS, número de puerto TCP/UDP de origen o destino. Basado en los valores de estos parametros, se genera un cifrado para un determinado flujo; como cada

flujo tiene el mismo cifrado, se asignará a la misma cola. Cabe aclarar que debido a que se necesita acceder a la informacion de la cabecera , WFQ no se puede utilizar con encriptación.

Si todos los flujos tienen el mismo peso y nivel de prioridad , WFQ divide en ancho de banda en forma equitativa, entre los flujos existentes. El número de colas es es dinámico, de acuerdo al número de flujos, WFQ añade o borra colas según se precise.

1.1.5.3.6 CBWFQ (Class Based Weighted Fair Queuing)

Este tipo de encolamiento permite que se establezcan clases manualmente; las clases se definen basadas en parámetros como protocolos, ACL o interfaces de entrada.

A cada clase se le asignan características específicas como una cola, un peso y un ancho de banda mínimo, que es el ancho de banda garantizado que se entregará a esta clase en caso de una congestión en la red, por supuesto al referirnos a un ancho de banda mínimo hay la posibilidad de que se emplee más ancho de banda en caso de estar disponible.

"CBWFQ, permite la creación de hasta 64 colas, cada una de las cuales es de tipo FIFO, con un ancho de banda garantizado y un número máximo de paquetes" (Ariganello & Barrientos Sevilla, 2010, p. 829). En congestión, es decir cuando el número de paquetes llegue al número máximo establecido para la cola FIFO, se producirá un tail drop, esto puede ser controlado con métodos como WRED.

CBWFQ, proporciona mayor control sobre el tráfico colocado en cola y el ancho de banda se asigna a flujos particulares.

Tail Drop, es un proceso que como se mencionó anteriormente, se produce al llenarse una cola, y no es más que descartar los paquetes entrantes sin importar su tipo o importancia.

WRED, es un mecanismo que ayuda prevenir el tail drop. WRED descarta paquetes pero permite determinar, que paquetes descartar, haciendo posible dar mayor prioridad (basada en IP precedence o DSCP) a ciertos tipos de tráfico; esto lo hace mediante la configuración de perfiles como umbral máximo o umbral mínimo, que se pueden aplicar a un subconjunto de tráfico destinado a una cola.

1.1.5.3.7 LLQ (Low-Latency Queuing)

LLQ es un método importante debido a que es utilizado para aplicaciones en tiempo real, este tiene una cola específicamente dedicada a aplicaciones en tiempo real. Esta es la cola de prioridad estricta, puede definirse más de una cola estricta. LLQ, posee los mismos métodos que CBWQ, solo que con la adición de prioridad estricta.

1.1.5.4 **Manipulación de tráfico**

El control del tráfico permite asegurar niveles de servicio en una red, controlar los flujos de tráfico significa controlar los recursos de la red y asegurar que se cumplan los requerimientos para los cuales la red ha sido diseñada, existen varios mecanismos que permiten la manipulación del tráfico para su control, dentro de los cuales se puede mencionar Shaping y Policing. Antes de definir estos mecanismos se debe abordar el concepto de Token Bucket.

1.1.5.4.1 Qué es un Token Bucket?

Un colector de testigos es un buffer que actúa como un contenedor el cual tiene dos elementos: la tasa que la denominaremos R (Rate) y Burst (B).

- La tasa(R) especifica la cantidad de datos pueden ser enviados o reenviados, medida normalmente en bps.
- Burst (B), que es la capacidad máxima del colector medida en bits.

Dependiendo de la aplicación particular los tokens se añaden al contenedor a una tasa(R), o bien cada vez que se procesa un paquete o cada cierto tiempo, en intervalos regulares hasta que se llegue a la cantidad máxima de tokens (Ver Figura 13). El número mínimo de tokens en el contenedor es cero.

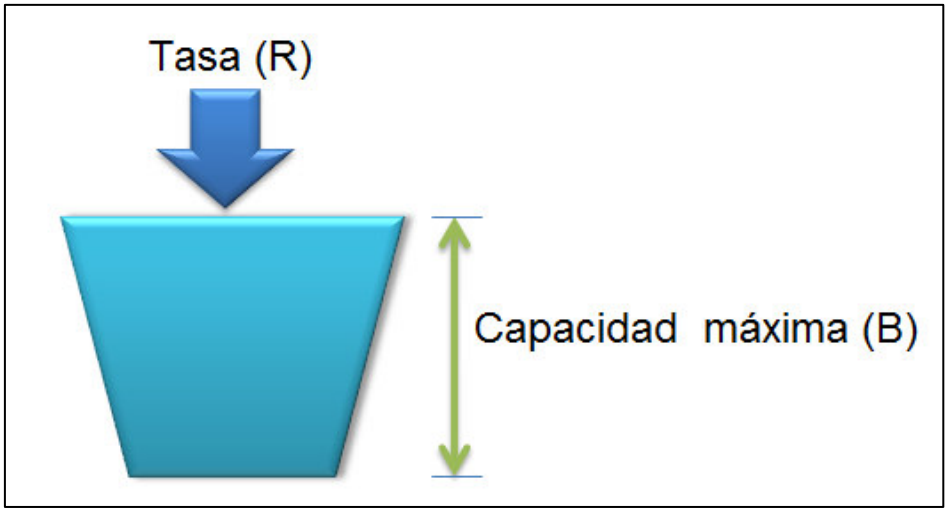


Figura 13. Token Bucket

Referencia (Evans & Filsfils , 2007, p. 101)

1.1.5.4.2 Shaping

Es un mecanismo mediante el cual, utilizando buffers se puede retrasar o limitar el tráfico, logrando así que no exceda la velocidad definida, este mecanismo se aplica en la salida del tráfico (Ver Figura 14).

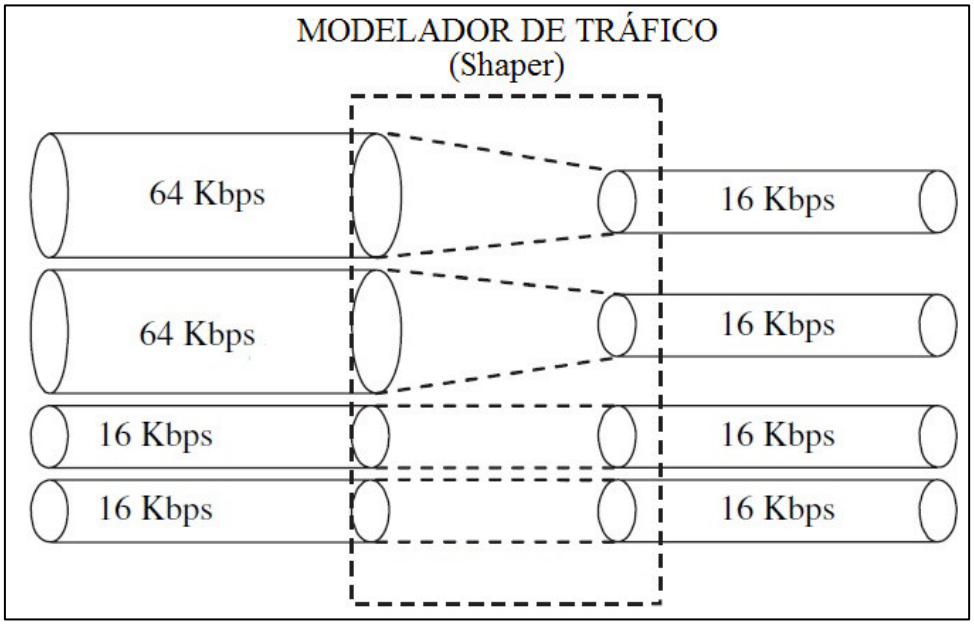


Figura 14. Shaper (Modelador de tráfico)

Referencia (Marchese, 2007, pág. 50) QoS over Heterogeneus network

Shaping utiliza un token bucket para realizar el siguiente proceso: cuando un paquete llega el tamaño de este se compara con el número de tokens que está actualmente en el contenedor: Si hay por lo menos tantos tokens en el contenedor como bytes en el paquete, entonces el paquete se transmite sin demora. Si hay menos tokens en el contenedor, que bytes en el paquete, entonces el paquete es retrasado (en una cola, por lo tanto, está implícito que el shaping debe utilizarse junto con el encolamiento) hasta que haya suficientes tokens en el contenedor, cuando los tokens son suficientes, el paquete se envía y el contenedor decrementa el número de tokens en el mismo número de bytes que contenía el paquete enviado. (Evans & Filsfils , 2007)

Además de token bucket, shaping también utiliza otro método denominado, leaky bucket (contenedor agujereado), basado en el algoritmo "Generic Cell Rate Algorithm" (GCRA) que fue estandarizado por ATM en 1996, se tuvo que hacer cambios ya que la unidad de información de ATM es de 53 bytes, mientras que los paquetes IP, tienen longitud variable. El concepto básico es que los paquetes, en lugar de tokens, entran y son almacenados en un contenedor con un orificio en la parte inferior, el cual está situado en los nodos de borde de la red y además tiene definido una capacidad máxima igual que el token bucket; que define el número máximo de paquetes que en él pueden ser almacenados. Si llega un paquete cuando el contenedor ya está lleno, el paquete es descartado. Los paquetes continuamente están fluyendo a través del orificio, es decir, se transmiten, a una tasa constante R, suavizando así ráfagas de tráfico (Ver Figura 15).

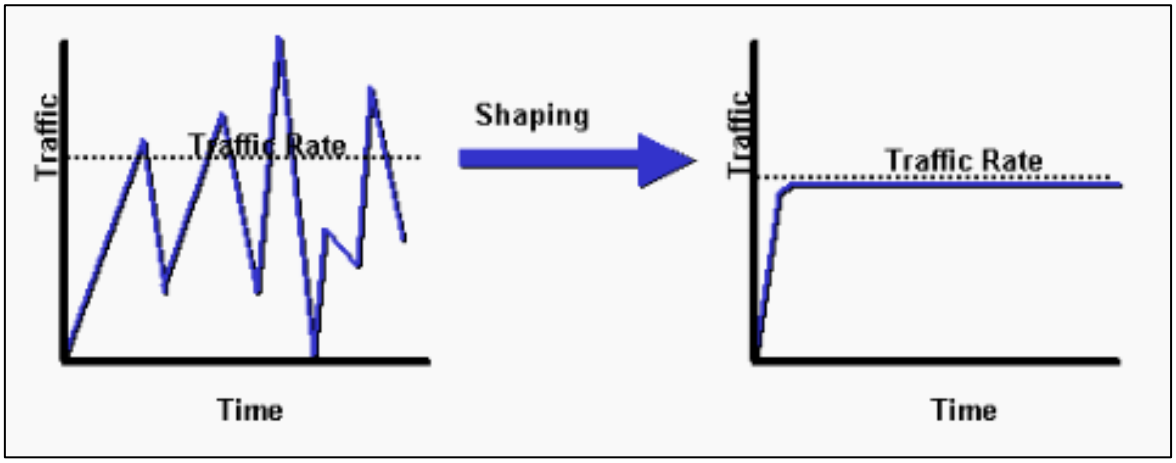


Figura 15. Efecto de Shaping en el tráfico

Referencia: CISCO, Comparing Traffic Policing and Traffic Shaping for Bandwidth Limiting Recuperado de : Ñhttp://www.cisco.com/en/US/tech/tk543/tk545/technologies_tech_note09186a00800a3a25.shtml

El shaping es aplicable en casos como disminuir la velocidad en una red WAN, o el envío de diversas clases de tráfico con una velocidad diferente establecida para cada clase de tráfico.

1.1.5.4.3 Policing

A diferencia del shaping que retrasa el tráfico, policing lo elimina o marca como "non-conformant", realizando la acción de cortar los picos de tráfico (Ver Figura 16). Este mecanismo se puede aplicar a la salida o a la entrada.

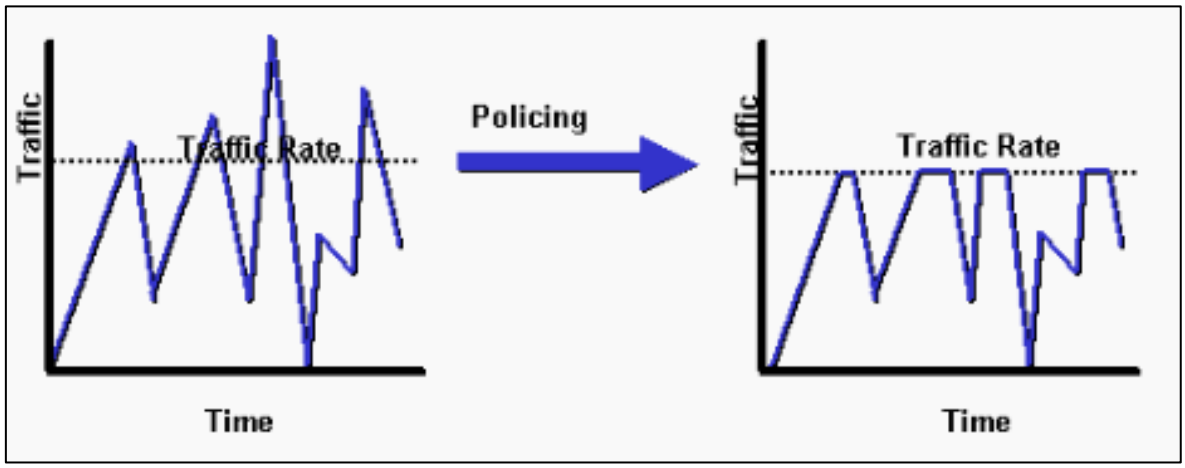


Figura 16. Efecto de Policing en el tráfico

Referencia: CISCO, Comparing Traffic Policing and Traffic Shaping for Bandwidth Limiting Recuperado de : Ñhttp://www.cisco.com/en/US/tech/tk543/tk545/technologies_tech_note09186a00800a3a25.shtml

Este mecanismo también se basa en un token bucket (colector de testigos), con las siguientes acciones: cuando un paquete llega el tamaño de este se compara con el número de tokens que está actualmente en el contenedor: Si hay por lo menos tantos tokens en el contenedor como bytes en el paquete, entonces el paquete se marca como "conformant". Si hay menos tokens en el contenedor, que bytes en el paquete, entonces el paquete se marca como "exceded" o non-conformant. Si el paquete fue marcado como "conformant" el contenedor decrementa el número de tokens en el mismo número de bytes que contenía el paquete enviado.

Dependiendo de si el paquete es "conformant" o "exceded" (non-conformant), se pueden tomar diferentes acciones; las más simples son, para "conformant" transmite y para "exceded" descarta (Ver Figura 17).

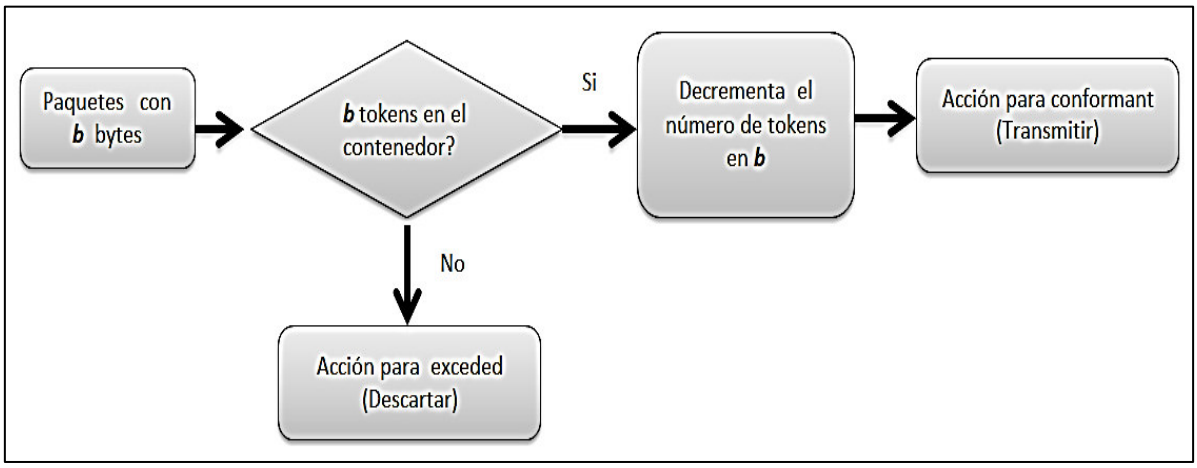


Figura 17. Algoritmo de Policing

Referencia (Evans & Filsfils , 2007, pág. 102)

1.1.6 GESTIÓN DE QoS MEDIANTE FIREWALL

1.1.6.1 Introducción

Se ha revisado en este capítulo varios parámetros que se deben configurar para obtener calidad de servicio en una red, estos parámetros se configuran en dispositivos de red como routers y switches; pero también se pueden implementar mecanismos de calidad de servicio en un servidor firewall.

1.1.6.2 Parámetros de QoS configurables dentro de un firewall

Mediante un firewall y dependiendo del tipo que este sea se pueden realizar varios filtros, en caso de estar trabajando dentro de la capa de red, es posible filtrar paquetes.

En software libre se implementan filtros mediante Iptables y varios comandos, los cuales permiten determinar paquetes a aceptar o rechazar, incluso es posible modificar el campo

ToS para el marcado de paquetes mediante el comando mangle. Con el comando tc "Traffic Control" se puede realizar la creación de clases.

Mediante el uso de firewalls sea estos propietarios o con software libre se pueden configurar la mayoría de parámetros que permiten implementar en una red políticas de calidad de servicio para aprovechar mejor sus recursos.

1.2 JERARQUIZACIÓN DE LA RED

La construcción de una red con un modelo jerárquico permite que esta se administre y expanda con mayor facilidad y los problemas se resuelven con mayor rapidez. El diseño de redes jerárquicas implica la división de la red en capas independientes. Cada capa cumple funciones específicas que definen su rol dentro de la red general. La separación de las diferentes funciones existentes en una red hace que el diseño de la red se vuelva modular y esto facilita la escalabilidad y el rendimiento.

El modelo de diseño jerárquico típico se separa en tres capas (Ver Figura 18):

- Capa de acceso
- Capa de distribución
- Capa núcleo

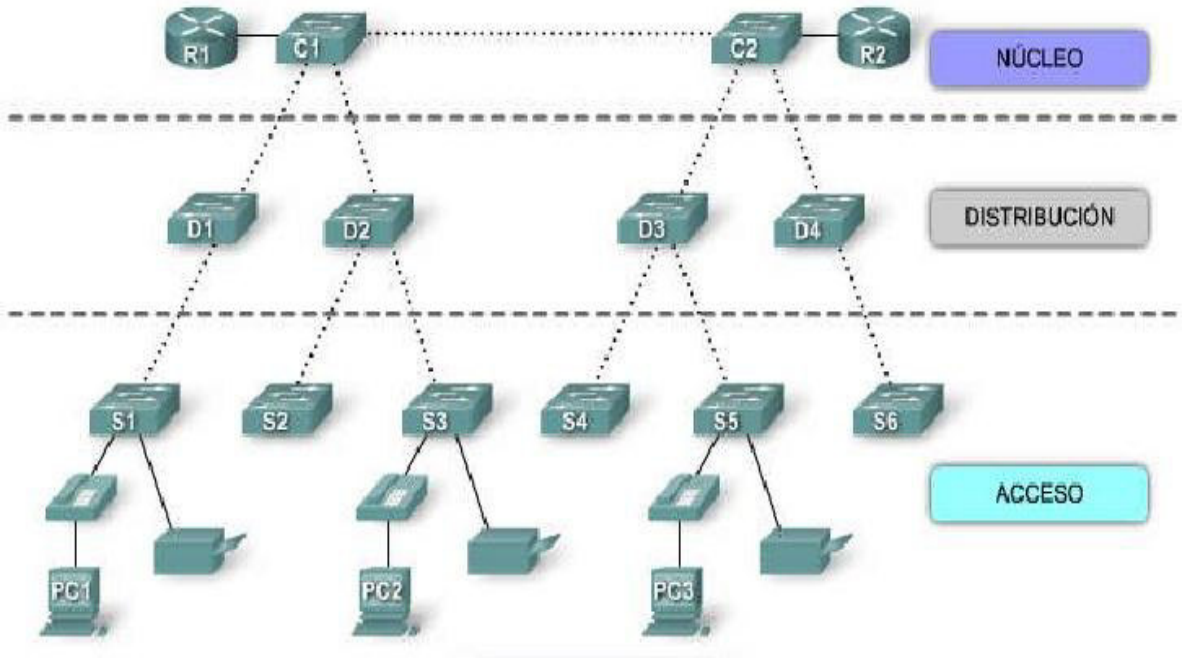


Figura 18. Modelo Jerárquico CISCO

Referencia: http://es.scribd.com/doc/17481738/Cisco-CCNA-3-Exploration-Conmutacion-y-Conexion-Inalambrica-de-Lan-Version-40-Espanol-

1.2.1 Descripción de las capas

1.2.1.1 Capa de Acceso

La capa de acceso hace interfaz con dispositivos finales como las PC, impresoras y teléfonos IP, para proveer acceso al resto de la red. El propósito principal de la capa de acceso es aportar un medio de conexión de los dispositivos a la red y controlar qué dispositivos pueden comunicarse en la red

1.2.1.2 Capa de Distribución

La capa de distribución agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final. La capa de distribución

controla el flujo de tráfico de la red con el uso de políticas y traza los dominios de broadcast al realizar el enrutamiento de las funciones entre las LAN virtuales (VLAN). La función primordial de esta capa es realizar funciones tales como enrutamiento, filtrado y acceso a WAN.

1.2.1.3 **Capa de Núcleo**

La capa del núcleo, principal o Core representa el backbone de alta velocidad que se encarga de desviar el tráfico lo más rápidamente posible hacia los servicios apropiados. Es decir su función es switchear tráfico tan rápido como sea posible y se encarga de llevar grandes cantidades de tráfico de manera confiable y veloz, por lo que la latencia y la velocidad son factores importantes en esta capa**.**

Normalmente, el tráfico transportado se dirige o proviene de servicios comunes a todos los usuarios. Estos servicios se conocen como servicios globales o corporativos (e-mail, el acceso a Internet).

1.3 HERRAMIENTAS DE MONITOREO

1.3.1 Wireshark

Consiste en una herramienta utilizada para identificar y analizar el tipo tráfico de una red, es un analizador de protocolos que permite capturar los paquetes directamente desde una interfaz de red y obtener en detalle la información del protocolo utilizado en el paquete capturado. Los paquetes son filtrados dependiendo de criterios definidos previamente.

También permite importar o exportar los paquetes capturados desde o hacia otros programas.

En la Figura 19 se puede visualizar la ventana de esta herramienta y las zonas de la misma.

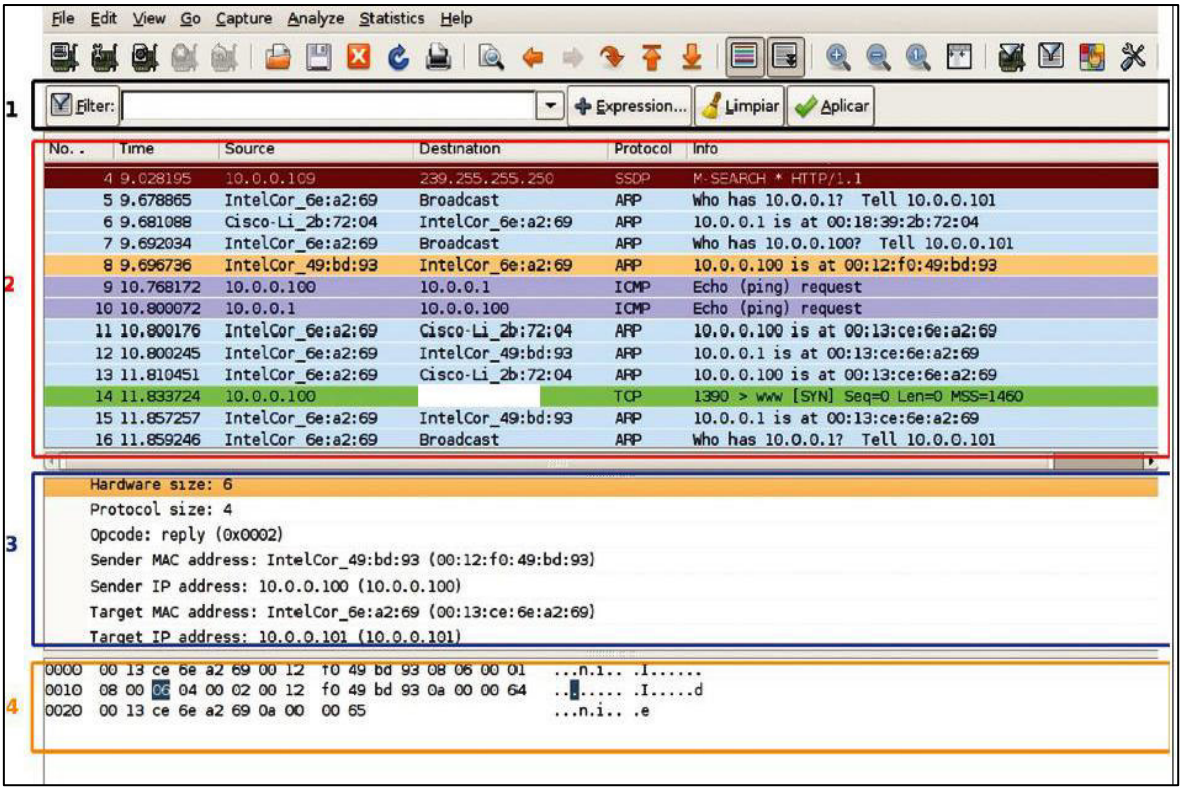


Figura 19. Entorno Wireshark

Referencia: Borja, M, ANÁLISIS DE TRÁFICO CON WIRESHARK (2011) Recuperado de http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

La zona 1 es el área de definición de filtros y, sirve para buscar paquetes o protocolos que determinados

La zona 2 es la de visualización de todos los paquetes que se están capturando en tiempo real.

La zona 3 permite desglosar por capas cada las cabeceras de los paquetes seleccionados en la zona 2.

En la zona 4 se representa, el paquete en formato hexadecimal tal y como fue capturado por la tarjeta de red.

1.3.2 NTOP (Network Top)

Esta herramienta permite monitorizar en tiempo real los usuarios y aplicaciones que están consumiendo recursos de red en un instante. NTOP se puede visualizar de forma remota con cualquier navegador, es decir su interfaz de cliente basada está en HTTP para crear aplicaciones de monitoreo que permiten almacenar persistentemente estadísticas de tráfico, está desarrollado para platarfomas Unix y Windows.

Los protocolos que permite de monitorizar, entre otros son: TCP/UDP/ICMP, (R)ARP, IPX, DLC, Decnet, AppleTalk, Netbios, y ya dentro de TCP/UDP es capaz de agruparlos por FTP, HTTP, DNS, Telnet, SMTP/POP/IMAP, SNMP.

Las Figuras 20 y 21 muestran dos tipos de reporte que se obtienen con Ntop.

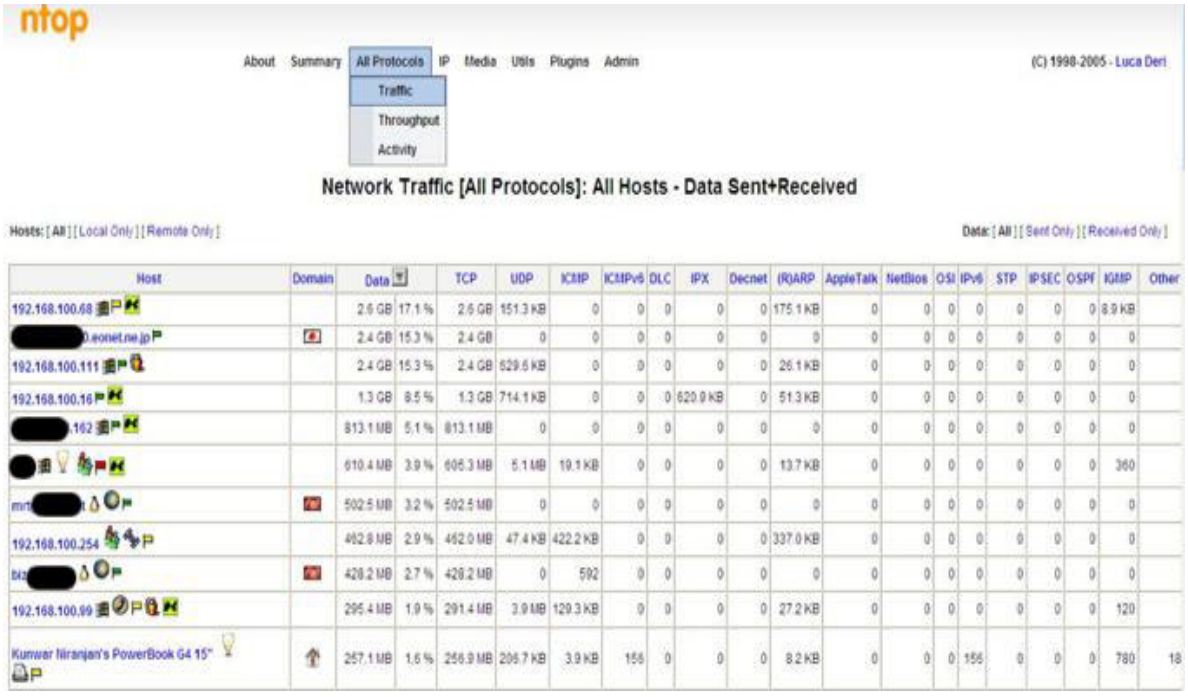


Figura 20. Entorno NTOP 1

Referencia: Method to log amount of transmitted data per each IP address in linux (2014) Recuperado de: http://serverfault.com/questions/626846/method-to-log-amount-of-transmitted-data-per-each-ip-address-in-linux

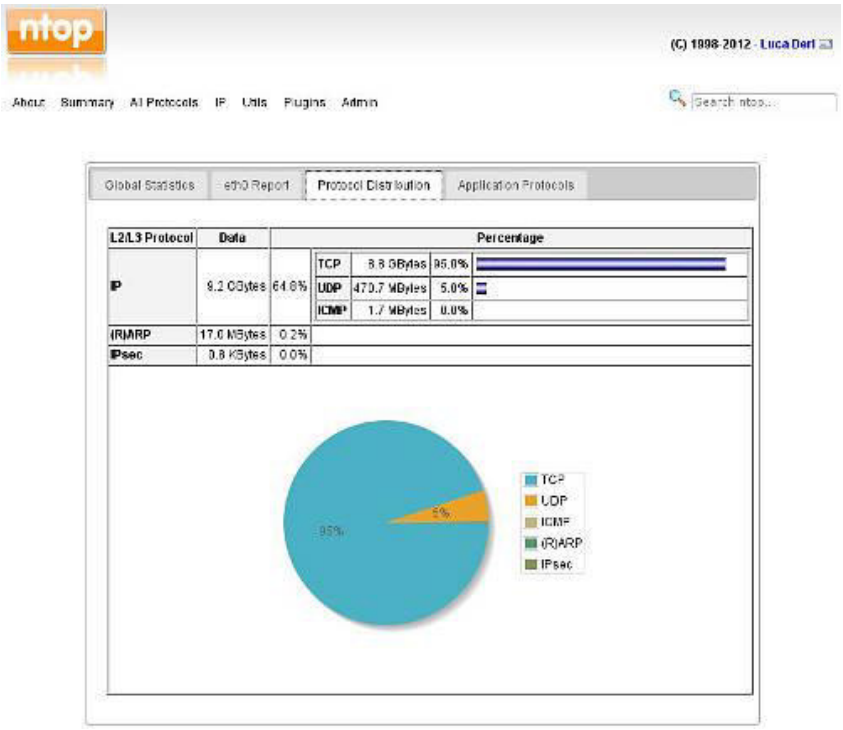


Figura 21. Entorno NTOP 2

Referencia Instalación y primeros pasos con ntop 5 en Debian (2013) Recuperado de http://blog.unlugarenelmundo.es/2013/03/25/instalacion-y-primeros-pasos-con-ntop-5-en-debian-6/

1.3.3 NET TOOLS

Net Tools, una completa herramienta de monitorización de red para Internet y redes de área local, Net Tools es una robusta combinación de varias utilidades entre las que se encuentran: escaneado de red, seguridad, archivo, sistema y herramientas de administración útiles en el diagnóstico y control de las conexiones de red del equipo para administradores, a continuación se detallan de forma particular algunas de sus utilidades:

- Permite obtener el IP local de nuestro equipo. Además de descubrir su IP en Internet utilizando sitios web externos.
- Permite medir el ancho de banda del internet.

- Escaneo de IP's LAN en un rango de IP's indicado, puede transformar a binario (para determinar la máscara de red) y nos indica así la clase de IP.
- Puerto de escucha, permite identificar que puertos están escuchando
- Escaneo de todos los puertos de un equipo en particular o también puedes especificarse un rango de direcciones (Ver Figura 22).
- Ping personalizado a otro equipo.
- Visualización de todas las IP's entrantes y salientes, que están en servicio y el puerto que está utilizando, los puertos locales, las IP's remotas, puertos remotos y su estado.
- Conexión una PC por medio de un puerto.
- Identificar del adaptador de red vinculado a nuestro equipo.
- Esas sin algunas de las funcionalidades, es importante también indicar que los reportes pueden ser guardados, pues se genera un bloc de notas con la información en la mayoría de los casos.

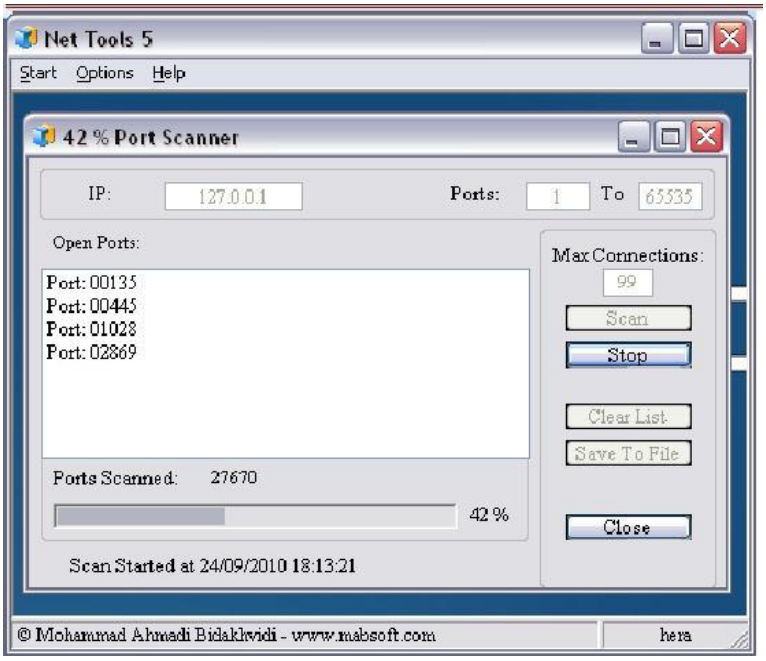


Figura 22. Herramienta Net Tools, escaneo de puertos.

Referencia: DIFERENTES HERRAMINENTAS DE "NET TOOLS 5" EXPLICADAS A FONDO Recuperado de: http://es.scribd.com/doc/38265513/Diferentes-Herraminentas-de-Net-Tools-5#scribd

1.3.4 Nmap

Esta herramienta es útil para realizar la para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes. Mediante paquetes en formas originales permiten determinar los equipos que se encuentran disponibles en una red, qué servicios ofrecen, qué sistemas operativos ejecutan, qué tipo de filtros de paquetes o cortafuegos se están utilizando entre otras características (Ver figura 23). Pese a que generalmente se utiliza Nmap en auditorías de seguridad, también es útil para realizar tareas como: el inventariado de la red, la planificación de actualización de servicios y la monitorización del tiempo que los equipos o servicios se mantiene activos.

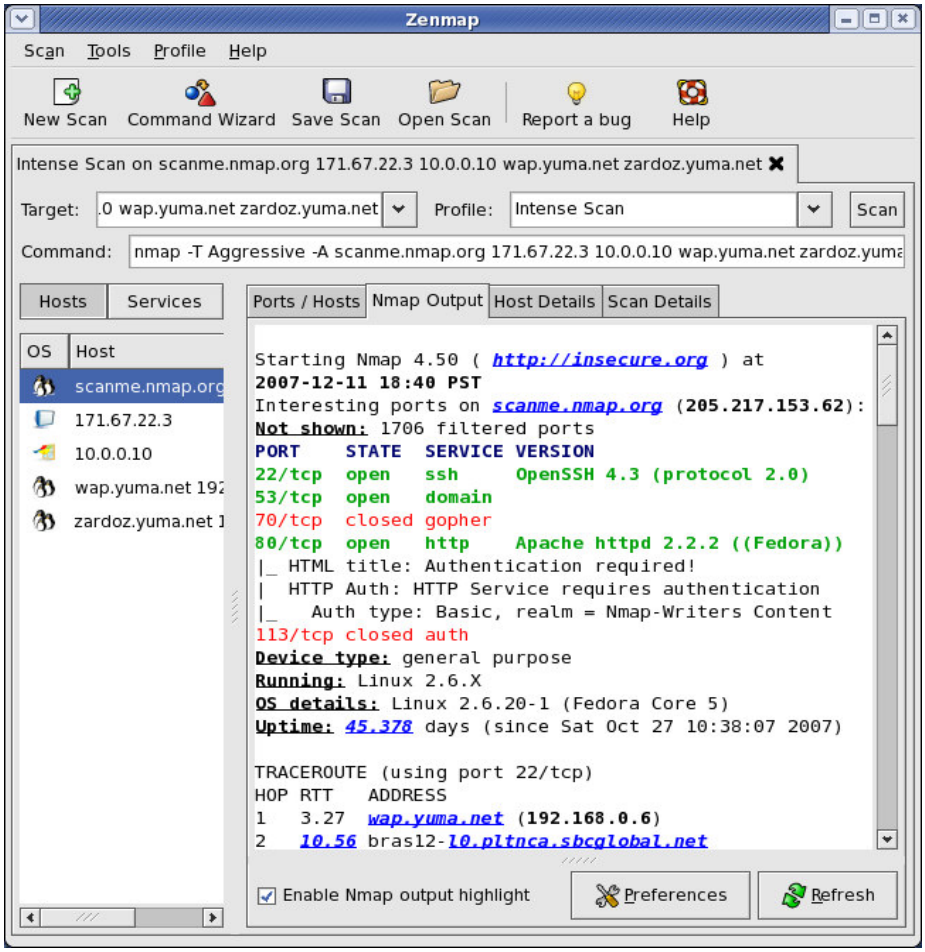


Figura 23. . Entorno NMAP

Referencia: NMAP.ORG (2014) Recuperado de:; https://nmap.org/zenmap/images/zenmap-no-648x700.png

1.4 GNS 3 (Graphic Network Simulator)

Es un software que permite realizar diseños de alta calidad con topologías de red complejas y ejecutar simulaciones en él. Es un programa Open Source (es una fuente abierta) y puede ser usado en múltiples Sistemas Operativos.

Una característica importante es que permite emular las IOS que ejecutan los routers Cisco, agregando todas las características y potencialidades de un router real, sin tener el problema de comandos no reconocidos o no funcionales. Para lograr una simulación precisa *y* completa GNS3 está vinculado con:

Dynamips: un emulador que permite diferentes plataformas de hardware usando IOS de CISCO en un mismo host. Emula las plataformas Cisco 1700, 2600, 2691, 3600, 3725, 3745 y 7200. También permite emular switches Ethernet, Frame-Relay y ATM con Funcionalidades básicas.

Dynagen: Una interfaz que provee la gestión, de las plataformas emuladas por Dynamips haciendo más fácil su uso, simplifica la gestión de las redes virtuales ya que implementa comandos para listar, iniciar, parar, reiniciar, suspender, reanudar los diferentes dispositivos emulados.

VirtualBox: un software de virtualización para que posibilita instalar sistemas operativos adicionales, conocidos como "sistemas invitados", dentro de otro sistema operativo "anfitrión", cada uno con su propio ambiente virtual. Por ejemplo, se podrían instalar diferentes distribuciones de GNU/Linux en VirtualBox instalado en Windows XP o viceversa (Características, recuperado de http://virtualbox.es/caracteristicas/)

CAPITULO 2

2 SITUACIÓN ACTUAL Y ANÁLISIS DE LA RED DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO SAN MIGUEL DE IBARRA

En este capítulo se presenta, la información general del Gobierno Autónomo Descentralizado de San Miguel de Ibarra, así como de la situación actual de la red, los recursos de hardware, las aplicaciones con que cuenta la misma.

Además el proceso de análisis del tráfico y servicios de red, previo al establecimiento de políticas. Esto permitirá garantizar no solo el correcto funcionamiento de las políticas, sino también de las aplicaciones de la red.

2.1 GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA

En el GAD[2]e San Miguel de Ibarra, se realiza varios tipos de trámites: determinación y cobro de impuestos, tasas y contribuciones, trámites relacionados con las propiedades desde su construcción, actualizaciones de datos, etc. Fieles a los principios institucionales, el GAD de San Miguel de Ibarra busca realizar todos sus procesos de manera óptima, y para llevarlos

[2] GAD: Gobierno Autónomo Descentralizado

a cabo se requiere no solo un buen desempeño del personal sino también de las aplicaciones de la red.

El GAD de San Miguel de Ibarra, está constituido por varias dependencias (Ver Figura 24), las cuales tienen sus propias aplicaciones, en el esquema se muestran las dependencias de la institución

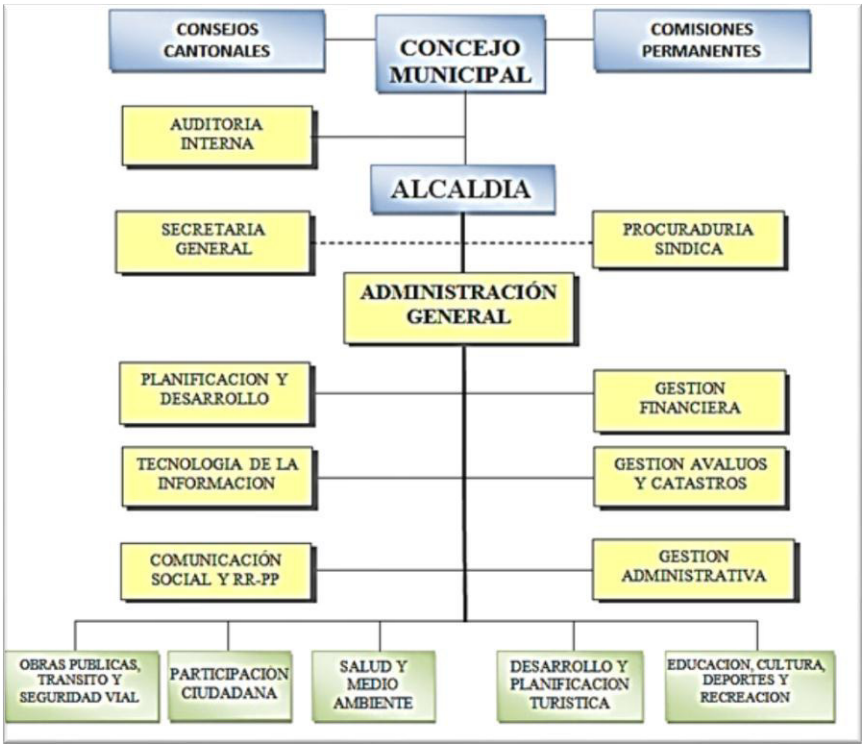


Figura 24. Organigrama Estructural del GAD de San Miguel de Ibarra

Referenci Recuperado de: http://www.ibarra.gob.ec/

2.1.1 Dirección de TIC

La dirección de TIC se divide en dos unidades: unidad de hardware y comunicaciones y unidad de software

Unidad de software se encarga de desarrollo y mantenimiento, de todas las aplicaciones (software).

Unidad de hardware se encarga de todo lo relacionado con la infraestructura de hardware tanto equipos de usuarios finales como dispositivos de red.

2.2 DESCRIPCIÓN DE LA RED

2.2.1 Usuarios

La red local del GAD de San Miguel de Ibarra, tiene 317 usuarios que son parte de las diferentes direcciones, que lo conforman (Ver figura 24), con miras a realizar una ampliación de puntos de red, por lo que se debe tomar en cuenta un total de 400 usuarios aproximadamente.

En la Tabla 7 podemos observar las diferentes dependencias y el número de usuarios de cada una.

Tabla 7. Distribución de usuarios por dependencias

DEPENDENCIA	NRO. DE USUARIOS
OBRAS PUBLICAS	20
DIRECCIÓN ADMINISTRATIVA	10
CONTRATACIÓN PUBLICA	8
SECRETARIA DE COMISIONES	3
PLAN DE ORDENAMIENTO	4
SISMERT	5
TESORERÍA	11
PROCURADURÍA SINDICA	9
COMISARIA DE HIGIENE	3

SECRETARIA GENERAL	4
ARCHIVO HISTÓRICO	2
ALCALDÍA	4
AUDITORIA INTERNA	3
SALUD Y MEDIO AMBIENTE	8
RADIO	6
AVALÚOS Y CATASTROS URBANO	22
AVALÚOS Y CATASTROS RURAL	9
FINANCIERA	13
COMISARIA DE CONSTRUCCIONES	6
PLANIFICACIÓN	26
TRANSITO Y TRANSPORTE	7
BIBLIOTECA	21
CONTROL AMBIENTAL	7
PARTICIPACIÓN CIUDADANA	12
COORDINACIÓN Y SEGURIDAD CIUDADANA	2
TRANSPORTE	5
CNH	5
CULTURA	12
DISPENSARIO MEDICO	5
MUSEO	2

LABORATORIO	20
INFORMACIÓN	3
ARCHIVO TESORERÍA	5
ATENCIÓN AL CLIENTE	15
TIC	20
TOTAL	**317**

Fuente: Gobierno Autónomo Descentralizado San Miguel de Ibarra de San Miguel de Ibarra, Dirección Talento Humano

2.2.2 Servidores y Aplicaciones

2.2.2.1 **Servidores**

Por la naturaleza de la institución, se tienen diversos tipos de aplicaciones y por lo tanto varios servidores (Ver tabla 8), por razones de seguridad no se detallará las IP reales de los diferentes servidores:

Tabla 8. Descripción Servidores GAD Municipal San Miguel de Ibarra

IP	SERVIDOR	TIPO
172.X.X.60	SERVIDOR HP BL 460 G6	Físico
172.X.X.203	SERVIDOR DOCUMENTAL	Virtual
172.X.X.116	SERVIDOR CONTROL DE PERSONAL	Virtual
172.X.X.65	SERVIDOR HP BL 460 G6	Físico
172.X.X.67	SERVIDOR CORREO	Virtual
172.X.X.66	SERVIDOR ESPEJO BASE DE DATOS	Virtual
172.X.X.94	SERVIDOR SERVICIOS DE RED DNS Y DHCP	Virtual

172.X.X.102	SERVIDOR HP 160 G5 (Srv3)	Físico
172..X.103	Sistema documental Quipux	Virtual
172..X.101	Servidor de BALANCE SCORD CARD	Virtual
172..X.109	SERVIDOR DE BASE DE DATOS POSTGRES Pruebas (deb101)	Virtual
172.X.X.69	SERVIDOR HP BL 460 G8	Físico
172.X.X.110	SERVIDOR APLICACIONES WEB	Virtual
172.X.X.119	SERVIDOR VIRTUAL MAPAS (MAPSERVER)	Virtual
172.X.X.104	SERVIDOR BDD POSTGIS	Virtual
172.X.X.91	SERVIDOR DE BDD POSTGREST	Físico
172.X.X.92	SEVIDOR DE APLCACIONES TERCEROS OLYMPO)	Físico
172.X.X.99	SERVIDOR DE ANTIVIRUS	Físico
172.X.X.121	SERVIDOR DE VOZ IP	Físico

Fuente: Gobierno Autónomo Descentralizado San Miguel de Ibarra de San Miguel de Ibarra, Dirección TIC

2.2.2.2 **Aplicaciones**

Los servidores descritos albergan varias aplicaciones que serán descritas a continuación:

2.2.2.2.1 Sistemas Avalúos y Catastros

Administración de los predios urbanos y rurales para valoración y determinación del impuesto.

2.2.2.2.2 Sistema de multas de construcciones

Se utiliza para registrar las infracciones que genera la Comisaría de Construcciones, respecto al incumplimiento por parte de los propietarios de predios.

2.2.2.2.3 Sistema de tasas de Control Urbano

Emite tasas de control urbano en la Unidad de Administración Urbana, generando los títulos correspondientes a: Aprobación de planos, de urbanizaciones y lotizaciones, garantías de construcciones, Fraccionamientos, Directrices Viales, Cerramientos, Trabajos varios, Uso de suelo, etc.

2.2.2.2.4 Sistema de Inquilinato

Basado en Se basa en los datos del predio y en los registrados por el propietario permite control y recaudación de la tasa de inquilinato de los predios que se destinan en arrendamiento.

2.2.2.2.5 Sistema SISMERT (Sistema de Estacionamiento Rotativo Tarifado)

Control parqueo tarifado, el Sistema registra: Multas generadas por los inspectores, Emisión de certificados de no adeudar, proporciona reportes de la información registrada.

2.2.2.2.6 Sistema de Gestión de Trasporte Público

Inventario de cooperativas de transporte: taxis camionetas buses y procesos ligados a legalización de estas.

2.2.2.2.7 Sistema de Recaudación y Tesorería

Permite el registro y recaudación de los impuestos, tasas y contribuciones municipales, correspondiente a los ingresos tributarios y no tributarios, valores exigibles y garantías, que generados en todos los departamentos.

2.2.2.2.8 Sistema de Actividades Económicas

Registro de actividades económicas negocios, etc para generar tasas de pagos: determina impuestos a la Patente y a los Activos Totales de personas naturales, jurídicas, sociedades.

2.2.2.2.9 Sistema de Talento Humano

Sistema en el cual se registra toda la información de los funcionarios: Datos personales, formación académica, cargos ejercidos dentro de la entidad, etc.

2.2.2.2.10 Sistema de SIG IMI (web)

El Sistema de Información Geográfica del Ilustre Municipio de Ibarra (SIG-IMI), es la integración de información geográfica, bases de datos, servicios y software; el cual permite manipular, analizar y desplegar en todas sus formas la información geográficamente referenciada, se ha implementado el IRC y el Visor GIS del cantón con sus capas respectivas como: predial, vías, parroquias, zonificación, manzaneros, etc.

2.2.2.2.11 Sistema de Participación Ciudadana

Registro de procesos ciudadanos: Organización Social y Territorial, Planificación Participativa, Presupuesto Participativo y Mecanismos de Participación Ciudadana y Control Social.

2.2.2.2.12 Sistema de Vallas Publicitarias

Cobro, registro de vallas y características de estas para cobro

2.2.2.2.13 Sistema de Ventanilla Única de Turismo

Complemento de actividades económicas para generación de tasas para actividades turísticas además realiza la re-categorización de las mismas.

2.2.2.2.14 Sistema de Transferencias de Dominio

Para compras de predios: Realiza la liquidación de un traspaso de dominio de bienes inmuebles de los predios generando los Impuestos de Alcabala y Utilidad Urbana.

2.2.2.2.15 Sistema de Alarmas Comunitarias

Control y activación de alarmas comunitarias ubicadas en los barrios del cantón Ibarra.

2.2.2.2.16 Sistema Olympo

Sistema Financiero Contable, en el cual se registran todo tipo de transacciones y pagos.

2.2.2.2.17 Sistema de Control Vehicular

Control de movilización de vehículos institucionales.

2.2.2.2.18 Sistema Control de Turnos (GOIA Turnos)

Sistema de Atención al Cliente que otorga Turnos a los servicios disponibles en la organización en las Ventanillas de Rentas

2.2.2.2.19 Réplica de base de datos ORACLE del servicio de rentas internas (SRI)

A través del Convenio de Cooperación Interinstitucional, para compartir la siguiente información:

Municipio de Ibarra: Catastros de bienes inmuebles urbanos y rurales, Impuesto de Patente Municipal, Espectáculos Públicos.

Servicio de Rentas Internas: Base de Datos del Registro Único de Contribuyentes, Impuesto a los vehículos, Información del Impuesto a la Renta e Impuesto al Valor Agregado.

2.2.2.2.20 Web Services de recaudación en línea para entidades financieras

Permite el enlace en línea con la empresa SwitchORM S.A. para el pago de impuestos municipales a través de convenios con las entidades financieras.

2.2.2.2.21 Sistema de Inquilinato

Basado en Se basa en los datos del predio y en los registrados por el propietario permite control y recaudación de la tasa de inquilinato de los predios que se destinan en arrendamiento.

2.2.2.2.22 Sistema de Archivo Documental

Almacenamiento y consulta de documentos generados en el Municipio de Ibarra, tales como Ordenanzas, Contratos, Convenios, Reglamentos, Proyectos, Actas y Resoluciones.

La Figura 25, muestra el Sistema Integrado que contiene las aplicaciones de valor agregado del GAD Municipal de San Miguel de Ibarra

Figura 25. Vista Sistema Integrado GAD Ibarra

Fuente: Gobierno Autónomo Descentralizado San Miguel de Ibarra de San Miguel de Ibarra, Dirección TIC

2.2.3 Topología

2.2.3.1 Topología Física

Al ser una red heterogénea, la red local del gobierno autónomo descentralizado de San Miguel de Ibarra está dispuesta, en forma general de la siguiente manera:

Tabla 9. Descripción general de la red GAD Ibarra

ENLACE	DESCRIPCIÓN
Edificio Principal-Edificio antiguo	Enlace con fibra
Edificio Principal- Antiguo Cuartel	Enlace con fibra
Edificio Principal-Dep. Cultura (Casa de la Ibarreñidad)	Enlace con fibra
Edificio Principal-Dep. Turismo(Esquina del Coco)	Enlace Inalámbrico
Edificio Principal- Bodegas	Enlace Inalámbrico
Edificio Principal- Mercado Amazonas	Enlace Inalámbrico

Fuente: Gobierno Autónomo Descentralizado San Miguel de Ibarra de San Miguel de Ibarra, Dirección TIC

El GAD de Ibarra cuenta con un data center, ubicado en edificio principal, el cual alberga a todos los equipos de red y desde donde parten las conexiones a las diferentes dependencias de la institución, según lo descrito en la Tabla 9.

En la Figura 26 se presenta un diagrama unifilar de la disposición general de la red, en donde se puede evidenciar la topología descrita:

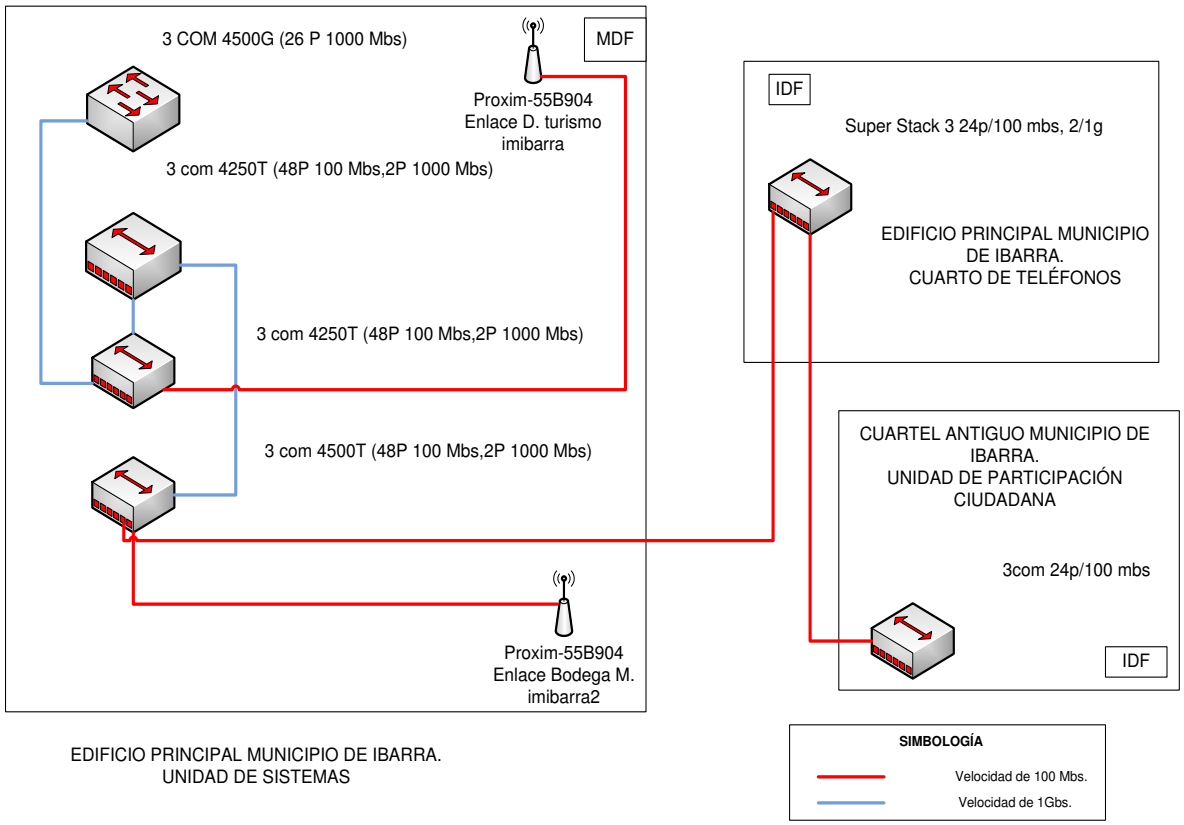


Figura 26. Diagrama unifilar de la red GAD Ibarra

Fuente: Gobierno Autónomo Descentralizado San Miguel de Ibarra de San Miguel de Ibarra, Dirección TIC

2.2.3.2 **Topología Lógica**

Dentro de la topología lógica se detallan las configuraciones principales los equipos que rige el funcionamiento de la red del GAD Ibarra.

2.2.3.2.1 VLAN

Dentro de la red del GAD Municipal de san Miguel de Ibarra se han configurado diferentes VLAN que permitan la mejor una administración y funcionamiento de la red. Son 4 VLAN, que tomando en cuenta los servicios de la red (por ejemplo se ha configurado una

VLAN exclusiva para VoIP), así como también la ubicación y configuración de dispositivos físicos de la red. En la siguiente tabla se describe las VLAN dentro de la red del GAD Municipal San Miguel de Ibarra.

Tabla 10. Distribución de VLANs

DISTRIBUCIÓN	NRO. DE VLAN	DESCRIPCIÓN	ENLACES	INTERFACES
EDIFICIO PRINCIPAL				
SW-4500-CORE	VLAN 1	172.x.x.x		
	VLAN 2	172.x.x.x		
	VLAN 3	172.x.x.x /VoIP		
	VLAN 7	172.x.x.x		
			Enlace troncal	Gigabit Ethernet 1/1-3-11-12-15-17-18-19-20 Gigabit Ethernet 2/47
			Servidor VoIP	Gigabit Ethernet 2/48
SW-2960-RACK2-01	VLAN 1	DHCP		
	VLAN 2	172.x.x.x		
	VLAN 7	Tecnología		Fast Ethernet 0/13-24
SW-2960POE-RACK2-01	VLAN 2	172.x.x.x		
	VLAN 3	VoIP		Fast Ethernet 0/1-48
	VLAN 7	Tecnología		Fast Ethernet 0/1-2
			Enlace troncal	Gigabit Ethernet 0/3
EDIFICIO ANTIGUO				
SW-2960POE-RACKS1-03	VLAN 3	VoIP		Fast Ethernet0/1-24
	VLAN 2	172.x.x.x		
			Enlace troncal	Gigabit Ethernet0/1
swea2960p101	VLAN 1	172.x.x.x		
CASA DE LA IBARREÑIDAD				

	VLAN 3	VoIP		Fast Ethernet 0/1-24
SW-2960POE-	VLAN 2	172.x.x.x		
CULT-S1			Enlace troncal	Gigabit Ethernet 0/1

Fuente: Gobierno Autónomo Descentralizado San Miguel de Ibarra de San Miguel de Ibarra, Dirección TIC

2.2.4 Equipos

Algunos de los equipos que forman parte de la red local del GAD de San Miguel de Ibarra a continuación en la Tabla 11.

Tabla 11. Dispositivos de red, GAD Ibarra

DESCRIPCIÓN	CANTIDAD
Switch 3 com 4250 T	2
Switch 3 com Office Conect 24 p	1
Switch 3 com Super Satck 3	1
Switch 3 com 5500 SI	1
Switch 3 com 4500G	1
Switch 3 com 4500	1
Cisco Switch core CORE 4503 E	1
Cisco WS-C2960-24PC-L	8
Firewall CheckPoint 4610	1

Fuente: Gobierno Autónomo Descentralizado San Miguel de Ibarra de San Miguel de Ibarra, Dirección TIC

En el Anexo 1, se encuentra la descripción de cada equipo, y en el caso del presente trabajo es importante conocer mejor las características del Switch de Core, el mismo se lo puede encontrar en el Anexo 9.

2.3 JERARQUIZACIÓN DE LA RED EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN MIGUEL DE IBARRA

Para determinar una estructura correcta de la red es necesario jerarquizarla, de acuerdo al modelo jerárquico propuesto por cisco.

La descripción de los elementos y de las capas a las que pertenecen los mismos se presente en la Tabla 12:

Tabla 12. Jerarquización de la red GAD Ibarra

CAPA	DISPOSITIVOS	DESCRIPCION
ACCESO	Switch 3Com Office Conect 24 p Switch 3Com Super Satck 3 Switch 3 com 5500 SI Switch 3 com 4500G Switch 3 com 4500 Cisco WS-C2960-24PC-L Switch 3 com 4250 T	Son los dispositivos por medio de los cuales los 317 usuarios tienen acceso a la red y sus servicios, entre los cuales se encuentran switches y Acces Points de las diferentes dependencias q están fuera del edificio central del GAD Municipal de Ibarra
NÚCLEO Y DISTRIBUCIÓN	Cisco Switch CORE 4503 E Firewall CheckPoint 4610 Servidores	De acuerdo al análisis del estudio realizado se determina que es una red de Núcleo Colapsado[3].

Fuente: Gobierno Autónomo Descentralizado San Miguel de Ibarra de San Miguel de Ibarra, Dirección TIC

[3] NÚCLEO COLAPSADO*:* Una red con un modelo Núcleo Colapsado es aquella en la que se combinan la capa de distribución y la capa núcleo en una sola capa.

En la Figura 27 se presenta un diagrama de la topología actual jerarquizada de la red del Gobierno Autónomo Descentralizado de San Miguel De Ibarra.

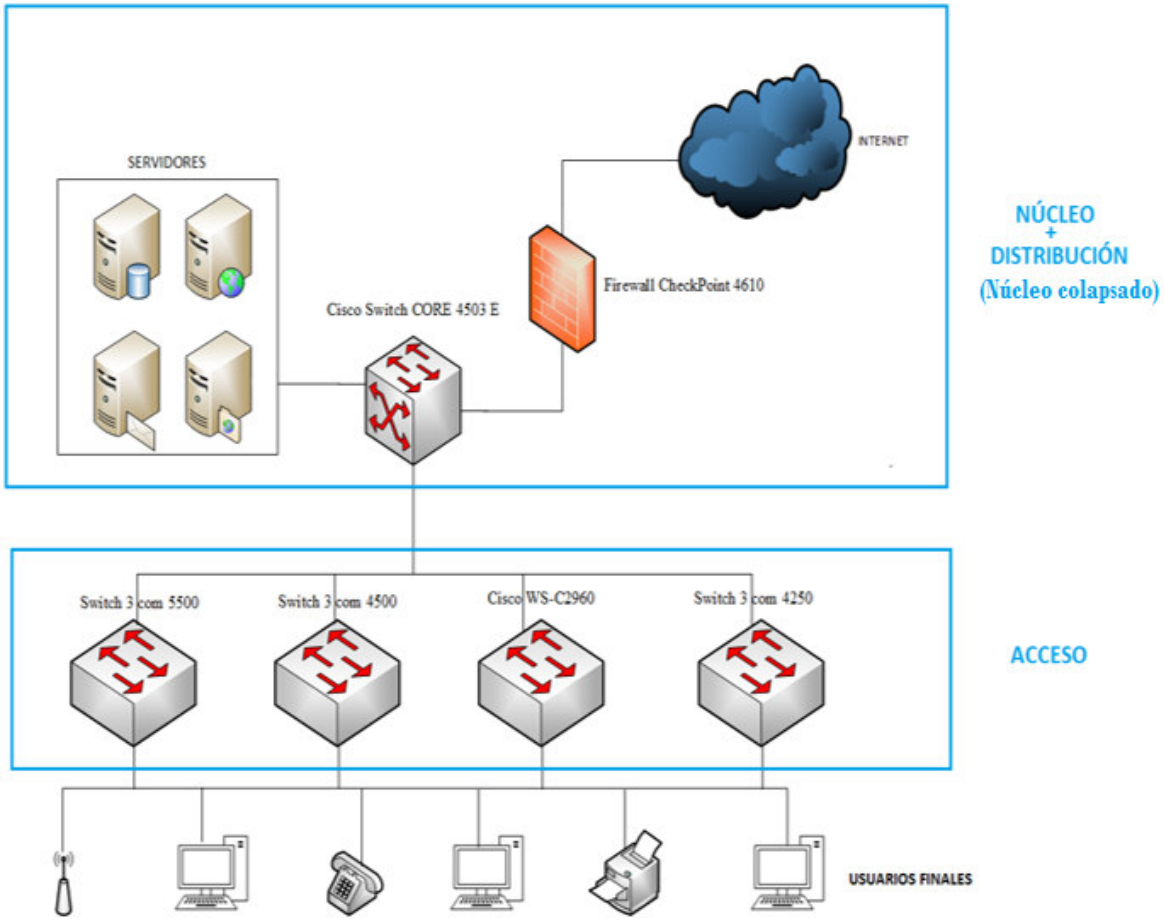


Figura 27. Diagrama de red jerarquizada

Fuente: Gobierno Autónomo Descentralizado San Miguel de Ibarra de San Miguel de Ibarra, Dirección TI

2.4 AUDITORIA DE LA RED

La ejecución del proceso de auditoría de la red está estrechamente ligada al estudio de su situación actual, pues en dicho estudio puede llegarse a determinar varios parámetros relevantes para el diseño de las políticas de calidad de servicio en una red determinada. Pero no solo basta con el análisis de la información recopilada, se hace necesario utilizar software especializado que permita analizar la red. En el capítulo anterior se describió varias herramientas para realizar este proceso.

A continuación se describirá los diferentes elementos y parámetros analizados con las herramientas seleccionadas.

2.4.1 ANÁLISIS GENERAL DE LA RED CON NTOP

Para realizar en análisis general de la red se utilizó la herramienta NTOP descrita en el capítulo anterior, con el cual se analizó varios parámetros durante un lapso determinado. En el Anexo 2 se encuentran los resultados obtenidos con NTOP, a continuación se muestran ejemplos de los parámetros analizados:

En primer lugar necesitamos un puerto al cual conectar el servidor para realizar el monitoreo respectivo, para lo cual se utilizó la funcionalidad de *Puerto espejo.*

2.4.1.1 **Puerto espejo**

Permite capturar el tráfico duplicado de un interfaz determinada, para poder analizarlo con cualquier herramienta de monitoreo.

Para configurarlo se debe activar la funcionalidad *port monitor* en las interfaces deseadas como se muestra en el ejemplo siguiente:

Para configurar el puerto Fa0/1 como puerto de destino, los puertos de origen Fa0/2 y Fa0/5, se debe seleccionar la la interfaz Fa0/1 en el modo de configuración:

```
Switch(config)#interface fastethernet 0/1
```

Introduzca la lista de puertos que deben supervisarse:

```
Switch(config-if)#port monitor fastethernet 0/2
```

```
Switch(config-if)#port monitor fastethernet 0/5
```

En el caso del presente trabajo se configuro en las interfaces que se muestran a continuación:

```
monitor session 1 source interface Fa1/0 - 1 , Fa1/5

monitor session 1 destination interface Fa1/10
```

2.4.1.2 **Monitoreo de los Hosts conectados**

En la Figura 28 se muestran las características de todos los hosts conectados a la red, incluyendo los servidores.

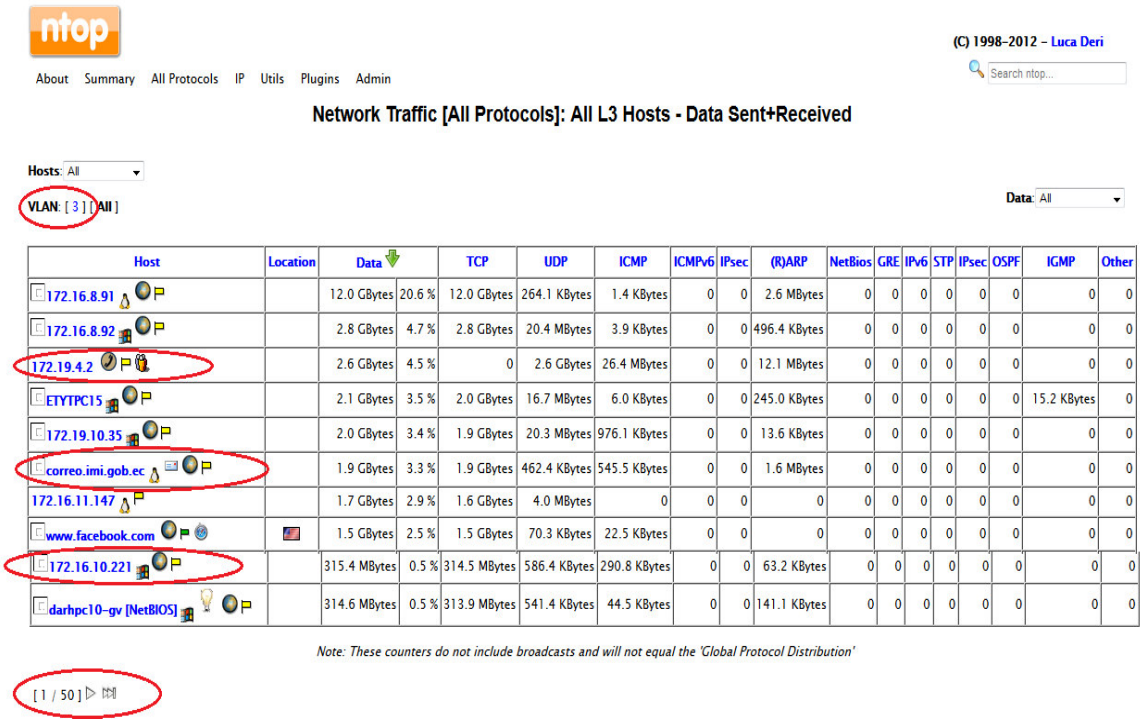


Figura 28. Captura de NTOP con los host de la red de GAD Ibarra

Fuente: Herramienta NTOP en la red del Gobierno Autónomo Descentralizado San Miguel de Ibarra

ANÁLISIS: En la figura 28 en los lugares señalados, se puede verificar que se muestran, en pestañas de la 1 a la 50, todos los dispositivos conectador en la red; la primera IP señalada, 172.19.4.2, corresponde a un teléfono IP, como muestra el icono. La segunda selección corresponde al servidor de correo, de acuerdo a los iconos. La tercera selección corresponde a la IP de un host en la red, se muestra el icono de su sistema operativo. Además la figura indica la cantidad y tipos de datos recibidos y enviados por cada host.

2.4.1.3 **Monitoreo de aplicaciones y protocolos**

Para empezar, la figura 29, muestra el porcentaje del tipo de tráfico generado dentro de la red, determina que prácticamente todo el tráfico (97%) es IPV4, que es el protocolo usado por la red:

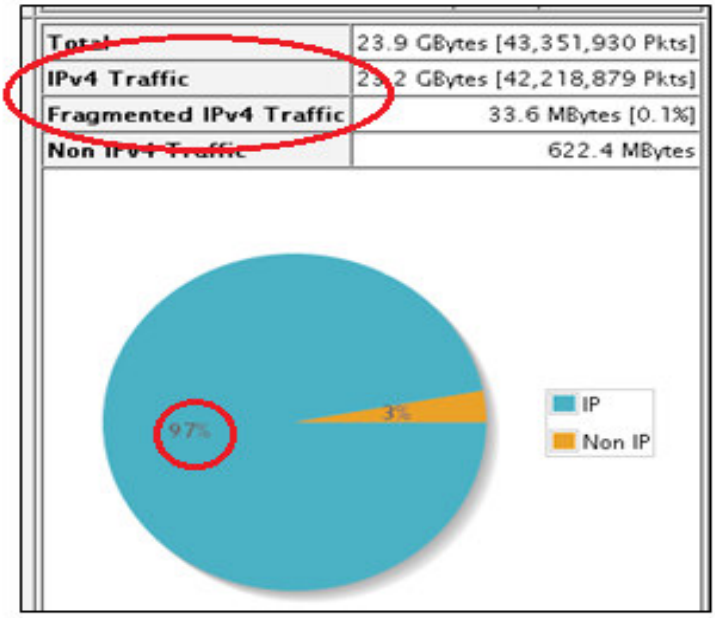


Figura 29. Tráfico IP en la red de GAD Ibarra

Fuente: Herramienta NTOP en la red del Gobierno Autónomo Descentralizado San Miguel de Ibarra

Como se detalló anteriormente, existen varias aplicaciones que se alojan en los diferentes servidores, la Figura 30 muestran los principales protocolos de las aplicaciones así podemos observar que el 76% pertenece a tráfico con protocolo TCP , el cual corresponde a aplicaciones como correo y base de datos, que es la mayoría de trafico cursado por la red y el 22% UDP, que corresponde a aplicaciones como VoIP. El resto del trafico representa una pequeña cantidad como por ejemplo el trafico ICMP, usado para pruebas de conectividad.

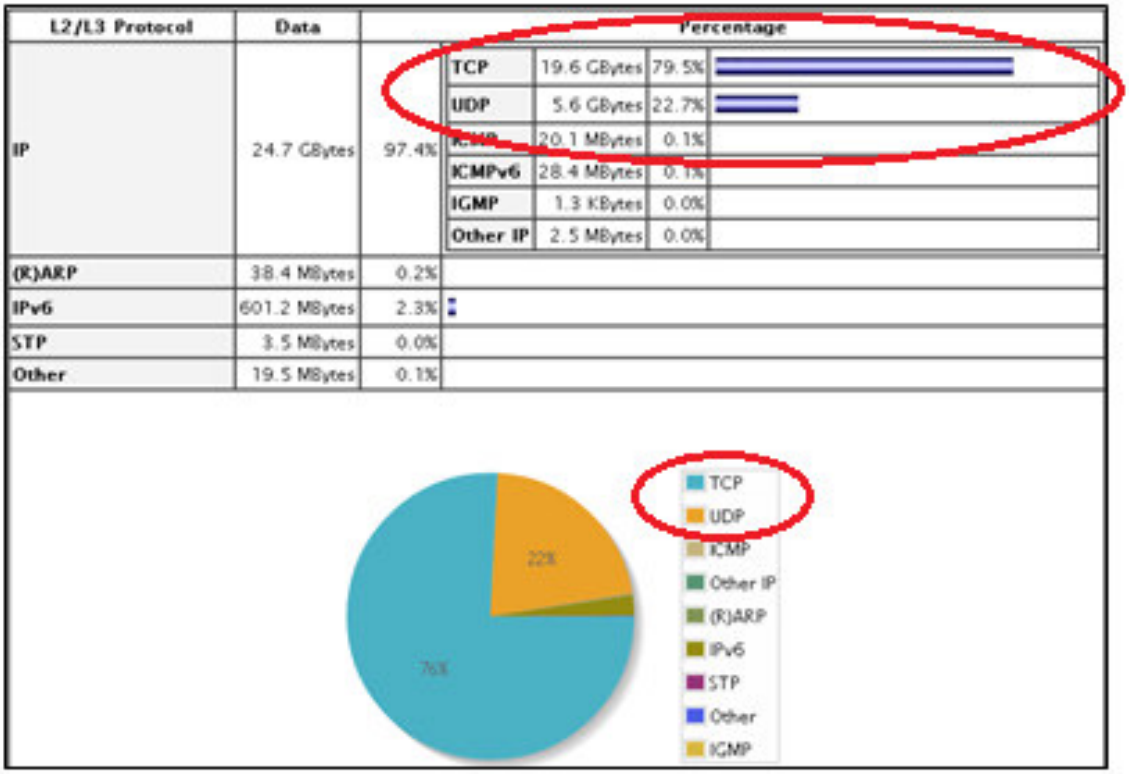


Figura 30. Principales Protocolos red GAD Ibarra

Fuente: Herramienta NTOP en la red Gobierno Autónomo Descentralizado San Miguel de Ibarra

En la Figura 31, se pueden observar los porcentajes de los diferentes protocolos de acuerdo a las aplicaciones que existen en la red, por ejemplo se han señalado para el ejemplo los protocolos como el FTP (43%) y HTTP (17%), utilizados en los servicios de correo, quipux y base de datos; también se ha señalado el servicio de PostgresSQL (5%), importante

también para el funcionamiento de las bases de datos. Los porcentajes se refieren en general a los tipos de protocolos y servicios cursados en la red.

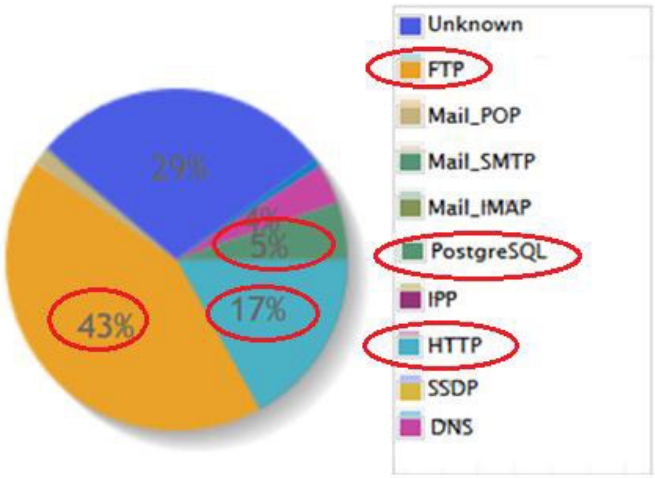


Figura 31. Protocolos según las aplicaciones red GAD Ibarra

Fuente: Herramienta NTOP en la red Gobierno Autónomo Descentralizado San Miguel de Ibarra

La herramienta también despliega el estado de cada protocolo con su respectivo consumo de ancho de banda. Las figuras 32,33, 34 y 35 muestran los consumos y el correspondiente porcentaje de ancho de banda que representan en el consumo de ancho de banda acumulado de la red durante el tiempo de medición así como los promedios por horas, por ejemplo en la figura 32 el máximo es 1.1MB, el promedio 123.3KB, el acumulado 15.8 GB, que representa el 17.3% de todo el consumo durante el tiempo de medición.

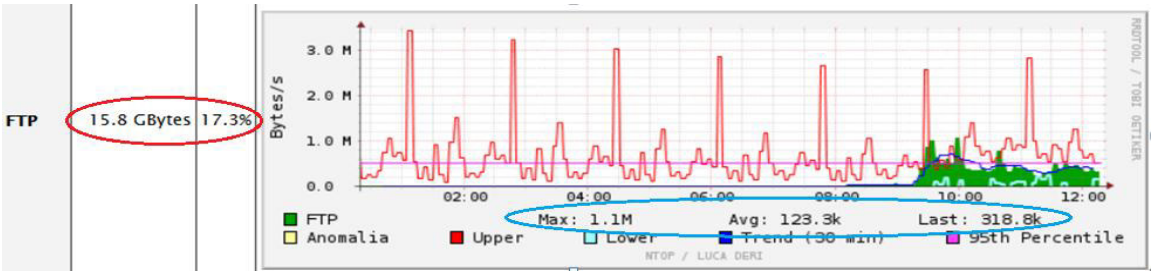


Figura 32. Protocolos/Aplicaciones y sus consumos 1

Fuente: Herramienta NTOP en la red Gobierno Autónomo Descentralizado San Miguel de Ibarra

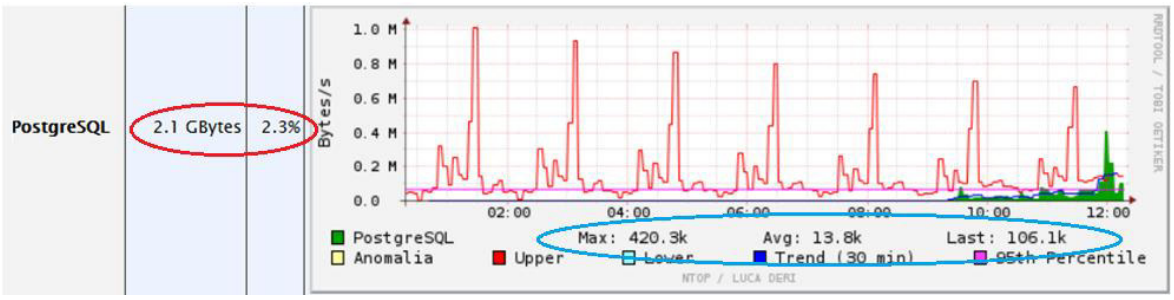


Figura 33. Protocolos/Aplicaciones y sus consumos 2

Fuente: Herramienta NTOP en la red Gobierno Autónomo Descentralizado San Miguel de Ibarra

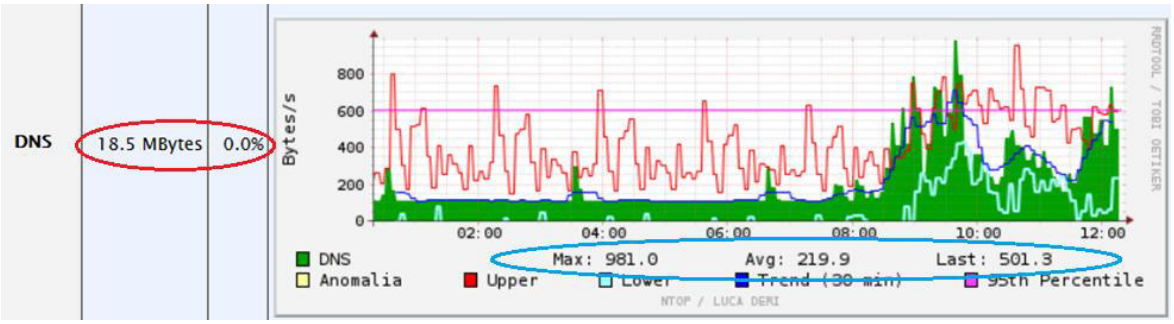


Figura 34. Protocolos/Aplicaciones y sus consumos 3

Fuente: Herramienta NTOP en la red Gobierno Autónomo Descentralizado San Miguel de Ibarra

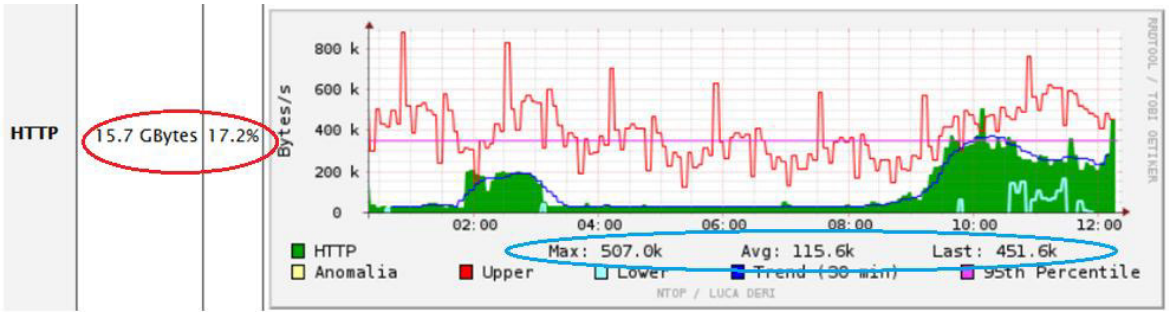


Figura 35. Protocolos/Aplicaciones y sus consumos 4

Fuente: Herramienta NTOP en la red Gobierno Autónomo Descentralizado San Miguel de Ibarra

2.4.1.4 **Monitoreo de Throughput**

Se realiza para determinar qué cantidad de tráfico está cursando por la red:

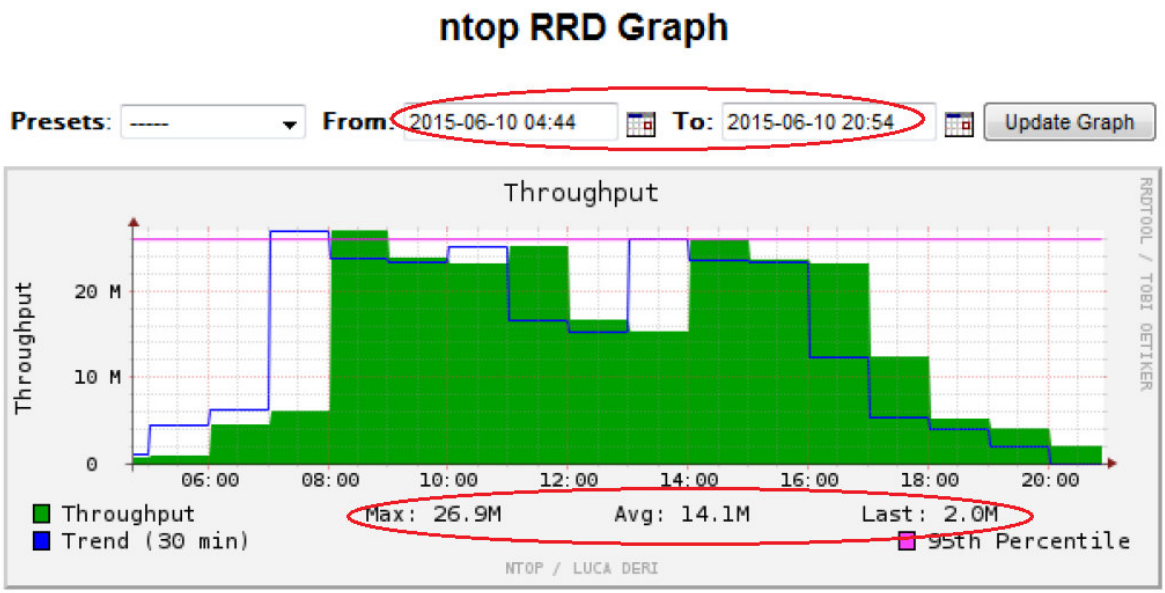


Figura 36. Throughput GAD Ibarra

uente: **Herramienta NTOP en la red Gobierno Autónomo Descentralizado San Miguel de Ibarra**

ANÁLISIS: En la figura 36 se muestra el tráfico capturado del durante un día se puede determinar qué: el tráfico mantiene niveles relativamente constantes. Claramente se observa como aumenta en las horas efectivas de trabajo a partir de las 08:00 a las 17:00. En el intervalo de tiempo del almuerzo baja notablemente, así como en la última media hora de trabajo aproximadamente desde las 17:00 a las 17:30. Esto permite verificar el comportamiento en general del tráfico dentro de la red.

2.4.1.5 **Reportes Checkpoint**

El Firewall CheckPoint 4610 genera también reportes en los que se pueden evidenciar los consumos en la red. El Anexo 3 contiene el reporte completo de un mes generado por el Firewall CheckPoint 4610.

En la figura 37 se observan los sitios web que más se visitan y sus consumos de ancho de banda, esa información puede utilizarse para denegar accesos y permitir un mejor usos de os recursos, se muestra claramente que la aplicación con más alto consumo es YouTube, y es muy utilizada por los funcionarios.

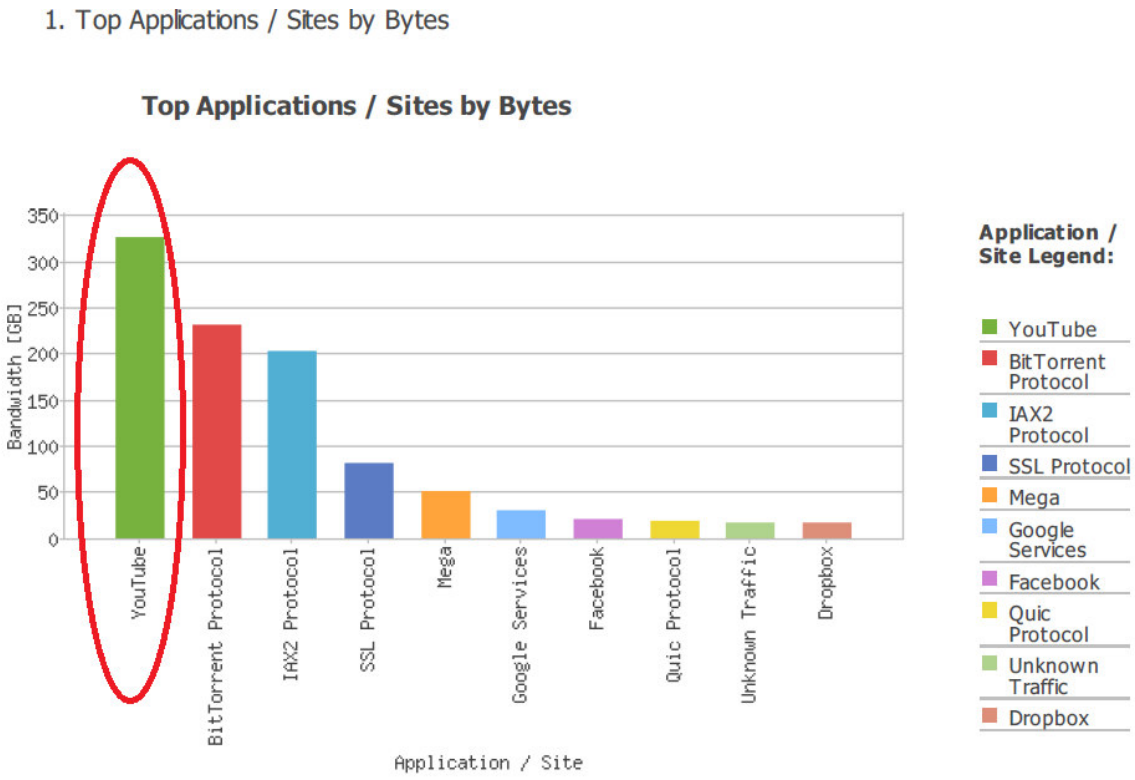


Figura 37. Reporte CheckPoint/Aplicaciones protocolos

Fuente: Reporte CheckPoint 4610 de en la red Gobierno Autónomo Descentralizado San Miguel de Ibarra

La figura 38, muestra en cambio los tipos de tráfico que circulan en la red, se puede apreciar que la mayor parte pertenece a Protocolos de red, representando el 82.8%, de este porcentaje forman parte protocolos como FTP, SMTP, DNS, etc, que hacen posible que los servicios de la red funciones correctamente.

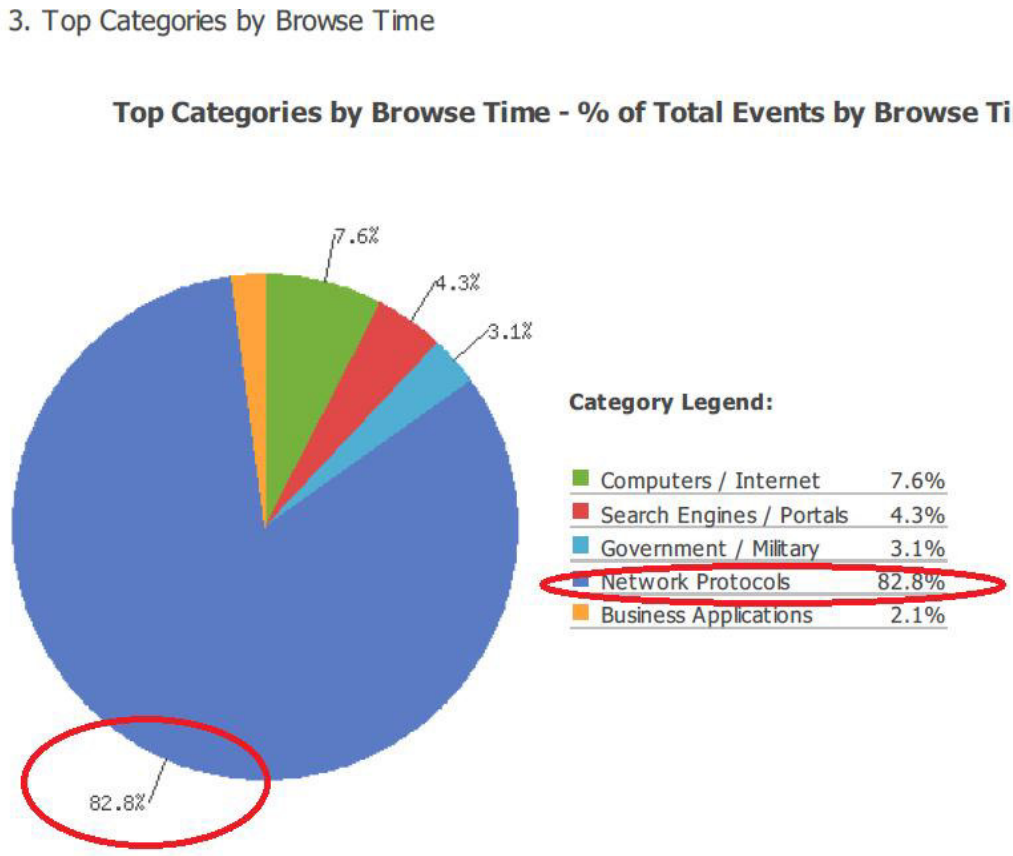


Figura 38. Reporte CheckPoint/ Protocolos

Fuente: Reporte CheckPoint 4610 de en la red Gobierno Autónomo Descentralizado San Miguel de Ibarra

2.4.1.6 **Escaneo de Puertos**

El escaneo de puertos constituye uno de los pasos más importantes dentro del proceso de auditoría, debido a que los puertos son las interfaces que permiten la comunicación dentro de la red y el correcto funcionamiento de las diversas aplicaciones.

Para realizar el escaneo de puertos se utilizó dos herramientas, para obtener una información más veraz acerca de los puertos activos en la red. A continuación se muestran los reportes de las herramientas usadas para determinar los puertos en la red, que posteriormente serán utilizados en el diseño de políticas de calidad de servicio.

2.4.1.6.1 Con Nmap

La figura 39, muestra un reporte del escaneo de puertos al servidor 172.16.8.103, obtenido utilizando la herramienta NMAp.

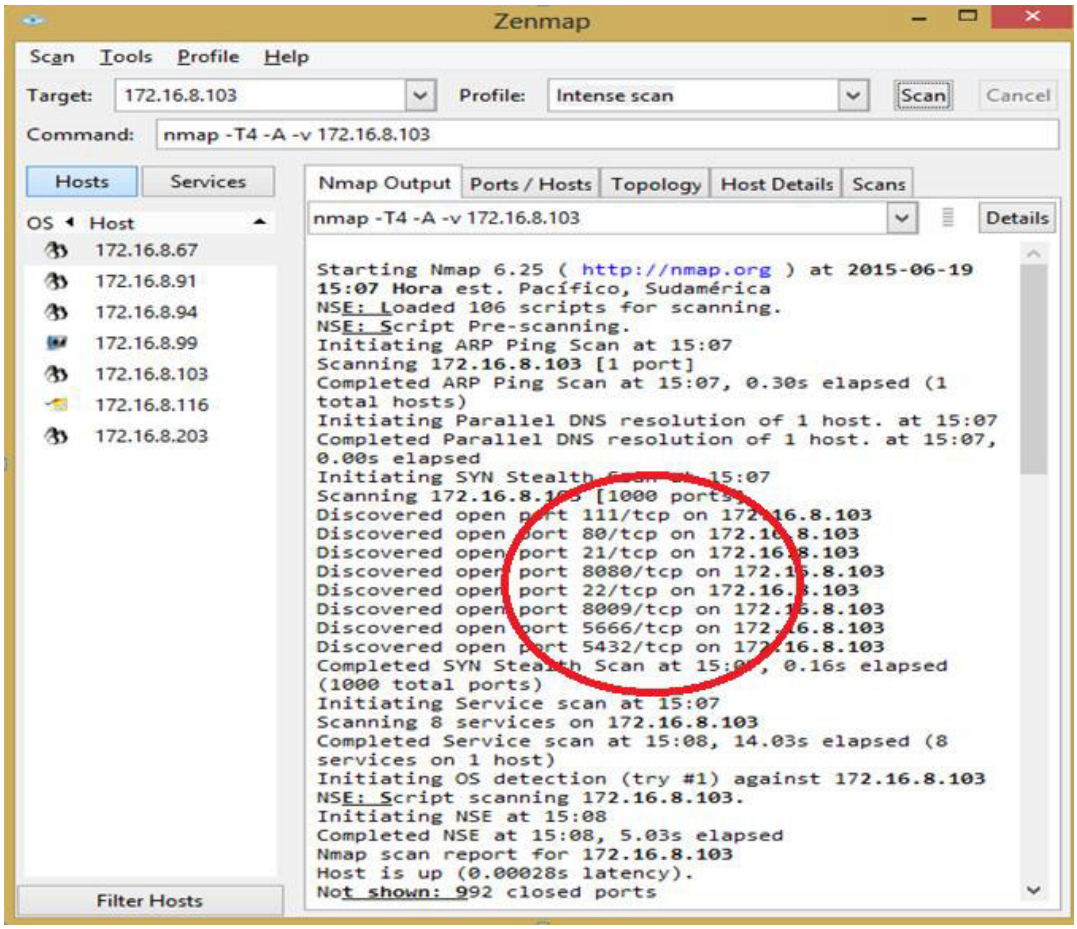


Figura 39. Descubrimiento de puerto con Nmap en un host de la red GAD Ibarra

Fuente: Nmap en la red Gobierno Autónomo Descentralizado San Miguel de Ibarra

2.4.1.6.2 Con Net Tools

En la Figura 40, se representa la captura del reporte generado al escanear el servidor 172.16.8.103 con la herramienta Net Tools.

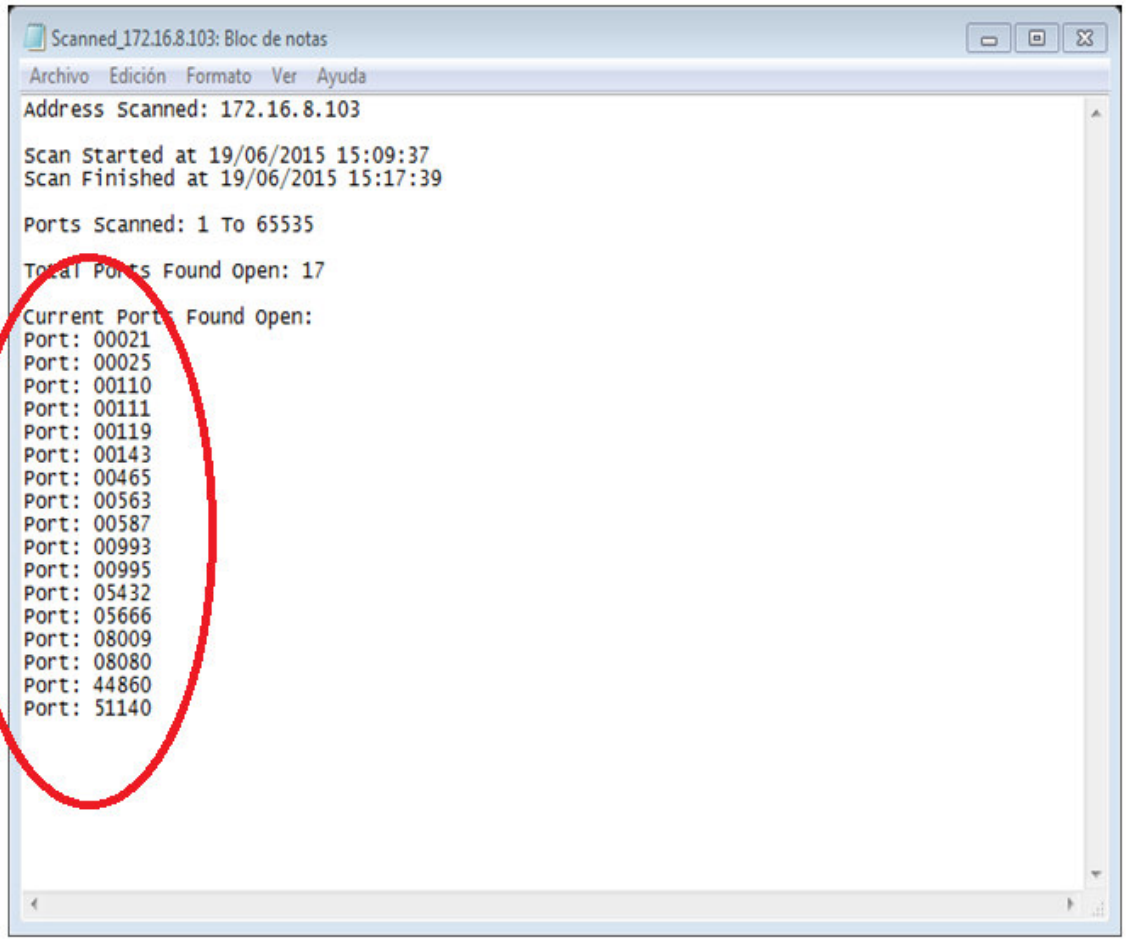


Figura 40. Archivo generado del descubrimiento de puertos con Net Tools en un host de la red GAD Ibarra

Fuente: Net Tools en la red Gobierno Autónomo Descentralizado San Miguel de Ibarra

Una vez realizado este proceso por cada servidor se cotejan los resultados para obtener los puertos de los principales servidores, mostrados en la Tabla 13.

Tabla 13. Resumen de puertos descubiertos en los servidores.

SERVIDOR	PUERTO
Servidor de base de datos	ftp [21], ssh [22], smtp [25], http [80], pop3 [110], sunrpc [111], nntp [119], netbios-ssn [139], imap [143], microsoft-ds [445], urd [465], nntps [563], submission [587], imaps [993], pop3s [995], postgresql [5432], npre [5666], unassigned [39915], unassigned [44788]
Servidor de quipux	ftp [21], ssh [22], smtp [25], http [80] pop3 [110], sunrpc [111], nntp [119], imap [143], urd [465], nntps [563], submission [587], imaps [993], pop3s [995], postgresql [5432], nrpe [5666], unassigned [8009], http-alt [8080]
Servidor de Control de Talento Humano	ftp [21], smtp [25], pop3 [110], nntp [119], epmap [135], netbios-ssn [139], imap [143], microsoft-ds [445], urd [465], nntps [563], submission [587], imaps [993], pop3s [995], iis [1025], bbn 8009 iad [1032],hermes [1248], ncube-lm [1521], pptp [1723], rhp-iibp [1912], ms wbt server [3389], unassigned [5800], rfb [5900], unassigned [8009], http-alt [8080], unassigned [9267].

Servisor VoIP	ssh [22], smtp [25], http [80], pop3 [110], sunrpc [111], nntp [119], imap [143], https [443], urd [465], nntps [563], submission [587], telnets [992], imaps [993], pop3s [995], mysql [3306], upnotifyp [4445], hylafax [4559]
Servidor de correo	ftp [21],smtp [25], pop3 [110], imap [143], https [443], urd [465], submission [587], imaps [993], jabber [5222], npre [5666], vmsvc-2 v[7025]
Servidor DNS Y DHCP	ftp [21], ssh [22], , smtp [25, domain [53], bootps [67], bootpc [68], http [80], streettalk **[**566], webmin [10000].
Servidor Antivirus	epmap [135], netbios-ssn [139], snpp [444]**,** microsoft-ds [445], hermes [1248], unassigned [5800], rfb [5900], ethernet/ip-1 [2222], distinct32 [9998]
Servidor OLYMPO	epmap [135], netbios-ssn [139], microsoft-ds [445], ms-sql-s[1433], cpq-wbem [2301], compaq-https [2381], mercantile [3398], unassigned [5800], rfb [5900].
Servidor Repositorios	ssh [22], http [80], npre [5666]
Servidor Webservice	ssh [22], http [80], npre [5666], http [8080]
Servidor de Aplicaciones Web	ssh [22], smtp [25], http [80], sunrpc [111], npre [5666]
Servidor GIS	ssh [22], http [80], postgresql [5432]

Fuente: Reporte de NMAP Y Net Tools aplicados en red GAD San Miguel de Ibarra

2.4.1.7 **Monitoreo de Llamadas**

Este monitoreo será útil para determinar los parámetros para una llamada con VoIP, los cuales será utilizados más adelante en la definición de políticas.

Se realizó llamadas de pruebas (Ver Figura 41) y se analizó con Wireshark para tomar los parámetros para los cálculos posteriores.

Figura 41. Llamada de teléfono IP con tiempo de duración

Fuente: Teléfonos IP, Gobierno Autónomo Descentralizado San Miguel de Ibarra

La figura 42 se puede observar el resultado de las capturas de Wireshark en donde se muestra los protocolos utilizados durante la transmisión de una llamada de VoIP.

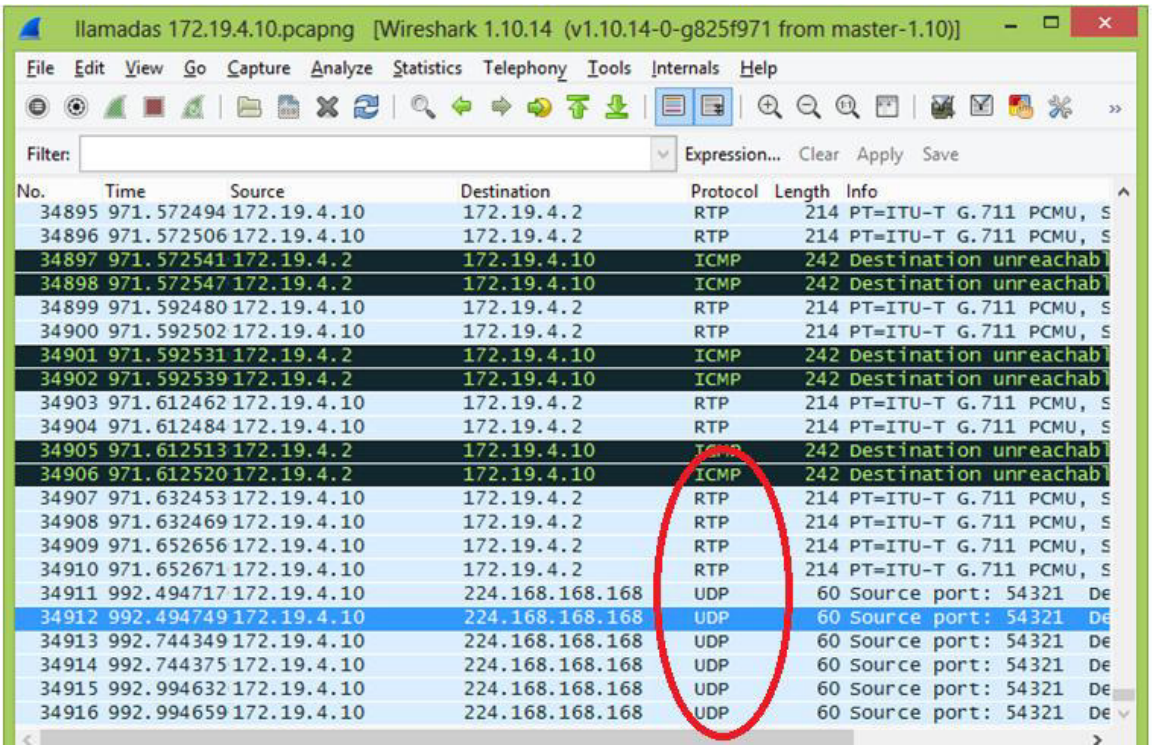


Figura 42. Captura de paquetes de llamada, con Wireshark

Fuente: Wireshark en la red Gobierno Autónomo Descentralizado San Miguel de Ibarra

Las Figuras 43 y 44 muestran el resumen de las dos llamadas con los datos de los paquetes, que pueden ser utilizados para cálculos.

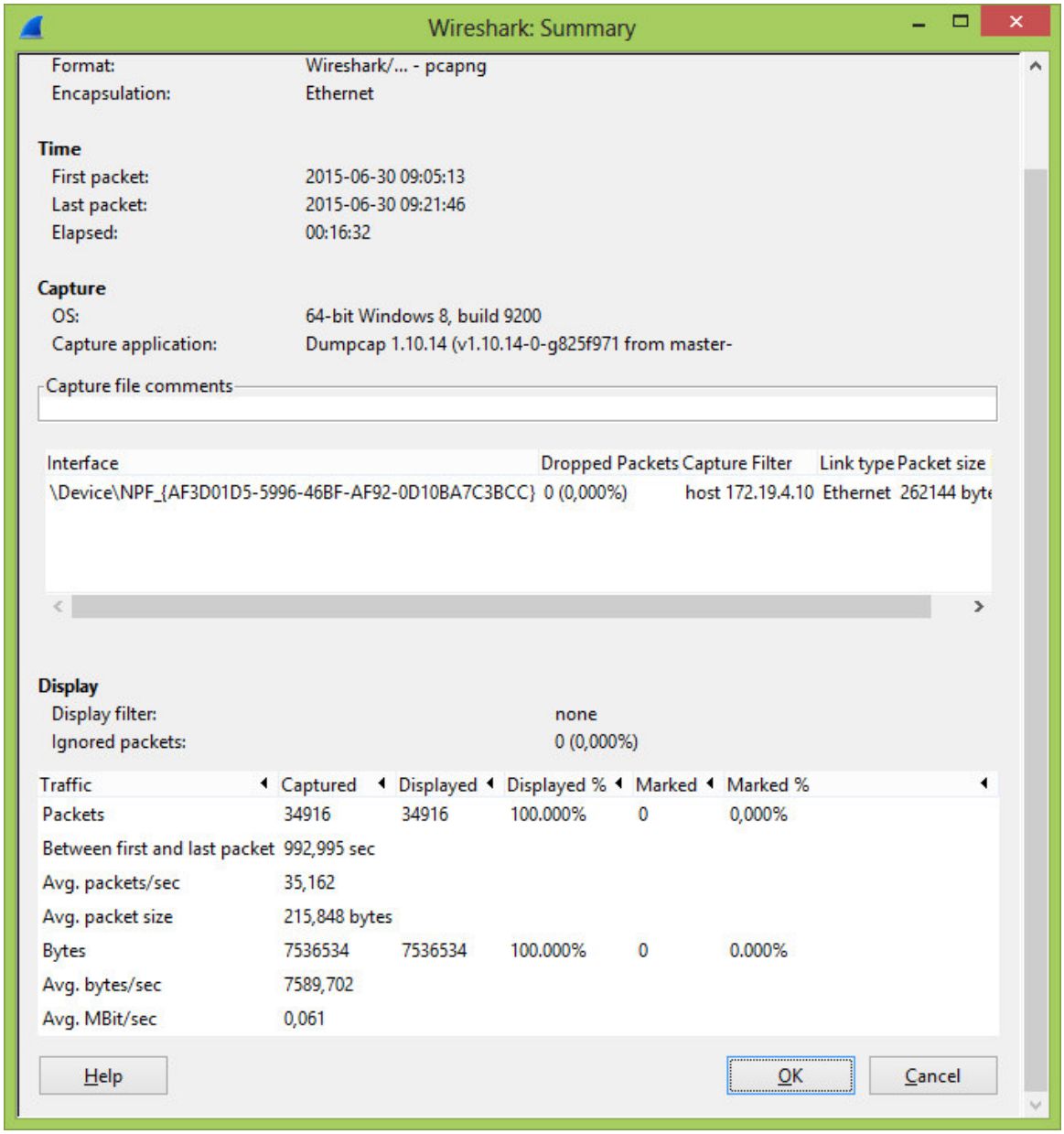


Figura 43. Datos de resumen generado por Wireshark en la llamada de prueba 1

Fuente: Wireshark en la red Gobierno Autónomo Descentralizado San Miguel de Ibarra

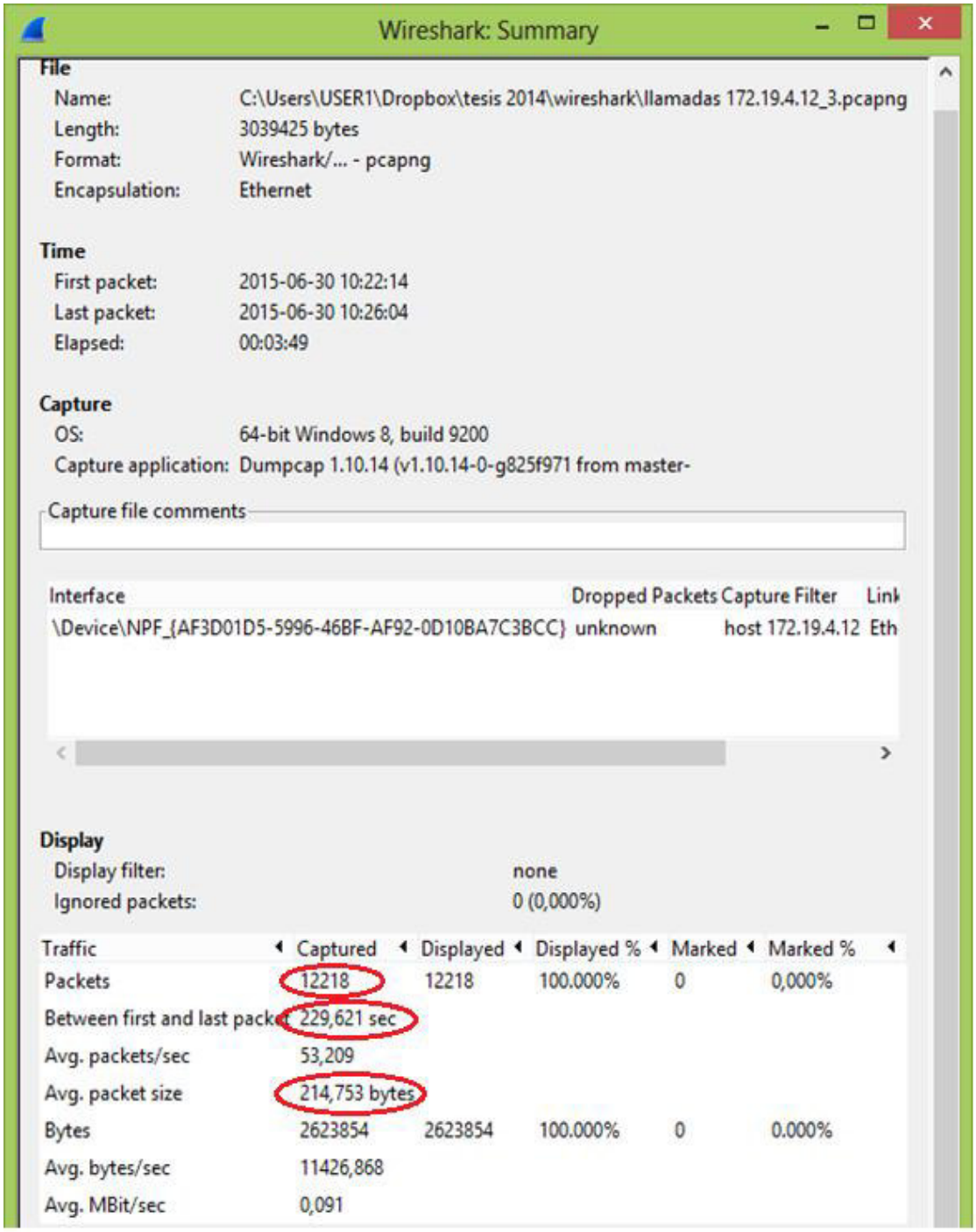


Figura 44. Datos de resumen generado por Wireshark en la llamada de prueba 2

Fuente: Wireshark en la red Gobierno Autónomo Descentralizado San Miguel de Ibarra

Wireshark permite también obtener gráficos por protocolos, en intervalos de tiempo determinados (Ver Figura 45), se muestra el grafico de los protocolos UDP y RTP:

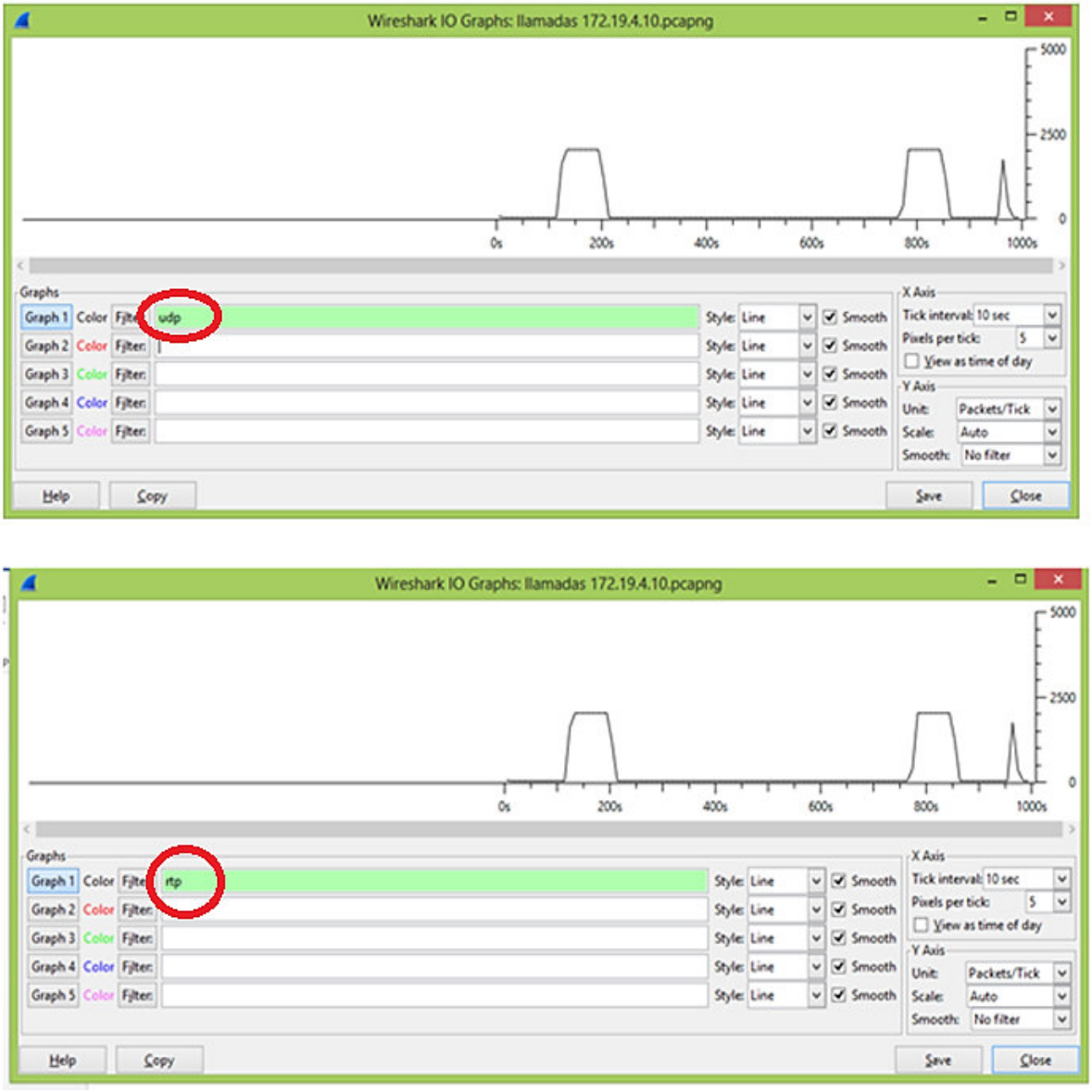


Figura 45. Gráfico de llamada de prueba

Fuente: Wireshark en la red Gobierno Autónomo Descentralizado San Miguel de Ibarra

Con los datos de la llamada de prueba arrojados por Wireshark, señalados en la Figura 44, podemos establecer la capacidad de una llamada promedio, esta información puede ser utilizada para determinar el Ancho de Banda de esta aplicación. Para lo cual se utiliza como

referencia los cálculos encontrados en el desarrollo de trabajo de grado *Rediseño de la red de voz, datos y video para la Unidad Educativa "Santa María de Nazzarello"*, (Aguilar O., 2012, pag.73-74)

$$capacidad = \frac{\#\ bits}{tiempo\ de\ transmision} \quad \textbf{(2)}$$

$$capacidad = \frac{\#\ paquetes\ x\ tamaño(paquete) * 8}{tiempo\ de\ transmision}$$

$$capacidad = \frac{\#\ 12218 * 214.753 * 8}{229.621}$$

$$capacidad = 91.4\ Kbps$$

CAPÍTULO 3

3 IMPLEMENTACIÓN DE POLÍTICAS PARA LA CALIDAD DE SERVICIO

Una vez realizado el estudio para determinar el estado en general de la red y sus principales características, se procede a implementar un entorno de prueba con características similares a la red del GAD Ibarra. Además de acuerdo a los resultados obtenidos en el capítulo anterior se diseña y configura las políticas de calidad de servicio. El presente capitulo detallará este proceso.

3.1 LA RED EN EL ENTORNO DE PRUEBA

El ambiente de prueba se implementó en el SIMULADOR GNS3, el cual nos permitió mediante sus herramientas realizar una topología de prueba similar a la red real.

3.2 TOPOLOGÍA DE LA RED EN GNS3

En esta sección se describe las consideraciones iniciales para la implementación del proyecto.

La figura 46 muestra la topología de la red de prueba la cual se realiza tomando en cuenta los siguientes parámetros:

Por efectos de simulación y dadas las limitaciones del simulador, se configuran todas las políticas de Calidad de Servicio en el Switch de Core, las VLans se configuraron en el

Switch Acceso, esto en cuanto a la simulación dentro de GNS3. Los Switches 1 y 2 son switches físicos básicos que se utilizan para armar la topología de prueba completa, se utilizan dos debido a que los switches básicos no son configurables, manejan un solo dominio de broadcast y se necesitan dos para probar la funcionalidad de las VLAN.

Sin embargo cabe aclarar que la topología real no se encuentra los dispositivos en cascada y no es recomendable esta disposición de elementos en una topología real.

También es importante precisar que para probar la funcionalidad de las políticas de Calidad de Servicio se realizó dos escenarios:

Primer escenario, se presenta una simulación en GNS3, con la red plana; con los servidores y clientes, los clientes que pueden hacer uso de los diferentes servicios de la red, se configuran las VLANS, existe conectividad entre clientes y en los dispositivos de red únicamente se configuran las interfaces que permita la comunicación entre los elementos de la red (Ver Anexo 6).

Segundo escenario, aquí se presenta en cambio la red con la configuración de políticas en los dispositivos correspondientes, esta configuración se detalla más adelante en el apartado 3.3.7

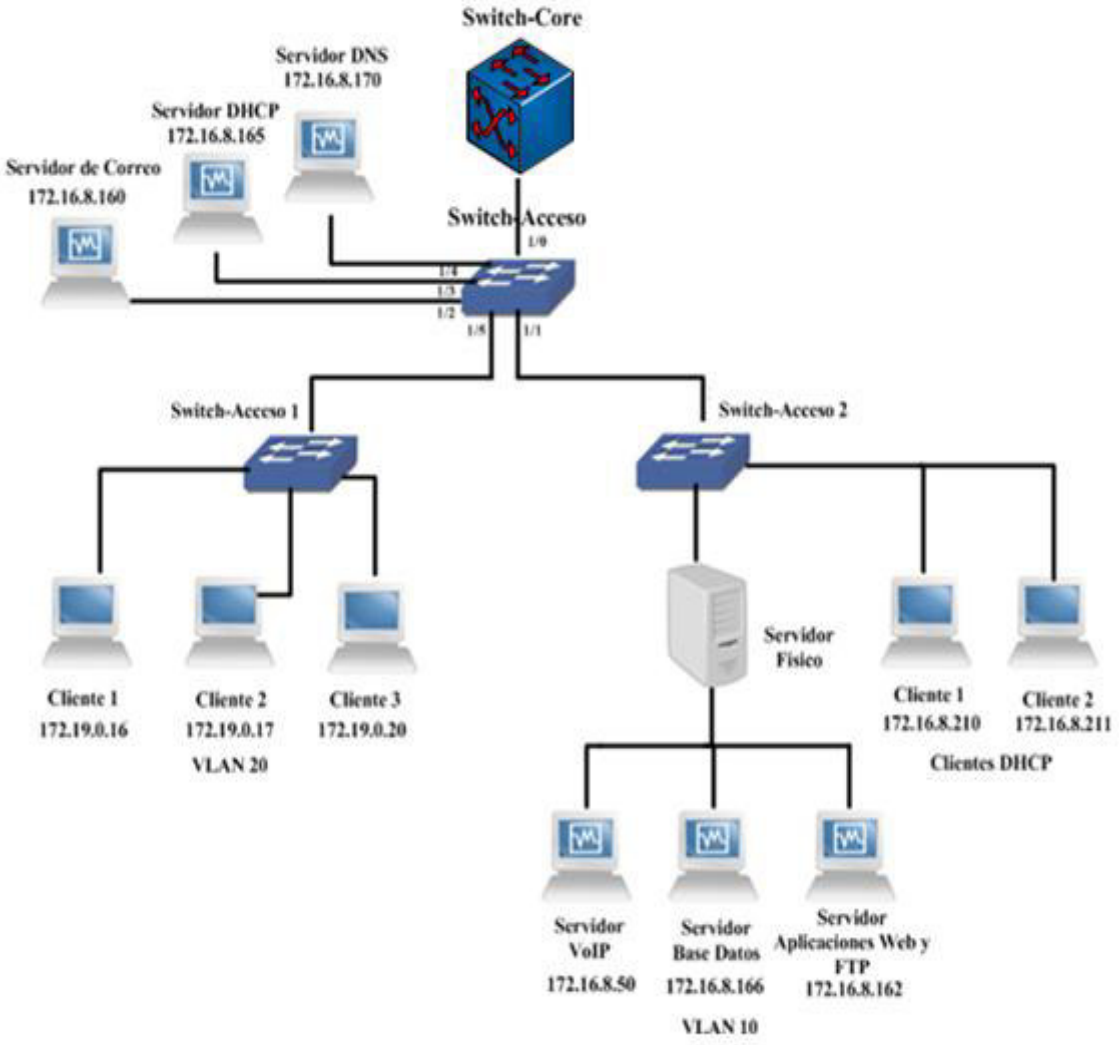


Figura 46. Topología Red GNS 3

Fuente: Simulador GNS3

3.2.1 Direccionamiento de la red:

Se muestran, en tablas 14, 15 y 16, las direcciones IP de los diferentes elementos utilizados en el diseño:

Tabla 14. Direccionamiento de VLAN del Switch

Nombre del Switch	Dirección IP de VLAN	Máscara de Subred	Nombres y Números de VLAN	Asignación de puertos del Switch
SW-CORE	172.X.X.1	255.255.255.0	VLAN 10 Servidores	Fa1/1 - 1/5
	172.Y.X.1	255.255.255.0	VLAN 20 Tecnologías	Fa 1/10

Fuente: Elaboración Propia

Tabla 15. Direccionamiento de servidores

Host	Dirección IP	Máscara de subred	Gateway
VoIP	172.X.X.50	255.255.255.0	172.16.8.1
Correo	172.X.X.160	255.255.255.0	172.16.8.1
Web y FTP	172.X.X.162	255.255.255.0	172.16.8.1
DHCP	172.X.X.165	255.255.255.0	172.16.8.1
Base de Datos	172.X.X.166	255.255.255.0	172.16.8.1
DNS	172.X.X.170	255.255.255.0	172.16.8.1

Fuente: Elaboración Propia

Tabla 16. Direccionamiento de host

Host	Dirección IP	Máscara de subred	Gateway
Cliente 1	172.Y.X.16	255.255.255.0	172.19.0.1
Cliente 2	172.Y.X.17	255.255.255.0	172.19.0.1

Cliente 3	172.Y.X.20	255.255.255.0	172.19.0.1
Cliente 4	DHCP		
Cliente 5	DHCP		

Fuente: Elaboración Propia

3.2.2 Servidores:

Utilizando servidores virtuales y físicos se implementa la topología de la red de prueba, dentro de la topología simulada en GNS3 se encuentran los servidores: DNS, DHCP y Correo; en una máquina externa se encuentran virtualizados los servidores de VoIP, Base de datos, Web y FTP. En el Anexo 5, se muestra el proceso de instalación de los mismos. Tabla 17, presenta los servidores con su respectivo sistema Operativo.

Tabla 17. Servidores y sus SO

Host	**Sistema Operativo**
VoIP	Elastix
Correo	Deepin
Web y FTP	Debian
DHCP	Debian
Base de Datos	Windows 7
DNS	Deepin

Fuente: Elaboración Propia

3.2.3 Puertos

Para la determinación de los puertos se tomó como base el estudio realizado en la red real, pero de igual forma se realizó el mapeo en el escenario con la red plana, con el objetivo de obtener una simulación sin errores.

De los resultados del Capítulo 2, apartado 2.4.1.6 y el escaneo de puertos en la red de la simulación en la VLAN de servidores, se obtiene los valores de la Tabla 18, que muestra el detalle de la dirección IP, el servicio y los puertos que utilizan para el caso de la simulación.

Tabla 18. Descubrimiento de puertos

IP	Servicio	Puertos
172.16.8.1	Puerta de enlace	telnet [23], smtp [25], pop3 [110], nntp [119], imap [143], urd [465], nntps [563], submission [587], imaps [993], pop3s [995], h323hostcall [1720], sip [5060]
172.16.8.50	Servidor de voip	ssh [22], smtp [25], http [80], pop3 [110], sunrpc [111], nntp [119], imap [143], https [443], urd [465], nntps [563],

		submission [587], telnets [992], imaps [993], pop3s [995], mysql [3306], upnotifyp [4445], hylafax [4559]
172.16.8.165	Servidor dhcp	bootps [67], bootpc [68], smtp [25], pop3 [110], nntp [119], imap [143], urd [465], nntps [563],, submission [587], imaps [993], pop3s [995]
172.16.8.170	Servidor de DNS	ftp [21], smtp [25], domain [53], http [80], pop3 [110], nntp [119], imap [143], urd [465], nntps [563], submission [587], imaps [993], pop3s [995]
172.16.8.162	Servidor ftp, y web	ftp [21], smtp [25], http [80], pop3 [110], sunrpc [111], nntp [119], imap [143], urd [465], nntps [563], submission [587], imaps [993], pop3s [995]
172.16.8.166	Servidor de base de datos	smtp [25], pop3 [110], nntp

		[119], epmap [135], netbios-ssn [139], imap [143], microsoft-ds [445], urd [465], rtsp [554], nntps [563], submission [587], imaps [993], pop3s [995], icslap [2869]
172.16.8.160	Servidor de Correo	smtp [25], pop3 [110], nntp [119], epmap [135], netbios-ssn [139], imap [143], microsoft-ds [445], urd [465], nntps [563], submission [587], imaps [993], pop3s [995], postgresql [5432], http-alt [8080]

Fuente: Elaboración Propia

Si bien la mayoría de los puertos son los mismos, se tiene algunos puertos adicionales y otros que no constan, debido a que, en primer lugar para la simulación solo se implementan los servicios más importantes, y en segundo lugar el software de simulación mantiene interconexión con otros software , para lograr el enlace con los servidores externos así como con las interfaces físicas , por lo tanto requiere puertos adicionales que deben estar activos para que la simulación funcione correctamente .Por lo tanto los puertos que no constan en la tabla anterior y difieren de la Tabla 13, se bloquean ya que en la red de simulación no se

encuentran activos y toda vez que no se realice ninguna regla en las ACL, los puertos quedan bloqueados.

3.3 DEFINICIÓN DE POLÍTICAS DE QoS

3.3.1 Determinación de frontera de confianza

En el caso del presente proyecto, considerando los recursos disponibles se define dentro frontera de confianza al Switch de Core, que cumple con los requerimientos teóricos de acuerdo al siguiente análisis:

- Soporta QoS
- Como se había determinado en el capítulo anterior (Ver Tabla 9), se trata de una red de núcleo contraído la cual fusiona la capa distribución y la de núcleo en una sola, razón por la cual el Switch de Core es parte de la capa de distribución, por lo que estamos cumpliendo con las recomendaciones teóricas
- Este dispositivo está dentro de nuestro control administrativo

3.3.2 Consideraciones iniciales

Basado en las necesidades de la institución se seleccionaran las aplicaciones y servicios más importantes. Esta información nos permite determinar la prioridad en los tráficos cursados por la red.

Es importante repasar la siguiente información:

3.3.2.1 **Aplicaciones de prioridad crítica**

Son aplicaciones en tiempo real por lo que se las considera como aplicaciones críticas a VoIP y videoconferencia, requieren un ancho de banda considerable para su que permita evitar la pérdida de paquetes y retardos en dichas aplicaciones.

3.3.2.2 **Aplicaciones de prioridad alta**

En este tipo de aplicaciones la importancia no radica en el ancho de banda que ocupa, pues no requieren demasiado; más bien en el impacto sobre el valor agregado de la Institución En este tipo de aplicaciones constan las bases de datos, Aplicaciones WEB.

3.3.2.3 **Aplicaciones de prioridad media**

Permiten que todos los recursos de red se identifiquen entre sí y se encuentren accesibles para los usuarios de acuerdo a su nivel, Un problema en este tipo de aplicaciones afecta directamente a la capacidad de los usuarios de realizar operaciones normales, Son tolerantes al retardo. En este tipo de aplicaciones se pueden mencionar: DNS, DHCP.

3.3.2.4 **Aplicaciones de prioridad baja**

Tienen mayor resistencia al retardo, y que en circunstancias de fallos no afectan al correcto funcionamiento de la red, sin impacto en la capacidad de los usuarios de realizar sus operaciones normales. En este tipo de aplicaciones constan: correo, descargas, etc.

3.3.2.5 **Aplicaciones y Prioridades para la red del GAD Municipal de San Miguel de Ibarra.**

Una vez definidos los tipos de aplicaciones y de acuerdo a lo establecido con los Analistas del área de TICs, encargados de la administración de la red, se despliega la Tabla 19 con los requerimientos:

Tabla 19. Clasificación del tráfico.

APLICACIÓN	PRIORIDAD	OBSERVACIÓN
Telefonía IP	Critica	Debido a que es una aplicación en tiempo real
Aplicaciones web	alta	De acuerdo a la definición de las necesidades instituciones, debido a que mediante estas se provee servicios e información a los usuarios diariamente (consulta, seguimiento e ingreso de trámites, información general)
Bases de datos	alta	De acuerdo a la definición de las necesidades instituciones, esta aplicación es la más usada ya que por medio de esta se controla el funcionamiento mismo de las actividades del GAD Municipal de San Miguel de Ibarra a través del sistema integrado explicado en el apartado 2.2.3.2
DNS	media	Servicio de red necesario para el adecuado funcionamiento de la misma.
DHCP	baja	Servicio de red importante para el adecuado funcionamiento de la misma.

Cualquier otro	default	Pertenecientes a varias aplicaciones restantes de la red en estudio

Fuente: Gobierno Autónomo Descentralizado San Miguel de Ibarra de San Miguel de Ibarra, Dirección TIC

3.3.3 Definición del modelo de QoS

Para empezar señalemos que el modelo TCP/IP fue diseñado para brindar un servicio Best-Effort, es decir no garantiza niveles de servicio para aplicaciones en tiempo real, es decir las aplicaciones con voz y video.

Basado en este análisis comparativo de apartado 1.1.4.4 se concluye que DiffServ ofrece mayores ventajas respecto IntServ con respecto escalabilidad, flexibilidad y clasificación por medio del marcado de paquetes y otras técnicas de control de tráfico. Se define entonces, el modelo *Diffserv (Servicios Diferenciados)*, como la alternativa más viable para la implementación en este proyecto.

3.3.4 Clasificación y marcado

3.3.4.1 **Clasificación mediante Lista de control de acceso ACL`*s***

Las Listas de Control de Acceso son un mecanismo para clasificar tráficos por separación de privilegios, Permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores.

Sus objetivos principales son:

- Filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

- Limitar el tráfico de red y mejorar el rendimiento de la red.

Las ACLs nos servirán para filtrar los tipos de tráfico y poder marcarlos de manera adecuada.

3.3.4.2 **Marcado**

El marcado de paquetes como es propio del modelo Diffserv se realiza mediante DSCP. DSCP define valores de marcado de un paquete conjuntamente estos los valores de define además acciones denominadas comportamientos de reenvío los valores posibles de DSCP y su comportamiento asociado, están definidos en la Tabla 5 en el apartado 1.1.5.1.4 del capítulo 1.

Se determinan entonces, en la Tabla 20, los valores de DSCP, que serán posteriormente configurados.

Tabla 20. Valores para el marcado por aplicación

PRIORIDAD	**APLICACIÓN**	**VALOR DSCP**
CRÍTICA	TELEFONÍA IP	EF
ALTA	BASES DE DATOS	AF31
	APLICACIONES WEB	AF33
MEDIA	DNS	AF21
BAJA	DHCP	AF23
DEFAULT	CUALQUIER OTRO	0

Fuente: Elaboración Propia

3.3.5 Asignación de Ancho de Banda

3.3.5.1 **Calculo AB para VoIP**

Para el cálculo de Ancho de Banda para VoIP, se utiliza la Ecuación 3 (CX INNOVATING COMUNICATIONS, 2013, Ancho de banda utilizado por VoIP. Recuperado de: http://www.3cx.es/ancho-de-banda-voip/)

$$AB = Vtrx * \#Llamadas * 2 \quad (3)$$

Dónde:

- AB: Ancho de banda
- Vtrx: Velocidad de transmisión de una llamada telefónica, según códec de audio (Ver Tabla 21)
- #Llamadas: Número de llamadas simultaneas.

Tabla 21. Codecs de audio y sus velocidades

CODEC	TAMAÑO TOTAL
G.711	95.2 kbps
G.722	95.2 kbps
G.723.1	21.9 kbps
G.729	39.2 kbps
GSM	44.2 kbps

Fuente: InPhonex (2014). Requerimientos de Banda Ancha y CODECs Recuperado de: http://www.inphonex.es/soporte/voip-codecs.php

Tabla 22. Valores de datos para cálculo de AB para VoIP

Dato	Valor
Vtrx:	Debido a q se usa el códec G711 la velocidad de transmisión es de **95,2 kbps** aproximadamente. (Ver Tabla 22)
#Llamadas:	**98 llamadas** , dato proporcionado por la Dirección de TIC del GAD de San Miguel de Ibarra

Fuente: Elaboración Propia

CÁLCULO:

$$AB = Vtrx * \#Llamadas * 2$$

$$AB = 95{,}2\ kbps * 98 * 2$$

$$\boldsymbol{AB = 18{,}7\ Mbps}$$

Con el valor de AB obtenido se procede a calcular el porcentaje que representa en la red:

$$\%\ AB = \frac{18{,}7\ Mbps}{97\ Mbps} * 100\ \%$$

$$\%\ AB = 0{,}19278 * 100\ \%$$

$$\%\ AB = 19{,}3\ \%$$

$$\%\ \boldsymbol{AB} \cong \mathbf{20}\ \%$$

3.3.5.2 **Calculo AB para Base de datos**

Para realizar el cálculo del AB para la base de datos, primero se procede a obtener el valor de una consulta de BBD, en la institución. Se tomó como referencia los cálculos

encontrados en el desarrollo de trabajo de grado *Integrar Servicios mediante el Diseño de la Red, Sobre el Anillo de Fibra Óptica en el Gobierno Autónomo Descentralizado de San Miguel de Ibarra, Basado en La Tecnología de Transmisión SDH*, (Anangonó J., 2015,pag.95)

El valor del tamaño de la consulta es 72KB.

El cálculo de Ancho de Banda para este tipo de tráfico se lo realiza utilizando la Ecuación 4 (*Como determinar/calcular el ancho de banda* Recuperado de: http://goo.gl/EOK7r8 & http://goo.gl/ctMfs7)

$$AB = T * t * N \quad (4)$$

En donde:

- AB: Ancho de banda.
- T: Tamaño promedio de una consulta.
- t: Tiempo de carga de una consulta.
- N: Número de consultas simultaneas

Tabla 23. Valores de datos para cálculo de AB para tráfico de base de datos

Dato	Valor
T	**72 KB** , Obtenido de Trabajo de Tesis, Anangonó J., 2015,pag.95
t	**3 s** Dato proporcionado por la Dirección de TIC del GAD de San Miguel de Ibarra. De acuerdo al Analista, Ing. Manuel Lara

N	**75 consultas simultaneas**, dato proporcionado por la Dirección de TIC del GAD de San Miguel de Ibarra, De acuerdo al Analista, Ing. Manuel Lara.

Fuente: Elaboración Propia

CÁLCULO:

$$AB = T * t * N$$

$$AB = \frac{72\ KBytes}{1\ consulta} * \frac{1\ consulta}{3\ s} * \frac{8\ bits}{1\ Byte} * 75$$

$$AB = 14{,}4\ Mbps$$

Con base en los cálculos anteriores se definen los porcentajes de ancho de banda sintetizados en la siguiente tabla:

$$\%\ AB = \frac{14{,}4 Mbps}{97\ Mbps} * 100\ \%$$

$$\%\ AB = 0{,}14845 * 100\ \%$$

$$\%\ AB = 14{,}85\%$$

$$\%\ \boldsymbol{AB} \cong \mathbf{15}\ \%$$

3.3.5.3 **Calculo AB para tráfico Web**

Para calcular el Ancho de Banda para este tipo de tráfico se utiliza la Ecuaci*ó*n 5 (*COMO DETERMINAR/CALCULAR EL ANCHO DE BANDA,* Recuperado de: http://goo.gl/EOK7r8 & http://goo.gl/ctMfs7)

$$AB = T * t * N \quad (5)$$

En donde:

- AB: Ancho de banda.
- T: Tamaño promedio de una consulta WEB
- t: Tiempo de carga para una consulta WEB
- N: Número de visitas simultaneas.

Tabla 24. Valores de datos para cálculo de AB para trafico web

Dato	Valor
T	**76.80KB** ≅ **77*KB*** Dato proporcionado por la Dirección de TIC del GAD de San Miguel de Ibarra, se toma el mayor valor entre los tamaños promedios (Ver anexo 4, pág. 8, apartado *Paginas URLs)*
t	**4.55 s** ≅ **5 *s*** Referirse a http://tools.pingdom.com/fpt/#!/bhpixS/http://ibarra.gob.ec
N	**78 visitas simultaneas** , dato proporcionado por la Dirección de TIC del GAD de San Miguel de Ibarra

Fuente: Elaboración Propia

CÁLCULO:

$$AB = T * t * N$$

$$AB = \frac{77KBytes}{1\ consulta\ WEB} * \frac{1\ consulta\ WEB}{5s} * \frac{8\ bits}{1\ Byte} * 78$$

$$AB = 9{,}61Mbps$$

Con el valor de AB obtenido se procede a calcular el porcentaje que representa en la red:

$$\% AB = \frac{9{,}61\ Mbps}{97\ Mbps} * 100\ \%$$

$$\% AB = 0{,}09906 * 100\ \%$$

$$\% AB = 9{,}91\ \%$$

$$\% \boldsymbol{AB} \cong \mathbf{10}\ \%$$

3.3.5.4 **AB para tráfico Web DNS y DHCP**

Los valores de ancho de banda para el tráfico DNS y DHCP, fueron determinados por requerimientos de los administradores de la red, basado en estadísticas recuperadas del análisis de la red realizado con NTOP (Ver figura 47). Así se estableció 3% para DNS como un promedio de los datos estadísticos arrojados por NTOP (Ver Anexo 2) y 2% para DHCP, como requerimiento de los administradores de la red considerando que es servicio ocupa menos ancho de banda que el DNS.

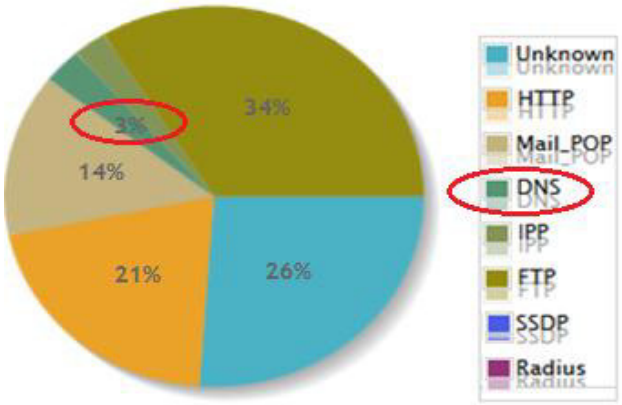


Figura 47. Porcentaje de uso de AB de diferentes servicios

Fuente: NTOP Gobierno Autónomo Descentralizado San Miguel de Ibarra

Con base en los cálculos anteriores se definen los porcentajes de ancho de banda sintetizados en la Tabla 25, cabe indicar que este representa el porcentaje mínimo asegurado para cada clase, dependiendo de la disponibilidad de la red las aplicaciones pueden utilizar mayor, pero nunca menos del valor determinado.

Tabla 25. Asignación de porcentaje de Ancho de Banda

APLICACIÓN	PRIORIDAD	VALOR DE DSCP	POLÍTICAS APLICADAS % DE ANCHO DE BANDA
Telefonía IP	Critica	EF	20%
Aplicaciones web	Alta	AF33	10%
Bases de datos	Alta	AF31	15%
DNS	Media	AF21	3%
DHCP	Baja	AF23	2%
Cualquier otro	Default	DEFAULT	----

Fuente: Elaboración Propia

3.3.6 Elección del método de encolamiento

En el capítulo 1 se detalló los tipos de encolamiento, para el desarrollo del presente trabajo de acuerdo a las características de cada encolamiento de determinan los tipos de encolamiento para cada clase:

Clase VoIP, para esta clase se eligió el método LLQ(Low-Latency Queuing), debido a que este es el método que debe ser usado para aplicaciones en tiempo real, este tiene una cola específicamente dedicada a aplicaciones en tiempo real. Esta es la cola de prioridad estricta.

Esta cola será configurada al momento de establecer las políticas para cada clase

Utilizando el comando `priority percent,` el cual permite establecer la cola de prioridad estricta propia de este método

Clase APLICACIONES_WEB y BASE_DATOS , para estas clases se establece el método CBWFQ (Class Based Weighted Fair Queuing), debido a que permite la creación de colas para cada clase de tráfico definida, cada una de las cuales es de tipo FIFO, con un ancho de banda garantizado y un número máximo de paquetes.

Clase DCHP, DNS y demás tipo de tráfico, se mantendrá con WFQ (Weighted Fair Queuing), el cual divide el tráfico en flujos y, a estos flujos se les asigna un ancho de banda adecuado; los flujos con mayor prioridad son los que tienen mayor ancho de banda asignado.

En la Tabla 26 se muestra un resumen de las políticas a configurarse:

Tabla 26. Resumen Politicas QoS

APLICACIÓN	PRIORIDAD	POLÍTICAS APLICADAS		
		VALOR DE DSCP	% AB	TIPO DE ENCOLAMIENTO
Telefonía IP	Critica	EF	20%	LLQ
Aplicaciones web	Alta	AF33	10%	CBWFQ
Bases de datos	Alta	AF31	15%	CBWFQ
DNS	Media	AF21	3%	WFQ
DHCP	Baja	AF23	2%	WFQ

Cualquier otro	Default	DEFAULT	----	WFQ

Fuente: Elaboración Propia

3.3.7 Configuración de políticas en equipos

Una vez determinadas las políticas, se procede a realizar la respectiva configuración en los equipos para implementarlas. En los Anexos 7 y 8, se muestran los archivos de configuración completos del Switch de Core y el Switch de Acceso.

3.3.7.1 **Configuraciones de access-list**

Como se describió anteriormente se procede a filtrar en tráfico; se implementa ACL's extendidas pues permiten filtrar tráfico de acuerdo al origen, destino, puerto y protocolo a diferencia de las ACL's estándar que bloquean o permiten únicamente de acuerdo al origen. Esto se realiza basado en el análisis de los puertos realizado por cada tipo de aplicaciones. Se crean las siguientes listas de control de acceso

- APLICACIONES_WEB
- BASE_DATOS
- DCHP
- DNS
- TELEFONIA_IP

Se consideran los siguientes comandos importantes para la configuración de este proceso:

ip access-list extented name: permite crear una lista de acceso, se debe indicar su nombre

{deny/permit} tipo de protocolo **{any/host}** [source wildcard] **{range/eq}** número de puerto: Especifica el tipo de tráfico a permitir o bloquear de acuerdo a las condiciones definidas:

deny/permit: Permite o bloquea dependiendo de las condiciones previamente establecidas. **tipo de protocolo:** Tipo de tráfico puede ser IP, TCP, UDP, ICMP, GRE, IGRP

any/host: Indica la red o host origen (any significa cualquier origen)

source wildcard: Ingresar la red o el host por donde los paquetes son enviados inicialmente. Se puede utilizar la palabra any como una abreviación para 0.0.0.0 255.255.255.255

number port: Es el puerto o rango de puertos que se van a filtrar

Se muestra las líneas de comandos utilizadas para esta configuración:

```
SW-CORE (config)#ip access-list extended APLICACIONES_WEB
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.162 eq ftp
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.162 eq smtp
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.162 eq www
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.162 eq pop3
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.162 eq sunrpc
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.162 eq nntp
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.162 eq 143
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.162 eq 465
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.162 eq 563
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.162 eq 587
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.162 eq 993
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.162 eq 995
```

```
SW-CORE (config)#ip access-list extended BASE_DATOS
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.166 eq smtp
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.166 eq pop3
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.166 eq nntp
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.166 eq 135
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.166 eq 139
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.166 eq 143
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.166 eq 445
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.166 eq 465
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.166 eq 563
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.166 eq 587
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.166 eq 993
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.166 eq 995
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.166 eq 5432
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.166 eq 8080

SW-CORE (config)#ip access-list extended DCHP
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.165 eq 67
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.165 eq 68
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.165 eq smtp
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.165 eq pop3
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.165 eq nntp
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.165 eq 143
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.165 eq 465
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.165 eq 563
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.165 eq 587
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.165 eq 993
SW-CORE(config-ext-nacl)#permit tcp host 172.16.8.165 eq 995
```

```
SW-CORE (config)#ip access-list extended DNS
SW-CORE(config-ext-nacl)#permit tcp host 172.16.6.170 eq ftp
SW-CORE(config-ext-nacl)#permit tcp host 172.16.6.170 eq smtp
SW-CORE(config-ext-nacl)#permit tcp host 172.16.6.170 eq domain
SW-CORE(config-ext-nacl)#permit udp host 172.16.6.170 eq domain
SW-CORE(config-ext-nacl)#permit tcp host 172.16.6.170 eq www
SW-CORE(config-ext-nacl)#permit tcp host 172.16.6.170 eq pop3
SW-CORE(config-ext-nacl)#permit tcp host 172.16.6.170 eq nntp
SW-CORE(config-ext-nacl)#permit tcp host 172.16.6.170 eq 143
SW-CORE(config-ext-nacl)#permit tcp host 172.16.6.170 eq 465
SW-CORE(config-ext-nacl)#permit tcp host 172.16.6.170 eq 563
SW-CORE(config-ext-nacl)#permit tcp host 172.16.6.170 eq 587
SW-CORE(config-ext-nacl)#permit tcp host 172.16.6.170 eq 993
SW-CORE(config-ext-nacl)#permit tcp host 172.16.6.170 eq 995

SW-CORE(config)#ip access-list extended TELEFONIA_IP
SW-CORE(config-ext-nacl)#permit udp any any range 16384 32767
SW-CORE(config-ext-nacl)#permit tcp any any eq 1720
SW-CORE(config-ext-nacl)#permit tcp any eq 1720
SW-CORE(config-ext-nacl)#permit udp any eq 1720
SW-CORE(config-ext-nacl)#permit tcp any eq 5060
SW-CORE(config-ext-nacl)#permit udp any eq 5060
SW-CORE(config-ext-nacl)#permit tcp any eq 563
SW-CORE(config-ext-nacl)#permit udp any eq 563
SW-CORE(config-ext-nacl)#permit udp any eq sunrpc
SW-CORE(config-ext-nacl)#permit tcp any eq sunrpc
SW-CORE(config-ext-nacl)#permit tcp any eq 994
SW-CORE(config-ext-nacl)#permit udp any eq 994
SW-CORE(config-ext-nacl)#permit tcp any eq 22
```

```
SW-CORE(config-ext-nacl)#permit tcp any eq smtp
SW-CORE(config-ext-nacl)#permit tcp any eq www
SW-CORE(config-ext-nacl)#permit tcp any eq pop3
SW-CORE(config-ext-nacl)#permit tcp any eq nntp
SW-CORE(config-ext-nacl)#permit tcp any eq 143
SW-CORE(config-ext-nacl)#permit tcp any eq 443
SW-CORE(config-ext-nacl)#permit tcp any eq 465
SW-CORE(config-ext-nacl)#permit tcp any eq 587
SW-CORE(config-ext-nacl)#permit tcp any eq 993
SW-CORE(config-ext-nacl)#permit tcp any eq 995
SW-CORE(config-ext-nacl)#permit tcp any eq 3306
SW-CORE(config-ext-nacl)#permit tcp any eq 4190
SW-CORE(config-ext-nacl)#permit udp any eq 4190
SW-CORE(config-ext-nacl)#permit udp any eq 4445
SW-CORE(config-ext-nacl)#permit tcp any eq 4445
SW-CORE(config-ext-nacl)#permit tcp any eq 4559
SW-CORE(config-ext-nacl)#permit tcp any eq 5058
SW-CORE(config-ext-nacl)#permit udp any eq 5058
SW-CORE(config-ext-nacl)#permit udp any eq 4559
```

3.3.7.2 **Configuración de las clases**

En esta parte se muestra los comandos para la creación de las distintas clases de tráfico a las que más adelante se aplican las políticas. Se crean las siguientes clases:

- APLICACIONES_WEB
- BASE_DATOS
- DCHP

- DNS
- TELEFONIA_IP

Comandos importantes para la configuración de este proceso:

class-map [match-all/match-any] class-map-name Crea una asignación de clase, y permite ingresar al modo de configuración de class-map.

match-all: Comunica a la clase asignada que debe cumplir todos los parámetros de la ACL, asignados a los paquetes que pertenecen a esta clase.

match-any: La clase asignada que debe cumplir con cualquier parámetro.

class-map-name: Colocar el nombre de la class-map

match {access-group name ACL} Con este comando se especifica número o nombre de la ACL a la cual se va a asociar la clase definida previamente.

```
SW-CORE(config)#class-map match-all TELEFONIA_IP
SW-CORE(config-cmap)#match access-group name TELEFONIA_IP
SW-CORE(config-cmap)#exit

SW-CORE(config)#class-map match-all BASE_DATOS
SW-CORE(config-cmap)#match access-group name BASE_DATOS
SW-CORE(config-cmap)#exit

SW-CORE(config)#class-map match-all APLICACIONES_WEB
SW-CORE(config-cmap)#match access-group name APLICACIONES_WEB
SW-CORE(config-cmap)#exit
```

```
SW-CORE(config)#class-map match-all DHCP
SW-CORE(config-cmap)#match access-group name DHCP
SW-CORE(config-cmap)#exit

SW-CORE(config)#class-map match-all DNS
SW-CORE(config-cmap)#match access-group name DNS
SW-CORE(config-cmap)#exit
```

3.3.7.3 **Configuración de las políticas**

Con los comandos que se muestran a continuación se configuran las políticas establecidas en los apartados 3.3.4.2 y 3.3.5

Comandos importantes:

`policy-map` `policy-map-name` Permite crear una asignación de políticas, y entra al modo de configuración de policy-map, se debe indicar el nombre de la política

`class` `class-map-name` Define la clasificación de tráfico e ingresa al modo de configuración policy-map-class

`set {ip dscp new-precedence}` Marca el tráfico mediante la asignación de un nuevo valor a DSCP, el cual pertenece a una clase.

`bandwidth percent value` Especifica la asignación del ancho de banda como un porcentaje de la velocidad de enlace subyacente

```
SW-CORE(config)#policy-map POLITICAS

SW-CORE(config-pmap)#class TELEFONIA_IP
SW-CORE(config-pmap-c)#set ip dscp ef
SW-CORE(config-pmap-c)#priority percent 20
SW-CORE(config-pmap-c)#exit

SW-CORE(config-pmap)#class BASE_DATOS
SW-CORE(config-pmap-c)#set ip dscp af31
SW-CORE(config-pmap-c)#bandwidth percent 15
SW-CORE(config-pmap-c)#exit

SW-CORE(config-pmap)#class APLICACIONES_WEB
SW-CORE(config-pmap-c)#set ip dscp af33
SW-CORE(config-pmap-c)#bandwidth percent 10
SW-CORE(config-pmap-c)#exit

SW-CORE(config-pmap)#class DHCP
SW-CORE(config-pmap-c)#set ip dscp af23
SW-CORE(config-pmap-c)#bandwidth percent 2
SW-CORE(config-pmap-c)#exit

SW-CORE(config-pmap)#class DNS
SW-CORE(config-pmap-c)#set ip dscp af21
SW-CORE(config-pmap-c)#bandwidth percent 3
SW-CORE(config-pmap-c)#exit
```

```
SW-CORE(config-pmap)#class class-default
SW-CORE(config-pmap-c)#set ip dscp default
SW-CORE(config-pmap-c)#exit
```

3.3.7.4 **Aplicación de las políticas a las interfaces**

`configure terminal:` permite conectarse en modo de configuración global

`Interface` `[nombre de la interfaz_ número de la interfaz]:` Especifica e ingresa la interfaz a configurar.

`service-policy input/ output` `[policy-map-name]:` Especifica el nombre de las políticas, y las aplica dependiendo del sentido en el que se dirige el tráfico ya sea input/output.

`end:` salir del modo configuración global

```
SW-CORE(config)#configure terminal
SW-CORE(config)#interface FastEthernet1/0
SW-CORE(config-if)#service-policy output POLITICAS
SW-CORE(config-if)# end
SW-CORE#copy running-config startup-config
```

CAPÍTULO 4

4 PRUEBAS DE FUNCIONAMIENTO

Para determinar la funcionalidad de las políticas establecidas se plantearon dos escenarios el primero que está configurado QoS y el segundo escenario no está configurado ninguna regla de QoS, en los cuales se probara la calidad de la voz transmitida con la medición de parámetros de jitter retardo en el programa Wireshark, además se determinará la velocidad de transferencia de descarga de un archivo y finalmente una prueba de conectividad con un ping extendido para visualizar el tiempo de respuesta.

En este apartado se mostrará las capturas de pantalla del router CISCO 7200 de las configuraciones de QoS implementadas en el programa de GNS3, que en nuestra simulación corresponden a la frontera de confianza y su correcto funcionamiento.

4.1 COMPROBACIÓN DE LA FUNCIONALIDAD DE LAS POLÍTICAS DE CALIDAD DE SERVICIO QoS

4.1.1 Comprobación del filtrado de tráfico en el switch de core/distribución

Se configuro ACLs extendidas para el proceso de filtrado del tráfico, el mismo que es indispensable para posteriormente clasificar los diferentes paquetes. En la Figura 48 se muestra el resultado del comando **`show access-list`**, que muestra todas las ACL creadas.

```
Extended IP access list TELEFONIA_IP
    10 permit udp any any range 16384 32767
    20 permit tcp any any eq 1720
    30 permit tcp any eq 1720 any
    40 permit udp any eq 1720 any
    50 permit tcp any eq 5060 any
    60 permit udp any eq 5060 any (385 matches)
    70 permit tcp any eq 563 any
    80 permit udp any eq 563 any
    90 permit udp any eq sunrpc any
    100 permit tcp any eq sunrpc any
    110 permit tcp any eq 994 any
    120 permit udp any eq 994 any
    130 permit tcp any eq 22 any
    140 permit tcp any eq smtp any
    150 permit tcp any eq www any (9980 matches)
    160 permit tcp any eq pop3 any
    170 permit tcp any eq nntp any
    180 permit tcp any eq 143 any
    190 permit tcp any eq 443 any (4200 matches)
```

Figura 48. ACL configuradas

Fuente: SW-CORE GNS3

4.1.2 Comprobación de la clasificación del tráfico en el switch de core

En el proceso de clasificación del tráfico se asoció las ACLs ya creadas dentro de una clase de tráfico las cuales se pueden ver con el comando **`show class-map`** como se muestra en la Figura 49.

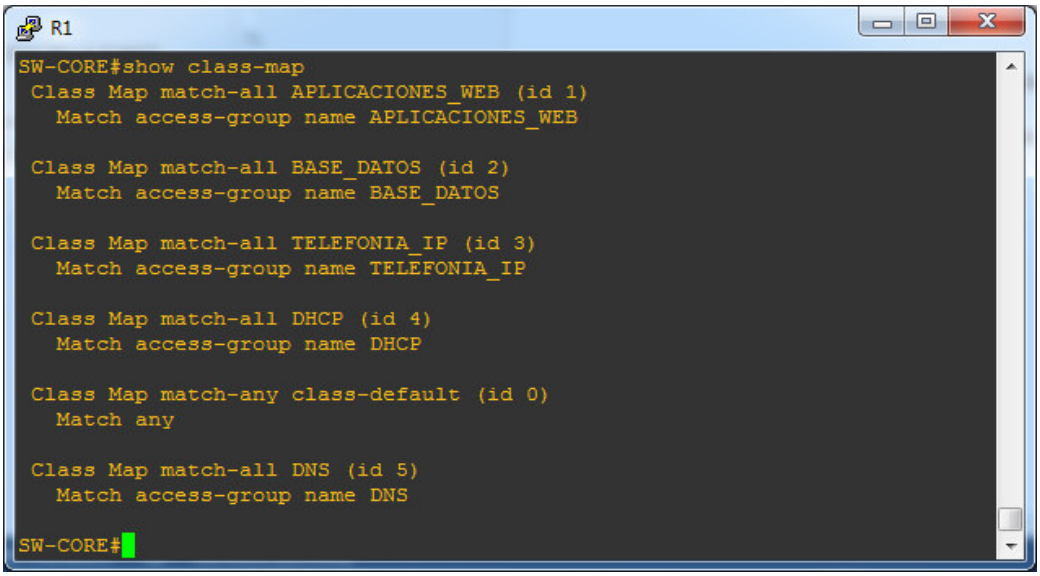


Figura 49. Verificación de clases creadas

Fuente: SW-CORE GNS3

4.1.3 Comprobación del marcaje y políticas del tráfico en el switch de core.

El proceso de marcaje se configuro en el switch de core , esto se basó en un previo clasificado con ACLs y marcado del tráfico a través del DSCP, con las respectivas políticas que permiten delimitar la tasa de transmisión para cada clase esto se basó en los criterios del DTIC.

En la tabla 26, se muestra en forma sintetizada el ancho de banda mínimo asegurado para cada clase, la clase telefonía IP y señalización se les asignó el 20% del ancho de banda disponible además de ser la única clase que se le ha dado prioridad por tratarse de tráfico en tiempo real, a las bases de datos un 15% y Aplicaciones web se les asignó un 10% del ancho de banda disponible respectivamente, generando así una estructura de red basada en niveles. Con el comando show policy-map se puede ver las clases creadas con su respectivo valor de dscp, como se puede ver en la Figura 50.

Se utiliza el comando **`show policy-map`**

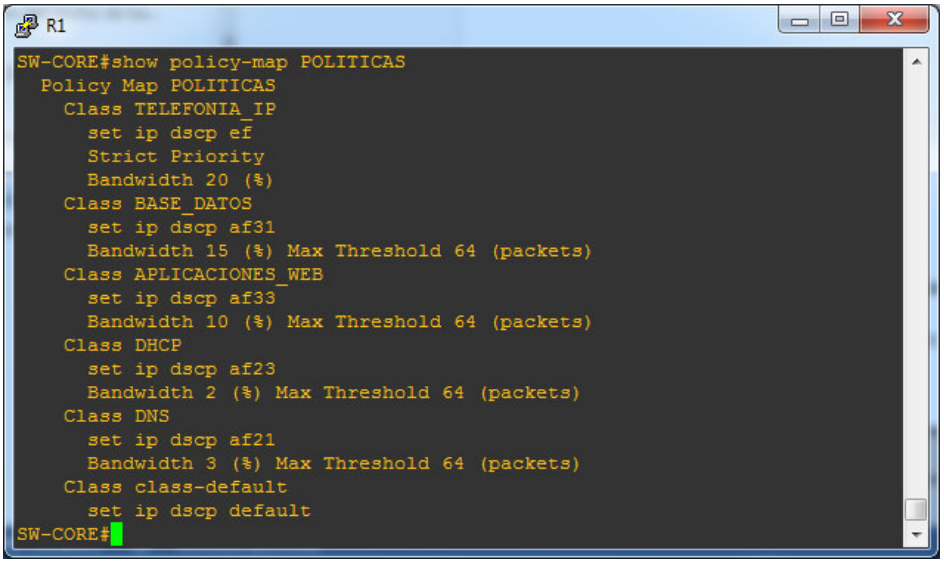


Figura 50. Políticas establecidas, para cada clase

Fuente: SW-CORE GNS3

De manera más específica utilizando el comando **`show policy-map interface [nombre + número de la interfaz],`** se puede obtener información con clase además de las estadísticas del marcado de los paquetes, esto se muestra en las Figuras 51 y 52

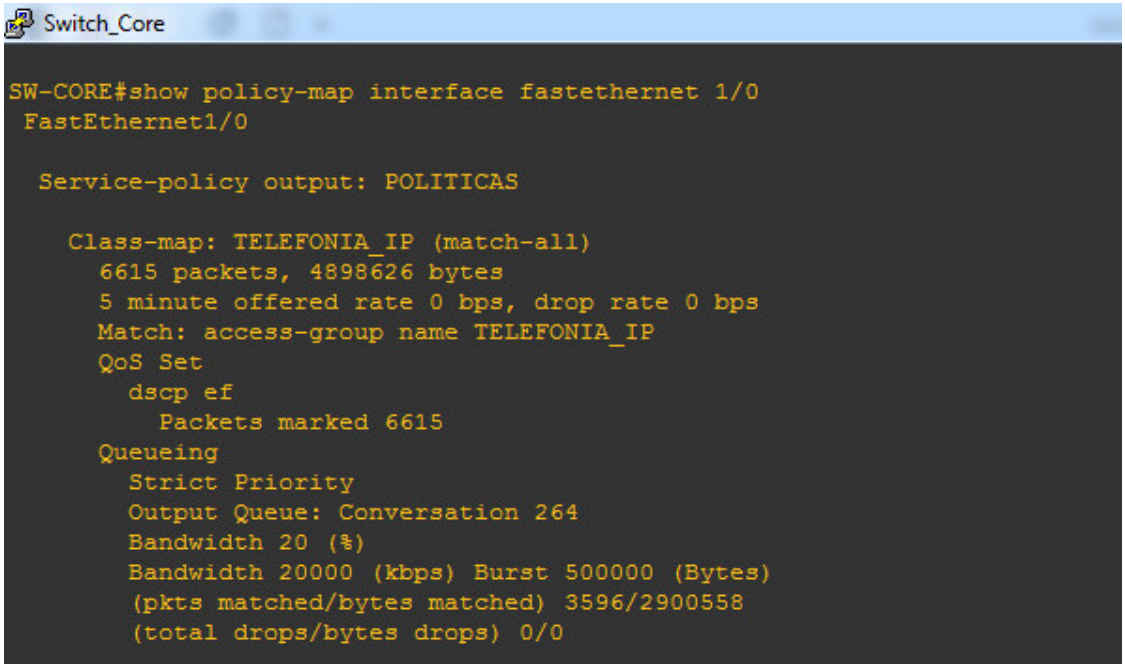


Figura 51. Información Políticas Clase Telefonia_IP

Fuente: SW-CORE GNS3

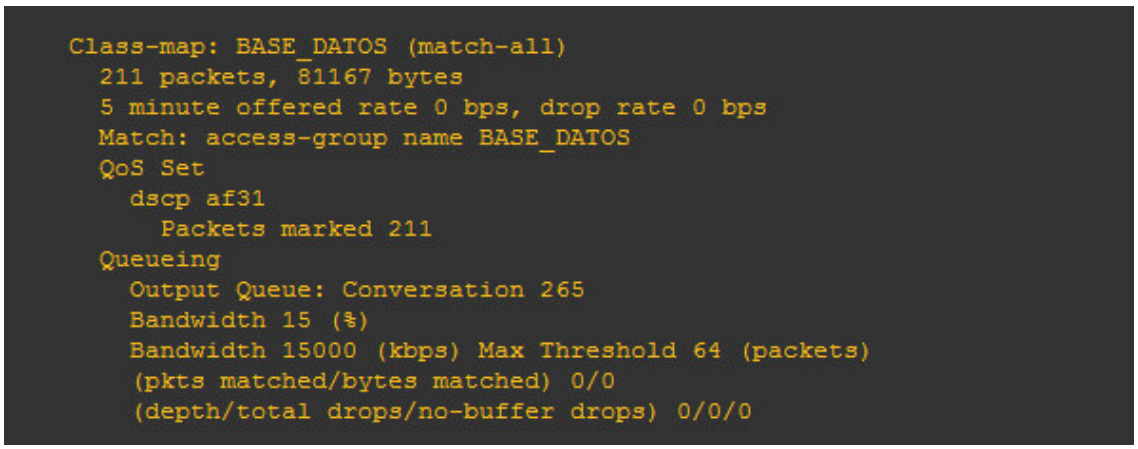


Figura 52. Información Políticas Clase BASE_DATOS

Fuente: SW-CORE GNS3

4.1.4 Comprobación encolamiento

El comando **`show queueing interface`** `[nombre + número de la interfaz],` permite observar que clase de encolamiento está configurado (Ver figura 53).

```
SW-CORE#show queueing interface fastethernet 1/0
Interface FastEthernet1/0 queueing strategy: fair
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 6978
  Queueing strategy: Class-based queueing
  Output queue: 0/1000/64/6978 (size/max total/threshold/drops)
     Conversations  0/7/256 (active/max active/max total)
     Reserved Conversations 4/4 (allocated/max allocated)
     Available Bandwidth 25000 kilobits/sec
```

Figura 53. Tipo de encolamiento configurado

Fuente: SW-CORE GNS3

También se puede utilizar el comando **`show queueing,`** para observar los tipos de cola, en la figura se puede apreciar la cola de tipo ***Priority,*** la cual fue configurada para la clase de VoIP (Ver figura 54).

```
SW-CORE#show queueing
Current fair queue configuration:

  Interface           Discard    Dynamic  Reserved  Link    Priority
                      threshold  queues   queues    queues  queues
  FastEthernet1/0     64         256      256       8       1
```

Figura 54. Tipos de colas

Fuente: SW-CORE GNS3

4.2 PRUEBAS DE FUNCIONAMIENTO

Para probar las políticas implementas en el diseño de la red del IMI, se procedió a poner a funcionar todos los servicios virtualizados que presta la red atraves de dos usuarios que hacen solicitudes a la red de servidores, generando asi que cursen por la red diferentes

tipos de trafico tanto TCP como ls voz y UDP como el correo, aplicaciones web, servicio de transferencia de archivos, paginas webs entre otros.

4.2.1 PRUEBAS SIN CALIDAD DE SERVICIO

Como resultados se obtuvo que la red funcionaba correctamente con el trafico TCP, pero el problema que se generaba cuando cursaba por la red trafico UDP, es decir cuando se realizaba una llamada, todos los servicios se perdían o se ejecutaban de manera inadecuada. El ping se perdía, la transferencia de archivos se cancelaba, no se podía acceder a la base de datos y la página web se cargaba lentamente.

4.2.1.1 **Prueba de descarga de un archivo**

En la figura se puede observar la descarga de un archivo desde un servidor FTP funciona correctamente antes de hacer una llamada telefónica (Ver figura 55).

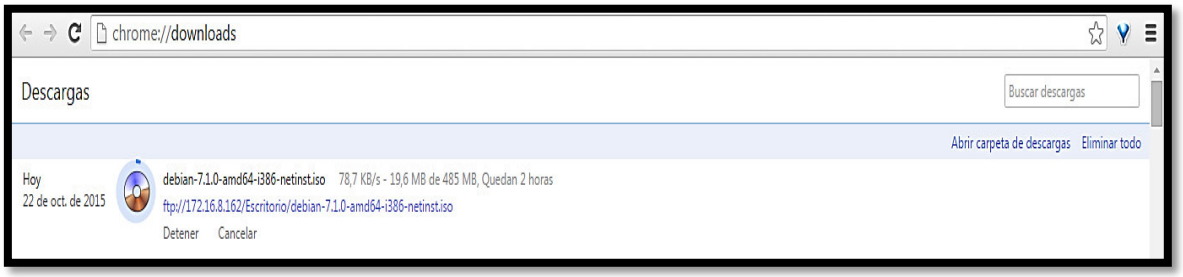


Figura 55. Descarga servidor FTP, sin llamada

Fuente: Host red topología de prueba

En la Figura 56 se puede observar que al hacer una llamada telefónica la descarga se cancela.

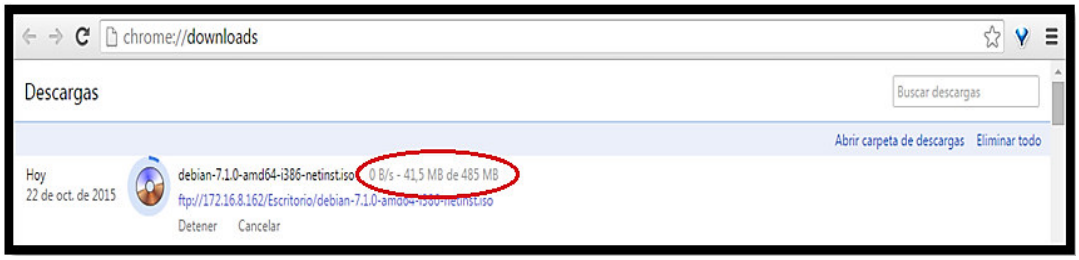


Figura 56. Descarga detenida servidor FTP, al realizar una llamada

Fuente: Host red topología de prueba

4.2.1.2 **Prueba de conectividad paquetes ICMP**

En la Figura 57 se puede observar cómo se detiene el envió de paquetes ICMP al iniciar una llamada.

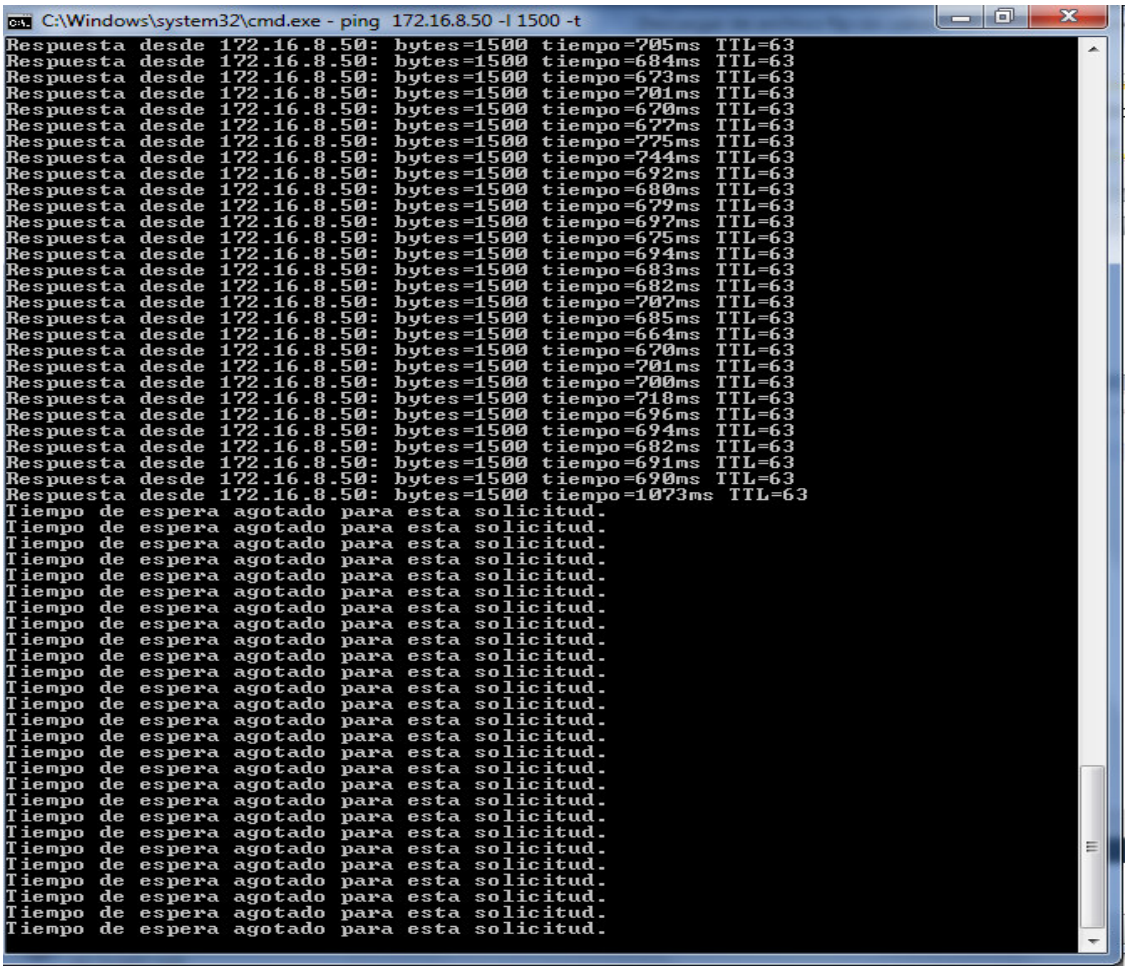
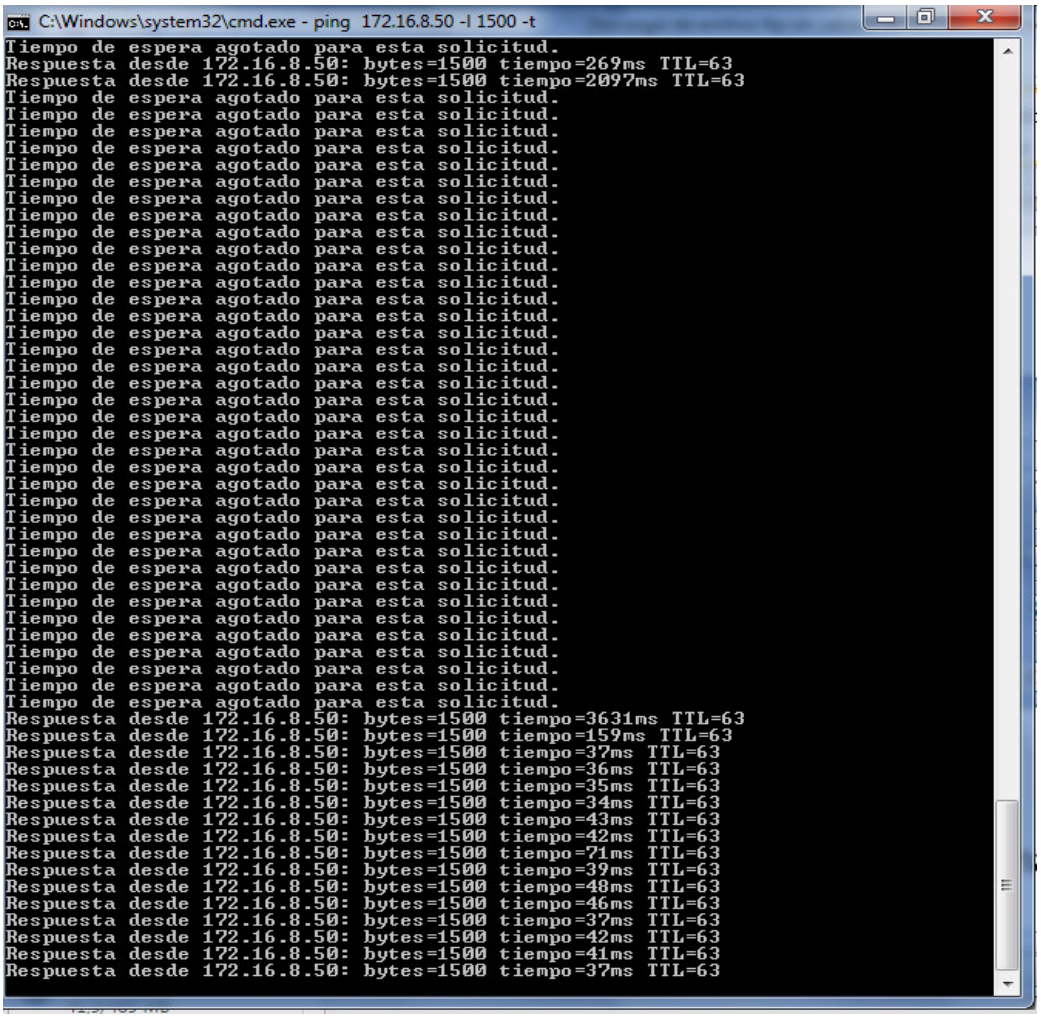


Figura 57. Paquetes se detienen al iniciar una llamada

Fuente: Host red topología de prueba

En la Figura 58 se muestra como regresan los paquetes ICMP después de colgar la llamada


C:\Windows\system32\cmd.exe - ping 172.16.8.50 -l 1500 -t
Tiempo de espera agotado para esta solicitud.
Respuesta desde 172.16.8.50: bytes=1500 tiempo=269ms TTL=63
Respuesta desde 172.16.8.50: bytes=1500 tiempo=2097ms TTL=63
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.
Tiempo de espera agotado para esta solicitud.

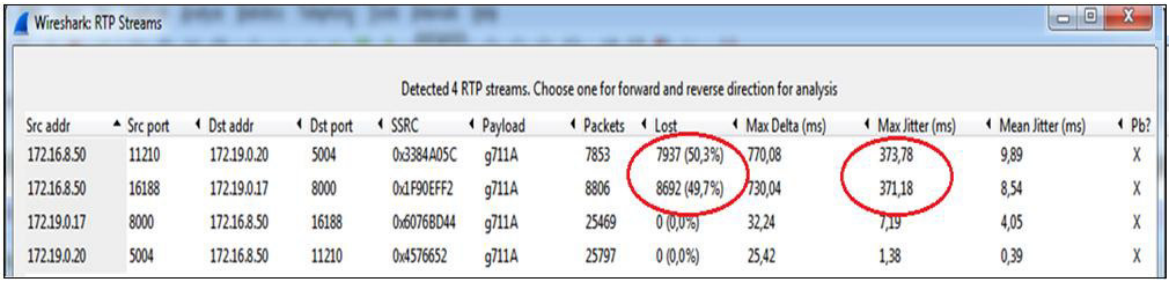


Figura 59. Parámetro VoIP sin QoS

Fuente: WIRESHARK en host red topología de prueba

Es importante señalar los parámetros recomendados de acuerdo a los estándares para VoIP (Ver Tabla 27)

Tabla 27. Valores Recomendados para VoIP

PARÁMETRO	VALOR
Pérdida de paquetes	**<1%**
Jitter	**<100 ms**

Referencia: QOS-CALIDAD DE SERVICIO PARA VOIP Recuperado de: http://elastixtech.com/qos-calidad-de-servicio-para-voip/

4.2.1.4 **Conectividad con servidores sin QoS**

Sin calidad de servicio se puede observar que las aplicaciones; correo, base de datos, web, ftp se cancelan al momento de realizar una llamada porque esta consume todo el ancho de banda de la red dejando sin inhabilitados a los demás servicios (Ver figura 60) y al instante que se cuelga la llamada los servicios empiezan a funcionar nuevamente.

Figura 60. Varios servicios sin Qos

Fuente: Host red topología de prueba

4.2.2 PRUEBAS CON CALIDAD DE SERVICIO

Como resultado de la aplicación de las políticas de calidad de servicio en nuestra red, la red mejora el desempeño de las distintas clases de tráfico. Funcionan correctamente el trafico TCP y UDP, se supera el problema que existía de caída de la red cuando se ejecutaba una llamada esto se debe a que el ancho de banda esta segmentado en porcentajes de acuerdo a las políticas de QoS.

4.2.2.1 **Prueba de descarga de un archivo**

En la figura 61 se puede observar que una vez realizada la configuración de parámetros de QoS en los switches de GNS3, se sigue teniendo acceso a los servicios y estos funcionan correctamente cuando se realiza una llamada telefónica.

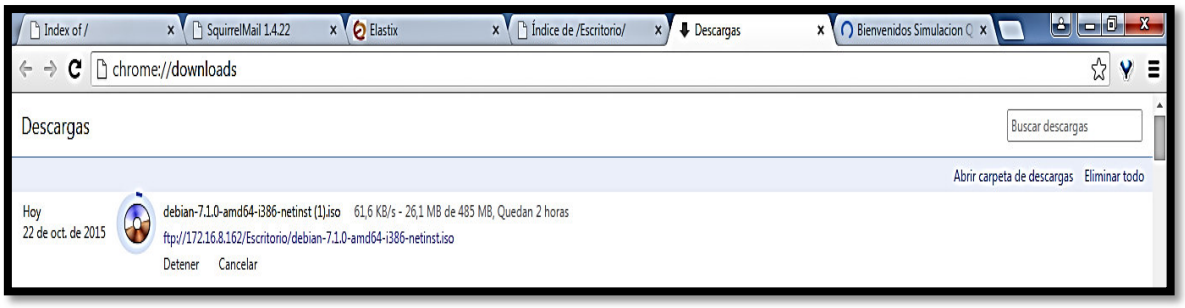


Figura 61. Descarga de archivo, con QoS,sin realizar llamada

Fuente: Host red topología de prueba

La figura 62, muestra, la descarga funcionando de manera normal, mientras se lleva a cabo una llamada

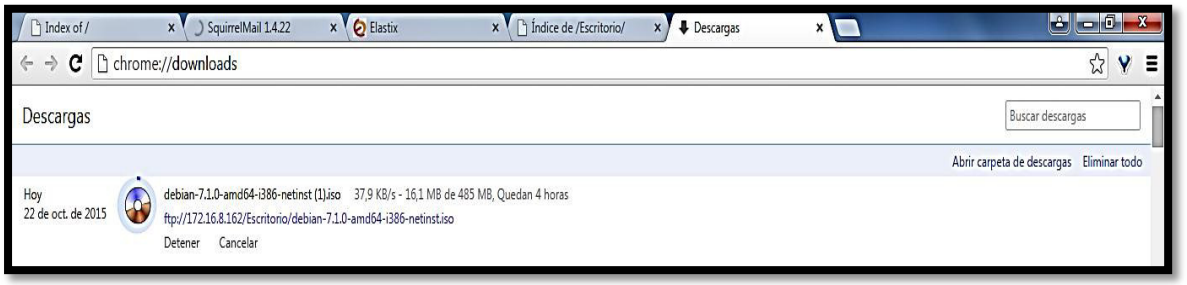


Figura 62. Descarga de archivo, con QoS, realizando llamada

Fuente: Host red topología de prueba

4.2.2.2 **Prueba de conectividad paquetes ICMP**

La conectividad paquetes ICMP no se pierde, al realizar una llamada una vez implementada la calidad de servicio, como se observa en la figura 63.

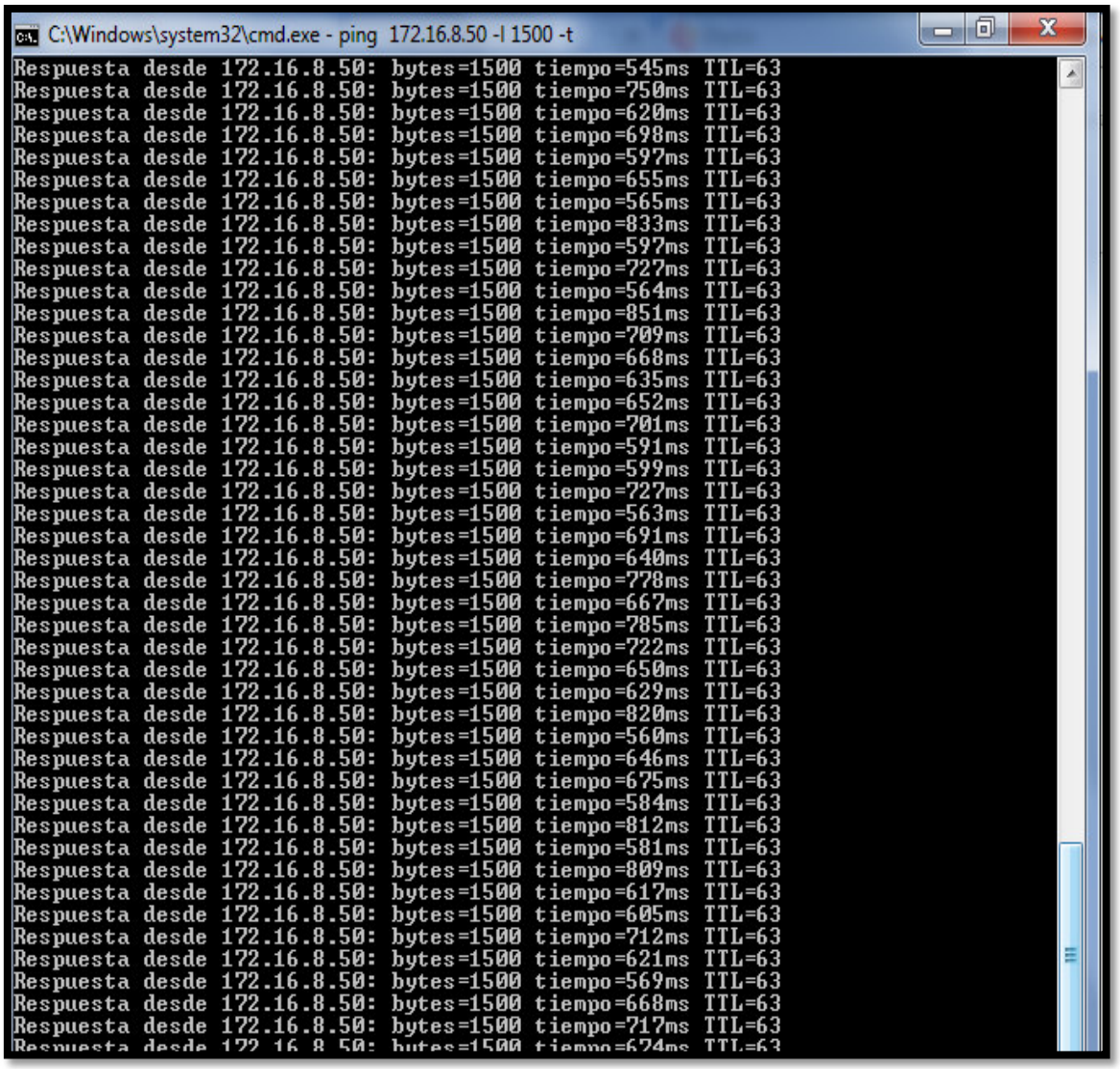


Figura 63. Paquetes se no se interrumpen mientras se lleva a cabo la llamada

Fuente: Host red topología de prueba

4.2.2.3 **Prueba de VoIP**

Con respecto al trafico UDP, los parámetros de calidad mejoran notablemente la calidad de las llamadas y los parámetros técnicos del máximo retardo y el jitter como se puede ver en la Figura 64.

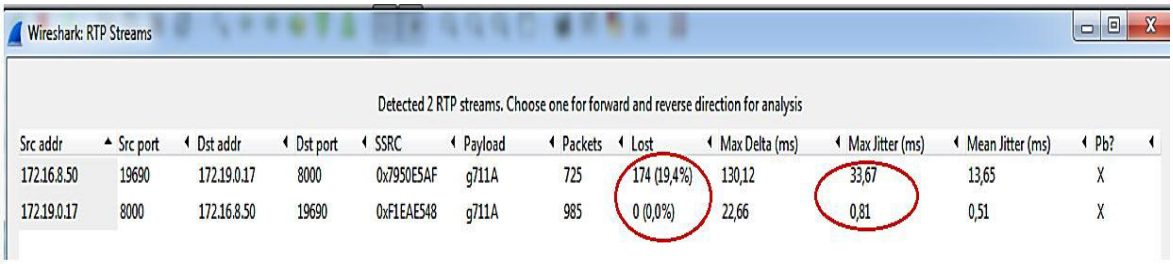


Figura 64. Parámetros VoIP con QoS

Fuente: WIRESHARK en host red topología de prueba

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

El Análisis en una red real nos permite identificar características que no siempre se pueden observar en las redes de pruebas aquí radica la importancia de la auditoria que es una forma de percibir el comportamiento real de una red.

Una vez configuradas las políticas de QoS se pudo notar claramente en la red de pruebas, el mejor rendimiento de la red, especialmente en una llamada telefónica en la cual se pudo visualizar mejores parámetros. Esto demuestra la funcionalidad de QoS para una red.

La implementación de políticas de QoS permite la disponibilidad de todos los servicios de la red, QoS hace posible que los usuarios accedan a los servicios de manera simultánea, percibiendo un funcionamiento óptimo de la red. Se logra realizar una llamada con VoIP, con buenos parámetros, mientras se utilizan servicios como descarga de archivos, correo, base de datos además de los servicios propios de la red como DNS y DHCP.

Basado en las características de la red y sus equipos se determinó que el modelo que mejor se adaptaba era 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.

Las políticas de QoS diseñadas y probadas en el presente trabajo poseen escalabilidad ya que no perderían su funcionalidad con el incremento de servicios y usuarios en la red,

permitiendo que las aplicaciones críticas (voz) y las más relevantes para la institución (base de datos), tengan asegurado su correcto funcionamiento.

RECOMENDACIONES

Al momento de la realización en GNS3 tomar en cuenta la compatibilidad en los sistemas operativos y software. En el desarrollo del trabajo, por ejemplo se encontró inconvenientes con el correcto funcionamiento del GNS3 en el Sistema Operativo Windows 8. Así mismo es importante la versión del VirtualBox a ser instalada.

La auditoría debe realizarse por un tiempo considerable en la red y utilizando varias herramientas para determinar veracidad en la información obtenida.

La clasificación de las aplicaciones debe realizarse bajo el requerimiento del administrador de la red, debido a que esto permitirá el funcionamiento óptimo de la red sin crear conflicto con los intereses institucionales. Cada institución es diferente, tiene sus objetivos, lineamientos de trabajo, servicios para usuarios internos y externos, al analizar estos factores conjuntamente con el requerimiento del administrador de la red es posible lograr la adecuada aplicación de políticas que permiten no solo un óptimo desempeño de los recursos tecnológicos sino también la consecución de los objetivos institucionales.

Para el caso de la simulación y en base al estado actual de la red, se realizó todo el proceso de implementación de políticas de Calidad de Servicio en el Switch de Core, sería importante realizarlo en switches de distribución. Se recomienda entonces un estudio de reingeniería para la red del GAD Municipal de Sam Miguel de Ibarra, el cual permita una

mejor distribución de la red y de esta manera a largo plazo se pueda implementar el modelo de QoS de manera óptima. Así como también considerar redundancia para el switch de core para asegurar el funcionamiento constante de la red.

BIBLIOGRAFÍA

LIBROS

Ariganello, E., & Barrientos Sevilla, E. (2010). *Redes Cisco: CCNP a fondo.* México: Alfaomega.

Braun, T., Diaz, M., Enríquez Gabeiras, J., & Staub, T. (2008). *End-to-End Quality of Service Over Heterogeneous Networks.* Berlin: Springer.

Evans, J., & Filsfils , C. (2007). *Deploying IP and MPLS QOS for Multiservice Networks.* San Francisco, EE.UU: Elsevier Inc.

Marchese, M. (2007). *QoS OVER HETEROGENEOUS NETWORKS.* Inglaterra: John Wiley & Sons Ltd.

DOCUMENTOS ELECTRÓNICOS

Verón Piquero, J. (2009). *PRÁCTICAS DE REDES* recuperado de http://es.scribd.com/doc/56742025/Practicas-de-Redes-Parte1

NTOP, recuperado de http://www.guia-ubuntu.com/index.php/Ntop

GUÍA DE REFERENCIA DE NMAP (PÁGINA DE MANUAL) recuperado de https://nmap.org/man/es/

NET TOOLS V5.0.70 PORTABLE, recuperado de http://www.fiuxy.net/programas-gratis/1124593-net-tools-v5-0-70-portable.html

EVALUACIÓN DE LA HERRAMIENTA GNS3 CON CONECTIVIDAD A ENRUTADORES REALES, 2010, Lisset Díaz Cervantes

CARACTERÍSTICAS DE VIRTUAL BOX, 2013 recuperado de http://virtualbox.es/caracteristicas/

IMPLEMENTACIÓN DE POLÍTICAS DE CALIDAD DEL SERVICIO (QOS) CON DSCP, 2013, recuperado de http://www.cisco.com/cisco/web/support/LA/102/1024/1024269_dscpvalues.html

COMPARACIÓN DE LOS COMANDOS BANDWIDTH Y PRIORITY DE UNA POLÍTICA DE CALIDAD DE SERVICIO (QoS), 2013, recuperado de http://www.cisco.com/cisco/web/support/LA/7/73/73466_priorityvsbw.html

QOS - CALIDAD DE SERVICIO - COMANDO MAX RESERVED BANDWITH, 2013, recuperado de https://supportforums.cisco.com/es/document/64796

CLASS-BASED WEIGHTED FAIR QUEUEING, recuperado de http://www.cisco. com/en/ US/docs/ios/12_0t/12_0t5/feature/guide/cbwfq.html

GUÍA DE ADMINISTRACIÓN DEL SISTEMA: SERVICIOS IP, 2010, Recuperado de https://docs.oracle.com/cd/E19957-01/820-2981/ipqos-intro-54/index.html

CISCO, (2014, abril 08) ENTERPRISE QOS SOLUTION REFERENCE NETWORK DESIGN GUIDE. Recuperado de: http://www.cisco.com/c/en/us/td/docs/solutions/ Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/QoSIntro.html,

QOS-CALIDAD DE SERVICIO PARA VOIP Recuperado de: http://elastixtech.com/qos-calidad-de-servicio-para-voip/

GLOSARIO DE TÉRMINOS

ACL: Lista de control de acceso, constituyen un mecanismo para determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido. Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición

IETF: Internet Engineering Task Force (Fuerza de Tareas de Ingeniería de Internet), Es un grupo de trabajo cuya misión es hacer que Internet funcione mejor mediante la producción de alta calidad, los documentos técnicos pertinentes que influyen en la manera como la gente de diseño, uso y gestión de la Internet.

MPLS Multiprotocol Label Switching, es un mecanismo de transporte de datos estándar Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.

HB Per Hop Behavior, Se refiere al comportamiento por salto definido para una determinada configuración.

RFC: Request for Comments (Petición De Comentarios), se refiere auna serie de publicaciones del grupo de trabajo de ingeniería de internet que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. y comentarios e ideas sobre los mismos.

RSVP Resource Reservation Protocol (Protocolo de reserva de recursos), es un protocolo de la capa de transporte diseñado para reservar recursos de una red bajo la arquitectura de servicios integrados (IntServ). RSVP reserva los canales o rutas en redes internet para la transmisión por unidifusión y multidifusión con escalabilidad y robustez.

SIP Session Initiation Protocol (Protocolo de Inicio de Sesiones) es un protocolo usado 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 que se realiza entre el cliente y proveedor, el cual permite determinar bajo q parámetros se medirá la calidad del servicio entregado.

RTP Real Time Transport Protocol (Protocolo de Transferencia en Tiempo Real), Este protocolo define un formato de paquete estándar para el envío de audio y video sobre Internet, está definido en el RFC1889. Utilizado principalmente en telefonía, aplicaciones de videoconferencias.

TCP Transmission Control Protocol (Protocolo de Control de Transmisión), es uno de los protocolos fundamentales en Internet, usado para crear "conexiones" entre computadores través de las cuales puede enviarse un flujo de datos. El 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.

UDP User Datagram Protoco (Protocolo de datagrama de usuario) es un protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 Modelo OSI). Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.

UIT-T: Unión Internacional de Telecomunicaciones, Sección Telecomunicaciones, con sede en Ginebra, es el órgano permanente de la Unión Internacional de Telecomunicaciones que estudia los aspectos técnicos, de explotación y tarifarios, y publica normativas sobre los mismos.

VLAN: virtual LAN (red de área local virtual) es un método para crear redes lógicas independientes dentro de una misma red física.1 Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red

FIFO (First IN-First OUT), el primero en entrar es el primero en salir, es algoritmo de encolamiento más elemental; los paquetes son enviados en el mismo orden en que llegan, sin tomar en cuenta la clase o prioridad únicamente su orden de llegada.

WFQ (Weighted Fair Queuing), este método de encolamiento se basa en un algoritmo que consiste en dividir el tráfico en flujos y, a estos flujos se les asigna un ancho de banda; los flujos con mayor prioridad tienen mayor ancho de banda y los de poco volumen son despachados más rápidamente.

CBWFQ (Class Based Weighted Fair Queuing), algoritmo de encolamiento que permite establecer clases manualmente; a cada clas e se le asignan características específicas como una cola, un peso y un ancho de banda mínimo.

CoS (Class of Service), Clase de Servicio, campo CoS de 3 bits, parte de los 4 bits añadidos a la cabecera Ethernet original por el estándar IEE 802.1Q , que permite establecer 8 niveles de prioridad como un mecanismo básico para marcar el tráfico.

DSCP (*Differentiated Services Code Point),* Punto de código de servicios diferenciados es un campo del paquete IP formado por 6 bits , el cual permite la asignación de distintos niveles de servicio al tráfico de red, mediante el marcado en el campo DSCP, con distintos valores de acuerdo a la clase de tráfico.

LLQ: Low-Latency Queuing, método de encolamiento usado para aplicaciones en tiempo real, permite definir una cola específica dedicada a aplicaciones en tiempo real (prioridad estricta).

QoS (Quality of Service), Calidad de Servicio, es un conjunto un conjunto de requisitos de servicios que permite a una red garantizar servicios a las aplicaciones.

ANEXOS

- **ANEXO 1:** Descripción de Principales Equipos
- **ANEXO 2**: Reportes Auditoria
- **ANEXO 3**: Reporte Mensual, Firewall Checkpoint GAD Ibarra
- **ANEXO 4**: Estadisticas Web GAD Ibarra
- **ANEXO 5**: Manual de Administrador
- **ANEXO 6:** Configuraciones Básicas y VLANS para la simulación
- **ANEXO 7:** Archivo de Configuración Activo del Switch de Core
- **ANEXO 8:** Archivo de Configuración Activo del Switch de Acceso
- **ANEXO 9:** Datasheet Switch Cisco Catalyst Serie 4500