TRABAJO ESPECIAL DE GRADO

DESARROLLO DE UNA ARQUITECTURA PARA SEPARAR Y PRIORIZAR EL TRÁFICO MEDULAR E INTERNO DE LA CORPORACIÓN DIGITEL

PROF. GUÍA:
Ing. David Sirit
TUTOR INDUSTRIAL:
Ing. Antonio Dávila

Presentado ante la Ilustre
Universidad Central de Venezuela
Por el Br. José Manuel Díaz Casique
Para optar al título de
Ingeniero Electricista

Caracas, octubre de 2009

CONSTANCIA DE APROBACIÓN

Caracas, octubre de 2009

Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Bachiller Jose Manuel Díaz Casique, titulado:

"DESARROLLO DE UNA ARQUITECTURA PARA SEPARAR Y PRIORIZAR EL TRÁFICO MEDULAR E INTERNO DE LA CORPORACIÓN DIGITEL"

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.

_____	_____
Prof.	Prof.
Jurado	Jurado
_____	_____
Prof. David Sirit	Ing. Antonio Dávila
Tutor académico	Tutor Industrial

DEDICATORIA

A Dios por darme la vida,
A mis padres Toguinarma Carlota y Víctor Enrique
por dedicar su vida al bienestar de sus tres hijos,
A mis hermanas Nailiud Verónica y Narvic Verónica
por siempre apoyarme y aconsejarme,
A mis sobrinos Ángelo Jesús y María Victoria
por llenar mi vida de mucha alegría y felicidad

AGRADECIMIENTOS

A mi tutor industrial, Ing. Antonio Dávila, por hacer de mi primera experiencia laboral una experiencia exitosa y llena de mucho aprendizaje. Siempre estaré altamente complacido y agradecido contigo porque fuiste mi primer jefe y fuiste la primera persona que me brindó la oportunidad y me abrió las puertas hacia el campo laboral.

A mi tutor académico, Prof. David Sirit, por sus precisos comentarios y consejos.

A María Auxiliadora Rojas, todo lo que rodea tu maravilloso trabajo funciona de buena manera. En gran medida gracias a tu excelente desempeño el departamento de Comunicaciones se mantiene en pie. ¡Eres la mejor secretaría de todas!

A todos los integrantes de la coordinación de Redes en la Corporación Digitel C.A. De manera especial quiero agradecer a las siguientes personas:

A Eneida Guzmán, por siempre estar dispuesta a apoyarme con tus valiosos comentarios y por ayudarme a desarrollar mi investigación gracias a tus grandes conocimientos de la red que maneja la Coordinación.

A Edgar Alecio, por brindarme tus conocimientos y apoyo en todo momento; a ti te atribuyo el gusto que le tomé al área de implementación por la experiencias laborales que tuve a tu lado. Pero sobre todo, te agradezco por hacerme entender que la experiencia profesional se gana y se construye con trabajo duro y muchas ganas.

A José Herrera, por tus comentarios y por aconsejarme a utilizar la herramienta de simulación GNS3, la cual fue de gran utilidad para el desarrollo de la parte final de esta investigación.

A mis compañeros pasantes Carlos Bolívar, Adeleine Sánchez, Jesús Avendaño y Juan Santiago.

Y por último. Gracias a todos los miembros de la gloriosa comunidad. Alex, Alexis, Andrés, Brunswick, Cristian, Fragachan, Gustavo, Jeanpaul, Jesús Montiel, Jesús Roldán, Karina, Leonardo, Philippe, Tony y Victor. Sin ustedes la vida dentro de la escuela no hubiera sido tan maravillosamente placentera.

Díaz Casique, José Manuel

DESARROLLO DE UNA ARQUITECTURA PARA SEPARAR Y PRIORIZAR EL TRÁFICO MEDULAR E INTERNO DE LA CORPORACIÓN DIGITEL

Título Académico a obtener: Ingeniero Electricista Mención Comunicaciones

Tutor Académico: Prof. David Sirit. Tutor Industrial: Ing. Antonio Dávila

Tesis. Caracas, U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica.

Año 2009, 104 páginas.

Palabras Claves: Calidad de Servicio, enrutamiento, priorización, clasificación, Ancho de Banda

RESUMEN

Actualmente el protocolo IP es usado por la mayoría de las redes. Su característica de envío no orientado a la conexión y de mejor esfuerzo ha resultado de manera exitosa, contribuyendo a su gran expansión. Sin embargo, las nuevas aplicaciones exigen mucho más de lo que IP puede ofrecer, como por ejemplo altos requerimientos de ancho de banda, necesidad de transmisión con bajo retardo y sin pérdidas. Para dar respuestas a estos requerimientos se han desarrollado varios mecanismos para dotar a las redes IP de Calidad de Servicio (Quality of Service, QoS). Uno de estos mecanismos y el más usado por las redes corporativas es la arquitectura de red basada en la Diferenciación de Servicios (Differentiated Services, DiffServ). Esta arquitectura permite hacer priorización de tráfico mediante la clasificación de los servicios, para posteriormente aplicar políticas de QoS dentro de un dominio establecido por el administrador de la red. Este es el marco de esta investigación, se realizó un estudio de la red IP de la Corporación Digitel C.A. que permitió plantear un modelo de red que segmenta los diferentes servicios que transporta la red, logrando de esta manera disponer de cantidades de ancho de banda exclusivo para las aplicaciones prioritarias. Se presenta en primer lugar la definición del problema, en segundo lugar se muestran las bases teóricas que permitieron desarrollar la arquitectura propuesta. En tercer lugar, se describe la red de estudio. Seguidamente se exponen los métodos para la obtención de los datos que permitieron hacer la priorización y clasificación del tráfico de las aplicaciones. Posteriormente, se presentan los resultados de la prueba realizada a modo de evaluar la configuración en los equipos de la red. Se cierra el documento con una sección de conclusiones y recomendaciones.

INDICE GENERAL

TABLA DE CONTENIDO

INDICE DE FIGURAS

INDICE DE GRÁFICOS

INDICE DE IMÁGENES

INDICE DE TABLAS

INTRODUCCIÓN

Actualmente IP es adoptado por la mayoría de las redes como su protocolo en capa de red. Su característica de envío no orientado a la conexión permite un traslado más rápido de los paquetes por las distintas rutas. Así mismo, IP es considerado un protocolo de mejor esfuerzo o no confiable. Esto significa que genera una menor sobrecarga en la red y se traduce directamente en menos demora en la entrega de los paquetes.

Todas estas bondades fueron diseñadas sin preveer el desarrollo vertiginoso de las aplicaciones actuales que gozan del uso de este protocolo. En otras palabras, las nuevas aplicaciones exigen mucho más de lo que IP puede ofrecer, como por ejemplo altos requerimientos de ancho de banda, necesidad de transmisión con bajo retardo y sin pérdidas.

Para dar respuestas a estos requerimientos, sin eliminar las funcionalidades descritas anteriormente, se han desarrollado varios mecanismos para dotar a las redes IP de Calidad de Servicio (Quality of Service, QoS). Uno de estos mecanismos y el más usado por las redes corporativas es la arquitectura de red basada en la Diferenciación de Servicios (Differentiated Services, DiffServ). Esta arquitectura permite crear distintas clases de servicio para hacer priorización de tráfico, y posteriormente aplicar políticas de QoS dentro de un dominio delimitado por el administrador de la red. Este es el marco de esta investigación. Se realizó un estudio de la red IP de la Corporación Digitel C.A. que permitió plantear un modelo de red que segmenta los diferentes servicios que transporta la red, logrando de esta manera disponer de cantidades de ancho de banda exclusivo para las aplicaciones prioritarias.

La investigación se subdivide en cinco capítulos. Cada uno trata los siguientes puntos:

Capítulo I: Se plantea, formula y se justifica el problema tratado en esta investigación. Se describen los objetivos, tanto el general como los específicos.

Capítulo II: Se muestran las bases teóricas que permitieron desarrollar la arquitectura propuesta.

Capítulo III: Se describe la infraestructura de la red de estudio, tato a nivel lógico como a nivel físico. Se presenta un informe que refleja el diagnóstico y la evaluación de los equipos para el soporte de las distintas políticas de QoS.

Capítulo IV: Se exponen los métodos que se utilizaron para la obtención de los datos que permitieron hacer la clasificación y priorización del tráfico de las aplicaciones.

Capítulo V: Se presentan los resultados de la prueba realizada bajo un ambiente de simulación, a modo de evaluar la configuración de los comandos necesarios en los equipos de la red.

Por último se presentan las conclusiones y recomendaciones, además de los anexos que complementan la información relacionada a los esquemas de red de la Corporación Digitel C.A.

CAPÍTULO I

1. DEFINICIÓN DEL PROBLEMA

1. DEFINICIÓN DEL PROBLEMA

1.1 Planteamiento del Problema

El tráfico de los servicios que transporta actualmente la red IP de la Corporación Digitel C.A. se encuentra en una situación delicada, donde existe el riesgo de eventuales intermitencias de las aplicaciones primordiales. Esto se convierte en una amenaza para lograr los objetivos de negocio que se ha planteado la Corporación Digitel C.A. y que se traducen en ofrecer servicios de calidad, de última tecnología y de mayores velocidades de transmisión, adaptados a las necesidades de los clientes.

El tráfico de los servicios se apoya en diferentes aplicaciones, cada una con una función específica. A fin de lograr la eficiencia operativa es primordial mantener en estado óptimo de funcionamiento estas aplicaciones. Entre las consideradas de alta importancia se pueden mencionar las siguientes:

Intranet Corporativa e Intranet de Ventas y Atención al Cliente: son portales WEB pertenecientes a la red interna de la Corporación Digitel C.A, las cuales alojan las aplicaciones WEB necesarias para atender las solicitudes de los clientes que se generan en los Centros de Atención. Entre las aplicaciones más importantes están: Siebel® (CRM), SIR, Administrador de aprovisionamiento Blackberry®, etc.

Oracle® Siebel® Customer Relationship Management (CRM): es una solución propiedad de la Corporación Oracle® que brinda a las empresas diseño, desarrollo y apoyo de gestión de relaciones con clientes. Este sistema debe mantener comunicación permanente con el sistema de facturación de servicios prepago y pospago para dar respuesta efectiva a los requerimientos del cliente.

SAP® R3®: Es un sistema integrado de gestión del tipo Planificación de Recursos Empresariales (Enterprise Resource Planning, ERP) propiedad de la empresa alemana SAP® que permite controlar los procesos que se llevan a cabo

en la empresa a través de los módulos Finanzas, Almacenes e Inventarios y Recursos Humanos.

El funcionamiento de estas aplicaciones esta vinculado a elementos de base de datos como el registro sobre las llamadas (Call Detail Record, CDR), estos registros son automáticamente generados cuando se inicia una llamada entre una estación móvil (Móvil Station, MS) y la estación base (Base Transceiver Station, BTS) y posteriormente archivados en distintos formatos. Estos reportes contienen información como el número de llamadas realizadas, la duración de las llamadas, el origen y destino de las llamadas y el costo generado de las mismas. La red IP de la Corporación es utilizada para el transporte de CDR a un punto central (Billing System) para su procesamiento. El sistema de facturación (Billing System) en telefonía móvil celular se encarga reunir la data desde los CDR para luego procesar la información según el plan del cliente y generar la facturación. Para clientes prepago y pospago, el proceso de facturación se hace de manera distinta.

Así mismo, es primordial dedicar una porción de ancho de banda a los servicios internos de la Corporación como Internet, Correo Electrónico y Files & Printers. Así como también a plataformas de gestión para la red.

Al hacer un estudio detallado de la situación actual de la red, tanto a nivel lógico como a nivel físico, es posible deducir algunas de las causas que originan este comportamiento inestable en la red IP de la Corporación.

En los últimos años la Corporación ha tenido un crecimiento sostenido y acelerado en el número de clientes, aumentando a su vez los servicios, lo cual implica mayor número de aplicaciones que deriva en aumento del número de enlaces. Para competir con los retos del mercado venezolano y mundial, Digitel se ha visto obligado a desarrollar nuevos servicios acordes a las necesidades de comunicación de los clientes, y mejorar la plataforma de red para cubrir las necesidades de ancho de banda y de velocidades de transmisión de estos nuevos servicios, como por ejemplo Internet 3G o el equivalente a su nombre comercial BAM (Banda Ancha Móvil).

Dado este incremento a nivel de clientes, la Corporación esta en proceso continuo de crecimiento interno en su cantidad de empleados. Todos los meses la empresa incorpora nuevo personal en las áreas requeridas para el desarrollo del negocio, aumentando la demanda de ancho de banda para los servicios internos antes mencionados.

Para dar respuesta a los requerimientos en el área de atención al cliente, Digitel incorporó un software propiedad de ORACLE bajo el concepto CRM llamado Siebel. Este paquete avanzado mejora la gestión de relaciones con los clientes, dando mayor soporte a los distintos Centros De Atención de la Corporación a nivel nacional.

Todo esto a su vez motivó de manera natural que la Corporación pensará en incorporar un sistema de Gestión de negocios que brindara acoplamiento y soluciones integradas para las funciones de la compañía, por lo que Digitel incorporó SAP, producto de tipo Enterprise Resource Planning (ERP). Este es un concepto de software donde se integra, sobre una misma base de datos, todas las herramientas funcionales para el manejo de una empresa: procesos de producción y manufactura, distribución, inventarios, controles financieros, administrativos, contables, de facturación y hasta la nómina de recursos humanos.

Al evidenciar el inminente aumento de tráfico, el problema real de la red actual de datos es que no se puede garantizar la calidad de servicio de estas aplicaciones primordiales para la Corporación, es por ello que los servicios críticos se ven afectados al estar los enlaces colapsados bajo el esquema central de la red actual, donde todas estas aplicaciones usan el mismo canal de transporte para el tráfico de datos, sin ningún tipo de priorización.

Al suponer que estas situaciones persisten y se acrecienten en un mediano plazo, las consecuencias serían muy negativas para la Corporación. La caída constante de estos servicios causaría, entre otras cosas, abandono inminente de clientes, disminución casi asegurada de nuevos clientes, estancamiento en el desarrollo de la empresa y mayor necesidad de dedicación por parte del personal

administrativo de la red IP de la Corporación para darle calidad de servicio al esquema actual de la red.

1.2 Formulación del Problema

Basados en el análisis previo, es necesario plantear las posibles maneras de atacar el problema. Se bosquejan diferentes alternativas que pueden acabar con la situación actual, como por ejemplo posibilitar una arquitectura que permita segmentar y priorizar la red de datos actual, tanto a nivel lógico (direccionamiento IP), así como a nivel físico (equipos de red, nuevos enlaces y/o nuevas tecnologías de transmisión). De la misma forma, se plantean interrogantes que ayudan a aclarar el planteamiento inicial, como por ejemplo: ¿Cuáles políticas de QoS (Calidad de Servicio) son las que mejor se adaptan a las necesidades de la red de la Corporación Digitel C.A.? ¿Será el protocolo MPLS (Multiprotocol Label Switching) la tecnología adecuada para segmentar los servicios de acuerdo a su requerimiento de ancho de banda y de velocidad de transmisión? ¿Se podrá segmentar la red a modo de obtener una Red exclusiva para el tráfico medular de los servicios y otra Red para los servicios internos corporativos y de gestión?

1.3 Objetivos General y Específicos

1.3.1 Objetivo General

Desarrollar una arquitectura para separar y priorizar el tráfico de datos medular e interno de la Corporación Digitel.

1.3.2 Objetivos Específicos

I. Levantar información de la arquitectura de red actual, tanto a nivel lógico como a nivel físico.

II. Dimensionar equipamiento, a nivel de fabricante y modelos, basados en la arquitectura propuesta y cantidad de enlaces.

III. Identificar el tráfico que transporta la red actual y clasificarlo según su tipo.

IV. Crear una matriz de servicios basados en el tipo de tráfico y aplicar los mecanismos de QoS más idóneos para la red.

V. Plantear el nuevo modelo de la red, tanto lógico como físico, para el soporte de lo establecido en función de los mecanismos aplicados.

VI. Evaluar la funcionalidad de la nueva arquitectura mediante la realización de pruebas bajo un esquema piloto.

1.4 Justificación e Importancia

Para lograr los objetivos de negocio de la Corporación es necesario mantener en alto nivel los estándares relacionados a la calidad de servicio y de esta manera lograr que los clientes se mantengan altamente satisfechos con el servicio por el cual están pagando.

Para cumplir estos objetivos se deben tomar en cuenta distintos factores, como por ejemplo el crecimiento acelerado en el número de clientes que la Corporación ha tenido en los últimos años.

Este crecimiento implica un aumento del tráfico, que trae como consecuencia una necesidad de optimizar periódicamente los enlaces de la red para mantener y mejorar aún más la calidad de los servicios que ofrece la Corporación a sus clientes. Optimizar el ancho de banda no es la única medida que debe tomarse, se necesita establecer prioridad en el tráfico y darle mayor solidez a la red ante las posibles fallas, en busca de que los principales servicios medulares permanezcan activos.

Es por ello que se debe dimensionar una nueva arquitectura basada en nuevas tecnologías de transmisión, que permita segmentar la red de datos actual, tanto a nivel lógico como a nivel físico, que brinde todos los beneficios de las políticas de QoS aplicadas a la red de la Corporación.

En Marzo del año 2005, Digitel en conjunto con HP realizaron un informe relacionado a un esquema de configuración piloto con el equipamiento existente de ese entonces para la implementación de QoS en el Core de la red IP.

Para esa época y como en la actualidad, el Core de Digitel TIM trabajaba en base al protocolo de enrutamiento Open Shortest Path First (OSPF). OSPF es un protocolo muy estable y confiable, este protocolo es capaz de manejar el tráfico de paquetes cambiándolos de un enlace a otro a su conveniencia, tomando en consideración diversas métricas. Por tal razón el orden de llegada de los paquetes al destino final no siempre es un correlativo, esto no representaba un problema para los paquetes de datos, pero si para los de voz. Por tal motivo la configuración elaborada por HP corregía este problema para el tráfico de VoIP. El objetivo principal que persiguió ese proyecto fue de buscar una configuración que lograra marcar el tráfico de voz, clasificarlo, aplicar políticas de marcado y enrutarlo a voluntad, dejando a OSPF la segunda opción en caso de que la opción principal falle.

Es importante crear un antecedente que sirva como documento referencial de estudio para futuras investigaciones relacionadas a implementar políticas de QoS en las redes. Uno de los fines que se quiere lograr a través de esta investigación es crear lineamientos que permitan escoger soluciones adecuadas a las necesidades puntuales de las redes, mediante la aplicación de las nuevas tecnologías soportadas por las redes IP. Así mismo, profundizar los conocimientos en políticas de QoS en redes, en la actualidad el tema de la priorización del tráfico es de suma importancia, debido a que asegura la disponibilidad de ancho de banda para las aplicaciones y recursos críticos de una empresa y de esta manera disponer de acceso permanente a las aplicaciones críticas.

1.5 Alcances y Limitaciones

Este proyecto pretende plantear el modelo de redes segmentadas en base a la priorización del tráfico de los servicios, queda por parte de la Corporación Digitel C.A. si se implementará la solución propuesta. La investigación se limitó a hacer pruebas que simularon el comportamiento de la red bajo la solución propuesta. El nivel de adecuación de la solución que se propone dependió en gran medida de la información que se logró recabar de parte de los empleados de la Corporación Digitel C.A. y de la documentación existente de la red actual.

Dentro de los planteamientos iniciales, se pretendía hacer el mismo estudio realizado en las redes de los Centros de Atención para las redes de usuarios Corporativos. Sin embargo, esto no se pudo efectuar debido a la ausencia de un equipo analizador de tramas para enlaces con velocidades de 2.048 Mbits/s que permite capturar tráfico en enlaces WAN de altas velocidades y alto volumen de tráfico.

CAPÍTULO II

2 MARCO TEÓRICO

2. MARCO TEÓRICO

2.1 Introducción

Este capítulo trata de manera precisa los conceptos relacionados con el ámbito de esta investigación. De esta forma, se lograron establecer definiciones que sirvieron de base para el desarrollo de este trabajo de investigación.

En primer lugar se desarrollan los conceptos enmarcados dentro de la capa 3 del modelo OSI o capa de Red, la cual centra la mayor atención de esta investigación. Enseguida, se habla acerca del significado de Calidad de Servicio (QoS) y de los mecanismos para aplicar QoS en redes IP. Posteriormente, se comenta sobre los acuerdos en los niveles de servicio y las métricas usadas para estimar estos acuerdos. Por último, se expone la arquitectura de servicios diferenciados o DiffServ, ampliamente usada para priorizar y segmentar tráfico en redes corporativas.

2.2 Protocolos de Redes TCP/IP

2.2.1 El modelo OSI

Inicialmente, el modelo OSI fue diseñado por la Organización Internacional para la Estandarización (ISO, International Organization for Standardization) para proporcionar un marco sobre el cual crear una suite de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizara para desarrollar una red internacional que no dependiera de sistemas propietarios.

El atributo principal del modelo OSI es como este procesa el mensaje desde que sale del emisor hasta que es recibido por el destinatario. El mensaje es procesado por cada uno de los protocolos que interactúan en cada capa, estos

protocolos trabajan en conjunto para asegurar que ambas partes reciban y entiendan los mensajes.

El modelo OSI se compone de 7 capas; describe la interacción de cada capa con las capas directamente por encima y por debajo de él.

Figura 2.2.1 El modelo OSI de 7 capas

2.2.2 La Capa de Red o Capa 3

"Los protocolos de la capa de Red del modelo OSI especifican el direccionamiento y los procesos que permiten que los datos de la capa de Transporte sean empaquetados y transportados. La encapsulación de la capa de Red permite que su contenido pase al destino dentro de una red o sobre otra red con una carga mínima.**"**[1]

La capa de red trabaja en base a cuatro procesos básicos:

[1] CISCO ©, Cisco Networking Academy, Software Aplication Exploration Módulo 1, Capítulo 5.0.1, p. 1

- Direccionamiento: Primeramente, los dispositivos finales deben estar identificados con direcciones, la capa de red opera de forma que los dispositivos intermediarios que se encargan de enrutar los paquetes elijen la mejor vía para que el paquete llegue a su destino de forma rápida y eficiente mediante el procesamiento de estas direcciones. El mecanismo de direccionamiento más usado actualmente es IPv4.

- Encapsulamiento: Todo el datagrama que compone el mensaje que viaja a través de la red se constituye de Partes de Datagrama del Usuario (PDU). Cada capa del modelo OSI tiene su PDU específico. En capa 3, estos PDU se denominan paquetes IP. Los dispositivos de capa 3 reciben los PDU provenientes de capa 4 y se encargan de encapsular el paquete IP agregándole un encabezado que contiene, entre otras cosas, dirección de origen y dirección de destino. Una vez realizado el proceso de encapsulamiento, el PDU de capa 3 esta listo para ser recibido por la capa 2 o capa de enlace.

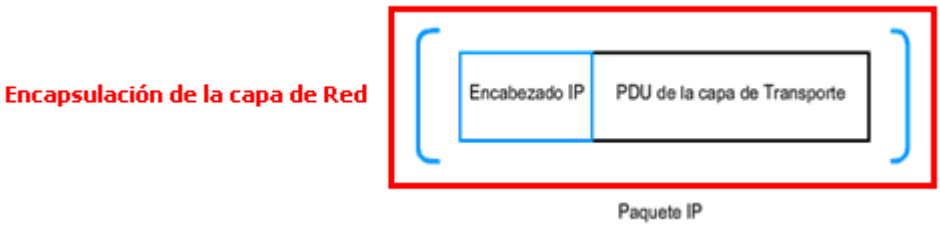


Figura 2.2.2.1 PDU de la capa 3: el Paquete IP

- Enrutamiento: Luego, cada paquete que es enviado debe ser guiado a través del tráfico de la red para alcanzar su destino final. Los dispositivos que se encargan de guiar estos paquetes por las rutas más idóneas son los routers y el proceso de seleccionar las rutas y dirigir el paquete a través de la red se denomina enrutamiento. A medida que el paquete es procesado por los enrutadores de la red, el contenido de la PDU de capa 4 permanece intacto hasta que alcanza el dispositivo final.

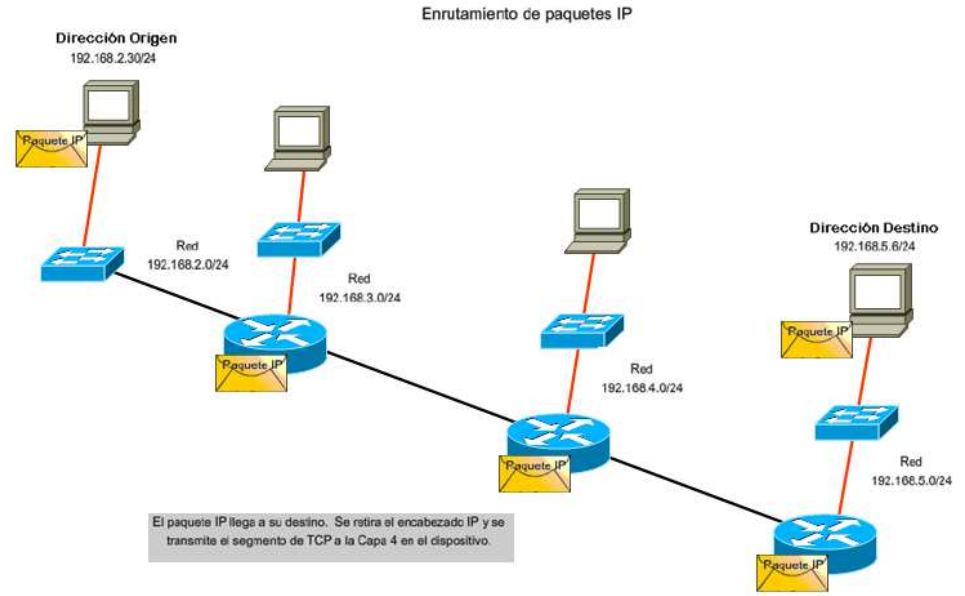


Figura 2.2.2.2 Enrutamiento de Paquetes IP

- Desencapsulamiento: Finalmente, el paquete llega al destino y es procesado en capa 3. El destino verifica en el encabezado del paquete que la dirección destino coincida con la suya. De ser así, el paquete es desencapsulado por parte de capa 3 y la PDU de capa 4 es procesada y trasladada al servicio apropiado en la capa de transporte.

"A diferencia de la capa de Transporte (Capa 4 de OSI), que administra el transporte de datos entre los procesos que se ejecutan en cada dispositivo final, los protocolos especifican la estructura y el procesamiento del paquete utilizado para llevar los datos desde un dispositivo hasta otro dispositivo. Operar ignorando los datos de aplicación llevados en cada paquete permite a la capa de Red llevar paquetes para múltiples tipos de comunicaciones entre dispositivos múltiples." [2]

[2] Ibídem, Capítulo 5.1.1, p. 1

2.3 El Protocolo IP

2.3.1 Definición

Los servicios de capa 3 que son implementados por el conjunto de protocolos TCP/IP conforman el protocolo de Internet (IP). Este es el único protocolo de capa 3 y se utiliza para llevar los datos de usuario a través de Internet. En la actualidad la versión más utilizada es la versión 4 o IPv4.

El protocolo de Internet fue diseñado como un protocolo de bajo costo. Es decir, fue diseñado para proveer solo las funciones necesarias para enviar un paquete desde el origen al destino a través de una red de dispositivos de datos interconectados entre sí. Esto significa que el protocolo no tiene la capacidad para rastrear ni administrar el flujo de paquetes, de estas funciones se encargan los protocolos en capas superiores.

Este modelo **no orientado a la conexión** ("no requiere un intercambio inicial de información de control para establecer una conexión de extremo a extremo antes de que los paquetes sean enviados […]"[3]) permite un traslado más rápido de los paquetes por las distintas rutas, ya que los routers leen solo en el encabezado la información para luego buscar en sus tablas de enrutamiento y, en base a una métrica en particular, decidir cual es la mejor ruta.

Sin embargo, la entrega de paquetes en un modelo no orientado a la conexión puede hacer que no lleguen a destino o lleguen fuera de secuencia. Si los paquetes están dañados o perdidos entonces crean inconvenientes para la aplicación que les da uso a los datos, es función de los servicios de capas superiores encargarse de solventar este tipo de situaciones. [4]

[3] Ibídem, Capítulo 5.1.3, p. 1
[4] Ídem

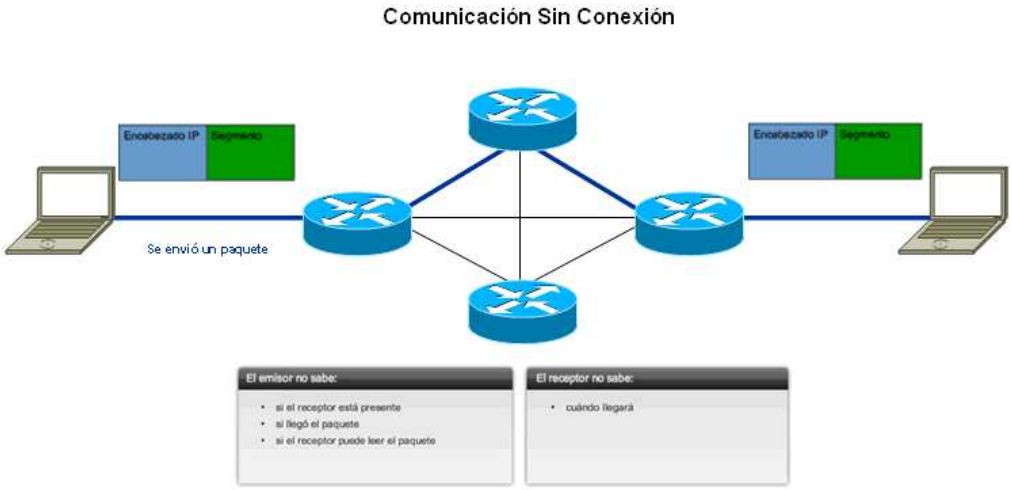


Figura 2.3.1.1 Envió de paquetes en un protocolo no orientado a la conexión

Así mismo, IP es considerado un protocolo de ***mejor esfuerzo*** o no confiable. Esto significa que genera una menor sobrecarga en la red y se traduce directamente en menos demora en la entrega de los paquetes. La función de la Capa 3 es transportar los paquetes entre los dispositivos finales tratando de colocar la menor carga posible. La Capa 3 no advierte el tipo de comunicación contenida dentro de un paquete. Esta responsabilidad es función de las capas superiores a medida que se requiera. Las capas superiores pueden decidir si la comunicación entre servicios necesita confiabilidad y si esta comunicación puede tolerar la sobrecarga que la confiabilidad requiere. [5]

"[…] Si se incluye la sobrecarga de confiabilidad en el protocolo de la Capa 3, las comunicaciones que no requieren conexiones o confiabilidad se cargarían con el consumo de ancho de banda y la demora producida por esta sobrecarga […] dejar la decisión de confiabilidad a la capa de Transporte hace que IP sea más adaptable y se adecue según los diferentes tipos de comunicación." [6]

[5] Ibídem, Capítulo 5.1.4, p. 1
[6] Ídem

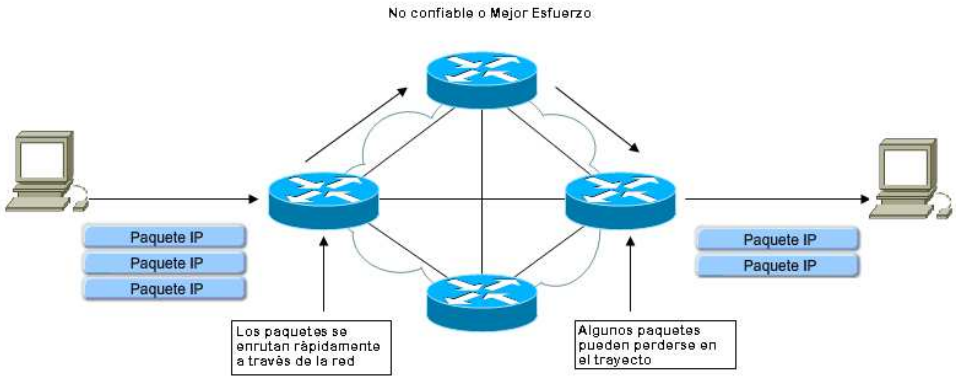


Figura 2.3.1.2 IP como protocolo No confiable o de Mejor Esfuerzo

Por otro lado, el protocolo IP es independiente del medio de transmisión usado para enviar los paquetes. Cualquier paquete IP puede ser comunicado eléctricamente por cable, como señales ópticas por fibra, o sin cables a través de señales de radio. La capa 2 o capa de Enlace de datos del modelo OSI es la que se encarga de tomar un paquete IP y prepararlo para transmitirlo por el medio de comunicación. Esto significa que el transporte de paquetes IP no está limitado a un medio en particular.

"En algunos casos, un dispositivo intermediario, generalmente un router, necesitará separar un paquete cuando se lo envía desde un medio a otro medio con una Unidad Máxima de Transmisión más pequeña. A este proceso se le denomina fragmentación de paquetes o fragmentación."[7]

[7] Ibídem, Capítulo 5.1.5, p. 1

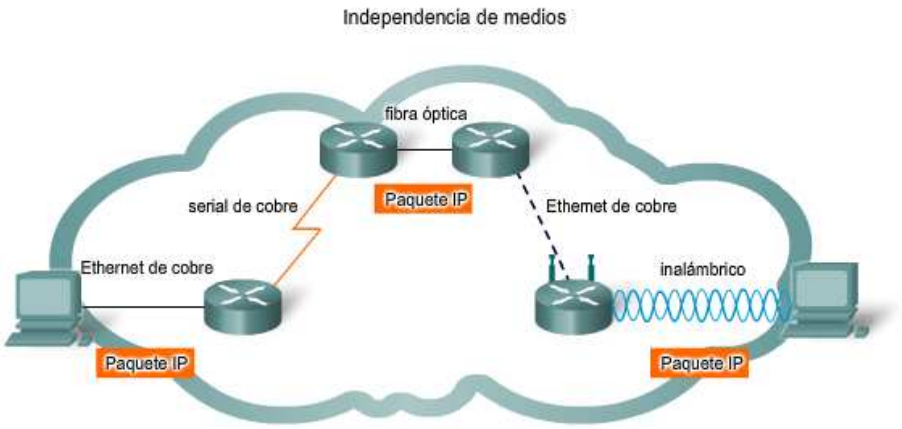


Figura 2.3.1.3 Independencia de medios de IP

En resumen, el protocolo IP se basa en 3 características esenciales:

- Sin conexión: No establece conexión antes de enviar los paquetes de datos.
- Mejor esfuerzo o no confiable: No se usan encabezados para garantizar la entrega de paquetes.
- Medios independientes: Operan independientemente del medio que lleva los datos.

2.3.2 Arquitectura del paquete IP

El protocolo IPv4 define muchos campos diferentes en el encabezado del paquete. Estos campos contienen valores binarios que los servicios IPv4 toman como referencia a medida que envían los paquetes a través de la red. Existen 6 campos claves en el encabezado dentro de un paquete IP[8]. Estos son:

1) Dirección IP destino: Este campo contiene un valor binario de 32 bits que representa la dirección de capa de red de destino del paquete.
2) Dirección IP origen: Este campo contiene un valor binario de 32 bits que representa la dirección de capa de red de origen del paquete.

[8] Ibídem, Capítulo 5.1.7, pp. 1, 2, 3

3) Tiempo de vida: El tiempo de vida (TTL) es un valor binario de 8 bits que indica el tiempo remanente de "vida" del paquete. El valor TTL disminuye al menos en uno cada vez que el paquete es procesado por un router. Cuando el valor se vuelve cero, el enrutador descarta el paquete y es eliminado del flujo de datos de la red. Este mecanismo evita que los paquetes se queden permanentemente en la red, evitando la congestión.
4) Protocolo: Este valor binario de 8 bits indica el tipo de relleno de carga que el paquete traslada. El campo de protocolo permite a la Capa de red pasar los datos al protocolo apropiado de la capa superior. Los valores de ejemplo son:

   01 para ICMP

   06 para TCP

   17 para UDP
5) Tipo de servicio: El campo de tipo de servicio contiene un valor binario de 8 bits que se usa para determinar la prioridad de cada paquete. Este valor permite aplicar mecanismos de Calidad del Servicio (QoS) a paquetes de alta prioridad, como aquellos que llevan datos de voz en telefonía. El enrutador que procesa los paquetes puede ser configurado para decidir qué paquete es enviado primero basado en el valor del Tipo de servicio.
6) Desplazamiento de fragmentos: Un router puede tener que fragmentar un paquete cuando lo envía desde un medio a otro medio que tiene una Unidad Máxima de transferencia más pequeña. Cuando se produce una fragmentación, el paquete IPv4 utiliza el campo Desplazamiento de fragmento y el señalizador Más Fragmentos en el encabezado IP para reconstruir el paquete cuando llega al destino. El campo de desplazamiento del fragmento identifica el orden en el cual ubicar el fragmento del paquete en la reconstrucción.

A manera de ejemplo, a continuación se visualiza un paquete IP con valores típicos en los campos que conforman el encabezado del paquete, esto para lograr un mejor entendimiento del tema en cuestión.[9]

[9] Ídem

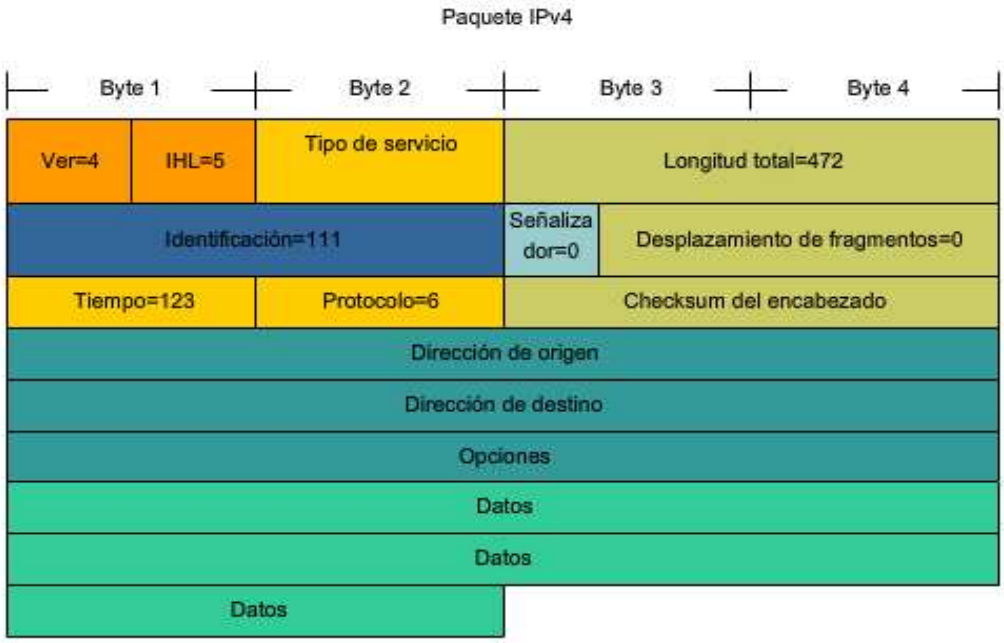


Figura 2.3.2.1 Paquete IPv4 típico

2.4 QoS en redes IP

2.4.1 Definición de QoS

El tema de la Calidad de Servicio en redes IP nace en función de la característica de "mejor esfuerzo" o "no confiable" con la cual fue diseñada la red IP, donde los paquetes no tienen garantía de alcanzar su destino. Surgió la necesidad de tratar de mejorar este aspecto en los nodos de la red donde se encuentran los routers que encaminan los paquetes a través de la red, siempre manteniendo el esquema de mejor esfuerzo que reduce el consumo de ancho de banda en el tráfico de los paquetes a nivel de capa 3. Cuando ocurre congestión en los nodos, se crean retardos, los paquetes se pierden o se agota su tiempo de vida y automáticamente tienen que ser desechados. En conclusión, se pierde información.

"Las funciones de QoS en IP están destinadas a garantizar entrega, así como diferentes servicios de Internet, otorgando los recursos de la red y el control

de uso al administrador de la red. QoS es un conjunto de requisitos de servicio que debe cumplir la red que transporta del flujo de datos. QoS ofrece garantía de servicio de extremo a extremo y medidas de rendimiento de una red IP mediante políticas basadas en el control de tráfico, tales como la asignación de recursos, de conmutación, enrutamiento, programas para paquetes, y mecanismos para desechar paquetes". [10]

Los siguientes son algunos beneficios principales de QoS en redes IP: [11]

- Permite a las redes soportar los requerimientos de servicios y aplicaciones multimedia, tanto existentes como las emergentes.
- Da al administrador de red control sobre los recursos y su utilización.
- Provee servicios garantizados y diferenciación de tráfico a lo largo de toda la red.
- Permite a los proveedores ofrecer servicios premium mediante la presente modalidad de "mejor esfuerzo". El proveedor puede clasificar los servicios que ofrece y configurar la red para diferenciar el tráfico en base a esta clasificación.
- Desempeña un papel esencial en las nuevas ofertas de servicios de red, tales como redes privadas virtuales (Virtual Private Network, VPN).

Emplear mecanismos de QoS en las redes IP actuales permite asegurar que las aplicaciones y recurso críticos de una organización reciban una cantidad garantizada de ancho de banda disponible en la red para su funcionamiento. Cada organización tiene necesidades distintas en cuanto a prioridad del tráfico de sus servicios. Por lo que aplicar QoS en las redes no es un proceso único, sino más bien dinámico el cual debe adecuarse a las necesidades particulares de la organización.

[10] SRINIVAS, Vegesna, IP Quality of Service, Cisco Press, 2001, p. 9
[11] Ídem

Para ubicarlo en un contexto, se supone un escenario muy frecuente en las redes actuales donde ciertos servicios de uso regular dentro de una organización, pero de menos prioridad o jerarquía (como correos con pesados anexos, largas colas de impresión, tráfico para efectuar respaldos y la copia, movimiento o transferencia de archivos) causan retraso y congestión en las redes provocando el colapso o inhabilitación de aplicaciones críticas, como servicios de cobro y facturación. Esto se puede evitar aplicando mecanismos de QoS en la red.

"En organizaciones grandes con oficinas remotas la priorización del tráfico WAN es crítica. Los enlaces WAN son costosos y muy limitados en ancho de banda. Muchas aplicaciones críticas como ERP, voz sobre IP, servidores remotos de aplicaciones, consultas a información crítica, etc., requieren de anchos de banda definidos y garantizados. Sin una priorización de los servicios y una repartición adecuada del ancho de banda estos servicios colapsan y los tiempos muertos o fuera de servicio son cada vez mas frecuentes e interminables […] Utilizando servicios QoS el ancho de banda de la red se puede garantizar para los servicios esenciales durante los períodos de alta congestión. Utilizando esquemas de priorización de tráfico que se modifiquen en el tiempo se logra una mejor administración y uso de los recursos de ancho de banda limitados."[12]

[12] Opalsoft.net, Página de OpalSoft creadora de software administrativo, http://www.opalsoft.net/qos/Spanish-QOS.htm, consultado el martes 9 de junio de 2009, 9:23 a.m.

2.4.2 Niveles de Acuerdo de Servicio (SLA) y Niveles de Acuerdos Operativos (OLA)

La calidad del tráfico de los servicios de los cuales se encarga la capa 3 es medida a través de métricas. Estas métricas contribuyen a definir los Niveles de Acuerdos de Servicio (Service Level Agreement, SLA), los cuales permiten llegar a un entendimiento sobre servicios, prioridades, responsabilidades y garantías entre el prestador de los servicios y sus clientes. Es importante establecer para cada servicio un mecanismo que contenga bien definidos los niveles de disponibilidad, servicio, rendimiento u otros atributos del servicio.

Cuando las empresas buscan asegurar estas métricas dentro de su misma organización, se habla de definir los Niveles de Acuerdos Operativos (Operating Level Agreement, OLA). Estos niveles se apoyan sobre los SLA para definir las necesidades de los niveles en los servicios internos.

"Calidad de servicio [...] implica un compromiso contractual (SLA) para garantizar la calidad de estas métricas [...]"[13]

Estos SLA representan un contrato para la prestación del servicio. Las pautas de cada SLA vienen dadas por los requerimientos de las aplicaciones que soporta el servicio en cuestión. Los usuarios del servicio dependen de este contrato para garantizar el funcionamiento de las solicitudes críticas para su negocio. Por lo tanto, al momento de definir los SLA se establece como será el transporte del servicio en la red IP en base al cumplimiento de las métricas definidas para ese servicio en particular.[14]

[13] EVANS, John, Deploying IP and MPLS QoS for Multiservice Networks, The Morgan Kaufmann Publishers, 2007, p. 2
[14] Ibídem, p. 1

2.4.2.1 Métricas SLA

Las métricas más importantes para evaluar el desempeño de los servicios en una red IP son las siguientes:

1) Retardo:

El retardo total de un paquete, o latencia, en cada salto se divide a su vez en retardo de serialización, retardo de propagación y retardo de conmutación.

- Retardo de serialización: es el tiempo que toma un dispositivo en transmitir un paquete en la velocidad de salida otorgada. Es decir, esta relacionado directamente con la tasa del reloj de transmisión. Depende del ancho de banda del enlace así como del tamaño del paquete a transmitir. Este retardo es proporcional al tamaño del paquete e inversamente proporcional al ancho de banda del enlace. [15]

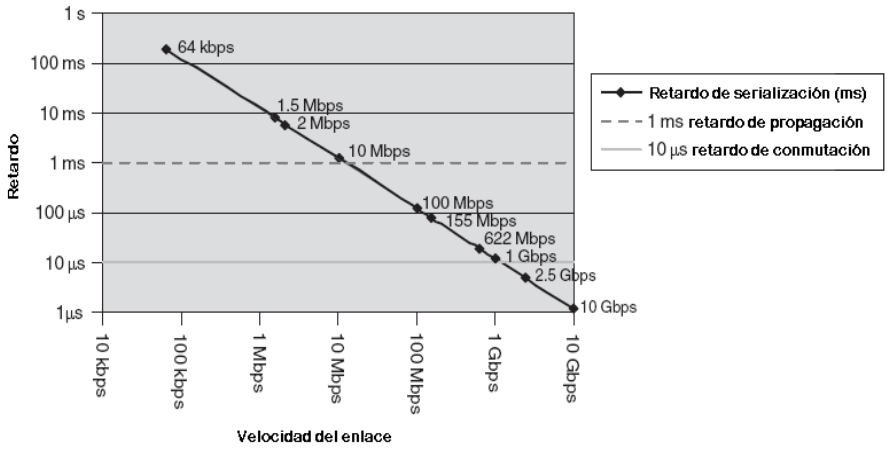


Figura 2.4.2.1 Retardo de serialización para un paquete de 1500 bytes

Por ejemplo, un paquete de 64 bytes a una velocidad de transmisión de 3 Mbps toma un tiempo de 0.171 ms en transmitirse. Es importante notar que este retardo depende del ancho de banda: el mismo paquete de 64 bytes en un enlace a 19.2 kbps tarda 26 ms. Evidentemente este

[15] Ibídem, p. 7

retardo es significativo en enlaces de bajas velocidades de transmisión. Este retardo también se conoce como retardo de transmisión.[16]

- Retardo de Propagación: Es el tiempo que toma un bit transmitido en un enlace para ir desde el puerto de salida de un router hasta el siguiente salto o puerto de entrada del siguiente router. Este retardo es significativo y es función de la distancia y del medio, más no del ancho de banda. Para enlaces WAN, los retardos de propagación en el orden de los milisegundos se consideran normales. En enlaces de cables coaxiales los retardos de propagación son de 4 ms por cada 1000 km, mientras que en los enlaces de fibra óptica son de 5 ms por cada 1000 km. [17]
- Retardo de Conmutación: Es el tiempo que tarda un router en empezar a transmitir un paquete después que lo recibió. Este tipo de retardo en routers de alto rendimiento generalmente puede ser considerado despreciable: para routers pertenecientes al Backbone de la red, donde el proceso de conmutación es típicamente implementado en el hardware, el retardo de conmutación esta en el orden de los 10-20 μs. Por otro lado, en routers basados en implementaciones de software, el valor de retardo de conmutación aumenta considerablemente a 2-3 ms.[18]

Todos los paquetes de un torrente no experimentan el mismo retardo, esto más bien depende de las condiciones transitorias de la red. Si la red no esta congestionada, no se formarán colas de paquetes en los enrutadores, y se reducen al mínimo los retardos de serialización y propagación, bajo estas condiciones la red sufre el menor retardo total posible. En cambio, si la red esta congestionada, se formarán colas de paquetes en los routers que influirán sobre los enlaces extremo a extremo y contribuirán a la variación del retardo entre los paquetes que estén bajo las misma conexión.

La figura 2.4.3.1 ilustra el impacto de los tres tipos de retardos anteriormente mencionados a medida que aumenta la velocidad de

[16] SRINIVAS, Op. cit., p. 12
[17] EVANS, Op. cit., p. 5
[18] Ibídem, p. 6

transmisión de un enlace. Es importante destacar como el retardo de serialización se reduce al mínimo comparado con el retardo de propagación a medida que se incrementa el ancho de banda del enlace.

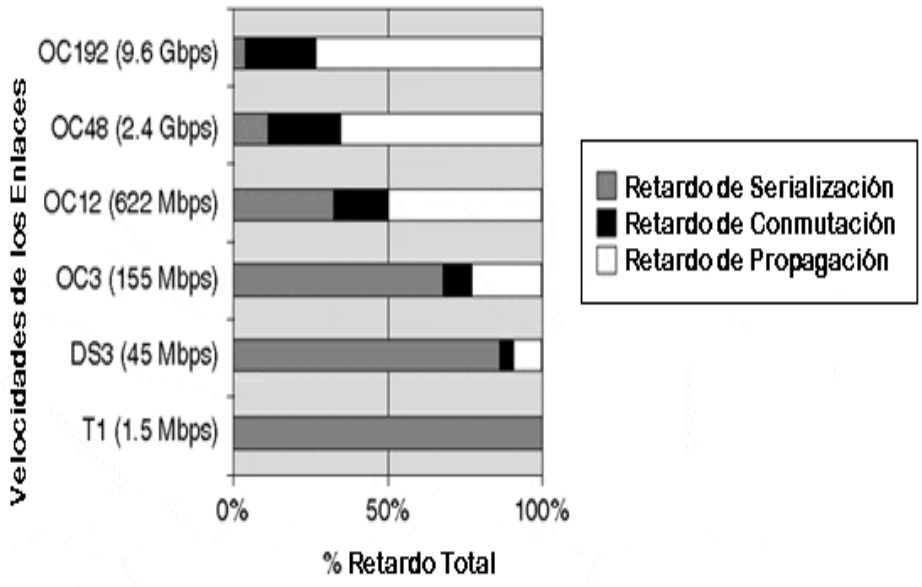


Figura 2.4.2.2 Impacto de los 3 tipos de retardo a medida que se incrementa la velocidad de transmisión de un enlace

2) Variación de Retardo o Jitter

El jitter caracteriza la variación en el retardo de la red. Generalmente se considera el jitter en la variación de un solo sentido de dos paquetes consecutivos, tal y como lo define la IETF [RFC3393]. En la práctica, sin embargo, las fluctuaciones pueden medirse también según la variación del retardo con respecto a alguna referencia o métrica particular, como puede ser el retardo promedio o el retardo mínimo. Es fundamental hacer notar que el jitter se relaciona con la variación del retardo en un solo sentido, la noción de jitter de ida y vuelta no tiene sentido.

El jitter es importante porque estima el retardo máximo entre paquetes recibidos contra el retardo de un paquete individual; y es causado por

variaciones de los tres componentes del retardo total mencionados en el apartado anterior.

Algunas aplicaciones, como aquellas soportadas por el protocolo TCP, no sufren de jitter. Aquellas aplicaciones que si lo sufren usan *buffers dejitter* para eliminar la variación de retardo mediante técnicas que convierten retardos fluctuantes en retardos constantes.

3) Pérdida de Paquetes

La pérdida de paquetes especifica el número de paquetes que se pierden durante una transmisión. Los paquetes que son descartados en una red congestionada y los paquetes dañados causan la pérdida de paquetes. El descarte de paquetes generalmente ocurre en los puntos de congestión, cuando los paquetes entrantes exceden por lejos el tamaño de cola permitida para colocarlos en la cola de salida del enrutador. También ocurre cuando no hay suficientes buffers en la entrada para el arribo de paquetes. La pérdida de paquetes se define como una fracción de los paquetes perdidos mientras se transmite un cierto número de paquetes en algunos intervalos de tiempo.

La métrica para medir la pérdida de paquetes ha sido definida en un solo sentido por la IETF mediante la norma [RFC2680]. Es medida en un solo sentido debido a que puede haber diferentes características entre la ruta desde el origen al destino y la ruta desde el destino al origen.

Además de medir la tasa de paquetes perdidos, en algunas aplicaciones se utiliza un patrón de pérdidas como parámetro clave que ayuda a medir el desempeño de la aplicación en los usuarios finales[19]. La norma [RFC3357] introduce una métrica adicional que describe el patrón de pérdidas:

- "Período de pérdidas" define la frecuencia y la duración de la pérdida una vez que esta empieza.
- "Distancia de pérdidas" define el espacio entre los períodos de pérdidas.

La pérdida de paquetes puede ser causada por diferentes razones:

[19] Ibídem, p. 9

- Congestión: cuando ocurre congestión, se forman colas y los paquetes son desechados. Las pérdidas durante una congestión se controlan mediante técnicas apropiadas para el manejo de tráfico entrante en los routers.
- Errores en capas inferiores: errores de los bits en la capa física, causados por ruido o atenuación en el canal de transmisión, pueden causar la pérdida de paquetes. Esta falla se puede detectar mediante un mecanismo denominado Chequeo de Redundancia Cíclica (Cyclic Redundancy Check, CRC), el cual trabaja desechando tramas enteras si los bits chequeados en la trama presentan un cheksum incorrecto. El CRC es utilizado en la mayoría de las tecnologías en capa de enlace y protocolos de transote IP.[20]
- Fallas de elementos de red: fallas en algunos elementos de la red pueden causar la pérdida de paquetes hasta que la conectividad entre los dispositivos con fallas sea restablecida. Inclusive si existen rutas alternas para el reenvío de paquetes, la pérdida de paquetes puede ocurrir. El período de pérdida resultante depende de las tecnologías de red que se utilizan. En redes bien diseñadas, la convergencia del protocolo de enrutamiento interior de puerta de enlace (Interior Gateway Routing Protocol, IGP) dura algunos cientos de milisegundos. [21]
- Pérdidas en las aplicaciones de usuario final: esto puede ocurrir durante exceso o carencia de flujo entrante en el buffer receptor. Cuando ocurre un arribo masivo de paquetes el buffer de entrada es incapaz de formar colas que permitan la recepción de todos los paquetes, lo cual puede afectar potencialmente toda clase de aplicaciones. Si por el contrario el buffer esta vacío porque no llegan paquetes, aplicaciones en tiempo real como VoIP o video se ven afectadas por este comportamiento.

[20] Ibídem, pp. 9, 10

[21] PIERRE, Francois, Achieving subsecond IGP convergence in large IP networks, ACM SIGCOMM Computer Communication Review, 2005, pp. 35–44

4) Ancho de Banda

Los servicios IP son comúnmente vendidos con un "ancho de banda" definido, cuando en realidad el ancho de banda a menudo refleja la capacidad del enlace en capa 2 para soportar el servicio; sin embargo, cuando es usado en el contexto de *networking* el término de "ancho de banda" puede adoptar diferentes significados respecto a la capacidad de un enlace, red o servicio para transportar tráfico de datos.

El término ancho de banda es usado para describir la capacidad de procesamiento de un medio, protocolo o conexión en particular. El ancho de banda describe "el tamaño del tubo" requerido por la aplicación para enviar el caudal de datos a través de al red. Generalmente, una conexión que requiere garantía de servicio tiene ciertos requisitos de ancho de banda y requiere asignación por parte de la red de un ancho de banda mínimo especial para la conexión. Como por ejemplo la voz digitalizada, que produce voz a 64 kbps, esta aplicación se convierte en inservible si llega a transmitirse a una velocidad menor a 64 kbps a lo largo de la ruta de conexión.[22]

2.4.3 Modelos de servicio QoS

El tráfico de una red es creado mediante flujos originados a partir de una variedad de aplicaciones en los dispositivos finales. Estas aplicaciones difieren en su tipo de servicio y requisitos de funcionamiento. Cualquier requerimiento de flujo en la red depende de la aplicación a la cual pertenece. Por lo tanto, entender y analizar los tipos de aplicaciones existentes es clave para comprender las diferentes necesidades de servicio para establecer el comportamiento de los flujos dentro de una red.

Un modelo de servicio, también llamado nivel de servicio, describe las características y beneficios que puede ofrecer QoS extremo a extremo. QoS

[22] SRINIVAS, Op. cit., p. 12

extremo a extremo se refiere a la habilidad que tiene la red para entregar los servicios requeridos por un tráfico específico de un extremo de la red a otro. Los diferentes modelos que se describen a continuación se adaptan al tipo de aplicación, como por ejemplo aplicaciones en tiempo real, transferencia de archivos o correo electrónico.

La capacidad de la red para ofrecer servicios específicos, que son críticos para algunas de las aplicaciones, con algún nivel de control sobre las medidas de rendimiento (es decir, el ancho de banda, retraso o el jitter, y pérdidas) es categorizada en tres modelos de servicio: [23]

1) Servicio de Mejor Esfuerzo: Conectividad básica sin ninguna garantía de entrega de paquetes al destino, aunque normalmente un paquete solo es desechado cuando las colas de paquetes en los routers son excesivamente grandes. El servicio de mejor esfuerzo no es realmente parte de QoS, ya que no garantiza la entrega. Sin embargo, la mayoría de aplicaciones de datos, tales como Protocolo de Transferencia de Archivos (FTP), funcionan correctamente con el servicio de mejor esfuerzo, aunque con rendimiento degradado. Para funcionar bien, todas las aplicaciones requieren ciertas asignaciones de recursos de red en términos de ancho de banda, retraso, y mínima pérdida de paquetes.

2) Servicio Diferenciado: El tráfico se agrupa en clases en base a sus requisitos de servicio. Cada servicio se diferencia en la red de acuerdo a mecanismos de QoS que son configurados para cada clase de servicio. Es importante tener en cuenta que este tipo de servicio no da garantías en sí. Más bien, la diferenciación de tráfico lo que permite es un trato preferencial de una clase sobre otras. Este esquema de QoS trabaja mejor en aplicaciones de consumo intenso de ancho de banda. Es importante que el tráfico de control se diferencie del resto del tráfico prioritario, a fin de garantizar la conectividad básica de la red todo el tiempo.

[23] SRINIVAS, Op. cit., pp. 9, 10

3) Servicio Garantizado: Este servicio requiere reservación de algunos recursos de la red para asegurar que se cumplan con los requisitos de servicio. El servicio garantizado requiere previa reserva de los recursos en los caminos de conexión a través de los cuales el flujo de datos va a ser transportado. Este servicio de QoS es considerado un mecanismo rígido, debido a la exigencia sobre los recursos de la red. Una limitante es que la reservación de rutas no se puede lograr en el Backbone de la red, debido a que en esta parte la red maneja un caudal de tráfico muy grande, incluyendo muchas clases de servicios en cualquier momento, lo cual hace imposible reservar recursos.

2.4.4 Arquitectura Servicios Diferenciados o DiffServ

"[…] DiffServ es por lejos la arquitectura más desarrollada que brinda QoS en redes IP, tanto para redes privadas de empresas como para proveedores de servicios […]" [24]

El modelo de arquitectura DiffServ es usado para satisfacer diferentes requerimientos de QoS de los múltiples servicios transportados dentro de una red. Trabaja en la entrega de un tipo de servicio particular basándose en la calidad de servicio especificada para cada paquete. La aplicación de QoS mediante este modelo de arquitectura comienza a través del marcaje de los paquetes, este proceso puede hacerse de diferentes maneras, por ejemplo, usando el campo DSCP (Differentiated Service Code Point) de 6 bits en la cabecera de los paquetes IP. La red usa estas especificaciones para clasificar, marcar, modelar y controlar el tráfico en cada salto que atraviesa a lo largo de la red; además de mejorar el desempeño de los routers al momento de formar las colas de paquetes.

Este modelo de arquitectura es usado para muchas de las aplicaciones críticas y para entregar QoS extremo a extremo, es apropiado para flujos de datos

[24] EVANS, Op. cit., p. 209

donde viajan varios tipos de tráficos, debido a que puede mejorar el desempeño de la red mediante la demarcación entre los distintos tipos de tráfico. También se aplica de la misma forma tanto para IPv4 como para IPv6.

DiffServ emplea un conjunto de bloques de paquetes bien definidos, donde en cada bloque se define una variedad de servicios. Estos bloques reciben un trato particular de envío en cada nodo o salto dentro del dominio donde sea configurado DiffServ en la red. Este modelo sólo especifica la manera como se procesan los paquetes en los nodos y asegura que los SLA establecidos se cumplan para cada servicio. [25]

Un servicio establece algunas métricas esenciales para realizar la transmisión de sus paquetes, como el retardo, jitter, pérdida de paquetes, etc. Además, se puede caracterizar la transmisión de sus paquetes en términos de la prioridad de acceso a los recursos de la red. Una vez definido un servicio bajo estos parámetros, se especifica un PHB (Per-Hop Behavior) en todos los nodos de la red que ofrecen ese servicio, estableciendo de esta manera el dominio DiffServ, luego un DSCP es asignado al PHB.

DiffServ le da un tratamiento al paquete de manera diferente en la frontera y en el Core de la red. Los routers en la frontera de la red, dentro de un dominio DiffServ, se encargan de recibir los paquetes y clasificarlos, para luego hacer el marcaje correspondiente en el campo DSCP. Una vez realizado este proceso, los dispositivos dentro del dominio DiffServ de la red usan el valor marcado en el campo DSCP para seleccionar el PHB y otorgarle el trato apropiado de QoS. [26]

[25] SRINIVAS, Op. cit., p. 19
[26] Ídem

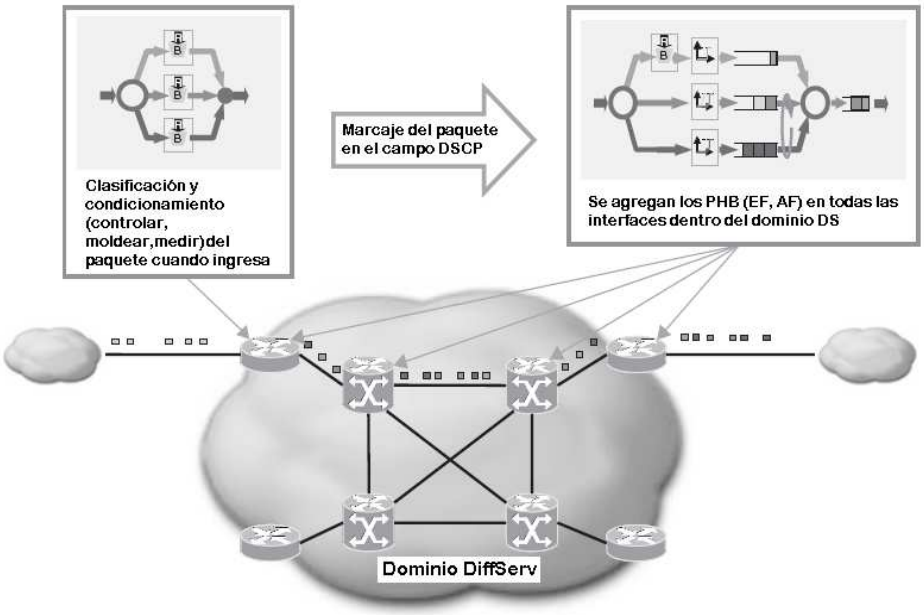


Figura 2.4.4.1 Procesamiento del paquete IP dentro de un dominio DiffServ.

DiffServ define un campo, llamado DS (Differentiated Services), que reemplaza la definición del Byte Type of Service [RFC 1349] y el Byte Traffic Class [RFC 2460] dentro de la cabecera IPv4 e IPv6 respectivamente. Este nuevo campo utiliza 6 bits como el DSCP para escoger el PHB en cada interfaz de un router. Los otros dos bits del octeto que conforma el nuevo campo DS se definen actualmente sin uso (Currently Unused, CU) y están reservados para notificaciones explícitas en casos de congestión.

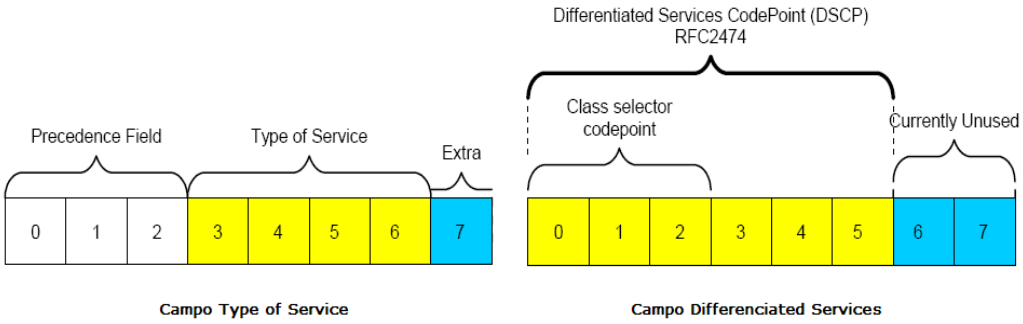


Figura 2.4.4.2 Campos Type of Service y Differentiated Services dentro de un paquete IP

DSCP es el campo que indica que tipo de trato va a recibir el paquete cuando ingresa dentro de un dominio DiffServ. Basándose en el valor de DSCP o la precedencia IP, el tráfico puede clasificarse en una clase particular en un

dominio DiffServ. Los paquetes dentro de esa clase son tratados en los dispositivos intermedios del dominio DiffServ de la misma forma.

El grupo de trabajo de la IETF ha definido los distintos valores para DSCP como sigue:

- Default DSCP: esta definido por el valor 000 000.
- Class Selector DSCP: estos valores son definidos para ser compatibles hacia atrás con los paquetes que tengan valores definidos en el campo precedencia IP.

Class Selectors	DSCP
Precedencia 1	001 000
Precedencia 2	010 000
Precedencia 3	011 000
Precedencia 4	100 000
Precedencia 5	101 000
Precedencia 6	110 000
Precedencia 7	111 000

Tabla 2.4.4.1 Valores de DSCP en función de los valores de precedencia IP.

- Expedited Forwarding (EF) PHB: define servicio premium. El valor DSCP recomendado es 101 110.
- Assured Forwarding (AF) PHB: define cuatro clases de servicio, cada uno tiene tres niveles de precedencia de descarte. Como resultado, AF PHB sugiere doce valores DSCP.

Precedencia de descarte	Clase 1 (AF1x)	Clase 2 (AF2x)	Clase 3 (AF3x)	Clase 4 (AF4x)
Bajo (AFx1)	AF11 = 001 010	AF21 = 010 010	AF31 = 011 010	AF41 = 100 010
Medio (AFx2)	AF12 = 001 100	AF22 = 010 100	AF32 = 011 100	AF42 = 100 100
Alto (AFx3)	AF13 = 001 110	AF23 = 010 110	AF33 = 011 110	AF43 = 100 110

Tabla 2.4.4.2 Valores DSCP en función de los valores de Precedencia de descarte y clase

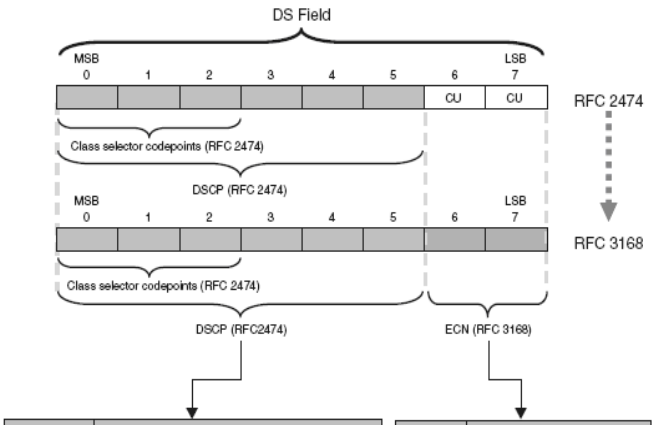
Existen 3 maneras de utilizar el campo DSCP:

1) Para seleccionar un paquete basándose en el contenido de algunas porciones del encabezado del paquete y aplicar PHB en

función de las características de servicio definidas por el valor de DSCP.

2) Para marcar el valor DSCP basándose en el perfil del tráfico.
3) Para comprobar el cumplimiento de medición de tráfico, ya sea usando la función de modelar o descarte de paquetes.

Reiterando, una vez definido el DSCP en un paquete que ingresa dentro de un dominio DiffServ se procede a escoger el PHB para otorgar el trato apropiado de QoS al paquete IP en cada salto dentro del dominio DiffServ. La IETF en la norma [RFC 2475] define PHB como un mecanismo de tratamiento de paquetes que actúa en función del tráfico perteneciente a un comportamiento en particular, y cómo se procesa este tráfico en los nodos de la red. La figura 2.4.4.3 ilustra de modo general el formato completo del campo DS, incluyendo todos los valores DSCP definidos por la IETF.



Codepoint	DSCP		
Default/CS0	000000		
EF PHB	101110		
CS1	001000		
CS2	010000		
CS3	011000		
CS4	100000		
CS5	101000		
CS6	110000		
CS7	111000		
AF PHB Group	Drop Precedence		
AF Class	Low (AFx1)	Medium (AFx2)	High (AFx3)
AF1x	AF11 = 001010	AF12 = 001100	AF13 = 001110
AF2x	AF21 = 010010	AF22 = 010100	AF23 = 010110
AF3x	AF31 = 011010	AF32 = 011100	AF33 = 011110
AF4x	AF41 = 100010	AF42 = 100100	AF43 = 100110

ECN Field		Meaning
0	0	Not ECT
0	1	ECT(0): not defined in [RFC 2481]
1	0	ECT(1)
1	1	CE

Figura 2.4.4.3 Formato del campo DS

CAPÍTULO III

3. ARQUITECTURA ACTUAL DE LA RED IP DE LA CORPORACIÓN DIGITEL C.A.

3.1 Análisis de la arquitectura actual

3.1.1 Análisis general

3.1.2 Topologías de red

3.1.3 Equipos que conforman la infraestructura física de la red

3.2 Informe de la evaluación a los equipos para implementación de QoS

3. ARQUITECTURA ACTUAL DE LA RED IP DE LA CORPORACIÓN DIGITEL C.A.

3.1 Análisis de la arquitectura actual

Al observar la documentación existente de las redes se realizó un profundo estudio de las diferentes topologías de conexión entre los dispositivos de red. Para un mejor entendimiento de los esquemas que se presentan a partir de ahora se expone la siguiente tabla con la simbología y descripción correspondiente para cada dispositivo.

Dispositivo	Símbolo	Capas de operación del modelo OSI	Modelos existentes en la red IP de Digitel	Solución que ofrece
Router		Capa 3	Cisco 1841	Doméstica, integración LAN/WAN, seguridad de datos
			Cisco 2611, 2621, 2811 y 2950. Huawei Quidway AR28-31 y AR 28-09	Mediana oficina, integración LAN/WAN, integración de múltiples servicios, Acceso a VPN, Soporte para Inter-VLAN routing
			Cisco 7206 VXR y 7609. Huawei Quidway NetEngine 20E-8	Sucursal, integración WAN, integración de múltiples servicios, mayor manejo de VPN desempeño mejorado de QoS,
Switch		Capa 3, Capa 2	Cisco 4507, 6509	Funciones de router/switch, integración LAN/WAN, gran capacidad de procesamiento, desempeño mejorado de QoS, soporte para Inter-VLAN routing
		Capa 2	Cisco 5505, 5509	Mediana oficina, Integración LAN/WAN, servicio hasta 384 puestos de trabajo o conexión para datos UTP
		Capa 2	Cisco 2900 Series, 3500. Huawei Quidway 3900-SI, Quidway S3952P-SI	Pequeña oficina, integración LAN, servicio hasta 48 puestos de trabajo o conexión para datos UTP
Firewall		Capa 3	Cisco 515, 515E	Seguridad, cortafuegos, elimina tráfico malintencionado

Tabla 3.1 Descripción de los equipos que conforman las distintas redes IP de la Corporación Digitel

3.1.1 Análisis general

La red Corporativa de Digitel está estructurada a partir de una topología tipo estrella y en base a un modelo jerárquico de tres niveles, que contempla las capas del Core, Distribución y Acceso.

La capa del Core está conformada por dos routers de alta capacidad de procesamiento y conmutación de paquetes, constituyendo la médula espinal por donde pasa todo el tráfico proveniente de cualquier punto de la Red. Estos equipos están situados físicamente en el cuarto de telecomunicaciones de Cubo Negro en el piso 5 de la torre B.

En la capa de distribución, los nodos principales de la red están conectados al Core a través de enlaces de alta velocidad mediante radio enlaces fijos punto a punto de alta frecuencia vía microondas. Están conformados por conexiones de red de área amplia (Wide Area Network, WAN). Existen cinco nodos en cuatro regiones principales que conforman este nivel en su etapa inicial: Región Capital (Cubo Negro), USB, Región Central, Región Oriente y Región Occidente. El nodo Región Occidente esta conectado al Core principal situado en Cubo Negro mediante equipos situados en la sede USB. Cada nodo perteneciente a la capa de distribución de la red está conectado al Core por uno ó mas enlaces redundantes, esto garantiza rutas alternativas en caso de falla de alguno de los enlaces principales.

El nivel de Acceso además incluye las conexiones desde los Centros de Atención de Digitel y redes pequeñas de propósitos específicos, como por ejemplo la red de atención telefónica al cliente (Call Center Los Ruices), sedes regionales de usuarios corporativos, grupos de trabajo, almacenes y distribuidores.

En la siguiente figura se muestra el esquema actual de la arquitectura lógica de la Red IP de Digitel. En los anexos se encuentran los esquemas detallados de los nodos regionales y las redes restantes.

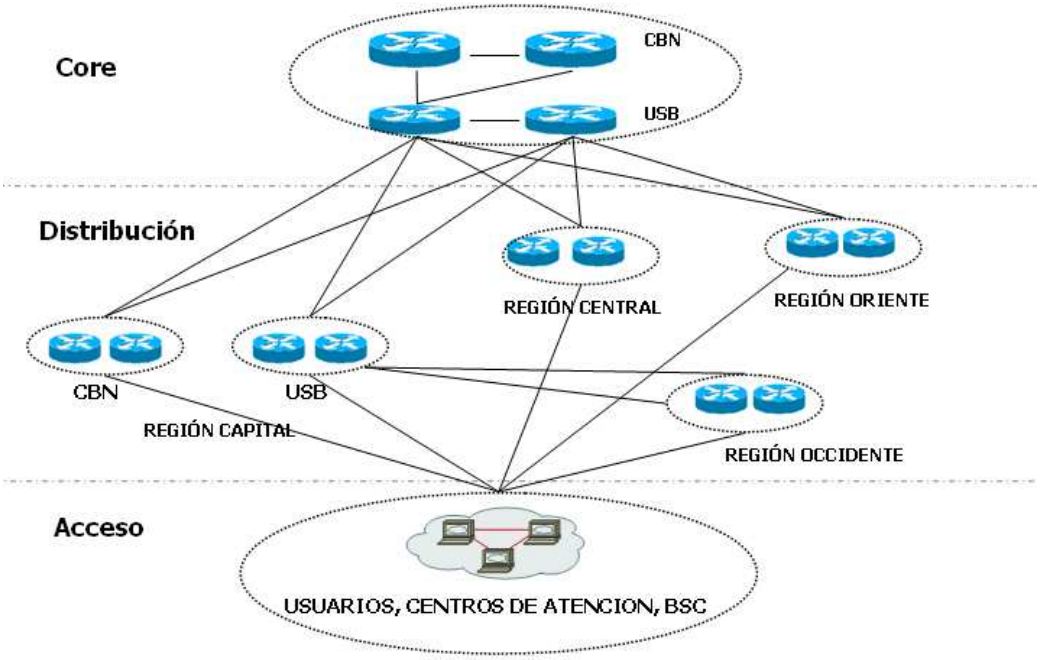


Figura 3.1.1 Esquema actual de la red IP de la corporación Digitel C.A.

Es importante aclarar que este esquema de red maneja enteramente el tráfico de datos de todos los servicios de la Corporación, desde los servicios de telefonía corporativa hasta los servicios básicos de Internet. Todo el tráfico importante de datos pasa por medio de los equipos que conforman el Core principal de la red.

Originalmente la red se constituía en su totalidad de equipos marca Cisco, por lo que se usó como protocolo de enrutamiento interno ***EIGRP*** (Enhanced Interior Routing Protocol). Sin embargo, hace algunos años los dispositivos de la red adoptaron como protocolo de enrutamiento ***OSPF*** (Open Shorest Path First), debido a la implementación de equipos marca Huawei. OSPF es un protocolo abierto, mientras que EIGRP es propietario de Cisco. Solo en algunos casos aislados se usa enrutamiento estático.

Así mismo, la empresa ha empleado el direccionamiento IP en base a la red privada ***clase A 10.0.0.0 /8*** para interconexión de equipos internamente. Esta

red ha sido dividida en varias subredes utilizando el procedimiento de subdivisión en bloques /12 y luego en bloques /16.

3.1.2 Topologías de red

La red IP de Digitel se puede definir en base a dos modelos. El primero es el esquema de interconexión entre los Centro de Atención (CDA's) y los equipos del Core, también incluye la red de usuarios corporativos de la USB; el cual sigue la siguiente topología, tanto lógica como física:

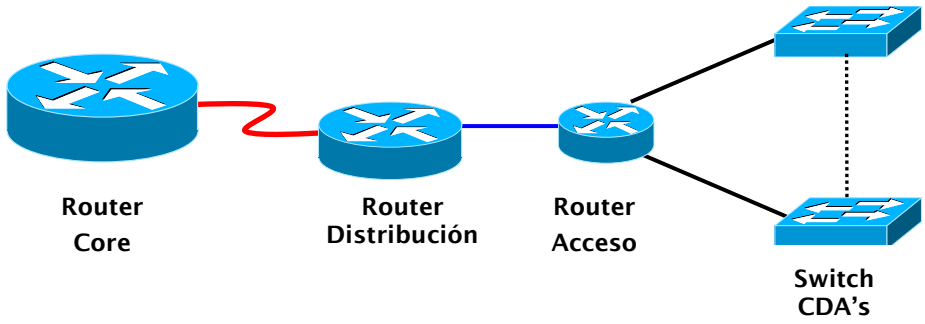


Figura 3.1.2.1 Topología física de conexión Core – Centros de Atención

Es importante recordar que para el caso de el nodo de Occidente se debe agregar la interconexión con la USB entre el router del Core y el router de distribución. La USB funciona como un Core distribuido que sirve de respaldo al Core principal.

El segundo modelo viene dado en función a como se interconectan los usuarios corporativos en las otras sedes de la Corporación a los equipos del Core. Este modelo es distinto al anterior en algunas regiones debido a que se decidió implementar los equipos Cisco con funcionalidad de Router/Switch (capa 3, capa 2) para dar mayor soporte y aliviar la operación de los equipos que siguen el esquema tradicional en la capa de distribución. Manteniendo la igualdad entre la topología lógica y física.

A diferencia del modelo anterior donde todos los Centros de Atención siguen la misma topología de interconexión, en esta ocasión cada región maneja un esquema de interconexión diferente.

En el caso de las redes que interconectan los usuarios corporativos de la sede principal en Cubo Negro con los equipos del Core se sigue la siguiente topología:

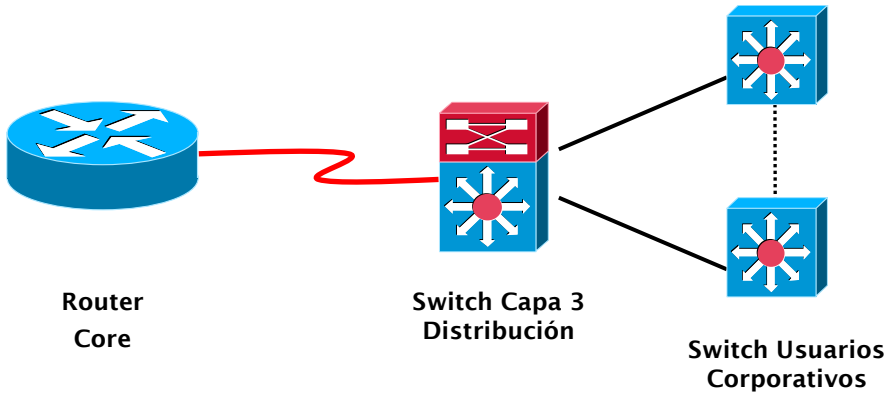


Figura 3.1.2.2 Topología física de conexión Core -Usuarios corporativos en la sede Cubo Negro

El dispositivo Switch capa 3 se conecta al Core y trabaja como un router de distribución para los Switch dispuestos en todas las oficinas en el edificio del Cubo Negro.

Para el caso de las redes que interconectan los usuarios corporativos de Centro-Llano con los equipos del Core y la red que interconecta el soporte telefónico a los clientes (Call Center) ubicado en los Ruices con los equipos del Core se tiene el siguiente esquema:

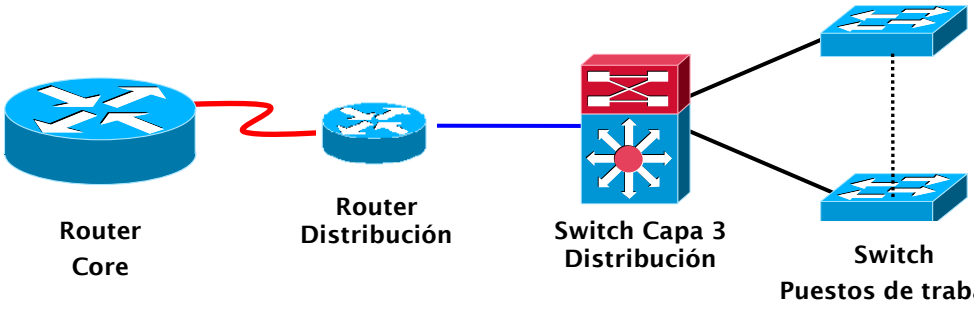


Figura 3.1.2.3 Topología física de conexión Core -Usuarios Corporativos Valencia y Core – Call Center Los Ruices

En esta oportunidad, el switch capa 3 trabaja como un elemento de conmutación a nivel LAN, estableciendo un enlace de alta velocidad (Gbps) con el router de distribución para luego administrar de manera más eficiente el ancho de banda hacia los switches de los puestos de trabajo.

Para la red que interconecta los usuarios corporativos en Occidente con el Core principal se sigue el mismo esquema anterior, salvo entre el router del Core y el router de distribución, donde se conecta un router de soporte WAN el cual está ubicado en la sede de la USB.

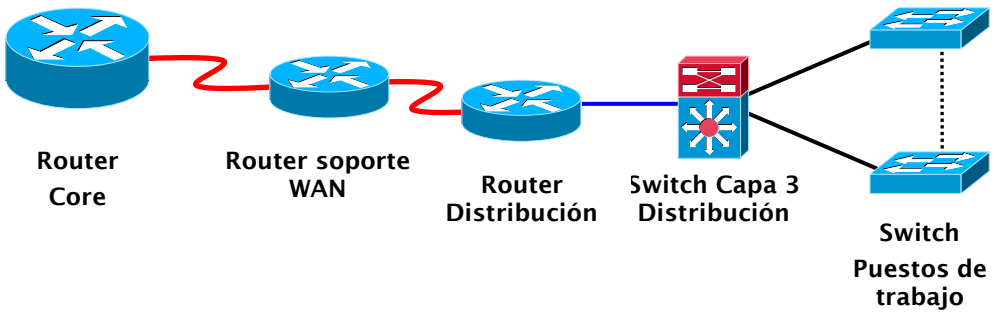


Figura 3.1.2.4 Topología física de conexión Core -Usuarios Corporativos Occidente

Finalmente, la red que interconecta los servidores que almacenan la información de la Corporación (Centro de Datos) con los equipos del Core sigue el siguiente esquema de interconexión física:

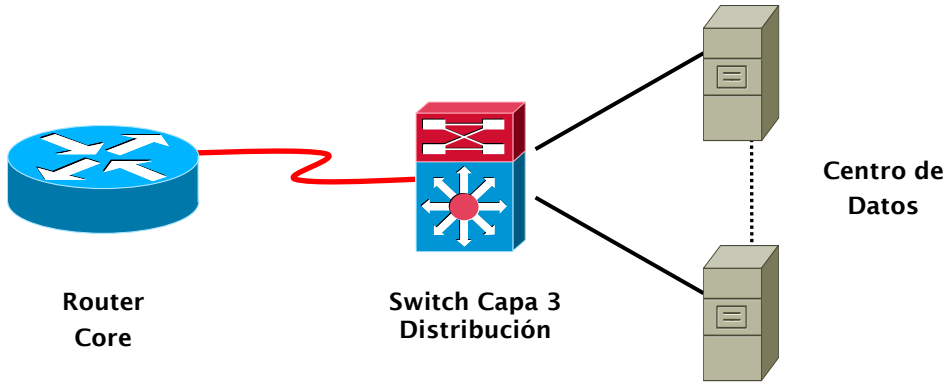


Figura 3.1.2.5 Topología física de conexión Core –Centro de Datos

El switch capa 3 opera como router y switch al mismo tiempo, de modo que el esquema real de funcionamiento lógico es el siguiente:

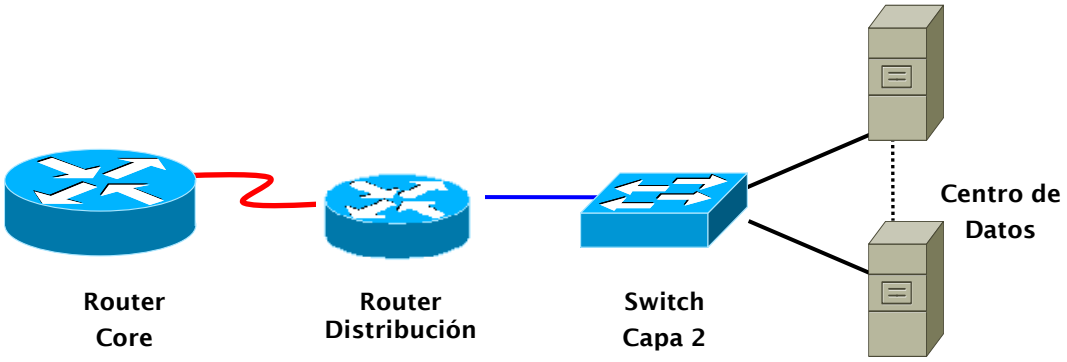


Figura 3.1.2.6 Topología lógica de conexión Core –Centro de Datos

3.1.3 Equipos que conforman la infraestructura física de la red

Los equipos que componen la ***capa del Core*** de la red son ***Cisco 7600 Series Routers***, específicamente el modelo OSR-7609. Estos equipos ofrecen, entre otras cosas, integración y enrutamiento a gran escala para redes WAN, conmutación Ethernet de alta densidad e interfaces con velocidades de hasta 10 Gbps cada una. Contiene nueve ranuras con dos tarjetas supervisoras y varios módulos de red para enrutamiento y conmutación; además de poseer una arquitectura modular que permite actualizar el equipo en función de los niveles de expansión que vaya obteniendo la red, sin necesidad de efectuar grandes migraciones.

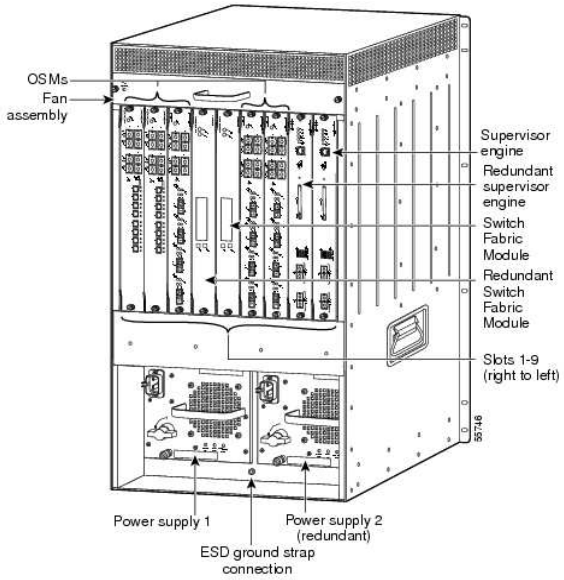


Figura 3.1.3.1 Cisco 7609 Router

Los módulos de red dan soporte a una variedad de interfaces de conexión LAN y WAN, como por ejemplo: Ethernet, ATM, serial, ISDN BRI, y opciones integradas CSU/DSU para conectividad WAN tanto principal como de respaldo.

Entre sus rasgos más destacados se encuentran:

- Un solo equipo maneja velocidades hasta 720 Gbps, cada ranura o tarjeta maneja 40 Gbps.
- Portador Ethernet, agregación de tráfico masivo y servicio de gestión. La suite del equipo es escalable y extensible para el hardware, además permite actualizaciones de software para aumentar la capacidad del equipo para servicios de Ethernet.
- Ofrece integración WAN para las empresas y acceso a redes Metro Ethernet.

Los equipos que componen la ***capa de distribución*** de la red en cuatro de los cinco nodos existentes (Cubo Negro, USB, Centro-Llano y Oriente) son ***Cisco 7200 Series Routers***, específicamente el modelo 7206 VXR. Este dispositivo se diseñó para dar soporte WAN a enlaces con velocidades en Gbps. Además de mejorar el desempeño en aplicaciones de datos, voz y video de ambientes empresariales y para proveedores de servicio. Esta equipado con una tarjeta controladora, una tarjeta procesadora y seis adaptadores de puerto de alta velocidad los cuales pueden ser ocupados con módulos de diferentes interfaces de conexión LAN y WAN. También pueden dar soporte a interfaces Gigabit Ethernet, ATM, serial e ISDN BRI.

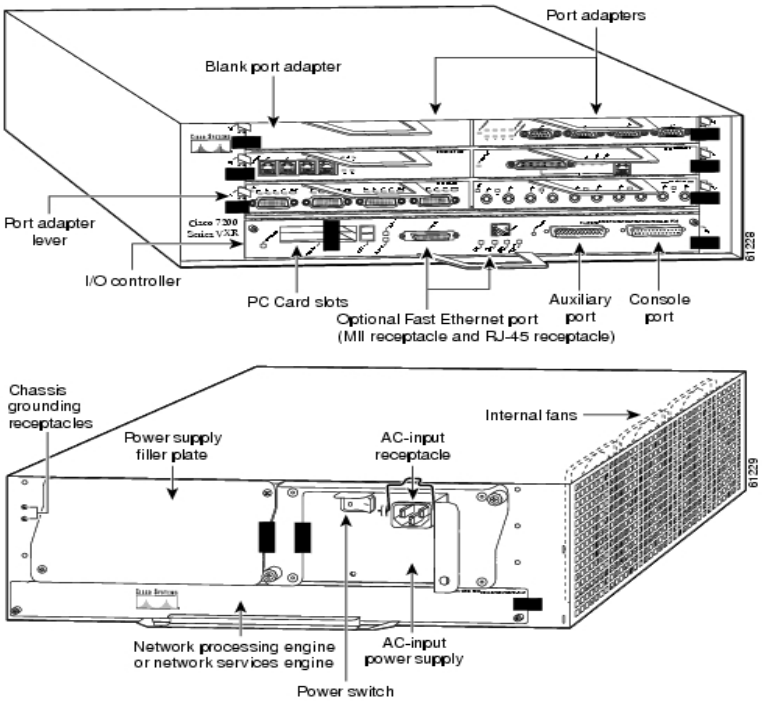


Figura 3.1.3.2 Cisco 7206 VXR Router

Los módulos NPE son actualizables, además procesan un millón de paquetes por segundo a través de sus 3 puertos 10/100/1000 Mbps (RJ-45 o convertidor de interfase Gigabit).

Las funcionalidades más destacadas de los equipos Cisco 7200 VXR son las siguientes:

- Inserción y remoción en línea. Se pueden agregar, reemplazar o remover módulos sin necesidad de interrumpir la operación general del equipo.
- Monitoreo detallado y funciones especiales. Mantiene la operación normal del sistema mientras se resuelven eventuales situaciones de operación crítica que se puedan presentar en módulos específicos.

El nodo restante de la ***capa de distribución*** (Región Occidente) esta conformado por dispositivos ***Huawei Quidway NetEngine 20E/20 Series***, específicamente el modelo NE20-8. Estos equipos poseen doce ranuras donde se pueden insertar módulos con interfaces Ethernet, ATM y serial que dan soporte

para envío de paquetes a altas velocidades de transmisión, incluyendo paquetes QoS y con información de seguridad.

Como función relevante, este equipo ofrece soporte QoS/DiffServ a través de clasificación de tráfico, Control y modelado de tráfico, servicio de congestión (PQ/CQ/WFQ/CBQ) y evasión de congestión (WRED), asegurando el ancho de banda y retardo para varios servicios.

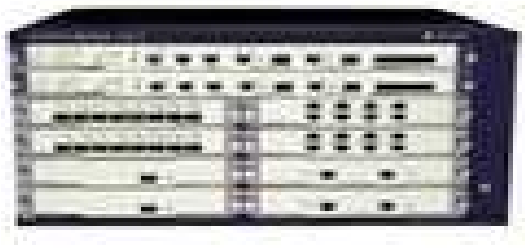


Figura 3.1.3.3 Huawei Quidway NetEngine NE20-8 router

A nivel de la ***capa de acceso*** se encuentran diversos equipos de menor envergadura, los cuales manejan un tráfico de datos en menor magnitud que los dispositivos de las dos capas superiores. Estos equipos son de distintas marcas y distintos modelos. En la red IP de Digitel se interconectan 43 Centros de Atención a los distintos nodos de distribución dispuestos a nivel nacional; cada uno de estos equipos cumple con las necesidades de comunicación de la zona donde esta ubicado. También se interconectan equipos a los distintos almacenes, distribuidores y pequeñas sucursales de trabajo. La siguiente tabla sintetiza los dispositivos dispuestos en la capa de acceso.

Marca	Serie	Modelo
Huawei	Quidway Series	AR28-09
	Quidway Series	AR28-31
Cisco	Series 2800	2811
	Series 1800	1841
	Series 2620	2621

Tabla 3.2 Equipos en la capa de Acceso

Huawei Quidway Series AR28-09: estos equipos proveen interfaces integradas Fast Ethernet, serial y auxiliar. Este versátil dispositivo puede actuar como un enrutador de capa de acceso en largos enlaces y como un enrutador en la capa del Core en redes pequeñas o medianas de empresas. Da soporte a interconexión Ethernet, Frame Relay y X.25 entre otros.

Figura 3.1.3.4 Huawei Quidway Series AR28-09

Huawei Quidway Series AR28-31: La estructura modular de este modelo satisface los requerimientos para dar la mejor calidad a servicios de telefonía en líneas dial-up como PSTN e ISDN, además de servicios de datos a través de las últimas tecnologías xDSL. Puede ser usado en la capa del Core de redes pequeñas o en redes medianas para dar seguridad y confiabilidad. Tiene dos puertos Ethernet 10/100 Mbps.

Figura 3.1.3.5 Huawei Quidway Series AR28-31

Cisco Series 1841: Los routers de la serie Cisco 1800 de servicios integrados incluye el Cisco 1841, que es exclusivamente de datos. Estos modelos admiten tarjetas de interfaz WAN (WIC), tarjetas de interfaz de voz/WAN (VWIC) en modo de sólo datos, tarjetas de interfaz WAN de ancho simple y alta velocidad (HWIC) y módulos de integración avanzada (AIM).

Figura 3.1.3.6 Cisco 1841

Cisco Series 2621: Los routers de la serie 2600 ofrecen integración multiservicio de voz y datos, acceso a redes privadas virtuales (VPN) con opciones de firewall y enrutamiento con gestión de ancho de banda y entre VLAN. Procesan hasta 25.000 paquetes por segundo. También disponen de tarjetas de interfaz WAN (WIC).

Figura 3.1.3.7 Cisco 2621

Cisco Series 2811: Los routers modelo 2811 de la serie Cisco 2800 de servicios integrados admiten un módulo de red mejorado (NME) simple, cuatro tarjetas de interfaz WAN de alta velocidad simples o dos dobles (HWIC), dos AIM, dos módulos de datos de voz en paquete (PVDM), dos conexiones Fast Ethernet y 24 puertos de salida de alimentación telefónica IP.

Figura 3.1.3.8 Cisco 2811

También se encuentran los ***Switch Cisco 4507 y 6509***. Estos equipos robustos tienen la versatilidad de operar en Capa 2 y/o en capa 3 del modelo OSI. Brindan soporte a nivel de distribución de la red, simplifican las tareas de enrutamiento de las redes virtuales de área local (*Inter-VLAN routing*) para los routers presentes en esta capa, además de conmutación para dar servicio a puestos de trabajo. Además incluyen funciones sofisticadas que ayudan a controlar el borde de la red, como por ejemplo funcionalidades mejoradas de QoS, seguridad avanzada y recuperación más rápida ante las caídas de energía (hasta 3 segundos).

Contienen siete y nueve ranuras respectivamente, cada uno con dos tarjetas supervisoras y módulos para enrutamiento y conmutación los cuales soportan interfaces Ethernet (E1's) y ópticas (STM-1's).

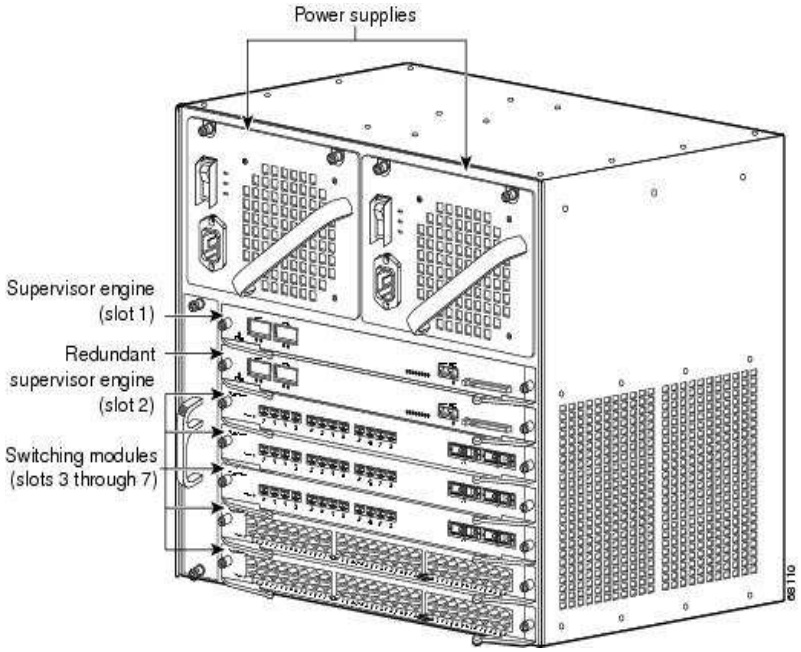


Figura 3.1.3.9 Cisco 4507 Switch

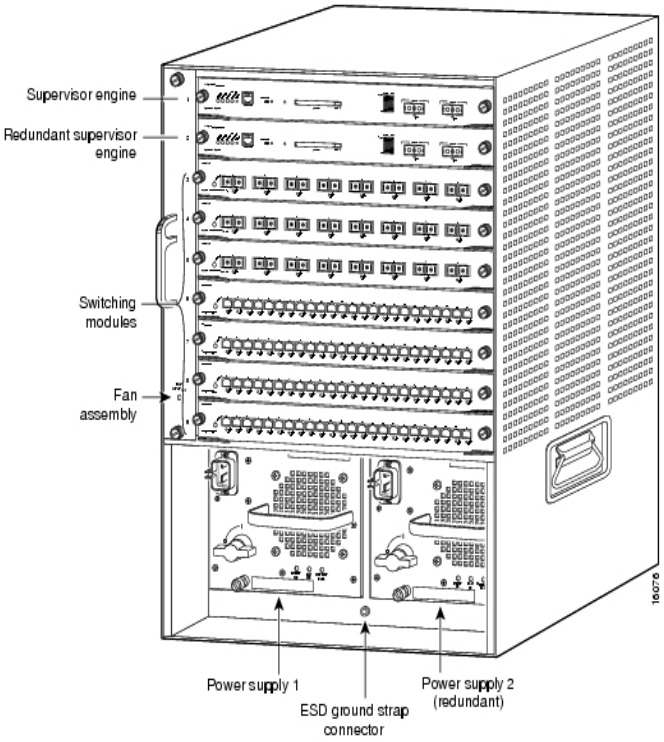


Figura 3.1.3.10 Cisco 6509 Switch

3.2 Informe de la evaluación a los equipos para implementación de QoS

Una vez realizado el estudio y análisis detallado de los equipos en las capas del Core, distribución y acceso, fue necesario evaluar los módulos, tarjetas y el sistema operativo actualmente instalado en los mismos para verificar el soporte de los mecanismos de QoS que se decidió utilizar.

Para lograr esto, se ingresó a las páginas Web de los fabricantes Cisco/Huawei (previo registro de usuario y contraseña) y se buscó información relacionada a los módulos, tarjetas y el sistema operativo de los dispositivos listados en el inventario 2009 de los equipos de la coordinación de redes. Se llegó a la conclusión que todos los equipos soportan políticas y comandos de configuración QoS, sin embargo existe la necesidad de efectuar migraciones y actualizaciones para la mayoría de ellos. Las recomendaciones que se presentan en este informe se basan en los equipos que conforman únicamente los enlaces WAN, ambiente de la red donde se van aplicar las políticas de QoS propuestas.

Observación:

Cisco ofrece información a sus clientes donde se anuncian fechas referidas a la salida del mercado, suspensión de soporte y de ventas para productos. Esta información se refiere como **End-of-Sale and End-of-Life Products Announcement Lists** y puede ser consultada a partir del siguiente enlace:

http://www.cisco.com/en/US/products/hw/tsd_products_support_end-of-sale_and_end-of-life_products_list.html

Así mismo Huawei ofrece una información similar referida como **End-of-Marketing and End-of-Service**, sin embargo no está agrupada de manera organizada. Para consultas del status de un producto en el mercado se debe ingresar en el buscador de la página www.huawei.com el modelo del producto junto con la frase End-of-Marketing.

Capa del Core

Cisco OSR-7609 Router

Descripción de los equipos:

Localidad	Área	Nombre del equipo	Versión de sistema operativo
Cubo Negro	CORE	ROU-CBN-COR-001	IOS Versión 12.1(11r)E1
		ROU-CBN-COR-002	

Recomendaciones:

Se recomienda migrar estos equipos, debido a que se encuentran en la lista **End-of-Life desde julio de 2003** y en la lista **End-of-Sale desde enero de 2004**. El equipo ya no tiene soporte desde enero de 2009, tampoco se puede renovar la licencia que permite servicio técnico al producto. Para mayor información acerca del anuncio de End-of-Sale / End-of-Life y limitaciones de soporte para este equipo consultar el siguiente enlace:

http://www.cisco.com/en/US/products/hw/routers/ps368/prod_eol_notice09186a008032d52e.html

Si no es posible la migración, se recomienda cambiar el sistema operativo a la más reciente Versión IOS Software 12.2.18-SXF16 (Early Deployment) lanzado el 05/03/09. Cisco destaca, entre otras cosas, beneficios de este nuevo software para QoS relacionado con las siguientes características:

- Aggregated DSCP / Precedence Values for Weighted Random Early Detection (WRED)
- Hierarchical Traffic Shaping
- Classification and WRED
- MQC: distribution of remaining bandwidth (supported only on WAN ports)

- Percentage Based Policing
- Network-Based Application Recognition (NBAR)

Para mayor información de los beneficios de esta versión de IOS consultar el siguiente enlace:

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html#wp4072792

Capa de Distribución

Cisco 7206 VXR Router

Descripción de los equipos:

Localidad	Área	Nombre del equipo	Versión de sistema operativo
Cubo Negro	DMZ	ROU-CBN-DMZ1-005	IOS Versión 12.2(1r)
		ROU-CBN-DMZ1-006	IOS Versión 12.1
	Internet	ROU-CBN-INT-001	IOS Versión 12.2(8r)T2
		ROU-CBN-INT-002	
	Distribución	ROU-CBN-05B-001	IOS Versión 12.3(5a)B5
		ROU-CBN-05B-002	
USB	USB	ROU-CSW-P01-001	IOS Versión 12.1
		ROU-CSW-P01-002	
		ROU-CSW-P01-005	IOS Versión 12.0
		ROU-CSW-P01-006	IOS Versión 12.2(4r)B2
Centro Llano	Valencia	ROU-VAL-PBA-001	IOS Versión 12.3(4r)T3
		ROU-VAL-PBA-002	
Oriente	Max Plaza	ROU-MAX-P02-001	
		ROU-MAX-P02-002	
Los Ruices	Call Center	ROU-RUI-P04-001	IOS Versión 12.1

Recomendaciones:

Se recomienda migrar todas estas versiones a la más reciente Versión IOS Software 12.4.25a (Maintence Deployement) lanzado el 28/05/09. Si todos los routers adoptan la misma versión de IOS se garantizará una mejor gestión de los dispositivos. Además Cisco asegura con este nuevo software, entre otras cosas, un mejor desempeño para QoS relacionado con las siguientes características:

- QoS Bandwidth Estimation
- Classification, Policing, and Marking on LAC
- Quality of Service for Virtual Private Networks
- Network-Based Application Recognition (NBAR)

Para mayor información de los beneficios de esta nueva versión de IOS consultar el siguiente enlace:

http://www.cisco.com/en/US/docs/ios/12_4/release/notes/124NEWF.html

Por otro lado, se recomienda migrar todas las tarjetas procesadoras a la *uBR7200-NPE-G2 Network Processing Engine*; esto traerá los siguientes beneficios:

- Aumento hasta el doble de la velocidad de procesamiento de los paquetes comparado con la versión inmediatamente anterior, la *uBR7200-NPE-G1*
- Integración de la tarjeta controladora con puertos auxiliar y consola, memoria flash y bootflash, en comparación a otros modelos que no tienen esta versatilidad.
- 1 GB de memoria DRAM (expandible hasta 2 GB). Lo cual permite, entro otras cosas, mayor soporte de rutas, tablas de enrutamiento, MPLS y aumento de ancho de banda.
- Puertos 10/100-Mbps Ethernet dedicados para gestión, esto ofrece una mejor administración al separar el tráfico de gestión con el tráfico medular de datos.

Actualmente existen localidades operando con modelos obsoletos como la USB (donde los cuatro routers están utilizando el modelo NPE-300) y Cubo Negro (donde los dos routers DMZ están utilizando el modelo NPE-300 y los dos routers de Internet están utilizando los modelos NPE-200 y NPE-450 respectivamente). Se recomienda efectuar los cambios a la NPE-G2 primeramente en estas localidades.

Para mayor información relacionada con la *uBR7200-NPE-G2 Network Processing Engine* consultar el siguiente enlace:

http://www.cisco.com/en/US/prod/collateral/modules/ps4917/data_sheet_cisco_ubr7200_npe_g2_network_processing_engine.html

Huawei Quidway NetEngine NE20-8 Router

Descripción de los equipos:

Localidad	Área	Nombre del equipo	Versión de sistema operativo
Occidente	**Sabaneta**	ROU-SAB-PBA-001	Versión 5.30
		ROU-SAB-PBA-002	

Recomendaciones:

Se recomienda efectuar las migraciones correspondientes para las tarjetas que se muestran en el siguiente cuadro, debido a que después de la fecha señanalada en la columna End-of-Service todo los servicios de soporte quedan inhabilitados, incluyendo soporte técnico (local, remoto, 800 call center) y soporte para hardware (mantenimiento y reemplazo).

Producto	Modelo Obsoleto	End-of-Marketing	End-of-Service	Modelo Sustituto
NE20E/NE20	NE-FIC-ATM-E3	30-4-2009	31-12-2009	Ninguno

NE20E	NE-FIC-STM1/ATM-MM/1310-2km-SC	30-4-2009	31-12-2011	NE20E-HIC-1ATM-SFP
	NE-FIC-STM1/ATM-SM/1310-15km-SC			NE20E-HIC-1ATM-SFP
	NE-FIC-STM1/ATM-SM/1310-30km-SC			NE20E-HIC-1ATM-SFP

Para mayor información del anuncio End-of-Marketing relacionado con los módulos para los routers Quidway NetEngine 20/20E consultar el siguiente enlace:

http://www.huawei.com/products/datacomm/catalog.do?id=3055

Capa de Acceso

Cisco 2811 Router

Descripción de los equipos:

Localidad	Área	Nombre del equipo	Versión de sistema operativo	Ubicación
Cubo Negro	CDA	ROU-DCM-PBA-001	IOS Versión 12.3(8r)T7	Los Dos Caminos
		ROU-OAS-P03-001		OASIS
USB		ROU-CHA-PBA-001		Chacaito
		ROU-MET-P03-001		Metrocenter

Recomendaciones:

Es recomendable hacer la migración del sistema operativo a la última versión del IOS Versión 12.4.25a (Maintence Deployment) lanzado el 28/05/09. Cisco asegura, entre otras cosas, mejora de las funcionalidades de QoS relacionada a los siguientes tópicos:

- QoS Bandwidth Estimation
- Classification, Policing, and Marking on LAC
- Quality of Service for Virtual Private Networks
- Network-Based Application Recognition (NBAR)

Para mayor información de los beneficios de esta nueva versión de IOS consultar el siguiente enlace:

http://www.cisco.com/en/US/docs/ios/12_4/release/notes/124NEWF.html

Cisco 2621 Router

Descripción de los equipos:

Localidad	Área	Nombre del equipo	Versión de sistema operativo	Ubicación
Cubo Negro	CDA	ROU-CCT-NC2-001	IOS Versión 12.1(3r)T2	CCCT
	DMZ	ROU-CBN-DMZ-003		CBN
		ROU-CBN-MER-001		
USB	CDA	ROU-MCY-MEZ-001		Maracay
Oriente	BSC	ROU-MAR-BSC-001	IOS Versión 12.3(18)	BSC Margarita
Centro Llano	CDA	ROU-BVC-PBA-001	IOS Versión 11.3(2)XA4	Beverly Center

Recomendaciones:

Se recomienda migrar estos equipos, debido a que se encuentran en la lista **End-of-Sale desde abril de 2003** y en la lista **End-of-Life desde abril de 2008**. El equipo ya no tiene soporte desde abril de 2006, tampoco se puede renovar la licencia que permite servicio técnico al producto. Cisco recomienda reemplazar los modelos 2621 por los 2621XM como se indica en el siguiente cuadro:

Modelo Obsoleto	Modelo Sustituto
CISCO2621	CISCO2621XM
CISCO2621-DC	CISCO2621XM-DC
CISCO2621-RPS	CISCO2621XM-RPS

Para mayor información acerca del anuncio de End-of-Sale / End-of-Life, limitaciones de soporte y beneficios del modelo sustituto sugerido para este equipo consultar el siguiente enlace:

http://www.cisco.com/en/US/products/hw/routers/ps259/prod_eol_notice09186a008032d4c2.html#wp42613ç

Cisco 1841 Router

Descripción de los equipos:

Localidad	Área	Nombre del equipo	Versión de sistema operativo	Ubicación
Cubo Negro	CDA	ROU-OPE-CCS-ACEL	IOS Versión 12.3(8r)T9	Accel
		ROU-PAM-P04-001		Paseo las Mercedes
		ROU-LIT-PBA-001		Litoral
		ROU-MAY-PBA-001		Macaracuay
		ROU-MAI-P01-001		Maiquetía
		ROU-HTE-PBA-001	IOS Versión 12.3(8r)T8	Higuerote
		ROU-ACA-PRA-001		Acarigua Prainca
		ROU-ACA-PRO-001		Acarigua Profil
		ROU-STR-PBA-001		Santa Teresa
USB	USB	ROU-USB-BSC-001	IOS Versión 12.3(8r)T9	USB
Oriente	CDA	ROU-ORI-PBA-001	Versión 12.3(8r)T8	Orinokia
		ROU-PLC-TUN-001	IOS Versión 12.3(8r)T9	Puerto La Cruz
		ROU-SAM-MAR-001		Sambil Margarita
Centro Llano	CDA	ROU-BQ6-PBA-001	IOS Versión 12.3(8r)T8	Barquisimeto
		ROU-SFP-PBA-001	IOS Versión 12.3(8r)T9	San Felipe
		ROU-SCA-PBA-001	IOS Versión 12.3(8r)T9	San Carlos
		ROU-LVI-PBA-001	IOS Versión 12.3(8r)T9	Victoria
	BSC	ROU-BSC-MOR-001	IOS Versión 12.3(8r)T9	BSC El Morro
		ROU-BSC-CAF-001	IOS Versión 12.3(8r)T9	BSC Café
	CDA	ROU-ACA-PBA-001	IOS Versión 12.3(8r)T9	Acarigua
		ROU-CAL-PBA-001		Calabozo
Occidente	CDA	ROU-OJD-PBA-001	IOS Versión 12.3(8r)T9	Ciudad Ojeda
		ROU-MBO-PAL-001	IOS Versión 12.3(8r)T9	Palacio de los Eventos
		ROU-MRD-P01-001		Mérida

Occidente	CDA	ROU-SCR-SAM-001	IOS Versión 12.3(8r)T8	Sambil San Cristóbal
		ROU-MBO-SAM-001	IOS Versión 12.3(8r)T9	Sambil Maracaibo

No hay recomendaciones para los routers 1841, debido que todos mantienen una versión de IOS aceptable para el funcionamiento de los equipos.

Huawei AR 28-31 y AR 28-09 Routers

Descripción de los equipos:

AR 28-31

Localidad	Área	Nombre del equipo	Versión de sistema operativo	Ubicación
Cubo Negro	CDA	ROU-CDA-MQZ-001	Versión 3.40	El Marqués
		ROU-TEQ-PBA-001		Los Teques
		ROU-PRO-PBA-001		Propatria
USB		ROU-ALM-CHA-001		Charallave
Oriente		ROU-CDB-PBA-001		Ciudad Bolívar
		ROU-CUM-PBA-001		Cumaná
		ROU-MAT-PBA-001		Maturín
		ROU-TIG-PBA-001		El Tigre
Centro Llano		ROU-VAL-AVB-001		Av. Bolívar
		ROU-GMY-P03-001		Galerías Maracay
		ROU-PCB-PBA-001		Puerto Cabello
		ROU-PZT-PBA-001		Plaza de Toros
Occidente		ROU-VRA-PBA-001		Valera
		ROU-BRQ-P01-001		Barquisimeto
		ROU-PFJ-PBA-001		Punto Fijo

AR 28-09

Localidad	Área	Nombre del equipo	Versión de sistema operativo	Ubicación
Occidente	CDA	ROU-CDA-BAR-001	Versión 3.40	Barinas
		ROU-SCR-BAR-001		Barrio Obrero
		ROU-SCR-CCE-001		CC Del Este - San Crsitóbal
		ROU-CDA-BQTO2-001		Sambil Barquisimeto

Recomendaciones:

Se sugiere estar alerta a las fechas mostradas en el cuadro a continuación anunciadas por Huawei debido a que después de las mismas se suspenderán todos los servicios de soporte técnico (local, remoto, 800 call center) y soporte para hardware (mantenimiento y reemplazo).

Serie	End-of-Marketing	End-of-Full-Service	End-of-Service
AR 28	30-11-2007	1-12-2009	1-12-2012

Cisco 4507 Switch

Descripción de los equipos:

Localidad	Área	Nombre del equipo	Versión de sistema operativo	Ubicación
Cubo Negro	CORE	FRS-CBN-05B-CR1	IOS Versión 12.1(23)E	Cubo Negro
		FRS-CBN-05B-CR2		
	Usuarios	SWI-CBN-07A-001	IOS Versión 12.2(20)EW	
Oriente	Max Plaza	FRS-MAX-P02-001	IOS Versión 12.2(25)EWA6	Max Plaza
		FRS-MAX-P02-002		
Centro Llano	Valencia	FRS-VAL-PBA-002	IOS Versión 12.2(25)EWA12	Valencia
Los Ruices	Call Center	FRS-RUI-P04-002	IOS Versión 12.2(25)EWA6	Los Ruices
		FRS-RUI-P04-003		
Occidente	Sabaneta	FRS-SAB-PBA-001	IOS Versión 12.2(25)EWA12	Sabaneta
		FRS-SAB-PBA-002		

Recomendaciones:

En esta oportunidad no es recomendable hacer cambios de sistema operativo, debido a que de las versiones actualmente instaladas en los equipos no hay mejoras sustanciales con la última versión del IOS Versión 12.2(53)SG (Early Deployment) lanzado el 22/07/09.

Para mayor información de esta nueva versión de IOS consultar el siguiente enlace:

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL_5184.html#wp1987516

Cisco 6509 Switch

Descripción de los equipos:

Localidad	Área	Nombre del equipo	Versión de sistema operativo
Cubo Negro	CORE	SWI-CBN-05B-DC1	IOS Versión 6.1(2)
		SWI-CBN-05B-DC2	
		SWI-CBN-06B-DC1	IOS Versión 6.1(2)
		SWI-CBN-06B-DC2	

Recomendaciones:

Se recomienda migrar las tarjetas a uno de los modelos siguientes: Supervisor Engine 2, Supervisor Engine 32, Supervisor Engine 32 PISA, Supervisor Engine 720, and Supervisor Engine 720-10GE. Así mismo, es recomendable hacer la migración del sistema operativo a la última versión del Cisco IOS Software Release 12.2(18)ZYA.

Para mayor información consultar el siguiente enlace:

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/product_bulletin_c25_468195.html

CAPÍTULO IV

4. IDENTIFICACIÓN DEL TRÁFICO DE LAS APLICACIONES

4.1 Identificación preliminar del tráfico

4.2 Esquema de planificación para la identificación del tráfico

4.3 Procedimientos efectuados para la identificación del tráfico

4.4 Resultados de la captura de tráfico

4.5 Análisis de los resultados de la captura de tráfico

4.5.1 Identificación final del tráfico de las aplicaciones

4.5.2 Clasificación del tráfico según su tipo y creación de la Matriz de las aplicaciones

4. IDENTIFICACIÓN DEL TRÁFICO DE LAS APLICACIONES

A partir del proceso de reconocimiento y noción de los distintos departamentos que componen la estructura organizacional de la empresa, se logró conseguir la información necesaria para identificar los distintos tipos de tráfico de datos que transporta la red IP de Digitel actualmente y que son usados por los empleados para llevar a cabo las distintas tareas que desarrolla la corporación. Toda esta información se reunió a través de entrevistas, consultando en la base de datos de la coordinación de redes y realizando estudios con el apoyo de software dedicado para la captura de tráfico.

4.1 Identificación preliminar del tráfico

De manera preliminar y según los requerimientos del Coordinador del departamento de Redes, se identificó y preclasificó el tráfico de datos que transporta la red actual de la siguiente manera:

- Medular: contiene el tráfico de los sistemas de Facturación/Cobro (Billing System), Plataformas de Servicios de Atención al Cliente y Ventas en los Centros de Atención.
- Corporativo: contiene el tráfico de los servicios de Internet para usuarios corporativos, correo electrónico para usuarios corporativos, servidores FTP, archivos e impresoras, inicio de sesión de usuario (login usuario).
- Gestión: contiene el tráfico de los servicios que gestionan y monitorean la red pertenecientes a los departamentos de Centro de Monitoreo y el NOC (Network Operation Center).

4.2 Esquema de planificación para la identificación del tráfico

El esquema de planificación que se decidió utilizar se fundamentó en realizar un estudio del tráfico de la red que conforman los Centros de Atención.

Actualmente esta red es valorada como de gran importancia dentro de la compañía, debido a la importancia en la operatividad de la misma dentro de la dinámica de negocio actual de la corporación.

Así mismo, se optó por el software ***WireShark*** como el mecanismo de obtención de los datos para el estudio del tráfico. Este software es un analizador de protocolos con muchas funcionalidades, es de fuente abierta y de libre descarga a través de Internet, el cual permite guardar en un archivo la captura en vivo del tráfico durante un período determinado de tiempo para su posterior análisis. Es soportado por plataformas como Windows, Linux, OS X, Solaris, FreeBSD y NetBSD.

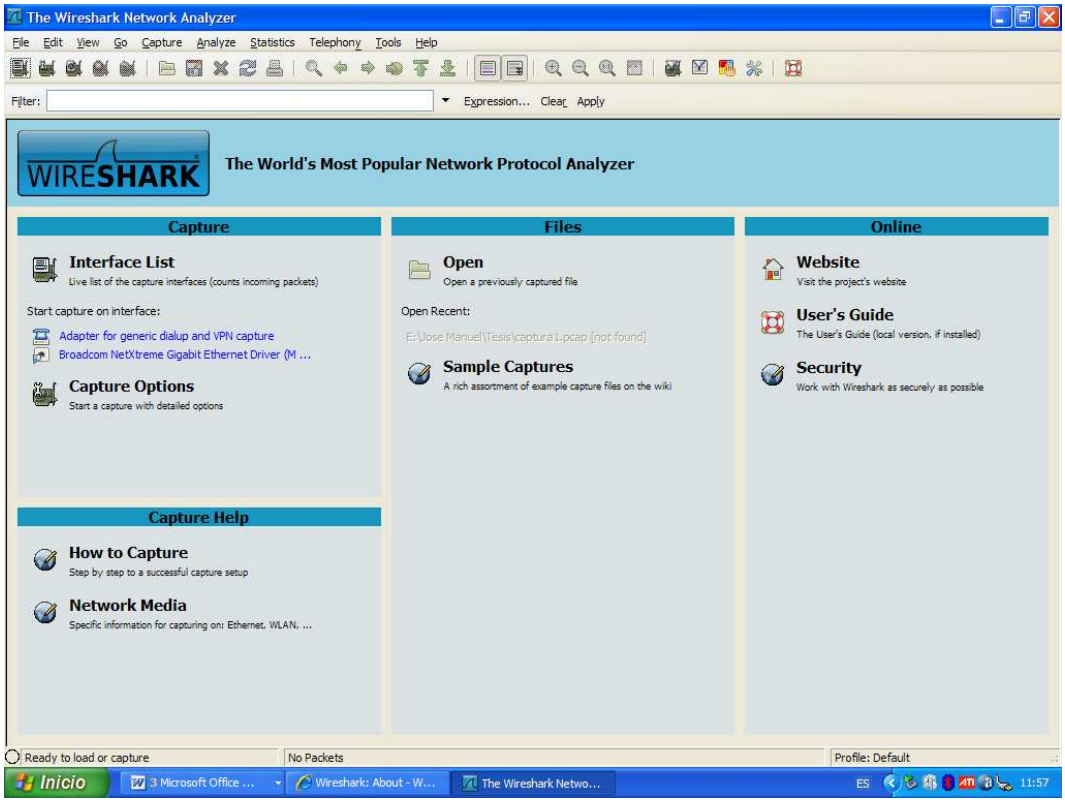


Imagen 4.2 Interfaz gráfica de entrada del software analizador de protocolos WireShark

4.3 Procedimientos efectuados para la identificación del tráfico

Para arrancar con el estudio del tráfico en las redes de los Centros de Atención fue necesario seleccionar un Centro de Atención (CDA) para la captura de tráfico. Según la percepción inicial, todos los CDA's utilizan las mismas aplicaciones y generan el tráfico de manera similar, unos en mayor medida en comparación con otros. Se prefirió el CDA de Los Dos Caminos, el cual está ubicado en el nodo de la Región Capital.

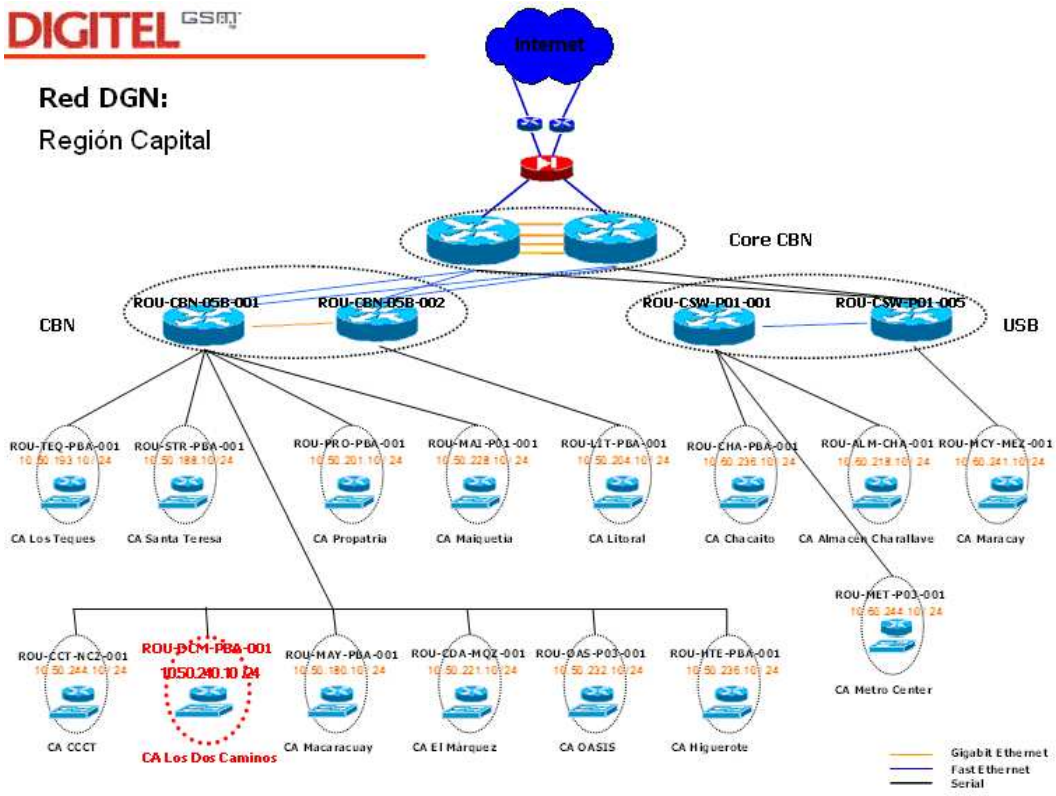


Figura 4.3.1 Red de los CDA´s en el nodo Región Capital

Como se observa en la figura 4.3.1, ***la dirección IPv4 para la red de este CDA es la 10.50.240.0 /24***. Las direcciones que se observan el la figura 4.3.1 son las ***Puerta de enlace predeterminada (Default Gateway)*** que utiliza cada una de las redes LAN para salir hacia otras redes. Se decidió escoger este CDA por dos razones principales:

- Junto con las sedes en Metrocenter, CCCT y Oasis en Guarenas-Guatire, este CDA es uno de los que atiende mayor cantidad de clientes en la región capital, esto se traduce en mayor volumen de tráfico generado hacia el Core de la red.
- Los beneficios en cuanto a la logística que brinda este CDA son mejores comparándolo con las sedes mencionadas en el enunciado anterior. El DCN donde se localizan los equipos de red presenta mayor comodidad para efectuar el trabajo de la captura de tráfico y además se encuentra físicamente más cerca de la sede principal en Chuao-Cubo Negro para el traslado.

En el CDA de Los Dos Caminos se tiene el siguiente esquema de interconexión en los equipos:

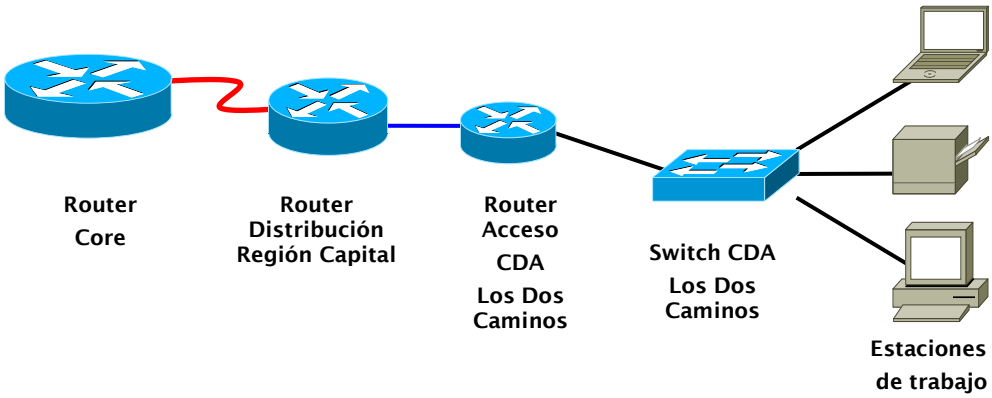


Figura 4.3.2 Esquema de interconexión desde el Core principal hasta el CDA de Los Dos Caminos

Para llevar a cabo la captura de tráfico se conectó una laptop, que tenía previamente instalado el software ***WireShark,*** en uno de los puertos disponibles del ***Switch Cisco 2950SX de 48 puertos*** ubicado en el CDA.

Figura 4.3.3 Esquema de interconexión con el Switch Cisco 2950SX para la captura de tráfico

Posteriormente, se necesitó realizar configuración adicional en este puerto para observar todo el tráfico generado por los 42 puestos de trabajo que están funcionando en el CDA, y que pasa por medio del enlace entre el router de acceso y el router de distribución, para lograr esto se configuró este puerto como puerto de monitoreo ***SPAN (Switched Port Analyzer)*** ingresando los siguientes comandos en el switch:

```
SWI-DCM-PBA-001#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SWI-DCM-PBA-001(config)# Monitor session 1 source interface gigabitEthernet 1/0/1
SWI-DCM-PBA-001(config)# Monitor session 1 destination interface fastEthernet 1/0/8
SWI-DCM-PBA-001(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
SWI-DCM-PBA-001#
```

Imagen 4.3.1 Línea de comandos para la configuración en modo SPAN

Para verificar que la configuración fue cargada con éxito se usó el siguiente comando:

```
SWI-DCM-PBA-001#
SWI-DCM-PBA-001# show monitor session 1
Session 1
---
Type     : Local Session
Source Ports     :
Both     : Gi1/0/1
Destination Ports        : Fa1/0/8
Encapsulation    : Native
Ingress          : Disabled

SWI-DCM-PBA-001#
```

Imagen 4.3.2 Línea de comandos que muestra la configuración en modo SPAN

De inmediato se configuró el ***WireShark*** para el inicio de la captura. Se realizaron dos capturas de tráfico, en un horario comprendido entre las 9 am y 12 pm (este horario es donde se genera el mayor tráfico del día). A continuación se muestran varias capturas de pantalla del trabajo realizado.

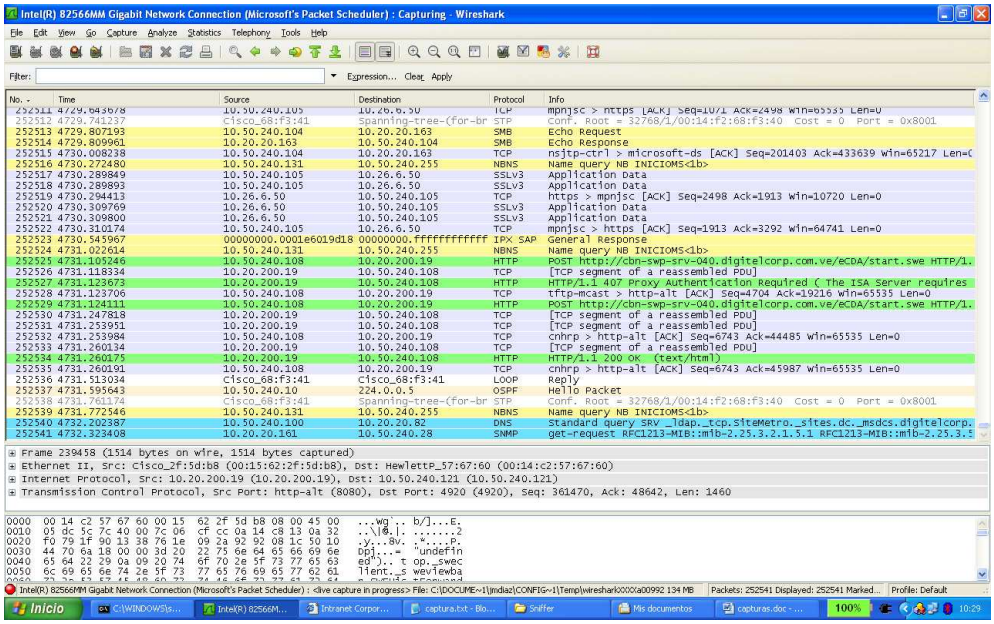


Imagen 4.3.3 Imagen de pantalla de la Captura 1

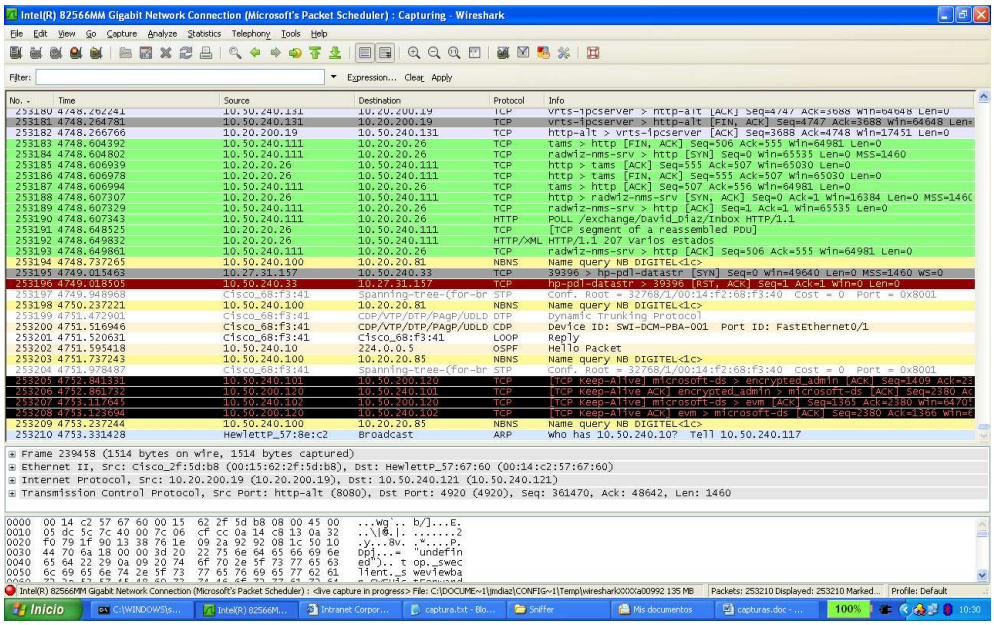


Imagen.4.3.4 Imagen de pantalla de la Captura 1

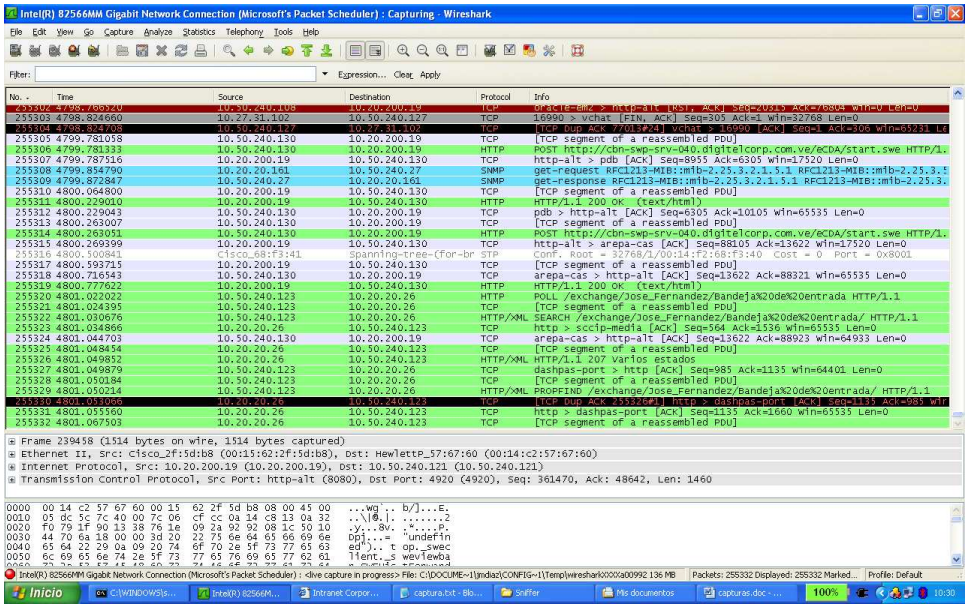


Imagen 4.3.5 Imagen de pantalla de la Captura 1

A su vez, mediante una entrevista con el subgerente del CDA se reveló que la mayoría del tráfico generado en los CDA´s es del tipo cliente/servidor, es decir, los empleados de los distintos CDA's hacen solicitudes a los diferentes servidores que manejan las aplicaciones. Seguidamente se identificó las aplicaciones que usan los empleados de los CDA's.

Aplicaciones utilizadas en los CDA's
Siebel® (CRM)
SIR
Intranet de Ventas y Atención al Cliente
Administrador de Aprovisionamiento BlackBerry®
SAP®
Reporte de IMEI
SCF
Portal de Activaciones
Módulo de Servicio Técnico
Administrador BlackBerry® Internet Services
Digimatic

Tabla 4.3.1 Aplicaciones utilizadas en los CDA's

De las cuales todas son aplicaciones WEB con excepción de ***SAP (Sistemas, Aplicaciones y Productos)*** que es una herramienta de Planificación de Recursos Empresariales o denominada también de tipo ***ERP (Enterprise Resource Planning)***, la cual trabaja de la misma manera que una solicitud WEB, es decir,

mediante una petición cliente/servidor. Según lo especificado por este subgerente, las cuatro herramientas más críticas y que son más prioritarias son las siguientes:

1. Siebel® (CRM)
2. SIR
3. Intranet de Ventas y Atención al Cliente
4. Administrador de Aprovisionamiento de BlackBerry®
5. SAP®

4.4 Resultados de la captura de tráfico

Una vez completada la captura del tráfico se procedió a utilizar las herramientas que dispone el **WireShark** para el análisis necesario.

En primer lugar, se generó la estadística titulada ***Summary***, que describe de manera general la captura realizada. A continuación se muestra la imagen de pantalla de la estadística en cuestión para las dos capturas realizadas.

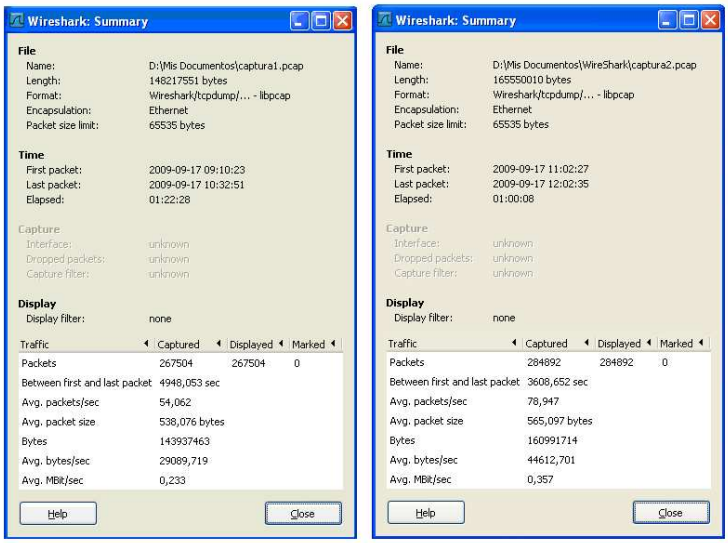


Imagen 4.4.1 Imágenes de pantalla de la estadística Summary para las dos capturas

En la imagen 4.4.1 se pueden apreciar los siguientes campos más destacados:

- File: información general relacionada con la captura, el tamaño de la mismas fueron 148,217 Mega bytes y 165,550 Mega bytes respectivamente
- Time: las marcas de los tiempos desde que se capturó el primer paquete hasta el momento de la captura del último paquete. El tiempo de duración total de la capturas fue de 01:22:28 y 01:00:08 respectivamente
- Traffic: información relacionada con el tráfico capturado. La cantidad de paquetes capturados fue de 267504 con un promedio de 54 paquetes capturados por segundo para la captura 1 y de 284892 con un promedio de 78,95 paquetes por segundo para la captura 2

En segundo lugar, se utilizó la estadística ***Endpoints a través del protocolo IPv4,*** la cual permite visualizar a través de distintos protocolos el número de paquetes enviados y recibidos por cada uno de los puntos finales de la red, así como el total y el tamaño de los mismos. Luego de analizar ambas capturas mediante esta estadística se observó un comportamiento similar, lo cual llevó a realizar el análisis de solamente una de las capturas, escogiendo la captura 1 como base de estudio entender cuales son las direcciones de los servidores más solicitadas por los clientes, es decir, los empleados del CDA Los Dos Caminos.

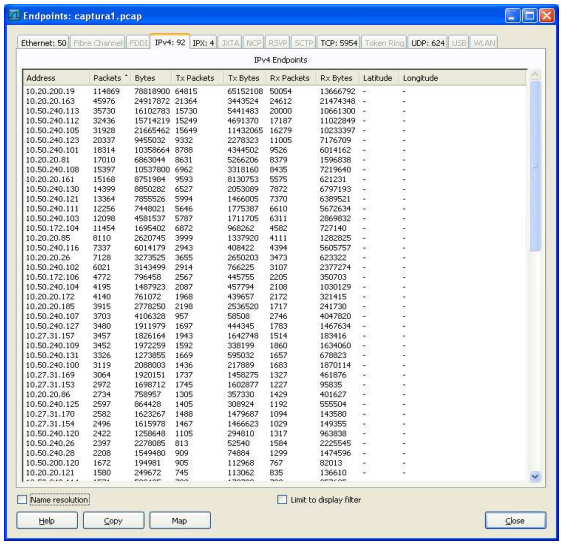


Imagen 4.4.2 Imagen de pantalla de la estadística Endpoints

Aquí se identificó de manera preliminar cuales son las direcciones IPv4 que no pertenecen a la red LAN del CDA (10.50.240.0 /24) que tuvieron mayor número de paquetes. Es decir, las que fueron más solicitadas por los empleados del CDA. Esto se ilustra mejor en la tabla y gráfico a continuación.

IPv4	Paquetes RX	Paquetes TX
10.20.200.19	50054	64815
10.20.20.163	24612	21364
10.20.20.81	8379	8631
10.27.31.28, 10.27.31.102, 10.27.31.153, 10.27.31.154, 10.27.31.157, 10.27.31.158, 10.27.31.169, 10.27.31.170.	6782	9214
10.20.20.161	5575	9593
10.50.172.104	4582	6872
10.20.20.85	4111	3999
10.20.20.26	3473	3655
10.50.172.106	2205	2567
10.20.20.172	2172	1968
10.20.20.185	1717	2128
10.20.20.86	1429	1305
Total	*115091*	*136111*

Tabla 4.4.1 Direcciones IPv4 de los servidores con mayor solicitud por parte de los usuarios del CDA

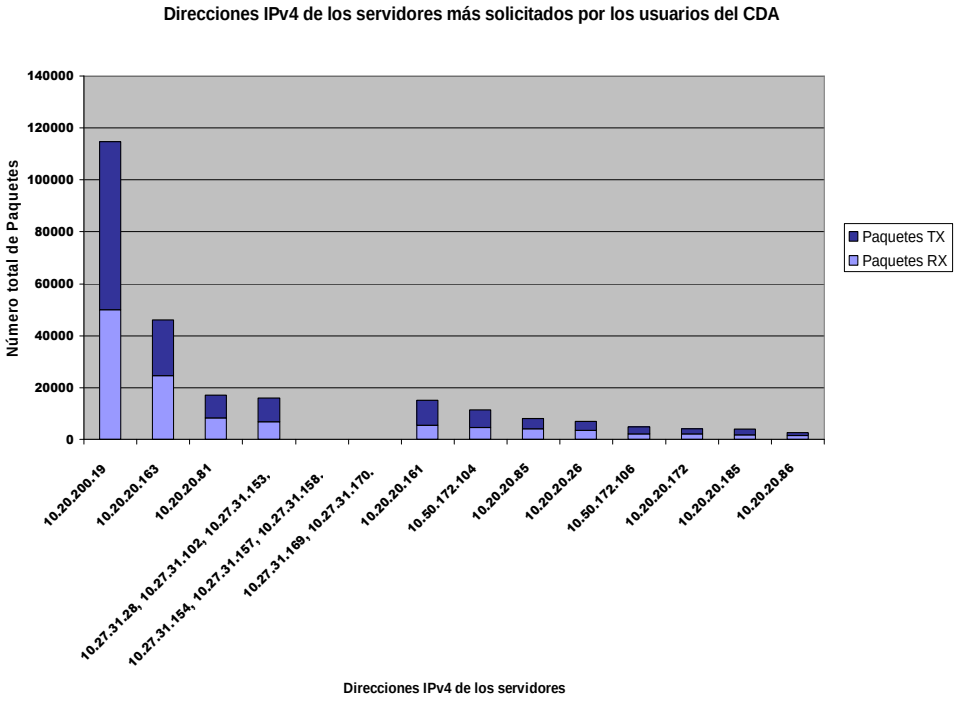
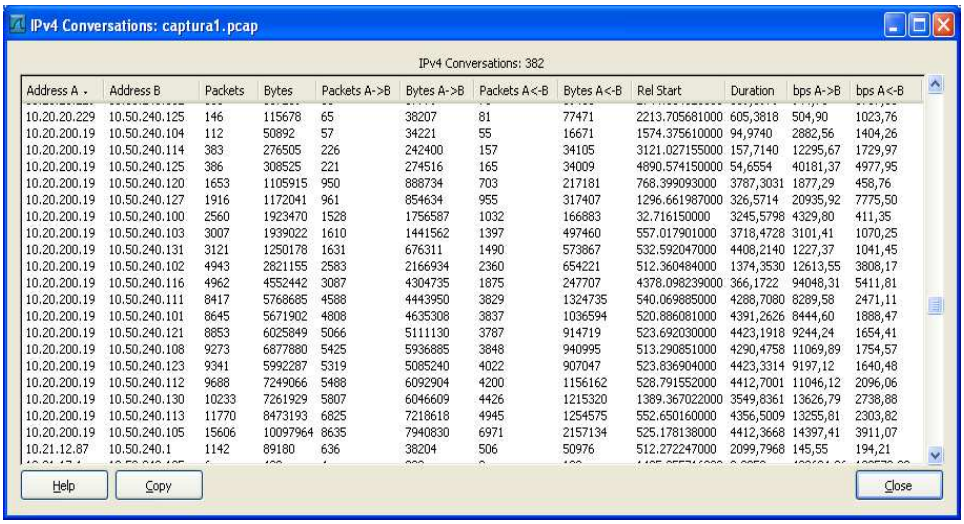


Gráfico 4.4.1 Direcciones IPv4 de los servidores más solicitados por los usuarios del CDA

En tercer lugar, se utilizó la estadística ***IPv4 Conversations***. Mediante esta estadística se pudo entender de forma detallada el comportamiento de todo el tráfico IPv4 entre dos específicos ***endpoints*** (puntos terminales). Se analizó solo las solicitudes cliente/servidor, de esta manera se identificó detalladamente las aplicaciones más importantes que son solicitadas por los empleados de este CDA.

Se organizó la estadística por las respuestas de los servidores. Siendo la primera columna las direcciones IPv4 de los servidores (Address A), en la columna siguiente se observan las direcciones IPv4 de los puestos de trabajo del CDA (Address B). De esta manera se visualizó todas las solicitudes cliente/servidor hechas por los empleados de la red LAN en este CDA hacia los distintos servidores.

A continuación se muestra las capturas de pantalla que reflejan de manera detallada las respuestas de los servidores a las solicitudes cliente de los empleados del CDA Los Dos Caminos.



Address A	Address B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B	Rel Start	Duration	bps A->B	bps A<-B
10.20.20.229	10.50.240.125	146	115678	65	38207	81	77471	2213.705681000	605,3818	504,90	1023,76
10.20.200.19	10.50.240.104	112	50892	57	34221	55	16671	1574.375610000	94,9740	2882,56	1404,26
10.20.200.19	10.50.240.114	383	276505	226	242400	157	34105	3121.027155000	157,7140	12295,67	1729,97
10.20.200.19	10.50.240.125	386	308525	221	274516	165	34009	4890.574150000	54,6554	40181,37	4977,95
10.20.200.19	10.50.240.120	1653	1105915	950	888734	703	217181	768.399093000	3787,3031	1877,29	458,76
10.20.200.19	10.50.240.127	1916	1172041	961	854634	955	317407	1296.661987000	326,5714	20935,92	7775,50
10.20.200.19	10.50.240.100	2560	1923470	1528	1756587	1032	166883	32.716150000	3245,5798	4329,80	411,35
10.20.200.19	10.50.240.103	3007	1939022	1610	1441562	1397	497460	557.017901000	3718,4728	3101,41	1070,25
10.20.200.19	10.50.240.131	3121	1250178	1631	676311	1490	573867	532.592047000	4408,2140	1227,37	1041,45
10.20.200.19	10.50.240.102	4943	2821155	2583	2166934	2360	654221	512.360484000	1374,3530	12613,55	3808,17
10.20.200.19	10.50.240.116	4962	4552442	3087	4304735	1875	247707	4378.098239000	366,1722	94048,31	5411,81
10.20.200.19	10.50.240.111	8417	5768685	4588	4443950	3829	1324735	540.069885000	4288,7080	8289,58	2471,11
10.20.200.19	10.50.240.101	8645	5671902	4808	4635308	3837	1036594	520.886081000	4391,2626	8444,60	1888,47
10.20.200.19	10.50.240.121	8853	6025849	5066	5111130	3787	914719	523.692030000	4423,1918	9244,24	1654,41
10.20.200.19	10.50.240.108	9273	6877880	5425	5936885	3848	940995	513.290851000	4290,4758	11069,89	1754,57
10.20.200.19	10.50.240.123	9341	5992287	5319	5085240	4022	907047	523.836904000	4423,3314	9197,12	1640,48
10.20.200.19	10.50.240.112	9688	7249066	5488	6092904	4200	1156162	528.791552000	4412,7001	11046,12	2096,06
10.20.200.19	10.50.240.130	10233	7261929	5807	6046609	4426	1215320	1389.367022000	3549,8361	13626,79	2738,88
10.20.200.19	10.50.240.113	11770	8473193	6825	7218618	4945	1254575	552.650160000	4356,5009	13255,81	2303,82
10.20.200.19	10.50.240.105	15606	10097964	8635	7940830	6971	2157134	525.178138000	4412,3668	14397,41	3911,07
10.21.12.87	10.50.240.1	1142	89180	636	38204	506	50976	512.272247000	2099,7968	145,55	194,21

Imagen 4.4.3 Respuesta del servidor con dirección IPv4 10.20.200.19

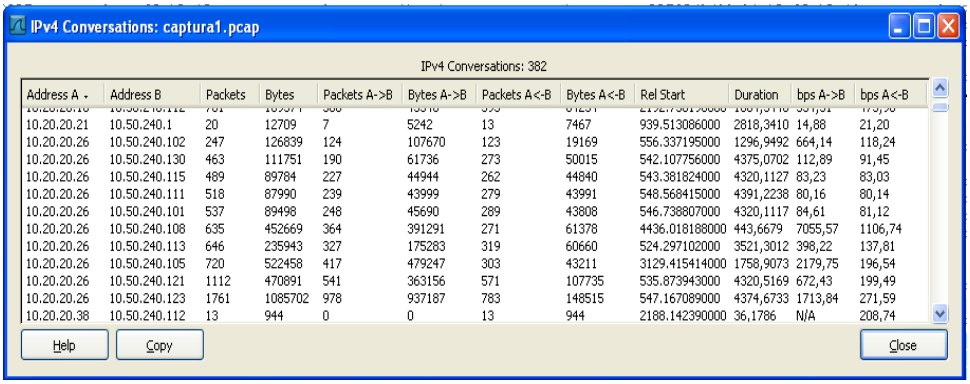


Imagen 4.4.4 Respuesta del servidor con dirección IPv4 10.20.20.26

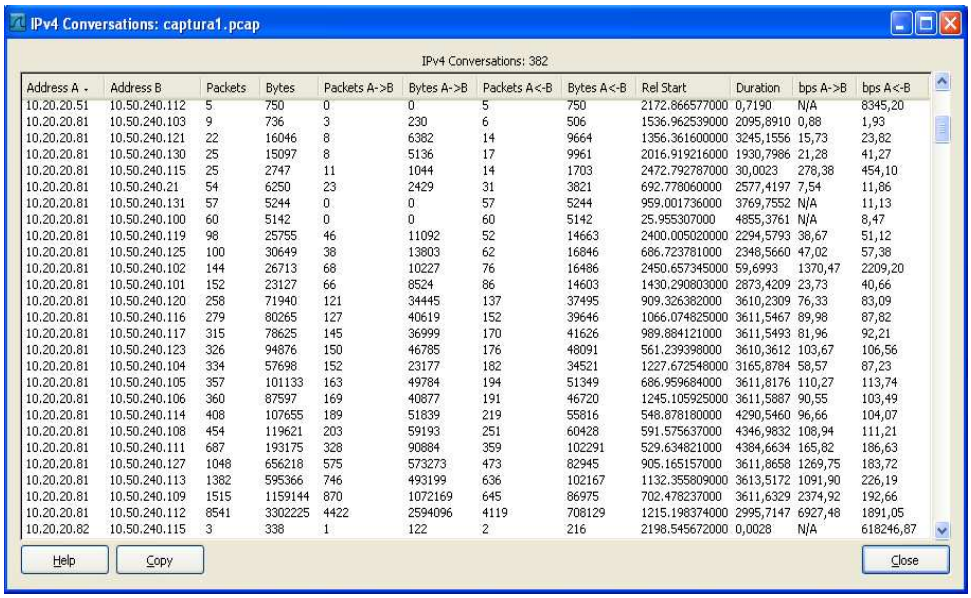


Imagen 4.4.5 Respuesta del servidor con dirección IPv4 10.20.20.81

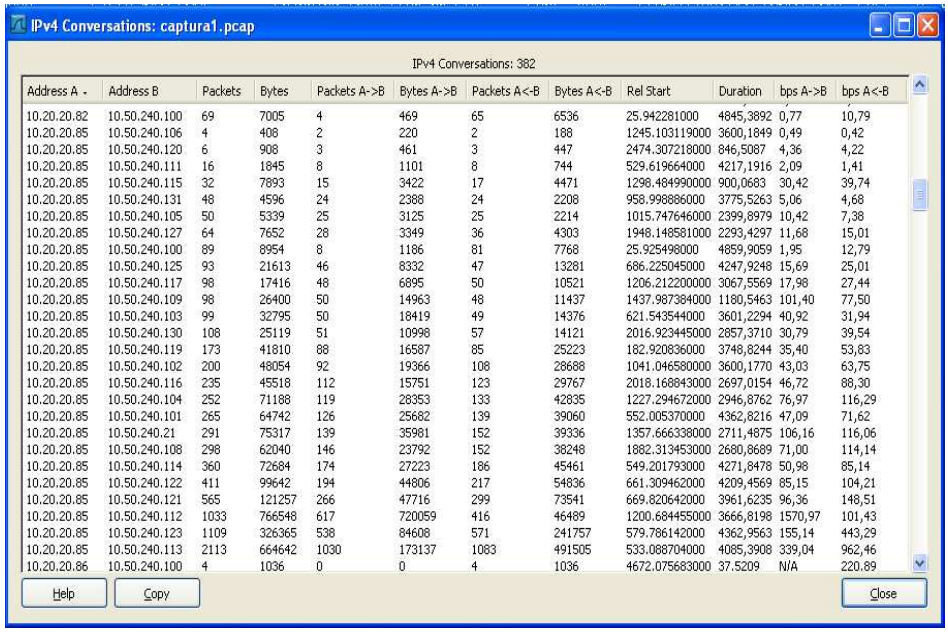


Imagen 4.4.6 Respuesta del servidor con dirección IPv4 10.20.20.85

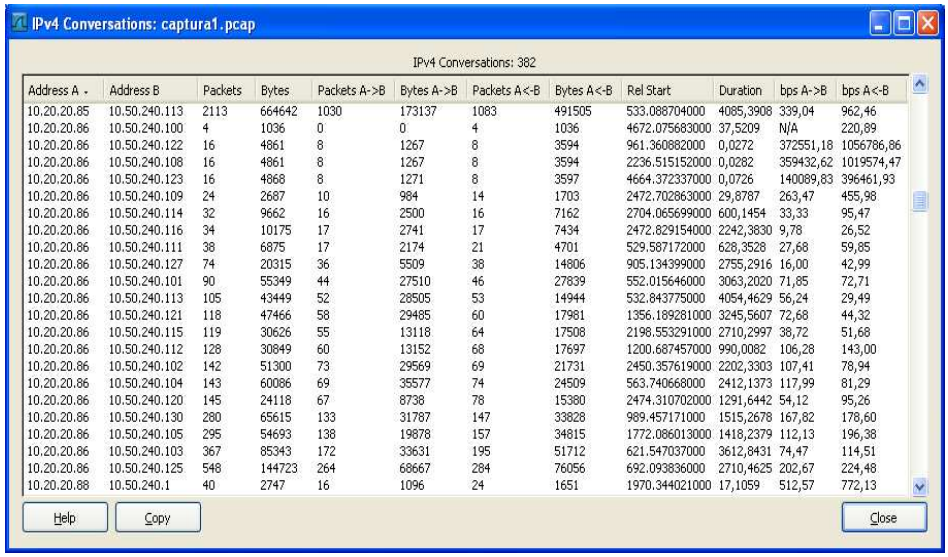


Imagen 4.4.7 Respuesta del servidor con dirección IPv4 10.20.20.86

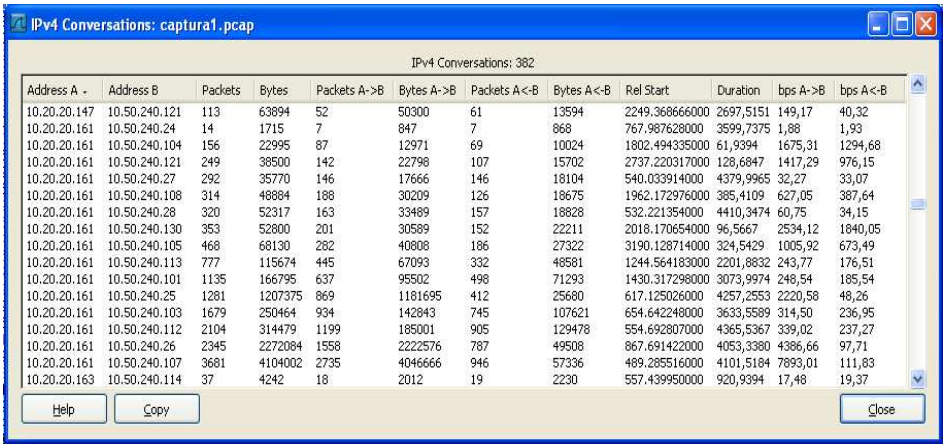


Imagen 4.4.8 Respuesta del servidor con dirección IPv4 10.20.20.161

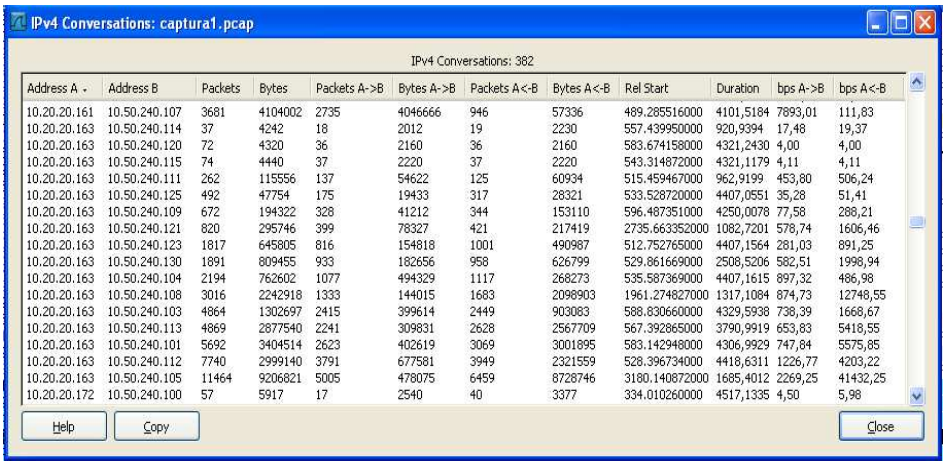


Imagen 4.4.9 Respuesta del servidor con dirección IPv4 10.20.20.163

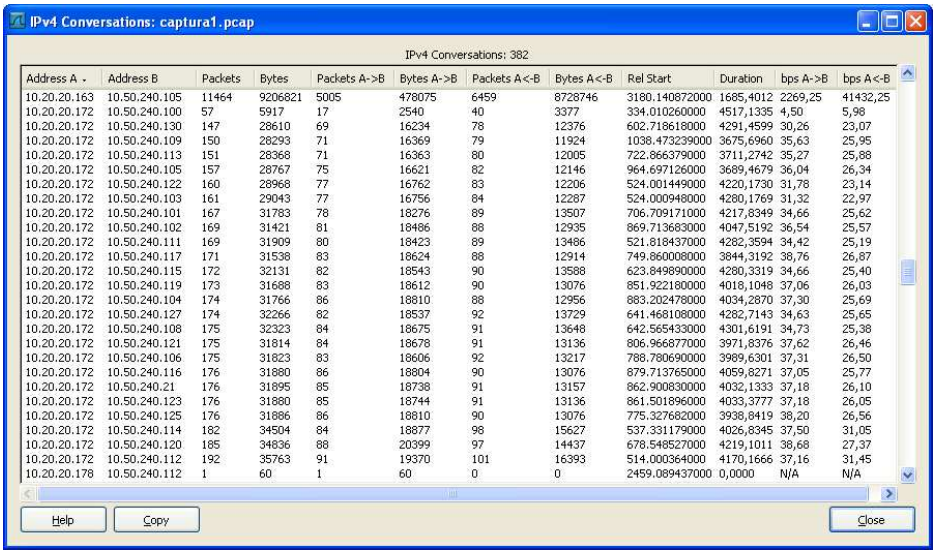


Imagen 4.4.10 Respuesta del servidor con dirección IPv4 10.20.20.172

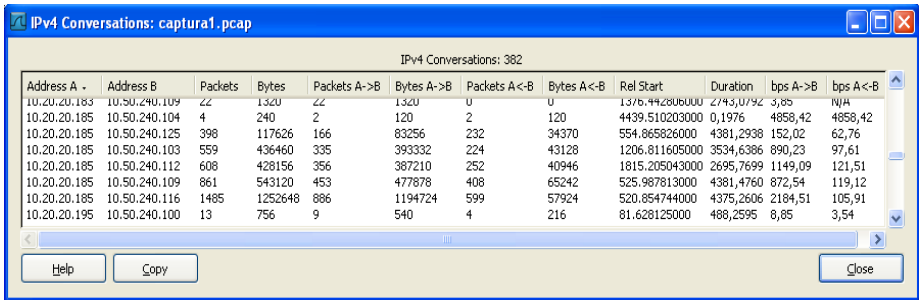


Imagen 4.4.11 Respuesta del servidor con dirección IPv4 10.20.20.185

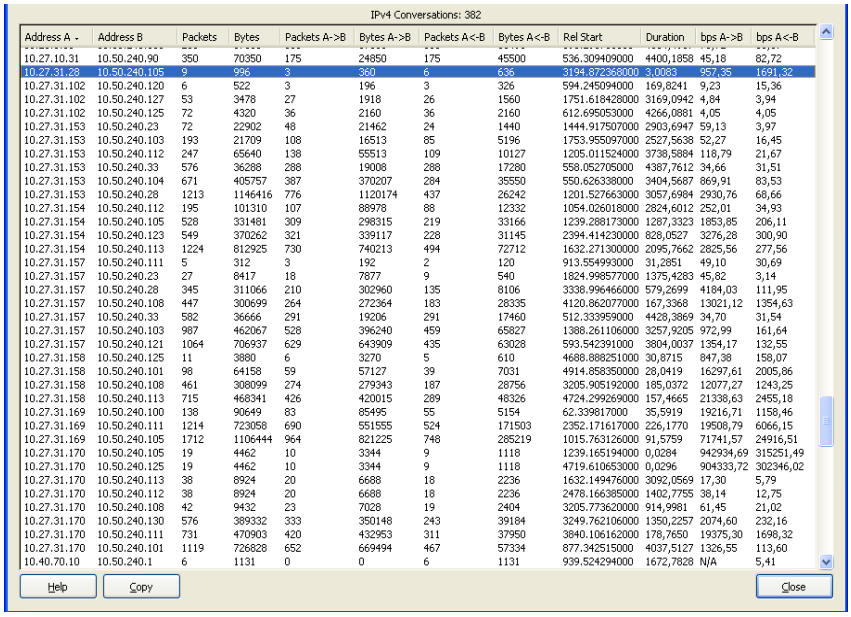


Imagen 4.4.12 Respuesta de los servidores con dirección IPv4 10.27.31.28, 10.27.31.102, 10.27.31.153, 10.27.31.154, 10.27.31.157, 10.27.31.158, 10.27.31.169 y 10.27.31.170

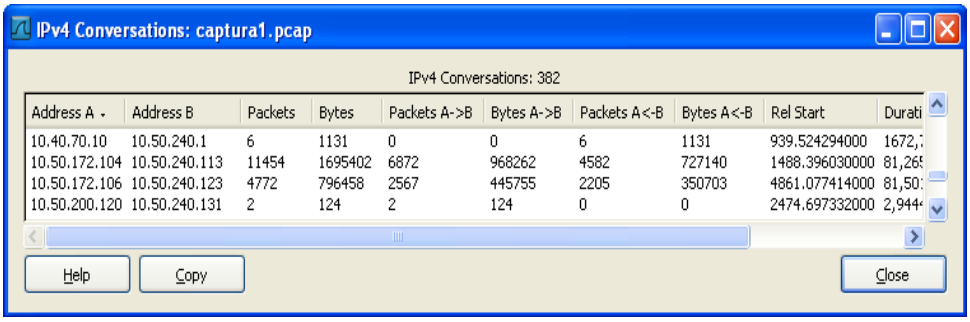


Imagen 4.4.13 Respuesta de los servidores con dirección IPv4 10.50.172.104 y 10.50.172.106

Al observar el gran número de direcciones IPv4 de la red 10.50.240 /24 en la columna Address B para la mayoría de estas estadísticas se concluye que estos servidores son solicitados por los empleados del CDA en cada uno de los puestos de trabajo. De esta manera se confirma la apreciación inicial que cada puesto de trabajo genera el mismo tráfico, y así se logró obtener una muestra fiel del comportamiento del tráfico; asegurando que este comportamiento es semejante en cada uno de los CDA's existentes.

Finalmente, la captura realizada en este CDA sirvió como parámetro principal para el análisis y la identificación final del tráfico creado desde los distintos CDA's existentes en la red de Digitel. De la misma manera, la captura de tráfico que se logró sirvió como punto de partida para aplicar los mecanismos de calidad de servicio en las redes de los CDA's.

4.5 Análisis de los resultados de la captura de tráfico

4.5.1 Identificación final del tráfico de las aplicaciones

Para identificar a cuales aplicaciones pertenece cada una de estas direcciones IPv4 obtenidas de las estadísticas ***Endpoints*** y ***IPv4 Conversations*** simplemente se utilizó la utilidad ***ping –a desde la consola de líneas de comandos para Windows XP.*** Esta utilidad permite (además de comprobar el estado de la conexión con equipos remotos) resolver la dirección del destino en nombres de dominio.

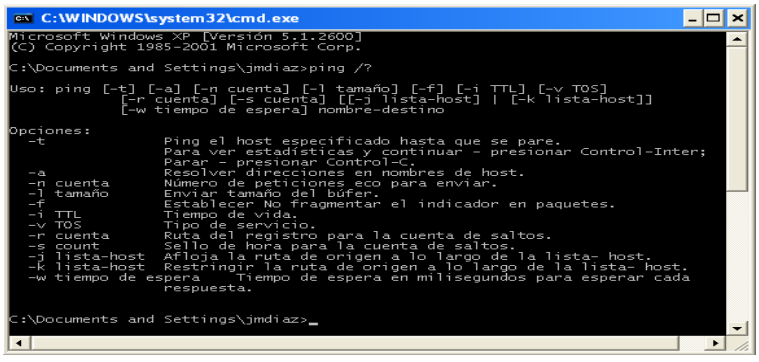


Imagen 4.5.1 Menú principal de la utilidad ping

Se conectó una laptop en una de las redes LAN de usuarios corporativos de la sede de Chuao-Cubo Negro, se hizo las pruebas ping –a. La siguiente tabla muestra los resultados obtenidos, así como también se muestra una imagen de referencia de una de las pruebas logradas.

Dirección IPv4	Nombre de dominio	Tipo de Servidor
10.20.200.19	cbn-isa-srv-010.digitelcorp.com.ve	Proxy
10.20.20.26	cbn-owa-srv-020.digitelcorp.com.ve	Outlook Web Access
10.20.20.185	cbn-mss-srv-050.digitelcorp.com.ve	Correo Electrónico
10.20.20.163	cbn-spa-srv-020.digitelcorp.com.ve	Files & Printers
10.20.20.161	cbn-spa-srv-030.digitelcorp.com.ve	
10.27.31.153	cssapapps1.digitelcorp.com.ve	SAP®
10.27.31.154	cssapapps2.digitelcorp.com.ve	
10.27.31.157	cssapapps3.digitelcorp.com.ve	
10.27.31.158	cssapapps4.digitelcorp.com.ve	
10.27.31.170	sapgrp.digitelcorp.com.ve	
10.27.31.28	Ninguno	
10.27.31.102		
10.27.31.169		
10.20.20.81	cbn-dom-srv-030.digitelcorp.com.ve	DNS
10.20.20.85	cbn-dom-srv-040.digitelcorp.com.ve	
10.20.20.86	cbn-dom-srv-020.digitelcorp.com.ve	
10.20.20.172	cbn-nav-srv-020.digitelcorp.com.ve	Norton Anti Virus
10.50.172.104	Ninguno	No identificado
10.50.172.106		

Tabla 4.5.1 Identificación de las direcciones IPv4 obtenidas de las estadísticas Endpoints y IPv4 Conversations mediante la utilidad ping –a

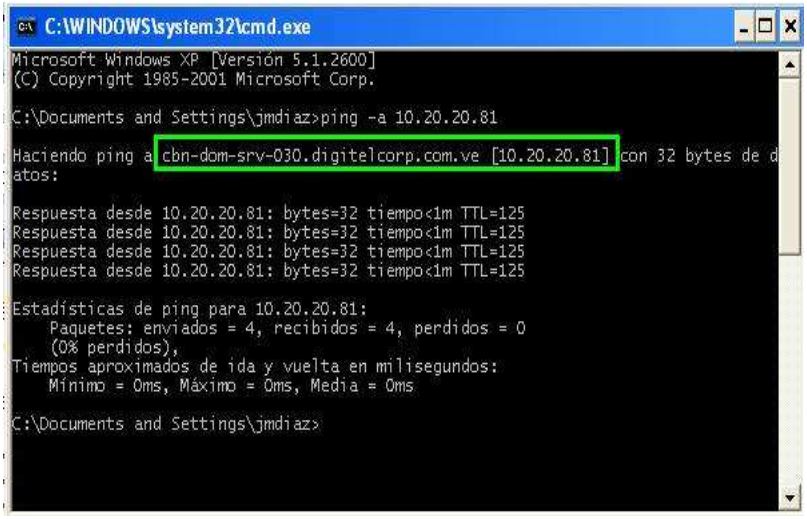


Imagen 4.5.2 Identificación de las direcciones IPv4 obtenidas de las estadísticas Endpoints y IPv4 Conversations mediante la utilidad ping –a

Se tienen las siguientes afirmaciones de la relación entre los resultados de la tabla 4.5.1 y varias entrevistas realizadas con el personal de la Coordinación de Redes:

- La dirección 10.20.200.19 pertenece al ***servidor Proxy*** de la red de la región Capital, este servidor permite el acceso a Internet y la comunicación de forma indirecta con las aplicaciones WEB requeridas por los empleados de los CDA's. Es importante señalar que solo los gerentes y supervisores de los CDA's tienen permitido el acceso a Internet, los demás puestos de trabajo tienen bloqueado el acceso a Internet y solo pueden hacer solicitudes a las aplicaciones WEB descritas en la tabla 4.3.1. Entonces, el tráfico generado hacia el servidor Proxy casi en su totalidad desde un CDA proviene de una solicitud a una aplicación WEB de la empresa, la cual pasa primero por el servidor Proxy, este analiza la solicitud y luego pasa la comunicación al servidor final que aguarda la aplicación solicitada desde el CDA. ***Esto significa que todo el tráfico de las aplicaciones utilizadas en los CDA's (con expeción de SAP®) apunta primero a la dirección del servidor Proxy.***

- La direcciones 10.20.20.26 y 10.20.20.185 pertenecen al ***servidor OWA (Outlook® Web Access) y al servidor de correo Microsoft® Outlook®*** respectivamente. El servidor OWA permite a los empleados de la corporación revisar sus correos configurados en ***Microsoft® Office® Outlook®*** vía Internet. En este caso en particular, son los usuarios internos de la red de la empresa que en ocasiones especiales utilizan esta herramienta. ***Entonces, debido a que es necesario salir a Internet para hacer uso de la herramienta, la comunicación se inicia con el servidor Proxy, este da la salida a Internet y luego establece la comunicación con el servidor OWA que archiva los correos.***
- El conjunto de direcciones 10.27.31.28, 10.27.31.102, 10.27.31.153, 10.27.31.154, 10.27.31.157, 10.27.31.158, 10.27.31.169 y 10.27.31.170 pertenecen a la red ***10.27.31.0 /24***, la cual esta asignada a servidores de la aplicación SAP®. ***Es decir, cualquier solicitud a una dirección perteneciente a la red 10.27.31.0 /24 esta asociada a una solicitud a la aplicación SAP®.***
- Las direcciones 10.20.20.81, 10.20.20.85 y 10.20.20.86 son direcciones de los ***servidores DNS (Domain Name System) primario, secundario y local respectivamente.*** Estos servidores se encargan de traducir nombres de dominio, como por ejemplo ***www.google.co.ve***, en direcciones IP.
- Las direcciones 10.20.20.161 y 10.20.20.163 pertenecen a los ***servidores Files & Printers*** de la región Capital. ***Es decir, cualquier solicitud de impresión, para buscar archivos en carpetas compartidas de red o en servidores FTP esta controlada por estos servidores.***
- Las direcciones 10.20.20.172, 10.50.172.104 y 10.50.172.106 no se asociaron a ninguna de las aplicaciones importantes. ***Por ende, este tráfico se sumó al considerado del tipo Mejor Esfuerzo y no se le aplicó políticas de QoS.***

4.5.2 Clasificación del tráfico según su tipo y creación de la Matriz de las aplicaciones

Una vez identificado el tráfico más importante en base a las afirmaciones anteriores, se procedió a clasificarlo según su tipo y se generó la matriz de servicios basada en el tipo de tráfico.

Se clasificó el tráfico de la siguiente manera:

1. **Premium:** La aplicación SAP® es considerada de alta criticidad, aunque no genera gran volumen de tráfico, es primordial asignarle una porción de ancho de banda exclusivo. Esta aplicación tiene como direcciones de destino las pertenecientes a la red ***10.27.31.0 /24***.
2. **Gold:** Incluye todas las aplicaciones WEB descritas en la tabla 4.3.1, además del tráfico de Internet exclusivo para los gerentes y supervisores de los CDA's. Estas aplicaciones tienen como dirección destino la ***10.20.200.19*** perteneciente al ***servidor Proxy*** y las direcciones ***10.20.20.81, 10.20.20.85 y 10.20.20.86*** pertenecientes a los ***servidores DNS***. Esta clase genera el mayor volumen de tráfico desde los CDA´s.
3. **Silver:** Está conformado por las solicitudes referentes a archivos e impresoras (Files & Printers) y correo electrónico. Tienen como direcciones destino ***10.20.20.26, 10.20.20.185, 10.20.20.161 y 10.20.20.163*** respectivamente.
4. **Bronze:** Esta conformando por el resto del tráfico en la red.

Observaciones:

- Dentro de las clases Premium y Gold ubicamos el considerado como tráfico ***medular***.
- Dentro de la clase Silver ubicamos el considerado como tráfico ***corporativo***.
- Dentro de la clase Bronze ubicamos el considerado como tráfico de ***gestión***.

- El tráfico de la clase bronze es considerado como del tipo ***Mejor Esfuerzo***, esta clase no goza de políticas de QoS.

Finalmente, para la creación de la matriz de las aplicaciones se necesitó calcular el porcentaje de tráfico utilizado por cada una de las clases definidas. En base a las tablas 4.4.1 y 4.5.1 se calculó este porcentaje de la siguiente manera:

1. Se calculó los porcentajes de los paquetes recibidos y transmitidos por los servidores tomando como 100 % el total de los paquetes capturados (267504 paquetes capturados). Así mismo, se hizo un promedio entre paquetes transmitidos y recibidos. En este sentido, la cantidad de paquetes transmitidos es similar a la de paquetes recibidos, debido a que son solicitudes cliente servidor, la otra mitad de los paquetes son generados por los empleados del CDA.

IPv4	Paquetes RX	Porcentaje de Paquetes RX (%)	Paquetes TX	Porcentaje de Paquetes TX (%)	Promedio entre Paquetes TX y RX	Porcentaje del promedio de Paquetes TX y RX (%)
10.20.200.19	50054	18,71	64815	24,22	57434,5	21,47
10.20.20.163	24612	9,20	21364	7,98	22988	8,59
10.20.20.81	8379	3,13	8631	3,22	8505	3,17
10.27.31.28, 10.27.31.102, 10.27.31.153, 10.27.31.154, 10.27.31.157, 10.27.31.158, 10.27.31.169, 10.27.31.170.	6782	2,53	9214	3,44	7998	2,98
10.20.20.161	5575	2,08	9593	3,58	7584	2,83
10.50.172.104	4582	1,71	6872	2,56	5727	2,14
10.20.20.85	4111	1,53	3999	1,49	4055	1,51
10.20.20.26	3473	1,29	3655	1,36	3564	1,33
10.50.172.106	2205	0,82	2567	0,95	2386	0,89
10.20.20.172	2172	0,81	1968	0,73	2070	0,77
10.20.20.185	1717	0,64	2128	0,79	1922,5	0,71
10.20.20.86	1429	0,53	1305	0,48	1367	0,51
Total	***115091***	***42,98***	***136111***	***50,8***	***125601***	***46,90***

Tabla 4.5.2 Porcentaje de paquetes enviados y recibidos por los servidores

IPv4	Paquetes RX	Porcentaje de Paquetes RX (%)	Paquetes TX	Porcentaje de Paquetes TX (%)	Promedio entre Paquetes TX y RX	Porcentaje del promedio entre Paquetes TX y RX (%)
10.50.240.0 /24	***152413***	***57,02***	***131393***	***49,02***	***141903***	***53.1***

Tabla 4.5.3 Porcentaje de paquetes enviados y recibidos por la red LAN 10.50.240.0 /24

2. Debido a que casi la totalidad de las solicitudes ocurren entre los empleados de los CDA y los servidores del nodo Región Capital, se utilizó como referencia el promedio entre paquetes transmitidos y paquetes recibidos para calcular el número de paquetes por clase de tráfico y en función de estas cifras estimar el ancho de banda requerido por cada una de las clases definidas. Para lograr una precisión más acertada se tomó como el 100 % de los paquetes el promedio entre paquetes recibidos y transmitidos (125601), y agrupando las direcciones de los servidores por su clase se hizo el cálculo en cuestión.

Clase	Dirección IPv4 de servidor	Promedio entre Paquetes TX y RX por servidor	Número de paquetes por clase de tráfico	Porcentaje de Ancho de banda requerido por clase de tráfico
Premium	10.27.31.28, 10.27.31.102, 10.27.31.153, 10.27.31.154, 10.27.31.157, 10.27.31.158, 10.27.31.169, 10.27.31.170.	7998	7998	6,37 %
Gold	10.20.200.19	57434,5	71361	56,81 %
	10.20.20.81	8505		
	10.20.20.85	4055		
	10.20.20.86	1367		
Silver	10.20.20.163	22988	36058,5	28,71 %
	10.20.20.161	7584		
	10.20.20.26	3564		
	10.20.20.185	1922,5		
Bronze	Resto de las direcciones del tráfico en la red	10183		Ninguno
Total		***125601***		***100 %***

Tabla 4.5.4 Cálculo del porcentaje de ancho de banda requerido por clase de tráfico

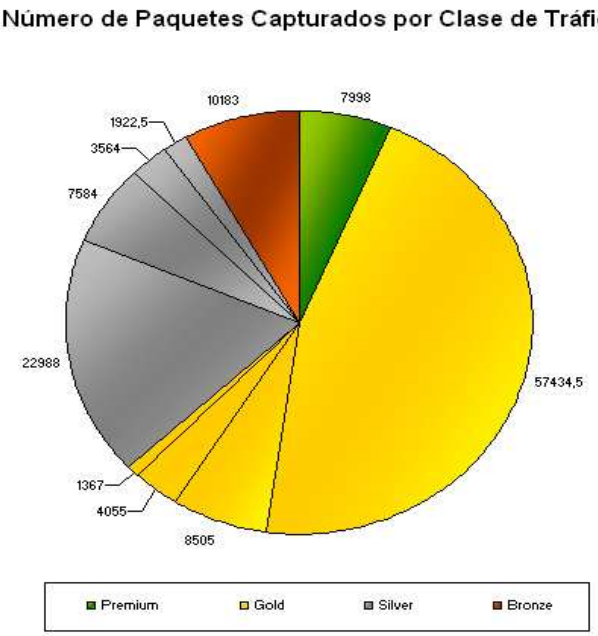


Gráfico 4.5.1 Número de paquetes capturados por clase de tráfico

3. Finalmente se agruparon las aplicaciones en una matriz donde se describe la clase de tráfico, las aplicaciones asociadas a esa clase de tráfico, el ancho de banda asignado por cada clase de tráfico. En base a esta matriz se aplicaron los mecanismos de QoS más idóneos para la red de estudio.

Clase	Nivel de Prioridad	Aplicaciones Asociadas	Ancho de banda Asignado por clase de tráfico
Premium	1 / 4	SAP®	7 %
Gold	2 / 4	Siebel®, SIR, Intranet de Ventas y Atención al Cliente, Administrador de Aprovisionamiento BlackBerry®, Reporte de IMEI, SCF, Portal de Activaciones, Módulo de Servicio Técnico, Administrador BlackBerry® Internet Services, Digimatic, Internet.	57 %
Silver	3 / 4	Files & Printers, Correo electrónico, Outlook Web Access	29 %
Bronze	4 / 4	Ninguna en específico	7 %

Tabla 4.5.6 Matriz final de las aplicaciones en las redes de los CDA's

Observación: Para la clase bronze no se asignó una porción de ancho de banda por ser esta la clase menos prioritaria, más bien este ancho de banda es producto del restante de la asignación a las demás clases de tráfico con prioridad mayor.

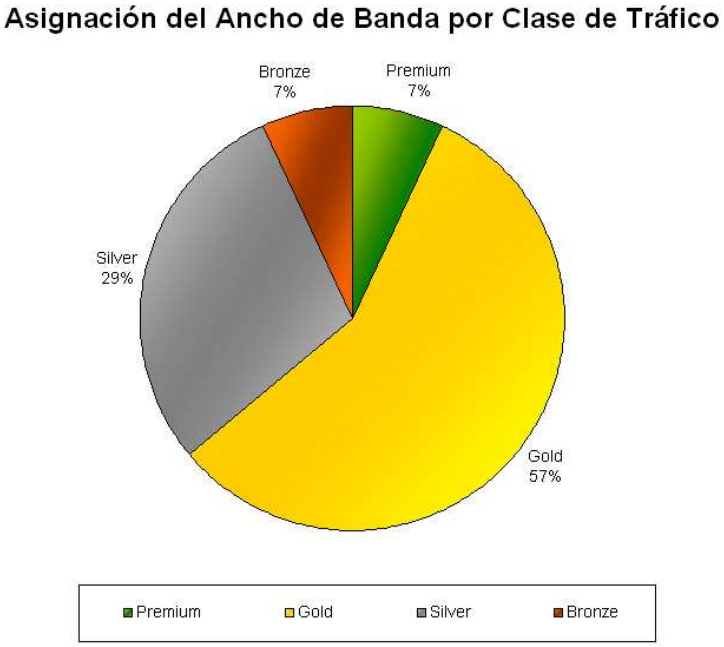


Gráfico 4.5.2 Asignación del Ancho de Banda por Clase de Tráfico

CAPÍTULO V

5. PLANTEAMIENTO DEL NUEVO MODELO DE RED BASADO EN POLÍTICAS DE QOS

5.1 Mecanismo de aplicación de QoS

5.2 Planteamiento de la arquitectura de red a implementar

5.3 Aplicación de la arquitectura de red propuesta bajo ambiente de prueba piloto

5. PLANTEAMIENTO DEL NUEVO MODELO DE RED BASADO EN POLÍTICAS DE QOS

5.1 Mecanismo de aplicación de QoS

La aplicación de los mecanismos de QoS descritos a continuación en la red de estudio se hizo con la finalidad de dedicar una porción de ancho de banda a cada una de las clases de tráfico definidas en el capítulo IV. De esta manera se permite el tráfico de las aplicaciones a través de canales diferenciados en cada uno de los enlaces. Lo cual garantiza un tráfico confiable de los servicios en función del volumen generado por cada uno de los mismos. En esta oportunidad, la red de estudio está conformada por la plataforma WAN para las redes de los CDA's, que comprende los routers de Acceso de los CDA´s, los routers a nivel de Distribución y los routers principales del Core.

5.2 Planteamiento de la arquitectura de red a implementar

Se recomienda implementar una arquitectura de red basada en la diferenciación de servicios. El método a seguir se inicia con un análisis del tráfico que maneja la red de estudio, seguido por la identificación de los servicios más críticos para posteriormente clasificarlos y otorgarle niveles de prioridad a cada una de estas clases. Finalmente, se aplican los mecanismos de QoS que más se ajusten a estas necesidades de tráfico.

El análisis para la identificación de tráfico efectuado en el capítulo IV demostró que el tráfico de los servicios se divide en cuatro clases principales:

- Premium: Contiene el tráfico de la aplicación SAP®.
- Gold: Contiene el tráfico de las aplicaciones WEB utilizadas por los empleados en los centros de atención y el tráfico de Internet permitido. Como por ejemplo: Siebel®, SIR, Intranet de Ventas y Atención al Cliente, etc.

- Silver: Contiene el tráfico de correo electrónico y solicitudes de archivos e impresión.
- Bronze: Contiene el resto del tráfico que circula por la red.

A su vez, la priorización de estas clases de tráfico se realizó mediante el marcado para cada clase de los paquetes en el campo DSCP de 6 bits ubicado dentro del encabezado del paquete IPv4, resultando de la siguiente manera:

- Premium: Se otorgó el valor definido por AF11 = 001010 (10)
- Gold: Se otorgó el valor definido por AF21 = 010010 (18)
- Silver: Se otorgó el valor definido por AF31 = 011 010 (26)

Finalmente se aplicó como mecanismo de QoS la asignación de un porcentaje de Ancho de Banda exclusivo para cada clase. El análisis efectuado en el capítulo 4.5 demostró que el Ancho de Banda debe segmentarse de la siguiente manera:

- Clase Premium: Asignación del 7 % de Ancho de Banda
- Clase Gold: Asignación del 57 % de Ancho de Banda
- Clase Silver: Asignación del 29 % de Ancho de Banda
- Clase Bronze: No se le asigna Ancho de Banda debido a que es considerada como tráfico de Mejor Esfuerzo y no relevante

5.3 Aplicación de la arquitectura de red propuesta bajo ambiente de prueba piloto

Para la realización de las pruebas se utilizó el software de libre descarga ***GNS3***, esta herramienta es un emulador de redes gráfico que permite trabajar sobre topologías de redes con equipos Cisco. La gran utilidad que tiene esta herramienta es que permite trabajar sobre la imagen del sistema operativo de los equipos, de esta manera se tiene acceso total al equipo como si se estuviera conectado al mismo vía consola o de manera remota. Para mayor información acerca de esta herramienta se puede consultar el siguiente enlace: http://www.gns3.net/

Imagen 5.1 Interfaz gráfica de la página Web del emulador GNS3

El procedimiento que se siguió para la aplicación de QoS mediante la arquitectura DiffServ en un ambiente de pruebas piloto de la red de estudio fue el siguiente:

I. Se definió el dominio DiffServ dentro de la red, este dominio va a gozar de las ventajas de QoS.

El dominio DiffServ de la red se definió por la topología Acceso-Distribución-Core-Red de Servidores. Esta integrado por los enlaces entre los routers que conforman estos niveles de la red a nivel WAN.

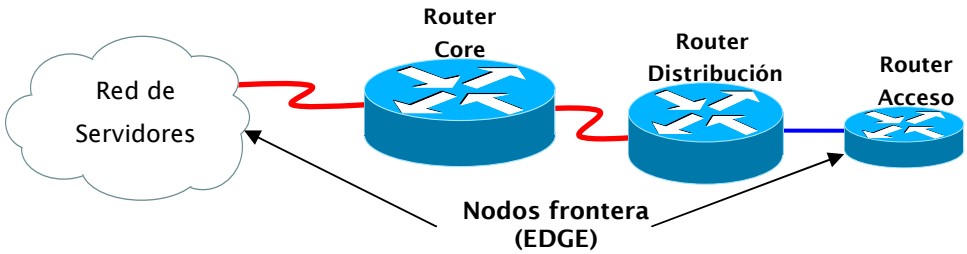


Figura 5.1 Dominio DiffServ definido en la red estudio. Nodos Frontera (EDGE)

Para las pruebas se montó en el GNS3 el enlace constituido entre el router de distribución del nodo Región Capital y el router de Acceso del

CDA Los Dos Caminos, se copiaron en estos equipos virtuales los archivos de configuración de los routers reales para ingresar solo las modificaciones necesarias. Esto para facilitar el trabajo de implementación si se decide aplicar la solución propuesta en esta investigación.

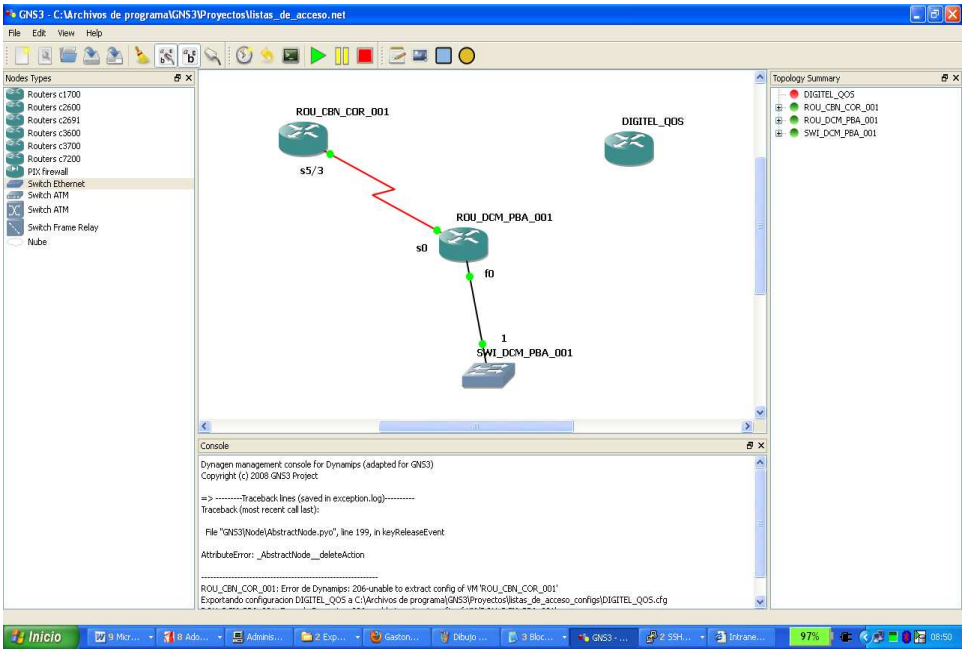


Imagen 5.2 Enlace montado sobre GNS3 conformado por el router de Distribución (ROU-CBN-05B-001) y el router de Acceso (ROU-DCM-PBA-001)

II. Una vez culminada la etapa de clasificación de tráfico, se continuó con el proceso de marcado y aplicación de las políticas de QoS en los Nodos EGDE del dominio DiffServ del ambiente de prueba

Este proceso permite organizar el flujo de paquetes entrantes en las clases ***Premium, Gold y Silver***. El proceso de marcado se puede lograr de muchas maneras, a continuación se ilustra el procedimiento escogido en esta prueba piloto. Se decidió utilizar la herramienta ACL (Access Control List o Lista de Control de Acceso) para filtrar el tráfico para cada clase. Para lograr esto, los routers de Acceso se tienen que configurar de la siguiente manera (***se recuerda que el procedimiento descrito a continuación es exclusivo para los routers CISCO***):

a) Se configuran las ACL's con las reglas necesarias. Las ACL's permiten filtrar paquetes a través diferentes formas, el filtrado permite o deniega el tráfico. ***Para este proceso de configuración se decidió hacer el filtrado para permitir el tráfico hacia los servidores mediante dirección IPv4 origen y destino***, para cada regla la dirección origen es toda la red designada al CDA y la dirección destino es la dirección del servidor o la dirección de la red destino. Se deben crear tantas reglas como direcciones de servidores destino y/o como tantas redes destino se tengan por clase. Por ejemplo, en la lista de acceso creada para la clase ***Silver*** se ingresaron cuatro reglas debido a que se tienen cuatro servidores destino (correo electrónico Outlook®, OWA y dos Files & Printers). Así mismo, la red de origen es la del CDA de Los Dos Caminos (10.50.240.0 /24). El último comando mostrado es para negar el tráfico con otros destinos.

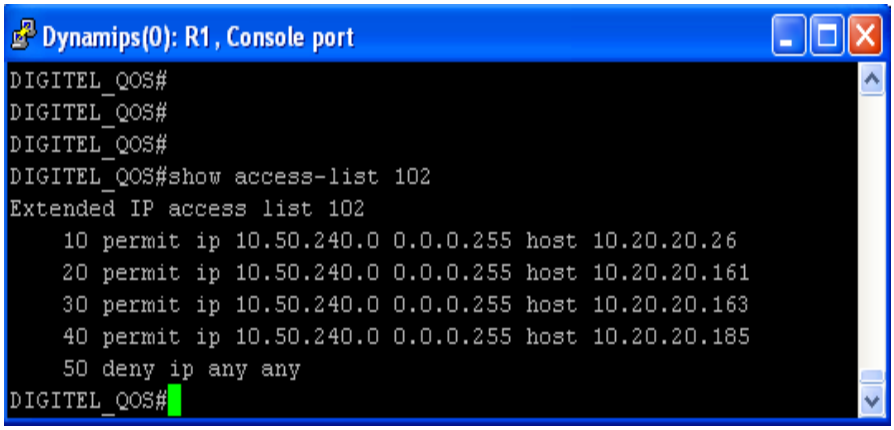


Imagen 5.3 Comando show access-list para la lista de acceso 102 creada en la clase Silver

A través del comando ***show access-list*** se verifican las listas de acceso creadas para el proceso de marcado de tráfico.

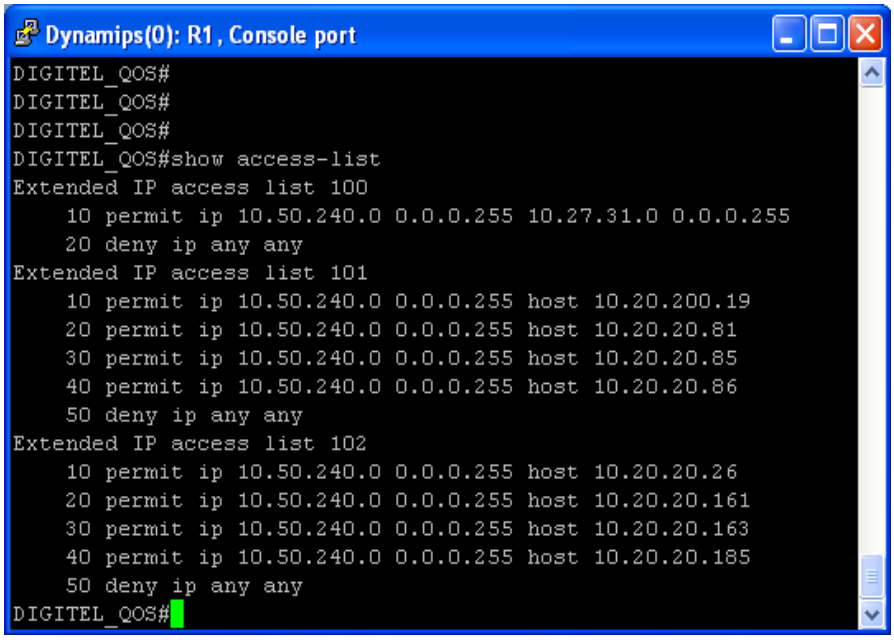


Imagen 5.4 Comando show access-list para las listas de acceso creadas

La lista 100 pertenece a la clase Premium, la lista 101 a la clase Gold y la lista 102 a la clase Silver.

Observación: *En los routers donde se conectan los servidores se configuran las ACL's de forma invertida, es decir, colocando como direcciones de origen la de los servidores y como dirección de destino las redes de los CDA's.*

b) Se declaran las clases de tráfico en los routers EDGE. En esta oportunidad se definieron las clases ***Premium, Gold y Silver***.

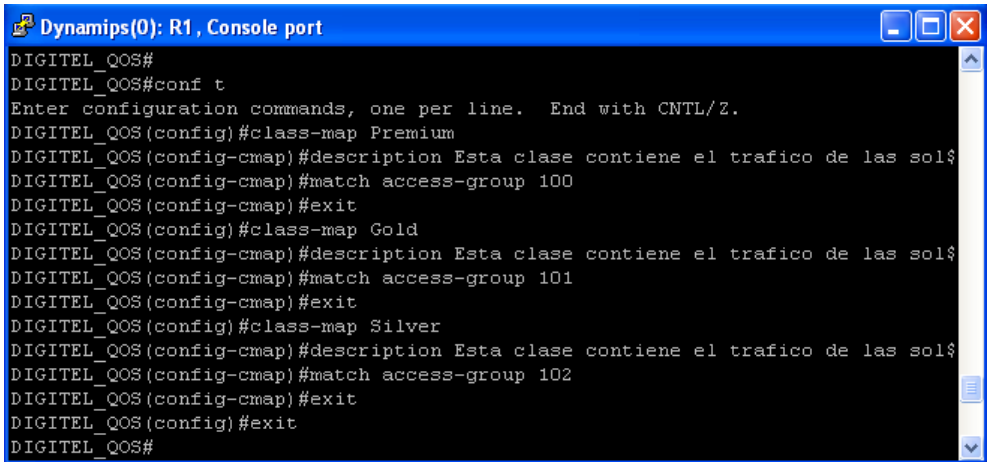


Imagen 5.5 Comandos para definir las clases de tráfico Premium, Gold y Silver

c) Se establecen las políticas de QoS marcando los paquetes que ingresan en los routers EDGE en el campo DSCP del encabezado del paquete IP para cada clase (***para mayor información consultar 2.4.4 Arquitectura Servicios Diferenciados o DiffServ***).

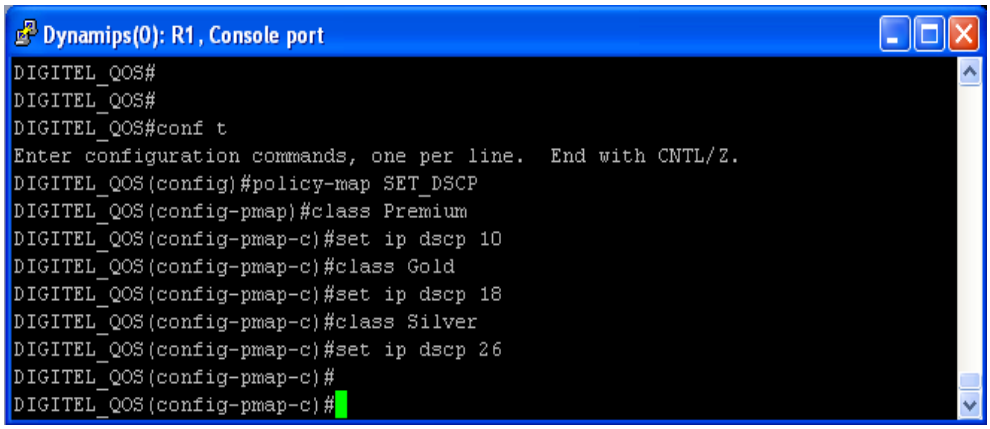


Imagen 5.6 Comandos para definir los valores en los campos DSCP del encabezado de los paquetes IPv4 para el marcado de las clases de tráfico

d) Una vez marcado el tráfico se procede a establecer la métrica del acuerdo del nivel de servicio alcanzado, en este caso se eligió como única métrica el ancho de banda, debido a que las otras métricas se consideraron despreciables en cuanto a relevancia en los requerimientos de la empresa (***para mayor información consultar***

2.4.2.1 Métricas SLA). Esto se logra redefiniendo unas nuevas clases de tráfico y aplicando las políticas de ancho de banda discutidas en 4.5.2.

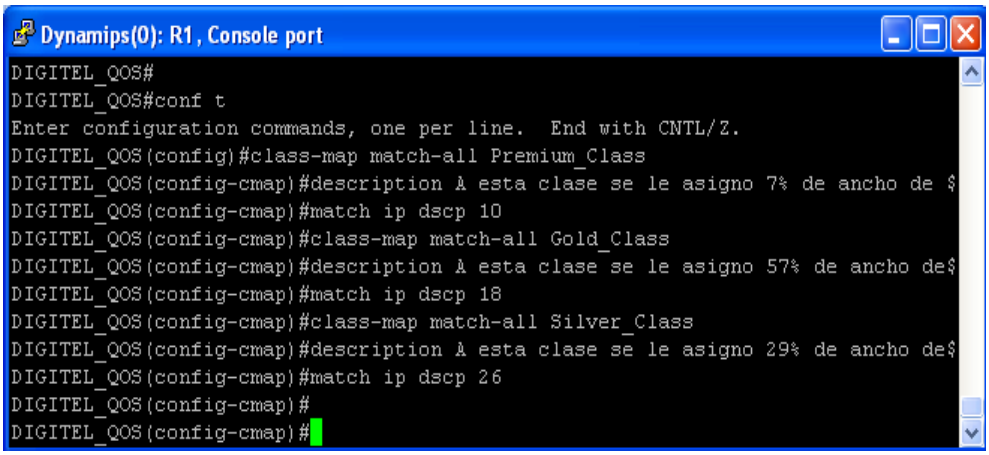


Imagen 5.7 Comandos para definir las clases de tráfico Premium_Class, Gold_Class y Silver_Class

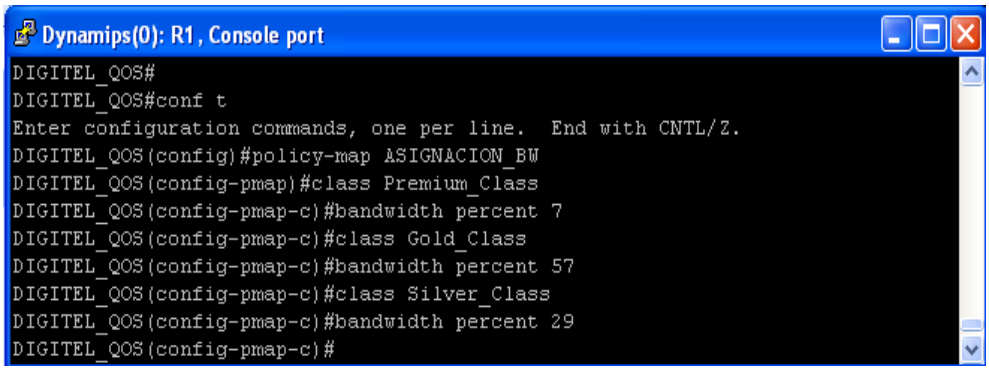


Imagen 5.8 Comandos para asignar los anchos de banda acordados en 4.5.2 para las clases de tráfico Premium_Class, Gold_Class y Silver_Class

A través del comando ***show class-map y show policy-map*** se verificaron las clases de tráfico creadas y las políticas de marcado utilizadas respectivamente.

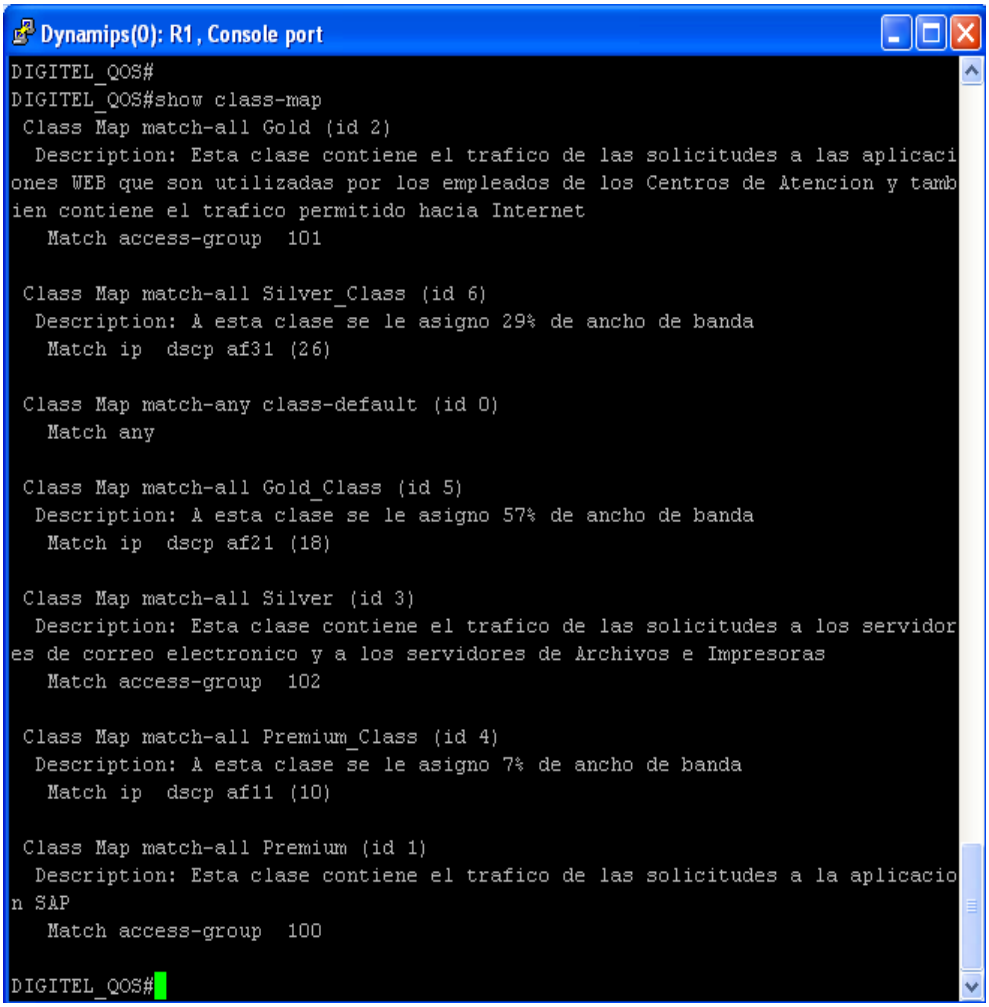


Imagen 5.9 Comando show class-map

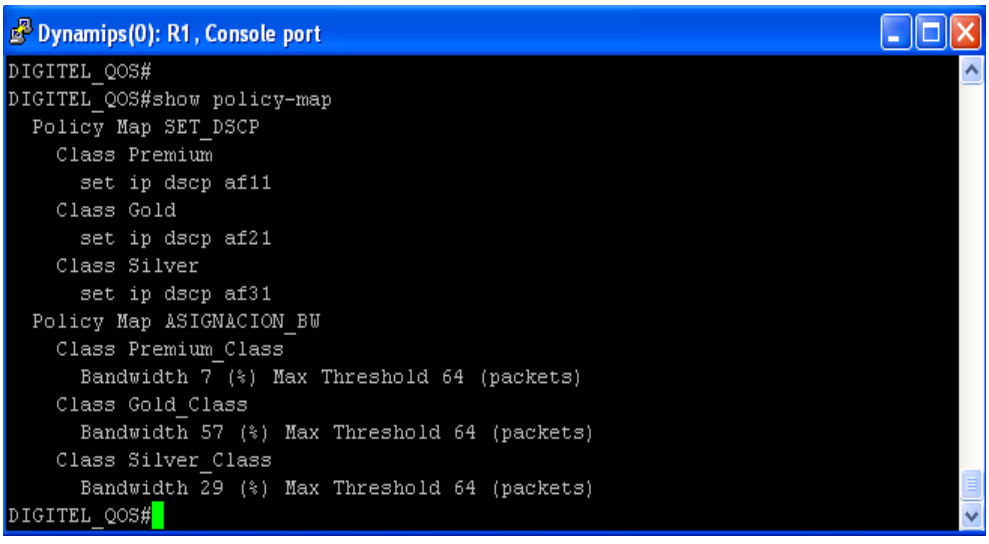


Imagen 5.10 Comando show policy-map

e) Finalmente, se aplican las políticas a través del comando ***service-policy input / service-policy output*** en las interfaces de cada router EDGE que conforma el dominio DiffServ. De la misma manera, se aplica el comando ***service-policy output*** en las interfaces de los routers de Distribución y de los routers del Core. Para la topología de prueba se aplicaron los comandos en las interfaces f0/0 y s1/0 del router ROU-DCM-PBA-001 y en la interfaz s5/3 del router ROU-CBN-05B-001 respectivamente.

De esta manera se completa la configuración de la arquitectura propuesta, definiendo completamente las configuraciones en la frontera del dominio DiffServ, así como también las configuraciones necesarias para el tratamiento de los paquetes marcados en los routers que constituyen el interior del dominio DiffServ, logrando de manera definitiva aplicar QoS en toda la red de los CDA's.

Es preciso resaltar que el método de encolamiento usado fue WFQ (Weighted Fair Queuin), este método de encolamiento es habilitado por defecto y no puede ser configurado por el administrador del router. En algunas instancias el sistema operativo de los routers Cisco habilita WFQ en lugar del otro método de encolamiento por defecto FIFO (First In First Out). Este proceso de encolamiento, verifica el patrón del tráfico basado en el tamaño de los paquetes y la naturaleza del tráfico, para distinguir el tráfico interactivo.

En los anexos se pueden consultar el comando ***show running-config*** que se configuró en los routers de la topología de prueba. Se expone a manera de analizar los comandos y los aspectos importantes a tomar en cuenta para el momento de configurar DiffServ en cualquier red particular que sea objeto de estudio.

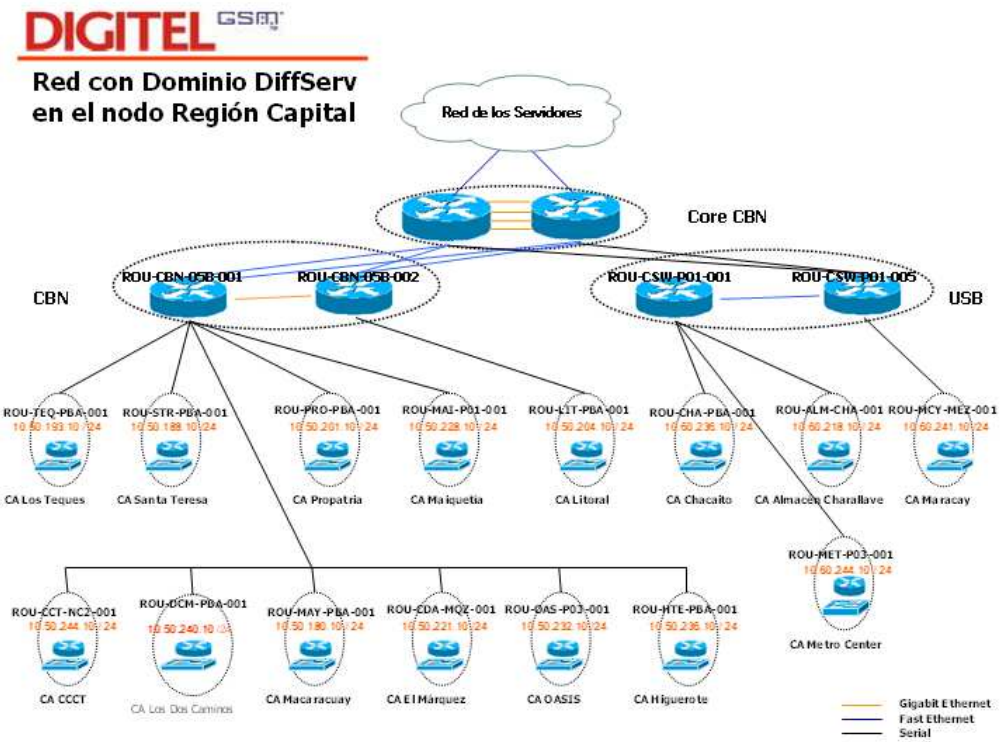


Figura 5.2 Red con Dominio DiffServ en el nodo Región Capital

CONCLUSIONES Y RECOMENDACIONES

Como se evidenció, el proceso para aplicar QoS de manera tipificada viene dado en función de las necesidades de cada red en específico. Por lo cual, si se requiere aplicar la arquitectura de Servicios Diferenciados o DiffServ (que permite optimizar el uso de ancho de banda disponible) de QoS en toda la red, es necesario levantar información de manera separada de cada subred para delimitar el dominio DiffServ de la red y seguir el procedimiento que en esta investigación se recomienda, el cual consiste en:

1. Identificar los servicios y aplicar un nivel de prioridad a cada uno de ellos
2. Clasificar los servicios en base a la priorización
3. Aplicar los mecanismos de QoS que más se adapten a las necesidades de la red

Para el caso de la Corporación Digitel C.A. y las redes de los Centros de Atención, se recomienda seguir el proceso descrito a continuación para todos los routers que conforman esta red, comenzando por la clasificación del tráfico:

- Premium: Contiene el tráfico de la aplicación SAP®.
- Gold: Contiene el tráfico de las aplicaciones WEB utilizadas por los empleados en los centros de atención y el tráfico de Internet permitido.
- Silver: Contiene el tráfico de correo electrónico y solicitudes de archivos e impresión.
- Bronze: Contiene el resto del tráfico que circula por la red.

Continuando con el marcaje de los paquetes en los routers EDGE:

- Premium: Otorgar el valor definido por AF11 = 001010 (10)
- Gold: Otorgar el valor definido por AF21 = 010010 (18)
- Silver: Otorgar el valor definido por AF31 = 011 010 (26)

Finalizando con la asignación de ancho de banda a cada clase:

- Clase Premium: Asignar del 7 % de Ancho de Banda
- Clase Gold: Asignar del 57 % de Ancho de Banda

- Clase Silver: Asignar del 29 % de Ancho de Banda
- Clase Bronze: No se asigna Ancho de Banda debido a que es considerada como tráfico de Mejor Esfuerzo y no relevante

Este proceso se realizó bajo un ambiente de simulación para el caso del Centro de Atención situado en Los Dos Caminos. Sin embargo, debido a que se reafirmó la percepción inicial, en la cual se suponía que el tráfico de las aplicaciones generado desde un CDA se equipara con cualquier tráfico generado desde otro CDA (se comporta de manera similar), entonces se puede adaptar la configuración realizada en esta prueba piloto y ejecutar las mismas reglas en todos los centros CDA a modo de aplicar QoS en todos los enlaces extremo a extremo que conforman la red entera de los CDA's, desde su nivel más bajo (Acceso) hasta su nivel más alto (Core), y de esta manera delimitar el dominio DiffServ que gozará de las bondades de la priorización de tráfico.

Por otro lado, el proceso de clasificación y marcado del tráfico de los servicios que transporta la red se recomienda hacerlo en base a la norma RFC 4594 titulada "Configuration Guidelines for DiffServ Service Classes", la cual fue publicada en agosto de 2006 por la IETF. Los autores de esta guía recomiendan usar este documento para definir una política de interoperabilidad y aplicar DiffServ de manera coherente, además describe como se deben configurar las clases de servicio mediante DiffServ y recomienda como se deben utilizar los Differentiated Service Code Points (DSCP's), acondicionadores de tráfico y Per Hop Behaviors (PHB's).

El software emulador de equipos reales *GNS3* utilizado en esta investigación para realizar las pruebas fue de gran ayuda; sobre todo en casos como el presentado donde es necesario realizar cambios importantes en la red que pueden afectar el funcionamiento de la misma. Para el caso de la Corporación Digitel C.A., que es una operadora prestadora de servicios de telecomunicaciones, los mismos se verían afectados si no se logran establecer las configuraciones de manera correcta. Por lo cual es importante montar un escenario simulado que

permita hacer las pruebas necesarias antes de hacer la implementación final, de esta manera se asegura acortar los tiempos de afectación de servicio al momento de realizar los controles de cambio que permiten colocar en producción la nueva arquitectura.

Sería interesante evaluar la posibilidad de unir los tipos de tráfico medular y de gestión en una sola clase, debido a que el tráfico de gestión es considerado igual o más importante que el tráfico medular de los servicios. Es trascendental que el tráfico de control se diferencie del resto del tráfico prioritario, a fin de garantizar la conectividad básica de la red todo el tiempo.

De la misma manera, la tecnología MPLS (Multi Protocol Label Switching), que aunque por sí misma no proporciona QoS, podría ser muy útil para realizar Ingeniería de tráfico y mejorar los servicios que requieran de bajo retardo como la voz y el video. MPLS actúa a nivel de enlace de red, proporcionando un método de envío rápido mediante la conmutación de etiquetas, evitando congestión en los nodos y la formación de colas de paquetes.

REFERENCIAS BIBLIOGRAFÍA

CISCO ©, Cisco Networking Academy, **Software Aplication Exploration Módulo 1**, 2008.

SRINIVAS, Vegesna, **IP Quality of Service**, Cisco Press, 2001.

3 EVANS, John, **Deploying IP and MPLS QoS for Multiservice Networks**, The Morgan Kaufmann Publishers, 2007.

PIERRE, Francois, **Achieving subsecond IGP convergence in large IP networks**, ACM SIGCOMM Computer Communication Review, 2005.

REFERENCIAS ELECTRÓNICAS

http://www.opalsoft.net/qos/Spanish-QOS.htm

http://www.cisco.com

http://www.huawei.com

http://www.cisco.com/en/US/products/hw/tsd_products_support_end-of-sale_and_end-of-life_products_list.html

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/release/notes/OL_4164.html#wp4072792

http://www.cisco.com/en/US/docs/ios/12_4/release/notes/124NEWF.html

http://www.cisco.com/en/US/prod/collateral/modules/ps4917/data_sheet_cisco_ubr7200_npe_g2_network_processing_engine.html

http://www.huawei.com/products/datacomm/catalog.do?id=3055

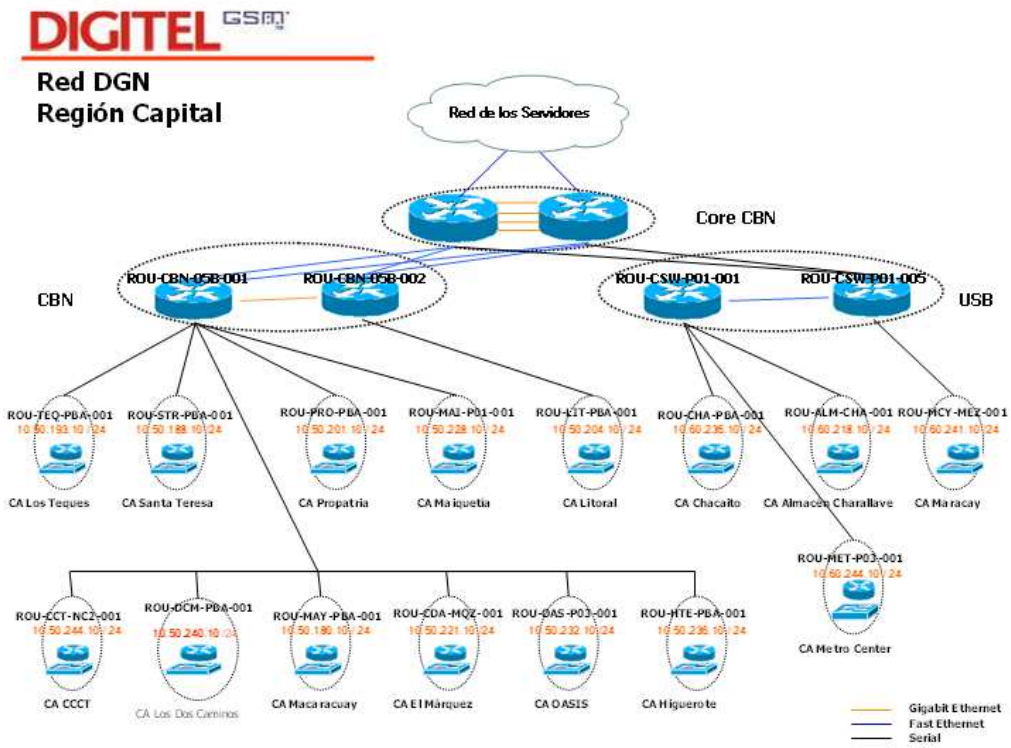
http://www.cisco.com/en/US/docs/ios/12_4/release/notes/124NEWF.html

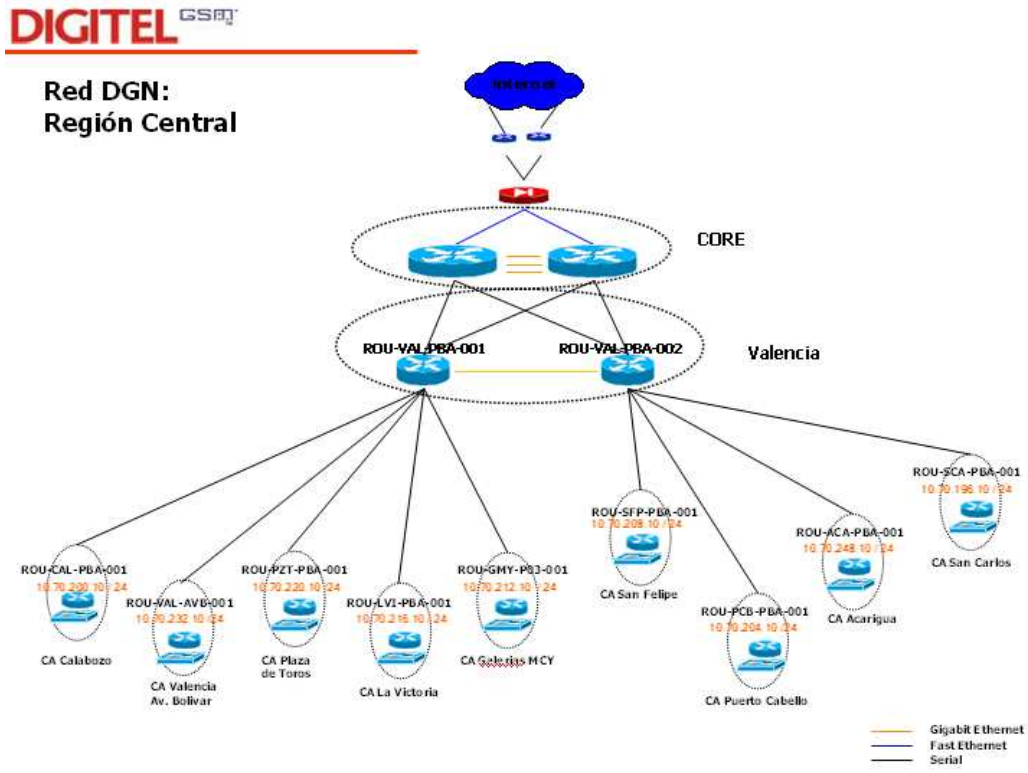
http://www.cisco.com/en/US/products/hw/routers/ps259/prod_eol_notice09186a008032d4c2.html#wp42613ç

http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/release/note/OL_5184.html#wp1987516

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/product_bulletin_c25_468195.html

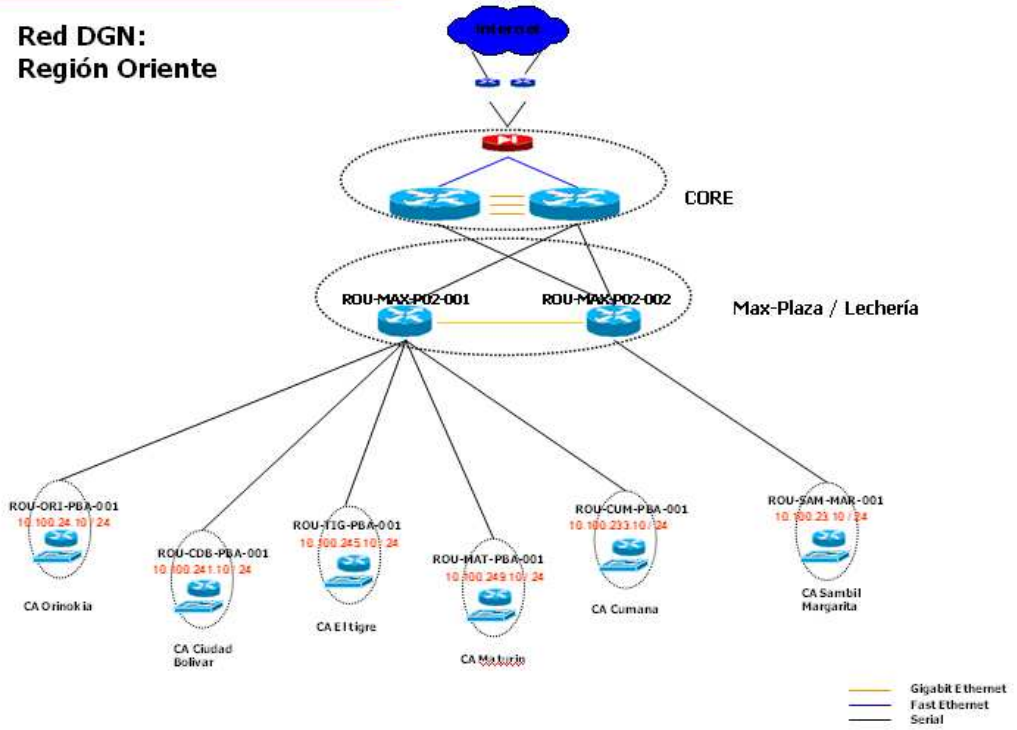
Esquemas de red de los nodos por Región





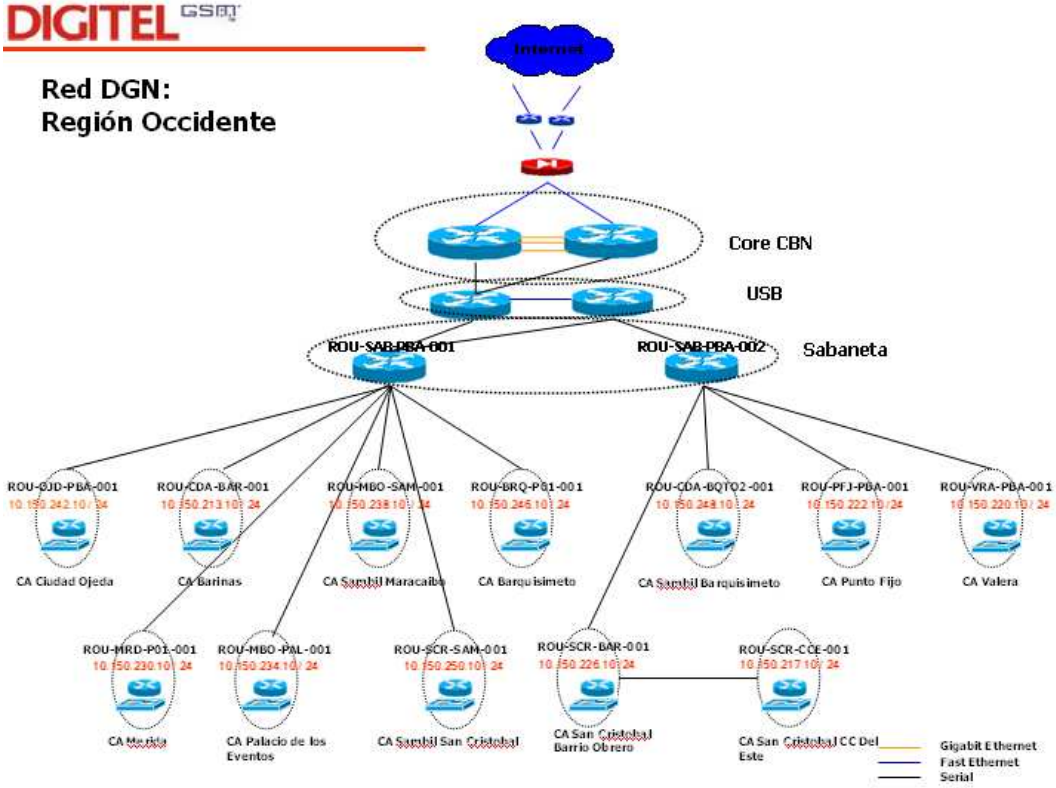
DIGITEL GSM

Red DGN:
Región Oriente



DIGITEL GSM

Red DGN:
Región Occidente



Comando show running-config del router de Distribución ROU-CBN-05B-001

```
ROU-CBN-05B-001#
ROU-CBN-05B-001#show running-config
Building configuration...

Current configuration : 11346 bytes
!
! Last configuration change at 01:29:56 VEN Sun Oct 4 2009
! NVRAM config last updated at 01:29:59 VEN Sun Oct 4 2009
!
version 12.3
service timestamps debug uptime
service timestamps log datetime localtime show-timezone
service password-encryption
!
hostname ROU-CBN-05B-001
!
boot-start-marker
boot-end-marker
!
(output omitted)
!
E1 6/6 to ROU-HTE-PBA-001 (E1 1/0)
!
controller E1 6/7
 channel-group 0 timeslots 1-31
 description Serial6/7:0 to ROU-BVC-PBA-001 (S0/0/0:0)
!
class-map match-any AutoQoS-VoIP-Remark
  match ip dscp ef
  match ip dscp cs3
class-map match-any AutoQoS-VoIP-Control-UnTrust
  match access-group name AutoQoS-VoIP-Control
class-map match-any AutoQoS-VoIP-RTP-UnTrust
  match protocol rtp audio
  match access-group name AutoQoS-VoIP-RTCP
!
```

```
class-map match-all Silver_Class
  description A esta clase se le asigno 29% de ancho de banda
 match ip dscp af31
class-map match-all Gold_Class
  description A esta clase se le asigno 57% de ancho de banda
 match ip dscp af21
class-map match-all Premium_Class
  description A esta clase se le asigno 7% de ancho de banda
 match ip dscp af11
!
!
policy-map ASIGNACION_BW
 class Premium_Class
  bandwidth percent 7
 class Gold_Class
  bandwidth percent 57
 class Silver_Class
  bandwidth percent 29
!
!
policy-map AutoQoS-Policy-UnTrust
  class AutoQoS-VoIP-RTP-UnTrust
   priority percent 70
   set dscp ef
  class AutoQoS-VoIP-Control-UnTrust
   bandwidth percent 5
   set dscp af31
  class AutoQoS-VoIP-Remark
   set dscp default
  class class-default
   fair-queue
!
!
!
!
interface Loopback0
 description Loopback0
 ip address 10.50.0.1 255.255.255.255
!
```

```
interface GigabitEthernet0/1
 description GigabitEhernet0/1 to ROU-CBN-05B-002 (GE0/1)
 bandwidth 200000
 ip address 10.50.251.1 255.255.255.252
 service-policy output ASIGNACION_BW
 no ip mroute-cache
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
 clns router isis
!
interface GigabitEthernet0/2
 description GEthernet0/2 to ROU-CBN-COR-001 (FE7/1)
 ip address 10.200.251.2 255.255.255.252
 ip load-sharing per-packet
 service-policy output ASIGNACION_BW
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
 clns router isis
!
interface GigabitEthernet0/3
 description GEthernet0/3 to ROU-CBN-COR-002 (FE7/2)
 ip address 10.200.251.14 255.255.255.252
 ip load-sharing per-packet
 service-policy output ASIGNACION_BW
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
 clns router isis
!
interface Serial5/0:0
 description Serial5/0:0 to ROU-MET-P03-001 (S1/1:0)
 bandwidth 2048
 ip address 10.50.251.9 255.255.255.252
 ip load-sharing per-packet
```

```
 service-policy output ASIGNACION_BW
!
interface Serial5/1:0
 description Serial5/1:0 to ROU-CCT-NC2-001 (S1/1:0)
 bandwidth 2048
 ip address 10.50.251.13 255.255.255.252
 ip load-sharing per-packet
 service-policy output ASIGNACION_BW
!
interface Serial5/2:0
 description Serial5/2:0 to ROU-OAS-P03-001 (S1/0:0)
 bandwidth 2048
 ip address 10.50.251.5 255.255.255.252
 ip load-sharing per-packet
 service-policy output ASIGNACION_BW
!
interface Serial5/3:0
 description Serial5/3:0 to ROU-DCM-PBA-001 (S1/0:0)
 bandwidth 2048
 ip address 10.50.251.25 255.255.255.252
 ip load-sharing per-packet
 service-policy output ASIGNACION_BW
 service-policy output AutoQoS-Policy-UnTrust
 auto qos voip
!
interface Serial5/4:0
 description Serial5/4:0 to ROU-MAI-P01-001 (S0/0/0:0)
 bandwidth 2048
 ip address 10.50.251.33 255.255.255.252
 service-policy output ASIGNACION_BW
!
interface Serial5/5:0
 description E1 S5/5:0 to ROU-BSC-LAT-001 0/0/0:0
 ip address 10.50.251.49 255.255.255.252
 clns router isis
!
(output omitted)
!
end
```

Comando show running-config del router de Distribución ROU-DCM-PBA-001

```
ROU-DCM-PBA-001#sh run
Building configuration...

Current configuration : 6050 bytes
!
! Last configuration change at 02:39:56 VEN Sun Oct 4 2009
! NVRAM config last updated at 02:39:59 VEN Sun Oct 4 2009
!
version 12.3
service timestamps debug uptime
service timestamps log datetime msec localtime
service password-encryption
!
hostname ROU-DCM-PBA-001
!
boot-start-marker
boot system flash c2800nm-entservicesk9-mz.123-14.T7.bin
boot-end-marker
!
(output omitted)
!
controller E1 0/0/1
 channel-group 0 timeslots 1-31
 description controller E1 0/0/1 to ROU-CBN-05B-002 (E1 5/2)
!
class-map match-any AutoQoS-VoIP-Remark
 match ip dscp ef
 match ip dscp cs3
 match ip dscp af31
class-map match-any AutoQoS-VoIP-Control-UnTrust
 match access-group name AutoQoS-VoIP-Control
class-map match-any AutoQoS-VoIP-RTP-UnTrust
 match protocol rtp audio
 match access-group name AutoQoS-VoIP-RTCP
!
```

```
!
!
class-map match-all Gold
 description Esta clase contiene el trafico de las
solicitudes a las aplicaciones WEB que son utilizadas
por los empleados de los Centros de Atencion y tambien
contiene el trafico permitido hacia Internet
 match access-group 101
class-map match-all Silver_Class
 description A esta clase se le asigno 29% de ancho de banda
 match ip dscp af31
class-map match-all Gold_Class
 description A esta clase se le asigno 57% de ancho de banda
 match ip dscp af21
class-map match-all Silver
 description Esta clase contiene el trafico de las
solicitudes a los servidores de correo electronico y a los
servidores de Archivos e Impresoras
 match access-group 102
class-map match-all Premium_Class
 description A esta clase se le asigno 7% de ancho de banda
 match ip dscp af11
class-map match-all Premium
 description Esta clase contiene el trafico de las
solicitudes a la aplicacion SAP
 match access-group 100
!
!
policy-map SET_DSCP
 class Premium
  set ip dscp af11
 class Gold
  set ip dscp af21
 class Silver
  set ip dscp af31
policy-map ASIGNACION_BW
 class Premium_Class
  bandwidth percent 7
 class Gold_Class
```

```
  bandwidth percent 57
 class Silver_Class
  bandwidth percent 29
!
policy-map AutoQoS-Policy-UnTrust
 class AutoQoS-VoIP-RTP-UnTrust
  priority percent 70
  set dscp ef
 class AutoQoS-VoIP-Control-UnTrust
  bandwidth percent 5
  set dscp af31
 class AutoQoS-VoIP-Remark
  set dscp default
 class class-default
  fair-queue
!
!
!
!
interface Loopback0
 description Loopback0
 ip address 10.50.0.5 255.255.255.255
!
interface FastEthernet0/0
 description FastEthernet0/0 to SWI-DCM-PBA-001 (Port 2/1)
 ip address 10.50.242.10 255.255.255.0 secondary
 ip address 10.50.240.10 255.255.255.0
 ip helper-address 10.20.20.85
 service-policy input SET_DSCP
 duplex full
 speed 100
 service-policy output AutoQoS-Policy-UnTrust
!
interface FastEthernet0/1
 bandwidth 2048
 no ip address
 ip access-group 100 in
 ip load-sharing per-packet
 shutdown
```

```
 duplex full
 speed 100
!
interface Serial0/0/0:0
 description Serial0/0/0:0 to ROU-CBN-05B-001 (S2/1:0)
 bandwidth 2048
 ip address 10.50.251.26 255.255.255.252
 ip load-sharing per-packet
 service-policy output ASIGNACION_BW
 service-policy output AutoQoS-Policy-UnTrust
!
interface Serial0/0/1:0
 description Serial0/0/1:0 to ROU-CBN-05B-002 (S5/2:0)
 bandwidth 2048
 ip address 10.50.251.22 255.255.255.252
 ip load-sharing per-packet
 service-policy output ASIGNACION_BW
 service-policy output AutoQoS-Policy-UnTrust
!
router ospf 62
 log-adjacency-changes
 network 10.50.0.5 0.0.0.0 area 0
 network 10.50.240.0 0.0.0.255 area 0
 network 10.50.242.0 0.0.0.255 area 0
 network 10.50.251.20 0.0.0.3 area 0
 network 10.50.251.24 0.0.0.3 area 0
!
ip classless
!
!
no ip http server
no ip http secure-server
ip ospf name-lookup
ip tacacs source-interface Loopback0
!
ip access-list extended AutoQoS-VoIP-Control
 permit tcp any any eq 1720
 permit tcp any any range 11000 11999
 permit udp any any eq 2427
```

```
 permit tcp any any eq 2428
 permit tcp any any range 2000 2002
 permit udp any any eq 1719
 permit udp any any eq 5060
ip access-list extended AutoQoS-VoIP-RTCP
 permit udp any any range 16384 32767
!
!
!
!
access-list 100 permit ip 10.50.240.0 0.0.0.255 10.27.31.0
0.0.0.255
access-list 100 deny   ip any any
access-list 101 permit ip 10.50.240.0 0.0.0.255 host
10.20.200.19
access-list 101 permit ip 10.50.240.0 0.0.0.255 host
10.20.20.81
access-list 101 permit ip 10.50.240.0 0.0.0.255 host
10.20.20.85
access-list 101 permit ip 10.50.240.0 0.0.0.255 host
10.20.20.86
access-list 101 deny   ip any any
access-list 102 permit ip 10.50.240.0 0.0.0.255 host
10.20.20.26
access-list 102 permit ip 10.50.240.0 0.0.0.255 host
10.20.20.161
access-list 102 permit ip 10.50.240.0 0.0.0.255 host
10.20.20.163
access-list 102 permit ip 10.50.240.0 0.0.0.255 host
10.20.20.185
access-list 102 deny   ip any any
!
no logging trap
access-list 103 permit tcp 10.50.241.0 0.0.0.255 any eq www
access-list 103 permit tcp 10.50.241.0 0.0.0.255 any eq 443
access-list 103 permit tcp 10.50.241.0 0.0.0.255 any eq 81
access-list 103 permit tcp 10.50.241.0 0.0.0.255 any eq 82
access-list 103 permit udp 10.50.241.0 0.0.0.255 host
10.20.20.38 eq domain
```

```
access-list 103 permit udp 10.50.241.0 0.0.0.255 host
10.20.20.44 eq domain
access-list 103 permit udp 10.50.241.0 0.0.0.255 any
access-list 103 permit icmp 10.50.241.0 0.0.0.255 any echo-
reply
access-list 103 permit tcp 10.50.241.0 0.0.0.255 any
established
access-list 103 deny   ip any any log
!
(output omitted)
!
end
```