

**ESTUDIO COMPARATIVO DE UNA RED CONVERGENTE CON  
CALIDAD DE SERVICIOS (QoS)**

**BERENICE JULIO RAMOS  
LILIBETH PÉREZ SALAS  
ESTUDIANTES DE INGENIERIA DE SISTEMAS**

**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR  
FACULTAD DE INGENIERÍA  
DIRECCION PROGRAMA DE INGENIERÍAS DE SISTEMAS  
CARTAGENA DE INDIAS D. T. Y C.  
DICIEMBRE DEL 2010**

**ESTUDIO COMPARATIVO DE UNA RED CONVERGENTE CON  
CALIDAD DE SERVICIOS (QoS)**

**BERENICE JULIO RAMOS  
LILIBETH PÉREZ SALAS  
ESTUDIANTES DE INGENIERIA DE SISTEMAS**

**TRABAJO DE GRADO PRESENTADO COMO REQUISITO PARA OPTAR EL  
TITULO DE INGENIERAS DE SISTEMAS**

**DIRECTOR**

**ING. ISAAC ZUÑIGA SILGADO**

**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR  
FACULTAD DE INGENIERÍA  
DIRECCION PROGRAMA DE INGENIERÍAS DE SISTEMAS  
CARTAGENA DE INDIAS D. T. Y C.  
DICIEMBRE DEL 2010**

Cartagena de Indias, D.T. y C. Diciembre del 2010

Señores

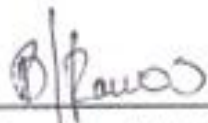
**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR**  
**COMITÉ DE EVALUACIÓN DE PROYECTOS**  
**FACULTAD DE INGENIERÍA DE SISTEMAS**  
Ciudad

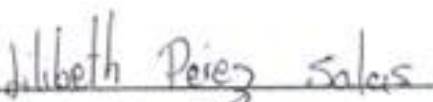
Estimados Señores

Con todo respeto me dirijo a ustedes, con el fin de presentarles a su consideración, estudio y aprobación la tesis de grado que lleva por título **“ESTUDIO COMPARATIVO DE UNA RED CONVERGENTE CON CALIDAD DE SERVICIOS (QoS)”**, como requisito para optar el título de Ingenieras de Sistemas.

Espero que este proyecto sea de su total satisfacción

Agradezco su amable atención

  
\_\_\_\_\_  
Berehice Julio Ramos  
c.c 32.936.868 de Cartagena

  
\_\_\_\_\_  
Lilibeth Pérez Salas  
C.c. 1'047.379.549 de Cartagena

Cartagena de Indias, D.T. y C. Diciembre del 2010

Señores

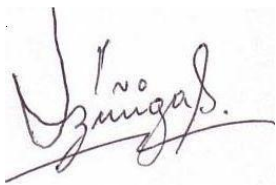
**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR**  
**COMITÉ DE EVALUACIÓN DE PROYECTOS**  
**FACULTAD DE INGENIERÍA DE SISTEMAS**

Ciudad

Estimados Señores

Tengo el agrado de comunicarles que el proyecto de grado el cual me desempeño como director, titulado **“ESTUDIO COMPARATIVO DE UNA RED CONVERGENTE CON CALIDAD DE SERVICIOS (QoS)”**, desarrollado por las estudiantes de Ingeniería de Sistemas BERENICE JULIO RAMOS Y LILIBETH PEREZ SALAS, lo apruebo como requisito para optar el título de Ingenieras de Sistemas.

Agradezco su amable atención



---

Ing. Isaac Zúñiga Silgado

C.c.73.116.898 de Cartagena

NOTA DE ACEPTACIÓN

---

---

---

---

---

PRESIDENTE DEL JURADO

---

JURADO

---

JURADO

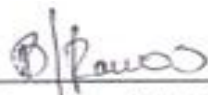
Cartagena de Indias, D.T y C Diciembre del 2010

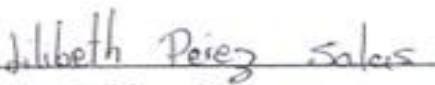
### **AUTORIZACIÓN**

Yo, Berenice Julio Ramos y Lilibeth Pérez Salas, manifestamos en este documento nuestra voluntad de ceder a la Universidad Tecnológica de Bolívar los derechos patrimoniales, consagrados en el artículo 72 de la ley 23 de 1982 sobre los derechos de autor, del trabajo final denominado ESTUDIO COMPARATIVO DE UN RED CONVERGENTE CON CALIDAD DE SERVICIOS (QoS) producto de nuestra actividad académica para optar el título de Ingenieras de Sistemas de la Universidad Tecnológica de Bolívar.

La Universidad Tecnológica de Bolívar, entidad sin ánimo de lucro, queda por tanto facultada para ejercer plenamente los derechos de anteriormente cedidos en su actividad ordinaria de investigación, docencia y extensión. La cesión otorgada se ajusta a lo que establece la ley 23 del 1992.

Con todo, en nuestra condición de autor me reservo los derechos morales de la obra antes citada con arreglo al artículo 30 de la ley 23 de 1982. En concordancia suscribo este documento que hace parte integral del trabajo antes mencionado y entrego al sistema de Bibliotecas de la Universidad Tecnológica de Bolívar.

  
Berenice Julio Ramos  
c.c 32.936.868 de Cartagena

  
Lilibeth Pérez Salas  
C.c. 1'047.379.549 de Cartagena

-----  
Firma

## TABLA DE CONTENIDO

INTRODUCCION.....	11
1. MARCO CONCEPTUAL.....	14
1.1. Redes de computadoras.....	14
1.1.1 Clasificación de Redes de computadoras .....	15
1.1.1.1. Redes de área local LAN.....	15
1.1.1.2 Redes de área metropolitana (MAN).....	17
1.1.1.3 Redes de área extendida (WAN).....	17
1.1.2. Estructura básica de una red de computadoras.....	18
1.2. Medios de transmisión.....	20
1.2.1. Medios magneto-ópticos.....	20
1.2.2. Cables de Par Trenzado.....	20
1.2.3. El cable coaxial.....	22
1.2.4. Fibra Óptica.....	24
1.2.5. Redes inalámbricas.....	26
1.2.5.1 Redes públicas de radio.....	29
1.3. Cableado estructurado.....	30
1.4 Topologías.....	32
1.4.1. Topología de BUS / Linear Bus.....	32
1.4.2. Topología de Estrella / Star.....	34
1.4.3 Topología de Estrella Cableada / Star – Wired Ring.....	34
1.4.4 Topología de Árbol/ Tree.....	34

1.5 Equipos Activos.....	35
1.5.1 Switch o Conmutadores.....	35
1.5.1.1 Donde Usar Switch.....	39
1.5.2 Router.....	40
1.5.3 Gateway.....	42
1.5.4 Transceivers o Media Converter.....	42
1.6 Servidores de Terminales.....	43
1.7. Sistemas operativos.....	43
1.7.1 Categorías de los sistemas operativos.....	43
1.8 Servidores.....	51
1.9 Protocolos.....	52
1.10. Bases de datos y aplicaciones.....	57
1.11 Seguridad informática.....	58
1.12. Calidad de Servicio QoS .....	60
2. REDES CONVERGENTES Y CALIDAD DE SERVICIO (QoS).....	61
2.1 Calidad de Servicios (QoS).....	65
2.2 Funcionamiento de los servicios (Voz IP, Datos, Video ip).....	68
2.3. Redes Convergentes.....	82



3. MÉTODOS PARA IMPLEMENTACIÓN DE CALIDAD DE SERVICIOS (QoS) BASADOS EN SERVICIOS INTEGRADOS, SERVICIOS DIFERENCIADOS y AUTOQoS.....	84
3.1 Servicios Integrados (IntServ).....	85
3.2 Servicios Diferenciados (DiffServ).....	87
3.3 AutoQoS.....	89
3.4 Implementación de una Red Convergente Con Calidad de Servicios (QoS)..	90
4. ESCENARIO DE PRÁCTICAS DE LABORATORIO.....	96
5. RESULTADOS DEL PROYECTO.....	110
6. CONCLUSIONES.....	103
7. RECOMENDACIONES.....	108
8. GLOSARIO.....	117
9. BIBLIOGRAFÍA.....	126
10. ANEXOS.....	127

## LISTA DE FIGURAS

1.	Figura 1. Diagrama de una Red de datos.....	19
2.	Figura 2. Sección de un cable coaxial.....	23
3.	Figura 3. Sección de un cable coaxial.....	23
4.	Figura 4. Composición de la fibra óptica.....	26
5.	Figura 5. Composición de la fibra óptica.....	26
6.	Figura 6. Cable Estructurado.....	32
7.	Figura 7. Switchs Netgear de 4 puertos y Linksys de 8 puertos.....	37
8.	Figura 8. Switchs Netgear de 4 puertos y Linksys de 8 puertos.....	37
9.	Figura 9. Switchs Cisco de 8 puertos y Linksys de 16 puertos.....	38
10.	Figura 10. Switchs Cisco de 8 puertos y Linksys de 16 puertos.....	38
11.	Figura 11. Switch switch Linksys de 24 puertos.....	38
12.	Figura 12. Switch Cisco de 48 puertos.....	38
13.	Figura 13. Router Cisco 2800 .....	41
14.	Figura 14: Topología de Red.....	99
15.	Figura 15: Direcccionamiento IP.....	100
16.	Figura 16. Llamada saliente de Manizales.....	105
17.	Figura 17. Llamada entrante a Cartagena .....	106
18.	Figura 18. Imagen sin implementación de métodos de QoS.....	106
19.	Figura 19. Imagen con implementación Métodos de QoS.....	107
20.	Figura 20: cuadro Comparativo de Resultados.....	109
21.	Figura 21: Router Cisco 2800.....	192
22.	Figura 22. Swicth Cisco 2950.....	193
23.	Figura 23. Softphone Cisco.....	194
24.	Figura 24: Access point 3com 8760.....	195

## INTRODUCCION

Actualmente se puede apreciar como surgen constantemente novedosas tecnologías, estas cada día son más pertinentes a las necesidades de productividad de los sectores empresariales, gubernamentales de los países, es por esta razón que existe la necesidad de investigar formas distintas de establecer la comunicación a través de las redes actuales, tratando de maximizar la utilización de las infraestructuras operativas existentes. De allí es por esto que se proponen soluciones alternativas que mejoren la multiplexación de servicios; el fin que se tiene con esto es crear soluciones que soporten las innovadoras aplicaciones crecientes en la reciente explosión en el uso del Internet y todo lo referente a las redes IP, a través, de las cuales se pretenden integrar en un mismo medio voz, video, mail, datos, etc. Estos servicios anteriormente y en muchas empresas en la actualidad se están trabajando por redes y medios independientes, ocasionando mayor costos de infraestructura.

Los beneficios que se obtienen al integrar en un mismo medio de transmisión lo antes mencionados servicios, es la mejora en la utilización de los recursos de la red, tener redes que sean mucho más productivas, óptimas y que balanceen la relación Costo – Beneficio a favor de las empresas y los usuarios que las necesiten y las implementen, para dar soluciones a sus necesidades de comunicaciones.

El hecho de poder enviar información variada, de diferentes servicios a través de una misma infraestructura al mismo tiempo es todo un reto para las calidades de las comunicaciones actuales, conocer como se implementan estas redes, su rendimiento, su comportamiento, cómo se pueden optimizar estas redes de comunicaciones es básicamente lo que se buscaba con este proyecto de grado, es por ello que para este trabajo de Investigación se implementaron varios

proyectos de laboratorios y se trabajó durante el desarrollo de este proyecto de grado en dos (2) prácticas y/o proyectos que tenía a su vez varias prácticas, donde se implementaron varios modelos y situaciones en redes, las cuales fueron:

1. Diseño, implementación y configuración de una red de computadoras y/o Comunicaciones convergente donde se enviaron servicios inicialmente de una forma individual y luego al mismo tiempo, es decir, envío de Voz IP, Datos, Video IP; esto para mirar el desempeño o performance de la red, buscando además observar el comportamiento de la calidad de estos servicios, sin implementar QoS. (Primera Práctica).

2. Diseño, implementación y configuración de una red de computadoras y/o Comunicaciones convergente donde se enviaron servicios inicialmente de una forma individual y luego al mismo tiempo, es decir, envío de Voz IP, Datos, Video IP, pero en esta práctica a diferencia de la anterior se realizó implementando los parámetros de Calidad de Servicios (QoS) existentes; esto para mirar el desempeño o performance de la misma red anterior, pero ahora con múltiples servicios, controlados por políticas y mecanismos de calidad de servicios; Y así poder determinar si con la QoS el comportamiento de la red desmejora, mejora y en que niveles varían estas calidades de servicios. (Segunda Práctica).

Este proyecto se realizó teniendo como eje central los siguientes objetivos:

### **Objetivo General**

✓ Realizar un estudio comparativo de Redes Convergentes con Calidad de Servicios (QoS).

## **Objetivos Específicos**

- ✓ Conocer los diferentes métodos de implementación de Calidad de Servicios (QoS), basados en servicios integrados, servicios diferenciados y AutoQoS.
  
- ✓ Ejecutar una práctica en laboratorio donde se trabaje con Router, Switch, Softphone, Diademas, Sistema de Videostream, Portátiles, Access Point, implementados en una red convergente para diagnosticar los comportamientos de los servicios evaluados (Datos, Voz ip y Video ip).
  
- ✓ Mostrar paso a paso la forma de instalar, configurar, operar y administrar los servicios implementados en la red convergente.

Al finalizar este estudio y prácticas quedaron bases para conocer cómo mejorar las calidades de servicios de las actuales redes convergentes o lo que hoy día se conoce como NGN (Redes de Nueva Generación). Se pueden apreciar estos resultados y detalles de las prácticas y/o laboratorios en la sección de Resultados, Escenario de prácticas, Conclusiones del proyecto y en la Sección de Anexos.

## **1. MARCO CONCEPTUAL**

Este tipo de proyecto práctico, de laboratorio y diseño óptimo en lo referente a redes de computadoras y de telecomunicaciones cuenta con una gran cantidad de bases o fundamentos teóricos, los cuales se resumieron; destacando los más importantes, básicos para el desarrollo y comprensión del proyecto; por ello es pertinente hablar en el estudio sobre:

### **1.1 Redes de computadoras.**

El concepto de redes de computadoras implica diferenciar entre el concepto de redes físicas y redes de comunicación. Respecto a la estructura física, los modos de conexión física, los flujos de datos, etc; se puede decir entonces que una red la constituyen dos o más computadores que comparten determinados recursos, sea hardware (impresoras, sistemas de almacenamiento) ó software (aplicaciones, archivos, datos).

Desde una perspectiva más comunicativa y que expresa mejor lo que puede hacerse con las redes en la educación, podemos decir que existe una red cuando están involucrados un componente humano que comunica, un componente tecnológico (ordenadores, televisión, telecomunicaciones) y un componente administrativo institución o instituciones que mantienen los servicios).

Una red mas que un grupo de computadores conectados entre si, por un medio de conexión; para permitir a cada una de estas computadoras compartir recursos o periféricos con los demás, la constituyen varias personas que solicitan, proporcionan e intercambian experiencias e informaciones a través de sistemas de comunicación. Teniendo en cuenta la zona geográfica que abarcan, tradicionalmente se habla de: Redes de Área Local (LAN), Redes de Área Metropolitana (MAN), Redes de Área extendida (WAN).

### **1.1.1 Clasificación de las redes de computadores**

Las redes de computadoras según el área geográfica en la cual se implementan se dividen:

#### **1.1.1.1 Redes de área local (LAN)**

Uno de los sucesos más críticos para la conexión en red lo constituye la aparición y la rápida difusión de la red de área local (LAN), como forma de normalizar las conexiones entre las máquinas que se utilizan para trabajar en los sistemas informáticos. Como su propio nombre indica, constituye una forma de interconectar una serie de equipos informáticos. A su nivel más elemental, una LAN no es más que un medio compartido (como un cable utp, stp, ftp y/o fibra óptica multimodal al que se conectan todas las computadoras y las impresoras) junto con una serie de reglas que rigen el acceso a dicho medio. La LAN más

difundida, es la Ethernet; utiliza un mecanismo denominado Call Sense Múltiple Access-Collision Detect (CSMA-CD).

Esto significa que cada equipo conectado sólo puede utilizar el cable cuando ningún otro equipo lo está utilizando.

Si hay algún conflicto, el equipo que está intentando establecer la conexión la anula y efectúa un nuevo intento más adelante. La Ethernet transfiere datos hoy día hasta a 10 Gbits/Seg, lo suficientemente rápido como para hacer inapreciable la distancia entre los diversos equipos y dar la impresión de que están conectados directamente a su destino.

Ethernet y CSMA-CD son dos ejemplos de LAN. Hay topologías muy diversas (bus, estrella, anillo) y diferentes protocolos de acceso. A pesar de esta diversidad, todas las LAN comparten la característica de poseer un alcance limitado (normalmente abarcan un edificio) y de tener una velocidad suficiente para que la red de conexión resulte invisible para los equipos que la utilizan.

Además de proporcionar un acceso compartido, las LAN modernas también proporcionan al usuario multitud de funciones avanzadas. Hay paquetes de software de gestión para controlar la configuración de los equipos en la LAN, la administración de los usuarios, y el control de los recursos de la red. Una estructura muy utilizada consiste en varios servidores a disposición de distintos (con frecuencia, muchos) usuarios. Los primeros, por lo general máquinas más



potentes, proporcionan servicios como control de impresión, ficheros compartidos y correo a los últimos, por lo general computadoras personales.

#### **1.1.1.2. Redes de Área Metropolitana (MAN)**

Corresponde a una versión más grande de una LAN en cuanto a topología, protocolos y medios de transmisión, que cubre un conjunto de oficinas corporativas o empresas en una misma ciudad. En general, cualquier red de datos, voz o video con una extensión de una a varias decenas de kilómetros puede ser considerada una MAN.

El estándar IEEE 802.6 define un tipo de MAN llamado DQDB que usa dos cables half-duplex por los cuales se recibe y transmiten voz, datos entre un conjunto de nodos. Un aspecto típico de las MAN es que el medio físico es de difusión, lo que simplifica el diseño de la red.

#### **1.1.1.3 Redes de área extendida (WAN)**

Cuando se llega a un cierto punto, deja de ser poco práctico seguir ampliando una LAN. A veces esto viene impuesto por limitaciones físicas, aunque suele haber formas más adecuadas o económicas de ampliar una red de computadoras. Dos de los componentes importantes de cualquier red son la red de teléfono y la de datos.

Son enlaces para grandes distancias que amplían la LAN hasta convertirla en una red de área extendida (WAN). Casi todos los operadores de redes internacionales

y nacionales, (como DBP en Alemania, EPM y Telecom en Colombia o British Telecom en Inglaterra) ofrecen servicios para interconectar redes de computadoras, que van desde los enlaces de datos sencillos y a baja velocidad que funcionan basándose en la red pública de telefonía hasta los complejos servicios de alta velocidad (como frame relay y SMDS “Synchronous Multimegabit Data Service”), adecuados para la interconexión de las LAN. Estos servicios de datos a alta velocidad suelen denominarse conexiones de banda ancha. Se prevé que proporcionen los enlaces necesarios entre LAN para hacer posible lo que han dado en llamarse autopistas de la información.

### **1.1.2. Estructura básica de una red de computadoras**

Las redes de computadoras se conforman a través de una serie de elementos, los cuales integran su estructura; estos elementos son:

- Muchas veces se utilizan armarios o gabinetes de telecomunicaciones, donde se colocan de manera ordenada los equipos activos (concentradores, Switch y routers), Patch Panels y Bandejas de Fibra Óptica; estos gabinetes tienen una medida estándar de 19 pulgadas de ancho.
- Los servidores en los cuales se encuentra y procesa la información disponible al usuario, son computadoras con grandes características y recursos, estas computadoras o servidores actúan en la red como administradores del sistema.

- Los equipos activos son los elementos que gestionan todo el tráfico en una red, estos equipos activos están conformados por: Concentradores, switches , routers y otros elementos de gestión de tráfico.
- Los "Pach Panel's", los cuales son unos organizadores de cables o centros de acopios de puntos de comunicaciones o puestos de trabajos.
- El "Pach Cord", el cual es un cable del tipo UTP solo que con mayor flexibilidad que el UTP corriente (el empleado en el cableado horizontal), el cual interconecta al "Pach Panel" con los "Equipos Activos"; así como también a los tomas o placas de pared con cada una de las terminales (PC's).
- Finalmente lo que se conoce como Cableado Horizontal en el cual suele utilizarse cable UTP o Fibra Óptica Multimodo; para enlazar el Pach panel con cada una de las placas de pared.

Diagrama de una red de datos

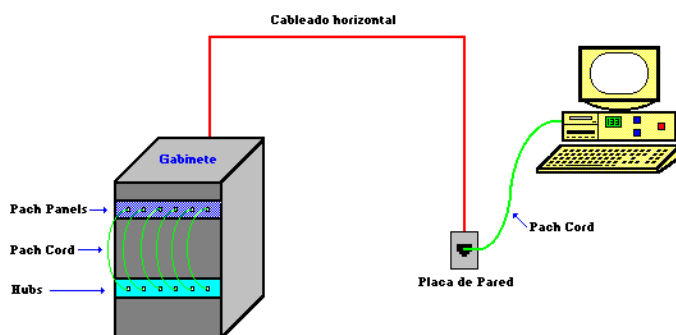


Figura 1

Así pues, a la hora de diseñar el cableado estructurado de una red de datos, se deben de tener en consideración una amplia gama de aspectos tanto desde el punto de vista técnico como económico, dependiendo de los requerimientos del

sistema, para lo cual existen diversos tipos de cables y categorías de los mismos, entre los cuales podemos citar los siguientes:

- SPT
- Coaxial
- UTP y ScTP
- Fibra Óptica

## **1.2. Medios de transmisión**

Los medios de transmisión, son la vía y/o la forma como se transmite la información en las redes de computadoras y entre computadores, de estos podemos señalar:

### **1.2.1 Medios magneto-ópticos**

Son aquellos que se pueden transportar de un lugar a otro, por ejemplo Disquetes, zips, CD-ROM y en general medios removibles.

### **1.2.2 Cables de Par Trenzado**

Constituyen el modo más simple y económico de todos los medios de transmisión. Sin embargo, presentan una serie de inconvenientes. En todo conductor, la resistencia eléctrica aumenta al disminuir la sección del conductor, por lo que hay que llegar a un compromiso entre volumen y peso, y la resistencia eléctrica del cable. Esta última está afectada directamente por la longitud máxima.

Cuando se sobrepasan ciertas longitudes hay que recurrir al uso de repetidores para restablecer el nivel eléctrico de la señal.

Tanto la transmisión como la recepción utilizan un par de conductores que, si no están apantallados, son muy sensibles a interferencias y diafonías producidas por la inducción electromagnética de unos conductores en otros (motivo por el que en ocasiones percibimos conversaciones telefónicas ajenas a nuestro teléfono).

Un cable apantallado es aquel que está protegido de las interferencias eléctricas externas, normalmente a través de un conductor eléctrico externo al cable, por ejemplo una malla.

Un modo de subsanar estas interferencias consiste en trenzar los pares de modo que las intensidades de transmisión y recepción anulen las perturbaciones electromagnéticas sobre otros conductores próximos. Esta es la razón por la que este tipo de cables se llaman de pares trenzados. Con este tipo de cables es posible alcanzar velocidades de transmisión comprendidas entre 2 Mbps y 10 Gbps. en el caso de señales digitales.

- La Categorías: Cada categoría especifica unas características eléctricas para el cable: atenuación, capacidad de la línea e impedancia.
- Las Clases: Cada clase especifica las distancias permitidas, el ancho de banda conseguido y las aplicaciones para las que es útil en función de estas características en la tabla 1 podemos ver de manera detallada esto.

CLASES	Clase A	Clase B	Clase C	Clase D
Ancho de banda	100 kHz	1 MHz	20 MHz	100 MHz
En categoría 3	2 km	500 m	100 m	no existe
En categoría 4	3 km	600 m	150 m	no existe
En categoría 5	3 km	700 m	160 m	100 m

Tabla 1

Características de longitudes posibles y anchos de banda para las clases y categorías de pares trenzados.

Dado que el UTP de categoría 6A es barato y fácil de instalar, se está incrementando su utilización en las instalaciones de redes de área local con topología en estrella, mediante el uso de conmutadores (Switch).

### 1.2.3 *El cable coaxial*

Presenta propiedades mucho más favorables frente a interferencias y a la longitud de la línea de datos, de modo que el ancho de banda puede ser mayor. Esto permite una mayor concentración de las transmisiones analógicas o más capacidad de las transmisiones digitales como lo vemos en la figura 1 tiene una malla conductora, dieléctrico, núcleo central y un recubrimiento externo.

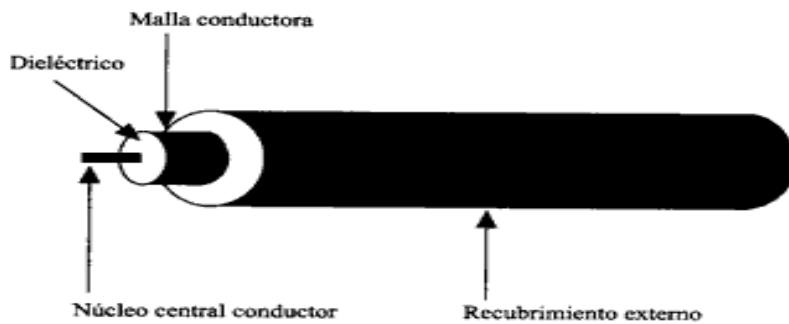
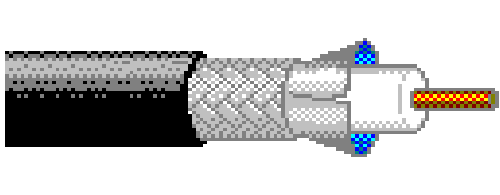


Figura 2



Sección de un cable coaxial. Figura 3

Su estructura es la de un cable formado por un conductor central macizo o compuesto por múltiples fibras al que rodea un aislante dieléctrico de mayor diámetro Figura 3. Una malla exterior aísla de interferencias al conductor central. Por último, utiliza un material aislante para recubrir y proteger todo el conjunto. Presenta condiciones eléctricas más favorables. En redes de área local se utilizan dos tipos de cable coaxial: fino y grueso.

Es capaz de llegar a anchos de banda comprendidos entre los 80 MHz y los 400 MHz (dependiendo de si es fino o grueso). Esto quiere decir que en transmisión de señal analógica seríamos capaces de tener, como mínimo. Del orden de 10.000 circuitos de voz. Actualmente se está implementando este medio de transmisión en redes inalámbricas para bajar la señal desde la antena hasta el radio (Emisor/Receptor), como también tiene mucha utilización en los enlaces

metropolitanos basados en la tecnología HFC (Redes Híbridas que utilizan Fibras Ópticas y Cable Coaxial).

#### **1.2.4. Fibra Óptica**

La fibra óptica permite la transmisión de señales luminosas y es insensible a interferencias electromagnéticas externas. Cuando la señal supera frecuencias de  $10^{10}$  Hz. hablamos de frecuencias ópticas. Los medios conductores metálicos son incapaces de soportar estas frecuencias tan elevadas y son necesarios medios de transmisión ópticos.

Por otra parte, la luz ambiental es una mezcla de señales de muchas frecuencias distintas, por lo que no es una buena fuente para ser utilizada en la transmisión de datos. Son necesarias fuentes especializadas:

- Fuentes láser. a partir de la década de los sesenta se descubre el láser, una fuente luminosa de alta coherencia, es decir, que produce luz de una única frecuencia y toda la emisión se produce en fase.
- Diodos láser. es una fuente semiconductor de emisión de láser de bajo precio.
- Diodos LED. Son semiconductores que producen luz cuando son excitados eléctricamente.



La composición del cable de fibra óptica consta de un núcleo, un revestimiento y una cubierta externa protectora Figura siguiente. El núcleo es el conductor de la señal luminosa y su atenuación es despreciable. La señal es conducida por el interior de éste núcleo fibroso, sin poder escapar de él debido a las reflexiones internas y totales que se producen, impidiendo tanto el escape de energía hacia el exterior como la adicción de nuevas señales externas.

Actualmente se utilizan tres tipos de fibras ópticas para la transmisión de datos:

1. Fibra monomodo. Permite la transmisión de señales con ancho de banda hasta 2 GHz.
2. Fibra multimodo de índice gradual. Permite transmisiones de hasta 500 MHz.
3. Fibra multimodo de índice escalonado. Permite transmisiones de hasta 35 MHz.

Se han llegado a efectuar transmisiones de decenas de miles de llamadas telefónicas a través de una sola fibra, debido a su gran ancho de banda.

Otra ventaja es la gran fiabilidad, su tasa de error es mínima. Su peso y diámetro la hacen ideal frente a cables de pares o coaxiales.

Normalmente se encuentra instalada en grupos, en forma de mangueras, con un núcleo metálico que les sirve de protección y soporte frente a las tensiones producidas. Su principal inconveniente es la dificultad de realizar una buena

conexión de distintas fibras con el fin de evitar reflexiones de la señal, así como su fragilidad podemos ver en la figura 4

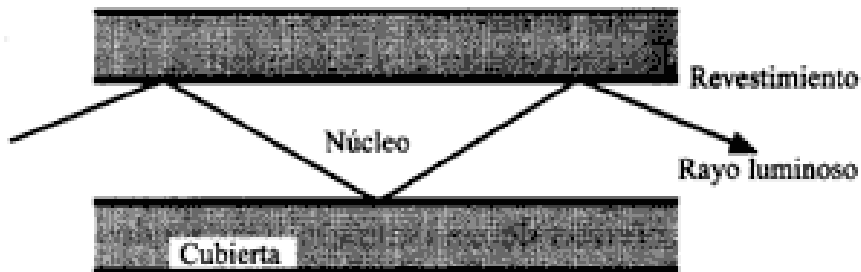


Figura 4

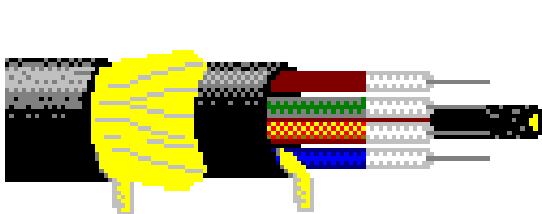


Figura 5

En la figura 5 se muestra de una manera la composición de la fibra.

### 1.2.5 *Redes inalámbricas*

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica<sup>3</sup>. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos.

También es útil para hacer posibles sistemas basados en plumas. Pero la realidad es que esta tecnología está todavía en pañales y se deben de resolver varios obstáculos técnicos y de regulación antes de que las redes inalámbricas sean utilizadas de una manera general en los sistemas de cómputo de la actualidad.

No se espera que las redes inalámbricas lleguen a remplazar a las redes cableadas. Estas ofrecen velocidades de transmisión mayores que las logradas con la tecnología inalámbrica. Mientras que las redes inalámbricas actuales ofrecen velocidades de 54 Mbps y 102 Mbps, las redes cableadas ofrecen velocidades de 10 Gbps y se espera que alcancen velocidades de hasta 40 Gbps. Los sistemas de Cable de Fibra Óptica logran velocidades aún mayores, hoy día se tienen redes inalámbricas que soportan velocidades e 54 Mbps como 102 Mbps, redes conocidas como Wi-Fi y Wi-Max.

Sin embargo se pueden mezclar las redes cableadas y las inalámbricas, y de esta manera generar una “Red Híbrida” y poder resolver los últimos metros hacia la estación. Se puede considerar que el sistema cableado sea la parte principal y la inalámbrica le proporcione movilidad adicional al equipo y el operador se pueda desplazar con facilidad dentro de un almacén o una oficina.

Existen dos amplias categorías de Redes Inalámbricas:

1. De Larga Distancia.- Estas son utilizadas para transmitir la información en espacios que pueden variar desde una misma ciudad o hasta varios países circunvecinos (mejor conocido como Redes de Área Metropolitana MAN), sus

velocidades de transmisión son relativamente bajas, de 4.8 a 8 Mbps, caso como Wi-Max, Radioenlaces, etc.

2. De Corta Distancia.- Estas son utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios que no se encuentran muy retirados entre si, con velocidades del orden de 280 Kbps hasta los 102 Mbps

Existen dos tipos de redes de larga distancia: Redes de Conmutación de Paquetes (públicas y privadas) y Redes Telefónicas Celulares. Estas últimas son un medio para transmitir información de alto precio. Debido a que los módems celulares actualmente son más caros y delicados que los convencionales, ya que requieren circuitos especiales, que permiten mantener la pérdida de señal cuando el circuito se alterna entre una célula y otra. Esta pérdida de señal no es problema para la comunicación de voz debido a que el retraso en la conmutación dura unos cuantos cientos de milisegundos, lo cual no se nota, pero en la transmisión de información puede hacer estragos; Otras desventajas de la transmisión celular son:

- La carga de los teléfonos se termina fácilmente.
- La transmisión celular se intercepta fácilmente (factor importante en lo relacionado con la seguridad).
- Las velocidades de transmisión son bajas.

Todas estas desventajas hacen que la comunicación celular se utilice poco, o únicamente para archivos muy pequeños como cartas, planos, etc. Pero se espera que con los avances en la compresión de datos, seguridad y algoritmos de verificación de errores se permita que las redes celulares sean una opción redituable en algunas situaciones.

La otra opción que existe en redes de larga distancia son las denominadas:

Red Pública De Conmutación De Paquetes Por Radio. Estas redes no tienen problemas de pérdida de señal debido a que su arquitectura está diseñada para soportar paquetes de datos en lugar de comunicaciones de voz. Las redes privadas de conmutación de paquetes utilizan la misma tecnología que las públicas, pero bajo bandas de radio frecuencias restringidas por la propia organización de sus sistemas de cómputo.

#### **1.2.5.1 Redes públicas de radio**

Las redes públicas tienen dos protagonistas principales: “*ARDIS*” (una asociación de Motorola e IBM) y “RAM Mobile Data” (desarrollado por Ericsson AB, denominado *MOBITEX*). Este último es el más utilizado en Europa. Estas Redes proporcionan canales de radio en áreas metropolitanas, las cuales permiten la transmisión a través del país y que mediante una tarifa pueden ser utilizadas como redes de larga distancia.

La compañía proporciona la infraestructura de la red, se incluye controladores de áreas y Estaciones Base, sistemas de cómputo tolerantes a fallas, estos sistemas soportan el estándar de conmutación de paquetes X.25.

Así como su propia estructura de paquetes. Estas redes se encuentran de acuerdo al modelo de referencia OSI. ARDIS especifica las tres primeras capas de la red y proporciona flexibilidad en las capas de aplicación, permitiendo al cliente desarrollar aplicaciones de software (por ejemplo. una compañía llamada RF Data, desarrollo una rutina de compresión de datos para utilizarla en estas redes públicas).

Los fabricantes de equipos de computo venden periféricos para estas redes (IBM desarrollo su "PCRadio" para utilizarla con ARDIS y otras redes, públicas y privadas).

La PCRadio es un dispositivo manual con un microprocesador 80C186 que corre DOS, un radio/fax/módem incluido y una ranura para una tarjeta de memoria y 640 Kb de RAM.

Estas redes operan en un rango de 800 a 900 Mhz. ARDIS ofrece una velocidad de transmisión de 4.8 Kbps. Motorola Introdujo una versión de red pública en Estados Unidos que opera a 19.2 Kbps; y a 9.6 Kbps en Europa (debido a una banda de frecuencia más angosta). Las redes públicas de radio como *ARDIS* y *MOBITEX* jugaran un papel significativo en el mercado de redes de área local (LAN's) especialmente para corporaciones de gran tamaño. Por ejemplo, elevadores OTIS utiliza *ARDIS* para su organización de servicios.

### **1.3. Cableado estructurado.**

En 1991, las asociaciones de las industrias electrónicas desarrollaron el estándar comercial de telecomunicaciones designado "EIA/TIA568, el cual cubre el cableado horizontal y los BackBone, cableado de las interiores, las cajillas estaciones de trabajo, cables y conexiones de hardware. Cuando el estándar 568 fue adoptado, los cables UTP de altas velocidades y las conexiones de hardware se mantenían en desarrollo. Más tarde, el EIA/TIA568, presentó el TSB36 y TSB40A para proveer los cables UTP y especificaciones para conexiones del hardware, definiendo él número de propiedades físicas y eléctricas particularmente para atenuaciones y crosstalk, el revisado estándar fue designado "ANSI/TIA/EIA568A", el cual incorpora la forma original de EIA/TIA568 más TSB36 aprobado en TSB40A, como fue en 1995, las categorías 6a UTP incluyen las siguientes jerarquías:

- Categoría 3: el cable UTP categoría 3 y las conexiones del Hardware han sido probados y certificados, para cumplir ciertas especificaciones a una velocidad máxima de 16 Mhz y una aceptable velocidad de transmisión de datos de 10mbps.

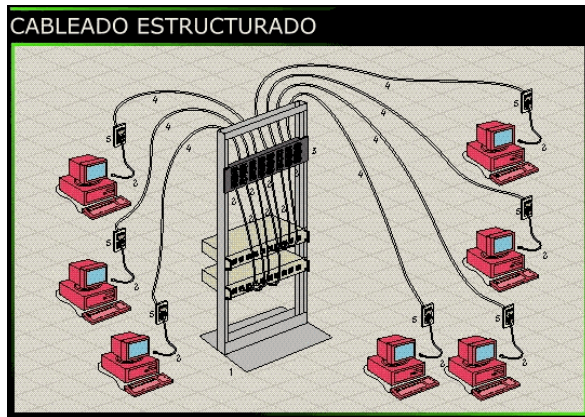


Figura 6

En la figura 6 se muestra como es gráficamente el cableado estructurado.

- Categoría 4: los productos categoría 4 han sido probados y certificados a una velocidad máxima de 20 Mhz y agradable velocidad de datos de 16 Mbps.
- Categoría 6a: Los productos categoría 6a han sido probados y certificados a una velocidad máxima de 1200 MHz y pueden soportar una velocidad de transmisión de datos de 10 Gbps.

## 1.4. Topologías

Entre los principales tipos de Topologías físicas tenemos:

### 1.4.1 Topología de *BUS / Linear Bus*

Consiste en un cable con un terminador en cada extremo del que se cuelgan todos los elementos de una red. Todos los Nodos de la Red están unidos a este cable.



Este cable recibe el nombre de "Backbone Cable". Tanto Ethernet como LocalTalk pueden utilizar esta topología.

➤ Ventajas de la topología de Bus

1. Es Más fácil conectar nuevos nodos a la red.
2. Requiere menos cable que una topología estrella.

➤ Desventaja de la topología de Bus

1. Toda la red se caería se hubiera una ruptura en el cable principal
2. Se requieren terminadores.
3. Es difícil detectar el origen de un problema cuando toda la red cae.
4. No se debe utilizar como única solución en un gran edificio.

#### **1.4.2. Topología de Estrella / Star**

Es una topología estrella todos y cada uno de los nodos de la red, estos se conectan a los equipos activos (Hub, Switch y Router).

Los datos en estas redes fluyen del emisor hasta el concentrador, este realiza todas las funciones de la red, además actúa como amplificador de los datos.

➤ Ventajas de la Topología Estrella

1. Gran facilidad de instalación

2. Posibilidad de desconectar elementos de red sin causar problemas
3. Facilidad para la detección de fallo y su reparación.

➤ Inconvenientes de la Topología de Estrella.

1. Requiere más cable que la topología de BUS.
2. Un fallo en el equipo activo provoca el aislamiento de todos los nodos a él conectados.
3. Se han de comprar equipos activos.

#### **1.4.3 Topología de Estrella Cableada / Star – Wired Ring**

Físicamente parece una topología estrella pero el tipo de equipo activo utilizado, la MAU se encarga de interconectar internamente la red en forma de anillo.

Esta topología es la que se utiliza en redes Token ring

#### **1.4.3. Topología de Árbol / Tree**

La topología de árbol combina características de la topología de estrella con la BUS. Consiste en un conjunto de subredes estrella conectadas a un BUS. Esta topología facilita el crecimiento de la red.

➤ Ventajas de la Topología de Árbol.

1. Cableado punto a punto para segmentos individuales.
2. Soportado por multitud de vendedores de software y de hardware.

➤ Desventajas de la Topología de Árbol.

1. La medida de cada segmento viene determinada por el tipo de cable utilizado.
2. Si se viene abajo el segmento principal todo el segmento se viene abajo con él.
3. Es más difícil su configuración.

## **1.5 Equipos Activos**

Son fundamentales los equipos encargados de gestionar cualquier red de computadoras, estos equipos activos los podemos denotar como Hub o Concentradores, Switch o Conmutadores y los Router o Enrutadores, existen otros equipos activos pero se han definidos los básicos.

### **1.5.1 Switch o Conmutadores**

Un Switch es un dispositivo de red situado en la capa 2 del modelo de referencia OSI, aunque también pueden ser de Capa 3 cuando permiten realizar Enrutamiento.

En esta capa además se encuentran las NIC (Network Interface Card; Placa de Red) pueden ser inalámbricas y los Bridges (Puentes).

Un Switch, al igual que un puente, es un dispositivo de la capa 2. De hecho, el Switch se denomina puente multipuerto, así como el Hub se denomina repetidor multipuerto. La diferencia entre el Hub y el Switch es que los switches toman decisiones basándose en las direcciones MAC y los hubs no toman ninguna

decisión. Como los switches son capaces de tomar decisiones, así hacen que la LAN sea mucho más eficiente. Los switches hacen esto "conmutando" datos sólo desde el puerto al cual está conectado el host correspondiente. A diferencia de esto, el Hub envía datos a través de todos los puertos de modo que todos los hosts deban ver y procesar (aceptar o rechazar) todos los datos. Esto hace que la LAN sea más lenta.

A primera vista los switches parecen a menudo similares a los Hubs. Tanto los Hubs como los switches tienen varios puertos de conexión (pueden ser de 8, 12, 24 o 48, o conectando 2 de 24 en serie), dado que una de sus funciones es la concentración de conectividad (permitir que varios dispositivos se conecten a un punto de la red).

La diferencia entre un Hub y un Switch está dada por lo que sucede dentro de cada dispositivo. El propósito del Switch es concentrar la conectividad, haciendo que la transmisión de datos sea más eficiente. Por el momento, piense en el Switch como un elemento que puede combinar la conectividad de un Hub con la regulación de tráfico de un puente en cada puerto. El Switch conmuta paquetes desde los puertos (las interfaces) de entrada hacia los puertos de salida, suministrando a cada puerto el ancho de banda total.

Un Switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos.

El Switch puede agregar mayor ancho de banda, acelerar la salida de paquetes, reducir tiempo de espera y bajar el costo por puerto.

El Switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final. No están diseñados con el propósito principal de un control íntimo sobre la red o como la fuente última de seguridad, redundancia o manejo.

Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor.

Básicamente un Switch es un administrador inteligente del ancho de banda.



Figura 7



Figura 8

En la figura 7 y figura 8 se ilustran diferentes Switchs Netgear de 4 puertos y Linksys de 8 puertos.

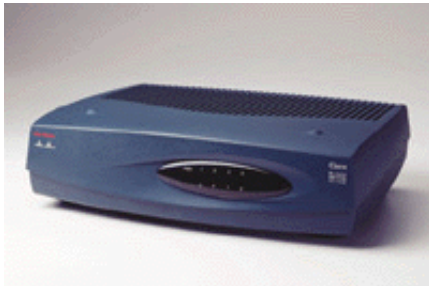


Figura 9



Figura 10

En la figura 9 y figura 10 se muestra switches Cisco de 8 puertos y Linksys de 16 puertos



Figura 11

En la figura 11 se muestra switch Linksys de 24 puertos.



Figura 12

En la figura 12 se muestra switch Cisco de 48 puertos.

### **1.5.1.1 *Donde usar Switch?***

Uno de los principales factores que determinan el éxito del diseño de una red, es la habilidad de la red para proporcionar una satisfactoria interacción entre cliente / servidor, pues los usuarios juzgan la red por la rapidez de obtener un prompt y la confiabilidad del servicio.

Hay diversos factores que involucran el incremento de ancho de banda en una LAN:

- El elevado incremento de nodos en la red.
- El continuo desarrollo de procesadores más rápidos y poderosos en estaciones de trabajo y servidores.
- La necesidad inmediata de un nuevo tipo de ancho de banda para aplicaciones intensivas cliente / servidor.
- Cultivar la tendencia hacia el desarrollo de granjas centralizadas de servidores para facilitar la administración y reducir el número total de servidores.

La regla tradicional 80/20 del diseño de redes, donde el 80% del tráfico en una LAN permanece local, se invierte con el uso del Switch.

Los switches resuelven los problemas de anchos de banda al segmentar un dominio de colisiones de una LAN, en pequeños dominios de colisiones.

### **1.5.2 Router**

Un dispositivo de la red que funciona como un Switch inteligente. Es capaz de aprender no solo la dirección de origen y de destino sino también las sendas que deben utilizar los paquetes para llegar a su destino. Múltiples routers pueden ser sesteados de modo de ser utilizados como respaldo en caso de una falla.

Cuando una señal viaja a lo largo de un cable va perdiendo fuerza a medida que avanza. Esta pérdida de fuerza puede causar pérdida de información. Los repetidores amplifican la señal que reciben permitiendo así que la distancia entre dos puntos de la red sea mayor que la que un cable solo permite.

Un ruteador es un dispositivo de propósito general diseñado para segmentar la red, con la idea de limitar tráfico de broadcast y proporcionar seguridad, control y redundancia entre dominios individuales de broadcast, también puede dar servicio de firewall y un acceso económico a una WAN.

El ruteador opera en la capa 3 del modelo OSI, es decir pueden filtrar protocolos y direcciones a la vez. Los equipos de la red saben que existe un router y le envían los paquetes directamente a él cuando se trate de equipos en otros segmentos.

El router tiene más facilidades de software que un Switch. Al funcionar en una capa mayor que la del Switch, el ruteador distingue entre los diferentes protocolos



de red, tales como IP, IPX, AppleTalk o DECnet. Esto le permite hacer una decisión más inteligente que al Switch, al momento de reenviar los paquetes.



Figura 13 Router Cisco 2800

En la figura 13 se muestra Router Cisco 2800, el ruteador realiza dos funciones básicas:

1. El router es responsable de crear y mantener tablas de ruteo para cada capa de protocolo de red, estas tablas son creadas ya sea estáticamente o dinámicamente. De esta manera el ruteador extrae de la capa de red la dirección destino y realiza una decisión de envío basado sobre el contenido de la especificación del protocolo en la tabla de ruteo.
2. La inteligencia de un router permite seleccionar la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC destino. Estos factores pueden incluir la cuenta de saltos, velocidad de la línea, costo de transmisión, retraso y condiciones de tráfico. La desventaja es que el proceso adicional de procesamiento de frames por un ruteador puede incrementar el tiempo de espera o reducir el desempeño del router cuando se compara con una simple arquitectura de Switch.

3. Poseen una entrada con múltiples conexiones a segmentos remotos, garantizan la fiabilidad de los datos y permiten un mayor control del tráfico de la red. Su método de funcionamiento es el encapsulado de paquetes.

Para interconectar un nuevo segmento a nuestra red, solo hace falta instalar un router que proporcionara los enlaces con todos los elementos conectados.

### **1.5.3 Gateway**

También llamados traductores de protocolos, son equipos que se encargan, como su nombre indica, a servir de intermediario entre los distintos protocolos de comunicaciones para facilitar la interconexión de equipos distintos entre sí.

Su forma de funcionar es que tienen duplicada la pila OSI, es decir, la correspondiente a un protocolo y, paralelamente, la del otro protocolo. Reciben los datos encapsulados de un protocolo, los van desencapsulando hasta el nivel más alto, para posteriormente ir encapsulando los datos en el otro protocolo desde el nivel más alto al nivel más bajo, y vuelven a dejar la información en la red, pero ya traducida. Los Gateways también pueden interconectar redes entre sí

### **1.5.4. Transceivers o Media Converter**

Son equipos que son una combinación de transmisor / receptor de información. El transceiver transmite paquetes de datos desde el controlador al bus y viceversa.

En una Ethernet, los transceivers se desconectan cuando el equipo al que están conectados no está funcionando, sin afectar para nada al comportamiento de la red.

## **1.6 Servidores de Terminales**

Son equipos que van conectados a la red, y en sus salidas generan una señal para un terminal, tanto síncrono como asíncrono, desde el cual se podrá establecer una sesión con un equipo o host.

El servidor de terminales es un dispositivo configurado para integrar terminales "tontas" o PCs por interface serie con un emulador de terminales. Puede utilizar los protocolos TCP/IP y LAT para una red Ethernet, y se puede acceder a cualquier ordenador que soporte TCP/IP o LAT (DECnet)

## **1.7 Sistemas Operativos**

Son los encargados de la funcionalidad y manejo de los recursos y/o periféricos de un equipo de cómputo.

### **1.7.1 Categorías de los sistemas operativos**

Sistema Operativo Multitareas: Es el modo de funcionamiento disponible en algunos sistemas operativos, mediante el cual una computadora procesa varias tareas al mismo tiempo. Existen varios tipos de multitareas. La conmutación de contextos (context Switching) es un tipo muy simple de multitarea en el que dos o más aplicaciones se cargan al mismo tiempo, pero en el que solo se esta

procesando la aplicación que se encuentra en primer plano (la que ve el usuario. En la multitarea cooperativa, la que se utiliza en el sistema operativo Macintosh, las tareas en segundo plano reciben tiempo de procesado durante los tiempos muertos de la tarea que se encuentra en primer plano (por ejemplo, cuando esta aplicación esta esperando información del usuario), y siempre que esta aplicación lo permita.

En los sistemas multitarea de tiempo compartido, como OS/2, cada tarea recibe la atención del microprocesador durante una fracción de segundo.

**Sistema Operativo Mono tareas:** Los sistemas operativos mono tareas son más primitivos y, solo pueden manejar un proceso en cada momento o que solo puede ejecutar las tareas de una en una.

**Sistema Operativo Monousuario:** Los sistemas monousuarios son aquellos que nada más puede atender a un solo usuario, gracias a las limitaciones creadas por el hardware, los programas o el tipo de aplicación que se este ejecutando.

**Sistema Operativo Multiusuario:** En esta categoría se encuentran todos los sistemas que cumplen simultáneamente las necesidades de dos o más usuarios, que comparten mismos recursos. Este tipo de sistemas se emplean especialmente en redes. En otras palabras consiste en el fraccionamiento del tiempo (timesharing).

**Secuencia por Lotes:** La secuencia por lotes o procesamiento por lotes en microcomputadoras, es la ejecución de una lista de comandos del sistema operativo uno tras otro sin intervención del usuario. Procesamiento por lotes también puede referirse al proceso de almacenar transacciones durante un cierto lapso antes de su envío a un archivo maestro, por lo general una operación separada que se efectúa durante la noche. Los sistemas operativos por lotes (batch), en los que los programas eran tratados por grupos (lote) en vez de individualmente. La función de estos sistemas operativos consistía en cargar en memoria un programa de la cinta y ejecutarlo. Al final este, se realizaba el salto a una dirección de memoria desde donde reasumía el control del sistema operativo que cargaba el siguiente programa y lo ejecutaba. De esta manera el tiempo entre un trabajo y el otro disminuía considerablemente.

**Sistema Operativo de Tiempo Real:** Procesa las instrucciones recibidas al instante, y una vez que han sido procesadas muestra el resultado.

**Sistema Operativo de Tiempo Compartido:** Consiste en el uso de un sistema por más de una persona al mismo tiempo. El tiempo compartido ejecuta programas separados de forma concurrente, intercambiando porciones de tiempo asignadas a cada programa (usuario)

Funciones de los sistemas operativos.

- Interpreta los comandos que permiten al usuario comunicarse con el ordenador.
- Coordina y manipula el hardware de la computadora, como la memoria, las impresoras, las unidades de disco, el teclado o el Mouse.
- Organiza los archivos en diversos dispositivos de almacenamiento, como discos flexibles, discos duros, discos compactos o cintas magnéticas.
- Gestiona los errores de hardware y la pérdida de datos.
- Servir de base para la creación del software logrando que equipos de marcas distintas funcionen de manera análoga, salvando las diferencias existentes entre ambos.

Los sistemas operativos más populares de las PC.

## **OS/2**

Desarrollado inicialmente por Microsoft Corporation e International Business Machines (IBM), después de que Intel introdujera al mercado su procesador 80286. Pero la sociedad no duro mucho ya que IBM veía a Windows como una amenaza para el SO/2.

El OS/2 al principio fue muy parecido al MS-DOS, tiene una línea de comando, pero la diferencia que existe con el DOS es el intérprete de comandos, el cual es un programa separado del kernel del sistema operativo y aparece únicamente cuando se hace clic en uno de los iconos "OS/2 prompt" dentro del Workplace Shell. Otra diferencia es que este sí es un sistema operativo multitarea. En el OS/2

muchos de los comandos son idénticos a los de su contra parte pero tiene más comandos debido a que es más grande, completo y moderno.

## **UNIX**

Es un sistema operativo multiusuario que incorpora multitarea. El sistema operativo UNIX tiene diversas variantes y se considera potente, más transportable e independiente de equipos concretos que otros sistemas operativos porque esta escrito en lenguaje C. El UNIX esta disponible en varias formas, entre las que se cuenta AIX, una versión de UNIX adaptada por IBM (para su uso en estaciones de trabajo basadas en RISC), A/ux (versión gráfica para equipos Apple Macintosh) y Mach (un sistema operativo reescrito, pero esencialmente compatible con UNIX, para las computadoras NeXT).

El UNIX y sus clones permiten múltiples tareas y múltiples usuarios. Su sistema de archivos proporciona un método sencillo de organizar archivos y permite la protección de archivos. Sin embargo, las instrucciones del UNIX no son intuitivas.

Este sistema ofrece una serie de utilidades muy interesantes, como las siguientes:

- Inclusión de compiladores e intérpretes de lenguaje.
- Existencia de programas de interfase con el usuario, como ventanas, menús, etc.
- Muchas facilidades a la hora de organización de ficheros.
- Inclusión de lenguajes de interrogación.
- Facilidades gráficas.
- Programas de edición de textos.

## **LINUX**

Linux es un sistema operativo completo con multitarea y multiusuario (como cualquier otra versión de UNIX). Esto significa que pueden trabajar varios usuarios simultáneamente en él, y que cada uno de ellos puede tener varios programas en ejecución.

Linux implementa la mayor parte de las características que se encuentran en otras implementaciones de UNIX, más algunas otras que no son habituales. En esta sección nos daremos una vuelta por todo ello.

El sistema Linux es compatible con ciertos estándares de UNIX a nivel de código fuente, incluyendo el IEEE POSIX.1, System V y BSD. Fue desarrollado buscando la portabilidad de las fuentes: encontrará que casi todo el software gratuito desarrollado para UNIX se compila en Linux sin problemas. Y todo lo que se hace para Linux (código del núcleo, drivers, librerías y programas de usuario) es de libre distribución.

Linux implementa todo lo necesario para trabajar en red con TCP/IP. Desde manejadores para las tarjetas de red más populares hasta SLIP/PPP, que permiten acceder a una red TCP/IP por el puerto serie. También se implementan PLIP (para comunicarse por el puerto de la impresora) y NFS (para acceso remoto a ficheros). Y también se han portado los clientes de TCP/IP, como FTP, TELNET, NNTP y SMTP.

El núcleo de Linux ha sido desarrollado para utilizar las características del modo protegido de los microprocesadores 80386 y 80486. En concreto, hace uso de la



gestión de memoria avanzada del modo protegido y otras características avanzadas. Cualquiera que conozca la programación del 386 en el modo protegido sabrá que este modo fue diseñado para su uso en UNÍX. Linux hace uso de esta funcionalidad precisamente.

El núcleo soporta ejecutables con paginación por demanda. Esto significa que sólo los segmentos del programa que se necesitan se cargan en memoria desde el disco. Las páginas de los ejecutables son compartidas mediante la técnica copy-on-write, contribuyendo todo ello a reducir la cantidad de memoria requerida para las aplicaciones.

Con el fin de incrementar la memoria disponible, Linux implementa la paginación con el disco:

Puede tener hasta 256 megabytes de espacio de intercambio o "swap"<sup>3</sup> en el disco duro. Cuando el sistema necesita más memoria, expulsará páginas inactivas al disco, permitiendo la ejecución de programas más grandes o aumentando el número de usuarios que puede atender a la vez. Sin embargo, el espacio de intercambio no puede suplir totalmente a la memoria RAM, ya que el primero es mucho más lento que ésta.

La memoria dedicada a los programas y a la caché de disco está unificada, Por ello, si en cierto momento hay mucha memoria libre, el tamaño de la caché de disco aumentará acelerando así los accesos. Los ejecutables hacen uso de las librerías de enlace dinámico, Esto significa que los ejecutables comparten el código común de las librerías en un único fichero, como sucede en Sun/OS. Así,

los ejecutables serán más cortos a la hora de guardarlos en el disco, incluyendo aquellos que hagan uso de muchas funciones de librería. También pueden enlazarse estáticamente cuando se deseen ejecutables que no requieran la presencia de las librerías dinámicas en el sistema.

El enlace dinámico se hace en tiempo de ejecución, con lo que el programador puede cambiar las librerías sin necesidad de recompilación de los ejecutables.

El nombre swap es inadecuado: no se intercambian procesos completos, sino páginas individuales.

Por supuesto, en muchos casos se expulsan al disco procesos completos, pero no siempre ocurre la imagen de memoria de los programas (ficheros). Entre esto y la posibilidad de compilar ejecutables con soporte de depuración, el programador podrá averiguar la causa de los fallos de su programa.

### **Microsoft Windows 2003 Server**

Microsoft no solo se ha dedicado a escribir software para PCs de escritorio sino también para poderosas estaciones de trabajo y servidores de red y bases de datos.

El sistema operativo Windows 2003 Server de Microsoft es un SO para redes que brinda poder, velocidad y nuevas características; además de las características tradicionales. Es un SO de 32, 64 bits, que puede trabajar en procesadores Pentium y Superiores.

Además de ser multitarea, multilectura y multiprocesador ofrece una interfaz gráfica.

Y trae todo el software necesario para trabajar en redes, permitiendo ser un cliente de la red o un servidor.

## **1.8 Servidores**

Con el nombre de Servidores se conocen los Microcomputadores o Computadores, utilizados para esta función dentro de una red de computadoras o dentro de un sistema de información empresarial o institucional.

Estos computadores tienen definidas características especiales, es decir, están conformados con altos recursos o elementos.

Existen equipos servidores que cuentan muchas veces con variedad de recursos, entre los que se destacan servidores con varios procesadores, variedad de procesadores, variedad de Discos Duros entre otras características más. Los servidores pueden contar con procesadores INTEL, RISC, entre otros más; de igual forma cuentan con variedad de sistemas de discos duros y sistemas de almacenamiento secundario, como es el caso de discos duros IDDE, SCSI entre otros.

En estos equipos servidores se procesan y/o almacenan toda la información que hace parte de las redes de computadoras.

En el mercado se conocen varios tipos y marcas de servidores entre los que se destacan:

Servidores de la Empresa IBM (AS/400, NEPHINITY, Otros)

Servidores Solaris, los cuales cuentan con el sistema operativo Unix de Sun Microsystems, Servidores de la Empresa Compaq, Servidores de la Empresa HP

## **1.9 Protocolos**

Un protocolo es la interfaz que permite la comunicación entre los equipos que se encuentren en red, aun cuando sean redes de distintas características. Los protocolos son muy fundamentales en todas las redes de computadoras ya que permiten que se pueda presentar la comunicación con los otros clientes o computadoras de una red, básicamente estos protocolos gestionan y nos permiten direccionar el tráfico a mover dentro de una red de computadoras.

Existe una gran variedad de protocolos pero básicamente en nuestro proyecto vamos a trabajar con el conjunto de protocolos TCP/IP y Netbios.

Pero antes de explicarlos es importante aprender que son los protocolos de la capa de red (IP), y de la capa de transporte (UDP, TCP), con esto haciendo la relación del modelo TCP/IP con el modelo OSI.

### **IP (Internet Protocol) Versión 4**

El Protocolo IP proporciona un sistema de distribución que es poco fiable incluso en una base sólida. El protocolo IP especifica que la unidad básica de transferencia de datos en el TCP/IP es el datagrama.

Los datagramas pueden ser retrasados, perdidos, duplicados, enviados en unas secuencias incorrectas o fragmentadas intencionadamente para permitir que un nodo con un buffer limitado pueda coger todo el datagrama. Es la responsabilidad del protocolo IP reensamblar los fragmentos del datagrama en el orden correcto. En algunas situaciones de error los datagramas son descartados sin mostrar ningún mensaje mientras que en otras situaciones los mensajes de error son recibidos por la maquina origen (esto lo hace el protocolo ICMP).

El protocolo IP también define cual será la ruta inicial por la que serán mandados los datos.

Cuando los datagramas viajan de unos equipos a otros, es posible que atraviesen diferentes tipos de redes. El tamaño máximo de estos paquetes de datos puede variar de una red a otra, dependiendo del medio físico que se emplee para su transmisión. A este tamaño máximo se le denomina MTU (Maximum Transmisión Unit), y ninguna red puede transmitir un paquete de tamaño mayor a esta MTU. El datagrama consiste en una cabecera y datos.

Hoy día muchas redes ya empezaron a trabajar con el protocolo IP V.6 la cual tiene 128 Bits.

### **UDP (User Datagram Protocol)**

El protocolo UDP (User Datagram Protocol) proporciona aplicaciones con un tipo de servicio de datagramas orientado a transacciones. El servicio es muy parecido al protocolo IP en el sentido de que no es fiable y no esta orientado a la conexión.

El UDP es simple, eficiente e ideal para aplicaciones como el TFTP y el DNS. Una dirección IP sirve para dirigir el datagrama hacia una maquina en particular, y el numero de puerto de destino en la cabecera UDP se utiliza para dirigir el datagrama UDP a un proceso especifico localizado en la cabecera IP. La cabecera UDP también contiene un número de puerto origen que permite al proceso recibido conocer como responder al datagrama.

### **TCP (Transmission Control Protocol)**

El protocolo TCP proporciona un servicio de comunicación que forma un circuito, es decir, que el flujo de datos entre el origen y el destino parece que sea continuo. TCP proporciona un circuito virtual el cual es llamado una conexión.

Al contrario que los programas que utilizan UDP, los que utilizan el TCP tienen un servicio de conexión entre los programas llamados y los que llaman, chequeo de errores, control de flujo y capacidad de interrupción.

### **TCP/IP**

Aunque poca gente sabe lo que es TCP/IP todos lo emplean indirectamente y lo confunden con un solo protocolo cuando en realidad son varios, de entre los cuales se destaca y es el más importante el protocolo IP. Bajo este nombre(TCP/IP)se esconde uno de los protocolos mas usados del mundo, debido a que es el mas usado por Internet y esta muy extendido en el sistema operativo UNIX.

En el 1973, la DARPA inició un programa de investigación de tecnologías de comunicación entre redes de diferentes características. El proyecto se basaba en la transmisión de paquetes de información, y tenía por objetivo la interconexión de redes. De este proyecto surgieron dos redes: Una de investigación, ARPANET, y una de uso exclusivamente militar, MILNET. Para comunicar las redes, se desarrollaron varios protocolos: El protocolo de Internet y los protocolos de control de transmisión. Posteriormente estos protocolos se englobaron en el conjunto de protocolos TCP/IP.

En 1980, se incluyó en el UNIX 4.2 de BERKELEY, y fue el protocolo militar estándar en 1983. Con el nacimiento en 1983 de INTERNET, este protocolo se popularizó bastante, y su destino va unido al de Internet. ARPANET dejó de funcionar oficialmente en 1990.

Algunos de los motivos de su popularidad son:

- Independencia del fabricante
- Soporta múltiples tecnologías
- Puede funcionar en máquinas de cualquier tamaño
- Estándar de EEUU desde 1983

La arquitectura de un sistema en TCP/IP tiene una serie de metas:

- La independencia de la tecnología usada en la conexión a bajo nivel y la arquitectura del ordenador
- Conectividad Universal a través de la red
- Reconocimientos de extremo a extremo
- Protocolos estandarizados
- Estructura Interna

El modelo básico en Internet es el modelo Cliente / servidor. El Cliente es un programa que le solicita a otro que le preste un servicio. El Servidor es el programa que proporciona este servicio.

La arquitectura de Internet esta basada en capas. Esto hace más fácil implementar nuevos protocolos. El conjunto de protocolos TCP/IP, al estar integrado plenamente en Internet, también dispone de este tipo de arquitectura. El modelo de capas de TCP/IP es algo diferente al propuesto por ISO (*International Standard Organization*) para la interconexión de sistemas abiertos (OSI). (Ver imágenes 1 y 2).

<b>Aplicación</b>						
<b>Presentación</b>	TELNET	FTP	SNMP	SMTP	DNS	HTTP
<b>Sesión</b>						
<b>Transporte</b>	TCP					
<b>Red</b>	IP					
<b>Liga de Datos</b>	802.2					X.25
	802.3	802.5	LAPB		LLC/SNAP	
<b>Física</b>	Ethernet	Token Ring	FDDI	Línea Síncrona WAN		SONET

Imagen 1. Relación del modelo TCP/IP con el modelo OSI



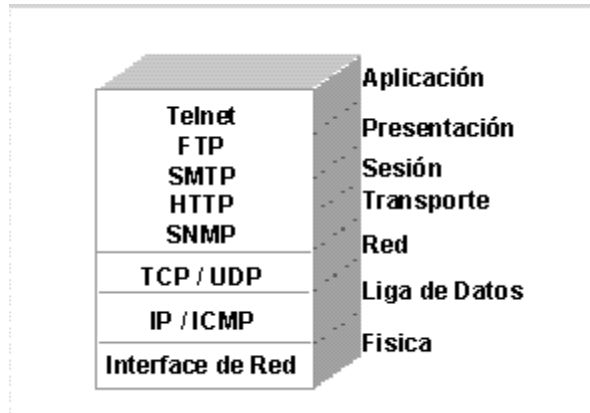


Imagen 2. Modelo de capas de TCP/IP

### 1.10. Bases de datos y aplicaciones

Son básicamente la información que se transportará, a través de las redes de computadoras y las cuales trabajan los usuarios finales de las redes de datos; este tipo de aplicaciones o bases de datos necesitan moverse eficientemente dentro de la red para que las personas que las utilizan puedan brindar un excelente servicio y puedan producir, mucho más que personas que posean bases de datos lentas y poco constantes.

Además otro aspecto a tener en cuenta en las redes de computadoras, es lo correspondiente a la integridad, seguridad de los datos y de los elementos que conforman la red.

Existen muchos gestores de bases de datos en el mercado, en el proyecto se tuvo en cuenta las bases de datos de la universidad, las cuales están bajo el gestor de bases de datos Oracle.

## **1.11 Seguridad informática**

Aunque una Intranet es una red privada en la que se tengan grupos bien definidos y limitados, esta no se encuentra exenta de ataques que pudiese poner en riesgo la información que maneja, ya que la mayoría de estos son provocados por sus mismos usuarios.

La mayoría de las estadísticas de seguridad en los sistemas de cómputo indican que cerca del 80% de los fraudes relacionados con las computadoras provienen de los usuarios internos, por esto las Redes de datos de los sistemas de información son las más vulnerables a ataques de ésta índole.

Según el CSI (Instituto de Seguridad de Computadores) de San Francisco el 90% de las empresas entrevistadas detectó ataques a sus computadoras, el 70% reportó que los más comunes fueron virus y ataques de abuso de la red de sus empleados.

Ahora también ahí que tener en cuenta que a menos que la computadora que usted esté tratando de proteger se encuentre en una habitación cerrada, en la que se controle el acceso y no existan conexiones con el exterior, su computadora estará en peligro. En todo el mundo, todos los días se producen entradas no autorizadas y violaciones de la seguridad.

Estos violadores no solo son los vándalos de Internet, sino también los empleados de la oficina de al lado que roban tiempo de computadoras y servicios para su uso personal o para fines mal intencionados<sup>1</sup>.

Además de los vándalos de Internet y de los empleados internos en este proyecto hay que tener en cuenta a los empleados mal intencionados que pueden utilizar cualquiera de los computadores de la Universidad, incluso los de los laboratorios para tratar de causar un caos o eliminar cualquier información que los afecte como es el caso de notas académicas bajas y que estarán dispuestos a sabotearlas o modificarlas, por ello hay que tener en cuenta a estos estudiantes en este Proyecto de Grado.

Entrando a definir el concepto de seguridad informática, seguridad en redes de computadoras podemos anotar que definir la seguridad informática como tal es muy complicado pero hay que tener en cuenta posibles diferencias de autores al respecto que definen la seguridad informática dependiendo de la información que queramos proteger o mantener estable y segura, es por ello que se escucha y se pueden leer documentos sobre:

Seguridad en intranet.

Seguridad en Internet.

Seguridad en la Web (En lo referente a Comercio Electrónico).

Seguridad en Redes de Computadores.

---

<sup>1</sup> Firewalls y la Seguridad en Internet (Segunda Edición) Keranyit Siyan y Chris Hare Prentice Hall Hispanoamericana s.a.

Seguridad en Base de Datos.

Seguridad Física de Centro de Computo.

Seguridad de Hardware o Equipos Activos.

Además de estas definiciones o temas sobre seguridad informática existen otros factores a proteger, por lo cual se concluye que es un tema bastante extenso e importante para la actual sociedad de la información.

### **1.12. Calidad de Servicio (QoS)**

Este es un concepto bastante amplio y de mucha importancia en las actuales de redes de computadores a nivel mundial, trata de herramientas y configuraciones que ayudan a garantizar los espacios, las prioridades y los anchos de banda que requieren los servicios convergentes que se mueven en las actuales Redes de Comunicaciones.

Existen muchos más conceptos que se trabajan en este proyecto caso puntuales como Telefonía IP, Videoconferencia IP y otros servicios específicos de muchos de los temas ya planteados y por ello no se tienen estas referencias.

Nota: Las imágenes de las figuras de dispositivos que se utilizaron eran de marca Linksys, Cisco Systems y 3com con esta últimas marca de dispositivos se trabajó debido a su rendimiento y porque teníamos disponible ese recurso, pero se debe aclarar que no solamente existe esas marcas de dispositivos existen otras marcas como por ejemplo D-link, Huawei, etc.

## 2. REDES CONVERGENTE Y CALIDAD DE SERVICIO (QoS)

En la actualidad es más práctico y económico portar voz sobre redes de datos que construir, operar y proveer redes separadas de datos y de voz. Las Redes Convergentes o de Nueva Generación son redes capaces de manejar comunicaciones de datos, voz y vídeo de manera eficiente, con disponibilidad y desempeño consistente, haciendo una diferenciación en la Clase de Servicio (CoS) y ofreciendo una Calidad de Servicio (QoS) fiable para cada tipo de tráfico. (Por ejemplo: voz, datos privados, acceso a Internet y vídeo.) La Red Convergente debe contar con la infraestructura de conmutación y transporte de paquetes nativos de datos y debe contar con un servicio flexible de control de elementos para habilitar las comunicaciones y soportar datos y QoS (Quality of Services).<sup>2</sup>

A nivel mundial están siendo implementadas estas redes y cada día son más las empresas que por la necesidad de optimizar sus gastos operativos están optando por tener redes convergentes que les permita disfrutar de todos los beneficios y bondades que esta ofrece; hay que tener presente que la tecnología está avanzando a paso agigantados y un ejemplo claro son las redes de telecomunicaciones, las cuales han avanzado tanto que es posible conectarse al mundo digital desde diversos aparatos electrónicos en casi cualquier parte del mundo, nos estamos refiriendo a las redes de nueva generación, estas redes son la integración de todos los servicios disponibles al momento de establecer la comunicación por voz, video, datos y otros servicios basados en el protocolo IP.

Los usuarios hoy día tienen muchas necesidades de comunicaciones por lo que demandan que esta comunicación se establezca de una manera rápida y eficiente; si se requiere reducir costos en el momento de realizar este proceso, una alternativa real sería unir estos medios de comunicación en un solo medio de transporte, esto se puede lograr utilizando Redes Convergentes, ya que estas integran bajo una misma plataforma voz, datos, vídeo y otra gran variedad de

---

<sup>2</sup> <http://www.itba.edu.ar/capis/epg-tesis-y-tf/garcia-tfe.pdf>

servicios; para ofrecer una gama de servicios como telefonía tradicional, servicios corporativos, Internet de alta velocidad y videoconferencias.

El término convergencia de redes hace mención a la “Unión de Infraestructuras basadas en distintos tipos de redes como son las correspondientes a las líneas telefónicas, las cuales se basan en técnicas de conmutación de circuitos y las redes que se emplean para el tráfico de datos, que como ya es sabido se basan en técnicas de conmutación de paquetes”<sup>3</sup>. Adicional a esta definición de Convergencia se puede decir que es la opción de trabajar múltiples servicios de redes como Voz IP, Telefonía IP, Datos, Video IP, Videoconferencias IP y otros servicios por un único sistema de interconexión o infraestructura tecnológica.

Estas redes convergentes son las que mayor utilización tienen hoy día a nivel mundial, pues cada vez más empresas ven la necesidad de implementarlas, dadas sus políticas de productividad y competitividad, estas redes son conocidas también a nivel mundial como NGN (Redes de Nueva Generación).

Estas ideas han surgido de diversos estudios relacionados con los tipos de datos en cuestión, la viabilidad de las distintas redes, la calidad de servicios integrados, la necesidad consumista de los distintos tipos de usuario, que ponen a este término como el nuevo símbolo del progreso, en síntesis como NGN (Redes de Nueva Generación).

Uno de los mayores logros de la convergencia en las redes de comunicaciones y de computadoras, es sin duda alguna el permitir en la misma “línea” la voz, los datos, videos, Telefonía, que en conclusión son muchos servicios y requerimientos de anchos de banda que estas infraestructuras tecnológicas debe soportar; es por

---

<sup>3</sup> AT&T , Boletín de Prensa, “Mayor Competitividad: Principal Beneficio De La “Convergencia De Redes

ejemplo que estas tecnologías se ven obligadas a establecer un modelo que pueda empaquetar la voz para que pueda ser transmitida junto con los datos, también y como apoyo a este proceso se hace necesario la optimización del uso del ancho de banda de la red, para la realización de este cometido.

En estas redes de nueva generación, existe un único elemento básico que es el paquete de información y todo el sistema está diseñado para su administración, acceso, transporte y conmutación de extremo a extremo y basado en una única tecnología.

Lo dicho anteriormente ha sido posible gracias a las investigaciones lideradas por empresas y academia que creen que este tipo de sistemas es la llave de la evolución, las cuales se fundamentan en el principio que dice que la mejoría al servicio, al cliente tiene más peso que los costos menores en telefonía. Además de esto, es posible decir que estas grandes empresas no son las únicas que se beneficiarían de este tipo de avances tecnológicos ya que este tipo de sistemas puede beneficiar también a los clientes finales, llevándoles servicios con mejores tiempos de respuestas, menor cantidad de equipos individuales, integración de servicios en los mismos dispositivos de comunicaciones, entre otras ventajas. En Colombia el SENA y CINTEL inauraron el 1 de septiembre del 2010 el primer laboratorio para latinoamerica para el desarrollo de conocimientos de redes Avanzadas NGN, Es importante destacar que la incorporación de las Redes de Nueva Generación (NGN) como plataformas de telecomunicaciones ha acelerado cada vez más el proceso de convergencia de redes fijas y móviles, la integración de servicios y la interoperabilidad entre diferentes dispositivos del cliente final. Es así como las redes NGN, en prospectiva tecnológica, se constituyen en la base para la creación y desarrollo de las sociedades donde los ciudadanos y empresas podrán tener acceso a los servicios desde cualquier lugar, con cualquier dispositivo, en cualquier momento promoviendo así el desarrollo de proyectos tecnológicos y la implementación de tecnologías de punta.

Los beneficios de utilizar e implementar estas tecnologías según fuentes universales serían:

- Autogestión y simplicidad de administración.
- Acceso permanente a Internet como servicio “básico”.
- Video streaming bajo demanda para Tele educación.
- Broadcasting de TV comercial.
- Video Básico para uso Familiar.
- Aplicaciones Peer to Peer y acceso a repositorios públicos de video y audio.

Se define en muchos libros y teorías que para tener unos excelentes parámetros de calidad de las comunicaciones en estas redes convergentes es indispensable contar con un rango de calidad en todos y cada uno de los servicios convergentes, es por ello que muchos letrados en la parte de internetworking recomiendan la implementación de estas políticas de Calidad de Servicio, reconocidas a nivel mundial como QoS.

Se podría decir que es más práctico y económico portar voz sobre redes de datos, que construir, operar y proveer redes separadas de datos y de voz. Las Redes Convergentes ó de Nueva Generación son redes capaces de manejar comunicaciones de datos, voz y vídeo de manera eficiente, con disponibilidad y desempeño consistente, haciendo una diferenciación en la Clase de Servicio y ofreciendo una Calidad de Servicio (QoS) fiable para cada tipo de tráfico.



## 2.1 CALIDAD DE SERVICIO (QoS)

El término calidad de servicio (QoS) se refiere a la capacidad de brindar un servicio que se ajuste a un conjunto de requisitos que la red debe cumplir para asegurar el nivel adecuado en la transmisión de los datos, en cuanto a tiempo de respuesta y ancho de banda, estos requisitos se basan en los estándares de funcionalidad de QoS, que a su vez indica la capacidad de garantizar un nivel aceptable de pérdida de paquete, definido contractualmente, por un uso dado (voz sobre IP, video-conferencia, etc.)<sup>4</sup>

En efecto, a diferencia de las redes de conmutación de circuitos, como la red telefónica conmutada, donde existe un circuito de comunicación dedicado exclusivamente a la comunicación, en Internet es imposible predecir la ruta que toman los diferentes paquetes.

Por lo tanto, nada garantiza que una comunicación que requiera de un ancho de banda constante se lleve a cabo sin incidentes. Es por ello que existen mecanismos, denominados mecanismos QoS, que posibilitan clasificar los diferentes flujos de red y reservar una parte del ancho de banda para aquéllos que necesiten un servicio continuo, sin interrupciones “Prioridades”.

Cuando no existe Calidad de Servicios se pueden percibir cosas como:

- En cuanto a la voz, se presentan interrupciones, no se comprende, se repite un efecto de entrecortado, no se sabe cuándo termina de hablar la persona o cuando empezó, se desconectan las llamadas, se escuchan voces robotizadas, entre otras situaciones más.
- Con los Videos se perciben movimientos erráticos, audio fuera de sincronismo, imágenes lentas.

---

<sup>4</sup>Guía de aprendizaje ccna 3 and 4, versión 3.1, cisco -networking

- Y los datos presentan tiempos variables de respuesta, pantallas que no terminan de abrirse”<sup>5</sup>.

Estos aspectos fueron tenidos en cuenta en este proyecto para convalidar estas afirmaciones y para tener bases prácticas sobre el tema.

Por estas razones y como solución a estos problemas en el mundo productivo, se han implementado varios protocolos para el manejo de la calidad de servicio, con el fin de que el usuario final no perciba retrasos en la información que maneja y además, el servicio prestado satisfaga todas las expectativas esperadas por el mismo.

Para que una red sea capaz de brindar un servicio punto a punto o extremo a extremo se deben definir los niveles de requisitos, con un determinado tráfico. Generalmente existen tres niveles de QoS definidos:

- ✓ Máximo esfuerzo no diferencia diferentes flujos de red y no brinda ninguna garantía. También se denomina falta de QoS.
- ✓ Servicio diferenciado o QoS bajo permite definir los niveles de prioridad de diferentes flujos de red, pero no brinda una garantía estricta.
- ✓ Servicio garantizado o QoS alto reserva todos los recursos de red para determinados tipos de flujo. El mecanismo principal utilizado para obtener dicho nivel de servicio es RSVP (Resource reservation Protocol [Protocolo de reserva de recursos])<sup>6</sup>.

La calidad de servicio se puede evaluar a través de diferentes criterios:

---

<sup>5</sup> <http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/1115/3/T10971CAP3.pdf>

<sup>6</sup> <http://en.kioskea.net/contents/internet/qos-qualite-de-service.php3>

- Ancho de banda: Es uno de los parámetros más importante en cuanto a la calidad del servicio, este define el volumen máximo de información (bits) por unidad de tiempo.
- Variación de retardo (jitter): Es la medida de variación de delay entre paquetes consecutivos en un determinado flujo de tráfico, genera un efecto importante sobre las aplicaciones sensibles al delay en tiempo real, como voz y video ya que estas deben recibir paquetes en una tasa relativamente constante, con un delay fijo entre los paquetes consecutivos. A medida que varía la tasa de delay, el jitter impacta sobre el rendimiento de la aplicación. Una cantidad mínima de jitter puede ser aceptable, pero a medida que éste se incrementa, esa aplicación puede terminar siendo inútil. .
- Retardo (Delay): esto caracteriza el retraso entre la transmisión y la recepción de un paquete, puede generar problemas en las aplicaciones como la voz y video cuando son excesivos.
- Pérdida de paquetes: esto se relaciona con la falta de entrega de un paquete de datos, la mayoría de las veces debido a una sobrecarga de la red.
- Pérdida de secuencia: es una modificación en el orden de llegada de los paquetes<sup>7</sup>.

Todos los anteriores Parámetros y elementos se estudiaron en este proyecto, dado que todos afectan y son indispensables de tener en cuenta en este tipo de transmisiones convergentes y por ende fueron contemplados todos en el proyecto. Algunos de estos se involucraron para convalidar estos datos y mirar de qué manera se pueden corregir este tipo de problemas en las redes de comunicaciones convergentes actuales.

---

<sup>7</sup>[http://anixtersoluciones.com/latam/co/informacion\\_general/2078/la\\_importancia\\_de\\_la\\_calidad\\_de\\_servicio\\_qos\\_\\_\\_parte\\_ii\\_es.htm](http://anixtersoluciones.com/latam/co/informacion_general/2078/la_importancia_de_la_calidad_de_servicio_qos___parte_ii_es.htm)

## 2.2 FUNCIONAMIENTO DE LOS SERVICIOS (VOZ IP, DATOS, VIDEO IP)

### SERVICIO VOIP

La voz sobre IP convierte las señales de voz estándar en paquetes de datos comprimidos que son transportados a través de redes de datos en lugar de líneas telefónicas tradicionales. La evolución de la transmisión conmutada por circuitos a la transmisión basada en paquetes toma el tráfico de la red pública telefónica y lo coloca en redes IP bien provisionadas. Las señales de voz se encapsulan en paquetes IP que pueden transportarse como IP nativo o como IP por Ethernet, Frame Relay.<sup>8</sup>

Para poder hacer la llamada y escuchar la voz en los dispositivos finales ocurre lo siguiente: se transforma la voz en paquetes de información manejables por una red IP, por medio de otros protocolos de comunicación, como el RSVP (Protocolo de Reserva de Recursos), es posible reservar cierto ancho de banda dentro de la red que garantice la calidad de la comunicación.

La voz puede ser obtenida desde un micrófono conectado a la placa de sonido de la PC, o bien desde un teléfono común. Una vez alcanzado el servidor más próximo al destino, esa llamada vuelve a ser traducida como información analógica y sea transmitida hacia un teléfono común por la red telefónica tradicional.

---

<sup>8</sup> <http://platea.pntic.mec.es/~lmarti2/voip/tecnologia/tecnologia.html>



### Pila de protocolos en VoIP

Después de haber constatado que desde un PC con elementos multimedia, es posible realizar llamadas telefónicas a través de Internet, podemos pensar que la telefonía en IP es poco más que un juguete, pues la calidad de voz que obtenemos a través de Internet es muy pobre. No obstante, si en una empresa se dispone de una red de datos que tenga un ancho de banda bastante grande, también se puede pensar en la utilización de esta red para el tráfico de voz entre las distintas delegaciones de la empresa. Las ventajas que se obtendrían al utilizar esta red para transmitir la voz son evidentes:

- Ahorro de costos de comunicaciones pues las llamadas entre las distintas sucursales de la empresa saldrían gratis.
- Integración de servicios y unificación de estructura

### Procesos para convertir la voz en paquetes

El Dr. Harry Nyquist (y muchos otros) ha creado un proceso que permite al equipo convertir las señales analógicas (formas de onda de flujo) en formato digital (1s y 0s). Después de mucha investigación, Nyquist encontró que él podría reconstruir con precisión los flujos de audio de la toma de muestras numeradas que el doble de la frecuencia más alta de audio utilizado en el audio.

Así es como se rompe las frecuencias de audio varían según el volumen, tono,

etc. Que componen el sonido Aquí están algunos hechos clave:

- El oído humano promedio es capaz de oír frecuencias de 20-20.000 Hz.
- El lenguaje humano utiliza frecuencias de 200-9000 Hz.
- Los canales telefónicos suelen transmitir frecuencias de 300-3400 Hz.
- El teorema de Nyquist es capaz de reproducir frecuencias de 300-4000 Hz.

Los estudios han encontrado que el equipo de teléfono puede transmitir con precisión la conversación humana comprensible mediante el envío de sólo una gama limitada de frecuencias. El canal telefónico gama de frecuencias (300-3400 Hz) le da un sonido de calidad suficiente para identificar a la persona que llama a distancia y el sentido de su estado de ánimo. El canal telefónico rango de frecuencias no envía toda la gama de inflexión de la voz humana y reduce la calidad real del audio. Por ejemplo, si alguna vez has escuchado hablar de radio, siempre se puede notar la diferencia de calidad entre el conductor de radio y de la persona que llama por teléfono. Nyquist creía que podía reproducir con exactitud una señal de audio mediante un muestreo al doble de la frecuencia más alta. Porque él fue después de las frecuencias de audio de 300-4000 Hz, significaría muestreo 8000 veces ( $2 * 4000$ ) por segundo. Entonces, ¿qué es una muestra? Una muestra es un valor numérico. Más concretamente, en el ámbito de voz, una muestra es un valor numérico que consume un solo byte de información el teorema de Nyquist establece que es necesario tener 8000 de las muestras de cada segundo, 8.000 muestras una segunda vez los 8 bits en cada muestra, y usted consigue 64.000 bits por segundo, A continuación se muestra los valores de consumo de ancho de banda de los códec de audio.

CODEC	CONSUMO DE ANCHO DE BANDA
<b>G.711</b>	64Kbps
<b>Internet Low Bitrate códec (iLBC)</b>	15.2 Kbps
<b>G.729</b>	8Kbps
<b>G.726</b>	32 Kbps
<b>G.729<sup>a</sup></b>	8 Kbps
<b>G.728</b>	16 Kbps

Antes de implementar VoIP a través de conexiones WAN, se debe saber exactamente el ancho de banda que el códec que se está utilizando consumen. Aunque es fácil ver una tabla de cantidades de ancho de banda códec, se puede utilizar varios métodos para encontrar la cantidad de ancho de banda necesario para una llamada de voz. El siguiente proceso es uno de los más fáciles de recordar.

Paso 1: Determinar el ancho de banda de audio requerido para el códec de audio  
 Para encontrar la cantidad de ancho de banda necesario para el códec de audio, es necesario determinar el tamaño (en bytes) de audio contenidas en cada paquete. Este tamaño es directamente afectado por el tamaño de la muestra de audio contenida en cada paquete. El tamaño de la muestra es un intervalo de tiempo específico de audio. Para la mayoría de los codecs de audio, el tamaño de la muestra es de 20 milisegundos (ms), de forma predeterminada. Aumentar el tamaño de la muestra le da un beneficio de ahorro de ancho de banda ya que el Router envía menos paquetes en general (y menos paquetes significan menos información de encabezado). El inconveniente de aumentar el tamaño de la muestra es que el retraso general en la construcción del paquete es mayor. Si los dos dispositivos que se comunican ya tiene un retraso significativo entre ellos (debido a la distancia, el tráfico de compartir el enlace, y así

sucesivamente), el retardo de codificación adicional podría perjudicar la calidad de servicio (QoS). Se puede utilizar la siguiente fórmula para determinar el tamaño de la carga útil de voz:<sup>9</sup>

$$\text{Bytes por Paquete} = (\text{tamaño de la muestra} * \text{ancho de banda del Códec}) / 8$$

Ejemplo

G-711

$$\text{Bytes por Paquete} = (.02 * 64000) / 8$$

$$\text{Bytes por Paquete} = 1280 / 8$$

$$\text{Bytes por Paquete} = 160$$

En el anterior ejemplo se tomó el códec G.711 para determinar la carga útil de voz.

Para que una red de VoIP pueda operar con éxito, el tráfico de voz debe tener prioridad sobre el tráfico de datos a medida que recorre su camino desde un extremo de la red a la otra. Las necesidades de el tráfico de voz, no solo requiere de ancho de banda (VoIP utiliza muy poco ancho de banda en comparación con la mayoría de las aplicaciones de datos), sino algunos requerimientos de Delay. A diferencia de los datos, el tiempo que tarda un paquete de voz para ir de un extremo de la red es otro asunto. Si un paquete de datos que cruzan la red tiene un retraso, una barra de transferencia de archivos puede tardar un par de segundos para completar o una página web puede tener una segunda mitad más en cargarse. Desde la perspectiva de un usuario, éste no es un gran problema. Sin embargo, si el tráfico de voz al cruzar la red tiene un retraso, las conversaciones comienzan a superponerse (una persona comienza a hablar al mismo tiempo que otra persona), la conversación se rompe, en casos extremos se caen las llamadas.

Para combatir estos problemas, se debe garantizar no solamente haya un ancho de banda disponible para tráfico de VoIP, pero que el tráfico de VoIP obtenga

---

<sup>9</sup> CCNA VOICE, Cisco Systems



primero el ancho de banda disponible. Esto significa que si hay un cuello de botella en la red donde un Router con tráfico en cola antes de que sea enviado, el router moverá el tráfico de voz en espera por delante del tráfico de datos que se enviarán en el primer intervalo disponible.

Los siguientes son los tres enemigos de para el tráfico de VoIP:

- ✓ **La falta de ancho de banda:** Múltiples flujos de tráfico de voz y datos están compitiendo por una cantidad limitada de ancho de banda, Una conversación de voz tradicional consume un ancho de banda de 64 Kbps, cuando se transmite a través de una red Voip, la información de voz puede ser comprimida y digitalizada. Esta compresión puede reducir el ancho de banda a cantidades próximas a los 5 Kbps Para transmitir los paquetes de voz a través de una red IP, deben añadirse como se ha dicho las cabeceras apropiadas de IP/UDP/RTP. Esto puede requerir un substancial aumento de ancho de banda para cada llamada (sobre 40 bytes por paquete). La compresión de cabeceras RTP, sin embargo, puede reducir el tamaño de dichas cabeceras , hasta los dos bytes solamente
  
- ✓ **Delay:** El tiempo que tarda un paquete para desplazarse desde el punto de partida original a la final destino; retraso se presenta en tres formas:
  
- ✓ **Delay Fijo:** Los valores de retraso que no se puede cambiar, por ejemplo, se necesita una cierta cantidad de tiempo para un paquete para viajar distancias geográficas específicas. Este valor se considera fijo. Calidad de servicio no puede tener un impacto problemas corregidos inmediatamente.
  
- ✓ **Delay Variable:** los valores de retardo que puede cambiar, por ejemplo, colas retraso (El tiempo que un paquete de espera en la cola de la interfaz de un router) es variable, ya que depende de cuántos paquetes se encuentran

actualmente en la cola. Usted puede tener un impacto cola demora selectivamente mover los paquetes de voz delante de los paquetes de datos.

✓ **Jitter (variaciones de retardo):** describe los paquetes que tienen diferentes cantidades de demora entre ellos, por ejemplo, de paquete de primera voz de una conversación podría tomar 100 ms para llegar a un destino, mientras que el paquete de segunda voz podría tomar 110 ms. No es de 10 m de la variación de retardo (jitter) entre estos paquetes.

✓ **La pérdida de paquetes:** Los paquetes perdidos debido a una conexión de red congestionada poco fiables, esta pérdida de paquetes también ocurre cuando un router no tiene suficiente espacio en el buffer sobre una interface para mantener la nueva entrada de paquetes y comienza a descartar estos nuevos paquetes, esto puede causar daños severos en la calidad de la voz transmitida por ip, cada paquete ip contiene entre 40 y 80ms de voz, que corresponde a una duración de unidades fundamentales de voz como lo son los fonemas: cuando se pierde un paquete se pierde un fonema. aunque el cerebro humano es capaz de reconstruir algunos fonemas perdidos, demasiadas pérdidas pueden generar una señal que no se puede comprender. <sup>10</sup>

✓ **Serialización:** Describe lo que ocurre cuando un router intenta enviar paquetes de voz y datos simultáneamente a través de una interfaz. En general, los paquetes de voz son más pequeños (de 80 a 256 bytes) que los paquetes de datos (de 1500 a 18000 bytes). En enlaces lentos, como conexiones WAN, los paquetes grandes pueden tardar en ser enviados, cuando estos paquetes están mezclados con pequeños paquetes de voz, el excesivo tiempo de transmisión puede llevar a retardos y jitter. <sup>11</sup>

---

<sup>10</sup> CCNA VOICE, Cisco Systems

<sup>11</sup> <http://upcommons.upc.edu/pfc/bitstream/2099.1/7966/1/PFC.pdf>

Los usuarios están acostumbrados a un ambiente PBX (Central Telefónica Digital) en el que existe una red separada y ancho de banda dedicado asignado sólo para el tráfico de voz. La tolerancia a eco, o caídas de llamadas de una red de voz es muy baja. Si se cuenta con un entorno de red en la que el cable de fibra óptica es la norma y las velocidades de gigabit abundan, nunca se podrá experimentar congestión de la red. Estos ambientes se consiguen poco o nada de ganancia mediante el uso de calidad de servicio porque las herramientas de calidad de servicio sólo participarían en momentos de congestión de la red. El objetivo con calidad de servicio es proporcionar ancho de banda constante para el tráfico de voz de tal manera de que si hay un pequeño y constante retraso de un extremo de la red a la otra. Para lograr esto, es necesario tener calidad de servicio de alguna forma en cualquier punto de la red donde existe congestión. Esto significa hacer una auditoría de extremo a extremo de la red para determinar los tipos de tráfico que existen y los niveles de servicio requeridos para los diversos tipos de tráfico.

Cuando los paquetes VoIP cruzan la red IP, estos son transportados mediante el Real-Time Transport Protocol (RTP) y RTP Control Protocol (RTCP) y se utiliza User Datagram Protocol (UDP) como protocolo de transporte. RTP utiliza mecanismos para la sincronización de los frames de la voz como los timestamps y números de secuencia.

RTCP provee mecanismos para informar de la calidad de la voz de las llamadas mediante medidas de retraso, jitter y paquetes perdidos. VoIP no utiliza TCP como protocolo de transporte debido a que TCP, que garantiza las retransmisiones, introduce para ello mecanismos de acuse de recibo, lo que conlleva retrasos intolerables en el tráfico de voz. VoIP usa, además de los citados protocolos (RTP/UDP/IP) para el transporte de llamadas, otros protocolos de señalización para el establecimiento y la desconexión de las llamadas, para transmitir la información de búsqueda de usuarios, y para el intercambio de algoritmos de

compresión de la voz. Los protocolos más usuales son H.323, Media Gateway Control Protocol (MGCP), Session Initiation Protocol (SIP), y Skinny Client Control Protocol (SCCP) propietario de Cisco.<sup>12</sup>

✓ **Requerimientos de servicios de voz, video y tráfico de Datos**

A diferencia del tráfico de datos, el tráfico de voz es muy predecible, considerando que el tráfico de datos puede saltar considerablemente si una descarga de Internet de gran tamaño o de transferencia de archivos se inicia, el tráfico de voz sigue siendo un valor constante para cada llamada que entra y sale de la red. La cantidad real de ancho de banda necesario para voz depende en gran medida el códec que esté utilizando. Además de los requisitos de ancho de banda, el tráfico de voz tiene los siguientes requisitos adicionales de un solo sentido:

Delay de extremo a extremo: 150 (milisegundos) ms o menos

Jitter: 30 ms o menos

La pérdida de paquetes: 1% o menos

El tráfico de voz difiere del tráfico de datos en los siguientes puntos:

- ✓ Los datos a menudo forman ráfagas, mientras que la voz sigue una pauta más determinista.
- ✓ Las aplicaciones de datos reenvían los paquetes perdidos, mientras que las aplicaciones de voz tratan de “disimular” los paquetes perdidos.
- ✓ Las aplicaciones de datos pueden tolerar algunos retardos, mientras que las aplicaciones de voz deben minimizar el retardo.

Estas diferencias provocan el uso de estrategias diferentes de QoS para obtener una estricta prioridad del tráfico de voz y garantizar de un lado la transmisión correcta de los datos y de otro un retardo mínimo en las redes que transportan voz y datos.

---

<sup>12</sup> <http://upcommons.upc.edu/pfc/bitstream/2099.1/7966/1/PFC.pdf>

## SERVICIO DE DATOS

Inicialmente, se puede pensar que los datos se envían desde un equipo a otro como una serie continua de unos y ceros. De hecho, los datos se dividen en paquetes pequeños y manejables, cada uno dividido con la información esencial para ir desde el origen hasta el destino. Los paquetes son bloques básicos que constituyen la comunicación de datos por la red.

✓ *Función de los paquetes en las comunicaciones en red*

Normalmente los datos existen como archivos de gran tamaño. Las redes no podrían funcionar si los equipos colocasen a la vez grandes cantidades de datos en la red. Un equipo que envíe grandes cantidades de datos hace que otros equipos tengan que esperar (incrementando la frustración de los otros usuarios) mientras se transmiten los datos. Hay dos razones por las que la colocación de grandes bloques de datos en el cable hace lenta a la Red:

1. Las grandes cantidades de datos enviados como un único bloque colapsan la red y hacen imposible la interacción y comunicación apropiada debido a que un equipo está desbordando el cable con datos.
2. El impacto de la retransmisión de grandes bloques de datos multiplica el tráfico de la red.

Estos efectos se minimizan cuando estos grandes bloques de datos se dividen en paquetes más pequeños para una mejor gestión del control de errores en la transmisión. De esta forma, sólo se afecta a una pequeña cantidad de datos, y por tanto, sólo se tienen que volver a transmitir pequeñas cantidades de datos, facilitando la recuperación de un error.

Para que varios usuarios puedan transmitir a la vez datos por la red de forma rápida y sencilla, hay que dividir los datos en bloques pequeños y manejables. De esta forma, los usuarios pueden compartir su acceso a la red. Estos bloques se denominan paquetes, o tramas. Aunque los términos de «paquete» y «trama» se suelen utilizar indistintamente, hay algunas diferencias dependiendo del tipo de red.

El término paquete se utiliza para hacer referencia a una unidad de información transmitida como una entidad desde un dispositivo a otro de la red.

Cuando el sistema operativo de la red del equipo de origen divide los datos en paquetes, añade a cada trama una información de control especial. Esto hace posible:

1. El envío de los datos originales en pequeños paquetes.
2. La reorganización de los datos en el orden apropiado cuando lleguen a su destino.
3. La comprobación de errores una vez que se hayan reorganizado los datos.<sup>13</sup>

✓ ***Requisitos de red de datos***

No se puede hablar de una forma radical para todas las aplicaciones de datos, ya que todas las aplicaciones de datos que existen tienen su propia exigencia de calidad de servicio. Cuando el diseño de QoS para las aplicaciones de datos en su red, usted debe dividir sus aplicaciones en no más de cuatro o cinco grandes categorías. Por ejemplo:

- ✓ ***Aplicaciones de misión crítica:*** Se trata de aplicaciones que son críticas para su organización, que requieren cantidades ancho de banda dedicado.

---

<sup>13</sup> [http://fmc.axarnet.es/redes/tema\\_03.htm](http://fmc.axarnet.es/redes/tema_03.htm)

- ✓ **Aplicaciones transaccionales:** Estas aplicaciones suelen ser interactivos con los usuarios y requieren tiempos de respuesta rápidos. Por ejemplo, un empleado de soporte técnico puede utilizar una aplicación de base de datos para recuperar información de la persona sobre la base de identificación.
- ✓ **Aplicaciones de Mejor - esfuerzo:** Estas aplicaciones son no críticas son no categorizada. Por ejemplo, la navegación web, correo electrónico y las transferencias de archivos FTP que entran en esta categoría.
- ✓ **Aplicaciones Scavenger:** Estas aplicaciones no productivas generalmente no tienen necesidad en la empresa, pero consumen una cantidad excesiva de ancho de banda. Por ejemplo, aplicaciones peer-to-peer para compartir archivos como Kazaa, BitTorrent, LimeWire y entrarían en esta categoría.

Puede asignar a cada una de estas categorías de datos de aplicación un determinado nivel de calidad de servicio. Se puede asignar las aplicaciones reales de estas categorías con una variedad de métodos (como la interfaz de entrada, interfaz de salida, las listas de acceso, y así sucesivamente).<sup>14</sup>

## SERVICIO DE VIDEO IP

El servicio de vídeo IP en red, que son flexibles y sólidos, le permiten supervisar y proteger personas, bienes y procesos industriales de forma remota y rentable. Pueden utilizarse para realizar sesiones de formación o resolución de errores remotas, o para retransmitir imágenes y sonidos en un sitio Web. Puede tener un sistema de vídeo en red sencillo o altamente sofisticado, según sus necesidades. El tráfico de video tiene requerimientos de delay idénticos como la voz, pero consume un poco más ancho de banda. Además, el ancho de banda puede variar dependiendo de la cantidad de movimiento en el vídeo (un montón de movimiento aumenta el ancho de banda requerida para video considerablemente).

---

<sup>14</sup> CCNA VOICE, Cisco Systems

### ***Ventajas de los Video IP***

Las redes IP son flexibles, sólidas y ventajosas, y son fundamentales para proporcionarle una amplia gama de posibilidades en cuanto a diseño de sistemas, aplicaciones y soluciones. Sólo se tiene que conectar una cámara de red (o un servidor de vídeo conectado a una cámara analógica) directamente a una red informática con cable o de forma inalámbrica para tener acceso a secuencias de vídeo en directo desde el escritorio del ordenador mediante un navegador Web estándar conectado a una red de área local o desde cualquier ubicación del mundo a través de Internet.

Pero las redes IP, en combinación con las soluciones de vídeo en red, pueden ofrecer mucho más. Algunas de las ventajas se explican brevemente a continuación:

***Calidad de imagen:*** La calidad de imagen es uno de los aspectos fundamentales de los productos de vídeo en red ofreciendo una serie de estándares de compresión de vídeo (Motion JPEG, MPEG-4, MPEG-2) entre los que pueden elegir los usuarios. En muchos productos de vídeo en red, se admiten Motion JPEG y MPEG-4 simultáneamente. Esto le permite, por ejemplo, ver imágenes con una velocidad de fotogramas completa con MPEG-4 y grabar al mismo tiempo con Motion JPEG, lo cual permite optimizar la calidad de las imágenes y el uso de ancho de banda.

***Amplia gama de productos de vídeo en red:*** Encontrará cámaras de red fijas para uso en interiores y exteriores, y cámaras de red domo y PTZ (movimiento horizontal/vertical/zoom) que permiten realizar el control remoto de las funciones PTZ a través de redes IP. También se ofrecen servidores de vídeo que ayudan a los sistemas CCTV analógicos a aprovechar las ventajas de un entorno digital conectado en red. También hay disponible software de gestión de vídeo y accesorios, como carcasas de cámaras de red y dispositivos que actúan como puente entre sistemas analógicos y digitales.



**Audio:** Además de poder ver las imágenes de forma remota desde cualquier ordenador conectado a la red, en cualquier lugar y momento, Tenemos productos que permiten establecer comunicaciones bidireccionales de audio a través de redes. Esto le permite no sólo oír lo que pasa a distancia, sino también hablar a través de la red. Con las comunicaciones en vídeo y audio, puede preguntar a los intrusos, realizar sesiones de formación remotas, solucionar problemas o retransmitir imágenes y sonidos de una ubicación o evento en sitios Web.<sup>15</sup>

**Funcionalidad de eventos:** Los productos de vídeo en red permiten a los usuarios definir y gestionar eventos de alarma. Una vez definida una alarma, tanto de forma programada mediante entradas/salidas, detección de movimiento por vídeo o detección de audio, puede solicitar automáticamente la realización de ciertas acciones; por ejemplo, iniciar el envío y la grabación de imágenes en destinos especificados, enviar alertas a personas concretas a través de correo electrónico o mediante SMS a un teléfono móvil, activar luces, activar o desactivar una alarma, abrir o cerrar puertas, controlar los niveles de temperatura, etc.

**Mecanismos de activación:** Se puede incorporar una amplia gama de mecanismos de activación (tanto integrados en el producto como disponibles en un paquete de software) en un sistema de vídeo en red.

**Programación:** Puede programar el momento en el que desea que el producto de vídeo en red realice ciertas acciones; por ejemplo, iniciar el envío y la grabación de imágenes cada noche, en fin de semana o durante las vacaciones.

**Entradas/Salidas (E/S):** Muchos de los servidores de vídeo y cámaras de red tienen puertos de entrada/salida que pueden conectarse a timbres, detectores (por ejemplo, de humo, movimiento, sonido o sensores de temperatura), luces, interruptores y relés de alarma. Al activarse los mecanismos de entrada, puede solicitar automáticamente que se realicen ciertas acciones.

---

<sup>15</sup> <http://www.videoenred.com/portal/node/>

**Detección de movimiento por vídeo:** Básicamente, esta característica le permite definir áreas de una pantalla en las que desea detectar cambios visuales. Al detectarse un cambio, puede solicitar que se realicen una serie de acciones automáticamente.

**Detección de audio:** Esta característica le permite definir el nivel de ruido que activaría la realización de ciertas acciones.

**Grabación:** Puede configurar el sistema de vídeo en red para que guarde los datos de vídeo en un servidor de archivos en una ubicación local o remota por motivos de seguridad y a intervalos de tiempo determinados, o bien al detectarse movimiento, para su visualización y análisis posteriores. Las imágenes se pueden cargar a través de correo electrónico, FTP o HTTP.

**Alimentación a través de Ethernet (PoE):** Con una solución de vídeo en red, tiene la opción de utilizar el mismo cable Ethernet para comunicaciones de datos y alimentación eléctrica. Esta característica facilita la instalación de los productos ya que no se necesita un electricista y el producto de vídeo IP puede funcionar aunque se produzca un corte de energía.<sup>16</sup>

## 2.3 REDES CONVERGENTES

Las redes convergentes o redes de Nueva Generación hacen referencia a la integración de los servicios de voz, datos y video sobre una sola red basada en IP como protocolo de red, deben contar con la infraestructura de conmutación y transporte de paquetes nativos de datos y debe contar con un servicio flexible de control de elementos para habilitar las comunicaciones, soportar datos y QoS. Además, debe existir paridad en voz con la Red Telefónica Conmutada Pública en términos de facilidades, calidad, escalabilidad y penetración de servicios.<sup>17</sup>

---

<sup>16</sup> <http://www.videoenred.com/portal/node/1>

<sup>17</sup> <http://dialnet.unirioja.es/servlet/articulo?codigo=2332462>

A nivel mundial están siendo implementadas estas redes y cada día son más las empresas que por la necesidad de optimizar sus gastos operativos están optando por tener redes convergentes que les permita disfrutar de todos los beneficios y bondades que esta ofrece; hay que tener presente que la tecnología está avanzando a paso agigantados y un ejemplo claro son las redes telecomunicaciones, las cuales han avanzado tanto que es posible conectarse al mundo digital desde diversos aparatos electrónicos en casi cualquier parte del mundo, nos estamos refiriendo a las redes de nueva generación, estas redes son la integración de todos los servicios disponibles al momento de establecer la comunicación por voz, video, datos y otros servicios basados en el protocolo IP.

Los usuarios hoy día tienen muchas necesidades de comunicaciones por lo que demandan que esta comunicación se establezca de una manera rápida y eficiente; si se requiere reducir costos en el momento de realizar este proceso, una alternativa real seria unir estos medios de comunicación en un solo medio de transporte, esto se puede lograr utilizando Redes Convergentes, ya que estas integran bajo una misma plataforma voz, datos, vídeo y otra gran variedad de servicios; para ofrecer una gama de servicios como telefonía tradicional, servicios corporativos, Internet de alta velocidad y videoconferencias.

### **3. MÉTODOS PARA IMPLEMENTACIÓN DE CALIDAD DE SERVICIOS (QOS) BASADOS EN SERVICIOS INTEGRADOS, SERVICIOS DIFERENCIADOS Y AUTOQOS**

En la actualidad el principal problema de Internet es la congestión y la falta de calidad de servicios (QoS), existen métodos para implementar calidad de servicios (QoS), TCP/IP fue diseñado para dar un servicio 'best effort' (Máximo esfuerzo) consiste en enviar "lo más posible, lo antes posible". Los paquetes con este tipo de servicio tienen la misma expectativa de tratamiento a medida que transitan por la red. Se caracteriza porque la complejidad se encuentra en los "host" de las puntas, siendo los routers el núcleo de la red. Sólo miran la cabecera, buscan en la tabla de ruteo y definen el próximo host. Si llegase a ocurrir congestión, se retardan o descartan los paquetes, esto hace muy escalable la red. Es suficiente para aplicaciones como mail, ftp, pero no para otras aplicaciones que no toleran retardos variables o pérdida de datos, como es el caso de servicios de voz ip y video ip en tiempo real. Hay una Convergencia de servicios no tradicionales: telefonía, radio, televisión, videoconferencia, etc. Los cuales tienen otras exigencias una solución podría ser agregar más ancho de banda, pero esto no es suficiente, ya que el tráfico es típicamente en ráfagas, produciendo congestiones temporales y retardos y pérdidas esto hace que las redes con cualquier servicio requiera lo máximo en Ancho de banda que pueda tomar de un canal, al verse simultáneamente con otros servicios que también requieren el máximo de ancho de banda es cuando hacen que las redes sean de mayores tiempos de respuestas y algunas terminen ocasionando un problema de DoS.

Por lo tanto la solución está en dotar a Internet de una mayor "inteligencia", por medio de mecanismos para obtener QoS. Se han desarrollado y estandarizado mecanismos de QoS, reserva y prioridad Servicios integrados (**IntServ**) y

Servicios diferenciados (**DiffServ**), Calidad de Servicio Automática (**AutoQoS**) Cisco IOS Software puede soportar estas arquitecturas.

### **3.1 SERVICIOS INTEGRADOS (INTSERV)**

Fue la primera arquitectura de Calidad de Servicios (QoS) desarrolladas por la IETF (Grupo de Trabajo de Ingeniería de Internet) a principios de los 90s. En el diseño se consideró que las aplicaciones de tiempo real serían las más importantes y sensibles de las aplicaciones necesitando QoS. Esta arquitectura está basada en el protocolo de reservación de recursos por flujo (RSVP). Para que se le aseguren recursos, una aplicación debe hacer una reservación antes de transmitir. Primero se caracteriza la fuente del flujo y sus requerimientos; la red luego utiliza un algoritmo de ruteo para elegir la ruta que cumpla con dichos requerimientos; y por último un protocolo de reservación establece el estado de reserva a lo largo de la ruta (cada nodo debe chequear si hay recursos disponibles antes de aceptar la reserva).

IntServ proporciona un mecanismo más estricto para la QoS del tráfico en tiempo real, tiene Poca escalabilidad, en todos los nodos se deben implementar IntServ, Ineficiencia debido al SoftState Ineficiencia debido aumento de tráfico. Borra un camino para el flujo antes de enviarlo, se puede garantizar QOS en determinadas circunstancias. Es preferido por su simplicidad, este en un punto clave, la capacidad de hacer llamadas de control de admisión (CAC) es importante en determinadas aplicaciones de tiempo real. Esto se debe a que los diseñadores pueden utilizar CAC para determinar si los recursos están disponibles para un servicio de apoyo y en efecto, enviar un "ocupado" la señal al usuario si no – para alertar al usuario y preservación de la calidad de todas las otras llamadas en curso, las necesidades de aplicaciones de tiempo real tales como vídeo remoto, conferencias multimedia, visualización y realidad virtual. Proporciona una forma de entregar extremo a extremo Calidad de Servicio (QoS) que en tiempo real de

aplicaciones requieren explícitamente la gestión de los recursos de la red para proporcionar QoS a los usuarios de paquetes.<sup>18</sup>

Servicios que deben habilitarse en IntServ

- ✓ **Control de Admisión**; responde a los requerimientos de la aplicación para los recursos de extremo a extremo.
- ✓ **Clasificación**: el tráfico perteneciente a una aplicación que ha reservado recursos deben ser clasificados y reconocidos por los router de transito, por lo tanto, se pueden entregar servicios apropiados a estos paquetes.
  
- ✓ Políticas
- ✓ Encolamiento
- ✓ Scheduling (elegir el próximo paquete para ser enviado por el enlace)

Cualquier aplicación que falle al iniciar es porque los requerimientos de RSVP para estos recursos fueron rechazados, RSVP hace un requerimiento para cada flujo estos incluyen identificador del que lo requiere y las políticas de tráfico que se necesitan. Esto permitirá a todos los router intermedios entre fuente y destino identificar cada flujo, RSVP provee parámetros de flujo como IP y un número de puerto.

### **Beneficios de IntServ**

- ✓ Recursos de control de admisión explícito de extremo a extremo.
- ✓ Políticas de control de admisión por requerimiento.
- ✓ Señalización de número de puertos dinámicos.

---

<sup>18</sup> [http://www2.ing.puc.cl/~iee3542/amplif\\_4.ppt](http://www2.ing.puc.cl/~iee3542/amplif_4.ppt)

## Desventajas

- ✓ El desperdicio de ancho de banda (overhead), en cada flujo tiene una señalización continua por lo que el overhead puede llegar a ser sustancialmente grande como el número de flujos que crece.
- ✓ No escalable, debido a que cada flujo es un camino y es mantenido.

## 2.2 SERVICIOS DIFERENCIADOS (DIFFSERV)

Esta arquitectura surgió como una alternativa a Intserv más simple y escalable, que da un mejor servicio que best-effort. En vez de una reserva explícita por flujo, está basado en PHB<sup>19</sup>, que significa que cada salto en una red debe ser programado para proveer un específico nivel de servicio para cada clase de tráfico y prioriza el tráfico para brindar diferenciación de tráfico. Este modelo es más escalable porque la señalización y el estado de monitoreo para cada flujo no es necesario. En esta arquitectura se pueden marcar directamente los paquetes de la "clase", están clasificados para recibir un tratamiento particular, en la transmisión (el comportamiento PHB) en los nodos a lo largo de su camino, y control de admisión como mecanismos fundamentales para establecer y mantener QoS, dicho protocolo de señalización requiere que los routers, los flujos de paquetes QoS tengan un tratamiento especial.

DiffServ QoS logra una mejor escalabilidad, divide el tráfico en un pequeño número de clases, y asigna recursos para cada clase de base, porque sólo tiene unas pocas clases de tráfico, el marcado, la policía, y la configuración de las operaciones sólo deberá aplicarse en los límites de red o hosts.<sup>20</sup>

IntServ fue desarrollado con anterioridad a DiffServ, Sin embargo DiffServ se ha extendido más que IntServ, Los fabricantes de routers no han desarrollado

---

<sup>19</sup> PHB: es el medio por el cual un nodo aloja recursos a los agregados de comportamiento.

<sup>20</sup> [http://www.cisco.com/en/US/products/ps6558/products\\_ios\\_technology\\_home.html](http://www.cisco.com/en/US/products/ps6558/products_ios_technology_home.html)

implementaciones eficientes de RSVP, debido al elevado costo pero si implementan versiones eficientes de DiffServ, Actualmente muchos ISP implementan DiffServ.

Las garantías de calidad de servicio que ofrecen los servicios diferenciados no son tan severas como en IntServ, La información de QoS no está en los routers sino que cabalga 'montada' en los datagramas, no puede garantizar QoS Extremo a Extremo de la red. Los routers tratan cada paquete según su categoría (que viene marcada en la cabecera del paquete). El Policy Control/Admission Control sólo se ha de efectuar en los routers de entrada a la red del proveedor y en los que atraviesan fronteras entre proveedores diferentes.

DiffServ la priorización de flujos mediante Clase de Servicio (CoS) No hay reservas, sino prioridades, No hay flujos, No hay estados, No es de extremos extremo, resuelve problemas de escalabilidad.<sup>21</sup>

El modelo Mixto entre (Servicios Integrados/Servicios Diferenciados) consiste en tomar lo mejor de cada servicio ya que son compatible y pueden coexistir este método hace que las aplicaciones tengan mejores desempeños y sean más optimas las comunicaciones como tal.

---

<sup>21</sup><http://www.ipv6.codarec.frm.utn.edu.ar/areas/QoS/Publicaciones/Resena%20de%20Calidad%20de%20Servicio%20en%20ambientes%20IPv6%20Filminas.pdf>



### 3.3 AUTOQoS

Es una implementación de los servicios Diferenciados (DiffServ), autoQoS permite automáticamente generar comandos de configuración de calidad de servicios, automatiza elementos críticos del despliegue de QoS como clasificar aplicaciones, generar políticas, configuraciones, monitoreo y reportes. También incrementa la disponibilidad de la red al reducir errores de operadores y de configuración.<sup>22</sup>

Se encuentra disponible en los routers Cisco IOS desde la serie 2600 hasta la serie 7200 y también en la mayoría de los routers Cisco que utilizan versiones de IOS 12.2 (15)T y posteriores. AutoQoS ofrece los siguientes beneficios:

- ✓ No requiere una comprensión avanzada de QoS del mismo modo que si se desea configurar desde la línea de comandos.
- ✓ Se pueden modificar las políticas de QoS y reutilizarlas, del mismo modo que si se tratara de un template.
- ✓ Se ahorra mucho tiempo de configuración.

Antes de ejecutar los comandos AutoQoS, se debe habilitar CEF<sup>23</sup> utilizando utilizando el siguiente comando

```
Router (config) #ip cef // Habilita CEF
```

Adicionalmente se requiere la configuración de la declaración de ancho de banda en las interfaces ya que AutoQoS utiliza esta información cuando se configuran limitaciones de ancho de banda por protocolo para ser priorizados.

```
Router(config)#interface serial0/3/0//Se entra a la interface serial
```

```
Router(config-if)#bandwidth 2000000 //Declaración del ancho de banda
```

---

<sup>22</sup> <http://www.scribd.com/doc/23309813/Proyecto-QoS-Sobre-VoIP>

<sup>23</sup> CEF: permite un modo de conmutación más rápido en los dispositivos Cisco.

Si se modifica la configuración de este parámetro una vez que se activó AutoQoS, será necesario reiniciar AutoQoS. También se debe tener presente no configurar AutoQoS en modo configuración global, sino en las interfaces.

Su configuración es muy simple y fácil, se necesita comprender qué es lo que se está configurando, modificar la configuración si es necesario, y probar lo que se realizó para ver si funciona como se esperaba.

Para configurar AutoQoS, la secuencia de comandos en la interfaz que hace de origen del tráfico que se desea controlar es:

```
Router(config)#interface serial0/3/0 //Se entra a la interface serial 0/3/0
```

```
Router(config-if)#auto qos voip //permite habilitar AutoQoS.
```

Con ese solo comando, Cisco IOS automáticamente genera una serie de comandos de configuración que se pueden verificar utilizando show running-config (muestra la configuración actual).

### **3.4 IMPLEMENTACIÓN DE UNA RED CONVERGENTE CON CALIDAD DE SERVICIOS (QoS)**

Una red convergente no es únicamente una red capaz de transmitir datos, voz y video sino un entorno en el que además existen servicios avanzados que integran estas capacidades, reforzando la utilidad de los mismos. A través de la convergencia, una compañía puede reinventar tanto sus redes de comunicaciones como toda su organización. Implementar redes convergentes de última generación con calidad de servicios (QoS), la cual es vital para el perfecto funcionamiento de la red, pues hoy día no es solo hacer que las redes estén funcionando todo el tiempo sino que hay que hacer y buscar que durante este tiempo de funcionamiento lo realicen con calidad en los servicios y mejoren los tiempos de respuestas de los servicios y aplicaciones que sobre estas redes se

están transportando, sobre todo si vemos que estos servicios de comunicaciones MAN y WAN tienen altos valores y hay que tratar de ser productivos con estos servicios.

Para la implementación de Calidad de servicios QoS, Cisco IOS brinda 4 posibilidades diferentes:

✓ *Configuración por CLI (Interfaz de líneas de comandos)*

Permite configurar manualmente interfaz por interfaz las opciones de QoS.

Es un método poco escalable.

✓ *Configuración por MQC (Modular de QoS interfaz de línea de comandos)*

Permite una configuración modular de QoS a partir de la definición de clases y Políticas (Diffserv). Es la opción para la configuración detallada de QoS en dispositivos Cisco IOS en la actualidad<sup>24</sup>.

✓ *AutoQoS VoIP (Calidad de Servicios automática voz ip)*

Permite de modo simple y rápido configurar requerimientos de QoS en redes que implementan VoIP.

✓ *AutoQoS Enterprise*

Permite la implementación que en base a la operación de NBAR <sup>25</sup> detecta hasta 10 tipos diferentes de tráfico que atraviesan enlaces WAN, disponible a partir de Cisco IOS 12.3 (7) T.

Un ejemplo de la implementación de Métodos de Calidad de servicios en este caso se utilizó AutoQoS por su facilidad.

---

<sup>24</sup> <http://www.scribd.com/doc/23309813/Proyecto-QoS-Sobre-VoIP>

<sup>25</sup> NBAR: Identificación de las aplicaciones de Red.

Es necesario realizar vlan(red LAN virtual)de voz, datos para que los teléfonos se puedan conectar y comunicarse con el Router y así poder descargar los ficheros de configuración.

En el Switch se crea las vlan

Switch# vlan database para entrar en el submenú de configuración

Switch (vlan)#vlan12 name Red datos se asigna un número y un nombre a la vlan

Switch(vlan)#vlan11 name Red teléfonos se asigna número y nombre a la vlan

Luego se introduce los puertos del switch a las vlan recién creadas:

```
interface FastEthernet0/24 // interface fastethernet 0 puerto 24
```

```
switchport trunk encapsulation dot1q
```

```
switchport mode trunk // modo de acceso virtual
```

Los interfaces que se conectan a los teléfonos directamente

```
interface FastEthernet0/23 //interface fastethernet 0 puerto 23
```

```
switchport mode access // modo de acceso
```

```
switchport voice vlan 11 // puerto para voz
```

Configuración en el Router

*Configuración de las vlan en el Router*

```
interface FastEthernet0/0.11//Creación de la subinterface para teléfonos.
```

```
encapsulation dot1Q 11// para que las vlan tengan comunicación entre ellas.
```

```
ip address 192.168.130.1 255.255.255.0// dirección ip y mascara de red
```

```
interface FastEthernet0/0.12 // Creación de la subinterface para teléfonos
```

```
encapsulation dot1Q 12 // para que las vlan tengan comunicación entre ellas.
```

```
ip address 192.168.131.1 255.255.255.0// Dirección ip y mascara de red
```

## Configuración de método de calidad de Servicio AutoQoS

```
Router#configure terminal //Modo configuración
Router(config)#ip cef //habilita CEF
Router(config)#interface serial 0/1 // Se ingresa a la interface serial 0/1
Router(config-if)#bandwidth 10000000 // Asignación de ancho de banda
Router(config-if)#ip address 10.0.1.1 255.255.255.252// asignación de ip y mascara de red
Router(config-if)#Auto qos voip trust Habilita AutoQos
```

Cuando se ingresa autoqos el Router construye class-map(Define la clase de tráfico), entonces crea y aplica un policy-map<sup>26</sup> a la interface

Para que los teléfonos reciban una IP dinámicamente es necesario que el router sea un servidor DHCP, por tal motivo se configura lo siguiente.

Se asigna el rango de direcciones IP que se pueden asignar a los teléfonos. La opción 150 permite que los teléfonos descarguen del router su imagen vía tftp

```
ip dhcp pool phone
network 192.168.130.0 255.255.255.0// Rango de direcciones para asignar a los teléfonos
default-router 192.168.130.1//Dirección del Router por defecto
option 150 ip 192.168.130.1// permite que los teléfonos descarguen del router su imagen vía tftp
```

Se asigna el rango de direcciones IP que se pueden asignar a otros dispositivos conectados en la red de datos.

```
ip dhcp pool datos
network 192.168.131.12 255.255.255.0 // rango de direcciones ip para asignar a los dispositivos.
default-router 192.168.131.1//Dirección del Router por defecto
```

---

<sup>26</sup> Policy-map: define políticas para asociar los requerimientos de QoS para las clases de tráfico defino en class-map

## Configuración de 2 teléfonos en el Router

En primer lugar se especifica la dirección IP de la subred de datos para que los teléfonos puedan descargarse su configuración por tftp. También se fija el número de teléfonos posibles (24) y el máximo número de dn (números de directorio)

```
Router (config) telephony-service // Habilita el servicio de telefonía
```

```
Router (config-telephony) max-ephones 24// máximo número de teléfonos
```

```
Router (config-telephony) max-dn 120// máximo número de Directorios
```

```
Router (config-telephony) ip source-address 192.168.131.1 port 2000 // dirección  
donde el teléfono obtiene los archivos de configuración
```

```
Router (config)ephone-dn 1// configuración del teléfono 1
```

```
Router (config-ephone)number 1234// número del teléfono
```

```
Router (config-ephone)name lola // nombre de quien pertenece el número de teléfono
```

```
Router (config)ephone-dn 2// configuración del teléfono 1
```

```
Router (config-ephone)number 6543// número del teléfono
```

```
Router (config-ephone)name María // nombre de quien pertenece el número de teléfono
```

Ahora se debe asignar los números de directorio definidos anteriormente a los teléfonos. En el router asigna el número de ephone en el orden en que se conectan los teléfonos, la dirección MAC es única y propia de cada teléfono, hay que asegurarse de que la MAC corresponde a cada ephone a la hora de configurarlo.

```
ephone 1 // número ephone correspondiente a esta dirección Mac: 1, 2 ó 3
```

```
mac-address 0011.93CE.F038 // Dirección MAC del Teléfono
```

```
button 1:11 // Este teléfono solo permite 1 número
```

ephone 2 // número ephone correspondiente a esta dirección Mac: 1, 2 ó 3  
mac-address 0011.5CD8.A724//Dirección MAC del Teléfono  
button 1:12 // Este teléfono solo permite 1 número

#### 4. ESCENARIO DE PRÁCTICAS DE LABORATORIO

A lo largo desarrollo de este proyecto comparativo de investigación se realizaron 8 prácticas, para llevarlas a cabo se debió hacer un alistamiento previo de una de las herramientas claves que se utilizaron los Routers, Switchs.

Se realizaron Prácticas de envío de Servicios sin implementar métodos de QoS y con la implementación de estos, para estas últimas la versión de la IOS que tenían los Routers Cisco 2800 no era la adecuada para la configuración, por tanto se hizo necesaria la actualización de la versión apropiada para nuestros requerimientos, a continuación se describen los pasos que se siguen para tener éxito en dicha actualización:

1. Se entró al Router por medio de una sesión Hiperterminal, luego a el modo privilegiado, se escribió el comando show versión para ver la versión de la IOS y show flash para ver la cantidad de memoria de la Flash:

***Router> enable***

***Router# Show version***

```
Cisco IOS Software, 2800 Software (C2800NM-ADVSECURITYK9-M),  
Version 12.4(3i), Rle hardwareils connection /  
ELEASE SOFTWARE (fc2) mult  
Technical Support: http://www.cisco.com/techsupport Show context information  
about modemcap  
Copyright (c) 1986-2007 by Cisco Systems, Inc.
```

El resultado que arrojó el anterior comando fue que el Router tenía la versión C2800NM-ADVSECURITYK9-M, la cual para nuestra prácticas no era la indicada, esta versión no acepta comandos de calidad de servicios, se hacía necesario tener otra versión más apropiada para la implementación de nuestro proyecto.

Luego se Verificó la cantidad de memoria que contenía la flash, el resultado fue el siguiente:



**Router# show flash:**

```
-#- --length-- -----date/time----- path
1 20267528 Feb 01 2008 20:00:38 +00:00 c2800nm-advsecurityk9-mz.124-3i.bin
2 1823 Feb 01 2008 20:10:14 +00:00 sdmconfig-2811.cfg
3 6036480 Feb 01 2008 20:11:04 +00:00 sdm.tar
4 861696 Feb 01 2008 20:11:24 +00:00 es.tar
5 1164288 Feb 01 2008 20:11:46 +00:00 common.tar
6 1038 Feb 01 2008 20:12:04 +00:00 home.shtml
7 113152 Feb 01 2008 20:12:18 +00:00 home.tar
8 527849 Feb 01 2008 20:12:38 +00:00 128MB.sdf
9 1697952 Feb 01 2008 20:13:04 +00:00 securedesktop-ios-3.1.1.45-k9.pkg
10 416354 Feb 01 2008 20:13:26 +00:00 sslclient-win-1.1.3.173.pkg
11 666 Oct 01 2008 14:42:42 +00:00 g
```

32903168 bytes available (31113216 bytes used)

2. Debido a los resultados que arrojó este comando no había capacidad para contener dos IOS por tal motivo se borró la IOS, en el caso de poseer un Router con mayor capacidad en la memoria flash no sería necesario borrar la IOS, se entra a modo configuración, para borrar la IOS se utilizó el comando delete flash: nombre de la IOS que se va a borrar, con la extensión .bin :

**Router# Configure terminal**

**Router (config) # delete flash: c2800nm-advsecurityk9-mz.124-3i.bin**

3. Se instaló un servidor TFTP de Cisco y se copió la nueva IOS en:

**C://archivosdeprograma/ciscosystems/ciscotftpserver.**

4. Se le asignó una dirección IP al computador y al router con sus respectivas mascararas de subred, se verifica con el comando ping la conectividad entre el PC y el router.

**Router (config) #interface fastethernet 0/0**

**Router (config-if) # ip address 10.0.1.1 255.255.255.0**

**Router (config-if) #end**

**Router# ping 10.0.1.2**

5. Se verificó que hiciera ping con la dirección ip del computador
6. Luego se copió la nueva IOS con el siguiente comando: Copy ftp flash:  
Nombre de la nueva IOS.bin

***Router # copy tftp flash: c2800nm-adventerprisek9-mz.124-19.bin***

7. Se escribió la dirección IP del computador.
8. Se confirmó el nombre del archivo con extensión .bin
9. Se activó el servidor TFTP.
10. Luego de haber terminado de copiar la IOS se reinició el router para que los cambios pudieran tener efectos y volviera a cargar la nueva versión de la IOS se utilizó el comando reload.

***Router# reload***

11. Por último se confirmó que la actual IOS sea la versión que se le estaba instalando se utilizó el comando show versión.

Al momento de actualizar la IOS en dos routers 2800 cisco se presentaron algunos inconvenientes ya que no había IOS en dos de los routers y fue necesario realizar esta actualización por modo ROMmON ya que por el modo privilegiado no se pudo realizar, a continuación los parámetros que se utilizaron para la realización de la actualización por modo RoMnOn:

1. **IP\_ADDRESS**: dirección de IP del router
2. **IP\_SUBNET\_MASK**: máscara de subred del router
3. **DEFAULT\_GATEWAY**: Gateway por defecto del router
4. **TFTP\_SERVER**: dirección IP donde esta el servidor TFTP.
5. **TFTP\_FILE** : nombre de la imagen del IOS en el servidor
6. **SET**: Para verificar los las variables del entorno RoMmon
7. **TFTPDNLD**: para descargar la IOS no se coloca ningún argumento.
8. Se debe resetear para que surjan efectos los cambios realizados se utiliza en este caso el comando **RESET**

Luego de la actualización de la IOS, todo queda listo para el montaje de la red.



**Figura 14: Topología de la red**

Se puede apreciar en la figura 14 la topología que se implementó para las dos Redes, para el montaje de la se tuvo como base el siguiente Direcccionamiento IP (ver figura 2), se utilizaron los siguientes dispositivos:

1. Cuatro (4) Routers, que correspondían a las Ciudades de Cartagena, Bogotá, Manizales y Pereira respectivamente.
2. Cuatro(4) Switchs.
3. Cuatro (4) Computadores, entre estos un portátil con cámara web integrada.
4. Dos (2) Diademas para la realización efectiva de las pruebas.
5. Tres (3) pares de cable Serial.
6. Cuatro (4) cables de consola.
7. Veinte (20) cables de red.

## Direccionamiento IP

red	# bitutiliza	ip subredes	Ip broadcast	Rango a utilizar	Mascara	Mascara decimal	
		WAN	200,20,0,0				
		LAN	172,16,0,0				
<b>A</b>	2	2	200,20,0,4	200.20.0.7	200.20.0.5 - 200.20.0.6	/30	255,255,255,252
<b>B</b>	2	2	200,20,0,8	200.20.0.11	200.20.0.9 - 200.20.0.10	/30	255,255,255,252
<b>C</b>	2	2	200,20,0,12	200.20.0.15	200.20.0.13 - 200.20.0.14	/30	255,255,255,252
<b>D</b>	2	2	200,20,0,16	200.20.0.19	200.20.0.17 - 200.20.0.18	/30	255,255,255,252
cartagena	8	254	172,16,2,0	172,16,2,255	172,16,2,1 - 172,16,2,254	/24	255,255,255,0
bogotá	8	254	172,16,3,0	172,16,3,255	172,16,3,1 - 172,16,3,254	/24	255,255,255,0
manizales	8	254	172,16,4,0	172,16,4,255	172,16,4,1 - 172,16,4,254	/24	255,255,255,0
pereira	8	254	172,16,5,0	172,16,5,255	172,16,5,1 - 172,16,5,254	/24	255,255,255,0
II1	7	126	172,16,2,0	172,16,2,127	172,16,2,1 - 172,16,2,126	/25	255,255,255,128
II2	6	62	172,16,2,128	172,16,2,191	172,16,2,129 - 172,16,2,190	/26	255,255,255,192
III3	6	62	172,16,2,192	172,16,2,255	172,16,2,193 - 172,16,2,254	/26	255,255,255,192
III1	7	126	172,16,3,0	172,16,3,127	172,16,3,1 - 172,16,3,126	/25	255,255,255,128
III2	6	62	172,16,3,128	172,16,3,191	172,16,3,129 - 172,16,3,190	/26	255,255,255,192
III3	6	62	172,16,3,192	172,16,3,255	172,16,3,193 - 172,16,3,254	/26	255,255,255,192
IV1	7	126	172,16,4,0	172,16,4,127	172,16,4,1 - 172,16,4,126	/25	255,255,255,128
IV2	6	62	172,16,4,128	172,16,4,191	172,16,4,129 - 172,16,4,190	/26	255,255,255,192
IV3	6	62	172,16,4,192	172,16,4,255	172,16,4,193 - 172,16,4,254	/26	255,255,255,192
V1	7	126	172,16,5,0	172,16,5,127	172,16,5,1 - 172,16,5,126	/25	255,255,255,128
V2	6	62	172,16,5,128	172,16,5,191	172,16,5,129 - 172,16,5,190	/26	255,255,255,192
V3	6	62	172,16,5,192	172,16,5,255	172,16,5,193 - 172,16,5,254	/26	255,255,255,192

**Figura 15: Direccionamiento IP**

En la figura 15 se muestra el direccionamiento ip que se tomó como base para la correcta comunicación entre ciudades.

### 4.1 Servicios y Parámetros para la primera práctica sin métodos de calidad de servicios (QoS)

Como se había dicho anteriormente las prácticas tienen dos panorámicas en cuanto a la implementación de los métodos de calidad de servicios utilizados, pero los servicios enviados y los parámetros que se tuvieron en cuenta para la evaluación de los resultados son los mismos.

Los servicios que se enviaron a través de las redes fueron:

## 1. Datos

Se descargaron dos archivos, primero se descargo un archivo con nombre casos\_de\_estudio.docx de tamaño de 12 Kb, inmediatamente después se inicio la descarga de otro archivo con nombre proyecto\_final\_QoS\_ultimo.docx con un tamaño de 3.83 MB, estos archivos se encontraban almacenados en un servidor TFTP "SERV\_U" que se encontraba ubicado en la ciudad de Manizales, desde el cual se accedía al servidor utilizando el Browser y en la barra de direcciones se escribía la dirección ip de la ciudad donde se encontraba el servidor en este caso Manizales.

Los parámetros que se tuvieron en cuenta para la evaluación de este servicios fueron:

1. Tiempo de Transferencia.
- 5 Velocidad de Transferencia.

## 2. Voz

Se estableció la siguiente conversación de una duración aproximada de 45 segundos, esta se originó a partir de una llamada realizada desde la ciudad de Manizales a Cartagena, Berenice se encontraba en Manizales y lilibeth en Cartagena, esta se realizó a través del Softphone Cisco IP comunicator instalado en todas las Ciudades.

### Conversación

**Berenice:** Hola, Buenos días hablas con Berenice con quien tengo el placer de hablar?

**Lilibeth:** Hola buen día hablas con lilibeth, en que te puedo ayudar Berenice?

**Berenice:** Necesito que me envíes unos documentos importantes que debo enviar a Estados Unidos a mas tardar mañana a primera hora, eso define unos negocios pendientes, por favor colabórame cuanto antes.

**Lilibeth:** ok veré que puedo hacer, ya que se presentaron unos inconvenientes en la oficina y no he podido hacértelos llegar, no te preocupes, nos vemos bye.

**Berenice:** Bye espero tu rápida colaboración y gracias de ante mano.

Los parámetros utilizados para la evaluación fueron:

1. Paquetes Perdidos.
2. Jitter.

### **3. Video**

Se envió un video de Bob Esponja.mpeg que demora 1:37 min/seg y tiene un tamaño de 23.6 MB esto se realizó desde la ciudad de Manizales mediante un programa de transferencia de video "Windows Media Encorer".

Los parámetros utilizados para la evaluación fueron:

1. Paquetes Perdidos.
2. Velocidad de Transferencia.

Luego de tener la red configurada sin métodos de Calidad de Servicios (QoS) y definidos los parámetros, se llevaron a cabo las prácticas de envíos de Datos, Voz y video en forma individual, luego de forma conjunta, Terminada la configuración se procedió a realizar las pruebas y se tomaron los resultados.

Para todas las pruebas Manizales fue la ciudad de origen de los servicios, allí fue donde se instaló el servidor, Windows Media Encorer y se realizó la llamada telefónica, Cartagena fue el destino, se hizo así para garantizar las mismas condiciones para las dos implementaciones de redes.

Para la toma de resultados se hizo necesaria la utilización de una herramienta de monitoreo de Redes llamada "Wireshark", ya que esta nos proporciona los parámetros que se necesitan para la evaluación adecuada de las prácticas.

## 4.2 Servicios y Parámetros de prácticas

Se tuvo en cuenta los mismos parámetros que se utilizó en la anterior práctica

Los servicios que se enviaron a través de la redes fueron:

### ✓ Datos

Se descargaron dos archivos, primero se descargo un archivo con nombre casos\_de\_estudio.docx de tamaño de 12 Kb, inmediatamente después se inicio la descarga de otro archivo con nombre proyecto\_final\_QoS\_ultimo.docx con un tamaño de 3.83 MB, estos archivos se encontraban almacenados en un servidor TFTP "SERV\_U" que se encontraba ubicado en el computador de Manizales, desde el cual se acedía al servidor utilizando el Browser y se escribía la dirección ip de la ciudad donde se encontraba el servidor en este caso Manizales.

Los parámetros que se tuvieron en cuenta para la evaluación de estos servicios son:

1. Tiempo de Transferencia.
2. Velocidad de Transferencia.

### ✓ Voz

Se estableció la siguiente conversación de una duración aproximada de 45 segundos, esta se originó a partir de una llamada realizada desde el router de Manizales a Cartagena, Berenice se encontraba en el router Manizales y lilibeth en el de Cartagena, esta se realizó a traves del Softphone Cisco IP communicator instalado en todos los computadores que hacían parte de las respectivas ciudades.

### Conversación

**Berenice:** Hola, Buenos días hablas con Berenice con quien tengo el placer de hablar?

**Lilibeth:** Hola buen día hablas con lilibeth, en que te puedo ayudar Berenice?

**Berenice:** Necesito que me envíes unos documentos importantes que debo enviar a Estados Unidos a mas tardar mañana a primera hora, eso define unos negocios pendientes, por favor colabórame cuanto antes.

**Lilibeth:** ok veré que puedo hacer, ya que se presentaron unos inconvenientes en la oficina y no he podido hacértelos llegar, no te preocupes, nos vemos bye.

**Berenice:** Bye espero tu rápida colaboración y gracias de ante mano.

Los parámetros utilizados para la evaluación fueron:

1. Paquetes Perdidos.
2. Jitter.

### **3. Video**

Se envió un video de Bob Esponja.mpeg que demora 1:37 min/seg y tiene un tamaño de 23.6 MB esto se realizó desde el computador de Manizales mediante un programa de transferencia de video "Windows Media Encorer".

Los parámetros utilizados para la evaluación fueron:

1. Paquetes Perdidos.
2. Velocidad de Transferencia.

Luego de tener la red configurada con métodos de Calidad de Servicios (QoS) "AutoQos", se llevó a cabo las prácticas de envíos de servicios de Datos, Voz IP y video IP en forma individual, luego de forma conjunta, y se tomaron las pruebas necesarias.

Para todas las prácticas al igual que la anterior Manizales fue el origen de los servicios, allí fue donde se instaló el servidor TFTP, Windows Media Encorer, se configuró el servicio de telefonía y se realizó la llamada telefónica, Cartagena fue el destino, se hizo así para garantizar las mismas condiciones para las dos redes implementadas.



Para la toma de resultados se hizo necesaria la utilización de una herramienta de monitoreo de Redes se escogió un software llamado “Wireshark”, ya que esta nos proporciona los parámetros que se necesitan para la evaluación adecuada de las prácticas.

### 4.3 Evidencias de las Prácticas

Durante el desarrollo de las prácticas se tomaron varias evidencias

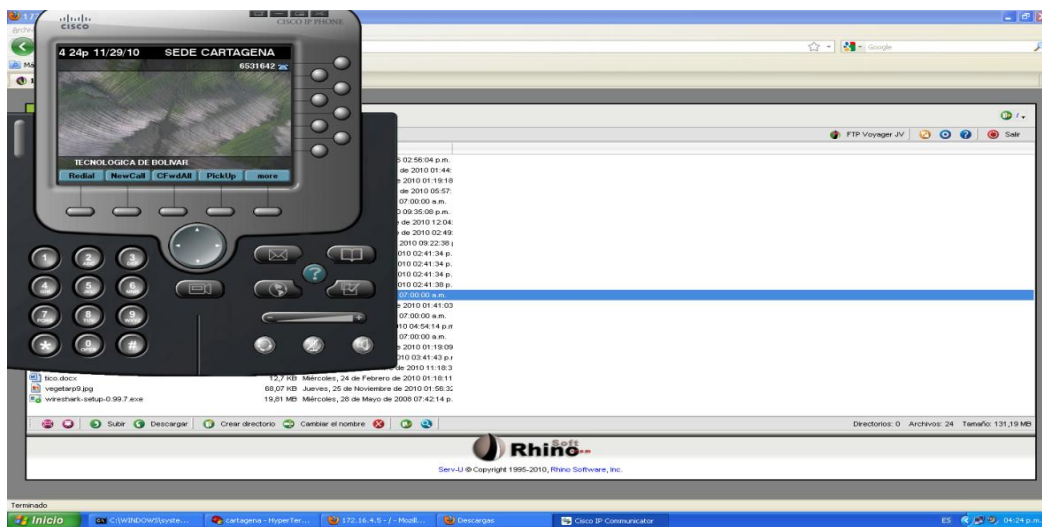


Figura 16. llamada saliente de Manizales

Se puede observar en la figura 16 la realización de una llamada saliente desde el router de Manizales a Cartagena.



Figura 17.Llamada entrante a Cartagena

En la figura 17 se muestra una llamada entrante del router de Manizales a Cartagena

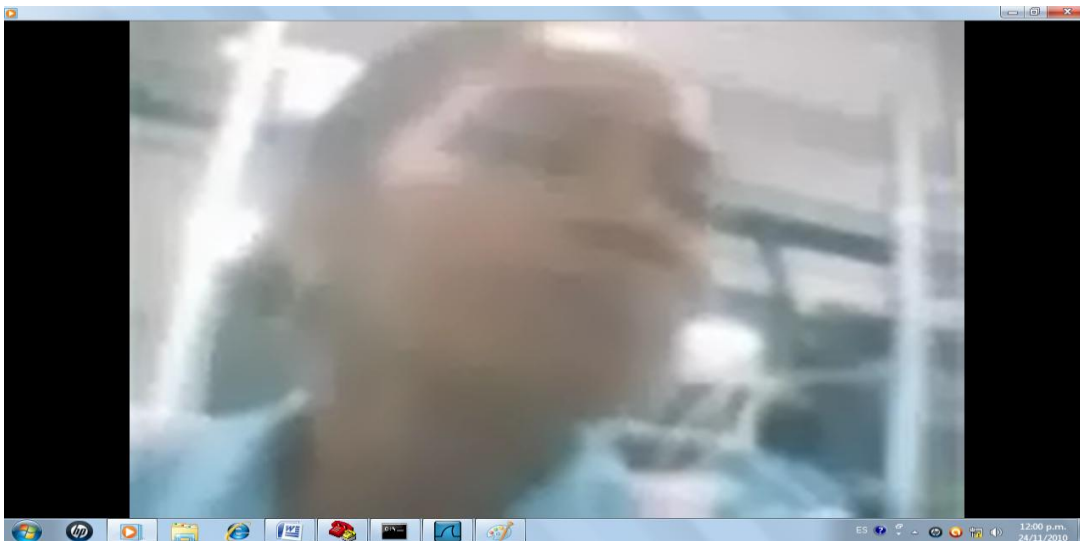


Figura 18.Imagen sin implementación de métodos de QoS

En la figura 18 se muestra un video cuando la red no tiene implementado métodos de calidad de servicios (QoS) la imagen se muestra borrosa y no se puede observar bien los movimientos.

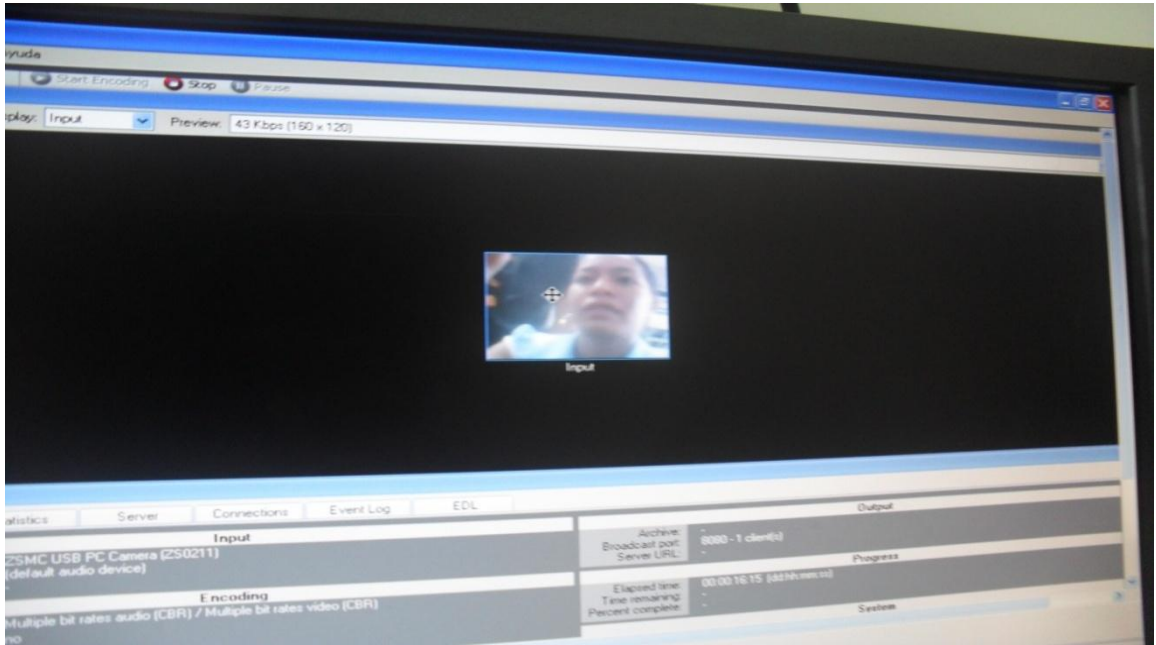


Figura 19. Imagen con implementación Métodos de QoS

En la figura 19 se presenta la transmisión de un video por medio de Windows media Encoder cuando la red tenía implementado métodos de calidad de servicios.

## **5.RESULTADOS DEL PROYECTO**

Para la toma de resultados se utilizó la herramienta Wireshark, el servidor Serv-U y Windows Media Encoder Server, esta se encontraba instalada en la ciudad de Manizales, una vez que la red estaba funcionando este programa se ejecutó y empezó a capturar paquetes, se iniciaron las pruebas y el siguió guardando la información que luego se utilizó para hacer el cuadro comparativo.

Una vez terminada las pruebas de la red sin métodos de calidad de servicios, se detuvieron las capturas y se tomaron los resultados arrojados por el software, estos se buscan en el ítem de Statistics en el protocolo que se active con el servicio enviado, se selecciona mostrar todos los streams y a continuación Analizar, estos datos se encuentran plasmados en los cuadros que se muestran a continuación.

Luego se dejó funcionando la red con métodos de calidad de servicios y se realizó el mismo proceso anterior.

Figura 20. Cuadro Comparativo de Resultados

ANALISIS COMPARATIVO DE LOS RESULTADOS DE LAS PRUEBAS							
Servicio	Parametros Evaluados Sin Calidad de Servicios QoS				IP Origen	IP Destino	Protocolo
	Paquetes Perdidos	Jitter	Velocidad de Transferencia	Tiempo de Transferencia			
Datos	NA	NA	14,9 Kbps	4,32 m	172.16.4.5	172.16.2.2	TCTP/HTTP
Voz IP	0%	3.66 ms	NA	NA	172.16.4.5	172.16.2.2	RTP/SKINNY
Video IP	0,35%	NA	38 Kbps	NA	172.16.4.5	172.16.2.2	TCP/HTTP
Datos-Voz-Video	0,61%	8,01 ms	6,6 Kbps	NA	172.16.4.5	172.16.2.2	RTP/HTTP/TCP/SIP
ANALISIS COMPARATIVO DE LOS RESULTADOS DE LAS PRUEBAS							
Servicio	Parametros Evaluados con Calidad de Servicios QoS				IP Origen	IP Destino	Protocolo
	Paquetes Perdidos	Jitter	Velocidad de Transferencia	Tiempo de Transferencia			
Datos	NA	NA	15,5 Kbps	4,21 m	172.16.4.5	172.16.2.2	TCTP/HTTP/IP
Voz IP	0%	3,4 ms	NA	NA	172.16.4.5	172.16.2.2	RTP/SKINNY
Video IP	0,16%	NA	43 Kbps	1,35 m	172.16.4.5	172.16.2.2	TCP/HTTP
Datos-Voz-Video	0%	3,34 ms	7,5 Kbps	4,39	172.16.4.5	172.16.2.2	RTP/HTTP/TCP/SIP

NA: No Aplica

Análisis: Basándonos en los resultados de los parámetros que se muestra en la figura 7 se puede concluir:

- Utilizando el servicio de voz son mas óptimos cuando la Red tiene implementados métodos de calidad de servicios QoS, ya que para esta prueba

aunque en ninguno de los dos casos vemos pérdida de paquetes, se pudo analizar por los datos que arrojó la herramienta Wireshark que se presentó una disminución de los Jitter.

- Utilizando el servicio de video ip también son más óptimos cuando la Red tiene implementados métodos de calidad de servicios QoS, en la figura 7 se puede observar que cuando la red tiene implementados métodos de calidad de servicios la velocidad de transferencia es mayor y el porcentaje de paquetes perdidos es menor, para video ip estos fueron los parámetros que utilizaron.
- Los parámetros utilizados en el servicio de Datos resultan más óptimos cuando la Red tiene implementados métodos de calidad de servicios QoS, ya que estos datos muestran como la velocidad de transferencia es mayor y el tiempo es menor.
- cuando los servicios son enviados de una forma simultánea, se dieron diferencias en los resultados y que cada uno de los parámetros mejoró para la prueba en donde la red tenía implementado Métodos de calidad de servicios QoS

De los anteriores cuadros comparativos se puede decir que aplicar los métodos de calidad de servicios, mejora visiblemente el rendimiento de una red, los tiempos de respuestas y disminuye la pérdida de paquetes y jitter, así las comunicaciones se hacen más efectivas y óptimas.

## 6. CONCLUSIONES

Para la realización de este trabajo de grado se planteó un objetivo general del proyecto se puede decir y definir lo siguiente:

Dado que este objetivo era “Realizar un Estudio Comparativo sobre las Redes Convergentes con Calidad de Servicios (QoS)”, se puede dar por cumplido, dado que en este estudio se realizaron los laboratorios con equipos activos de última generación y de gama empresarial, nos ayudó a conocer sobre la configuración de estos equipos activos, los detalles de estas configuraciones, reforzar la parte de redes de computadores y de telecomunicaciones de nuestra carrera profesional, en fin estas prácticas, laboratorios no solo permitieron lograr los resultados esperados, sino que se adquirieron nuevos conocimientos en networking, enrutamiento, manejo de servicios en redes convergentes, conocer el desempeño y lógica de utilización de equipos activos, se logra evidenciar que esta parte del Objetivo General se cumplió a cabalidad. También se plantearon tres objetivos específicos uno de ellos era Conocer los diferentes métodos de implementación de Calidad de Servicios (QoS), basados en servicios integrados, servicios diferenciados y AutoQoS, podemos decir que se cumplió este objetivo ya que se realizaron investigaciones sobre los métodos de la implementación de calidad de servicios que existen, se analizaron, y se decidió utilizar el método de AutoQoS ya que es fácil de implementar y, dejó mejores respuestas y los mejores resultados ya que se no produce esa carga tan grande como lo hace los servicios integrados, el cual sería el último método a recomendar para esta calidad que requieren los servicios, pero sin embargo algunas aplicaciones ya en producción tienen mayor desempeño y mayor aprovechamiento de sus anchos de Banda, el método mixto que toma lo mejor del método diferenciado y de método Integrado; este método hace que las aplicaciones tengan mejores desempeños y sean más óptimas las comunicaciones como tal. Por otro lado se puede decir que En el modelo DiffServ un paquete de la "clase" se pueden marcar directamente en los

paquetes, están clasificadas para recibir un tratamiento particular, en la transmisión (el comportamiento PHB) en los nodos a lo largo de su camino, lo que contrasta con el modelo IntServ donde se utiliza el Protocolo de Reserva de Recursos (RSVP) y control de admisión como mecanismos fundamentales para establecer y mantener QoS, dicho protocolo de señalización requiere que los routers, los flujos de paquetes QoS tengan un tratamiento especial.

DiffServ QoS logra una mejor escalabilidad, mientras que IntServ proporciona un mecanismo más estricto para la QoS del tráfico en tiempo real, divide el tráfico en un pequeño número de clases, y asigna recursos para cada clase de base, porque sólo tiene unas pocas clases de tráfico, el marcado, la policía, y la configuración de las operaciones sólo deberá aplicarse en los límites de red o hosts.<sup>27</sup>

AutoQoS permite automáticamente generar comandos de configuración de QoS para el equipo. El segundo objetivo específico era el de Ejecutar una práctica en laboratorio donde se trabaje con Router, Switch, Softphone, Diademas, Sistema de Videostream, Portátiles, Access Point, implementados en una red convergente para diagnosticar los comportamientos de los servicios evaluados (Datos, Voz ip y Video ip), podemos concluir que este objetivo se cumplió a cabalidad ya que se realizaron nueve (9) prácticas en las cuales trató temas de configuración de equipos activos, protocolo de enrutamiento dinámico OSPF, el cual quedó en el proyecto final dados sus resultados, su convergencia y sus rendimientos. Las prácticas se realizaron en el laboratorio de redes de la Universidad Tecnológica estas ayudaron a determinar cual importante es la calidad de servicios en los servicios que se movilizan en las actuales redes convergentes y multipropósito. La topología que se utilizó se expuso en la sección de escenario de prácticas del proyecto, en la parte de resultados se encuentran los cuadros comparativos y evidencias de las pruebas realizadas, Hay que tener en cuenta que para este proyecto se utilizaron equipos activos de la Universidad Tecnológica Bolívar de

---

<sup>27</sup> [http://www.cisco.com/en/US/products/ps6558/products\\_ios\\_technology\\_home.html](http://www.cisco.com/en/US/products/ps6558/products_ios_technology_home.html)



las marcas Cisco System, 3COM, herramientas informáticas como Sistema Operativo Microsoft, como un sinnúmero de elementos y herramientas adicionales para la parte de redes, supervisión de tráfico, etc.

El tercer objetivo específico era el de Mostrar paso a paso la forma de instalar, configurar, operar y administrar los servicios implementados en la red convergente en las prácticas realizadas se logró implementar esta red convergente con Calidad de Servicios (QoS), logrando de esta manera implementar varios modelos que como se describía anteriormente los mejores resultados se obtuvieron implementando el método de AutoQoS.

En la primera práctica donde se implementaba una red convergente sin métodos de calidad de servicios (QoS) podemos concluir que al momento de utilizar un servicio de esta red sin que los demás servicios se utilizaran no existían o no se presentaron problemas, pero cuando se utilizaban más de un servicio de manera simultánea se empezaban a aumentar los tiempos de respuestas, se empezaron a sentir las fallas en la calidad de los servicios, algunas veces las voces robotizadas o degradadas, los datos tenían mayores tiempos al momento de transferirse en fin todos los servicios si eran utilizados simultáneamente empezaban a causar retardos y perdidas en las calidades de los servicios, haciendo algunas veces sentir que toda la red se bloqueaba o los tiempos en las respuestas eran casi que extremadamente exagerados; notándose así que muy a pesar de tener varios servicios en las actuales redes convergentes si no se toman las medidas y los controles necesarios se puede llegar a tener problemas graves en las transmisiones de estos servicios multipropósito. Esto funciona de esta manera debido a que las redes IP trabajan por defecto con la opción del Mejor esfuerzo, “La mayor cantidad, en el menor tiempo posible”, esto hace que las redes con cualquier servicio requiera lo máximo en Ancho de banda que pueda tomar de un canal, al verse simultáneamente con otros servicios que también requieren el máximo de ancho de banda es cuando hacen que las redes sean de mayores tiempos de respuestas y algunas terminen ocasionando un problema de DoS

(Denegación de Servicios) a los usuarios finales.

En la segunda práctica donde se implementó una red convergente con métodos de calidad de servicios se llegó a la conclusión que la red se podía transmitir servicios variados simultáneamente de manera óptima y con las calidades y requerimientos que cada servicio sugería, esto funcionaba bastante bien y solo se veía afectado cuando se tenían demasiadas sesiones simultáneamente para el mismo ancho de banda anterior o cuando servicios como FTP trataban de obtener para ello todo el ancho de banda existente.

Para la realización del proyecto se llevó a cabo la metodología que habíamos propuesto con anterioridad, dicha metodología fue la Experimental, se tuvo buenas experiencias cuando la aplicamos nos dio muy buenos resultados ya que se pudo ampliar nuestros conocimientos y tener un mejor dominio del tema; podemos concluir que es buena al momento de la realización de este proyecto de grado y lo podemos apreciar a lo largo del trabajo de grado.

Al principio de la realización de este trabajo de grado se tuvo varios inconvenientes ya que no contábamos con los equipos suficientes para llevar a cabo la totalidad del proyecto, tuvimos el apoyo de la Universidad tecnológica de Bolívar (UTB) nos colaboró con el préstamo de equipos como routers 2800, switch, pcs, cables, laboratorio de redes en general. Al el momento de realizar las pruebas se presentaron algunas fallaban la comunicación entre las ciudades a veces por error en la configuración y otras por fallas técnicas de los equipos, las cuales solucionábamos realizando la revisión exhaustiva de la configuración y remplazando los equipos que estaban en mal estado; en general podemos decir que este trabajo de grado fue una experiencia grata, se tuvo la oportunidad de aprender y conocer las ventajas que hay en implementar red Convergente con métodos de calidad de servicios (QoS) que sin implementar métodos de Calidad de servicios (Qos).

## 7. RECOMENDACIONES

Para tener éxito en la implementación de redes de nueva generación con QoS les sugerimos lo siguiente:

- ✓ Realizar un estudio detallado del estado actual de la red para ver que tan factible es la implementación de esta tecnología ya que a través de esta podemos evitar la congestión de algunos nodos, para que esto no afecte algunas aplicaciones que requieran de un ancho de banda especial como es el caso de la videoconferencia y telefonía IP, debido a que en estas se hace necesario garantizar que la transmisión de los datos sea realizada sin interrupción y sin pérdida de paquetes.
- ✓ Verificar que la empresa cuente con los dispositivos que admitan la implementación de QoS, en cuanto a los Routers se recomienda utilizar la Versión Cisco 2800 en adelante con IOS c2800nm-adventerprisek9-mz.124-19.bin, y los Switchs Cisco a partir de la Versión 2950, verificar que la red se encuentre funcionando.
- ✓ Utilizar un mayor ancho de banda para obtener mejores resultados ya que en este proyecto se utilizó un ancho de banda de 128Kps puesto que ese era la capacidad que soportaba los cables seriales.
- ✓ Utilizar una herramienta de monitoreo de red la cual le permita analizar y evaluar los parámetros de calidad de servicios (Jittler, Delay, Perdida de Paquetes, velocidad de transferencia, tiempo de transferencia).

✓ Conformer grupos de estudios e investigación liderados por los docentes de la universidad no solo con miras a la implementación óptima de redes convergentes de acuerdo con las necesidades q tienen, sino también con miras al desarrollo de protocolo y arquitectura que permitan garantizar las calidades de servicio en este tipo de redes de nueva generación, ya que muchas de las tecnologías son susceptible a ser mejoradas.

## 8. GLOSARIO

**Acuse de Recibo:** Las estaciones receptoras envían acuses de recibo para confirmar la recepción de datos se utilizan ACK.

**Access Point:** significa punto de acceso, se trata de un dispositivo utilizado en redes inalámbricas de área local (WLAN - *Wireless Local Area Network*), se encarga de ser una puerta de entrada a la red inalámbrica en un lugar específico y para una cobertura de radio determinada, para cualquier dispositivo que solicite acceder, siempre y cuando esté configurado y tenga los permisos necesarios.

**AutoQoS:** Es un método de implementación que utiliza cisco par implementar de calidad de servicios (QoS) de una forma automática y más fácil al momento de configurar.

**Ancho de banda:** Cantidad de datos que se pueden transmitir en una cantidad de tiempo determinada.

**Backbone:** La parte de la red que actúa como ruta principal para el tráfico que se origina en otras redes o que las tienen como destino.

**Broadcast:** Forma de transmisión por la cual un dispositivo transmite a todos los dispositivos dentro de la red o de otra red.

**Calidad de Servicios (QoS):** Quality of Services Medida del rendimiento de un sistema de transmisión que refleja la calidad de la transmisión y disponibilidad de servicio.<sup>28</sup>

---

<sup>28</sup> <http://www.codorama.com/diccionario.html#q>

**Clases de Servicios:** Destaca las configuraciones incorrectas o las aplicaciones no priorizadas visualizando una categoría Desconocida, esta función le ayuda a localizar rápidamente la configuración incorrecta y a mejorar el rendimiento de la aplicación. Además, puede ver cuánto ancho de banda utilizan para cada clase aplicaciones como voz, video, web, streaming.

**CLI:** (Interfaz de líneas de Comandos) Permite configurar manualmente interfaz por interfaz las opciones de QoS, es un método poco escalable.<sup>29</sup>

**Class-map:** Se utiliza para crear una clase de tráfico, y definir los criterios que deben cumplir los paquetes para pertenecer a ella. Los criterios pueden ser: Listas de acceso, otras clases, valor de CoS de capa 2, MAC de destino, MAC de origen, interfaz de entrada, DSCP, precedencia IP, rango de puertos RTP y no de protocolo.<sup>30</sup>

**DoS:** Es la negación de un servicio esta puede ser temporal o prolongada, puede ocasionar diversos trastornos en la red como la falta de conectividad, generalmente se debe a una falla técnica.<sup>31</sup>

**Delay:** tiempo que transcurre de ida y vuelta de un paquete.

**Diademas:** Es un dispositivo que sirve para realizar conferencias de voz sobre ip, grabar mensajes digitales.

---

<sup>29</sup> <http://www.scribd.com/doc/23309813/Proyecto-QoS-Sobre-VoIP>

<sup>30</sup> <http://toip.uchile.cl/mediawiki/upload/9/92/Redaccion73.pdf>

<sup>31</sup> <http://tecnologia.glosario.net/terminos-tecnicos-internet/dos-550.html>

**DSCP:** (*Differentiated Services Code Point*) hace referencia al segundo byte en la cabecera de los paquetes IP que se utiliza para diferenciar la calidad en la comunicación que quieren los datos que se transportan.

Originalmente se definió este byte para un uso con otro formato: ToS (type of service = tipo de servicio) pero con el mismo objetivo de diferenciar el tráfico. bit 0 a 5 DSCP bit 6 y 7 sin uso.<sup>32</sup>

**EIGRP:** Es un protocolo de enrutamiento con clase propietario de Cisco basado en IGRP, ofrece tiempos de convergencia más rápidos, mejor escalabilidad y gestión superior de los bucles de enrutamiento.

**Enrutamiento:** Proceso para encontrar la ruta hacia un host destino, el enrutamiento en redes de gran tamaño es muy complejos debido a la cantidad de destinos intermediarios que se debe atravesar un paquete para llegar a su destino.

**Escalable:** La capacidad que tiene una red para adaptarse a los incrementos de la demanda sin sufrir efectos negativos sobre su rendimientos.

**Ethernet:** Es el nombre de una tecnología de redes de computadoras de área local (LANs) basada en tramas de datos.

**Gateway:** Dispositivo con fines especiales que efectúa conversión de capa de aplicación de la información de un stack de protocolo a otra.

**Frame Relay:** Protocolo estándar industrial de capa de enlace de datos conmutados, maneja múltiples circuitos mediante el encapsulamiento HDLC entre los dispositivos conectados.<sup>33</sup>

---

<sup>32</sup> [http://es.wikipedia.org/wiki/Differentiated\\_Services\\_Code\\_Point](http://es.wikipedia.org/wiki/Differentiated_Services_Code_Point)

**HDLC:** Control de enlace de enlace de datos de alto nivel, protocolo de enlace de datos sincrónico, orientado a bits.<sup>34</sup>

**ICMP:** Protocolo de mensajería de control y error de internet, se utiliza para controlar si un paquete no puede alcanzar su destino, si su vida ha expirado si el encabezamiento lleva un valor no permitido, si es un paquete de eco o respuesta.

**Infraestructura:** Es la topología de una red que consta de elementos básicos.

**IETF:** (Internet Engineering Task Force - Grupo de Trabajo de Ingeniería de Internet) Organización de técnicos que administran tareas de ingeniería de telecomunicaciones, principalmente de Internet (ej: mejora de protocolos o darlos de baja, etc.

**Jittler (Variación de retardo):** Los paquetes IP se envían por Internet a intervalos regulares a través de diferentes rutas. Lo que se espera es recibir los paquetes en el mismo orden y con el mismo intervalo. Sin embargo, en ocasiones los paquetes pueden desordenarse, por lo que necesitan ser reconstruidos.

**Latencia:** Es el tiempo que requiere un paquete IP para viajar del punto A al punto B y de vuelta, el exceso de latencia puede ocasionar retrasos en la conversación.

**Multiplexación:** Es el proceso que se utiliza para entrelazar las piezas de una conversaciones separadas en la red.

---

<sup>33</sup> <http://www.codorama.com/diccionario.html#e>

<sup>34</sup> <http://www.inf.uct.cl/~amellado/archivos/teleprocesos2.pdf>



**MQC:** (configuración de Qos Modular) permite la configuración modular a partir de la definición de clases y políticas.

**NBAR:** (Network-Based Application Recognition) Es un motor de clasificación de tráfico que reconoce una amplia variedad de aplicaciones, incluyendo aquellas que utilizan asignación dinámica de puertos TCP o UDP.

**OSPF:** Protocolo de enrutamiento interior de estado de enlace que utiliza algoritmo de Dijkstra para calcular el árbol con la ruta más corta.<sup>35</sup>

**Performance:** Desempeño con respecto al rendimiento de un dispositivo, programa o una conexión a una red.

**Pérdida de paquetes:** esto se relaciona con la falta de entrega de un paquete de datos, la mayoría de las veces debido a una sobrecarga de la red.

**Pérdida de secuencia:** es una modificación en el orden de llegada de los paquetes.

**Per-Hop-Behavior (PHB):** define el tratamiento en cada nodo, es una descripción del comportamiento de reenvío observado exteriormente, puede ser implementado por distintos mecanismos.

**Policing:** el proceso de descarte de paquetes dentro de un arroyo de tráfico en Concordancia con el estado de un correspondiente medidor (meter) cumpliendo un determinado perfil.

---

<sup>35</sup> Guía de aprendizaje ccna 3 and 4, version 3.1, cisco networking

**Policy-map:** Especifica las políticas asociadas a cada clase. Se puede garantizar ancho de banda mínimo (lo que configura el peso de la cola asociada). Se puede acondicionar tráfico (tráfico shapping). Se permite asociar una cola de prioridad estricta a un grupo de clases. Se puede especificar Policing configurando ancho de banda permitido.<sup>36</sup>

**Power over Ethernet:** Transfiere de forma segura potencia eléctrica con datos, a dispositivos remotos sobre un cableado de categoría 3,5 ó 6 en una red ethernet sin necesidad de modificar el cableado existente.

**RTT:** Tiempo de ida y vuelta tiempo necesario para que una comunicación viaje desde el origen hasta el destino y regrese, es utilizado por algunos algoritmos para calcular rutas óptimas.

**RTP:(** Protocolo de Tiempo Real) Provee la entrega en tiempo real de audio y video. Es típicamente usado para transmisión de datos usando UDP. Se encarga de la identificación de la carga útil, secuencia y entrega supervisada.

**RTCP:** Realiza el control del RTP.

**RSVP:** Protocolo de reserva de recursos.

**Redes Convergentes:** Redes que Integran Video, Voz, Datos y Telefonía IP y viaja por un mismo medio.

**Redes de Nueva Generación:** también se le puede llamar redes Convergentes, se refiere a la evolución de la actual infraestructura de redes de telecomunicación y acceso telefónico con el objetivo de lograr la congruencia de los nuevos servicios multimedia (voz, datos, video).

---

<sup>36</sup> <http://toip.uchile.cl/mediawiki/upload/9/92/Redaccion73.pdf>

**Redes Inalámbricas:** Son aquellas que se comunican por un medio de transmisión no guiado (sin cables) mediante ondas electromagnéticas. La transmisión y la recepción se realizan a través de antenas.

**Retardo:** esto caracteriza el retraso entre la transmisión y la recepción de un paquete.

**Router:** Dispositivo de capa de red que utiliza una o más métricas para la determinar la ruta optima a través de la cual se debe enviar el tráfico de la red.

**Servicios Diferenciados:** Estos servicios logran una mejor escalabilidad, divide el tráfico en un pequeño número de clases, y asigna recursos para cada clase de base, garantías de calidad de servicio no son tan severas la priorización de flujos mediante Clase de Servicio.

**Servicios Integrados:** Estos servicios utilizan el Protocolo de Reserva de Recursos (RSVP) y control de admisión como mecanismos fundamentales para establecer y mantener QoS, dicho protocolo de señalización requiere que los routers, los flujos de paquetes QoS tengan un tratamiento especial. Proporciona un mecanismo más estricto para la QoS del tráfico en tiempo real, borra un camino para el flujo antes de enviarlo, hay poca escalabilidad, Todos los nodos deben implementar Int Serv.

**Servicios Mejor Esfuerzo (BEST EFFORT):** La mayor cantidad, en el menor tiempo posible, esto hace que las redes con cualquier servicio requiera lo máximo en Ancho de banda que pueda tomar de un canal, al verse simultáneamente con otros servicios que también requieren el máximo de ancho de banda es cuando

hacen que las redes sean de mayores tiempos de respuestas y algunas terminen ocasionando un problema de DoS.

**Service-policy:** Adjunta la política de servicio creada con policy-map a una interfaz, especificando la dirección en que se debe aplicar (in o out).<sup>37</sup>

**SIP:** (Protocolo de Inicio de Sesión) Es un protocolo a nivel de aplicación que puede establecer, modificar y terminar sesiones o llamadas multimedia a través de red ip, incluyendo conferencias, telefonía en internet, mensajería a través de internet.

**Skinny:** Protocolo de control de clientes, es el protocolo por defecto para los puntos finales en un cisco call manager PBX.

**Softphone:** Es un software que hace una simulación de teléfono convencional por computadora. Es decir, permite usar la computadora para hacer llamadas a otros softphones o a otros teléfonos convencionales.

**Swicth:** Dispositivo electrónico o mecánico que permite que se establezca una conexión según sea necesario y que se termine cuando no haya ninguna sesión que se deba mantener.

**System Log:** Describe visualizado en texto todos los pasos del procesador, se utiliza también para encontrar y analizar problemas.

**Tiempo de establecimiento de llamada:** El tiempo que se requiere para establecer una llamada conmutada entre dispositivos.<sup>38</sup>

---

<sup>37</sup> <http://toip.uchile.cl/mediawiki/upload/9/92/Redaccion73.pdf>

<sup>38</sup> [www.gratisweb.com/gulle79/glosario/t.htm](http://www.gratisweb.com/gulle79/glosario/t.htm)

**UDP:** Protocolo de datagramas de usuario.

**UTP:** Par trenzado no blindado, medio de cableado que se utiliza cuatro pares se utiliza en diversas redes, existen cinco tipos de categorías.<sup>39</sup>

**Video ip:** Sistema que ofrece a los usuarios la posibilidad de controlar y grabar en vídeo a través de una red IP.<sup>40</sup>

**Voip:** Es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos sin necesidad de contar con su propia infraestructura de red, las cabeceras IP/UDP/RTP encapsulan la información de voz y la pasan a través de la pila ip, en la parte receptora, la información es desencapsulada.

**WDS:** (Sistema de Distribución Inalámbrico) Es una función que permite la interconexión inalámbrica entre routers o puntos de acceso, de esta manera se puede usar el router como repetidor de otra señal o para interconectar dos redes.

---

<sup>39</sup> [docente.ucol.mx/a1972052/public\\_html/CABLE%20PAR%20TRENZADO.htm](http://docente.ucol.mx/a1972052/public_html/CABLE%20PAR%20TRENZADO.htm)

<sup>40</sup> [http://www.axis.com/products/video/about\\_networkvideo/network\\_video.es.htm](http://www.axis.com/products/video/about_networkvideo/network_video.es.htm)

## 9. BIBLIOGRAFÍA

- ✓ Trabajo de Grado, Análisis del estándar IMS 3GPP orientado a la interconexión de Redes fijas y móviles en conjunto con las redes de Nueva generación NGN TISPAN/ETS, Darwin José Calle Torres, <http://www.itba.edu.ar/capis/epg-tesis-y-tf/garcia-tfe.pdf>
- ✓ AT&T , Boletín de Prensa, “Mayor Competitividad: Principal Beneficio De La “Convergencia De Redes”, Nacarid Useche, [http://www.corp.att.com/latin\\_america\\_es/docs/20050912-1-es.pdf](http://www.corp.att.com/latin_america_es/docs/20050912-1-es.pdf)
- ✓ Calidad de Servicios QoS, [http://www2.ing.puc.cl/~iee3542/amplif\\_4.ppt](http://www2.ing.puc.cl/~iee3542/amplif_4.ppt)
- ✓ Quality of Service (QoS), Cisco, [http://www.cisco.com/en/US/products/ps6558/products\\_ios\\_technology\\_home.html](http://www.cisco.com/en/US/products/ps6558/products_ios_technology_home.html)
- ✓ Reseña de Calidad de Servicio en ambientes IPv6, Gustavo Mercado, <http://www.ipv6.codarec.frm.utn.edu.ar/areas/QoS//Publicaciones//Resena%20de%20Calidad%20de%20Servicio%20en%20ambientes%20IPv6%20Filminas.pdf>
  
- ✓ La evolución de los sistemas de vigilancia por vídeo, ,Axis Communications, [http://www.axis.com/products/video/about\\_networkvideo/network\\_video.es.htm](http://www.axis.com/products/video/about_networkvideo/network_video.es.htm)
  
- ✓ Diccionario Online, <http://www.codorama.com/diccionario.html#q>
  
- ✓ <http://www.inf.uct.cl/~amellado/archivos/teleprocesos2.pdf>
  
- ✓ Guía de aprendizaje ccna 3 and 4, versión 3.1, cisco networking
  
- ✓ Calidad de Servicio Ip, Capitulo 2, Scribd <http://www.scribd.com/doc/20063585/Capitulo-2-ONT>

## 10. ANEXOS

Para la realización de este proyecto se tuvo que realizar diferentes actividades entre ellas las instalaciones de algunos softwares que eran fundamentales para el momento de realizar las respectivas prácticas y pruebas a continuación le anexamos las configuraciones realizadas en cada uno de los router con y sin calidad de servicios QoS y los pasos a siguieron para las instalaciones de los servidores y software:

### **Configuración de la Primera práctica sin métodos de calidad de servicios**

A continuación se muestra la configuración de las 4 ciudades teniendo en cuenta la topología (ver figura1) sin implementar métodos de calidad de servicios.

### **✓ Configuraciones de los Routers Sin Implementación de Métodos de Calidad de Servicios QoS**

#### **a) Cartagena**

Current configuration: 1676 bytes

!

Version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption *//no servicio de encriptación de password*

!

Hostname Cartagena *// Asigna nombre al Router*

!

boot-start-marker

boot-end-marker

```

enable secret 5 $1$SXkE$rXDMNAprAzKVF2uCwJHW..//está habilitado el password secreto
!
no aaa new-model // no nuevo modelo
!
ip cef
no ip dhcp use vrf connected //no ip dhcp vrf conectado
!
// Declaración de los DHCP para Datos esto se hace para tener una dirección de forma dinámica en el rango que se le ha establecido en la red
ip dhcp pool datos
network 172.16.2.0 255.255.255.128 //sirve para declarar el rango de dirección ip a asignar
default-router 172.16.2.1// Dirección del Router por defecto
!
// Declaración de los DHCP para Voz esto se hace para tener una dirección de forma dinámica en el rango que se le ha establecido en la red para voz
ip dhcp pool voz
network 172.16.2.128 255.255.255.192//sirve para declarar el rango de dirección ip a asignar a los teléfonos
default-router 172.16.2.129 // Dirección del Router por defecto
option 150 ip 172.16.2.129 // permite que los teléfonos descarguen del router su imagen vía tftp
!
// Declaración de los DHCP para Video esto se hace para tener una dirección de forma dinámica en el rango que se le ha establecido en la red
ip dhcp pool video
network 172.16.2.192 255.255.255.192//sirve para declarar el rango de dirección ip a asignar
default-router 172.16.2.193 // Dirección del Router por defecto
!
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3

```



```

!
voice-card 0 //tarjeta de voz 0
no dspfarm // no tarjeta dspfarm
!
interface FastEthernet0/0.10 //Declaración de la subinterface de Datos
encapsulation dot1Q 10 // sirve para que hay comunicación entre las vlan
ip address 172.16.2.1 255.255.255.128 //Asignación de la dirección Ip y Mascara de Red
!
interface FastEthernet0/0.20 //Declaración de la subinterface de voz
encapsulation dot1Q 20 // permite que los teléfonos descarguen del router su imagen vía tftp
ip address 172.16.2.129 255.255.255.192 //Asignación de la dirección Ip y Mascara de Red
!
interface FastEthernet0/0.30 //Declaración de la subinterface de de video
encapsulation dot1Q 30// permite que los teléfonos descarguen del router su imagen vía tftp
ip address 172.16.2.193 255.255.255.192 //Asignación de la dirección Ip y Mascara de Red
!
interface Serial0/3/1
bandwidth inherit 10000000 // Se utiliza para que las subinterfaces hereden el ancho de
banda de la interfaz principal
ip address 200.20.0.9 255.255.255.252 //asignación de Ip y mascara de red
clock rate 128000 // establece la velocidad de la señal del reloj que se generaran en las
interfaces seriales
!
router ospf 101 // Se entra en modo de configuración del protocolo OSPF , Iniciando un proceso
de enrutamiento definido.

log-adjacency-changes //Creación de un registro en un archivo log de los cambios de
adyacencias, esto asegura que así que el intercambio de información no se pierda así algún
dispositivo pierda conexión.

network 172.16.2.0 0.0.0.127 área 0 // sirve para configurar un proceso de enrutamiento
OSPF y se asignan las redes a un mismo área, el área 0.

```

```
network 172.16.2.128 0.0.0.63 area 0
network 172.16.2.192 0.0.0.63 area 0
network 200.20.0.8 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server // no ip servidor http
no ip http secure-server // no ip servidor http seguro
!
control-plane // plano de control
!
Line con 0 //asignación de las líneas vty para asignar un password
line aux 0
line vty 0 4
password cisco // establecimiento del password
login
!
end //fin
```

## **b) Bogotá**

```
Current configuration: 1865 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
```

```

Hostname Bogotá // Asigna nombre al Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$SXkE$rXDMNAprAzKVF2uCwJHW...//está habilitado el password
secreto
!
no aaa new-model // no nuevo modelo
!
!
ip cef
no ip dhcp use vrf connected //no ip dhcp vrf conetado
!

ip dhcp pool datos // // Declaración de los DHCP para Datos esto se hace para tener una
dirección de forma dinámica en el rango que se le ha establecido en la red
network 172.16.3.0 255.255.255.128
default-router 172.16.3.1// ip de Router por defecto
!
ip dhcp pool video // // Declaración de los DHCP para Video esto se hace para tener una
dirección de forma dinámica en el rango que se le ha establecido en la red
network 172.16.3.192 255.255.255.192
default-router 172.16.3.193// ip de Router por defecto
!
ip dhcp pool voz // // Declaración de los DHCP para Voz esto se hace para tener una dirección
de forma dinámica en el rango que se le ha establecido en la red
network 172.16.3.128 255.255.255.192
default-router 172.16.3.129// ip de Router por defecto

```

```

option 150 ip 172.16.3.129 // permite que los teléfonos descarguen del router su imagen vía tftp
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
voice-card 0
no dspfarm
!
interface FastEthernet0/0.10//Declaración de la subinterface de Datos
encapsulation dot1Q 10 //sirve para haya comunicación entre las vlan
ip address 172.16.3.1 255.255.255.128 //Asignación de IP y mascara de Red
!
interface FastEthernet0/0.20//Declaración de la subinterface de voz
encapsulation dot1Q 20 // sirve para que haya comunicación entre las vlan

ip address 172.16.3.129 255.255.255.192//Asignación de IP y mascara de Red
interface FastEthernet0/0.30 //Declaración de la subinterface de Video
encapsulation dot1Q 30 // sirve para que haya comunicación entre las vlan
ip address 172.16.3.193 255.255.255.192//Asignación de IP y mascara de Red
!

interface Serial0/3/0
bandwidth 10000000 //Se utiliza para asignar una velocidad en la interfaz del router
ip address 200.20.0.13 255.255.255.252 //asignación de Ip y mascara de red
clock rate 128000 // establece la velocidad de la señal del reloj que se generaran en las
interfases seriales.
!
interface Serial0/3/1
bandwidth 10000000 // Se utiliza para asignar una velocidad en la interfaz del router

```

```
ip address 200.20.0.10 255.255.255.252 // asignación de Ip y mascara de red
!
router ospf 101 // Se entra en modo de configuración del protocolo OSPF , Iniciando un proceso
de enrutamiento definido.
Log-adjacency-changes//Creación de un registro en un archivo log de los cambios de
adyacencias, esto asegura que así que el intercambio de información no se pierda así algún
dispositivo pierda conexión.
network 172.16.3.0 0.0.0.127 área 0 // se configura un proceso de enrutamiento OSPF y se
asignan las redes a un mismo área, el área 0.
network 172.16.3.128 0.0.0.63 area 0
network 172.16.3.192 0.0.0.63 area 0
network 200.20.0.8 0.0.0.3 area 0
network 200.20.0.12 0.0.0.3 area 0
!
ip forward-protocol nd
!
ip http server // no ip servidor de http
no ip http secure-server// no ip servidor de http seguro.
!
control-plane //plano de control
!
Line con 0 //asignación de las líneas vty para asignar un password
line aux 0
line vty 0 4
password cisco // establecimiento del password
login
!
end //fin
```

### c) Manizales

Current configuration: 2982 bytes

!

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

Hostname Manizales *// Asigna nombre al Router*

!

boot-start-marker

boot-end-marker

!

enable secret 5 \$1\$MPoG\$QOhDli3ND7NWycR6wWYQ20*//está habilitado el password*

!

ip cef

no ip dhcp use vrf connected *//no ip dhcp vrf conectado*

!

ip dhcp pool datos *// Declaración de los DHCP para Datos esto se hace para tener una dirección de forma dinámica en el rango que se le ha establecido en la red*

network 172.16.4.0 255.255.255.128

default-router 172.16.4.1*// ip del router por defecto*

!

ip dhcp pool voz *// Declaración de los DHCP para Voz esto se hace para tener una dirección de forma dinámica en el rango que se le ha establecido en la red*

network 172.16.4.128 255.255.255.192

default-router 172.16.4.129*// ip del router por defecto*

option 150 ip 172.16.4.129*// sirve para que los teléfonos descargue su imagen vía tftp*

!

```

ip dhcp pool video // Declaración de los DHCP para Video esto se hace para tener una
dirección de forma dinámica en el rango que se le ha establecido en la red
network 172.16.4.192 255.255.255.192
default-router 172.16.4.193// ip del router por defecto
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
voice-card 0 // tarjeta de voz 0
no dspfarm // no tarjeta dspfarm
!
interface Loopback0 //declaración de la interface loopback, permite que si se cae una interface
siga funcionando el OSPF.
ip address 172.16.1.1 255.255.255.255 //asignación de la ip y mascara de la loopback
!
interface FastEthernet0/0.40 //Declaración de la subinterface de Datos
encapsulation dot1Q 40 // permite que hay comunicación entre las vlan
ip address 172.16.4.1 255.255.255.128//Asignación de IP y mascara de Red
!
interface FastEthernet0/0.50 //Declaración de la subinterface de voz.
encapsulation dot1Q 50// permite que haya comunicación entre las vlan
ip address 172.16.4.129 255.255.255.192//Asignación de IP y mascara de Red
!
interface FastEthernet0/0.60 //Declaración de la subinterface de video
encapsulation dot1Q 60// permite que haya comunicación entre las vlan
ip address 172.16.4.193 255.255.255.192//Asignación de IP y mascara de Red
!
interface Serial0/3/0
bandwidth 10000000 // Se utiliza para asignar una velocidad en la interfaz del router
ip address 200.20.0.17 255.255.255.252 //asignación de Ip y mascara de red

```

```

clock rate 128000 // asignación de clock rate establece la velocidad de la señal del reloj que se
generaran en las interfaces seriales
!
interface Serial0/3/1
bandwidth 10000000 // Se utiliza para asignar una velocidad en la interfaz del router
ip address 200.20.0.14 255.255.255.252 // asignación de dirección ip y mascara de red
!
router ospf 101 // Se entra en modo de configuración del protocolo OSPF, Iniciando un proceso
de enrutamiento definido.
log-adjacency-changes // Creación de un registro en un archivo log de los cambios de
adyacencias, esto asegura que así que el intercambio de información no se pierda así algún
dispositivo pierda conexión.
network 172.16.1.1 0.0.0.0 área 0 //Con este comando se configura un proceso de
enrutamiento OSPF y se asignan las redes a un mismo área, el área 0.
network 172.16.4.0 0.0.0.127 area 0
network 172.16.4.128 0.0.0.63 area 0
network 172.16.4.192 0.0.0.63 area 0
network 200.20.0.12 0.0.0.3 area 0
network 200.20.0.16 0.0.0.3 area 0
!
ip http server
no ip http secure-server // no ip de servidor http seguro
!
!
control-plane // plano de control
!
telephony-service //Habilita el servicio de Telefonía
max-ephones 20 //asignación del número máximo de teléfonos
max-dn 20// máximo número de directorio
ip source-address 172.16.1.1 port 2000 // ip para conseguir los archivos de configuración.

```



system message TECNOLOGICA DE BOLIVAR //asignación del mensaje en el sistema  
network-locale ES //Red local  
max-conferences 8 gain -6 //asignación número máximo de conferencias  
directory last-name-first //Permite ingresar de número y nombre en el Directorio  
directory entry 1 6531641 name SEDE MANIZALES  
directory entry 2 6531642 name SEDE CARTAGENA  
directory entry 3 6531643 name SEDE BOGOTA  
directory entry 4 6531644 name SEDE PEREIRA  
!  
ephone-dn 1 // Configuración del teléfono 1  
number 6531641// número del teléfono  
description SEDE MANIZALES// Descripción del teléfono  
name SEDE MANIZALES//Nombre de la sede  
!  
!  
ephone-dn 2 // Configuración del teléfono 2  
number 6531642// número del teléfono  
description SEDE CARTAGENA// Descripción del teléfono  
name SEDE CARTAGENA//Nombre de la sede  
!  
ephone-dn 3 // Configuración del teléfono 3  
number 6531643// número del teléfono  
description SEDE BOGOTA// Descripción del teléfono  
name SEDE BOGOTA//Nombre de la sede  
!  
ephone-dn 4 // Configuración del teléfono 4  
number 6531644// número del teléfono  
description SEDE PEREIRA // Descripción del teléfono  
name PEREIRA//Nombre de la sede

```
!  
ephone 1 // Configuración del teléfono 1  
mac-address 0025.648E.C074 //Dirección MAC  
button 1:1// permite un solo número de teléfono  
!  
ephone 2// Configuración del teléfono 2  
mac-address 0025.648F.7D87//Dirección MAC  
button 1:2// permite un solo número de teléfono  
!  
ephone 3 // Configuración del teléfono 3  
mac-address 0025.648F.7E56 //Dirección MAC  
button 1:3// permite un solo número de teléfono  
!  
ephone 4 // Configuración del teléfono 4  
mac-address 0026.22C3.D1E4 //Dirección MAC  
button 1:5// permite un solo número de teléfono  
!  
line con 0  
line aux 0  
line vty 0 4//Configuración líneas vty para asignación de un password  
password cisco// establecimiento del password  
login  
¡End// fin
```

#### **d) Pereira**

Current configuration : 1722 bytes

```
!  
version 12.4  
service timestamps debug datetime msec
```

```

service timestamps log datetime msec
no service password-encryption // no servicio de encriptación de password
!
hostname Pereira //Asignación del nombre del router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$iT30$OPzVd9TyB5X1tpx0HqW.n1 // Habilitado el password
!
no aaa new-model // no nuevo modelo

ip cef
no ip dhcp use vrf connected// no ip dhcp vrf conectado
!
ip dhcp pool voz // // Declaración de los DHCP para Voz esto se hace para tener una dirección
de forma dinámica en el rango que se le ha establecido en la red
network 172.16.5.128 255.255.255.192
default-router 172.16.5.129// ip del router por defecto
option 150 ip 172.16.5.129 //permite que los teléfonos descargen su imagen vía tftp
!
ip dhcp pool datos // // Declaración de los DHCP para Datos esto se hace para tener una
dirección de forma dinámica en el rango que se le ha establecido en la red
network 172.16.5.0 255.255.255.128
default-router 172.16.5.1// ip del router por defecto
!
ip dhcp pool video// // Declaración de los DHCP para Datos esto se hace para tener una
dirección de forma dinámica en el rango que se le ha establecido en la red
network 172.16.5.192 255.255.255.192
default-router 172.16.5.193// ip del router por defecto

```

```

!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
voice-card 0 // tarjeta de voz 0
no dspfarm // no tarjeta dspfarm
!
interface FastEthernet0/0.40 //Declaración de la subinterface de Datos
encapsulation dot1Q 40 // permite que haya comunicación entre vlan
ip address 172.16.5.1 255.255.255.128 //Asignación de IP y mascara de Red
!
interface FastEthernet0/0.50 // Declaración de la subinterface de Voz
encapsulation dot1Q 50// permite que haya comunicación entre vlan
ip address 172.16.5.129 255.255.255.192 // Asignación de IP y mascara de Red
!
interface FastEthernet0/0.60//Declaración de la subinterface de video
encapsulation dot1Q 60// permite que haya comunicación entre vlan
ip address 172.16.5.193 255.255.255.192//Asignación de IP y mascara de Red
!
interface Serial0/3/0
bandwidth 10000000 // Se utiliza para asignar una velocidad en la interfaz del router
ip address 200.20.0.18 255.255.255.252 //Asignación de la dirección Ip y Mascara de Red
!
router ospf 101 // Se entra en modo de configuración del protocolo OSPF , Iniciando un proceso
de enrutamiento definido.
log-adjacency-changes // Creación de un registro en un archivo log de los cambios de
adyacencias, esto asegura que así que el intercambio de información no se pierda así algún
dispositivo pierda conexión.
network 172.16.5.0 0.0.0.127 area 0 //Con este comando se configura un proceso de
enrutamiento OSPF y se asignan las redes a un mismo área, el área 0.

```

```

network 172.16.5.128 0.0.0.63 area 0
network 172.16.5.192 0.0.0.63 area 0
network 200.20.0.16 0.0.0.3 area 0
!
ip forward-protocol nd
!
ip http server
no ip http secure-server //no ip de servidor http seguro
control-plane//plano de control
!
line con 0
line aux 0
line vty 0 4 //configuración de líneas vty
password cisco// establecimiento del password
login
!
End // fin

```

✓ Configuración de los Switch sin calidad de servicios QoS

### Switch Bogota – Manizales

```

Current configuration : 4924 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption //no servicio de encriptación de password
!
hostname bog-manizales //Asignación del nombre al switch
!
no aaa new-model // no nuevo modelo
ip subnet-zero
!

```

```

interface FastEthernet0/1
 switchport mode trunk // modo de acceso trunk
!
interface FastEthernet0/2
!
interface FastEthernet0/3
 switchport access vlan 10// acceso vlan 10
 switchport voice vlan 20// Puerto de voz vlan 20
!
interface FastEthernet0/13// interface fastethernet 0/13
 switchport mode trunk// modo trunk indica que por esa puerta pasarán diferente vlan que
 se permitan
 spanning-tree portfast
!
!
interface FastEthernet0/15// interface fastethernet 0/15
 switchport access vlan 40//Acceso a vlan 40
 switchport voice vlan 50 //Puerto de voz vlan 50
interface Vlan1
 no ip address
 no ip route-cache
!
 ip http server
!
 control-plane // plano de control
!
 line con 0
 line vty 0 4
 no login // no asignado password
!
End

```

### **Switch Cartagena – Pereira**

Current configuration : 5004 bytes

```

!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption//no servicio de encriptación de password
!
hostname crtg-pereira //Asignación del nombre al switch
!
no aaa new-model // no existe nuevo modelo

ip subnet-zero
!

```

```

interface FastEthernet0/1
  switchport mode trunk // modo de acceso trunk
  !
interface FastEthernet0/2
  !
interface FastEthernet0/3
  switchport access vlan 10// acceso vlan 10
  switchport voice vlan 20// Puerto de voz vlan 20
  !
interface FastEthernet0/13// interface fastethernet 0/13
  switchport mode trunk// modo trunk indica que por esa puerta pasarán diferente vlan que
  se permitan
  spanning-tree portfast
  !
  !
interface FastEthernet0/15// interface fastethernet 0/15
  switchport access vlan 40//Acceso a vlan 40
  switchport voice vlan 50 //Puerto de voz vlan 50
interface Vlan1
  no ip address
  no ip route-cache
  !
  ip http server
  !
  control-plane // plano de control
  !
  line con 0
  line vty 0 4
  no login // no asignado password
End

```

### 3.3 Implementación de la segunda práctica con parámetros de calidad de servicios (Qos)

A continuación se muestra las configuraciones los routers de cada una de las cuatro ciudades, implementando métodos de calidad de servicios.

✓ **Configuración de los routers con Implementación de Métodos de Calidad de Servicios (QoS)**

**a) Cartagena**

```
cartagena#show running-config
Building configuration...
Current configuration : 1676 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Cartagena // Asigna nombre al Router
!
boot-start-marker
boot-end-marker
!
no aaa new-model // no nuevo modelo
!
ip cef // habilitado CEF
no ip dhcp use vrf connected // no ip dhcp vrf conectado
!
// Declaración de los DHCP para Datos esto se hace para tener una dirección de forma dinámica
en el rango que se le ha establecido en la red
ip dhcp pool datos
network 172.16.2.0 255.255.255.128
default-router 172.16.2.1 // ip del router por defecto
!
```



*// Declaración de los DHCP para Voz esto se hace para tener una dirección de forma dinámica en el rango que se le ha establecido en la red*

ip dhcp pool voz

network 172.16.2.128 255.255.255.192

default-router 172.16.2.129 *// ip del router por defecto*

option 150 ip 172.16.2.129 *//permite que los teléfonos descargen su imagen vía tftp*

!

*// Declaración de los DHCP para Video esto se hace para tener una dirección de forma dinámica en el rango que se le ha establecido en la red*

ip dhcp pool video

network 172.16.2.192 255.255.255.192

default-router 172.16.2.193 *// ip del router por defecto*

!

ip auth-proxy max-nodata-conns 3

ip admission max-nodata-conns 3

!

voice-card 0 *// tarjeta de voz 0*

no dspfarm *// no tarjeta dspfarm*

!

class-map match-any AutoQoS-VoIP-RTP-Trust *//Define Clase de tráfico*

match ip dscp ef

class-map match-any AutoQoS-VoIP-Control-Trust

match ip dscp cs3

match ip dscp af31

!

policy-map AutoQoS-Policy-Trust *//Define Políticas de entrada y salida para cada interface*

class AutoQoS-VoIP-RTP-Trust

priority percent 70

class AutoQoS-VoIP-Control-Trust

```

bandwidth percent 5 // porcentaje de ancho de banda
class class-default
  fair-queue
!
interface FastEthernet0/0.10 //Declaración de la subinterface de Datos
encapsulation dot1Q 10 //permite que hay comunicación entre las vlan
ip address 172.16.2.1 255.255.255.128 //Asignación de la dirección Ip y Mascara de Red
!
interface FastEthernet0/0.20 //Declaración de la subinterface de voz
encapsulation dot1Q 20 //permite que hay comunicación entre las vlan
ip address 172.16.2.129 255.255.255.192 //Asignación de la dirección Ip y Mascara de Red
!
interface FastEthernet0/0.30 //Declaración de la subinterface de de video
encapsulation dot1Q 30//permite que haya comunicación entre las vlan
ip address 172.16.2.193 255.255.255.192 //Asignación de la dirección Ip y Mascara de Red
!
interface Serial0/3/1
bandwidth inherit 10000000 // Se utiliza para que las subinterfaces hereden el ancho de
banda de la interfaz principal
ip address 200.20.0.9 255.255.255.252 //asignación de Ip y mascara de red
clock rate 128000 //establece la velocidad de la señal del reloj que se generaran en las
interfaces seriales
!
router ospf 101 // Se entra en modo de configuración del protocolo OSPF , Iniciando un proceso
de enrutamiento definido.

log-adjacency-changes //Creación de un registro en un archivo log de los cambios de
adyacencias, esto asegura que asi que el intercambio de información no se pierda asi algún
dispositivo pierda conexión.

network 172.16.2.0 0.0.0.127 area 0 //Con este comando se configura un proceso de
enrutamiento OSPF y se asignan las redes a un mismo área, el área 0.

```

```
network 172.16.2.128 0.0.0.63 area 0
network 172.16.2.192 0.0.0.63 area 0
network 200.20.0.8 0.0.0.3 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server // no ip de servidor http seguro
!
control-plane// plano de control
!
rmon event 33333 log trap AutoQoS description "AutoQoS SNMP traps for Voice
Drops" owner AutoQoS rmon alarm 33333 cbQosCMDropBitRate.1059.1061 30
absolute rising-threshold 1 333 33 falling-threshold 0 owner AutoQoS mon alarm
33334 cbQosCMDropBitRate.1095.1097 30 absolute rising-threshold 1 33333
falling-threshold 0 owner AutoQoS
!
line con 0
line aux 0
line vty 0 4 //Asignación líneas vty
password cisco// Establecimiento del password
login
!
End// fin
```

## **b) Bogotá**

```
bogota#show running-config
Building configuration...
Current configuration : 2620 bytes
```

```
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname bogota //Asignación Nombre del Router  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 5 $1$SXkE$rXDMNAprAzKVF2uCwJHW..  
!  
no aaa new-model // no nuevo modelo  
!  
ip cef //Habilitado el CEF  
no ip dhcp use vrf connected //no ip dhcp vrf conectado  
!  
ip dhcp pool datos // Declaración de los DHCP para Datos esto se hace para tener una  
dirección de forma dinámica en el rango que se le ha establecido en la red  
  
network 172.16.3.0 255.255.255.12  
default-router 172.16.3.1// ip del router por defecto  
!  
ip dhcp pool video // Declaración de los DHCP para Video esto se hace para tener una  
dirección de forma dinámica en el rango que se le ha establecido en la red  
network 172.16.3.192 255.255.255.192  
default-router 172.16.3.193// ip del router por defecto  
!
```

```

ip dhcp pool voz // Declaración de los DHCP para Voz esto se hace para tener una dirección
de forma dinámica en el rango que se le ha establecido en la red
network 172.16.3.128 255.255.255.192
default-router 172.16.3.129// ip del router por defecto
option 150 ip 172.16.3.129 // permite que los teléfonos desde el router descarguen su imagen
vía tftp
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
voice-card 0 // tarjeta de voz 0
no dspfarm // no tarjeta dspfarm
!
class-map match-any AutoQoS-VoIP-RTP-Trust //Define Clase de tráfico
match ip dscp ef
class-map match-any AutoQoS-VoIP-Control-Trust
match ip dscp cs3
match ip dscp af31
!
policy-map AutoQoS-Policy-Trust //Define Políticas de entrada y salida para cada interface
class AutoQoS-VoIP-RTP-Trust
priority percent 70
class AutoQoS-VoIP-Control-Trust
bandwidth percent 5 //percentage de ancho de banda
class class-default
fair-queue
!
interface FastEthernet0/0.10 //Declaración de la subinterface para Datos
encapsulation dot1Q 10 // permite que haya comunicación entre las vlan
ip address 172.16.3.1 255.255.255.128 //Asignación de la dirección Ip y Mascara de Red

```

```

!
interface FastEthernet0/0.20 //Declaración de la subinterface para Voz
encapsulation dot1Q 20 // permite que haya comunicación entre las vlan
ip address 172.16.3.129 255.255.255.192//Asignación de la dirección Ip y Mascara de Red
!
interface FastEthernet0/0.30 //Declaración de la subinterface para Video
encapsulation dot1Q 30// permite que haya comunicación entre las vlan
ip address 172.16.3.193 255.255.255.192 //Asignación de la dirección Ip y Mascara de Red
!
interface Serial0/3/0
bandwidth 10000000 //se utiliza para asignar una velocidad a la interfaz del Router.
ip address 200.20.0.13 255.255.255.252 //Asignación de la dirección Ip y mascara de Red
auto qos voip trust //Declaración de AutoQoS (Método de Calidad de Servicio)
clock rate 128000 // establece la velocidad de la señal del reloj que se generaran en las
interfaces seriales
service-policy output AutoQoS-Policy-Trust // Habilitado servicio de Políticas AutoQos
!

interface Serial0/3/1
bandwidth 10000000 //se utiliza para asignar una velocidad a la interfaz del Router.
ip address 200.20.0.10 255.255.255.252 //Asignación de la dirección Ip y mascara de Red
auto qos voip trust//Asignación de AutoQoS (Método de Calidad de Servicio)
service-policy output AutoQoS-Policy-Trust //Habilitado servicio de Políticas AutoQos
!

router ospf 101 // Se entra en modo de configuración del protocolo OSPF , Iniciando un proceso
de enrutamiento definido.
log-adjacency-changes //Creación de un registro en un archivo log de los cambios de
adyacencias, esto asegura que asi que el intercambio de información no se pierda asi algún
dispositivo pierda conexión.
network 172.16.3.0 0.0.0.127 area 0 //Con este comando se configura un proceso de
enrutamiento OSPF y se asignan las redes a un mismo área, el área 0.

```

```

network 172.16.3.128 0.0.0.63 area 0
network 172.16.3.192 0.0.0.63 area 0
network 200.20.0.8 0.0.0.3 area 0
network 200.20.0.12 0.0.0.3 area 0
!
ip forward-protocol nd
!
ip http server
no ip http secure-server //no ip de servidor http seguro
!
control-plane // plano de control
!
rmon event 33333 log trap AutoQoS description "AutoQoS SNMP traps for Voice
Drop s" owner AutoQoS rmon alarm 33333 cbQosCMDropBitRate.1059.1061 30
absolute rising-threshold 1 333 33 falling-threshold 0 owner AutoQoS rmon alarm
33334 cbQosCMDropBitRate.1095.1097 30 absolute rising-threshold 1 333 33
falling-threshold 0 owner AutoQoS
!
line con 0
line aux 0
line vty 0 4 //Asignación líneas vty
password cisco // Establecimiento de password
login
!
End // fin

```

### c) Manizales

```

manizales# show running-config
Building configuration...

```

Current configuration : 3843 bytes

!

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname Manizales *//Asignación del nombre del Router*

!

boot-start-marker

boot-end-marker

!

enable secret 5 \$1\$MPoG\$QOhDli3ND7NWycR6wWYQ20// *Habilitado el password secreto*

!

no aaa new-model *//no nuevo modelo*

!

ip cef *//Habilitado CEF*

no ip dhcp use vrf connected*//no ip dhcp vrf conectado*

!

ip dhcp pool datos *// Declaración de los DHCP para Datos esto se hace para tener una dirección de forma dinámica en el rango que se le ha establecido en la red*

network 172.16.4.0 255.255.255.128

default-router 172.16.4.1*// ip router por defecto*

!

ip dhcp pool voz *// Declaración de los DHCP para Voz esto se hace para tener una dirección de forma dinámica en el rango que se le ha establecido en la red*

network 172.16.4.128 255.255.255.192

default-router 172.16.4.129*// ip router por defecto*

option 150 ip 172.16.4.129 *// permite a los teléfonos descargar su imagen del router vía tftp*



```

!
ip dhcp pool video// Declaración de los DHCP para Video esto se hace para tener una dirección
de forma dinámica en el rango que se le ha establecido en la red
network 172.16.4.192 255.255.255.192
default-router 172.16.4.193// ip router por defecto
!
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
voice-card 0 // tarjeta de voz 0
no dspfarm // no tarjeta dspfarm
!
class-map match-any AutoQoS-VoIP-RTP-Trust //Define la clase de Tráfico
match ip dscp ef
class-map match-any AutoQoS-VoIP-Control-Trust
match ip dscp cs3
match ip dscp af31
!
policy-map AutoQoS-Policy-Trust//Define las políticas de entrada y salida para las interfaces
class AutoQoS-VoIP-RTP-Trust
priority percent 70// porcentaje de prioridad
class AutoQoS-VoIP-Control-Trust
bandwidth percent 5// porcentaje de ancho de banda
class class-default
fair-queue
!
interface Loopback0 //Declaración de Interfaz loopback permite que si un a interfaz se caiga
siga funcionando OSPF
ip address 172.16.1.1 255.255.255.255 // Declaración de la dirección ip y mascara de red

```

```

!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
auto qos voip trust // Habilita AutoQoS (Método de Calidad de servicio)
service-policy output AutoQoS-Policy-Trust
!
interface FastEthernet0/0.40 // Declaración de Subinterface para Datos
encapsulation dot1Q 40 // permite que haya comunicación entre las vlan
ip address 172.16.4.1 255.255.255.128 //Asignación de Dirección Ip y Mascara de Red
!
interface FastEthernet0/0.50//Declaración de Subinterface para voz
encapsulation dot1Q 50 // permite que haya comunicación entre las vlan
ip address 172.16.4.129 255.255.255.192 //Asignación de Dirección Ip y Mascara de Red
!
interface FastEthernet0/0.60 //Declaración de Subinterface para video
encapsulation dot1Q 60 // permite que haya comunicación entre las vlan
ip address 172.16.4.193 255.255.255.192//Asignación de Dirección Ip y Mascara de Red
!
interface Serial0/3/0
bandwidth 10000000 //se utiliza para asignar la velocidad a la interfaz del router
ip address 200.20.0.17 255.255.255.252 //Asignación de la dirección Ip y mascara de Red
auto qos voip trust //configuración de AutoQoS (Método de Calidad de Servicio)
clock rate 128000 // establece la velocidad de la señal del reloj que se generaran en las
interfaces seriales
service-policy output AutoQoS-Policy-Trust //Habilitado servicio de Políticas AutoQoS
!
interface Serial0/3/1

```

```

bandwidth 10000000 //Asignación Ancho de Banda
ip address 200.20.0.14 255.255.255.252 //Asignación de la dirección Ip y mascara de Red
auto qos voip trust //Asignación de AutoQoS (Método de Calidad de Servicio)
service-policy output AutoQoS-Policy-Trust //Habilitado servicio de Políticas AutoQoS
!
router ospf 101 // Se entra en modo de configuración del protocolo OSPF , Iniciando un proceso
de enrutamiento definido.
log-adjacency-changes //Creación de un registro en un archivo log de los cambios de
adyacencias, esto asegura que así que el intercambio de información no se pierda así algún
dispositivo pierda conexión.
network 172.16.1.1 0.0.0.0 área 0 //Con este comando se configura un proceso de
enrutamiento OSPF y se asignan las redes a un mismo área, el área 0.
network 172.16.4.0 0.0.0.127 area 0
network 172.16.4.128 0.0.0.63 area 0
network 172.16.4.192 0.0.0.63 area 0
network 200.20.0.12 0.0.0.3 area 0
network 200.20.0.16 0.0.0.3 area 0
!
ip forward-protocol nd
!
ip http server
no ip http secure-server //no ip de servidor http seguro
!
control-plane// plano de control
!
rmon event 33333 log trap AutoQoS description "AutoQoS SNMP traps for Voice
Drops" owner AutoQoS rmon alarm 33333 cbQosCMDropBitRate.1059.1061 30
absolute rising-threshold 1333 33 falling-threshold 0 owner AutoQoS rmon alarm
33334 cbQosCMDropBitRate.1095.1097 30 absolute rising-threshold 1 333 33
falling-threshold 0 owner AutoQoS

```

```
!  
telephony-service //Habilitado el servicio de Telefonía  
max-ephones 20 // Declara el número Máximo de Teléfonos  
max-dn 20// máximo número de directorio  
ip source-address 172.16.1.1 port 2000  
system message TECNOLOGICA DE BOLIVAR //Asignación del mensaje en el sistema es  
opcional  
network-locale ES// Red local  
max-conferences 8 gain -6 //Asignación de número máximo de conferencias puede ser el que desee  
directory last-name-first // Asignación de número y nombre en el Directorio  
directory entry 1 6531641 name SEDE MANIZALES// se asignan los números y nombres que  
usted desee  
directory entry 2 6531642 name SEDE CARTAGENA  
directory entry 3 6531643 name SEDE BOGOTA  
directory entry 4 6531644 name SEDE PEREIRA  
!
```

```
ephone-dn 1 //Configuración del teléfono 1  
number 6531641// número del teléfono  
description SEDE MANIZALES//Descripción del teléfono  
name SEDE MANIZALES //nombre del teléfono
```

```
!  
ephone-dn 2 //Configuración del teléfono 2  
number 6531642// número del teléfono  
description SEDE CARTAGENA//Descripción del teléfono  
name SEDE CARTAGENA// nombre del teléfono
```

```
!  
ephone-dn 3 //Configuración del teléfono 3  
number 6531643// número del teléfono  
description SEDE BOGOTA//Descripción del teléfono
```

```
name SEDE BOGOTA//nombre del teléfono
!
ephone-dn 4 //Configuración del teléfono 4
number 6531644// número del teléfono
description SEDE PEREIRA//Descripción del teléfono
name SEDE PEREIRA//nombre del teléfono
!
ephone 1 //Configuración del teléfono 1
mac-address 0025.648E.C074// MAC del teléfono
button 1:1 // permite asignar solo un número de teléfono
!
ephone 2 //Configuración del teléfono 2
mac-address 0025.648F.7D87/ MAC del teléfono
button 1:2// permite asignar solo un número de teléfono
!
ephone 3 //Configuración del teléfono 3
mac-address 0025.648F.7E56 MAC del teléfono
button 1:3// permite asignar solo un número de teléfono
!
ephone 4//Configuración del teléfono 4
mac-address 0027.136E.B6E1 MAC del teléfono
button 1:4// permite asignar solo un número de teléfono
!
line con 0
line aux 0
line vty 0 4 //Asignación líneas vty para la asignación del password para sesión de telnet
password cisco // Establecimiento del password
login
!
```

End// fin

**d) Pereira**

Building configuration...

Current configuration : 2334 bytes

!

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname Pereira *//Asignación nombre al Router*

!

boot-start-marker

boot-end-marker

!

enable secret 5 \$1\$iT30\$OPzVd9TyB5X1tpx0HqW.n1 *//habilitado password secreto*

!

no aaa new-model *// no nuevo modelo*

!

ip cef *//Habilitado CEF*

no ip dhcp use vrf connected *//no ip dhcp vrf conectado*

!

ip dhcp pool voz *// Declaración de los DHCP para Voz esto se hace para tener una dirección de forma dinámica en el rango que se le ha establecido en la red*

network 172.16.5.128 255.255.255.192

default-router 172.16.5.129 *//ip del router por defecto*

```

option 150 ip 172.16.5.129 //permite que los teléfonos descarguen su imagen del router vía
ftp
!
ip dhcp pool datos // Declaración de los DHCP para Datos esto se hace para tener una
dirección de forma dinámica en el rango que se le ha establecido en la red
network 172.16.5.0 255.255.255.128
default-router 172.16.5.1//ip del router por defecto
!
ip dhcp pool video // Declaración de los DHCP para Video esto se hace para tener una
dirección de forma dinámica en el rango que se le ha establecido en la red
network 172.16.5.192 255.255.255.192
default-router 172.16.5.193 //ip del router por defecto
!
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
voice-card 0// tarjeta de voz 0
no dspfarm // no tarjeta dspfarm
!
class-map match-any AutoQoS-VoIP-RTP-Trust // Define la clase de Tráfico
match ip dscp ef
class-map match-any AutoQoS-VoIP-Control-Trust
match ip dscp cs3
match ip dscp af31
!
policy-map AutoQoS-Policy-Trust // Define las políticas de entrada y salida para las interfaces
class AutoQoS-VoIP-RTP-Trust
priority percent 70 // porcentaje de prioridad
class AutoQoS-VoIP-Control-Trust
bandwidth percent 5// Porcentaje de ancho de banda

```

```

class class-default
fair-queue
!
interface FastEthernet0/0.40 //Declaración de subinterface para datos.
encapsulation dot1Q 40// permite la comunicación entre vlan
ip address 172.16.5.1 255.255.255.128 //Asignación de Dirección Ip y Mascara de Red.
!
interface FastEthernet0/0.50 //Declaración de subinterface para voz.
encapsulation dot1Q 50 // permite la comunicación entre vlan
ip address 172.16.5.129 255.255.255.192 //Asignación de Dirección Ip y Mascara de Red.
!
interface FastEthernet0/0.60 //Declaración de subinterface para video
encapsulation dot1Q 60 // permite la comunicación entre vlan
ip address 172.16.5.193 255.255.255.192 //Asignación de Dirección Ip y Mascara de Red
!
interface Serial0/3/0
bandwidth 10000000 // Asignación de Ancho de Banda
ip address 200.20.0.18 255.255.255.252 //Asignación de la dirección Ip y mascara de Red
auto qos voip trust //asignación AutoQoS (Método de calidad de servicios)
service-policy output AutoQoS-Policy-Trust //Habilitado servicio de Políticas AutoQoS
!
router ospf 101 // Se entra en modo de configuración del protocolo OSPF , Iniciando un proceso
de enrutamiento definido.
log-adjacency-changes //Creación de un registro en un archivo log de los cambios de
adyacencias, esto asegura que asi que el intercambio de información no se pierda asi algún
dispositivo pierda conexión.
network 172.16.5.0 0.0.0.127 area 0 //Con este comando se configura un proceso de
enrutamiento OSPF y se asignan las redes a un mismo área, el área 0.
network 172.16.5.128 0.0.0.63 area 0
network 172.16.5.192 0.0.0.63 area 0

```



```

network 200.20.0.16 0.0.0.3 area 0
!
ip forward-protocol nd

ip http server
no ip http secure-server //no ip del servidor http seguro
!
control-plane // plano de control
rmon event 33333 log trap AutoQoS description "AutoQoS SNMP traps for Voice
Drops" owner AutoQoS rmon alarm 33333 cbQosCMDropBitRate.1059.1061 30
absolute rising-threshold 1 333 33 falling-threshold 0 owner AutoQoS
line con 0 //Asignacion líneas vty
line aux 0
line vty 0 4 //Asignacion líneas vty para establecer password para sesión de telnet
password cisco//establecimiento de password
login
end //fin

```

✓ **Configuración de los Switchs con implementación de métodos de calidad de servicios(QoS)**

Se tuvo que utilizar 2 switchs para la implementación de las prácticas ya que en el momento de realizarlas no contábamos con la cantidad que se requería (4), los switch se segmentaron para así poder utilizar un switch para dos ciudades para esta segmentación utilizamos VLAN

**a) Switch de la ciudad de Bogotá y Manizales**

Current configuration : 4924 bytes  
!

```

version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption //no servicio de encriptación de password
!
hostname bog-cartagena//Asignación del nombre al switch
!
no aaa new-model // no existe nuevo modelo
ip subnet-zero
!
//Se configuran una serie de servicios basados en hardware para algunas series de switches Cisco, se usa para la identificación de las características del tráfico y para brindar QoS a través del uso de colas y se asignan los valores DSCP que corresponden a cada cola de ingreso.
mls qos map policed-dscp 24 26 46 to 0
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0
mls qos srr-queue input cos-map queue 2 threshold 1 2
mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3 3 5
mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 32
mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15

```

```

mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 138 138 92 138
mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
mls qos queue-set output 1 buffers 10 10 26 54
mls qos queue-set output 2 buffers 16 6 17 61
mls qos
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
class-map match-all AutoQoS-VoIP-RTP-Trust // Define la clase de tráfico
match ip dscp ef // Definición previa, en base al DSCP que es como vendrán todos los
paquetes marcados
class-map match-all AutoQoS-VoIP-Control-Trust
match ip dscp cs3 af31// Definición previa, en base al DSCP que es como vendrán todos
los paquetes marcados
!
!
policy-map AutoQoS-Police-SoftPhone //Definición de las políticas de entrada y salida en
la interfaz de comunicación
class AutoQoS-VoIP-RTP-Trust
set dscp ef
police 1000000 8000 exceed-action policed-dscp-transmit
class AutoQoS-VoIP-Control-Trust
set dscp cs3
police 1000000 8000 exceed-action policed-dscp-transmit
!
interface FastEthernet0/1
switchport mode trunk // modo de acceso trunk
!

interface FastEthernet0/3
switchport access vlan 10// acceso vlan 10
switchport voice vlan 20// Puerto de voz vlan 20
service-policy input AutoQoS-Police-SoftPhone //servicio de políticas AutoQoS Softphone
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 10 0 0 0
auto qos voip cisco-softphone //Habilita AutoQoS cuando se utiliza el Softphone de cisco
spanning-tree portfast

```

```

!
interface FastEthernet0/13// interface fastethernet 0/13
switchport mode trunk// modo trunk indica que por esa puerta pasarán diferente vlan que se permitan
spanning-tree portfast //Se deshabilita el SPT(Shortest Path Tree), Cuando ocurra un loop este no se detecta
!

interface FastEthernet0/15// interface fastethernet 0/15
switchport access vlan 40//Acceso a vlan 40
switchport voice vlan 50 //Puerto de voz vlan 50
service-policy input AutoQoS-Police-SoftPhone //servicio de políticas AutoQoS- políticas softphone
srr-queue bandwidth share 10 10 60 20
srr-queue bandwidth shape 10 0 0 0
auto qos voip cisco-softphone//Habilita AutoQoS cuando se utiliza el Softphone de cisco
spanning-tree portfast
!
interface Vlan1
no ip address
no ip route-cache
!
ip http server
!
control-plane // plano de control
!
line con 0
line vty 0 4
no login // no asignado password
!
end

```

## **b) Switch Cartagena y Pereira**

Current configuration : 5004 bytes

```

!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption// no servicio de encriptación de password

!
hostname crtg-pereira //Asignación del nombre al switch
!
no aaa new-model // no existe nuevo modelo

ip subnet-zero

```

!

*//Se configuran una serie de servicios basados en hardware para algunas series de switches Cisco, se usa para la identificación de las características del tráfico y para brindar QoS a través del uso de colas y se asignan los valores DSCP que corresponden a cada cola de ingreso.*

```
mls qos map policed-dscp 24 26 46 to 0
mls qos map cos-dscp 0 8 16 26 32 46 48 56
mls qos srr-queue input bandwidth 90 10
mls qos srr-queue input threshold 1 8 16
mls qos srr-queue input threshold 2 34 66
mls qos srr-queue input buffers 67 33
mls qos srr-queue input cos-map queue 1 threshold 2 1
mls qos srr-queue input cos-map queue 1 threshold 3 0
mls qos srr-queue input cos-map queue 2 threshold 1 2
mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7
mls qos srr-queue input cos-map queue 2 threshold 3 3 5
mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue input dscp-map queue 1 threshold 3 32
mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48
mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56
mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output cos-map queue 1 threshold 3 5
mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 2 4
mls qos srr-queue output cos-map queue 4 threshold 2 1
mls qos srr-queue output cos-map queue 4 threshold 3 0
mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47
mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15
mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7
mls qos queue-set output 1 threshold 1 138 138 92 138
mls qos queue-set output 1 threshold 2 138 138 92 400
mls qos queue-set output 1 threshold 3 36 77 100 318
mls qos queue-set output 1 threshold 4 20 50 67 400
mls qos queue-set output 2 threshold 1 149 149 100 149
mls qos queue-set output 2 threshold 2 118 118 100 235
mls qos queue-set output 2 threshold 3 41 68 100 272
mls qos queue-set output 2 threshold 4 42 72 100 242
mls qos queue-set output 1 buffers 10 10 26 54
```

```

mls qos queue-set output 2 buffers 16 6 17 61
mls qos
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
class-map match-all AutoQoS-VoIP-RTP-Trust // Define la clase de tráfico
  match ip dscp ef // Definición previa, en base al DSCP que es como vendrán todos los
  paquetes marcados
class-map match-all AutoQoS-VoIP-Control-Trust
  match ip dscp cs3 af31// Definición previa, en base al DSCP que es como vendrán todos
  los paquetes marcados
!
policy-map AutoQoS-Police-SoftPhone //Definición de las políticas de entrada y salida en
  la interfaz de comunicación
class AutoQoS-VoIP-RTP-Trust
  set dscp ef
  police 1000000 8000 exceed-action policed-dscp-transmit
class AutoQoS-VoIP-Control-Trust
  set dscp cs3
  police 1000000 8000 exceed-action policed-dscp-transmit
!
interface FastEthernet0/1
  switchport mode trunk // modo de acceso trunk
!
interface FastEthernet0/2
  switchport access vlan 10 // acceso vlan 10
  switchport trunk native vlan 10
!
interface FastEthernet0/3
  switchport access vlan 10 // acceso vlan 10
  switchport voice vlan 20 //Puerto de voz vlan 20
  service-policy input AutoQoS-Police-SoftPhone //servicio de políticas AutoQoS- políticas
  softphone
  srr-queue bandwidth share 10 10 60 20
  srr-queue bandwidth shape 10 0 0 0
  auto qos voip cisco-softphone //Habilita AutoQoS cuando se utiliza el Softphone de cisco
  spanning-tree portfast
!
interface FastEthernet0/5
  switchport access vlan 20 //acceso a vlan 20
!
interface FastEthernet0/7
  switchport access vlan 10 //acceso a vlan 10

```

```

!
interface FastEthernet0/13
 switchport mode trunk // modo de acceso trunk
!
interface FastEthernet0/15 // interface fastethernet 0/15
 switchport access vlan 40 // Acceso a vlan 40
 switchport voice vlan 50 // Puerto de voz vlan 50
 service-policy input AutoQoS-Police-SoftPhone // servicio de políticas AutoQoS- políticas
 softphone
 srr-queue bandwidth share 10 10 60 20
 srr-queue bandwidth shape 10 0 0 0
 auto qos voip cisco-softphone
 spanning-tree portfast
!
interface FastEthernet0/17
 switchport access vlan 40 // Acceso vlan 50
 switchport voice vlan 50 // Puerto de voz vlan 50
 spanning-tree portfast
!
interface Vlan1
 no ip address // no ip address
 no ip route-cache // no ip route-cache (este commando deshabilita cualquier método para
 el reenvío de paquetes IP )
!
ip http server
!
control-plane // plano de control
!
!
line con 0
line vty 0 4
 no login
 length 0
line vty 5 15
 no login // no asignado password
!
end

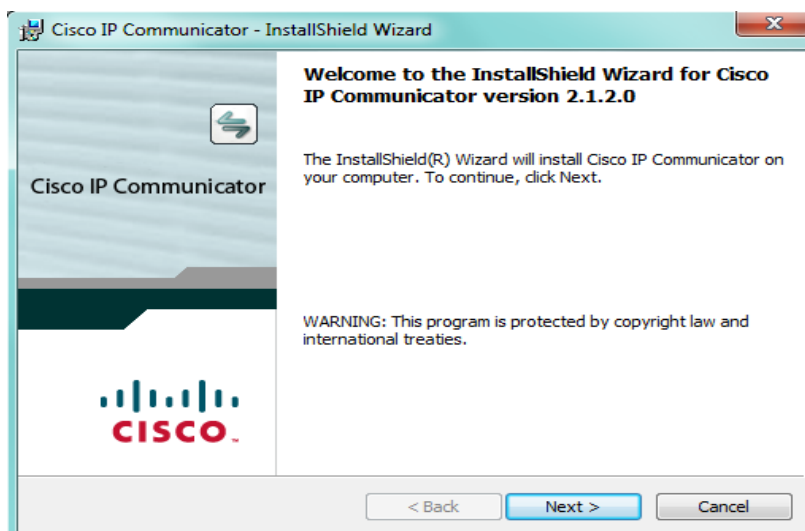
```

### ✓ Instalación de Softphone Cisco IP Communicator

“Cisco IP Communicator es una aplicación de escritorio que convierte su equipo en un teléfono IP de Cisco con todas las funciones, con el que podrá realizar, recibir o gestionar llamadas. Si instala Cisco IP Communicator en un computador

portátil, puede utilizar también todos los servicios del teléfono y su configuración, desde cualquier ubicación en la que pueda conectarse a la red de su empresa”<sup>41</sup>.

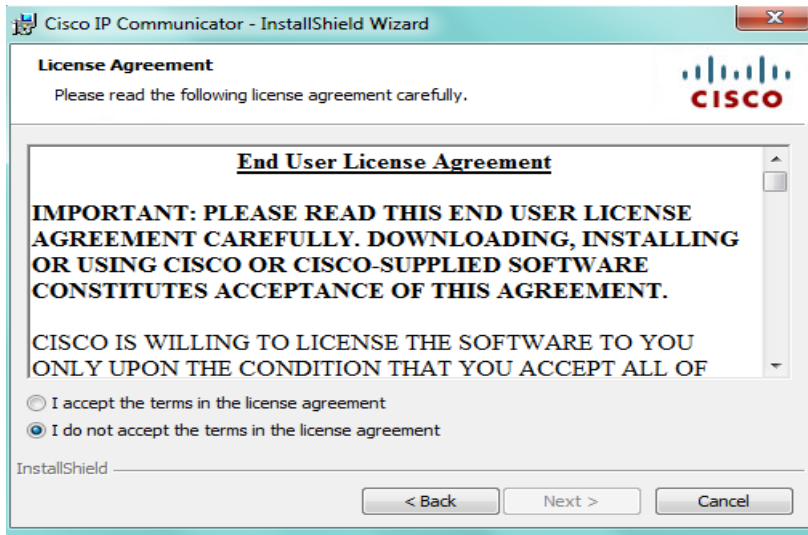
1. Se abrió el CiscoIPCommunicatorSetup.exe, apareció el asistente InstallShield y comenzó la preparación para la instalación.
2. Se hizo clic en Next para iniciar el asistente InstallShield.



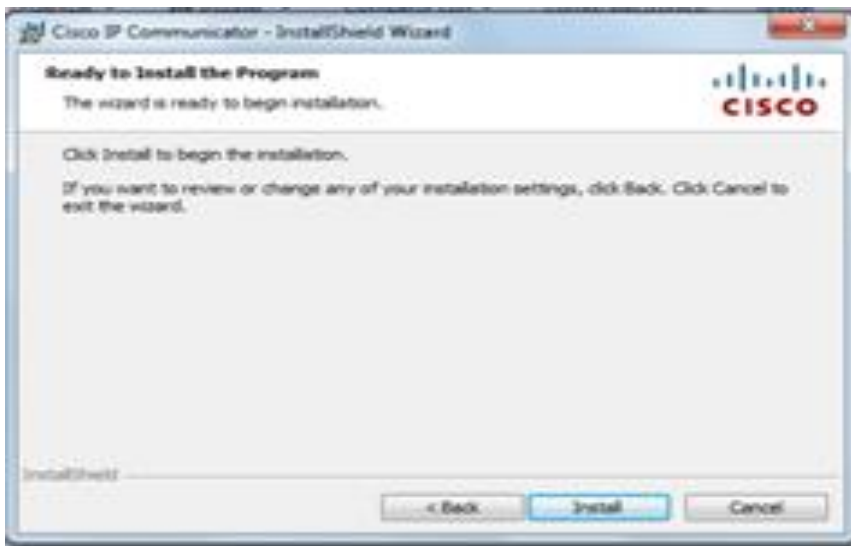
3. Cuando apareció el acuerdo de licencia, se leyó y se hizo clic en “Acepto” y en botón next “Siguiente”.

<sup>41</sup> [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cipc/2\\_0/spanish/user/guide/ipcF1esp.pdf](http://www.cisco.com/en/US/docs/voice_ip_comm/cipc/2_0/spanish/user/guide/ipcF1esp.pdf)





4. En la ventana listo para instalar el programa, se hizo clic en Instalar.



5. Se hizo clic en Finalizar.



Seguidamente se configura el la voz y el sonido



Se le dio click en Next "siguiente"



Se escogieron los dispositivos por los cuales se iba a reproducir el sonido y el micrófono y se le dio click en Next “siguiente”.



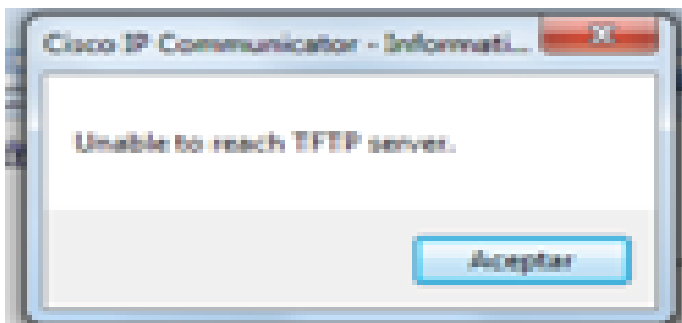
Se hizo una prueba para ver el funcionamiento de los altavoces y luego se le dio click en Next “siguiente”.



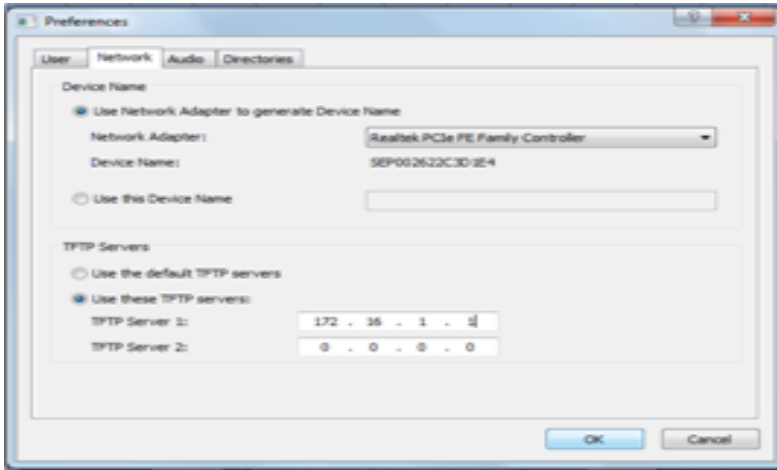
Se probó el micrófono para ver su funcionamiento y se le dio click en el botón Next “siguiente”.



Por último se le dio click en el botón finish



Seguidamente el Softphone informó que el TFTP server no estaba habilitado, se le dio click en el aceptar.



Se le configuró la dirección IP del servidor TFTP y se le dio click en el botón OK, si no se hubiese configurado el sonido, el micrófono y el servidor TFTP enseguida se terminó de instalar el Softphone, cuando se abriera el software se tendría que configurar para que este pudiese funcionar y esto se hace haciéndole click derecho encima del Softphone y escogiendo la opción Preferences en la pestaña Network se escribe la dirección ip del servidor TFTP y se le da click en el botón OK, luego en la pestaña de audio se configura el sonido y el audio y se le dá click en el OK.

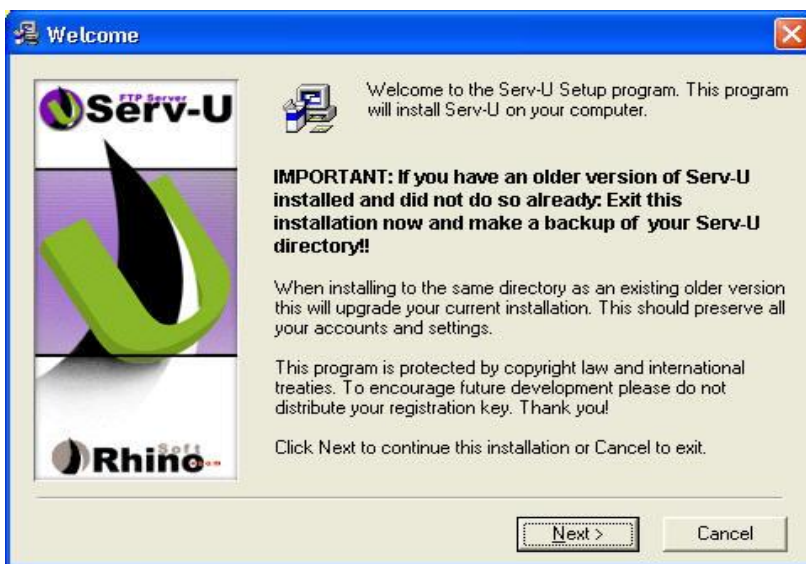
#### ✓ **Instalación del Servidor Ftp Serv-U**

El servidor FTP SERV-U permite gestionar alojamientos FTP para miles de usuarios, y fue utilizado en este proyecto por ser una herramienta de fácil uso, pero a la vez muy potente y segura.

Pasos para la instalación:

1. Se descargó de su Web oficial [www.serv-u.com](http://www.serv-u.com)
2. Se ejecutó el Serv-USetup.exe

3. Primero el software avisó de que si tenemos un Serv-u anterior instalado que se haga copia del serv-u directorio para conservar las configuraciones.
  4. Se siguió los pasos habituales al instalar un programa de Windows. Se le dió next hasta que ya esté instalado y él se ejecuta automáticamente.
- Clic en Next para continuar



- Clic en Next para continuar



- Clic en Next para continuar



- Clic en Next para continuar



- Clic en Next para continuar



- Clic en Next para continuar





- Clic para Finalizar



### ✓ Instalación de la herramienta de monitoreo de Redes “Wireshark”

**Wireshark** Es un analizador de protocolos basado en las librerías pcap utilizado comúnmente como herramienta de diagnóstico de redes y de desarrollo de aplicaciones de red. Entre sus cualidades nos encontramos con una enorme versatilidad que le lleva a soportar más de 480 protocolos distintos, además de la posibilidad de trabajar tanto con datos capturados desde una red durante una sesión como con paquetes previamente capturados que hayan sido almacenados en el disco duro, para que funcione bien necesita tener instalado el paquete de librerías Wincap.

### *Funcionalidad de Wireshark*

Cuando se abrió el programa, este mostró una interfaz de usuario con varias funciones:

1. **File:** contiene las funciones para manipular archivos y para cerrar la aplicación Wireshark.
2. **Edit:** Este se puede aplicar funciones a los paquetes, por ejemplo, buscar un paquete específico, aplicar una marca al paquete y configurar la interfaz de usuario.
3. **View:** Permite configurar el despliegue del paquete capturado.
4. **Capture:** Para iniciar y detener la captura de paquetes.
5. **Analyze:** Desde analyze podemos manipular los filtros, habilitar o deshabilitar protocolos, flujos de paquetes, etc.
6. **Statistics:** podemos definir u obtener las estadísticas del tráfico capturado.
7. **Help:** menú de ayuda.

Para la instalación de este software se siguió los siguientes pasos:

1. Se Bajó programa de la web oficial: <http://www.wireshark.org/download.html>
2. se ejecutó el archivo wireshark-setup-1.0.0.exe, las librerías necesarias como WinPcap están incluidas en el instalador.



3. Se le dio click en Next y se desplegó la siguiente ventana para la selección de los componentes que se iban a instalar.



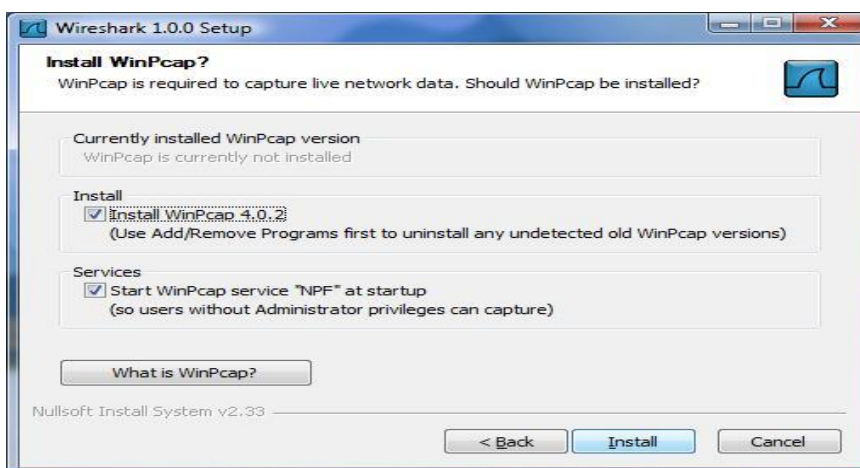
Para esta instalación se seleccionó los siguientes:

- Wireshark, GUI del analizador de protocolos.
- TShark, línea de comando del analizador de protocolos.
- Plugins/Extensions, especificar plugins y extensiones para TShark y Wireshark en este punto debió seleccionar todos los ítems listados.
- Tool, ofrece herramientas adicionales aplicar a los archivos que contienen los paquetes para su análisis se seleccionó todas las ofrecidas durante la instalación.

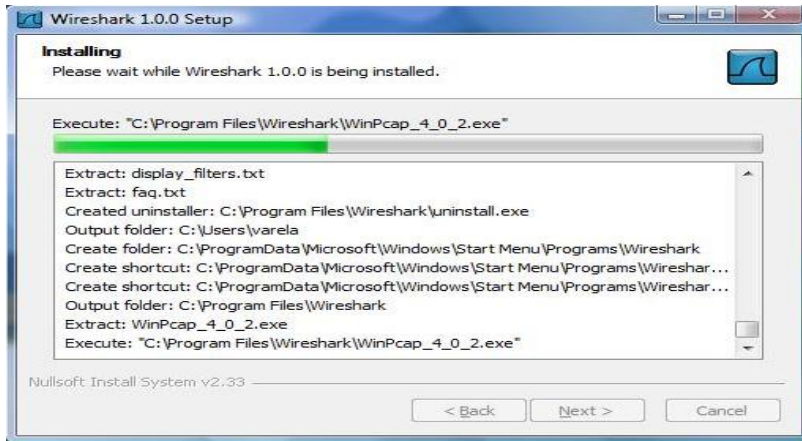
4. La siguiente pantalla permitió seleccionar si se desea crear un acceso directo, crear un menú de inicio y visualizar el icono en la barra de tareas.



8. Se seleccionó el directorio donde se instalará la aplicación, en este punto se acepta el indicado por defecto en el instalador, Se presiona la opción Install para iniciar el proceso de instalación.



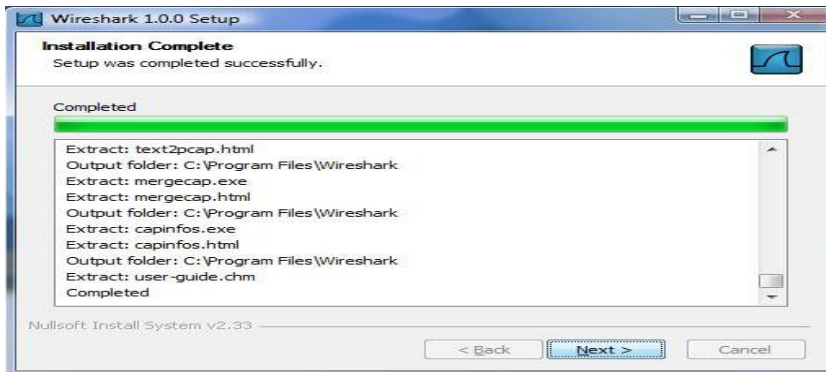
Luego se empezó a instalar



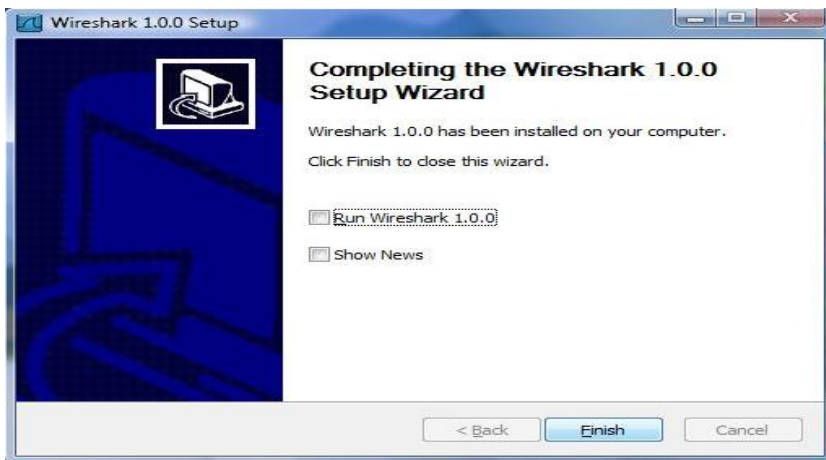
9. Como se mencionó anteriormente el instalador de WireShark para Windows permite hacer la instalación de las librerías, plugins, servicios. Para el caso de WinPcap se interrumpe la instalación en el punto que muestra la pantalla arriba e inicia el asistente para la instalación de WinPcap. Se debe seleccionar la opción next hasta finalizar la instalación.



Luego se dio click en next



10. Finalmente salió en pantalla que la instalación a finalizado.



### Instalación Windows Media Encoder

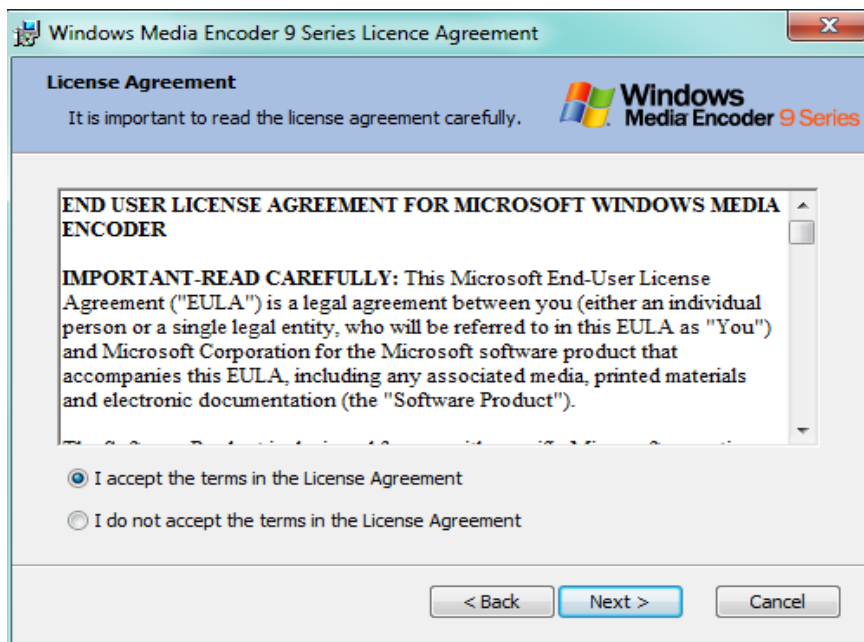
Windows media Encoder es una aplicación desarrollada por Microsoft para la captura de vídeos desde el dispositivo adecuado y la conversión entre formatos.

Para la instalación se siguió los siguientes pasos:

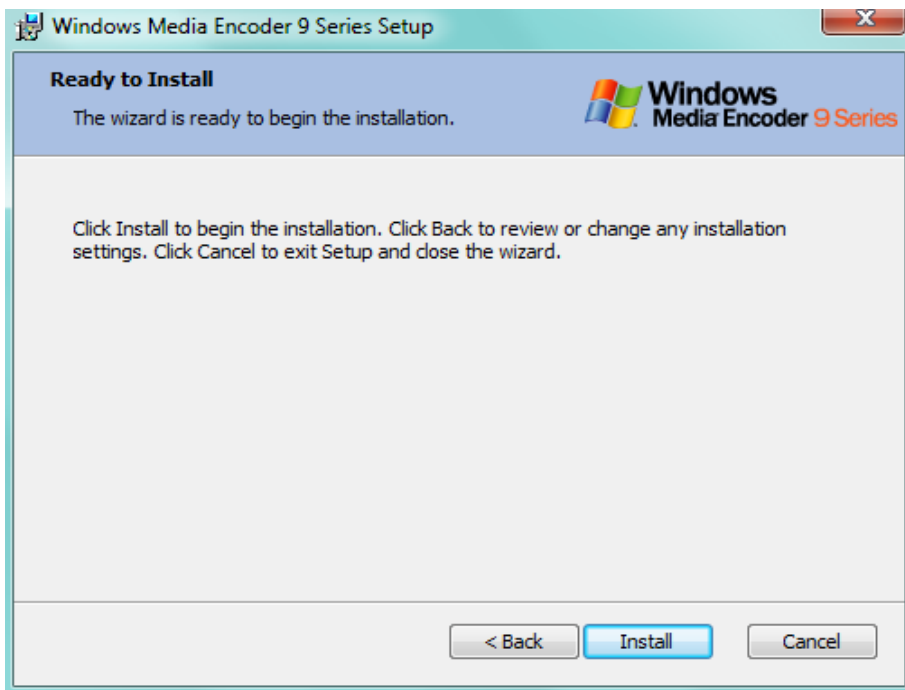
- Se hizo doble click en el instalador, aparece una pantalla inicial de instalación, se hace Click en Next.



- Aparece la relación de términos de Contrato de Licencia del codificador, se Seleccionó la opción “Acepto los términos del Contrato de Licencia” y dio click en Next.



- Seguidamente pidió la confirmación de la Instalación del programa y se le dio click en Install.



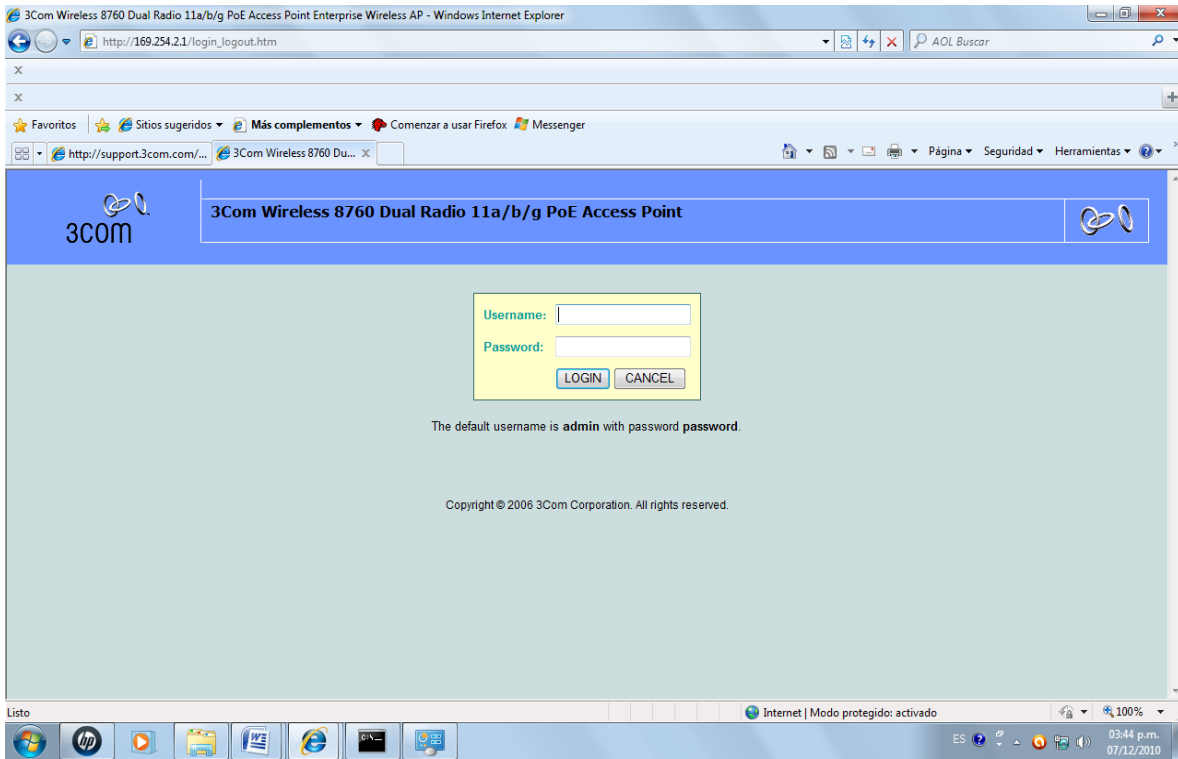
- Cuando se terminó la instalación del Windows Media Encoder, salió una última pantalla en donde indicaba que había completado la instalación y se dio click en botón Finish.



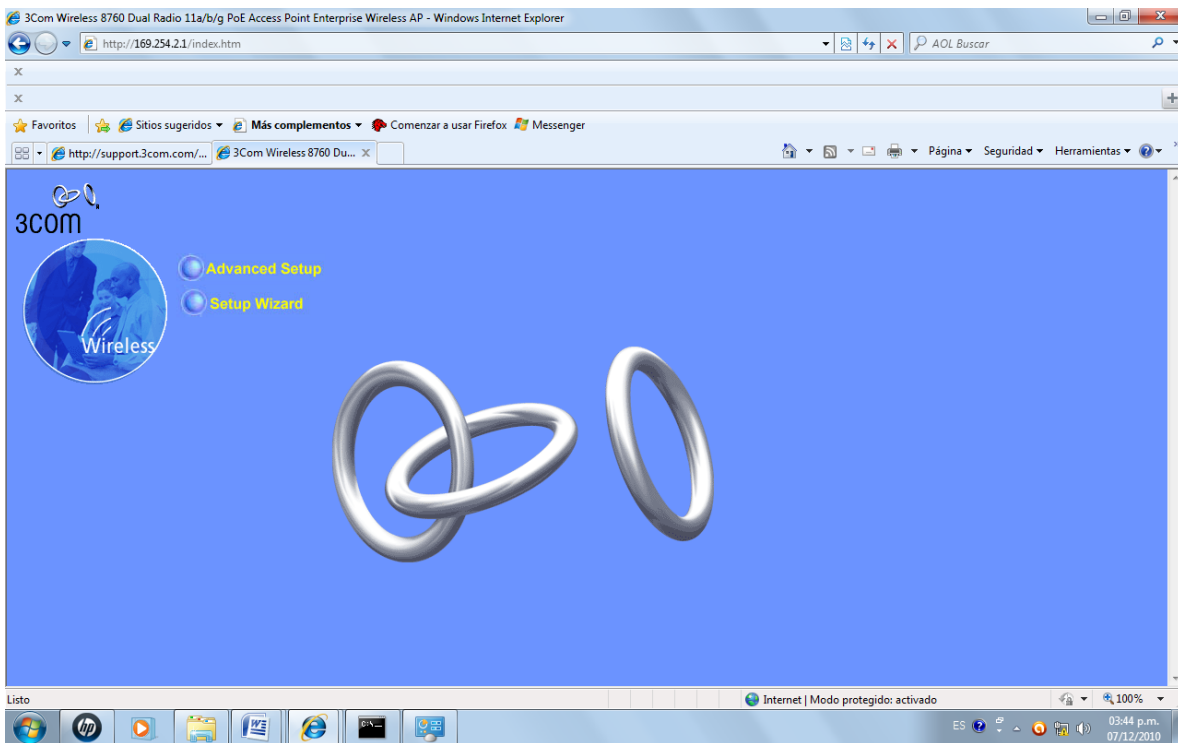


#### ✓ **Configuración del Access Point 3com 8760**

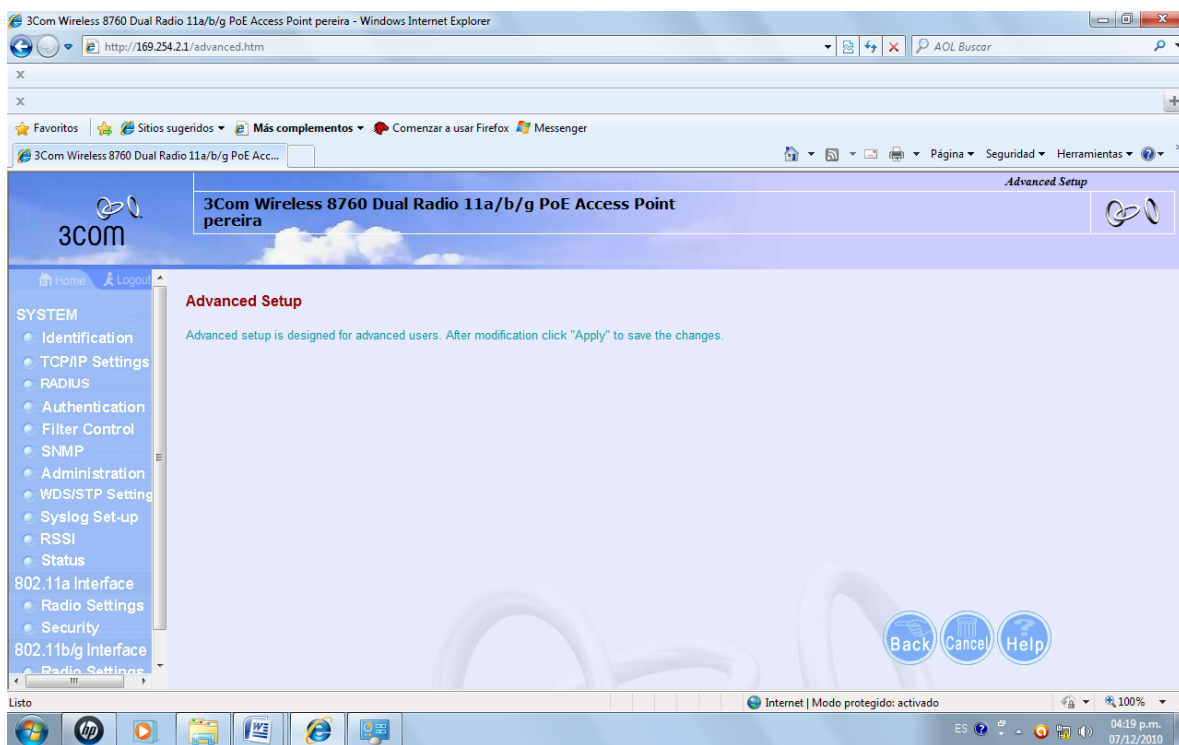
El Access point 3com 8760 trae un cargador, dos antenas, un cable power over Ethernet (corriente sobre ethernet), un CD con un software, en este software venía la dirección ip (169.254.2.1) por defecto del Access point, la cual se utilizó para su configuración; Para Configurarlos se debió conectar el cargador que trae, las antenas, se abrió el browser y en la barra de direcciones se escribió la dirección IP del access point y se abrió una interfaz de modo gráfico como se muestra en la siguiente figura, se escribió en usuario: admin y en el password: password en este caso porque estos eran los que tenía por defecto el Access point.



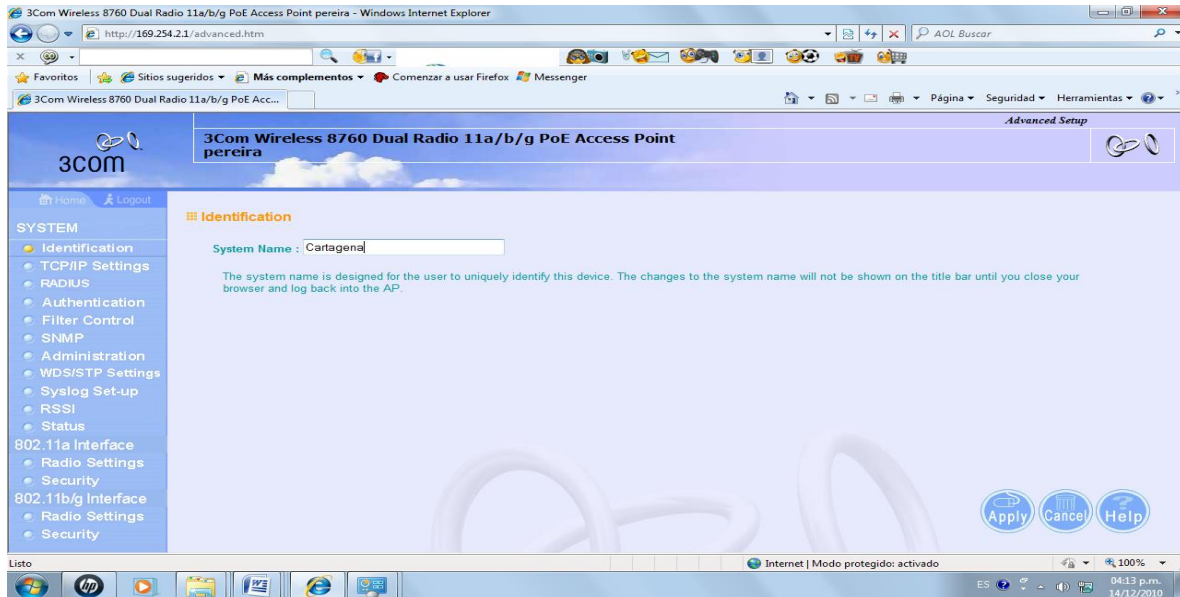
Luego se dio click en el botón login



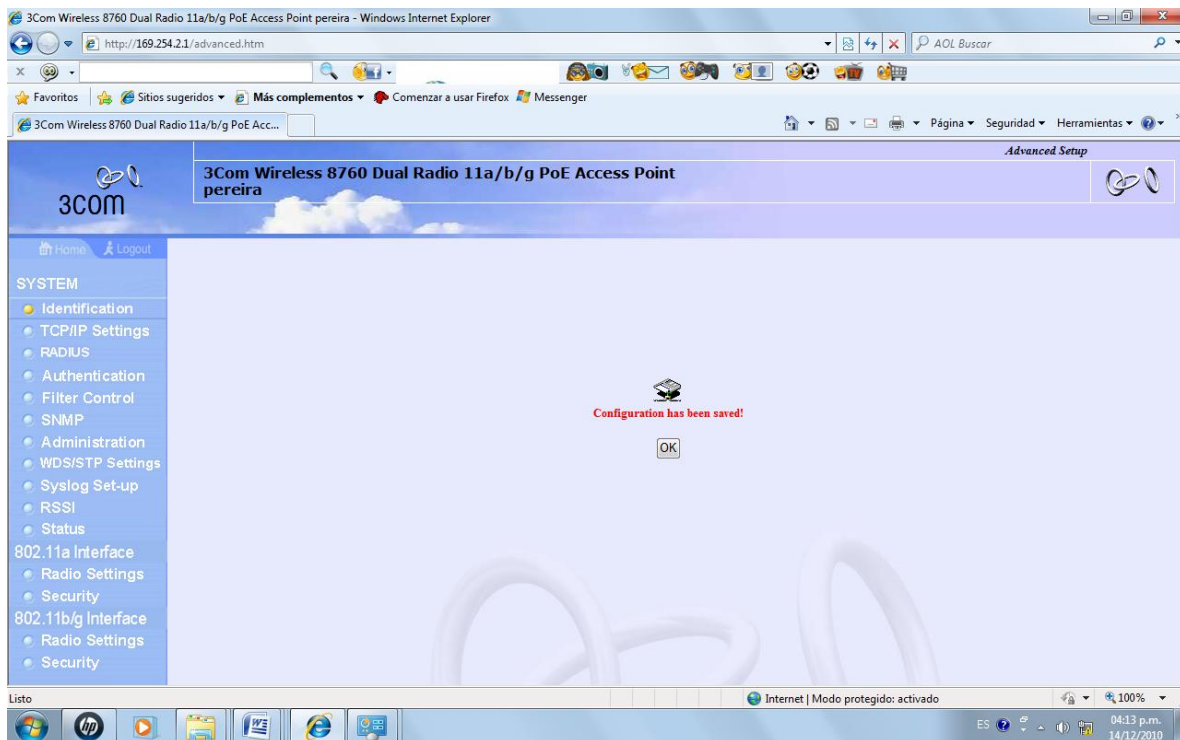
Después se escogió el ítem advanced setup(configuración avanzada) como se muestra en la siguiente figura



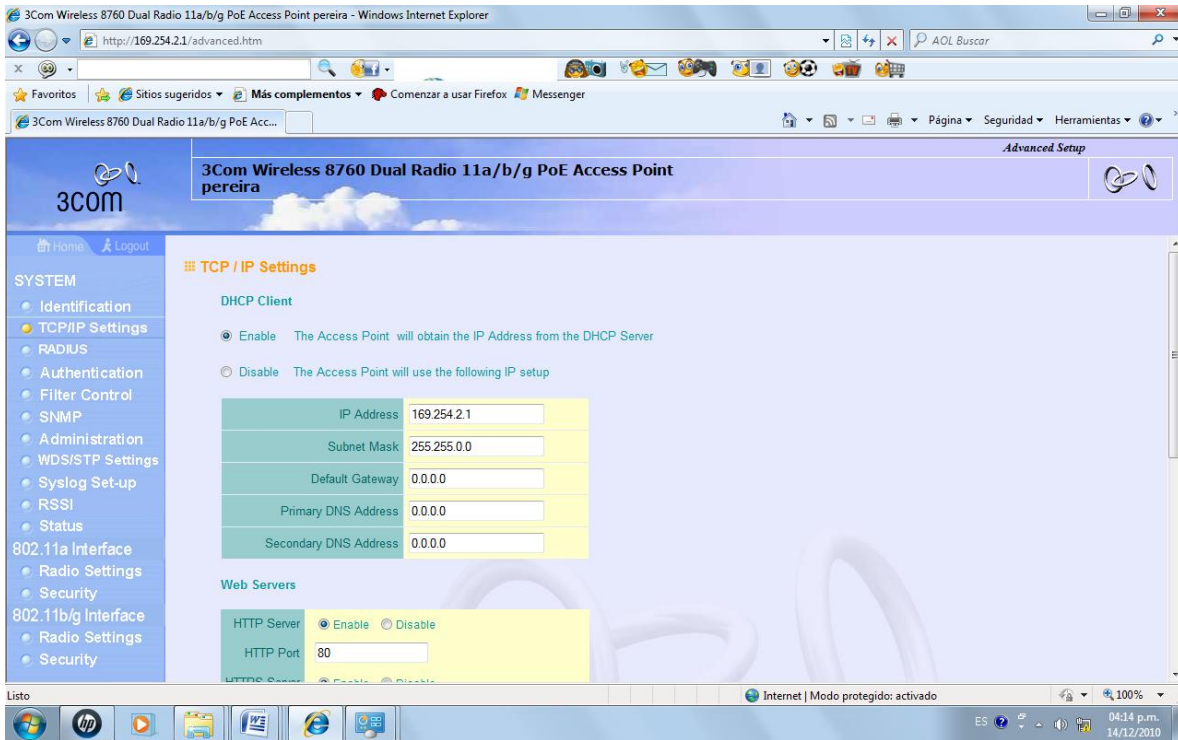
Seguidamente se le asignó un nombre para identificar la red como lo podemos apreciar en la siguiente figura y se le dio click en el botón apply (aplicar).



Luego se confirmó el nombre que estableció en este caso fue Cartagena.



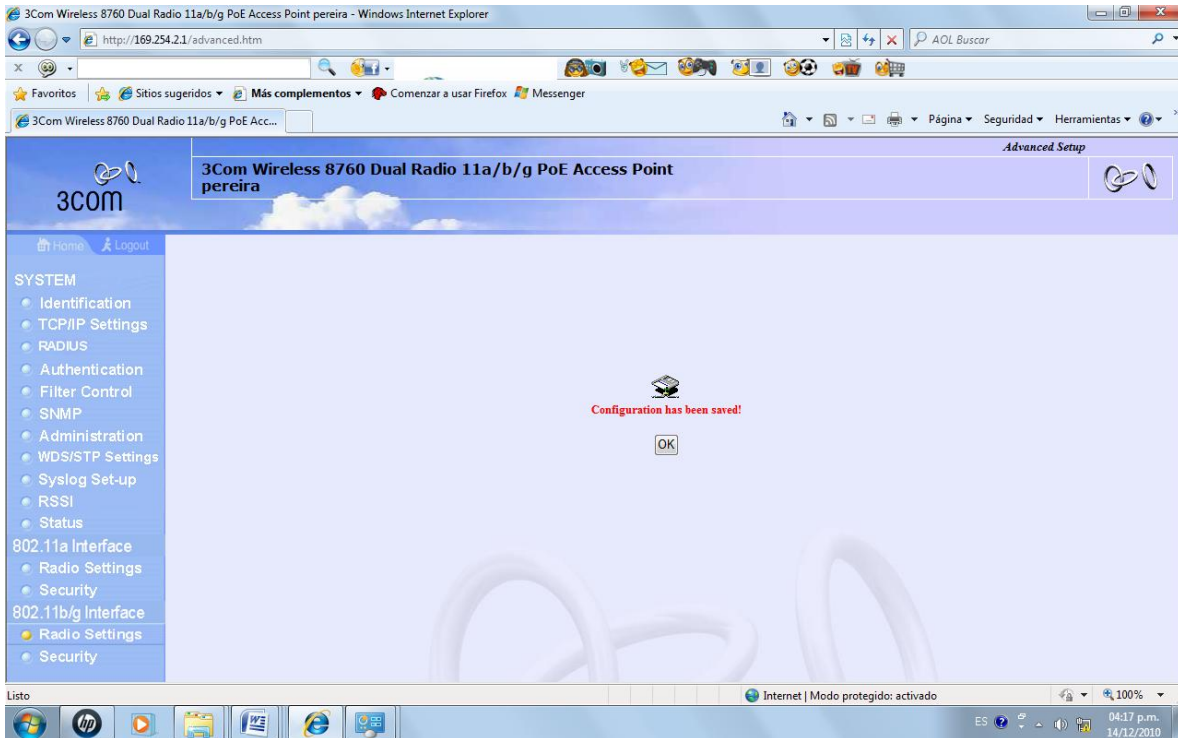
Entramos en el ítem de TCP/IP setting y puede ver la dirección que traía por defecto



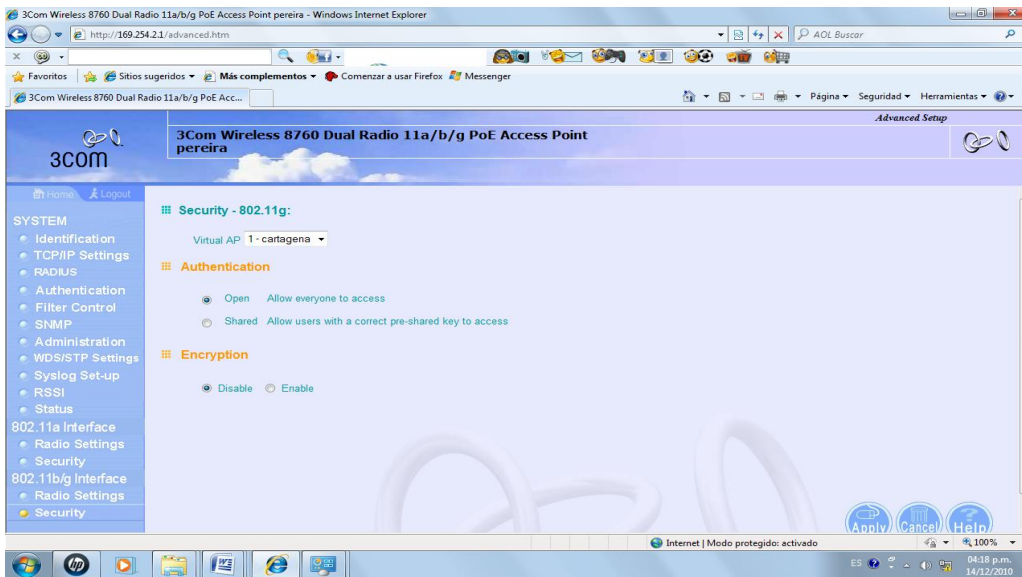
Se entró en el ítem de radio setting(Configuración de Radio) y se escribió el nombre de la red y la vlan en este caso de escribió la 1 que es por defecto, como se puede observar en la figura y luego se le da click en apply"aplicar".



Luego de se confirmaba la configuración anterior



Luego se entró en el ítem security (Seguridad) y se escogió en autenticación el ítem de open que significa no se va escribir contraseña para entrar a la red.







## FICHA TECNICA DE LOS EQUIPOS UTILIZADOS



Figura. 21 Router Cisco 2800

<b>FICHA TECNICA</b>
<b>DENOMINACION:</b> Router
<b>DENOMINACION TECNICA:</b> Router Cisco 2800
<b>CARACTERISTICAS FISICAS</b> Dimensiones: 4,45cm Altura x 43,81cm Anchura x 41,66cm Profundidad Compatible Rack Unit: 1U
<b>INTERFACES/PUERTOS :</b> 2 x RJ-45 10/100Base-TX 10/100Base-TX LAN 1 x Auxiliar Gestión 1 x Consola Gestión 2 x USB Número de Puertos: 2 Fast Ethernet Port: Sí Ranuras de Expansión: (2 Total) AIM, (4 Total) HWIC, (1 Total) NME, (2 Total) PVDM Número de Ranura de Expansión: 9 Protocolos: TCP/IP, SNMP v3 Memoria Flash: 64 MB Memoria Máxima: 760MB Memoria Estándar: 256MB Tecnología: DRAM Sistema Operativo: Cisco 2800 IOS basado IP Voltaje de Entrada: 110V AC, 220V AC Frecuencia: 50 Hz o 60 Hz <sup>42</sup>

<sup>42</sup> <http://www.wvs.com.mx/index.php?act=viewProd&productId=23>





Figura 21. Swith Cisco 2950

<b>FICHA TECNICA</b>
<b>DENOMINACION:</b> Switch
<b>DENOMINACION TECNICA:</b> Switch Cisco serial 2950
<b>DESCRIPCION GENERAL:</b> Dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. <sup>43</sup>
<b>CARACTERISTICAS FISICAS</b> Dimensiones: 44.5 cm x 24.2 cm x 4.4 cm Peso: 3,2 Kg
<b>INTERFACES/PUERTOS :</b> Memoria Flash: 8 MB Cantidad de puertos: 24 x Ethernet 10Base-T, Ethernet 100Base-TX Velocidad de transferencia de datos: 100 Mbps Protocolo de interconexión de datos: Ethernet, Fast Ethernet Protocolo de gestión remota: SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, HTTP Modo comunicación: Semidúplex, dúplex pleno Características: Control de flujo, capacidad duplex, concentración de enlaces, soporte VLAN, snooping IGMP, soporte para Syslog, Weighted Round Robin (WRR) queuing, actualizable por firmware Cumplimiento de normas: IEEE 802.3, IEEE 802.3u, IEEE 802.1D, IEEE 802.1Q, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s Alimentación: CA 120/230 V CA 110/220 V ± 10% ( 50/60 Hz )

<sup>43</sup> <http://www.aprendergratis.com/componentes-y-funcionamiento-basico-de-las-redes-locales.html>



Figura 22. Softphone Cisco

<b>FICHA TECNICA</b>
<b>DENOMINACION:</b> Softphone Cisco ip Communicator
<b>DEFINICION:</b> Un Softphone es un software que hace una simulación de teléfono convencional por computadora. Es decir, permite usar la computadora para hacer llamadas a otros softphones o a otros teléfonos convencionales usando un VSP.
<b>GENERALIDADES:</b> El Softphone utilizado permite el funcionamiento a través de la multimedia normal del los PCs en los que se instalo o a través de dispositivos USB estándares de forma opcional. Permite multilínea con mínimo 2 call appearances y maneja el registro de todas las llamadas, tanto entrantes, salientes como perdidas.
<b>FUNCIONES MÍNIMAS:</b> Desvío de llamadas internos Llamada en espera. Bloqueos de llamadas no permitidas. Códigos de cuenta. Funciones básicas: Redial, Flash, Music, hold. Movilidad de extensión, permitiendo que el teléfono IP pueda ser desplazado a cualquier punto de la red, sin modificar su configuración.



Figura 23. Access point 3com 8760

<b>FICHA TECNICA</b>
<b>DENOMINACION:</b> Access point 3com
<b>DENOMINACION TECNICA:</b> Access point 3com 8760 dual radio 11 a/b/g
<b>CARACTERISTICAS FISICAS</b> Dimensiones: Ancho 19.5 cm, Profundidad 18 cm, Altura 16 cm Peso: 1 kg Capacidad Guía Telefónica: 100 Números y nombres. Capacidad de registro de llamadas: 60 números Pantalla gráfica LCD a color sensible al tacto, capacidad para mostrar contenido XML, altavoz, entradas para audífonos o bocinas auxiliares, tecla para ver páginas anteriores en la pantalla, compatible con PoE, conectividad 10/100 BaseT, detección de actividad de voz, cancelación de ruido, cliente DHCP
<b>INTERFACES/PUERTOS :</b> Protocolos: VoIPSIP v2 Códecs de voz: G.711, G.723.1, G.729a Calidad del servicio: IEEE 802.1Q (VLAN), DifferentiatedServices (DiffServ), IEEE 802.3 Asignación de dirección: IPDHCP Protocolos de red: DNS Cantidad de puertos: red 1 x Ethernet 10Base-T Propiedades de voz: Detección de actividad de voz (VAD) Propiedades de red: Network AddressTranslation (NAT) Alimentación: Tipo Adaptador de corriente – externo

## COMANDOS CISCO AUTOQOS PARA LA CONFIGURACION DE QoS<sup>44</sup>

COMANDOS	DESCRIPCION
auto qos [ voip] [ trust]	Configura las características de cisco AutoQoS en una interfaces
ip cef	Habilita cef en el Router
Ping	Realiza un ping en una ip extendida
show auto discovery qos	Muestra el resultado de cisco AutoQoS discovery
show auto discovery qos [interface [interface- type]]	Muestra las configuraciones creadas por cisco AutoQoS, características en una interface específica o en todas las interfaces.
show interface	Muestra los detalles de la interface
Auto qos voip trust	Habilita AutoQoS confiando en que ninguna Qos marca al entrar a la interfaz.
Auto qos voip	Habilita AutoQoS sin confiar en ninguna marca de paquetes.el router remarcará todo tipo de tráfico access lists or Network-Based, este commando se utilice en router y switch capa 3.
Auto qos Voip cisco-softphone	Habilita AutoQoS , confiando en que ninguna de las marcas de calidad de servicio existentes que entran en la interfaz sólo si el interruptor detecta un Cisco IP Softphone (tales como Cisco IP Communicator) se usa en los switch.

<sup>44</sup> [http://digeset.ucol.mx/tesis\\_posgrado/Pdf/Arturo%20Torres%20Gutierrez.pdf](http://digeset.ucol.mx/tesis_posgrado/Pdf/Arturo%20Torres%20Gutierrez.pdf)

En la tabla anterior se muestra una lista de comandos utilizados para la configuración de QoS en los Routers cisco 2800.