
# UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

## FACULTAD DE INGENIERÍA

## ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE REDES VIRTUALES EN EL COLEGIO DE MÉXICO, A.C.

**T E S I S**

**QUE PARA OBTENER EL TÍTULO DE INGENIERO EN COMPUTACIÓN**

**P R E S E N T A :**

**JOSÉ HÉCTOR GUTIÉRREZ PÉREZ**

**DIRECTOR DE TESIS:**
**M.T.I.A. SANTIAGO DARÍO ORTEGA ACEVES**


**CODIRECTOR DE TESIS:**
**M.I. AURELIO ADOLFO MILLÁN NÁJERA**

**CIUDAD UNIVERSITARIA**

**2004**

# ÍNDICE

# 1. INTRODUCCIÓN

Uno de los grandes recursos del hombre para mejorar sus condiciones de vida ha sido poder comunicarse eficientemente con otros para satisfacer ya sea alguna necesidad, o bien, con fines de esparcimiento. En los inicios de la humanidad, el perfeccionamiento de la comunicación entre individuos en sus diversas facetas (señas, pictogramas, lenguaje, y escritura), permitió mejor coordinación entre individuos y obtener así beneficios, que de otra forma no hubiera conseguido. A partir de entonces las formas de comunicarse entre seres humanos han ido adaptándose a las necesidades de desarrollo de la sociedad en general, y la comunicación ha sido y seguirá siendo un factor de éxito para este punto.

Hoy, las redes de computadoras facilitan la comunicación, haciendo la vida personal más sencilla o mejorando la productividad en grupo dentro de una empresa. Son muchos los ejemplos de aplicaciones que corren sobre una red de datos que forman parte de la vida cotidiana de millones de personas y van desde el sencillo, pero muy usado, correo electrónico hasta aplicaciones que son compartidas por múltiples empresas. Sin embargo las redes de datos no operan solas; en realidad, cada una de ellas es un complejo sistema donde convergen tecnologías y protocolos que, bajo un buen diseño y mantenimiento, dará el servicio de comunicación deseado.

Para El Colegio de México, el reestructurar el diseño lógico y físico de la red local es de vital importancia por los cambios tecnológicos que se van generando continuamente; esto también origina que los equipos de comunicaciones vayan siendo obsoletos al paso del tiempo y, en consecuencia, deban renovarse al cumplir su tiempo de utilidad. Otro punto importante en la reestructuración es el crecimiento de la red local de la Institución; en cuanto a equipo de cómputo principalmente computadoras personales e impresoras, lo que genera problemas de conectividad, eficiencia, seguridad y desempeño en la red.

Es por ello que este proyecto de tesis contempla una propuesta de solución que resuelva los problemas de la red local de la Institución en los puntos antes señalados, así como la actualización de equipo de comunicación y su adecuación al sistema de seguridad existente en El Colegio.

## 1.1 Descripción de El Colegio de México

El Colegio de México fue fundado el 8 de octubre de 1940 por el Gobierno Federal, el Banco de México, la Universidad Nacional Autónoma de México y el Fondo de Cultura Económica con los fines de organizar y realizar investigaciones en algunos campos de las ciencias sociales y las humanidades, impartir educación superior para formar profesionistas, investigadores y profesores universitarios, editar libros y revistas sobre materias relacionadas con sus actividades y colaborar con otras instituciones nacionales y extranjeras para la realización de objetivos comunes.

Además de contribuir a la formación de los recursos humanos del país, en el más alto nivel académico posible, los profesores de El Colegio de México dedican una parte sustancial de su tiempo a la investigación. A esto se debe que la Institución haya sido pionera en el estudio y diagnóstico de importantes problemas nacionales. La creación y consolidación de sus programas ha estado estrechamente ligada a anticipar, diagnosticar y sugerir posibles campos de acción para el Estado y la Sociedad.

El Colegio de México ha sido reconocido como una de las instituciones líderes de la investigación y docencia en ciencias sociales y humanidades del país. Desarrolla sus actividades en siete centros de estudio: Centro de Estudios Históricos, Centro de Estudios Lingüísticos y Literarios, Centro de Estudios Económicos, Centro de Estudios Internacionales, Centro de Estudios de Asia y África, Centro de Estudios Demográficos y de Desarrollo Urbano y Centro de Estudios Sociológicos, de los cuales han egresado estudiantes en su mayoría mexicanos, aunque es considerable el número de Centro y Sudamericanos que han pasado por sus aulas y han recibido títulos académicos de El Colegio.

Como Institución acreditada de educación superior, El Colegio de México ofrece siete programas de doctorado: Historia, Lingüística, Literatura Hispánica, Economía, Estudios de Población, Estudios de Asia y África y Ciencia Social; cinco de maestría: Economía, Estudios Urbanos, Demografía, Estudios de Asia y África y Estudios de la Mujer; y dos de licenciatura: Relaciones Internacionales y Política y Administración Pública. Además, El Colegio ofrece tres programas especiales: Formación de Traductores, Ciencia y Tecnología y Estudios de la Mujer. Complementan la organización la Biblioteca “Daniel Cosío Villegas”, la Administración y la Coordinación de Servicios de Cómputo.

La Biblioteca “Daniel Cosío Villegas”, nombre que recibió en 1976 en memoria del que fuera presidente de El Colegio, está clasificada como biblioteca universitaria, especializada y de investigación, abierta a maestros, investigadores y alumnos, así como a toda persona de instituciones de educación superior y de otros sectores del país. Su propósito es apoyar los programas de investigación, docencia y difusión de El Colegio mediante la selección, adquisición, acceso, organización, conservación y canje de materiales bibliográficos para desarrollar las colecciones especializadas sobre los temas de estudio, enseñanza e investigación; la catalogación, clasificación y organización de las colecciones para ponerlas a disposición de sus usuarios y la oferta de servicios de referencia, información, préstamo de materiales e instrucciones de usuarios además de mantener convenios de cooperación con otras unidades de información y organizaciones afines para ampliar el acceso a los recursos informativos.

El área Administrativa colabora con el presidente de El Colegio en la planeación, organización, dirección y supervisión de los servicios proporcionados por la administración para asegurar el cumplimiento de los objetivos estratégicos; coordina y supervisa la ejecución de los planes, programas y actividades de las Direcciones de Recursos Humanos, Presupuestos, Finanzas, Servicios Generales y Asuntos Jurídicos. Planea, dirige y supervisa la administración financiera de la Institución, también en los procesos relativos a la administración de los servicios generales para asegurar que los sistemas de adquisición de bienes y contratación de servicios se brinden oportunamente.

La Coordinación de Servicios de Cómputo se inicio en el año de 1966, para facilitar el manejo de censos y encuestas con la aplicación de las computadoras y de las técnicas computacionales, y se ha convertido hoy en parte esencial de casi todas las tareas académicas y de investigación. La Coordinación de Cómputo provee un servicio de calidad, difunde a través de medios electrónicos los avances de las investigaciones que realizan los Centros de Estudios, administra los sistemas de información de Internet e Intranet, establece los estándares en hardware y software e integra la tecnología de la información para el uso de datos, voz y video. La Coordinación está organizada en seis áreas que son: Redes y Telecomunicaciones, Seguridad, Sistemas, Servicios de Información, Asesoría Técnica y Laboratorio de Análisis Espacial.

## 1.2 Organización de Documento

En la elaboración del tema de tesis “Análisis, diseño e implementación de redes virtuales en El Colegio de México”, se realizó en diferentes etapas para su desarrollo, con el fin de obtener resultados adecuados de principio a fin.

Los procedimientos generales que se realizaron en cada capítulo se explican a continuación.

En el capítulo 1. INTRODUCCIÓN, se da un resumen del contenido, donde se hace una descripción general de El Colegio de México, así como los objetivos alcanzados en la realización del proyecto de tesis.

En el capítulo 2. MARCO TEÓRICO, se plantean los conceptos fundamentales, los cuales proporcionan herramientas teóricas y dan apoyo al entendimiento del tema.

El capítulo 3. ANÁLISIS, muestra la situación actual en que se encuentra la red de El Colegio, y se realiza un estudio de la red local para saber su problemática. Hecho lo anterior se dará la propuesta de solución.

El capítulo 4. DISEÑO, se aboca principalmente a generar el diseño de las redes virtuales. Esto es, se diseñan los dominios lógicos, servicios y aplicaciones de las redes virtuales, direccionamiento y el ruteo entre las redes virtuales.

El capítulo 5. IMPLEMENTACIÓN, corresponde a la fase final del proyecto de tesis. Incluye las etapas de configuración de servidores, selección y configuración del *Backbone*, así como la etapa de integración de las redes virtuales con el *firewall* de la red local.

El capítulo 6. ADMINISTRACIÓN DE LAS VLANs, describe las opciones para la administración de las redes virtuales que pueden ser por línea de comandos, manejador de dispositivos y manejador de redes virtuales.

Al final se exponen las conclusiones generadas a partir del desarrollo del proyecto de tesis y un anexo, que contiene información de gráficas de la red local haciendo comparaciones de utilización, colisiones, errores, *broadcast* y *drops*, que fueron generadas antes y después de la implementación de las redes virtuales.

## 1.3 Objetivos

Los objetivos planteados para el tema de tesis son los siguientes:

- El objetivo principal y por el cual se elaboró el proyecto de tesis es el análisis, diseño e implementación de redes virtuales en El Colegio de México, A.C; como una propuesta de solución a los problemas en la red local de la Institución.

- Otro objetivo que se plantea como un agregado en el proyecto es la interconexión de las redes virtuales en el sistema de seguridad ya existente en El Colegio.

# 2. MARCO TEÓRICO

En el desarrollo del proyecto se tiene que hablar de conceptos, definiciones y términos que se van a utilizar posteriormente en la tesis. Esto es para tener una mejor comprensión y facilidad del tema que se va a tratar; es por eso que en este capítulo los abordaremos.

## 2.1 Conceptos de Redes de Datos

Una red de datos se puede definir como una colección de dispositivos interconectados entre sí, capaces de intercambiar algún tipo de información, tal como bases de datos, acervos bibliográficos, archivos, imágenes, correos electrónicos, etc. Además, permite compartir recursos como unidades de almacenamiento de información, dispositivos de impresión entre otros.

Entre las ventajas de usar redes de datos están las siguientes:

- Hoy en día la mayoría de las organizaciones se encuentran ampliamente distribuidas de manera geográfica por lo que una red de datos les permite un fácil, rápido y eficiente intercambio de información en localidades dispersas.
- Las redes de computadoras posibilitan compartir recursos de cómputo (*hardware* y *software*) como capacidad de procedimiento o la disponibilidad de conexión a otras redes.
- La integración del flujo de información requerido por empresas permite que muchas de las tareas que aún están íntimamente relacionadas y que se realizaban típicamente de manera independiente, puedan ahora integrase en un solo sistema que ahorra recursos y minimiza los tiempos.

La implementación de una red funcional no es tarea fácil. Se deben enfrentar muchos retos, sobre todo en confiabilidad, administración de red y flexibilidad. Cada área es clave en el establecimiento de una red eficiente y efectiva. El reto al conectar varios sistemas es soportar la comunicación entre tecnologías diferentes ya que, por ejemplo, varios sitios pueden utilizar diferentes medios de transmisión, o bien operar a velocidades variables.

En toda red se debe tener siempre una atención esencial hacia la confiabilidad del servicio. Tanto usuarios individuales como organizaciones empresariales dependen del acceso constante y confiable a los recursos de la red. Además, la administración de la red debe proporcionar soporte centralizado y capacidades de corrección de fallas. La flexibilidad es necesaria para la expansión de la red y la implementación de nuevas aplicaciones y servicios, entre otros factores.

## 2.2 Clasificación de Redes de Datos

La red de datos juega un papel muy importante en las comunicaciones. En los últimos años se le ha dado mucha importancia al transporte de información a largas distancias,

para ser más exactos a mediados de los setenta; siendo en la actualidad uno de los campos de más rápido crecimiento, dando cabida a la tecnología del transporte de datos.

Existen redes para comunicarnos a diversas distancias con sus propias características y alcances, y que se mencionan a continuación.

### 2.2.1 Redes LAN

Las redes LAN (*Local Area Networks*, Redes de Área Local), son de propiedad privada dentro de un solo edificio o campus de hasta unos cuantos kilómetros de extensión. Se usan ampliamente para conectar computadoras personales y estaciones de trabajo con el objeto de compartir recursos (por ejemplo: impresoras, archivos, programas, etc.), e intercambiar información. Las LAN se distinguen de otro tipo de redes por tres características: su tamaño, su tecnología de transmisión y su topología.

Las LAN están restringidas en tamaño, lo cual significa que el tiempo de transmisión en el peor caso está limitado y se conoce de antemano. Conocer este límite simplifica la administración de la red y hace posible usar ciertos tipos de diseños que de otra manera no serían prácticos.

Las LAN tradicionales operan a velocidades de 10 a 100 Mbps, tienen bajo retardo (décimas de microsegundos) y experimentan muy pocos errores. Las LAN más nuevas pueden operar a velocidades muy altas, de hasta cientos y miles de Megabits/seg.

La topología de una red LAN es el arreglo físico en el cual los dispositivos de red (computadoras, impresoras, servidores, *hubs*, *switches*, puentes, etc.) se interconectan entre sí sobre un medio de comunicación.

### 2.2.2 Redes MAN

Una red MAN (*Metropolitan Area Network*, Red de Área Metropolitana), es básicamente una versión más grande de una LAN y normalmente se basa en una tecnología similar. Podría abarcar un grupo de oficinas corporativas cercanas o una ciudad y podría ser privada o pública. Una MAN puede manejar datos y voz, e incluso podría estar relacionada con la red de televisión por cable local. Una MAN sólo tiene uno o dos cables y no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potencial. Al no tener que conmutar, se simplifica el diseño.

La principal razón para distinguir las MAN como una categoría especial es que se ha adoptado un estándar para ellas, y este estándar se llama DQDB (*Distributed Queue Dual Bus*). El estándar consiste en dos buses (cables) unidireccionales, a los cuales están conectadas todas las computadoras. Cada bus tiene una cabeza terminal (*head-end*), y un dispositivo que inicia la actividad de transmisión. El tráfico destinado a una computadora situada a la derecha del emisor usa el bus superior. El tráfico hacia la izquierda usa el inferior.

### 2.2.3 Redes WAN

Una red WAN (*Wide Area Network*, Red de Área Amplia), se extiende sobre un área geográfica extensa, a veces un país o un continente; contiene una colección de máquinas dedicadas a ejecutar programas de usuario (es decir, de aplicación), común y tradicionalmente llamados *hosts*. Los *hosts* están conectados por una subred de comunicación, o simplemente subred. El trabajo de la subred es conducir mensajes de un *host* a otro, así como el sistema telefónico conduce palabras del que habla al que escucha. La separación entre los aspectos exclusivamente de comunicación de la red (la subred) y los aspectos de aplicación (los *hosts*), simplifica el diseño total de la red.

En muchas redes de área amplia, la subred tiene dos componentes distintos: las líneas de transmisión y los elementos de conmutación. Las líneas de transmisión (también llamados circuitos, canales o troncales) mueven bits de una máquina a otra.

Los elementos de conmutación son computadoras especializadas que conectan dos o más líneas de transmisión. Cuando los datos llegan por una línea de entrada, el elemento de conmutación debe escoger una línea de salida para reenviarlos. Desafortunadamente, no hay una terminología estándar para designar estas computadoras; se les denomina nodos conmutadores de paquetes, sistemas intermedios y centrales de conmutación de datos, entre otros. Como término genérico para los equipos de conmutación, usaremos la palabra *router*.

En casi todas las WAN, la red contiene numerosos cables o líneas telefónicas, cada una conectada a un par de *routers*. Si dos *routers* que no comparten un cable desean comunicarse, deberán hacerlo indirectamente, por medio de otros *routers*. Cuando se envía un paquete de un *router* a otro a través de uno o más *routers* intermedios, el paquete se recibe completo en cada *router* intermedio, se almacena hasta que la línea de salida requerida está libre, y a continuación se reenvía. Una subred basada en este principio se llama, punto a punto, almacenar y reenviar, o de paquete conmutado. Casi todas las redes de área amplia (excepto aquellas que usan satélites) tienen subredes de almacenar y reenviar. Cuando los paquetes son pequeños y el tamaño de todos es el mismo, suelen llamarse celdas.

Una segunda posibilidad para una WAN es un sistema de satélite o de radio en tierra. Cada *router* tiene una antena por medio de la cual puede enviar y recibir. Todos los *routers* pueden oír las salidas enviadas desde el satélite y en algunos casos pueden también oír la transmisión ascendente de los otros *routers* hacia el satélite. Algunas veces los *routers* están conectados a una subred punto a punto de gran tamaño, y únicamente algunos de ellos tienen una antena de satélite. Por su naturaleza, las redes de satélite son de difusión y son más útiles cuando la propiedad de difusión es importante.

## 2.3 Topologías de Red

La topología de una red define como interconectar los diferentes equipos, es decir, es el mapa de distribución que forma una red. A la hora de instalar una red, es importante seleccionar la topología más adecuada a las necesidades existentes. Hay una serie de factores a tener en cuenta a la hora de decidirse por una topología de red concreta: la distribución de los equipos a interconectar, el tipo de aplicaciones que se van a ejecutar, la inversión que se quiere hacer y el costo que se quiere dedicar al mantenimiento y actualización de la red local.

En topologías de red existen las siguientes configuraciones básicas para la interconexión de dispositivos (ya sea de manera lógica o física).

### 2.3.1 Topología Bus

Consta de un único cable que se extiende de un dispositivo al siguiente en modo serie (véase Figura 2.1), es decir, la transmisión del llamado terminador, que además de indicar que no existen más dispositivos en el extremo, permiten cerrar el bus. Si se rompe el cable en algún punto, la red queda inoperable por completo.

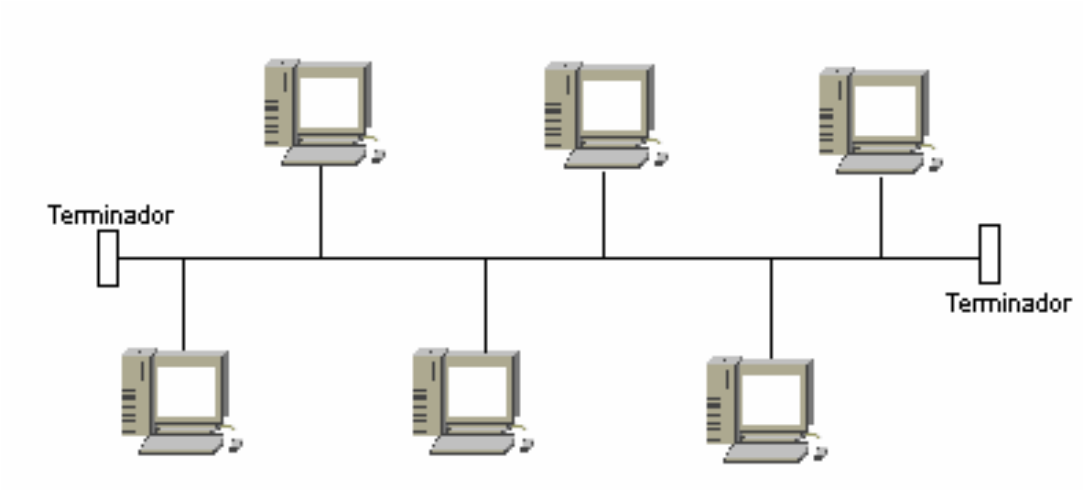



Figura 2.1 Topología Bus

### 2.3.2 Topología Anillo

Los dispositivos se conectan uno tras otro en cadena para formar un anillo (véase Figura 2.2). Si un dispositivo quiere transmitir información a otro no directamente conectado, los dispositivos intermedios tendrán que retransmitir la información generada por el primer dispositivo hasta llegar a su destino final. Si se rompe el cable que forma el anillo se paraliza toda la red.

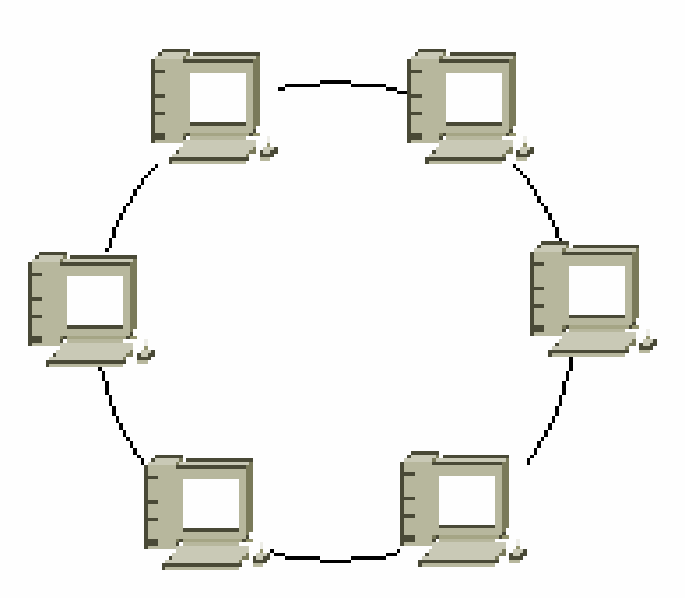


Figura 2.2 Topología Anillo

### 2.3.3 Topología Estrella

Todas las estaciones de trabajo están conectadas a un punto central (véase Figura 2.3). Cada vez que se quiere establecer comunicación entre dos equipos, la información transferida de uno hacia el otro debe pasar por el punto central, si éste llegara a fallar toda la red se detendría. Si se rompe un cable sólo se pierde la conexión del nodo que se interconecta al punto central. Su distribución general facilita la detección y localización de problemas en la red.

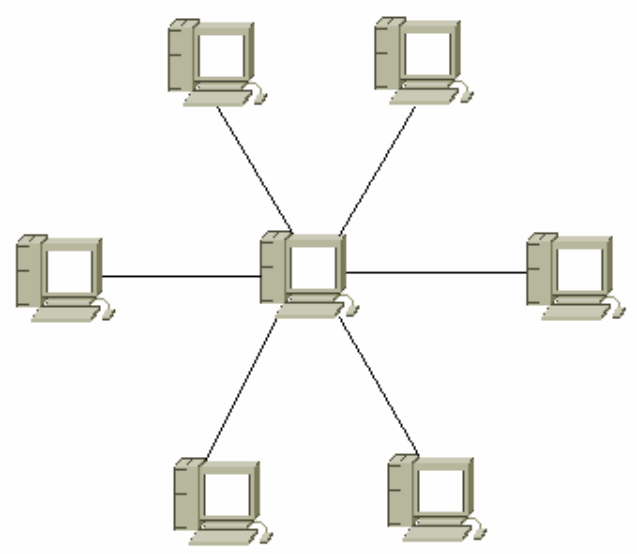


Figura 2.3 Topología Estrella

### 2.3.4 Topología Jerárquica o Árbol

En esta topología varios dispositivos son concentrados en uno para su comunicación (véase Figura 2.4), el cual a su vez puede estar concentrado en otro dispositivo de mayor prioridad para su comunicación.

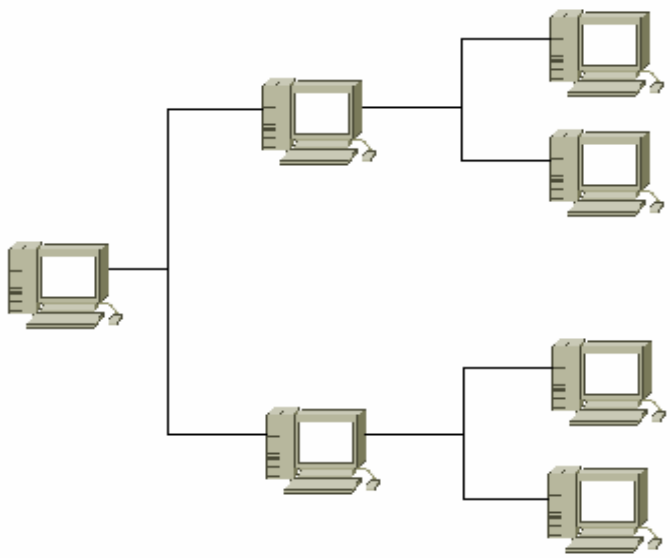


Figura 2.4 Topología Jerárquica o Árbol

### 2.3.5 Topología Malla

En esta topología cada nodo se enlaza directamente con los demás nodos (véase Figura 2.5). Las ventajas son que cada nodo se conecta físicamente a los demás nodos y, por consiguiente se crea una conexión redundante; así como una estrategia de tolerancia a fallas. Si algún enlace deja de funcionar la información puede circular a través de los demás enlaces hasta llegar al destino.

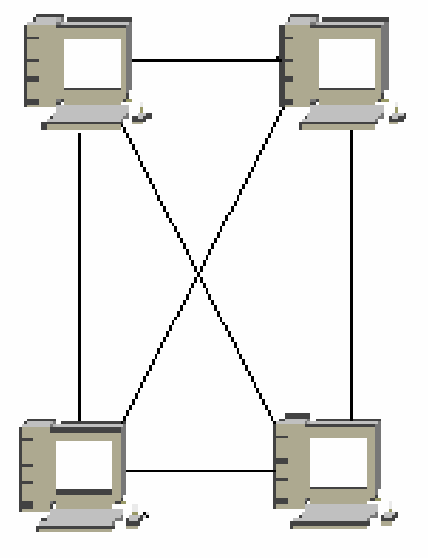


Figura 2.5 Topología Malla

## 2.4 Modelo de Referencia OSI

El modelo de referencia OSI (*Open System Interconnection*, Interconexión de Sistemas Abiertos) describe la manera como la información en una computadora es transferida a una aplicación residente en otro equipo. El modelo de referencia OSI es un modelo conceptual compuesto de siete capas, cada una especifica funciones particulares, es decir que entre capas no existen funciones comunes. OSI es considerado como un modelo de arquitectura para comunicaciones entre computadoras, y es usado como referencia en la comparación de diferentes tecnologías.

El modelo OSI no constituye una arquitectura de red de computadores en sí, solo se utiliza como un marco de referencia en la comunicación de equipos. Este modelo hace referencia a la conexión de sistemas heterogéneos, es decir, a sistemas dispuestos a establecer comunicación con otros distintos. Es por ello que el modelo OSI estriba su importancia por su creación que realizó la ISO (*International Standards Organization*, Organización Internacional de Estándares y Normas)

La Figura 2.6 muestra las siete capas que componen el modelo.

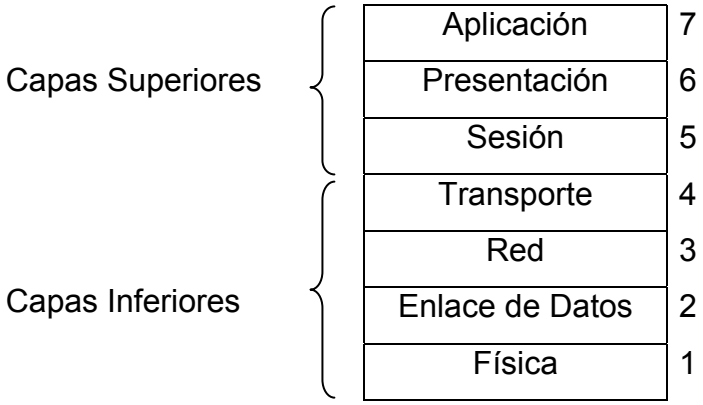



Figura 2.6 Capas del Modelo OSI

Las siete capas del modelo de referencia OSI se pueden dividir en dos categorías, capas superiores y capas inferiores. Las capas superiores del modelo OSI están implementadas en software. La capa superior, la de aplicación, es la interfaz del usuario final. Tanto los usuarios como los procesos de la capa de aplicación interactúan con aplicaciones de software que contienen un componente de comunicación.

Las capas inferiores del modelo OSI manejan lo concerniente a la transferencia de datos. La capa física y de enlace de datos se encuentran implementadas en hardware. Las otras capas inferiores están implementadas en software. La capa inferior, la física, es donde está el medio de transmisión de la red (el cableado de la red).

La comunicación que procede de una capa del modelo generalmente se da con otras tres: la capa inmediata superior, la capa inmediata inferior, y la capa análoga en la computadora a la que se comunicará.

La Figura 2.7 muestra un ejemplo de comunicación entre capas:

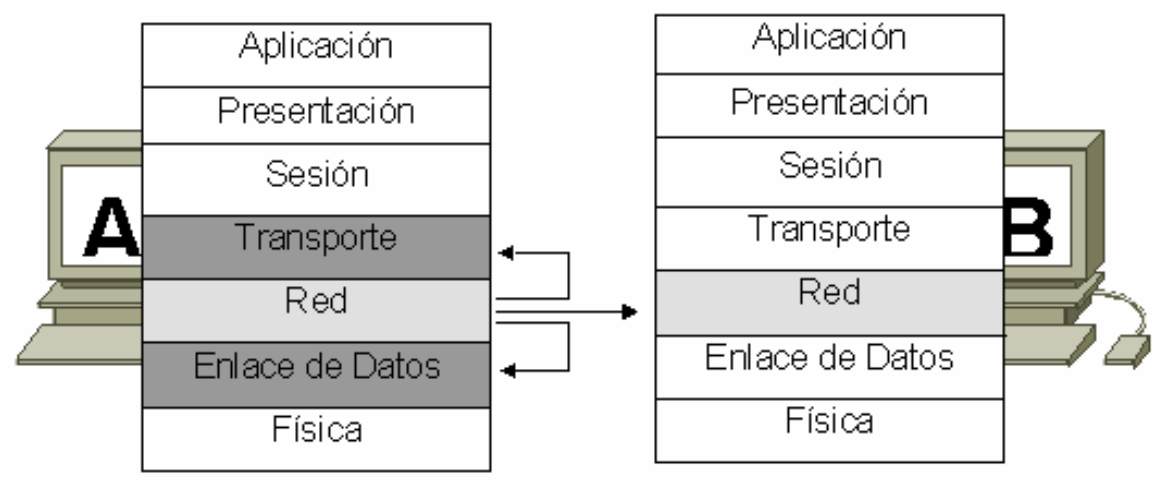



Figura 2.7 Comunicación entre capas del modelo de referencia OSI

La comunicación entre capas de un mismo sistema se da en términos de los servicios que ofrece una capa a la capa inmediata superior, y de los servicios que obtendrá de la capa inmediata inferior.

Las siete capas del modelo usan información de control para comunicarse con otras capas. Esta información de control toma las formas de encabezado o colas. El encabezado es información añadida al principio de los datos, mientras que las colas se generan de información añadida al final de los datos que pasan de capas superiores a capas inferiores del modelo de referencia.

La Figura 2.8 muestra la adición de información de control entre capas:

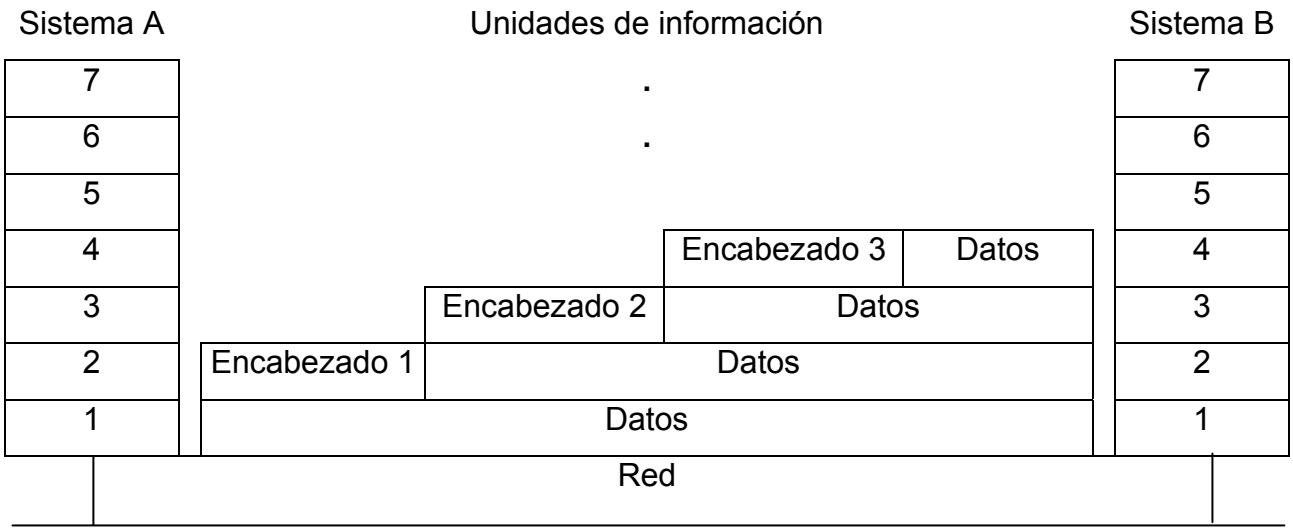



Figura 2.8 El intercambio de información siempre se da entre capas del mismo nivel

### 2.4.1 Capa Física

Define las especificaciones mecánicas, eléctricas, de procedimiento y funcionales para activar, mantener y desactivar un enlace físico entre sistemas de redes de comunicaciones. Las especificaciones de la capa física definen características tales como niveles de voltaje, sincronía, tasas de transmisión, distancias de conexión y conectores físicos. Las implementaciones de la capa física se pueden categorizar como especificaciones LAN y WAN.

### 2.4.2 Capa de Enlace

Proporciona el tránsito confiable de datos a través del enlace físico. Especificaciones en esta capa definen diferentes características de red y protocolo, incluyendo el direccionamiento físico, topología de red, notificación de errores, control de flujo y secuencia de tramas.

### 2.4.3 Capa de Red

Esta capa proporciona el ruteo y funciones relacionadas que permiten a múltiples enlaces de datos combinarse en una red. Esto se logra a través del direccionamiento lógico de los dispositivos. La capa de red soporta servicios orientados y no orientados a conexión de los protocolos de las capas superiores.

### 2.4.4 Capa de Transporte

Implementa servicios confiables de datos a través de la capa de red. Las funciones que otorga esta capa son múltiplexaje, control de flujo, detección y corrección de errores, además de administración de circuitos virtuales.

### 2.4.5 Capa de Sesión

Establece, administra y finaliza sesiones de comunicación entre entidades de la capa de presentación. Las sesiones de comunicación constan de solicitudes y respuestas de servicio que se presentan entre aplicaciones ubicadas en diferentes dispositivos de red.

### 2.4.6 Capa de Presentación

Provee la representación de la información, que las entidades de aplicación comunican. La capa de presentación cubre dos aspectos complementarios:

- La representación de los datos que debe transferirse entre entidades de presentación.

- La representación de la estructura de datos a la cual entidades de aplicación hacen referencia a lo largo de su comunicación.

A la capa de presentación le atañe la sintaxis, pero no la semántica.

### 2.4.7 Capa de Aplicación

Provee los medios necesarios a los procesos de aplicación para acceder al ambiente OSI, además de que es la capa más alta en el modelo de referencia, aquí se ubica la interfaz de las aplicaciones con los usuarios finales del sistema.

## 2.5 Medios de Transmisión

En el diseño de una red local uno de los factores primordiales a considerar es la elección del medio del que nos vamos a valer para realizar la transmisión de datos, es decir, el enlace físico. Para ello tenemos que tomar en cuenta principalmente los siguientes aspectos:

- La velocidad de transmisión de datos que la red requiere.
- El costo que se tendrá en función de la conexión.
- Facilidad de instalación y mantenimiento del enlace.
- Alcance geográfico.

Un enlace o medio físico de transmisión es la ruta física entre un transmisor y un receptor, pueden clasificarse en dos tipos:

- Medios de transmisión alámbricos: son aquellos que siguen una trayectoria cerrada como un cable o un alambre, en donde el transmisor y receptor están conectados directamente al medio.

- Medios de transmisión inalámbricos: son los que no siguen una trayectoria cerrada como podrían ser las señales que viajan a través del aire, las cuales son emitidas en más de una dirección, la transmisión y recepción se efectúa por antena.

### 2.5.1 Medios de Transmisión Alámbricos

A continuación se mencionan las características de algunos medios de transmisión alámbricos más comunes.

#### 2.5.1.1 Cable Coaxial

El cable coaxial (véase Figura 2.9) es una línea de transmisión de señal eléctrica formada por un conductor de cobre en el centro o núcleo, rodeado de un material aislante o dieléctrico, que a su vez está cubierto por un blindaje hecho de una o varias capas de mallas metálicas de tejido trenzado y por último de un aislante de plástico o vinil en la exterior.

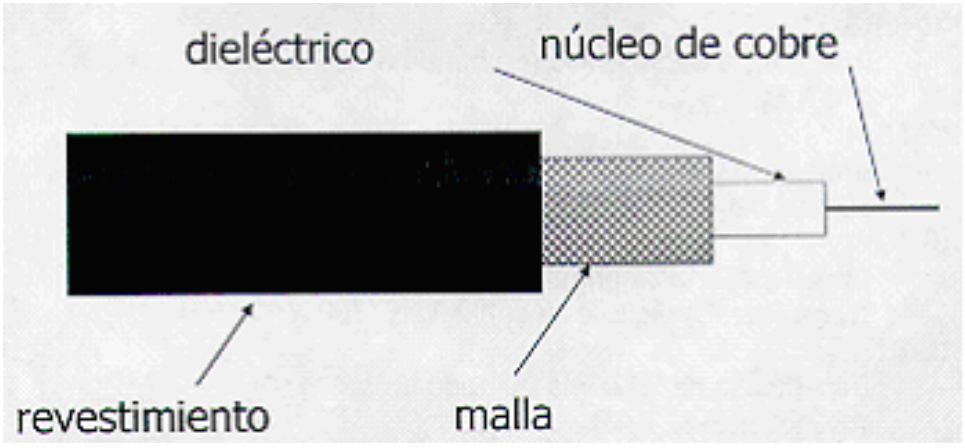



Figura 2.9 Cable Coaxial

Características generales:

- Tiene un diámetro de aproximadamente entre 1 y 2.5 cm.
- Es utilizado tanto para señales analógicas como para señales digitales.
- En señales analógicas se pueden alcanzar frecuencias de 300 a 400 Mhz.
- Es aplicable a configuraciones punto a punto y multipunto.
- La transmisión de alta velocidad (50 Mbps) digital o analógica, está limitada a cerca de 1 Km.
- Su inmunidad al ruido es superior al par trenzado para altas frecuencias.

Tipos de cable coaxial son:

- RG-8/RG-11: impedancia de 50 ohms (en Banda Base) utilizado en redes Thick Ethernet (Coaxial Grueso).
- RG-58: impedancia de 50 ohms (en Banda Base) utilizado en redes Thin Ethernet (Coaxial Delgado).
- RG-59: impedancia de 75 ohms usado para CATV (*Community Antenna Television*), en transmisiones digitales y analógicas (300 a 400 MHz).
- RG-62: impedancia de 93 ohms utilizado en redes ARCnet (*Attached Resource Computing architecture Network*).

#### 2.5.1.2 Cable Par Trenzado

El cable par trenzado (véase Figura 2.10) esta formado por pares de hilos de cobre, envueltos en una cubierta de PVC (*Polyvinyl Chloride*), dichos conductores tienen un diámetro comprendido entre 20 AWG (*American Wire Gauge*) y 26 AWG, con un número de torsiones entre 2 y 12 por pie.

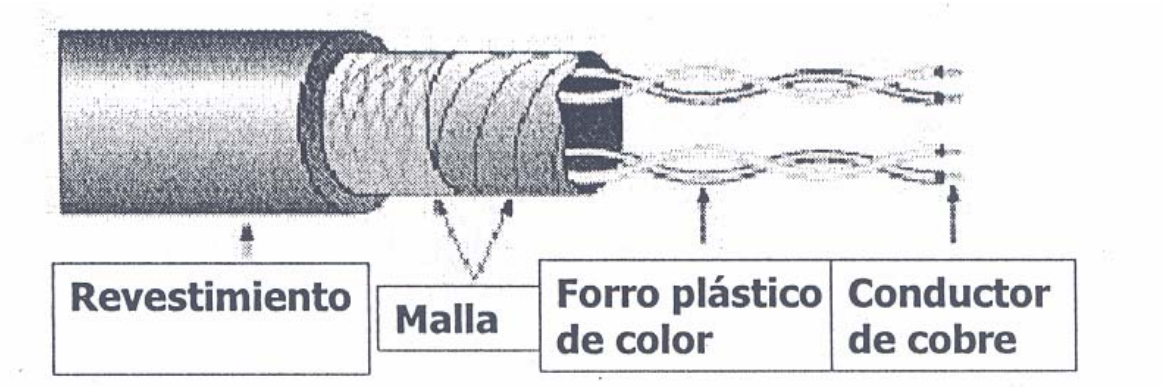



Figura 2.10 Cable Par Trenzado

Tipos de Cable Par trenzado:

- UTP (*Unshielded Twisted Pair*, Par Trenzado sin Blindar): diseño balanceado para compatibilidad EMC (*Electromagnetic Compatibility*), fácil de instalar, bajo en costo, alto desempeño.
- STP (*Shielded Twisted Pair*, Par Trenzado Blindado): diseño balanceado para compatibilidad EMC, fácil de instalar, un poco más costoso, alto desempeño
- FTP (*Foiled Twisted Pair*, Par Trenzado hoja Metalizada): beneficio marginal respecto a EMC, difícil de terminar, más espacio en tubería
- ScTP (*Screened Twisted Pair*, Par Trenzado Malla).

Características generales del cable:

- Atenuación: pérdida de potencia de una señal eléctrica que circula por un conductor metálico.
- *Crosstalk*: energía no deseada radiada de un conductor a otro.
- *Return Loss*: señal que se pierde a causa de la diferencia en impedancias de los componentes de un cableado.
- *Delay Skew*: tiempo necesario para que la señal se propague a través de un conductor.

- *Attenuation Crosstalk Relation*: diferencia entre la atenuación y el *Next* (efecto de traslape espectral entre señales que viajan en direcciones opuestas) a frecuencias específicas.

#### 2.5.1.3 Fibra Óptica

Es una fibra de vidrio muy delgada capaz de conducir un rayo óptico, como lo muestra la Figura 2.11.

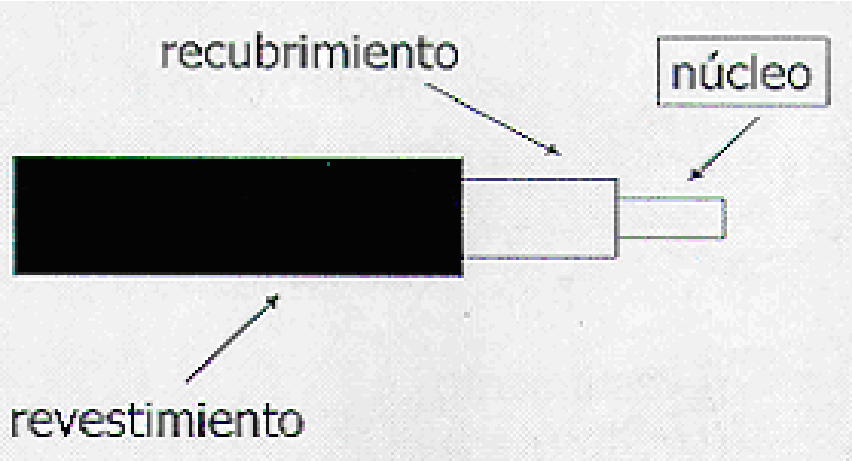



Figura 2.11 Fibra Óptica

Consiste en tres secciones concéntricas:

- El núcleo: es la región de guía de luz, generalmente de vidrio.
- El recubrimiento: contiene la luz en el centro, es de vidrio de diferente índice de refracción que el núcleo.
- El revestimiento: protege el vidrio durante el manejo.

La luz, cuando pasa a través de medios diferentes, está sujeta a la reflexión y a la refracción.

- Reflexión: es cuando el rayo de la luz rebota en el mismo medio.

- Refracción: es la forma como viaja la luz en otro medio, no lo efectúa en la misma dirección.

Para poder transmitir señales ópticas son necesarios el emisor y el receptor, por lo que se requieren dos fibras, una para transmitir y otra para recibir.

- Emisor:
  - Genera la señal de información hacia la fibra óptica.
  - Acopla señales electrónicas a ópticas.
  - Generadores de señal: el LED (*Light Emitting Diode*) provee una señal luminosa amplia de múltiples frecuencias de luz a una distancia máxima de tres kilómetros y el láser (*Light Amplification by Stimulated Emission of Radiation*) provee una señal luminosa angosta que puede tener un alcance de hasta 30 Km.

- Receptor:
  - Convierte los pulsos de luz en señal eléctrica. El más común es el tipo PIN (*Photo-Intrinsic-Type*).

Los diferentes tipos de fibra óptica están determinados por el diámetro del núcleo, el diámetro del recubrimiento y por la composición del material.

El modo, es la trayectoria tomada por una onda de luz conforme ésta viaja a través de la fibra óptica:

- Fibra óptica multimodo: puede ser de índice de un paso o de índice gradual.
  - Fibras multimodo de índice de un paso: el diámetro es de 50 ó 62 μm. Utiliza como fuente de luz el LED. La luz tiende a dispersarse a grandes distancias por lo que sólo alcanzan distancias de hasta 3 Km. Se emplean en redes LAN y MAN.

- Fibras multimodo de índice gradual: el núcleo está compuesto de múltiples capas con diferente densidad, por lo que el índice de refracción del núcleo varía de acuerdo con su diámetro. El resultado es que la diferencia en el retardo de propagación de la luz, debido a los modos de propagación es mínima (múltiples ángulos de reflexión). Estas fibras se usan para enlaces de hasta 2 Km. Los diámetros más comunes de estas fibras son de 50/125 μm, 62.5/125 μm, 85/125 μm y 100/140 μm.

- Fibra óptica monomodo: puede ser de índice de un paso o de dispersión desplazada. Utiliza como fuente de luz el láser. Éste proporciona una señal que no se dispersa fácilmente por lo que alcanza distancias de hasta 30 Km. Se utilizan en redes MAN y WAN. La fibra óptica monomodo es una guía de onda óptica. Solo existe un único modo de propagación, es decir, dentro del pequeño núcleo la luz solamente puede viajar en una trayectoria (modo) de un extremo al otro de la fibra.
  - La fibra monomodo de índice de un paso: la transmisión es generalmente a 1310 nm, donde la dispersión cromática es cero.
  - La fibra monomodo de dispersión desplazada: el núcleo está dividido en una capa interior y otra exterior, la longitud de onda con cero dispersiones está desplazada a 1550 nm, donde la atenuación es más baja.

Características generales:

- En la fibra óptica las señales son transmitidas a través de la luz, por ello, es inmune a interferencias electromagnéticas y radiofrecuencia.
- Las fibras ópticas tienen un amplio ancho de banda.
- Su alcance geográfico es bastante amplio de 6 a 8 Km sin repetidores.
- La compra e instalación de la fibra óptica resulta costosa.

### 2.5.2 Medios de Transmisión Inalámbricos

Este tipo de medio de transmisión representa grandes ventajas para usuarios móviles que necesitan obtener datos para sus computadoras como *laptop*, *notebook*, etc., y no necesariamente estar atados a la infraestructura de comunicaciones terrestres. Al conectarse una antena del tamaño apropiado a un circuito eléctrico, las ondas electromagnéticas se pueden difundir de manera eficiente y captarse por un receptor a cierta distancia. Toda la comunicación inalámbrica se basa en este principio.

Algunos medios de transmisión Inalámbricos son los siguientes:

#### 2.5.2.1 Radio

Las señales de radio se transmiten a velocidades bajas, del orden de los Kbps (Kilo bits por segundo) y frecuencias menores a 1 GHz (Giga Herz), el problema principal de este medio de transmisión es la interferencia generada por diferentes fuentes, así como la reflexión de las señales que provoca que el receptor reciba señales duplicadas fuera de fase. Este método de propagación es a través de una antena omnidireccional.

#### 2.5.2.2 Microondas

En las microondas las velocidades de transmisión son de alrededor de 2 Mbps, con frecuencias mayores a 1 GHz y menores de 600 GHz. En este medio es necesaria una línea de vista sin obstáculos entre las dos antenas (que generalmente son platos parabólicos), la transmisora y la receptora. Estos sistemas son afectados por fenómenos climatológicos y electromagnéticos, y se utilizan para comunicaciones telefónicas, de televisión y datos en distancias no muy grandes.

#### 2.5.2.3 Satélites

En este sistema de comunicaciones las velocidades de transmisión son menores a 1 Mbps y se utilizan dos frecuencias; una de transmisión y otra de recepción que dependen de la banda utilizada. El sistema consta de dos antenas terrestres y el satélite en el espacio. Estos sistemas son afectados por antenas de microondas y por fenómenos climatológicos. Generalmente se utilizan para cubrir áreas geográficas inaccesibles por los demás medios o para grandes extensiones geográficas. Algunas de sus aplicaciones se emplean para transmisión de radio, televisión, comunicación de datos, telefonía, sistemas de radiolocalización y redes WAN.

## 2.6 Tecnologías LAN

En este apartado hablaremos de algunas de las tecnologías LAN mas comunes: *Ethernet*, *Token Ring* y FDDI (*Fiber Distributed Data Interface*); así como también sus métodos de acceso, operación básica, formato de su *trama* y dispositivos que se utilizan en cada tecnología.

Bajo el punto de vista de la IEEE (*The Institute of Electrical and Electronics Engineers*), la capa de enlace (véase Figura 2.12) está dividida en dos partes: en la región inferior se encuentra la subcapa MAC (*Media Access Control*) responsable de las técnicas de acceso al medio de transmisión y el direccionamiento físico de los dispositivos; mientras que en la parte superior se ubica el estándar IEEE 802.2 ó LLC (*Logical Link Control*) que define las funciones lógicas de la capa de enlace, así como la disponibilidad de SAPs (*Service Access Point*) para la adecuada transmisión o recepción de información a protocolos que operan en capas superiores del modelo de referencia OSI.

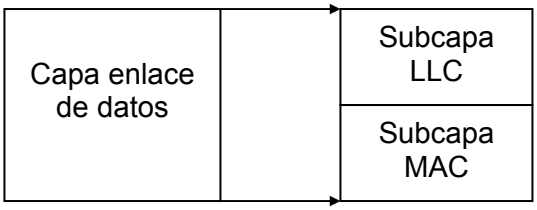



Figura 2.12 División de la capa de enlace de datos

La subcapa LLC administra las comunicaciones entre los dispositivos unidos por un enlace individual de red. La subcapa LLC está definida en la especificación IEEE 802.2 y soporta los servicios orientado y no orientado a la conexión; utilizados por los protocolos de las capas superiores. El IEEE 802.2 define varios campos en las tramas de la capa de enlace de datos, que permiten que varios protocolos de las capas superiores compartan un sólo enlace físico de datos.

LLC provee los siguientes servicios a la capa de red:

- Modo sin conexión y sin reconocimiento, definido como Tipo 1 de operación: en éste las tramas son enviados con la esperanza de que lleguen correctamente a su destino; es decir no existe ningún mecanismo de detección de errores y/o retransmisión de información.
- Modo con conexión, definido como el Tipo 2 de operación: en éste se establecen, usan, reinician y terminan conexiones a nivel enlace entre estaciones terminales, con objeto de efectuar la retransmisión de tramas en caso de pérdida o transmisión errónea, así como el control de flujo entre estaciones.

El formato de la trama LLC se forma como se muestra en la Figura 2.13.

| 1 byte | 1 byte | 1 ó 2 bytes | N bytes |
|---|---|---|---|
| DSAP | SSAP | Control | Información |

Figura 2.13 Formato de la trama LLC

Donde:

DSAP: SAP destino.

SSAP: SAP origen.

N: Entero mayor o igual a cero.

La subcapa MAC de la capa de enlace de datos, administra el protocolo de acceso al medio de transmisión físico en la red. La especificación IEEE MAC define las direcciones MAC, las cuales permiten a múltiples dispositivos identificarse de manera única sobre la capa de enlace de datos.

Para la parte MAC existen diferentes técnicas de acceso al medio:

- Por Contención: cuando un dispositivo necesita transmitir información, verifica primero que el medio esté libre, si es así, transmite inmediatamente, si no, esperará un tiempo finito hasta que el medio de transmisión esté libre y así poder realizar su transmisión. En este tipo de estrategia no existe control sobre que dispositivo será el siguiente en ocupar el medio de transmisión. Tecnologías típicas que utilizan este esquema son *Ethernet* y derivados.
- *Round Robin*: en esta técnica los dispositivos comparten un mismo medio de transmisión y tienen asignada una secuencia en tiempos o turnos para la transmisión de su información de forma rotatoria. Si el dispositivo en turno no tiene nada que transmitir, cede su lugar al siguiente dispositivo en la cola de transmisión. Tecnologías típicas que emplean este esquema son *Token Ring*, FDDI.
- Por Reservación: se trata del uso de la técnica *Round Robin*, pero con la posibilidad de que un dispositivo reserve el siguiente turno de transmisión para si mismo. Tecnologías típicas que usan este esquema son *Token Ring*, FDDI.

El direccionamiento MAC más común para dispositivos de red, requiere seis bytes que se representan con números hexadecimales y esta representado en la Figura 2.14.

| 3 bytes | 3 bytes |
|---|---|
| Código del fabricante. | Número de serie de la interfaz |

Figura 2.14 Formato de la trama MAC

### 2.6.1 Tecnología Ethernet

El término *Ethernet* se refiere a la familia de implementaciones de LAN que incluyen tres categorías principales:

- *Ethernet* e IEEE 802.3: son las especificaciones LAN que operan a 10 Mbps a través de cable coaxial o par trenzado.
- *Ethernet* a 100 Mbps: es una sola especificación LAN, también conocida como *Fast Ethernet* (IEEE 802.3u), que operan a 100 Mbps a través de par trenzado o fibra óptica.
- *Ethernet* a 1000 Mbps: es una sola especificación LAN, también conocida como *Gigabit Ethernet* (IEEE 802.3z), que opera a 1000 Mbps (1Gbps) a través de par trenzado o fibra óptica.

Todas las versiones del estándar *Ethernet* tienen una interface común MAC. La diferencia entre cada una de ellas es solamente la implementación de la capa física, señalización de los datos y el medio soportado. La red *Ethernet* ha prevalecido como una tecnología de transmisión fundamental, gracias a su flexibilidad y a que es relativamente fácil de comprender e implementar.

Aunque se han propuesto otras tecnologías como sus posibles reemplazos, los administradores de red prefieren la red *Ethernet* y sus tecnologías derivadas como soluciones eficaces para un amplio rango de requerimientos de implementación en

campus. Para resolver las limitaciones de *Ethernet*, los innovadores de redes han creado, de manera continua, redes *Ethernet* de mayor cobertura.

#### 2.6.1.1 Ethernet

*Ethernet* es una tecnología LAN muy común dada su simplicidad de operación; cuya implementación más común opera a 10 Mbps. *Ethernet* fue creado por Xerox en 1972 y se liberó la versión 1 de esta tecnología en 1980 por el consorcio DIX (DEC/Intel/Xerox). En 1982 es liberada la versión 2 por el mismo consorcio e inicia en el mismo año su estandarización por parte de la IEEE.

En 1983 Novell *Netware* libera un formato de trama propietario basado en el estándar preliminar de 802.3. Dos años después la versión final de 802.3 es liberada, ésta incluye el encabezado LLC, haciendo a la trama de *Netware* incompatible. Finalmente el formato 802.3 SNAP (*Standard Network Access Protocol*, Protocolo de Acceso a Red Estándar) fue creado para permitir la compatibilidad entre la versión 2 de *Ethemet* y 802.3.

En una red del tipo *Ethernet*, la transmisión realizada por un dispositivo es "escuchada" por todos los demás dispositivos conectados a la LAN, bajo una topología lógica tipo Bus, la cual se implementa físicamente usando cable coaxial como medio de transmisión; sin embargo, para facilitar su implementación se ha hecho popular el uso del par trenzado como medio de transmisión donde los dispositivos son conectados a un *hub* (concentrador) en una topología tipo estrella. Debe recalcarse que la topología lógica sigue siendo un bus en todos los casos.

La tabla 2.1 muestra las diferencias entre *Ethernet* e IEEE 802.3, así como las variaciones entre las diferentes especificaciones de la capa física del IEEE 802.3.

| Características | Valores Ethernet | Valores IEEE 802.3 | | | | |
|---|---|---|---|---|---|---|
| | | 10Base5 | 10Base2 | 10BaseT | 10BaseFL | 100BaseT |
| Tasa de transmisión(Mbps) | 10 | 10 | 10 | 10 | 10 | 100 |
| Método de señalización | Banda Base | Banda Base | Banda Base | Banda Base | Banda Base | Banda Base |
| Máxima longitud de cable(m) | 500 | 500 | 185 | 100 | 2,000 | 100 |
| Medio | 50 ohm coaxial | 50 ohm coaxial | 50 ohm coaxial | Par trenzado sin blindaje | Fibra óptica | Par trenzado sin blindaje |
| Topología | Bus | Bus | Bus | Estrella | Punto a punto | Bus |

Tabla 2.1 Tabla comparativa de las diferentes especificaciones de la capa física del IEEE 802.3

En 802.3 las implementaciones físicas son nombradas de acuerdo a ciertas convenciones, descritas en la Figura 2.15.

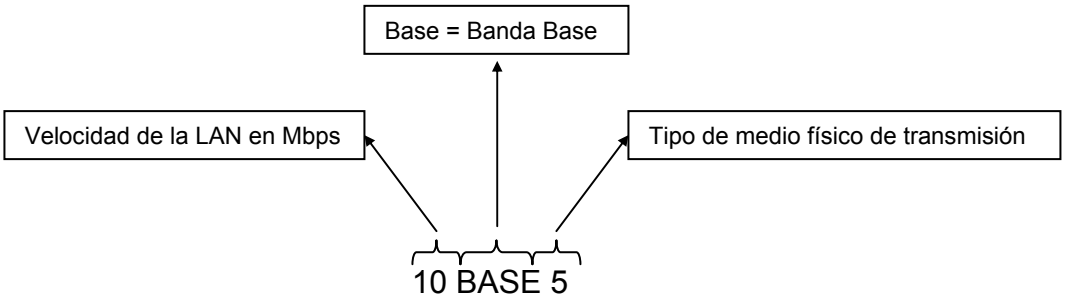



Figura 2.15 Convenciones de las implementaciones físicas del 802.3

La técnica de acceso al medio que usa *Ethernet* en cualquiera de sus implementaciones es la llamada CSMA/CD (*Carrier Sense Multiple Access with Collision Detection*), clasificada como de contención.

La técnica se desglosa a continuación.

Si un dispositivo tiene información que transmitir:

- Censa el medio para ver que nadie esté transmitiendo, es decir verifica que el medio de transmisión esté libre para su uso.
- Si no hay señal en el medio, el dispositivo inicia la transmisión de información.
- Si el medio está ocupado, esperará hasta que esté libre.
- Si ocurre que dos dispositivos comienzan a transmitir al mismo tiempo, se produce una colisión, la cual es detectada por los dispositivos como una variación inusual de voltaje. Detectada la colisión, se interrumpe inmediatamente la transmisión de la trama y se transmite una señal "jam" (32 bits, comúnmente sólo unos) mientras se espera un tiempo aleatorio para volver intentar acceder al medio.

Como ya se había mencionado, existen cuatro tipos de tramas para *Ethernet*; *Ethernet* versión 2, 802.3, Novell y SNAP. Todos tienen una longitud mínima de 64 bytes y una máxima de 1518 bytes, sin contar el campo preámbulo. En este apartado mencionaremos los más relevantes que es el *Ethernet* versión 2 y 802.3.

**Trama Ethernet versión 2**

Esta trama (véase figura 2.16) posee los siguientes campos:

*Preamble*: secuencia de 64 bits consistentes en unos y ceros alternados con terminación en “11”. La sincronía y el inicio del campo de dirección destino (MAC) se logran con este campo.

DA: 6 bytes que contienen la dirección MAC destino.

SA: 6 bytes que contienen la dirección MAC origen.

Type: 2 bytes que identifican a qué protocolo de la capa superior va dirigida la información.

Data: de 46 a 1500 bytes, contiene la información destinada a capas superiores.

FCS: 4 bytes que contienen el código generado por un proceso polinomial sobre los campos DA, SA, *Type* y *Data*. La máquina receptora genera este código cuando recibe la trama y lo compara con el que recibe; si son iguales la información está correcta, si son diferentes la información contiene errores y la trama es descartada.

| 8 bytes | 6 bytes | 6 bytes | 2 bytes | Variable | 4 bytes |
|---|---|---|---|---|---|
| *Preamble* | *Destination Address* | *Source Address* | *Type* | *Data* | FCS |

Figura 2.16 Trama *Ethernet* versión 2

**Trama IEEE 802.3**

Esta trama (véase figura 2.17) tiene los siguientes campos:

*Preamble*: secuencia de 64 bits consistentes en unos y ceros alternados con terminación en “11”. La sincronía y el inicio del campo de dirección destino (MAC) se logran con este campo.

DA: 6 bytes que contienen la dirección MAC destino.

SA: 6 bytes que contienen la dirección MAC origen.

*Length*: 2 bytes que proporcionan la longitud del campo *Data*.

LLC *header*: 3 bytes de *header* LLC ó 802.2

*Data*: de 43 a 1497 bytes, contiene la información destinada a capas superiores.

FCS: 4 bytes que contienen el código generado por un proceso polinomial sobre los campos DA, SA, Length, LLC y Data. La máquina receptora genera este código cuando recibe la trama y lo compara con el que recibe; si son iguales la información está correcta, si son diferentes, la información tiene errores y la trama es descartada.

| 8 bytes | 6 bytes | 6 bytes | 2 bytes | 1 byte | 1 byte | 1 byte | Variable | 4 bytes |
|---|---|---|---|---|---|---|---|---|
| Preamble | Destination Address | Source Address | Length | DSAP | SSAP | Control | Data | FCS |

Figura 2.17 Trama IEEE 802.3

#### 2.6.1.2 Fast Ethernet

Como resultado de la necesidad de una mayor tasa de transmisión, surge *Fast Ethernet* que opera a 100 Mbps con el mismo formato de la trama y técnica de acceso al medio que usa *Ethernet* a 10 Mbps. Además de la tasa de transmisión, tiene algunas diferencias como la autonegociación y el uso opcional de fibra óptica como medio de transmisión.

La recomendación 802.3u define tres tipos de implementación física para *Fast Ethernet*:

- 100baseTX: para UTP categoría 5, se usan dos pares trenzados para la transmisión y recepción de datos.
- 100baseT4: para UTP categoría 3, se emplean tres pares para la transmisión de datos, y uno para la señalización de éstos.
- 100baseFX: implementación sobre fibra multimodo, alcanzándose distancias de 400 metros en transmisión *half duplex* y 2 Km en transmisión *full duplex*.

La autonegociación es una característica opcional que habilita el intercambio de información entre dos dispositivos de acuerdo con sus recursos, ya sea a 10 ó a 100 Mbps. La autonegociación es ejecutada mediante el paso de información encapsulada en un tren de pulsos, éstos son los mismos usados por 10baseT para verificar la integridad del enlace.

Si una estación tiene un pulso sencillo, referido como NPL (*Normal Link Pulse*), ésta reconoce que el dispositivo en la otra punta sólo es capaz de manejar 10baseT. Si la autonegociación esta siendo usada por una estación, ésta transmitirá un tren de pulsos referidos como FLP (*Fast Link Pulse*). Un FLP consiste de 17 pulsos de reloj intercalados con 16 pulsos de señal para formar una palabra código de 16 bits. Si un pulso de señal ocurre entre dos pulsos de reloj, tal bit es 1, si no ocurre pulso de señal, tal bit es cero. La palabra código de 16 bits describe qué implementación de *Ethernet* es soportada, de tal forma que las estaciones en autonegociación seleccionan cual implementación se usará de acuerdo con las siguientes prioridades:

100BASE-TX *full duplex*
100BASE-T4 *half duplex*
100BASE-TX *half duplex*
10BASE-T *full duplex*
10BASE-T *half duplex*

#### 2.6.1.3 Gigabit Ethenet

Recién surge *Fast Ethernet* cuando las necesidades de mayores tasas de transmisión ya están en la puerta, para lo cual se desarrolla Gigabit Ethernet. La tasa de transmisión para esta tecnología es de 1000 Mbps (1Gbps) y se usa básicamente como *Backbone* (es la columna vertebral de una red) en redes LAN. La red Ethernet Gigabit ofrece nuevos modos de operación *full duplex*, para conexiones *switch* a *switch* y *switch* a estación terminal.

### 2.6.2 Tecnología Token Ring

La tecnología *Token Ring* es desarrollada originalmente por IBM en 1970 y es la segunda en popularidad después de *Ethernet*. La especificación 802.5 de la IEEE es casi

idéntica y totalmente compatible con *Token Ring*, operando a tasas de transmisión de 4 y 16 Mbps.

*Token Ring* utiliza una topología lógica del tipo anillo, donde la información circula en un solo sentido de éste. Para su implementación física usa unos dispositivos llamados MAU (*Multistation Access Unit*), los cuales concentra en una topología tipo estrella en la red.

Entre las funciones del MAU están el paso secuencial y rotatorio de información entre dispositivos conectados a éste (en un MAU o en múltiples MAU's conectados) y el uso de relevadores para desviar la información en caso de que un dispositivo sea sacado del anillo. Los cables usados para conectar los dispositivos a los MAU's son llamados cables “lobe", y los cables utilizados entre MAU's se denominan cables "patch", ambos hechos de cable UTP.

La tabla 2.2 muestra un comparativo entre *Token Ring* IBM e IEEE 802.5:

| | IBM Token Ring | IEEE 802.5 |
|---|---|---|
| Tasa de transmisión | 4 ó 16 Mbps | 4 ó 16 Mbps |
| Dispositivos por segmento | 260 (STP)<br>72 (UTP) | 250 |
| Topología física | Estrella | Estrella |
| Medios | Par trenzado | Par trenzado |
| Método de acceso | Token passing | Token passing |

Tabla 2.2 Comparación entre *Token Ring* e IEEE 802.5

La técnica de acceso al medio usada por *Token Ring* se conoce como *Token Passing*, y está clasificada como del tipo Round Robin. En esta técnica se mueve una pequeña trama llamado “*token*” a través del anillo y la posesión de éste garantiza el derecho a transmitir. Si un dispositivo recibe el *token* y no tiene nada que transmitir, simplemente

pasa el *token* al siguiente dispositivo en el anillo. Cada dispositivo solo puede mantener el *token* por un periodo máximo.

Cuando un dispositivo con información quiere transmitir, recibe el *token*, inserta en éste último nuevos campos de control, así como la información a transmitir y cambia el bit *token* para transformar el *token* en una trama de datos y/o control. Realizado lo anterior, transmite la información al siguiente dispositivo en el anillo. Cuando la trama generada llega a su destino final (identificado por la MAC destino), el dispositivo en cuestión reconoce la trama y la copia a su buffer retransmitiéndolo al siguiente dispositivo una vez que ha modificado los bits de "*address*" (para indicar que la trama llegó al destino final) y el bit "*copied*" (para indicar que la trama fue copiada por el dispositivo destino). Una vez que la trama llega al dispositivo que originalmente lo transmitió, éste lo retira del anillo y verifica el valor de los bits "*address*" y "*copied*" para saber si la transmisión fue exitosa. Si el dispositivo no tiene más información que transmitir o se ha terminado su tiempo máximo de transmisión, éste libera un nuevo *token* que envía al siguiente dispositivo en el anillo.

La trama *Token Ring* de datos o de control consta de los siguientes campos:

SD: de una longitud de un byte, indica el inicio de la trama y consiste de una señal patrón distinguible de los datos, codificada como JKOJKOOO, donde J y K son símbolos que no representan datos.

AC: con un byte de longitud, indica si la trama en curso es un *token* o una trama de datos, la prioridad de la trama y si el *token* ha sido reservado para transmisión. El formato de este campo es PPPTMRRR, donde PPP y RRR son tres bits que indican el nivel de prioridad o de reservación respectivamente. M es el bit de monitor y T indica si se trata de un *token* o una trama de datos.

FC: este campo de un byte indica si la trama en curso es del tipo LLC o de control. Su formato es FFZZZZZZ, donde F es un bit de tipo de trama y Z es un bit de control.

DA: 6 bytes que contienen la dirección MAC destino.

SA: 6 bytes que contienen la dirección MAC origen.

*Data*: contiene la información destinada a capas superiores.

FCS: 4 bytes que contienen el código generado por un proceso polinomial sobre los campos AC, FC, DA, SA y *Data*. La máquina receptora genera este código cuando recibe la trama y lo compara con el que recibe; si son iguales la información está correcta, si son diferentes, la información tiene errores y la trama es descartada.

ED: de un byte de longitud, contiene el bit de detección de errores (Error, E), el cual es encendido si cualquier repetidor encuentra un error en la trama; también contiene el bit de intermedio (*Intermediate*, I) que sirve para indicar que esta trama es uno de varios en una transmisión multiframe. El formato de este campo es JK1JK1IE.

FS: éste campo de un byte contiene los bits de dirección reconocida (*Address*, A) y el de la trama copiado (*Copied*, C), los cuales están incluidos dos veces para verificar errores en este campo, dado que éste no está abarcado por el FCS. Cuando una trama destinado a cierto dispositivo es reconocido por éste, el dispositivo pone en '1' el bit A. Si el dispositivo copia la trama a su buffer de memoria, también pone en '1' el bit C. El formato del campo es ACRRACRR, donde R es un bit reservado.

Un Token sólo posee los campos SD, AC y ED, tal y como se muestra en la figura 2.18.

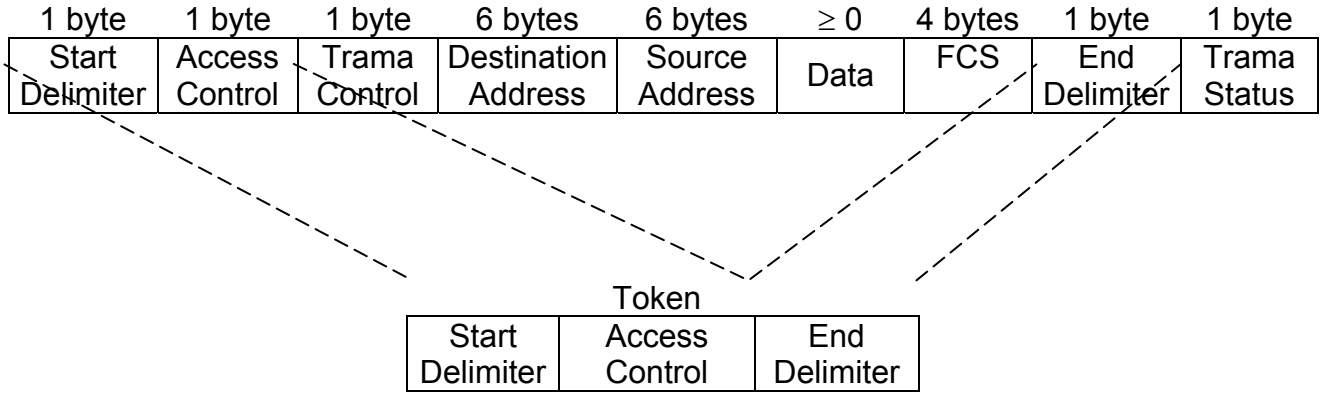



Figura 2.18 Trama del *Token Ring* y del *token*

La prioridad en *Token Ring* está diseñada para que estaciones con prioridades altas puedan utilizar un mayor número de veces el *token* para transmitir datos que aquellas con una prioridad baja.

Las reglas básicas son:

Cualquier estación que desee capturar el *token* podrá hacerlo sólo si la prioridad de éste es menor o igual a la prioridad de la estación. Si la prioridad del *token* es mayor que la de la estación, ésta deberá prender los bits de reservación con su nivel de prioridad para reservar el *token*, pudiéndolo hacer únicamente si ninguna estación con una prioridad mayor no lo ha reservado ya. Cualquier estación que eleve la prioridad del token deberá bajarla a su valor original la próxima vez que ésta vea un *token* libre, de tal forma que todo dispositivo tenga oportunidad de transmitir eventualmente.

### 2.6.3 Tecnología FDDI

FDDI (*Fiber Distributed Data Interface*) es un estándar para transmisión de datos en LANs que opera sobre fibra óptica a 100 Mbps. Fue definido en los años 80 por la ANSI (*America National Standards Institute*) ante la necesidad de contar con una tecnología para LANs de gran ancho de banda. Para alcanzar este objetivo fue necesaria la adopción de la fibra óptica como medio físico (la tecnología de cable de par trenzado estaba muy inmadura en la época que se definió el estándar), aunque elevara mucho los costos de instalación.

FDDI proporciona interconexión a alta velocidad entre redes LAN y WAN. Las principales aplicaciones es la interconexión de redes LAN Ethernet y de éstas con redes WAN X.25. Tanto en la conexión de estas tecnologías de red como con otras, todas se conectan directamente a la red principal FDDI. Otra aplicación es la interconexión de periféricos remotos de alta velocidad a ordenadores tipo mainframe.

La tecnología FDDI permite la transmisión de los datos a 100 Mbps, según la norma ANSI X3T9.5, con un esquema tolerante a fallos, flexible y escalable. Esta norma fue definida, originalmente, en 1982, para redes de hasta siete nodos y un Km de longitud, denominada LDDI (*Locally Distributed Data Interface*). Sin embargo, en 1986 fue modificada y publicada como borrador de la norma actual, e inmediatamente aprobada, aparecieron los primeros productos comerciales en 1990.

El método de acceso es similar al *Token Ring*, con la diferencia de que las estaciones negocian el tiempo de circulación y el tiempo de retención del *token* al conectarse con el resto de las estaciones de la red. El primero es el tiempo máximo que puede tardar el *toke*n en completar una vuelta al anillo y el segundo es el tiempo máximo que una estación puede retener el *token* para transmitir sus datos. Esto permite tener un retardo de red garantizado, y posibilita, en principio, el tránsito de datos sincrónico, característica que hace factible el envío de voz y video. Lamentablemente FDDI, no puede garantizar el acceso al medio a intervalos de tiempo constantes (el *token* puede estar en poder de otra estación) razón por la cual no permite la transmisión de datos asíncronos, como telefonía digital.

FDDI utiliza un protocolo de entrega de *tokens* múltiples. El *token* circula por la red detrás del último paquete transmitido desde un dispositivo. Si una estación desea enviar datos, captura el *token*, lo extraerá y colocara su paquete o paquetes en el anillo volviendo a colocar el *token* justo a continuación de la corriente de datos.

La topología de la red es de tipo anillo, similar al *Token Ring*; el cableado de la FDDI está constituido por dos anillos de fibras, uno transmitiendo en el sentido de las manecillas del reloj y el otro en sentido contrario, uno principal y otro de respaldo o *backup* (véase figura 2.19). El hecho de poseer dos anillos hace que la red FDDI sea altamente tolerante a fallas. El control de la red es distribuido, razón por la cual si falla un nodo real el resto recompone la red automáticamente.

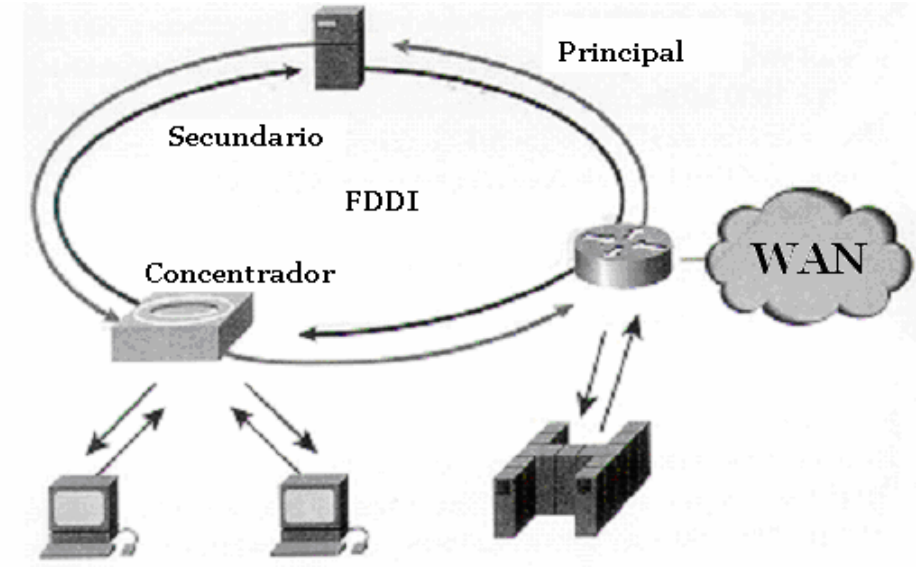



Figura 2.19 Topología de FDDI

Al igual que en *Token Ring* existen concentradores FDDI que convierten la topología de anillo en estrella, lo cual es más conveniente para realizar el cableado. En una red FDDI, pueden coexistir un máximo de 500 estaciones, distanciadas en un máximo de 2 Km y conectadas por medio de fibra óptica 62.5/125 μm, en una circunferencia máxima de 100 Km.

La tecnología permite el uso de fibra monomodo como multimodo. La distancia máxima entre las estaciones depende del tipo utilizado, siendo de 2.5 Km para fibra multimodo. Las estaciones de fibra multimodo son más baratas que las monomodo, pues éstas últimas deben utilizar láser en los transmisores y las primeras simplemente LED.
Se define como estación a cualquier equipo, concentrador, *bridge*, *brouter*, *router*, estación de trabajo, u otro dispositivo conectado a la red FDDI.

Los tipos de estaciones que componen una red FDDI son:

- DAS (*Dual Attachment Station*, Estación de Doble Conexión): estación que se conecta tanto al anillo primario como al anillo secundario.

- DAC (*Dual Attachment Concentrador*, Concentrador de Doble Conexión): concentrador que permite la conexión de dispositivos tipo SAS al anillo FDDI.
- SAS (*Single Attachment Station*, Estación de Una Conexión): estación que se conecta sólo al anillo primario a través de un DAC.

Las estaciones FDDI de clase A (DAS o DAC), usan ambos anillos, ya que tienen la capacidad de reconfigurarse en caso de interrupción del servicio en el primer anillo. Por el contrario, las estaciones de clase B (SAS), sólo pueden enlazarse al anillo primario, como solución de conexión de bajo costo, en el caso de equipos en los que no es crítica la interrupción del servicio. En la figura 2.20 se muestran los tipos de elementos que forman una red FDDI.

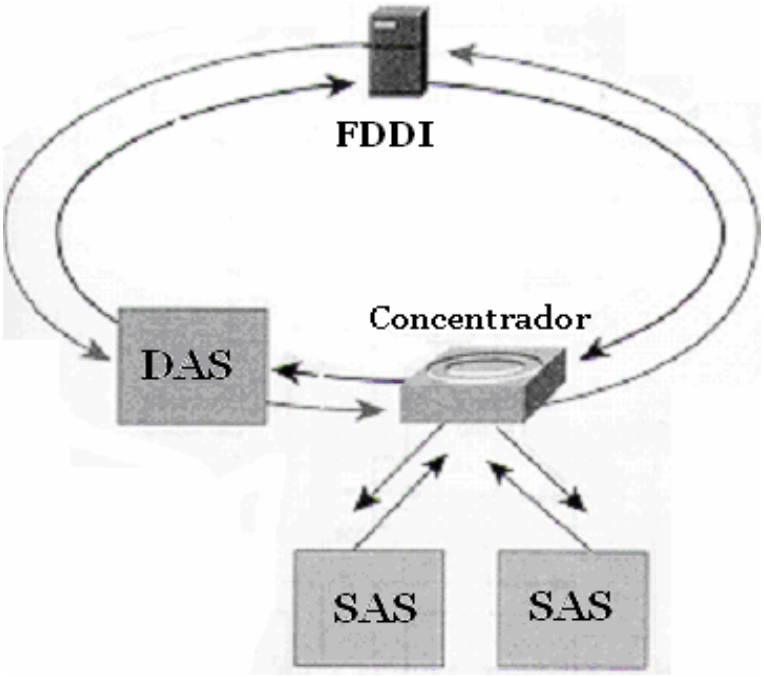



Figura 2.20 Elementos que forman una red FDDI

En la estructura FDDI se distinguen cuatro subcapas básicas (véase figura 2.21), cada una con funciones totalmente separadas:

- PMD (*Physical Media Dependent*, Dependencia del Medio Físico): especifica las señales ópticas y formas de onda a circular por el cableado, incluyendo las

especificaciones de éste, así como las de los conectores, por ello es la responsable de definir la distancia máxima de 2 Km. Entre estaciones FDDI y el tipo de cable multimodo con un mínimo de 500 MHz y LEDs transmisores de 1300 nm. Estas especificaciones se cumplen en los cables de 62.5/125 μm y por la mayoría de los cables de 50/125 μm. La atenuación máxima admitida en el anillo FDDI es de 11 decibeles (dB) de extremo a extremo, típicamente referenciada a 2.5 dB por Km. Corresponde con la mitad inferior de la capa uno (capa de enlace físico) del modelo OSI. Existe también una especificación de fibra monomodo, que emplea detectores/transmisores láser para distancias de hasta 60 Km entre estaciones.

- PHY (*Physical Layer Protocol*, Protocolo de la Capa Física): se encarga de la codificación y decodificación de las señales, además de la sincronización, mediante el esquema 4-bytes/5-bytes, que otorga una eficiencia del 80%, a una velocidad de señalización de 125 MHz, con paquetes de un máximo de 4500 bytes, además de que proporciona la sincronización distribuida. Corresponde con la mitad superior de la capa uno del modelo OSI.

- MAC (*Media Access Control*, Control de Acceso al Medio): su función es la programación y transferencia de datos hacia y desde el anillo FDDI, así como la estructuración de los paquetes, reconocimiento de direcciones de estaciones, transmisión del *token*, además de la generación y verificación de secuencias de control de tramas. Corresponde con la mitad inferior de la capa dos del modelo OSI (capa de enlace de datos).

- SMT (*Station Management*, Gestión de Estaciones): se encarga de la configuración inicial del anillo FDDI, monitoreo y recuperación de errores. Incluye los servicios y funciones basadas en tramas, así como la gestión de conexión (*Connection Management*, CMT), y la gestión del anillo (*Ring Management*, RMT). Se agrupa con las otras tres subcapas FDDI.

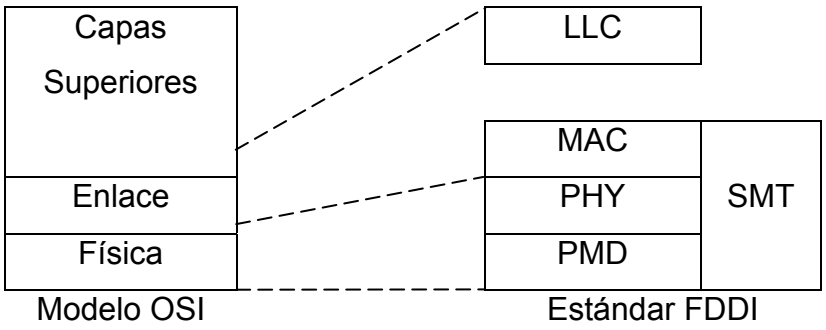



Figura 2.21 Arquitectura FDDI

La máxima longitud de la trama FDDI es limitada por 9000 símbolos ó 4500 bytes para tener sincronización. La longitud máxima de 4500 bytes es determinada por la codificación empleada, denominada 4B/5B (4 bytes/5 bytes), con una frecuencia de reloj de 125 MHz, siendo por tanto la eficiencia del 80%.

El formato de la trama FDDI se muestra en la figura 2.22, donde:

*Preamble*: cuatro o más símbolos de *Idle* (para sincronización).
SD: delimitador de inicio (utiliza los símbolos "J" y "K").
FC: control de la trama. Tipo de la trama (síncrona o asíncrona).
DA: 6 bytes que contienen la dirección MAC destino.
SA: 6 bytes que contienen la dirección MAC origen.
Data: información (N bytes).
FCS: redundancia de la trama (con CRC-32).
ED: delimitador del final (Utiliza el símbolo "T").
FS: estado de la trama. (Trama erróneo, bien recibida, entre otras).

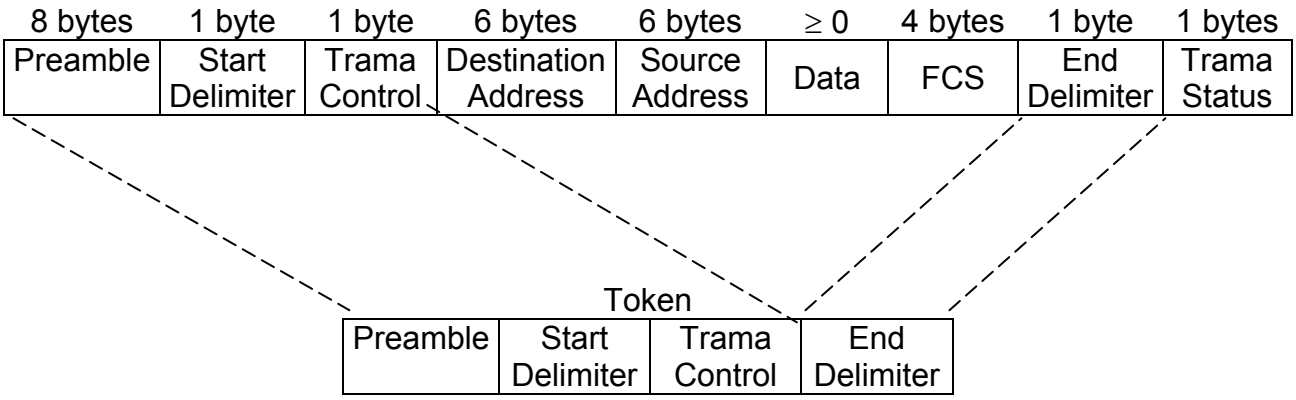



Figura 2.22 Formato de la trama de FDDI

## 2.7 Equipos de Interconexión

Los equipos de Interconexión son dispositivos que se utilizan para conectar redes LAN y/o WAN; y que son los siguientes: repetidor, *hub*, *bridge*, *switch*, *router* y *gateway*.

### 2.7.1 Repetidor

Son equipos que trabajan a nivel físico; prolongan la longitud de la red, unen segmentos de red, amplifica la señal, pero junto con ella también se amplifica el ruido. La red sigue como una sola, con lo cual, siguen las limitaciones en cuanto al número de estaciones que pueden compartir el medio. Los repetidores sólo se pueden utilizar para extender redes bajo una misma tecnología de red. Una desventaja de los repetidores, es el hecho de que extienden el dominio de *broadcast* de una red, esto ocasiona que el número de colisiones aumente, así como también el tráfico.

### 2.7.2 Hub

Son equipos que permiten estructurar el cableado de las redes. En un principio eran solo concentradores de cableado, pero cada vez se dispuso de mayor número de

capacidades, como aislamiento de tramos de red, capacidad de conmutación de las salidas para aumentar la capacidad de la red, gestión remota, etc. La ventaja de este tipo de dispositivos es que aísla los puertos que se encuentran dañados o sin conexión y permite que el resto de sus puertos continúe trabajando sin ningún problema.

### 2.7.3 Bridge

Son equipos que unen dos redes, trabajan sobre los protocolos de bajo nivel (Control de Acceso al Medio). Estos dispositivos filtran el tráfico en función de una tabla de direcciones físicas que ellos mismos se encargan de actualizar de forma dinámica. Esta tabla se guarda en memoria y se compone de tantas columnas como puertos tenga el *bridge*. En cada columna se encuentra las direcciones físicas de los dispositivos conectados al puerto correspondiente. El *bridge* produce señales, con lo cual no se transmite ruido a través de ellos. Al igual que el repetidor, el *bridge* se utiliza para redes con la misma tecnología de red.

### 2.7.4 Switch

El *switch* es un conmutador que tiene funciones de nivel 2 del modelo OSI, se parece a un *bridge* en cuanto a su funcionamiento. Sin embargo, tiene algunas características que lo distinguen: la velocidad de operación del *switch* es mayor que la del *bridge*, que introduce mayores tiempos de retardo; en un switch se puede repartir el ancho de banda de la red de una manera apropiada en cada segmento de red o en cada nodo, de modo transparente a los usuarios, esto proporciona facilidades para la construcción de redes virtuales.

Algunos conmutadores no sólo interconectan segmentos de red del mismo nodo, sino que son capaces de realizar la integración de distintos tipos de redes. En este sentido, existen conmutadores modulares con un bus interno de mayor ancho de banda que

integran *Ethernet*, *Token Ring*, FDDI, ATM, etc., permitiéndose incluso pequeños cambios de protocolos, siempre que se operen en el nivel 2.

### 2.7.5 Router

Es un equipo de interconexión de red que opera en la capa de red del modelo OSI. Utiliza varios sistemas de interconexión que mejora el rendimiento de la transmisión entre redes; su funcionamiento es más lento que el *bridge* pero su capacidad es mayor. Permite, incluso, enlazar dos redes que utilizan protocolos diferentes. Puesto que el *router* es un dispositivo de capa 3, pueden servirse del direccionamiento lógico para conducir los paquetes por las distintas redes que conecta. El *router* divide la red en subredes lógicas, y mantiene su propio tráfico local. El *router* delimita los dominios de *broadcast*.

### 2.7.6 Gateway

Son equipos para interconectar redes con protocolos y arquitecturas completamente diferentes a todos los niveles de comunicación. Los *gateways* operan en las capas superiores del modelo OSI (capas 4,5,6 y 7). El *gateway* se ubica normalmente en segmentos principalmente de alta velocidad, como las redes FDDI, donde conectan un sistema central o de microcomputadoras con redes LAN, que a su vez, están conectadas al segmento principal FDDI por medio del *router*.

## 2.8 Métodos de Transmisión de Datos en LAN

La transmisión de datos en redes LAN tiene tres clasificaciones: *unicast*, *multicast* y *broadcast*. En cada tipo de transmisión, se envía un solo paquete a uno o más nodos que están en los segmentos de red.

- Transmisión *unicast*: se envía el paquete de un nodo origen a un nodo destino de la red. Primero, el nodo origen direcciona el paquete utilizando la dirección del nodo destino y es enviado a los segmentos de red, después, la red transfiere el paquete al nodo destino.
- Transmisión *multicast*: constan de un paquete de datos que se copia y envía, a un subconjunto específico de nodos en la red. Primero, el nodo origen direcciona el paquete utilizando una dirección de *multicast*. Después, el paquete es enviado a través de los segmentos de red, los cuales generan copias del paquete, y envía estas copias a cada uno de los nodos que se indican en la dirección de *multicast*.
- Transmisión *broadcast*: constan de un paquete de datos que se copia y envía, a todos los nodos de los segmentos de red. En este tipo de transmisión, el nodo origen dirige el paquete utilizando la dirección de *broadcast*. El paquete es, después, enviado a través de los segmentos de red, los cuales hacen copias del paquete y los envía a cada uno de los nodos de los segmentos de red.

### 2.8.1 Dominio de Colisión

El dominio de colisión es un grupo de *hosts* conectados a los segmentos de red; si dos o más de ellos envían una trama a los segmentos al mismo tiempo, se produce una colisión. En tecnologías LAN como son *Token Ring* y FDDI son del tipo determinista, al contrario de la de *Ethernet* y como consecuencia no se producen colisiones, por tanto no hay dominio de colisiones en *Token Ring* y FDDI.

Los repetidores y *hubs* (véase figura 2.23 y 2.24) reproducen la información que reciben de un puerto y la propagan a los demás puertos, lo que provoca que todos estén en el mismo dominio de colisión.

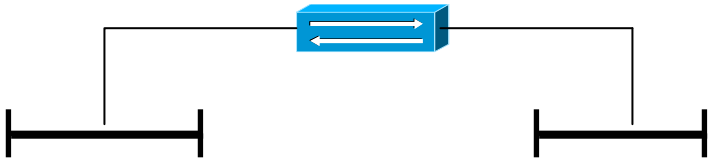


Figura 2.23 Repetidor 2 puertos, 1 solo dominio de colisión

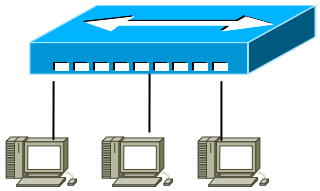


Figura 2.24 *Hub* n puertos, 1 solo dominio de colisión

Los *bridges*, *switches* y *routers* (véase figura 2.25, 2.26 y 2.27), limitan el dominio de colisión generando n dominios de colisión con base en el número de puertos.

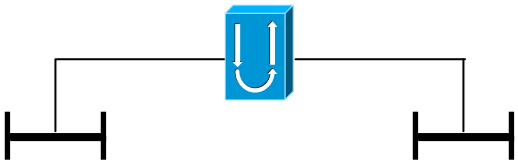


Figura 2.25 *Brigde* 2 puertos, 2 dominios de colisión

Figura 2.26 *Switch* n puertos, n dominios de colisión

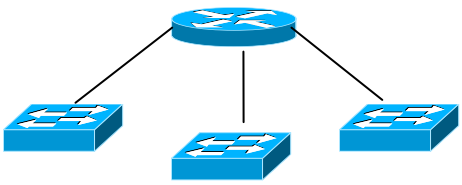


Figura 2.27 *Router* n puertos, n dominios de colisión

### 2.8.2 Dominio de Broadcast

El dominio de *broadcast* es un grupo de hosts conectados a los segmentos de red; si uno de los *hosts* genera *broadcast*, el resto lo recibe.

Los repetidores, *hubs*, *bridges* y *switches* (véase figura 2.28, 2.29, 2.30 y 2.31) propagan los *broadcast* que son recibidos en cualquiera de sus puertos a los demás puertos, lo que provoca que todos los puertos estén en el mismo dominio de *broadcast*.

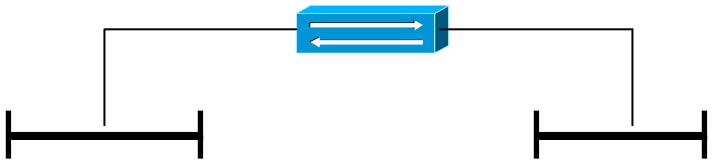


Figura 2.28 Repetidor 2 puertos, 1 solo dominio de *broadcast*

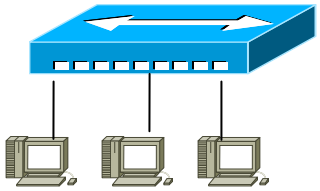


Figura 2.29 *Hub* n puertos, 1 solo dominio de *broadcast*

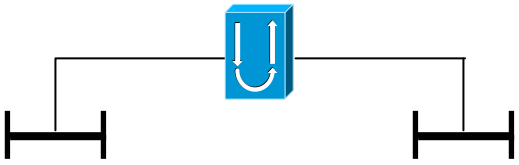


Figura 2.30 *Brigde* 2 puertos, 1 solo dominio de *broadcast*

Figura 2.31 *Switch* n puertos, 1 solo dominio de *broadcast*

Los *routers* (véase figura 2.32) limitan el dominio de *broadcast* generando n dominios de *broadcast* en base al número de puertos.

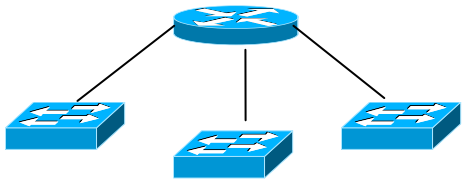


Figura 2.32 *Router* n puertos, n dominios de *broadcast*

## 2.9 Conceptos de TCP/IP

En 1973, la DARPA (*Defense Advanced Research Proyects Agency*, Agencia de Proyectos de Investigación Avanzada para la Defensa) de los Estados Unidos, inició un programa para la investigación de tecnologías que permitieran la transmisión de paquetes de información entre redes de diferentes tipos y características. El proyecto tenía por objetivo la interconexión de redes, por lo que se le denominó "*Internetting*", y a la familia de redes de computadoras que surgió de esta investigación se le denominó "Internet". Los protocolos desarrollados se englobaron en un conjunto de protocolos denominados TCP/IP (*Transmission Control Protocol*/*Internet Protocol*, Protocolo de Control de Transmisión/Protocolo de Internet).

TCP/IP se ha convertido en el lenguaje común del mundo de las conexiones entre redes y es el conjunto de protocolos que más se utiliza en las redes; también es el pilar donde se asienta Internet. Muchos sistemas operativos de red, como NT (*New Technology*, Nueva Tecnología) 4.0 *Server*, *Windows* 2000 *Server* y Novell *Netware* 5.0, utilizan TCP/IP como protocolo de red predeterminado. TCP/IP se desarrolló en la década de los setenta, por lo que se anticipó a la conclusión del modelo OSI. Esto significa que los distintos protocolos que incluye la pila TCP/IP no corresponde exactamente con una capa única del modelo OSI (véase figura 2.33).

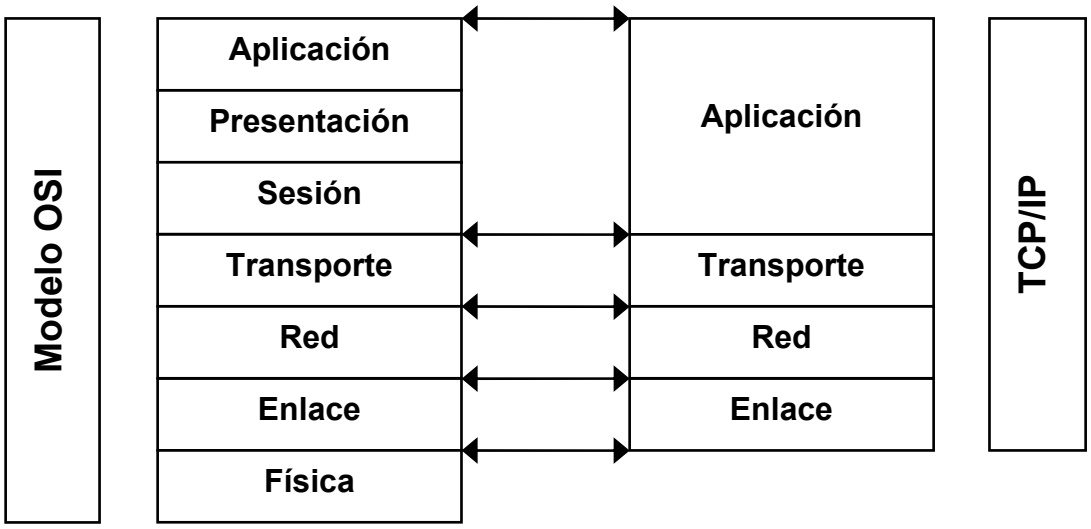



Figura 2.33 El modelo OSI y TCP/IP

### 2.9.1 Capa de Aplicación

Los protocolos de la capa de aplicación proporcionan la interfaz de usuario para los distintos protocolos y aplicaciones que acceden a la red. Los protocolos de la capa de aplicación en la pila TCP/IP administran la transferencia de archivos, la conexión con otros nodos, los servicios de correo electrónico y el control de la red.

Algunos ejemplos de protocolos residentes en esta capa son los siguientes:

- FTP (*File Transfer Protocol*, Protocolo de Transferencia de Archivos): es un protocolo que permite transferir archivos entre dos computadoras. El FTP en realidad es, una aplicación que se puede descargar desde Internet y utilizarlo para mover archivos entre varias computadoras.
- TFTP (*Trivial File Transfer Protocol*, Protocolo de Transferencia de Archivos Trivial): es una versión reducida de FTP que permite mover archivos sin ningún tipo de autenticación (es decir, sin nombre de usuario ni contraseña).
- SMTP (*Simple Mail Transfer Protocol*, Protocolo de Transporte de Correo Simple): es un protocolo que permite la entrega de mensajes de correo electrónico entre

dos computadoras. Este protocolo, lo soportan los clientes de correo electrónico y se utiliza para enviar y/o recibir mensajes en Internet.

- SNMP (*Simple Network Management Protocol*, Protocolo Simple de Administración de Red): es un protocolo que permite recopilar información de dispositivos en la red. SNMP utiliza agentes (vigilantes de software que supervisan los procesos de red) para recoger datos relativos al estado que guardan los dispositivos.
- *Telnet*: es un protocolo de emulación de terminal que permite conectar una computadora local con una computadora remota (u otros dispositivos). La computadora local se convierte en una terminal virtual que tiene acceso a las aplicaciones y demás recursos que incorpora la computadora remota.

### 2.9.2 Capa de Transporte

Los protocolos de la capa de transporte controlan el flujo y la confiabilidad de la conexión cuando los datos se transmiten de una computadora emisora a otra receptora. Esta capa toma los datos de los protocolos de la capa de aplicación e inicia un proceso de lectura de los mismos para transmitirlos por la red. La capa de transporte incluye dos protocolos de la pila de protocolos TCP/IP: TCP y UDP.

- TCP (*Transmission Control Protocol*, Protocolo de Control de Transmisión): es un protocolo orientado a conexión que proporciona un circuito virtual. TCP toma los datos de los protocolos de la capa de aplicación y los divide en fragmentos, después se asegura de que vuelven a ensamblarse correctamente en la computadora receptora. TCP requiere que en la computadora emisora y receptora se establezca una conexión sincronizada.
- UDP (*User Datagram Protocol*, Protocolo de Datagramas de Usuario) es un protocolo de transporte sin conexión que proporciona una conexión entre los protocolos de la capa de aplicación que no requieren aceptación ni sincronización.

### 2.9.3 Capa de Red

La capa de red se encarga de encaminar los datos a través de rutas lógicas de red y proporciona un sistema de direccionamiento a las capas superiores del modelo. Esta capa también define el formato de paquete que debe utilizarse en los datos que se transmiten por la red. Una tarea importante de la capa de red es la resolución (o conversión) de direcciones lógicas (direcciones IP) en direcciones físicas (MAC) de los nodos en la red.

- IP (*Internet Protocol*, Protocolo Internet): es el protocolo que proporciona el servicio de envío de paquetes para los protocolos soportados TCP, UDP e ICMP. IP es el protocolo encargado de fragmentar, reensamblar y llevar la información de los protocolos superiores de la estación origen a la destino a través de distintas redes.
- ICMP (*Internet Control Message Protocol*, Protocolo de Mensajes de Control de Internet): es el protocolo responsable de proporcionar información de control sobre la capa de red. También se encarga de informar a la máquina origen de los posibles errores IP que puedan surgir a lo largo del tránsito de un paquete. Facilita, asimismo, un sistema de gestión de encaminamiento y control de flujo. ICMP se utiliza básicamente como protocolo de soporte para el direccionamiento IP.
- ARP (*Address Resolution Protocol*, Protocolo de Resolución de Direcciones): es el protocolo encargado de convertir las direcciones IP en direcciones físicas. Este protocolo utiliza una tabla denominada “Tabla de Direcciones ARP”, que contiene la correspondencia entre dirección IP y direcciones físicas utilizadas recientemente. Si la dirección buscada no esta en la tabla, el protocolo envía un mensaje a toda la red.
- RARP (*Reverse Address Resolution Protocol*, Protocolo de Resolución de Direcciones Inverso): es el protocolo encargado de traducir direcciones físicas en direcciones IP.

### 2.9.4 Capa de Enlace

Es la capa de nivel inferior de TCP/IP, y es responsable de aceptar los datagramas IP y transmitirlos hacia una red específica. La capa de enlace también es responsable de proveer los siguientes servicios: delimitar el principio y fin de las tramas a ser enviados, establece el sistema de direccionamiento físico de la red y detecta los errores de envío o recepción de información entre dos o más computadoras.

## 2.10 Direccionamiento IP

Al igual que con cualquier otro protocolo de la capa de red, el esquema de direccionamiento IP es fundamental en el proceso de ruteo de los datagramas a través de la red. Cada dirección IP tiene componentes específicos y sigue un formato básico. Esta dirección es única para cada *host* que se comunica mediante TCP/IP.

Las direcciones IP tienen una longitud de 32 bits y consta de dos partes:

- La dirección de red: es la parte de la dirección IP destinada para asignar la dirección de la red a la cual pertenece el *host*.
- La dirección de *host*: identifica una estación de trabajo, servidor, *router* u otro dispositivo TCP/IP dentro de un segmento de red. En otras palabras, todo dispositivo que necesite enviar y recibir datagramas o paquetes IP, se debe diferenciar con una dirección de *host* y debe ser ubicado en un segmento de red.

La dirección IP de 32 bits, está segmentada en 4 octetos de 8 bits (véase figura 2.34); cada bit en el octeto tiene un peso binario (128, 64, 32, 16, 8, 4, 2, 1). El valor mínimo de un octeto es 0, y el valor máximo de un octeto es 255. Estos octetos se convierten a formato decimal (sistema numérico de base 10) y se separan con puntos.

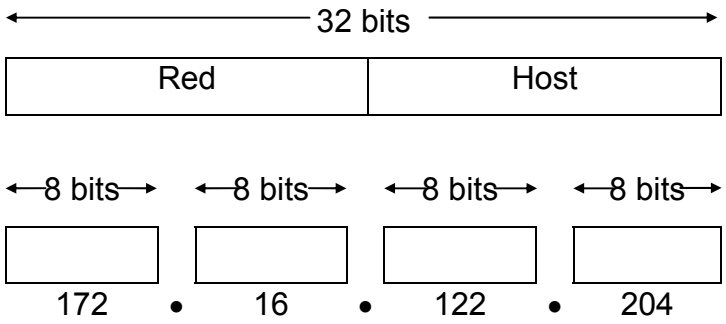



Figura 2.34 Esquema de direccionamiento IP

Para conseguir mayor funcionalidad podemos dividir nuestra red en subredes dividiendo en dos partes la dirección de *host*, una para identificar la subred, y la otra para identificar la máquina (*subnetting*).

### 2.10.1 Clases de Direcciones en IP

El direccionamiento IP soporta cinco diferentes clases de direcciones: A, B, C, D y E (véase tabla 2.3). Solamente las clases A, B y C están disponibles para uso comercial. Los bits más a la izquierda (el primer octeto de la izquierda) indican de qué clase de red se trata.

| Clase de direcciones IP | Formato | Propósito | Bit(s) de orden superior | Rango de direcciones | Rango máximo de *Hosts* |
|---|---|---|---|---|---|
| A | N.H.H.H | Para pocas organizaciones grandes | 0 | 1.0.0.0 a 126.0.0.0 | 16,777,214 ($2^{24}$ - 2) |
| B | N.N.H.H | Para organizaciones de tamaño mediano | 1,0 | 128.1.0.0 a 191.254.0.0 | 65,534 ($2^{16}$ - 2) |
| C | N.N.N.H | Para organizaciones relativamente pequeñas | 1,1,0 | 192.0.1.0 a 223.255.254.0 | 254 ($2^{8}$ - 2) |

| | | | | | |
|---|---|---|---|---|---|
| D | N/A | Grupos de *multicast* (RFC 1112) | 1,1,1,0 | 244.0.0.0 a 239.255.255.255 | N/A |
| E | N/A | Experimental | 1,1,1,1 | 240.0.0.0 a 254.255.255.255 | N/A |

N = *Network* (Red), H = *Host*, N/A = No aplica

Tabla 2.3 Clases de direcciones en IP

### 2.10.2 Máscara de Subred IP

Otro aspecto fundamental que determina el funcionamiento del direccionamiento IP es el uso de máscaras de subred. La máscara de subred para una determinada dirección IP es lo que permite al *router* saber qué parte de la dirección IP se refiere a la dirección de red y qué parte de la dirección apunta a la dirección de *host*. Las máscaras básicas de subred para cada clase se muestran en la tabla 2.4.

| Clase | Máscara de subred |
|---|---|
| A | 255.0.0.0 |
| B | 255.255.0.0 |
| C | 255.255.255.0 |

Tabla 2.4 Máscaras básicas de subred

Las máscaras de subred utilizan el mismo formato y técnica de representación que las direcciones IP. Sin embargo, la máscara de subred tiene 1s binarios en todos los bits, los cuales especifican los campos de red y subred, y 0s binarios en todos los bits que especifican el campo de *host*, como se muestra en la figura 2.35.

| | Red | Red | Subred | Host |
|---|---|---|---|---|
| Representación binaria | 11111111 | 11111111 | 11111111 | 00000000 |
| Representación decimal de puntos | 255 • | 255 • | 255 • | 0 |

Figura 2.35 Ejemplo de una máscara de subred para una dirección clase B

Los bits de la máscara de subred deben provenir de los bits de orden superior (los que están más a la izquierda) del campo de *host*, como se muestra en la figura 2.36.

| 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | = | 128 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | = | 192 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | = | 224 |
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | = | 240 |
| 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | = | 248 |
| 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | = | 252 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | = | 254 |
| 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | = | 255 |

Figura 2.36

La máscara de subred predeterminada para la dirección clase B que no tiene subred es 255.255.0.0, en tanto que la máscara de subred para una dirección clase B por ejemplo la 171.16.0.0, que especifica 8 bits de subred, es 255.255.255.0. Lo que permite manejar 8 bits de subred ó $2^8$ -2 (1 para la dirección de la red y 1 para la dirección de *broadcast*) = 254 subredes posibles, con $2^8$ –2 = 254 *hosts* por subred (véase tabla 2.5).

La máscara de subred para una dirección clase C por ejemplo 192.168.2.0, que especifica 5 bits de subred es 255.255.255.248. Con 5 bits disponibles para la subred, $2^5$ –2 = 30 subredes posibles, con $2^3$ –2 = 6 *hosts* por subred. Los diagramas de referencia que se muestran a continuación se pueden utilizar al planear las redes clase B y clase C para determinar el número de subredes y de *hosts* que se requieren y la máscara de subred correspondiente (véase tabla 2.6).

| Número de bits | Máscara de subred | Número de subredes | Número de *hosts* |
|---|---|---|---|
| 2 | 255.255.192.0 | 2 | 16382 |
| 3 | 255.255.224.0 | 6 | 8190 |
| 4 | 255.255.240.0 | 14 | 4094 |
| 5 | 255.255.248.0 | 30 | 2046 |
| 6 | 255.255.252.0 | 62 | 1022 |
| 7 | 255.255.254.0 | 126 | 510 |
| 8 | 255.255.255.0 | 254 | 254 |
| 9 | 255.255.255.128 | 510 | 126 |
| 10 | 255.255.255.192 | 1022 | 62 |
| 11 | 255.255.255.224 | 2046 | 30 |
| 12 | 255.255.255.240 | 4094 | 14 |
| 13 | 255.255.255.248 | 8190 | 6 |
| 14 | 255.255.255.252 | 16382 | 2 |

Tabla 2.5 Referencia para la subred clase B

| Número de bits | Máscara de subred | Número de subredes | Número de *hosts* |
|---|---|---|---|
| 2 | 255.255.255.192 | 2 | 62 |
| 3 | 255.255.255.224 | 6 | 30 |
| 4 | 255.255.255.240 | 14 | 14 |
| 5 | 255.255.255.248 | 30 | 6 |
| 6 | 255.255.255.252 | 62 | 2 |

Tabla 2.6 Referencia para la subred clase C

## 2.11 Administración de Redes

La administración de la red es un servicio que utiliza una gran variedad de herramientas, aplicaciones y dispositivos para ayudar a los administradores de la red a supervisar y mantener en operación las redes. La mayoría de las arquitecturas de administración de la red utilizan el mismo conjunto de relaciones y estructura básica, éstos pueden ser Dispositivos Administrados (*Managed Devices*) que son dispositivos críticos en el funcionamiento y desempeño de una red, pueden ir desde computadoras hasta *switches*, y las Entidades de Administración (*Management Entities*) que son sistemas capaces de detectar problemas e informar acerca del desempeño de los dispositivos de una red (véase figura 2.37).

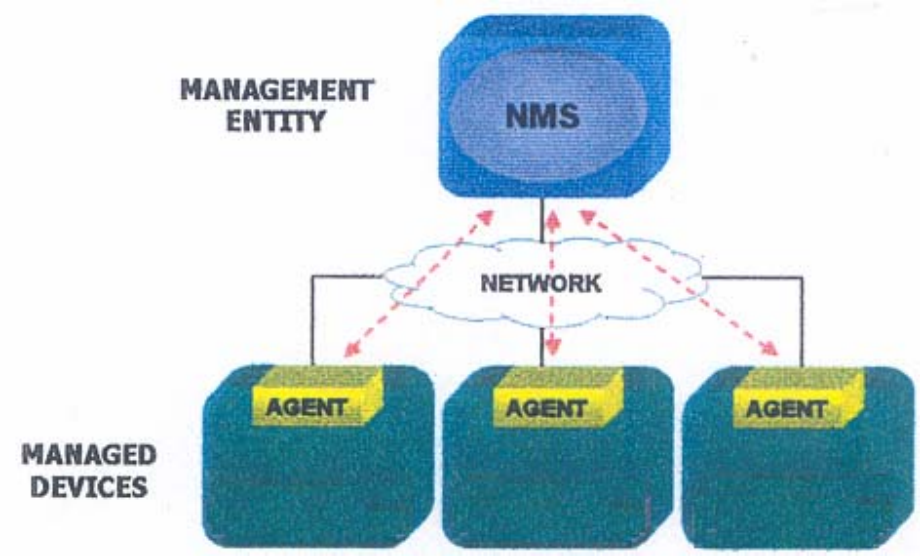



Figura 2.37 Diagrama del Sistema de Administración de Red

Las entidades de administración también pueden sondear a las estaciones terminales para verificar los valores de determinadas variables. El sondeo puede ser automático o iniciado por el usuario, pero los agentes en los dispositivos que se están administrando responden a todos los sondeos.

Los agentes son módulos de software que, en primer lugar, compilan información acerca de los dispositivos administrados en los que residen, después almacenan esta información en una base de datos de administración y, por último, la ponen a disposición de las entidades de administración que forman parte de los NMS (*Network Management System*, Sistema de Administración de Red) vía un protocolo de administración de red.

Entre los protocolos más conocidos de administración de redes están SNMP, RMON (*Remote Monitoring*, Monitorización Remota) y CMIS/CMIP (*Common Management Information Services/Common Management Information Protocol*, Servicios de Información de Administración Común/Protocolo de Información de Administración Común).

### 2.11.1 Modelo ISO de Administración de Redes

La ISO (*International Standards Organization*, Organización Internacional de Estándares y Normas) ha contribuido en gran medida a la estandarización de las redes. Su modelo de administración de redes es el medio que ayuda a comprender las funciones de los sistemas de administración de redes.

Este modelo consta de cinco áreas:

- Administración de desempeño: sus funciones principales son medir los parámetros de desempeño de una red y sus recursos.
- Administración de la configuración: se encarga del control, monitoreo y mantenimiento de las versiones de hardware y software instaladas en los dispositivos.
- Administración de la contabilidad: mide los parámetros de utilización de los recursos de una red y regula el uso de los recursos a los usuarios.
- Administración de fallas: detecta, registra, notifica y soluciona los problemas que se presentan en la red.

- Administración de la seguridad: las actividades que se deben llevar a cabo son la identificación de los recursos de la red con carácter crítico, determinación de las constantes de uso de los recursos de carácter crítico por parte de los usuarios de la red, monitoreo de los puntos de acceso a los recursos críticos de la red y el registro de todo tipo de acceso a recursos críticos, principalmente los no autorizados.

### 2.11.2 Arquitecturas de los NMS

Las arquitecturas que se pueden implementar para los NMS son las siguientes:

- Arquitectura Centralizada: el sistema de administración, se encuentra únicamente en una computadora. Esto es, el sistema de administración recibe todas las alarmas y eventos de la red, almacena toda la información acerca de la red, y hospeda a todas las aplicaciones (véase figura 2.38).

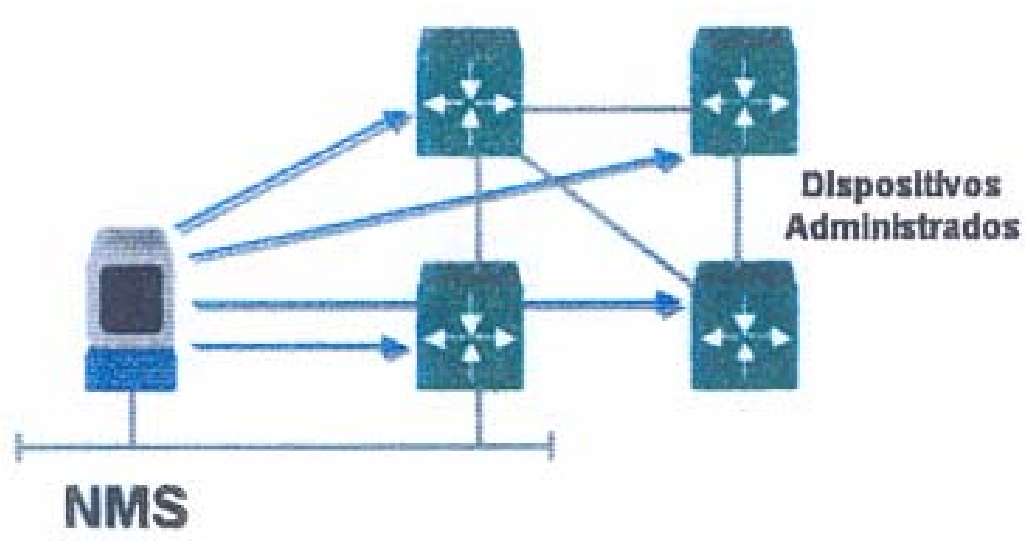



Figura 2.38 Arquitectura Centralizada

- Arquitectura Jerárquica: el sistema de administración se encuentra en varios equipos, donde uno de ellos actúa como sistema central. Esto es, no depende de un solo sistema, administra de forma distribuida (menor carga en el punto central), y la información que se recolecta se almacena en una base de datos central (véase figura 2.39).

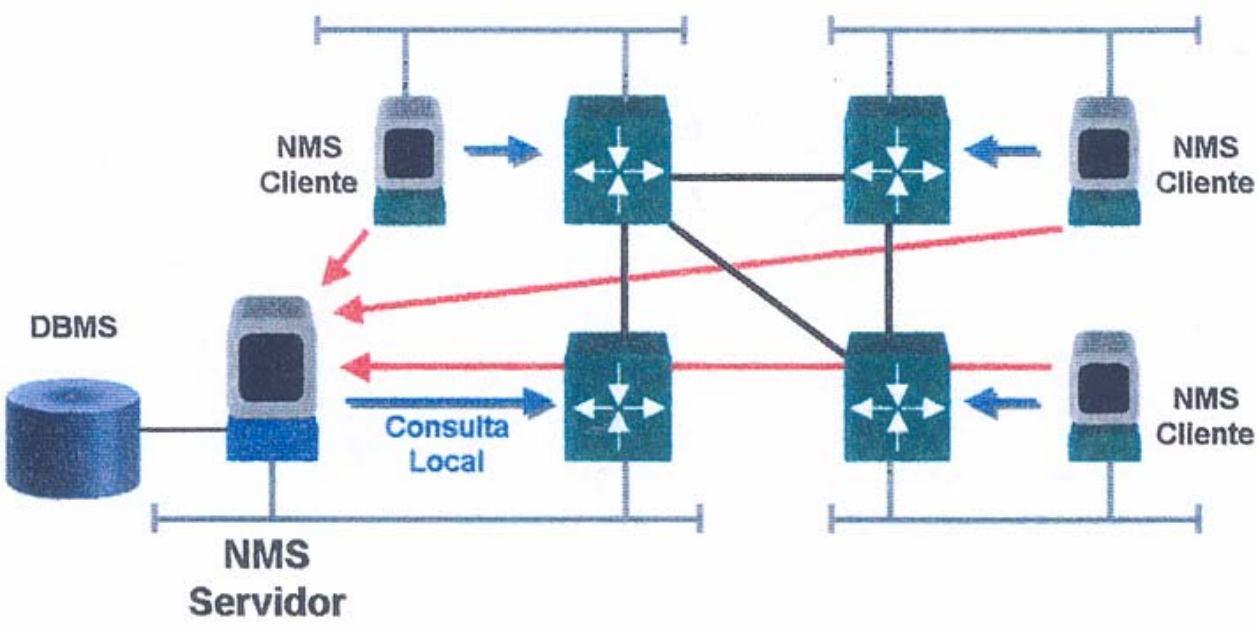



Figura 2.39 Arquitectura Jerárquica

- Arquitectura Distribuida: es una combinación de la arquitectura centralizada y la arquitectura jerárquica. Esto es, no depende de un solo sistema, mantiene funciones de administración distribuida, conserva un sólo lugar para obtener la información de alarmas y eventos de la red (véase figura 2.40).

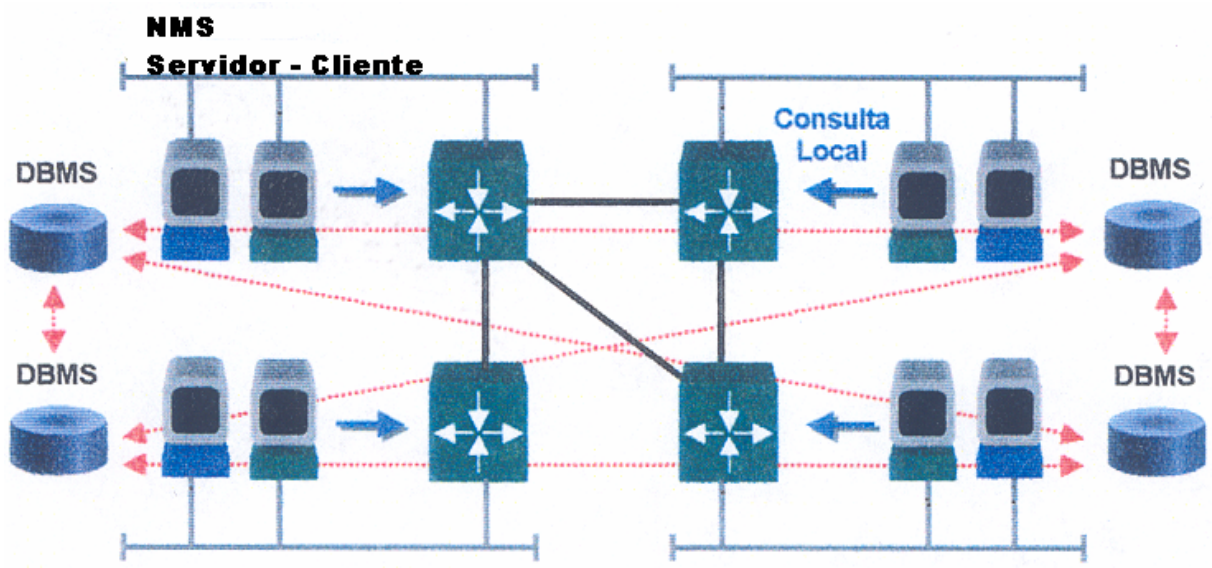



Figura 2.40 Arquitectura Distribuida

## 2.12 LANs Virtuales

Los modelos de red basados en compartir ancho de banda, presentes en las arquitecturas LAN a principios de los noventa, carecen de mejora para proporcionar los cada vez mayores anchos de banda que requieren las aplicaciones multimedia. Por lo que se necesitan nuevas implementaciones capaces de satisfacer creciente necesidad de ancho de banda, y también para soportar el crecimiento de usuarios en la red.

En las LAN basadas en compartir ancho de banda, los usuarios comparten un único canal de comunicaciones, de modo que todo el ancho de banda de la red se asigna al equipo emisor de información, quedando el resto de equipos en situación de espera. Para aumentar el ancho de banda disponible para cada usuario, se puede optar por la segmentación de su red.

### 2.12.1 Conmutación LAN

La técnica idónea para proporcionar elevados anchos de banda es la conmutación. Mediante esta técnica, cada estación de trabajo y cada servidor poseen una conexión dedicada dentro de la red, con lo que se consigue aumentar considerablemente el ancho de banda a disposición de cada usuario.

Las LANs basadas en compartir ancho de banda se configuran mediante *hubs* y *routers*. En una LAN conmutada, la función tradicional del *router* pasa a ser realizada por el conmutador LAN, quedando aquél destinado a funciones relacionadas con la mejora de las prestaciones en lo que respecta a la administración de la red.

Los conmutadores pueden realizar su función de dos modos diferentes:

- Cortar-continuar: dado que la dirección destino está en la primera parte de paquete, el reenvío del mismo puede iniciarse antes incluso de que el paquete entero haya sido recibido por el conmutador, y en ello se basa el método cortar-continuar (*cut-through*). Es decir, el paquete se examina tan pronto como se ha podido recibir la parte donde está la dirección destino, al mismo tiempo continúa recibiendo el resto del paquete. En el momento en que se ha podido decidir sí ha de ser reenviado o filtrado, se puede iniciar su transmisión, aunque no haya sido recibido en su totalidad.
- Almacenar-transmitir: cuando se emplea la técnica de almacenar y transmitir (*store-and-forward*), el conmutador recibe el paquete completo, lo almacena en su memoria interna y lo examina por entero antes de decidir sí debe de ser transmitido o filtrado.

Sin embargo, el continuo despliegue de conmutadores, divide la red en más y más segmentos, y no reduce el contenido de *broadcast*. Las LANs virtuales (VLANs) representan una solución alternativa a los *routers* con función de administrador de la red.

Además, las VLANs pueden enrutar movimientos de las estaciones de trabajo hacia nuevas localizaciones, sin requerimiento de reconfigurar manualmente las direcciones IP.

### 2.12.2 Definición de una VLAN

Las LANs virtuales son agrupaciones de estaciones LAN que se comunican entre sí como si estuvieran conectadas al mismo cable, incluso pueden estar situadas en segmentos diferentes de una red de un edificio o de un campus. Es decir, la VLAN es la tecnología que permite separar la visión lógica de la red de su estructura física mediante el soporte de comunidades de interés, con definición lógica para la colaboración en sistemas informáticos de redes. Este concepto, es fácilmente asimilable a grandes trazos, sin embargo, es todo un complejo conjunto de cuestiones tecnológicas. Quizás, por ello, los fabricantes de conmutación LAN se introducen en este nuevo mundo a través de caminos diferentes, y complican aún más su divulgación entre los usuarios.

Además, las VLANs simplifican el problema de administrar los movimientos, adiciones y cambios del usuario dentro de la empresa. Por ejemplo, si un departamento se desplaza a un edificio a través del campus, este cambio físico será transparente gracias a la visión lógica de la VLAN. Asimismo, se reduce notablemente el tiempo y los datos asociados con los movimientos físicos, esto permite que la red mantenga su estructura lógica. Puesto que todos los cambios se realizan bajo el control de software, los centros de cableado permanecen seguros y a salvo de interrupciones.

### 2.12.3 Tipos de VLANs

Existen diversas formas de crear o definir una VLAN; los fabricantes han implementado principalmente cuatro mecanismos en la arquitectura del *switch*:

- VLAN por puerto: cada puerto del *switch* puede asociarse a una VLAN.
    - Ventajas:
        1. Facilidad de movimientos y cambios: un movimiento supone que la estación cambia de ubicación física, pero sigue perteneciendo a la misma VLAN.
        2. Microsegmentación y reducción del movimiento de *broadcast*: aunque los *switches* permiten dividir la red en pequeños segmentos, el tráfico *broadcast* sigue afectando el rendimiento de las estaciones y se precisan *routers* o VLANs para aislar los dominios de *broadcast*.
        3. Multiprotocolo: la definición de VLAN por puerto es totalmente independiente del protocolo o protocolos utilizados en las estaciones.
    - Desventajas:
        1. Administración: los movimientos y cambios implican normalmente una reasignación del puerto del *switch* a la VLAN a la que pertenece el usuario.

- VLAN por dirección MAC: la relación de pertenencia a la VLAN se basa en la dirección MAC.
    - Ventajas:
        1. Facilidad de movimientos: las estaciones pueden moverse a cualquier ubicación física perteneciendo siempre a la misma VLAN sin que se necesite ninguna reconfiguración del *switch*.
        2. Multiprotocolo: no presenta ningún problema de compatibilidad con los diversos protocolos y soporta incluso la utilización de protocolos dinámicos tipo DHCP (Dynamic Host Configuration Protocol, Protocolo de Configuración Dinámica para los Anfitriones).
    - Desventajas:
        1. Problemas de rendimiento y control de *broadcast*: este método de definición de VLAN implica que en cada puerto del *switch* coexisten miembros de distintas VLANs (se evita el problema si se utilizan puertos dedicados a estaciones pues cada puerto pertenecerá a una

única VLAN) por lo que cualquier tráfico *broadcast* afecta al rendimiento de todas las estaciones.

2. Complejidad en la administración: todos los usuarios deben configurarse inicialmente en una VLAN. El administrador de la red introduce de forma manual, en la mayoría de los casos, todas las direcciones MAC de la red en algún tipo de base de datos. Cualquier cambio o nuevo usuario requiere modificación de la base de datos.

- VLAN por filtros: la asignación a las VLANs se basa en información de protocolos de red. La pertenencia a la VLAN se basa en la utilización de unos filtros que se aplican a las tramas para determinar su relación de pertenencia a la VLAN. Los filtros han de aplicarse por cada trama que entre por uno de los puertos del *switch*.
    - Ventajas:
        1. Segmentación por protocolo: es el método apropiado sólo en aquellas redes en las que el criterio de agrupación de usuarios esté basado en tipo de protocolo de capa 3 del modelo de regencia OSI y la segmentación física existente sea muy diferente a los patrones de direccionamiento.
        2. Asignación dinámica: tanto la definición de VLANs por dirección MAC como por protocolo de capa 3 ayudan a automatizar la configuración del puerto del *switch* en una VLAN determinada.
    - Desventajas:
        1. Problemas de rendimiento y control de *broadcast*: la utilización de las VLANs de capa 3 requiere complejas búsquedas en tablas de pertenencia que afectan al rendimiento global del *switch*. Los retardos de transmisión pueden aumentar entre 50% y un 80%.
        2. No soporta protocolos de nivel 2 ni protocolos dinámicos: la estación necesita una dirección de capa 3 para que el *switch* la asigne a una VLAN. Las estaciones que utilicen protocolos de capa 2 como NETBIOS y LAT (*Local Area Transport*, Transporte de Área Local) no

podrán asignarse a una VLAN. Si existen protocolos dinámicos como DHCP y la estación no tiene configurada su dirección IP ni su *router* por *default*, el *switch* no puede clasificar la estación dentro de una VLAN.

- ELANs o redes emuladas: la relación de pertenencia a una red emulada es implícita al estándar LANE (*LAN Emulation*, LAN Emulada) ya que en el proceso de inicialización del LEC (*LAN Emulation Client*, Cliente LANE) con sus LECS (*LAN Emulation Configuration Server*, Servidor de Configuración LANE), el servidor le transmite toda la información necesaria para que el cliente se registre en una determinada LAN emulada (dirección del LES [*LAN Emulation Server*, Servidor de LANE], tipo de red emulada, tamaño máximo de paquetes y nombre de ELAN).
    - Ventajas:
        1. Facilidad de administración: las funciones de administración se centralizan en el LECS de forma que el administrador puede definir diversos ELANs en la red ATM y asignarlas a puertos de los *switches*, *routers* o *host* ATM independientemente de su ubicación física.
        2. Facilidad de movimiento y cambios: la pertenencia a una ELAN se mantiene aunque se produzcan movimientos y los cambios de ELAN no suponen ningún cambio físico.
        3. Multiprotocolo: LANE es esencialmente un protocolo de capa 2 sobre ATM y por tanto totalmente independiente de los protocolos del nivel superior.
    - Desventajas:
        1. Aplicable sólo a *Ethernet* y *Token Ring*: LANE define métodos de emulación para *Ethernet* y *Token Ring* únicamente. No explota la funcionalidad ATM de QoS (*Quality of Services*, Calidad de Servicio) o cualidades de servicio y una de las características esenciales de ATM a los protocolos de nivel superior.

### 2.12.4 Beneficios de implementar una VLAN

Reducción del Costo de Movimientos y Cambios.- Una de las justificaciones para implementar una VLAN es la reducción en el costo de los cambios y movimientos de usuarios. En general los costos asociados a cambios y movimientos en una red típica son elevados, a consecuencia de una flexibilidad deficiente.

La implementación de una VLAN resultará más conveniente a la hora de habilitar la administración de redes dinámicas, y que esto supondrá bastante ahorro. Esto se puede aplicar con buenos resultados a redes IP, ya que, normalmente, cuando un usuario se mueve a una diferente subred, las direcciones IP han de ser actualizadas manualmente en la estación de trabajo. Este proceso consume gran cantidad de tiempo que puede ser utilizado para otras tareas, tales como producir nuevos servicios de red. Una VLAN elimina ese hecho, porque los miembros de una VLAN no están sujetos a una localización física en la red, y permite que las estaciones cambien de sitio y conserven su dirección IP original.

Sin embargo, cualquier implementación de VLAN no siempre reduce este costo. Una VLAN añade una nueva capa de conexión virtual que ha de ser administrada al mismo tiempo que la conexión física. Esto no quiere decir que no se puedan reducir los costos. Sólo que no hay que precipitarse a la hora de implementar una VLAN y es mejor estar bien seguro de que la solución no genere más trabajo de administración de red que el que pueda ahorrar.

Grupos de Trabajo Virtuales.- Uno de los objetivos más ambiciosos de una red virtual es el establecimiento del modelo de Grupos de Trabajo Virtuales. El concepto es que, con una completa implementación de una VLAN a través de todo el entorno de red del campus, miembros del mismo departamento o sección puedan aparentar el compartir la misma red local, sin que la mayoría del tráfico de la red LAN esté en el mismo dominio de *broadcast* de la VLAN. Alguien que se mueva a una nueva localización física pero que

permanezca en el mismo departamento se podría mover sin tener que reconfigurar la estación de trabajo.

Esto ofrece un entorno dinámicamente organizado, y permite la tendencia hacia equipos con funciones cruzadas. La lógica del modelo de Grupos de Trabajo Virtuales lleva la siguiente forma: los equipos pueden estar conectados virtualmente a la misma LAN sin necesidad de mover físicamente a las personas, para minimizar el tráfico a través de una red troncal colapsada. Además, estos grupos son dinámicos: un equipo destinado a un proyecto puede ser configurado mientras dure ese proyecto, y ser eliminado cuando se complete, esto permite a los usuarios retornar a sus mismas localidades físicas.

Seguridad.- El único tráfico de información en un segmento de un sólo usuario será de la VLAN de ese usuario, por lo que sería imposible "escuchar" la información si no nos es permitida, incluso poniendo el adaptador de la red en modo promiscuo, porque ese tráfico de información no pasa físicamente por ese segmento. Adicionalmente, los miembros de una VLAN pueden protegerse con filtros específicos a sus necesidades de acuerdo a las capacidades del conmutador.

## 2.13 Seguridad en Redes de Datos

Con el incremento en el uso de Internet y el aumento de empresas que utilizan la red para la generación de portales para negocios electrónicos, la protección de la información se convierte en un factor crítico, sobre todo cuando cada vez es más sencillo encontrar herramientas que no requieren de un alto nivel de conocimiento técnico para explorar vulnerabilidades de los sistemas de información, las cuales pueden provocar pérdidas en la confidencialidad, integridad o disponibilidad, que repercute de manera directa o indirecta en pérdidas económicas.

El principio de seguridad se basa en mitigar el impacto de un ataque. Para lograrlo, es esencial saber contra qué o quiénes nos enfrentamos y, a su vez, medir el impacto real

de una amenaza o vulnerabilidad de los diferentes activos, entendiendo como activo a software o hardware que mantiene o posee procesos y/o información crítica.

#### 2.13.2.1 Políticas de seguridad

Una política de seguridad se define como un conjunto de requisitos que se deben tomar en relación con la seguridad, por lo que se requiere la disposición de todos los miembros de la organización para lograr una visión conjunta de lo que se considera importante. Algunos elementos que deben contener son:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre los cuales aplica.
- Objetivos de la política y descripción clara de los elementos involucrados en su definición.
- Definición de los servicios y recursos informáticos a todos los niveles de la organización.
- Requerimientos mínimos para configuración de los sistemas que cubren el alcance de la política.
- Definición de violaciones y de las consecuencias del no cumplimiento de la política.
- Responsabilidades de los usuarios con respecto a la información a la que cada uno tiene acceso.
- Explicar las razones de las tomas de decisiones; es decir, por qué el cuidado de los servicios o recursos de información es prioritario.

Las políticas de seguridad deben mantener un lenguaje común, libre de tecnicismos y términos legales que impidan la compresión clara del escrito, aunque no hay que sacrificar su precisión y formalidad dentro de la organización. Finalmente, las políticas de seguridad son documentos dinámicos dentro de la organización, por lo que deben seguir un proceso de actualización periódica sujeta a los cambios organizacionales relevantes.

### 2.13.2 Tecnologías de seguridad

No existe una receta o método único para construir una arquitectura de seguridad en redes; sin embargo, hay una gran disponibilidad de tecnologías para integrarlas y ajustarlas a los planes de prevención. Las tecnologías idóneas para esta integración son las siguientes:

- *Firewalls*: controla el tráfico de las redes al seleccionar la información que entra y sale de éstas para garantizar que no ocurra accesos no autorizados. Un buen *firewall* tiene que proporcionar una protección integral frente a amenazas internas y externas, al tiempo que garantiza el acceso de la información a los usuarios.
- Detección de intrusos: detecta el acceso no autorizado y proporciona alertas e informes que se pueden analizar en cuanto a la identificación de la configuración y programas de trabajo de la computadora. Existen soluciones eficaces que detectan, monitorean y expulsan a usuarios no autorizados.
- Autenticación y autorización: garantiza la identidad de cada usuario, desde la simple protección de *passwords* (contraseñas) hasta la implementación de soluciones, como huellas digitales y el uso de tarjetas inteligentes. Cuanto más avanzada sea la técnica de autenticación, será menos probable que se produzca una infracción en la seguridad.
- Filtrado de contenidos: identifica y elimina el tráfico no deseado. Diversas soluciones de software, incluso suites que integran antivirus y desfragmentadores de disco, entre otros, se encargan de evitar el despliegue de sitios en Internet que no son de incumbencia para los objetivos de trabajo de una organización.
- VPN (*Virtual Private Network*, Redes Privadas Virtuales): su implementación protege las conexiones fuera del perímetro, lo que le permite a las organizaciones comunicarse en Internet de manera segura. Además, encripta los datos antes de enviarlos a una red pública.
- Manejo de la vulnerabilidad: descubre fisuras en la seguridad y sugiere mejoras.

- Protección antivirus: una infección por virus informativos extendida representa una amenaza para el negocio u organización. Todos los puntos de entrada de los virus deben estar completamente protegidos y los puntos de entrada potenciales pueden identificarse todos los días para que ningún virus sea transmitido en los sistemas.
- Protocolos de seguridad: resuelven los problemas de autenticación. Entre los más comunes destacan el SSL (*Secure Sockets Layer*, Nivel de Conexión Seguro) y el más reciente IPSec (*Internet Protocol Security*, Protocolo de Seguridad IP); este último resuelve muchos de los problemas que se generan en la autenticación y confidencialidad de los datos.

# 3. ANÁLISIS

La interconectividad de múltiples aplicaciones, dispositivos y protocolos es uno de los principales objetivos de la red. Sin olvidar que es de primordial importancia soportar toda la gama de requerimientos, presentes y futuros bajo un esquema de alto desempeño.

De esta manera, se realiza un análisis previo que empieza por una reseña del cómputo en la Institución, la situación actual de la infraestructura de red, la problemática presente, así como la propuesta de solución para su optimización.

## 3.1 Reseña Histórica del Cómputo en la Institución

La aplicación de las computadoras y de las técnicas computacionales a las labores de El Colegio de México se inició en 1966 para facilitar el manejo de censos y encuestas, y se ha convertido hoy en parte esencial de casi todas las tareas académicas y de la gran mayoría de las tareas de apoyo a la academia.

En sus 36 años de historia, el uso de recursos de cómputo en El Colegio ha sufrido un proceso de evolución y desarrollo que puede analizarse basándose en algunos eventos clave: su inicio, en 1966; la instalación de la primera computadora propia, en 1977; el inicio en la adquisición de microcomputadoras, en 1983; el establecimiento de la primera red de cómputo, en 1988; la entrada a las redes internacionales, en 1994; el análisis técnico para la incorporación de El Colegio a Internet2, en 2001; y la constitución de El Colegio como un polo de desarrollo informático, en el momento actual. Estos eventos influyen decisivamente en la modalidad mayoritaria de uso de los recursos de cómputo.

En el periodo 1966-1977, El Colegio de México no cuenta con equipo de cómputo propio. Son los tiempos en los que el uso directo de computadoras está técnicamente limitado a ingenieros, actuarios, físicos y matemáticos especializados en análisis y programación. Los investigadores de El Colegio que se enfrentan a la necesidad de procesar grandes volúmenes de información buscan apoyo en otras instituciones académicas u oficiales. Se utilizan los equipos de cómputo de la Universidad Nacional Autónoma de México (la BURROUGHS 550 del Centro de Cálculo Electrónico que posteriormente sería el Instituto de Investigación en Matemáticas Aplicadas y Servicios), la Secretaría de Obras Públicas y la Secretaría de Educación Pública (la UNIVAC 1106 del Centro de Procesamiento “Arturo Rosenblueth”). Los investigadores de El Colegio resuelven sus necesidades de procesamiento de datos gracias a la intermediación de unos cuantos especialistas de cómputo, unos contratados por El Colegio y otros bajo colaboraciones institucionales.

Como es natural, la aplicación del cómputo se inicia con proyectos que requieren procesamiento numérico de datos, a saber, los censos y las encuestas nacionales analizados en el entonces Centro de Estudios Económicos y Demográficos. Posteriormente, surgen en El Colegio proyectos que plantean problemas de análisis computarizado de información no numérica, pocos trabajados en aquel entonces. Éstos son los casos del Diccionario del Español de México (DEM) y del Cancionero Folklórico de México (CFM). El DEM requirió, entre sus tareas de cómputo, del diseño y la elaboración de un analizador morfosintáctico automático para el procesamiento del

Corpus del Español Mexicano Contemporáneo. La especializada programación de este sistema de cómputo lo hizo, a la postre, merecedor del Premio “Arturo Rosenblueth” en Sistemas de Cómputo 1981. Hacia 1974 se inició el proyecto de constitución de una Unidad de Cómputo (UC) en El Colegio.

Para 1975 se realizó la contratación de personal, en su mayoría, jóvenes formados como ingenieros. Durante un par de años se trabajó fundamentalmente con el equipo UNIVAC 1106 del Centro de Procesamiento “Arturo Rosenblueth” que generosamente instaló terminales remotas en el edificio anexo al de Guanajuato 125, a través de líneas privadas de telefonía. La construcción del actual edificio de la institución, incluyó un área específica con instalaciones especializadas, inclusive una jaula de Faraday y energía eléctrica regulada para albergar la primera computadora propia de El Colegio. En 1977 se pone en marcha la PDP-11/70 con lo cual se inicia una nueva modalidad en el trabajo de cómputo de El Colegio.

En el periodo 1977-1983 se diferencian las funciones básicas de la UC. La existencia de un equipo de cómputo propio hace imprescindible el desempeño de actividades de operación y administración técnica. Para realizar estas funciones se constituye y capacita un grupo de entre los entonces miembros de la UC. Posteriormente, la UC se enriquece con nuevo personal con formación en Matemáticas y en aspectos teóricos de las Ciencias de la Computación. Los programas comerciales adquiridos para la PDP eran un par de paquetes estadísticos, un recuperador de información (antecesor de los manejadores de bases de datos), y algunos otros paquetes demográficos y matemáticos de uso muy especializado. La utilización de esos paquetes se realiza a través de sus propios lenguajes de programación, por lo que su uso directo sigue en manos de los especialistas de cómputo. Los investigadores que se interesan por utilizar los paquetes estadísticos o de recuperación de información para el procesamiento de sus datos acuden con los analistas-programadores de la UC para obtener el apoyo computacional.

Los proyectos del DEM y del CFM continúan trabajándose en el exterior; mientras que, se inician otros proyectos que requieren del manejo computarizado de información no numérica, entre los que se cuentan el proyecto de Automatización de la Biblioteca, el de

Sociolingüística del Lenguaje Infantil y el de las Guías de Protocolos del Archivo General de Notarías. En la UC, se diseñan y programan los sistemas para dar solución computacional a los problemas planteados en estos proyectos. Es así como la función de desarrollo de sistemas de cómputo, originada en el periodo 1966-1977, queda definitivamente establecida. Además, se constituye un grupo en el área de Metodología, el cual se encarga de identificar los problemas computables correspondientes a los problemas de investigación planteados por los científicos sociales. Algunos miembros de la UC imparten cursos de Metodología, Estadística, Matemáticas e Informática en los programas docentes de El Colegio, con lo cual queda también establecida la función de docencia.

En 1983, la UC adquiere las primeras microcomputadoras. Inicialmente se compran tres ALTOS-586 con sistema operativo multiusuario tipo UNIX, y varios meses después dos CORONA compatibles con IBM con sistema operativo DOS. Una de las ALTOS se destina a la automatización de ciertos procesos de la Biblioteca, mientras que el resto son utilizadas directamente por los profesores-investigadores de El Colegio para procesamiento de textos y por los analistas-programadores de la UC para el desarrollo de sistemas. La utilización directa del equipo de cómputo por parte de los profesores-investigadores provoca el surgimiento de dos nuevas funciones en la UC: la capacitación y la asesoría en materia de cómputo.

Durante el periodo 1983-1988 se viven serios cambios. Por una parte, aumenta entre los investigadores el interés por la aplicación de técnicas estadísticas, matemáticas o de recuperación de información, lo cual genera una creciente interacción entre investigadores y personal de cómputo. Paralelamente, se incrementan de manera considerable los proyectos que demandan la solución computacional de problemas de carácter no numérico, muchos de ellos relacionados con algún tipo de acervo documental. Entre éstos destacan: el manejo de archivos con información histórica, el análisis lingüístico de información textual, la creación de catálogos de material literario, el manejo de toda la bibliografías especializadas, el tratamiento de fichas temáticas o de investigación y la construcción de diccionarios de lengua. En ese momento, no es posible resolver con paquetes comerciales las necesidades de procesamiento de

cómputo de estos proyectos, ya sea porque no existen paquetes que contemplen la solución de problemas de esta naturaleza o ya sea porque los paquetes existentes no pueden trabajar con las limitaciones del hardware de la PDP-11 y El Colegio no tiene los recursos económicos para adquirir nuevo hardware. Los problemas se resuelven en la UC a través del desarrollo de sistemas de cómputo especializados. La gran cantidad de sistemas de tratamiento de información no numérica, que deben desarrollarse, lleva a la acumulación de conocimiento y a la creación de métodos generales de programación. En 1985, la UC recibe el Accesit de plata del Centro Regional para la Enseñanza de la Informática (CREI) de Madrid, España, por el trabajo titulado “Manejo automatizado de acervos documentales”; trabajo en el que se describen las metodologías y los sistemas de cómputo creados.

Por otra parte, también hacia 1985, la PDP-11, que cumple ocho años de servicio intenso, resulta insuficiente para la demanda, presenta constantes descomposturas y es totalmente obsoleta; se decide no usarla más. Ya que El Colegio no puede solventar la fuerte inversión que significaría la compra de una nueva computadora central, paulatinamente se adquieren con presupuestos de los Centros o de Proyectos especiales computadoras personales (IBM-compatibles), que se usan descentralizadamente.

Durante el periodo 1986-1988, cambia la forma de trabajo: se incrementa el uso directo de las computadoras por los profesores-investigadores para el procesamiento de texto, pero los proyectos de investigación se vuelven menos ambiciosos en sus expectativas de uso del Cómputo. El personal de la UC aprovecha, lo mejor que puede, las pocas computadoras personales con las que cuenta. Para el proyecto de Automatización de la Biblioteca se desarrollan sistemas para control de compra de libros y publicaciones periódicas, producción de listas de obras catalogadas y marcaje de libros. En este periodo se apoya también a la Administración de El Colegio: se desarrollan los sistemas de nómina, control de presupuestos, contabilidad y contraloría. Para mediados de 1988, El Colegio cuenta con 42 computadoras personales IBM-compatibles, seis microcomputadoras multiusuarios y 34 impresoras.

En 1987, la UC se propone conseguir recursos económicos para comprar el equipo de cómputo que requiere El Colegio. Sus búsquedas y negociaciones fructifican, en 1988, en la forma de un Convenio de Colaboración entre El Colegio de México y la Compañía IBM de México. Gracias a este Convenio, El Colegio recibe el equipo con el que constituirá su primera red: un servidor y 16 clientes PS/2 conectados bajo una arquitectura *Token Ring*. Además, recibe una computadora RT PC *System Unit* orientada a procesos de graficación, con un monitor de alta resolución, un scanner, un graficador y una tableta digitalizadora. El Convenio obliga a El Colegio de México a realizar dos proyectos en el equipo entregado: el desarrollo de una versión del analizador morfosintáctico desarrollado años antes para el proyecto del DEM; y la creación del Laboratorio de Cartografía Automatizada y Análisis Espacial. Ambas obligaciones son exitosamente cumplidas tiempo después.

El periodo 1988-1994 se caracteriza por el crecimiento distribuido de la infraestructura de red *Token Ring*: los nodos de la red llegan a los propios cubículos de la gran mayoría de los profesores-investigadores. Se calcula que, para mediados de 1988, El Colegio contaba con 42 computadoras personales y 34 impresoras de matriz; para fines de 1988, con 102 computadoras personales, 35 impresoras de matriz y cuatro impresoras láser; para mediados de 1990, las cifras respectivas aumentan a 168, 62 y cinco; para fines de 1990, a 173, 69 y cinco; para 1991, a 206, 70 y 11; para 1992, a 304, 81 y 26; para 1993, a 320, 90 y 28; y para 1994 a 514, 95 y 30.

Debido al crecimiento distribuido de los recursos de cómputo en el periodo 1988-1994, los profesores-investigadores tienen una mayor participación en el procesamiento computarizado de su información, y como consecuencia, los analistas de la UC deben dedicar mayores esfuerzos a la instalación de equipos y programas, y a la asesoría y capacitación en el uso de éstos.

En 1992 la red de El Colegio estaba configurada con el siguiente diseño, como lo muestra la figura 3.1.

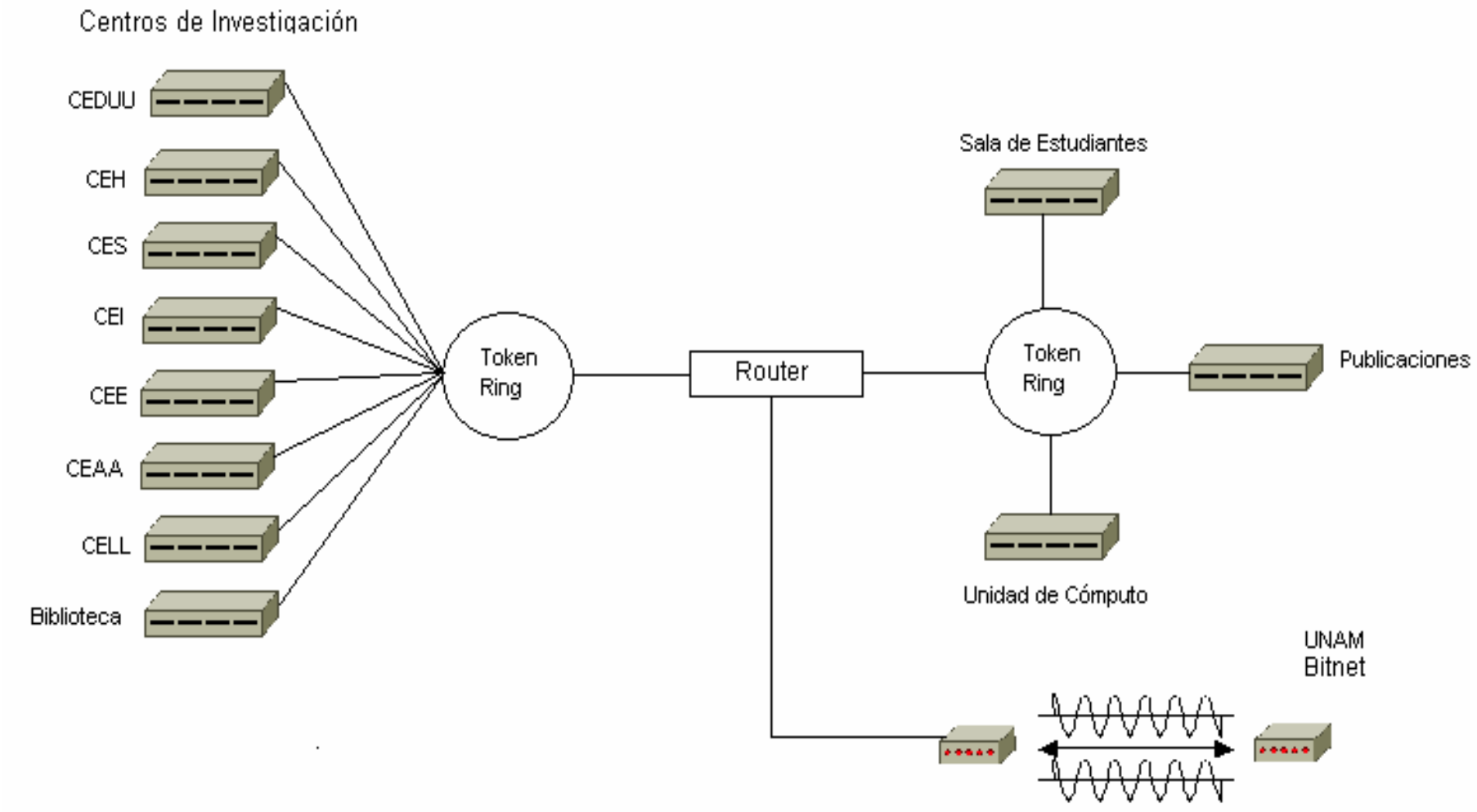



Figura 3.1 Topología de la red *Token Ring* de El Colegio de México

En 1989 se inicia el servicio de una sala de cómputo para estudiantes en la UC, con 18 equipos instalados y cuatro becarios de investigación del área de cómputo para asesorar en el uso de las máquinas y de los programas instalados. Dadas las restricciones de espacio de esta sala se implementa una nueva sala de cómputo para estudiantes ubicada en la Biblioteca, con 23 computadoras personales (pero con capacidad para albergar 50) y dos impresoras. También en 1989, se concluye la conexión de El Colegio a REDUNAM, lo que permite utilizar el servicio de correo electrónico a través de la red académica internacional BITNET. La conexión a REDUNAM se establece mediante dos terminales y dos líneas telefónicas ubicadas en la UC, por lo que los investigadores tienen que acudir a la UC para utilizar el servicio.

En 1988, haciendo uso de uno de los equipos multiusuario ALTOS 586, se inicia el desarrollo del Sistema de Información Integral para el Control Escolar (SIICE); pero es en 1990 cuando se adquiere una computadora IBM PS/2 modelo 30 en la cual se instrumenta el SIICE, que se conecta a la red *Token Ring* para posibilitar el intercambio de información entre el Departamento de Asuntos Escolares y las coordinaciones académicas de los Centros. En 1990 se adquiere una computadora multiusuario ALTOS 1000 que se dedica a la automatización de los procesos administrativos, en sustitución de la ALTOS 686.

En 1990, El Colegio obtiene un presupuesto especial de la SEP para apoyar el proyecto de Automatización de la Biblioteca. Con él, se adquiere para la Biblioteca una computadora multiusuario de la marca SUN modelo SPARCserver 470 con 16 terminales de trabajo y el manejador de bases de datos denominado STAR orientado al tratamiento de información textual. Aprovechando el trabajo realizado en años anteriores, se desarrolla un sistema de cómputo integral que permite la consulta automatizada del catálogo de obras de la Biblioteca, facilita la catalogación, clasificación y realización de los procesos técnicos del material bibliográfico, hace prácticamente automática la actualización del catálogo, y permite el control de los procesos de adquisición de las obras. A mediados de 1993, el Catálogo de Libros de la Biblioteca puede ser consultado en línea por los lectores en terminales ubicadas en la sala de referencia.

Para finales de 1993, la infraestructura y los servicios de cómputo establecidos en El Colegio impulsan a profesores-investigadores y alumnos a la utilización creciente de las computadoras y las técnicas computacionales con las que cuentan, esto produce en ellos acercamiento al Cómputo, mayor conocimiento de él, mayores necesidades y, por lo tanto, mayor interés en la aplicación de los nuevos productos de cómputo del mercado.

Para satisfacer dichas necesidades e intereses de profesores, investigadores y alumnos, y tomando en cuenta el avance tecnológico en materia de cómputo, informática, redes y telecomunicaciones, se decide realizar un cambio tecnológico en lugar de continuar el crecimiento de la infraestructura instalada. De esta forma se establece una nueva función básica para la UC: la planeación para la aplicación de nuevas tecnologías de información. Como paso transitorio se aumenta la velocidad de transmisión de datos en el canal principal de comunicación de 4 a 100Mb y para cada usuario se aumenta la velocidad de 4 a 10Mb compartidos. A fines de 1993 la Unidad de Cómputo pasa a ser Coordinación de Servicios de Cómputo (CSC).

En 1994 se inicia el cambio de la red *Token Ring* a una red de anillo redundante de fibra óptica FDDI. Se llevan a cabo los trámites ante el NIC (*Network Information Center*, Centro de Información para Redes) de Estados Unidos para registrar a El Colegio en la red académica Internacional Internet. En este mismo año se inicia el cableado estructurado de El Colegio con el estándar internacional de nivel 5 certificado por AT&T; se elige el nivel 5 porque con este tipo de cableado se asegura el buen funcionamiento de la red independientemente de los avances tecnológicos de los equipos.

Para finales de 1994 El Colegio tiene instalada una red como se muestra en la figura 3.2. La transición entre la red *Token Ring* y la red FDDI provoca un crecimiento aproximado de 120% anual en el número de usuarios de correo electrónico. Al instalarse la red FDDI se establece en la CSC una más de sus funciones básicas: la de operación y administración de redes y telecomunicaciones.

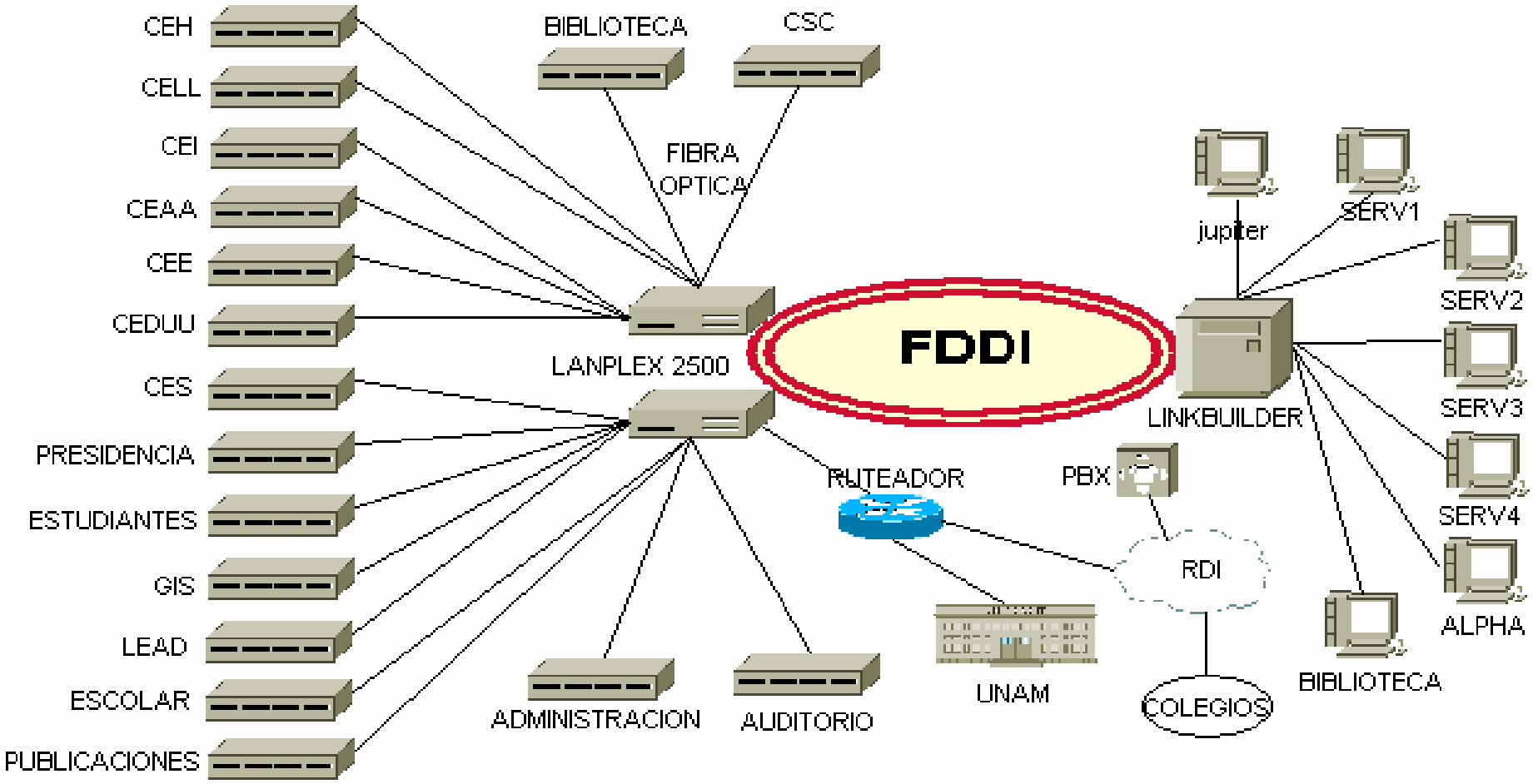



Figura 3.2 Topología de la red de Fibra óptica de El Colegio de México

En el periodo 1994-2000, esto es, a partir de la instalación de la red FDDI y el registro de El Colegio en Internet se tiene que cambiar la forma de utilizar el Cómputo. El problema sustantivo que se presenta en la CSC en éste periodo es la capacitación del personal de cómputo en las nuevas tecnologías de Internet. Hay que adquirir velozmente el conocimiento necesario de las siempre nuevas herramientas de cómputo para aplicarlas durante la implantación de infraestructura (redes de área local, redes de área amplia, infraestructura de telecomunicaciones...); durante la instrumentación de servicios informáticos (correo electrónico, transmisión de archivos, manejo de páginas Web institucionales, comunicación telefónica a través de la red de cómputo, servidores de aplicaciones, acceso a Internet...); o durante la creación de aplicaciones informáticas propias (sistemas de cómputo, de procesamiento o de información, bases de datos, interfaces Web para difusión de información o para consulta de bancos de datos...).

La demanda de soluciones a los muy variados problemas de cómputo es tanta que, generalmente, la capacitación se realiza a través de la consulta de manuales en el propio momento en que se aplica la herramienta; excepcionalmente es posible que los miembros de la CSC asistan fuera de El Colegio o del país a cursos sobre alguna herramienta de cómputo.

A pesar del problema descrito, el periodo 1994-2000 se caracteriza por la constante modernización de los recursos y los servicios de cómputo. En 1995 se crea un área en la CSC donde los profesores-investigadores pueden usar scanners y equipos multimedia para el procesamiento de información contenida en discos compactos y discos digitales que usan video y sonido.

A finales de 1998 El Colegio instala equipo de conmutación (*switching*), y la red institucional pasa a ser una red conmutada (*switched*) *Ethernet* con velocidad de 100 Mb en su *Backbone*; gracias a este equipo, es posible instrumentar el servicio de procesamiento en red de datos, voz y video.

En 1998 se crea un aula computarizada, con ocho equipos conectados a la red, destinada a impartir cursos y a la realización de seminarios que requieren de la informática. En 1998 se consolida el equipamiento del Laboratorio de Sistemas de Información Geográfica en el que se llevan a cabo labores de análisis espacial, cartografía automatizada y graficación para apoyar a investigadores y alumnos. Durante el periodo 1994-2000 se actualiza en dos ocasiones la sala de cómputo para estudiantes con 48 equipos Pentium III conectados a la red.

En 1999 se instalan más equipos en red en las áreas de los Centros de Estudios, Biblioteca, Publicaciones, Administración, cubículos del 5° nivel, salones y bodegas, alcanzando una cobertura física de 85%. De 1995 al 2000 hubo un crecimiento de 464 a 740 equipos conectados a la red; actualmente la cobertura de equipos respecto a profesores-investigadores es de 100 por ciento.

En 1998 se adquiere el programa estadístico SPSS con licencia para 10 usuarios en red. En 1999 se actualizan los programas de uso general gracias a un contrato celebrado con *Microsoft* llamado *Campus Agreement*. Bajo este contrato, todo el personal de El Colegio, sin importar el número, puede usar los productos de *Office*, los programas de correo electrónico y las herramientas de desarrollo. En el 2000, El Colegio adquiere sendos programas para monitorear el tráfico de la LAN y WAN e Internet para establecer los parámetros de seguridad internos y externos respectivamente que nos protejan en la mayor medida posible de los intrusos (*hackers*), de ésta forma se implementa el sistema de seguridad Institucional con el uso de un *Firewall* y un detector de intrusos.

En 1998 El Colegio realiza los trámites necesarios ante el NIC de México para definir técnicamente a El Colegio como un nodo AS (*Autonomous System*, Sistema Autónomo), lo que permite direccionar el acceso a Internet por más de un nodo exterior. En el mismo año se instala un enlace redundante de 512 Kb a Internet a través de la compañía Alestra, de manera que El Colegio cuenta con dos accesos a Internet, la UNAM y Alestra.

En 1999, también ante NIC México se llevan a cabo las gestiones necesarias para que a El Colegio se le asignen en forma exclusiva direcciones IP. NIC México asignó el *Net Block*: 10.0.240.0 – 10.0.255.0 (16 direcciones tipo C) para uso exclusivo de El Colegio, lo que permite direccionar en forma autónoma las salidas a Internet. En este año 2000 la CSC ha realizado diferentes trabajos de investigación para instrumentar el servicio de videoconferencia que integre a El Colegio en el Sistema Nacional de Educación a Distancia.

En 1998 se adquiere un servidor para la Biblioteca con el que se transformará en red la infraestructura anterior; además, se adquiere el programa Aleph gracias al cual se automatiza el control de circulación. El sistema integral desarrollado hacia 1993 se migra paulatinamente a Aleph.

Actualmente la Biblioteca ofrece el servicio de consulta al catálogo público a través de Internet. A partir de 1996 el desarrollo de nuevos sistemas de cómputo propios se orienta a su uso en Internet; además, se rediseñan y reprograman con la misma orientación casi todos los sistemas previamente creados.

En el periodo 2000–2002 se realizaron importantes renovaciones de equipo de cómputo, específicamente computadoras de escritorio para profesores-investigadores de El Colegio. A finales del 2000 se adquieren 250 computadoras de escritorio Pentium III para renovar equipos del personal académico, administrativo y biblioteca, al igual que para salas de cómputo de estudiantes. Otra adquisición se realizo también a finales del 2002, donde fueron 80 computadoras Pentium IV para renovar equipos que ya eran obsoletos para los nuevos programas y aplicaciones.

Con la renovación y adquisición de equipos de cómputo para el personal de El Colegio, la necesidad de utilizar los servicios y aplicaciones de red que El Colegio proporciona y de Internet, fue realmente necesario por lo que en éste periodo se realizo una reestructuración y ampliación del cableado estructurado, para que todo aquel que tuviera una computadora personal pudiera acceder a los recursos de red, como es: correo

electrónico, acceso a Internet, impresoras, aplicaciones y programas. Por lo anterior el tráfico hacia Internet se vio saturado lo que se requirió aumentar el ancho de banda del enlace de Alestra, de 512 Kb a 2048 Kb (E1); para satisfacer la demanda de los usuarios.

En el 2001 la CSC llevó a cabo el análisis técnico para integrar a El Colegio en el nuevo servicio de Internet 2, que es una red académica de alta velocidad. En el mes de junio de ese año los Centros Públicos de Investigación CONACYT y la Corporación Universitaria para el Desarrollo de Internet, A.C. (CUDI) firmaron la carta de adhesión mediante la cual los Centros manifestaron su voluntad de pertenecer como Asociados Académicos a la Asociación Civil CUDI. Esto le permite a El Colegio participar en proyectos de investigación que requieran del servicio de Internet 2. Durante el primer semestre de 2003 se realizarán los trabajos necesarios para llevar a cabo la conexión física de El Colegio a éste servicio.

El Colegio de México (Colmex) ha coordinado los trabajos de la instalación de una red digital de área amplia llamada Red de Colegios (RdeC, véase la figura 3.3) en ella participan otras instituciones con enfoques similares de investigación y con las cuales El Colmex tiene una estrecha relación: El Colegio de la Frontera Norte (Colef), El Colegio de la Frontera Sur (Ecosur), El Colegio de Michoacán (Colmich), El Colegio de San Luis (Colsan), El Instituto de Investigaciones Dr. José María Luis Mora (IMora) que forman parte del Sistema SEP-Conacyt (SSC) en el área de Ciencias Sociales y Humanidades, así como El Colegio de Sonora (Colson) y El Colegio Mexiquense (Cmq).

Gracias a la integración de la RdeC se ha podido construir un catálogo colectivo de Bibliotecas entre El Ecosur, El Colmich, El Colmex y El Colsan, lo que permite hacer búsquedas de información bibliográfica y documental en un catálogo unificado.

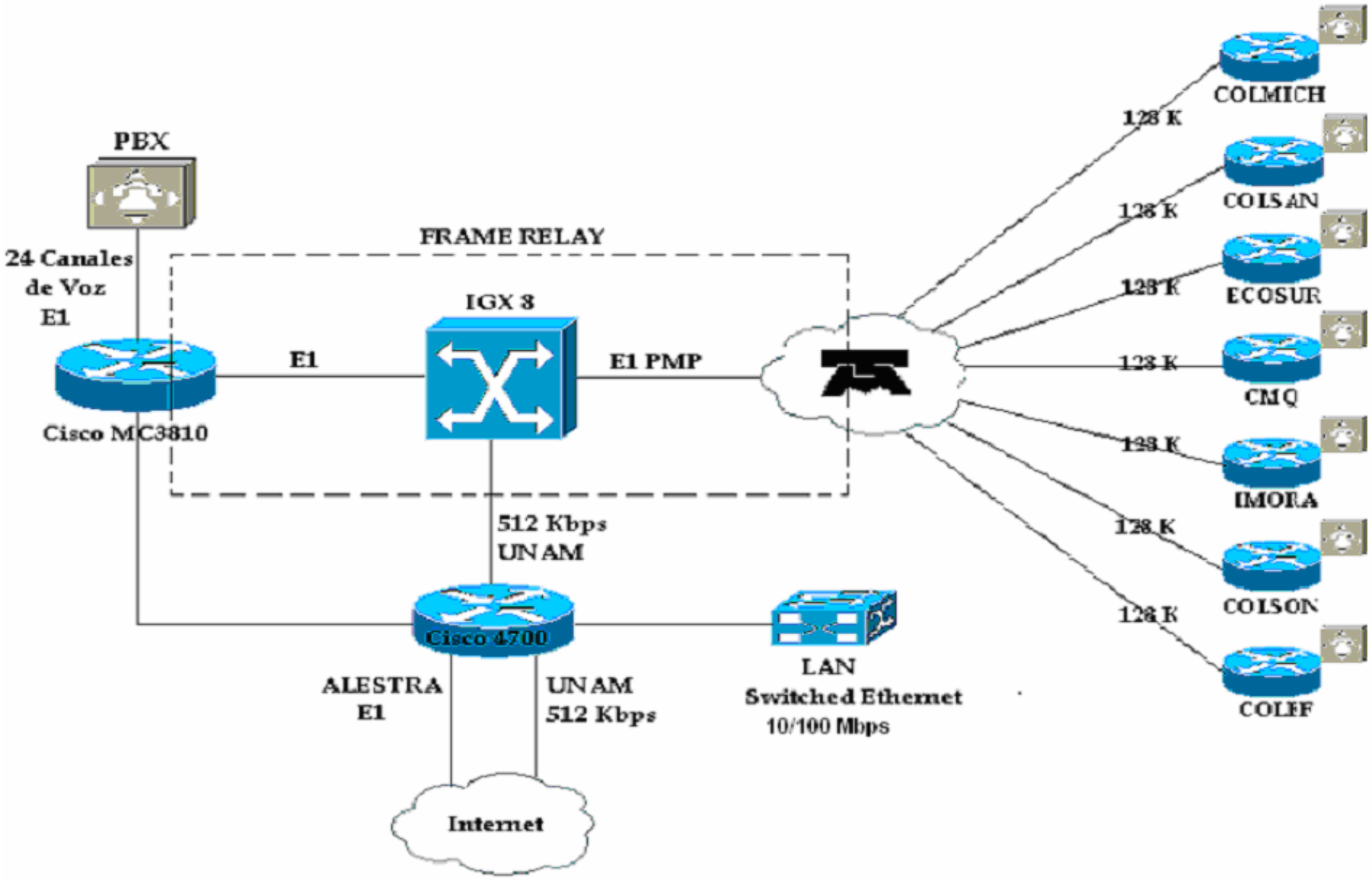



Figura 3.3 Diagrama de la Red de Colegios (Voz y Datos)

## 3.2 Infraestructura de la Red

La infraestructura de red de El Colegio se divide en dos secciones muy importantes, la parte WAN que engloba a instituciones afines (RdeC) y enlaces de Internet; y la parte LAN que está conformada principalmente por el *Backbone*, *switches* de acceso, servidores y el cableado estructurado.

La arquitectura de la LAN está constituida con tecnología *Ethernet* a nivel lógico bajo una topología tipo estrella a nivel físico. Como *Backbone* se tiene un *switch* 3Com *Corebuilder* 7000 con 24 puertos *Fast Ethernet* donde se conectan *switches* de acceso 3Com *SuperStack* 1100 y 3300 por medio de fibra óptica monomodo a los centros de investigación ubicados en los distintos niveles del Colegio. El *CoreBuilder* también cuenta con 16 puertos tipo RJ45 *Fast Ethernet* para los servidores de prioridad mayor. Los *SuperStack* 1100 tienen 24 puertos a 10 Mbps y 2 puertos 10/100 Mbps en half y full duplex. Los *SuperStack* 3300 con 24 puertos, todos con 10/100 Mbps en *half* y *full duplex*. Estos equipos permiten el acceso a los recursos de la red por medio de las computadoras de los profesores-investigadores, administrativos y estudiantes (véase figura 3.4).

El *Backbone* está a su vez conectado a un *router* cisco 4700 que tiene 6 interfaces *Ethernet* 10 Mbps y 4 puertos seriales a WAN. Las interfaces *Ethernet* soportan al conjunto de segmentos que engloban a los usuarios o nodos finales de El Colegio. Mientras que los enlaces seriales permiten la conexión con la RdeC y a Internet. Para el enlace a la RdeC se tiene un E1 PMP (Punto Multipunto), este enlace esta dividido entre los Colegios con un ancho de banda de 128 Kb para cada uno, este enlace a su vez está dividido en dos conexiones virtuales, uno para datos y la otra para la red de voz, lo que permite extender la red telefónica. En el mismo E1 se tiene la conexión a Internet con la UNAM a 512 Kb. El Colegio cuenta con otra salida alterna a Internet a través de Alestra, con un ancho de banda de un E1 utilizando microondas como medio de comunicación.

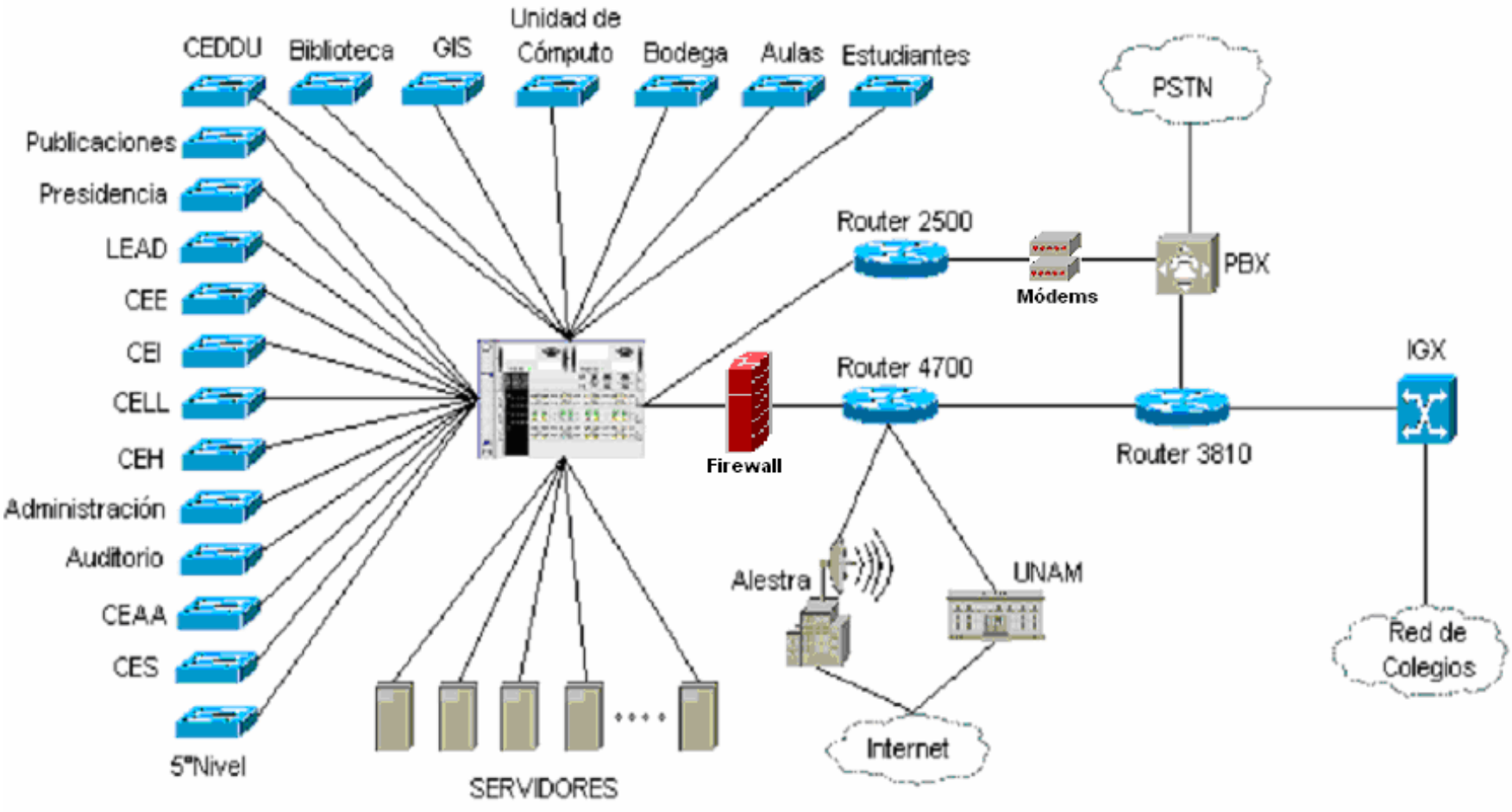



Figura 3.4 Topología Actual de El Colegio de México

Otros equipos importantes en la infraestructura de la RdeC es un *router* cisco 3810 y un IGX 8. El IGX 8 recibe directamente el E1 PMP, lo cual significa que su función principal es la integración de todos los Colegios generando así lo que denominamos “La nube de *Frame Relay*”, esto es por que el protocolo y configuración que se utiliza para la comunicación con los Colegios es *Frame Relay*. Del IGX 8 hay una conexión con el *router* 3810, que es el E1 de los Colegios (voz y datos). La función del *router* 3810 es la de direccionar el tráfico de voz al conmutador y la parte de datos al *router* 4700.

Se cuenta con un conjunto de direcciones IP clases C para los segmentos que dan servicio a las estaciones finales y que son otorgadas en su mayoría en forma dinámica, por DHCP. También se cuenta con direccionamiento para la administración de los equipos de comunicaciones, servidores y estaciones de trabajo. Véase tabla 3.1 de las aplicaciones y descripciones de los segmentos.

El Colegio cuenta con el servicio de acceso remoto a Internet para los profesores-investigadores y está constituido por un *router* cisco 2500 con puertos asíncronos, estos puertos tienen conectados 16 módems y son validados por medio de un *software* TACACS (*Terminal Access Controller Access Control System*, Sistema de Acceso al Controlador de Acceso de Terminal).

La infraestructura en el cableado estructurado que está en operación y que parte de las estaciones finales a los dispositivos de acceso (3Com SuperStack 1100 y 3300), utiliza cable UTP nivel 5 con un número aproximado de 634 nodos, ubicados en los niveles de El Colegio.

Los protocolos que utilizan principalmente las aplicaciones y sistemas operativos son: TCP/IP, IPX/SPX, NetBEUI y NetBIOS (*Network Basic Input/Output System*, Sistema Básico de Entrada/Salida para Red). Pero se lleva acabo actividades para unificar los protocolos, de tal manera que sólo se utilice protocolo TCP/IP como predeterminado; lo que optimizará notablemente el manejo de tráfico y la administración de la red.

| Direccionamiento IP | Áreas Atendidas | Descripción | Tipo de Aplicaciones |
|---|---|---|---|
| 10.0.160.0 | • Centros de Investigación<br>• Biblioteca<br>• Administración | Se conectan PCs de profesores-investigadores, administrativos y biblioteca | • Servicios de Internet<br>• Servicio de archivos<br>• Impresión en red<br>• Programas específicos |
| 10.0.161.0 | • Centros de Investigación<br>• Biblioteca<br>• Administración | Se conectan PCs de profesores-investigadores, administrativos y biblioteca | • Servicios de Internet<br>• Servicio de archivos<br>• Impresión en red<br>• Programas específicos |
| 10.0.162.0 | • Centros de Investigación<br>• Biblioteca<br>• Administración | Se conectan PCs de profesores-investigadores, administrativos y biblioteca | • Servicios de Internet<br>• Servicio de archivos<br>• Impresión en red<br>• Programas específicos |
| 10.0.163.0 | • Centros de Investigación<br>• Biblioteca<br>• Administración | Se conectan PCs de profesores-investigadores, administrativos y biblioteca | • Servicios de Internet<br>• Servicio de archivos<br>• Impresión en red<br>• Programas específicos |
| 10.0.175.0<br>(Asignación Fija) | • Sala de alumnos<br>• Área de salones | PCs de alumnos | • Servicios de Internet<br>• Servicio de archivos<br>• Impresión en red |
| 10.0.173.0<br>(Asignación Fija) | • Unidad de cómputo<br>• Área administrativa<br>• Biblioteca | Se conectan *server*, *workstation*, equipo de comunicaciones (*routers, modems, switches*, etc.) e impresoras | • Servicios de archivos<br>• Impresión en red<br>• Servicio acceso remoto |
| 10.0.158.0<br>(Asignación Fija) | • Red de Colegios | Se conectan los *routers* de la red de colegios para su administración | • Servicios de Internet<br>• Servicio de voz |

Tabla 3.1 Descripción de segmentos y aplicaciones

La distribución de servidores donde están los servicios y aplicaciones que brinda El Colegio se encuentran en su mayoría en la CSC, en el domino de colmex.mx, en éste mismo dominio se encuentra los servidores de Biblioteca pero físicamente se encuentran en su área. Se tienen otros subdominios como es el de admin.colmex.mx que corresponde al área de Administración, donde controlan sus propios servidores; otro subdominio es el de estud.colmex.mx, aquí corresponde a la parte de estudiantes y la administra la CSC. Para mayor detalle consultar la tabla 3.2.

## 3.3 Análisis de la Red

La capacidad del *Backbone* se mide por el número de paquetes y/o bytes que pueden entrar y salir, ancho de banda entre sus componentes, el poder de procesamiento y también por la densidad de puertos que contiene el equipo.

La capacidad, se considera por el monto requerido de puertos para todos los dispositivos de acceso, los enlaces entre los componentes del *Backbone* y el ancho de banda dentro de los propios enlaces para el conjunto de puertos. Los componentes del *Backbone* son diseñados considerando la utilización y carga. Una vez que la carga de los dispositivos de acceso es determinado, la capacidad del *Backbone* puede ser calculado.

Para el cálculo de capacidades del *Backbone* se realizó un análisis genérico de la red. El cual nos permite hacer las mediciones en los segmentos que conforman el *Backbone* y con esto emitir un reporte de utilización, el uso de protocolos y problemáticas generales.

Este análisis se realizó con la ayuda de software y hardware, por medio de un analizador de protocolos llamado “sniffer”, el cual se conecta directamente a la red LAN para las capturas de información de datos y la elaboración de un análisis detallado.

| SERVER | IP | Dominio | S.O | DNS | WINS | DHCP | MAIL | WEB | SQL | DATOS |
|---|---|---|---|---|---|---|---|---|---|---|
| ***UNIDAD DE CÓMPUTO*** | | | | | | | | | | |
| **GAMA** | 10.0.173.134, 10.0.160.1, 10.0.161.252, 10.0.162.254, 10.0.163.252, | colmex | w2000 | X | X | X | | | | |
| **DELTA** | 10.0.160.250 | colmex | w2000 | | | | | | | X |
| **EPSILON** | 10.0.160.14 | colmex | w2000 | | | | | | | |
| **URANO** | 10.0.173.58 | colmex | w2000 | | | | X | | | |
| **JUPITER** | 10.0.173.129 | colmex | w2000 | X | | | | | | |
| **MERCURIO** | 10.0.173.65 | colmex | w2000 | X | | | | X | | |
| **ANDROMEDA** | 10.0.160.3 | colmex | w2000 | | | | | | | X |
| **MEXICA** | 10.0.173.233 | colmex | w2000 | | | | | | | X |
| **TEQUILA** | 10.0.162.250 | colmex | w2000 | | | | | | X | |
| **MEZCAL** | 10.0.160.172 | colmex | w2000 | | | | | X | X | |
| **VEGA** | 10.0.162.15 | colmex | w2000 | | | | | | | |
| **CYBERCOP** | 10.0.173.59 | colmex | w2000 | | | | | | | |
| **SNIFFER** | 10.0.173.57 | colmex | w2000 | | | | | | | |
| **MON-RED** | 10.0.173.228 | colmex | w2000 | | | | | X | | |
| **HUEB** | 10.0.173.62 | colmex | w2000 | | | | | X | | |
| ***ADMINISTRACIÓN*** | | | | | | | | | | |
| **XELHA** | 10.0.162.5 | admin | w2000 | | | | | | | |
| **IO** | 10.0.162.8 | admin | w2000 | | | | | | | |
| **TRITON** | 10.0.162.6 | admin | w2000 | | | | | | X | X |
| **JANUS** | 10.0.162.7 | admin | w2000 | | | | | X | | |
| ***BIBLIOTECA*** | | | | | | | | | | |
| **HANDEL** | 10.0.160.202 | colmex | w2000 | | | | | X | | X |
| **BIBLIO2** | 10.0.160.200 | colmex | w2000 | | | | | X | | X |
| **VIVALDI2** | 10.0.161.177 | colmex | NT4 | | | | | | | |
| **CODEX2** | 10.0.161.251 | colmex | Linux | | | | | X | | |
| **CODEX** | 10.0.161.172 | colmex | UNIX v4 Alpha | | | | | X | | |
| **SATURNO** | 10.0.173.131 | colmex | UNIX SUN Spark | | | | | | | X |
| ***ESTUDIANTES*** | | | | | | | | | | |
| **ORION** | 10.0.175.4 | estud | w2000 | | | X | | | | X |
| **CENTAURI** | 10.0.175.3 | estud | w2000 | | | | | | | |
| **CALYPSO** | 10.0.175.1 | estud | w2000 | | | | X | | | |

**DNS** (*Domain Name System*, Sistema de Nombres de Dominios), **WINS** (*Windows Internet Name Service*, Servicio de Nombres de Internet para windows), **SQL** (*Structured Query Language*, Lenguaje de Consultas Estructurado)

Tabla 3.2 Descripción general de servidores de El Colegio

Se realizaron capturas periódicas en horarios y tiempos aleatorios para saber el comportamiento de la red; una de estas capturas se muestra en la figura 3.5. En esta gráfica se ve la utilización del enlace *Ethernet* de la red LAN de El Colegio, la cual en promedio supera el 60 % de utilización con algunos picos en horas de saturación, lo que provoca tiempos de respuesta en la comunicación que son muy elevados.

En la figura 3.6 se muestra en forma detallada los protocolos más utilizados en la red, tanto en número de paquetes como en número de bytes. De esta gráfica se concluye que el protocolo más utilizado es el de HTTP. Por último para el estudio de la red tenemos la gráfica de la figura 3.7 que muestra el protocolo de red TCP/IP que es el predeterminado para configurar los clientes.

Una vez hechas las capturas de información con su respectivo análisis y elaboración de gráficas, se puede concluir que la utilización del enlace *Ethernet* de la red LAN se encuentra saturado por el ancho de banda limitado, como consecuencia del número de usuarios que demandan más conexiones a la red, así como el número de subredes que se tiene en la LAN con tiempos de respuesta elevados.

## 3.4 Problemática de la Situación Actual

- Número de usuarios por subred: el aumento de usuarios que utilizan los recursos de la red e Internet es notorio, por lo tanto la cantidad de tráfico que generan va en aumento lo que provoca un exceso de colisiones, *broadcast* y tiempos de respuesta muy elevados, tanto en la conexión a equipos de su propia subred como la comunicación a otras subredes.

- Subredes: varias subredes de la red se encuentran cercanas a la saturación, lo que degrada sus tiempos de respuesta.

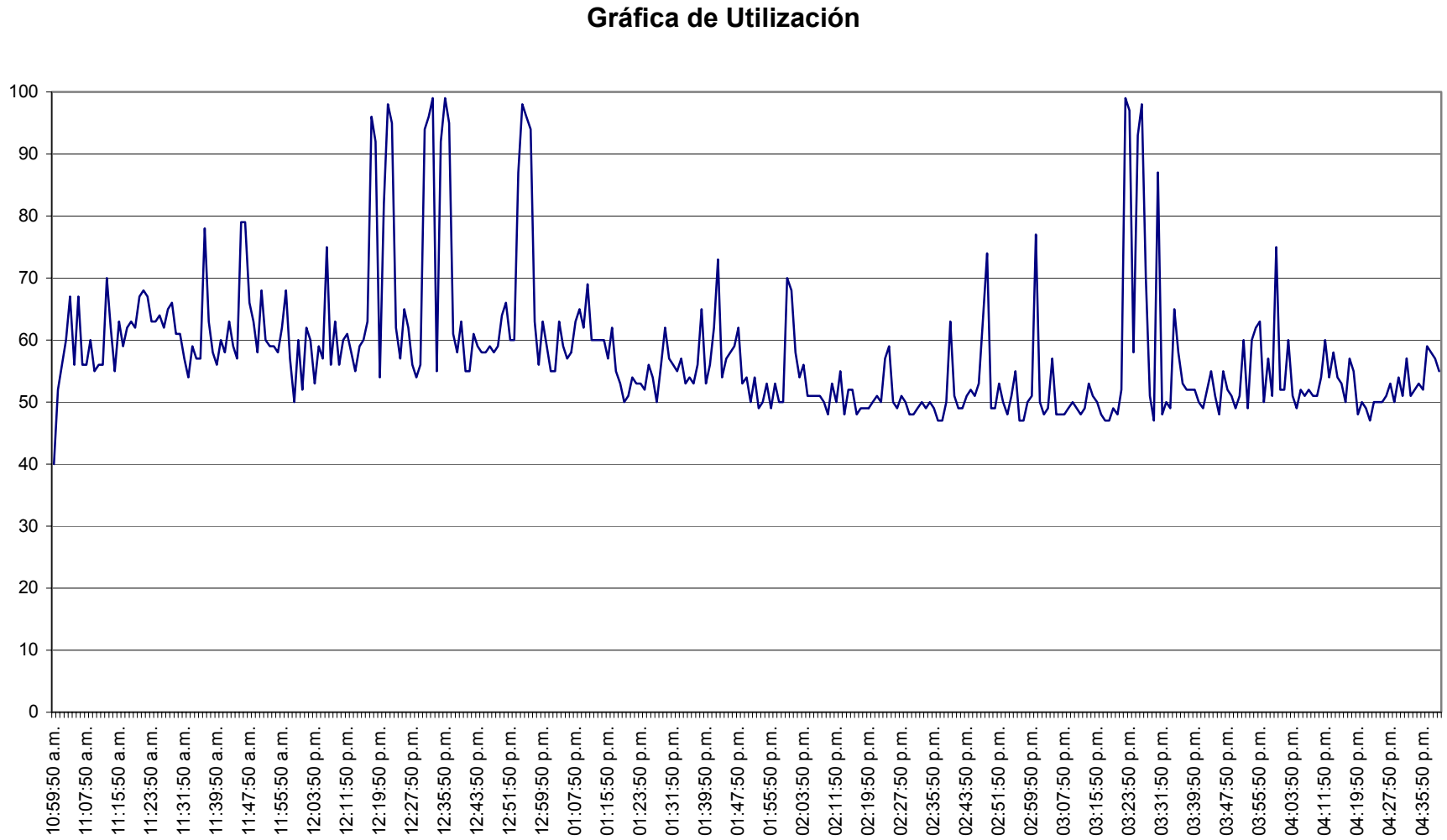
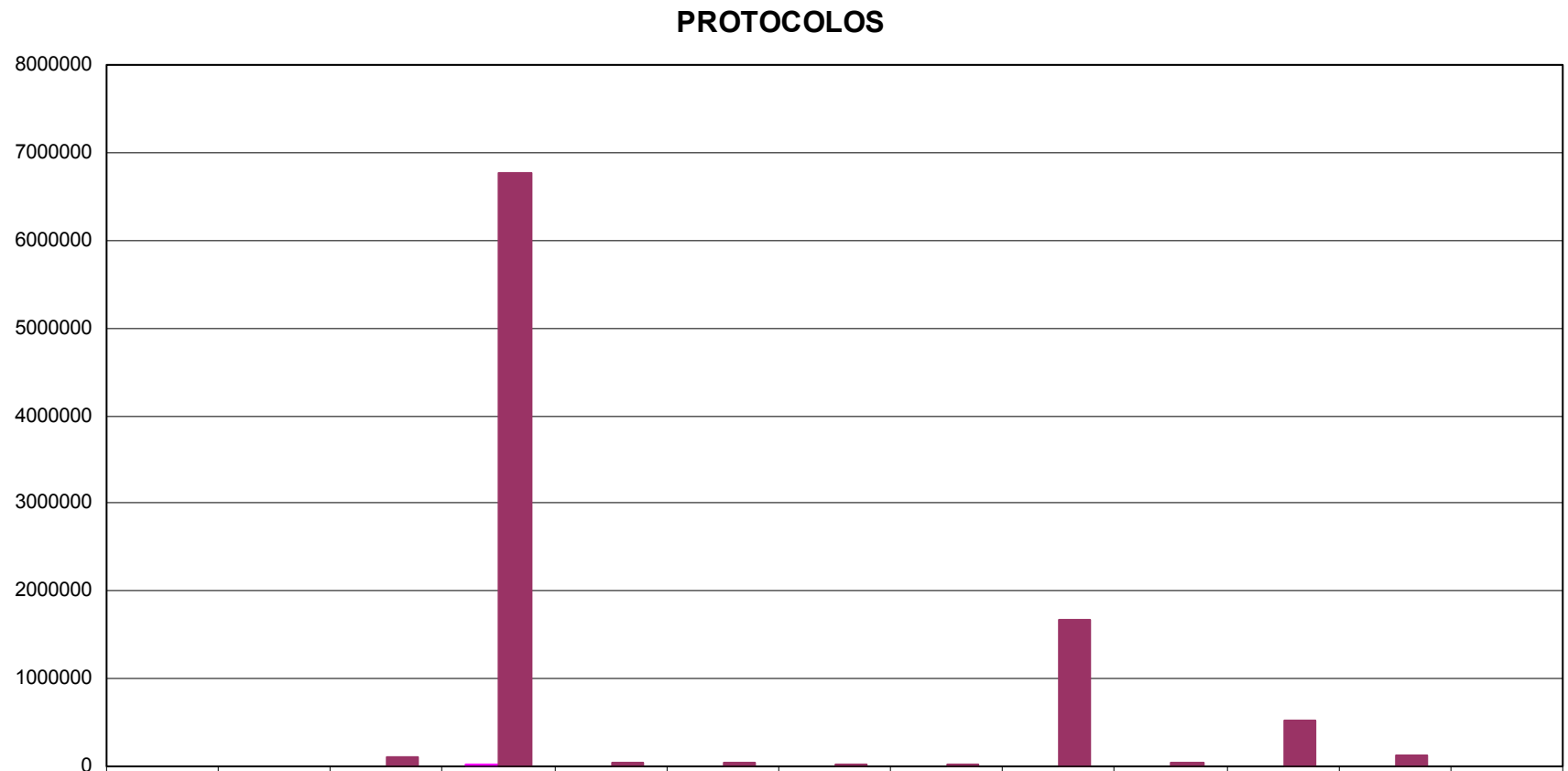



Figura 3.5 Gráfica de utilización de la Red LAN en El Colegio




| | Bootpc | Bootps | DNS | HTTP | HTTPS | ICMP | NetBIOS_DGM_T | NetBIOS_NS_T | NetBIOS_SSN_T | POP3 | SMTP | SNMP | Telnet |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Packets | 8 | 5 | 838 | 13351 | 84 | 514 | 63 | 139 | 5412 | 298 | 1242 | 994 | 6 |
| Bytes | 2768 | 1805 | 114797 | 6759413 | 51642 | 34439 | 16596 | 14294 | 1669105 | 51521 | 513548 | 130688 | 439 |

Figura 3.6 Gráfica de protocolos más utilizados en la red LAN

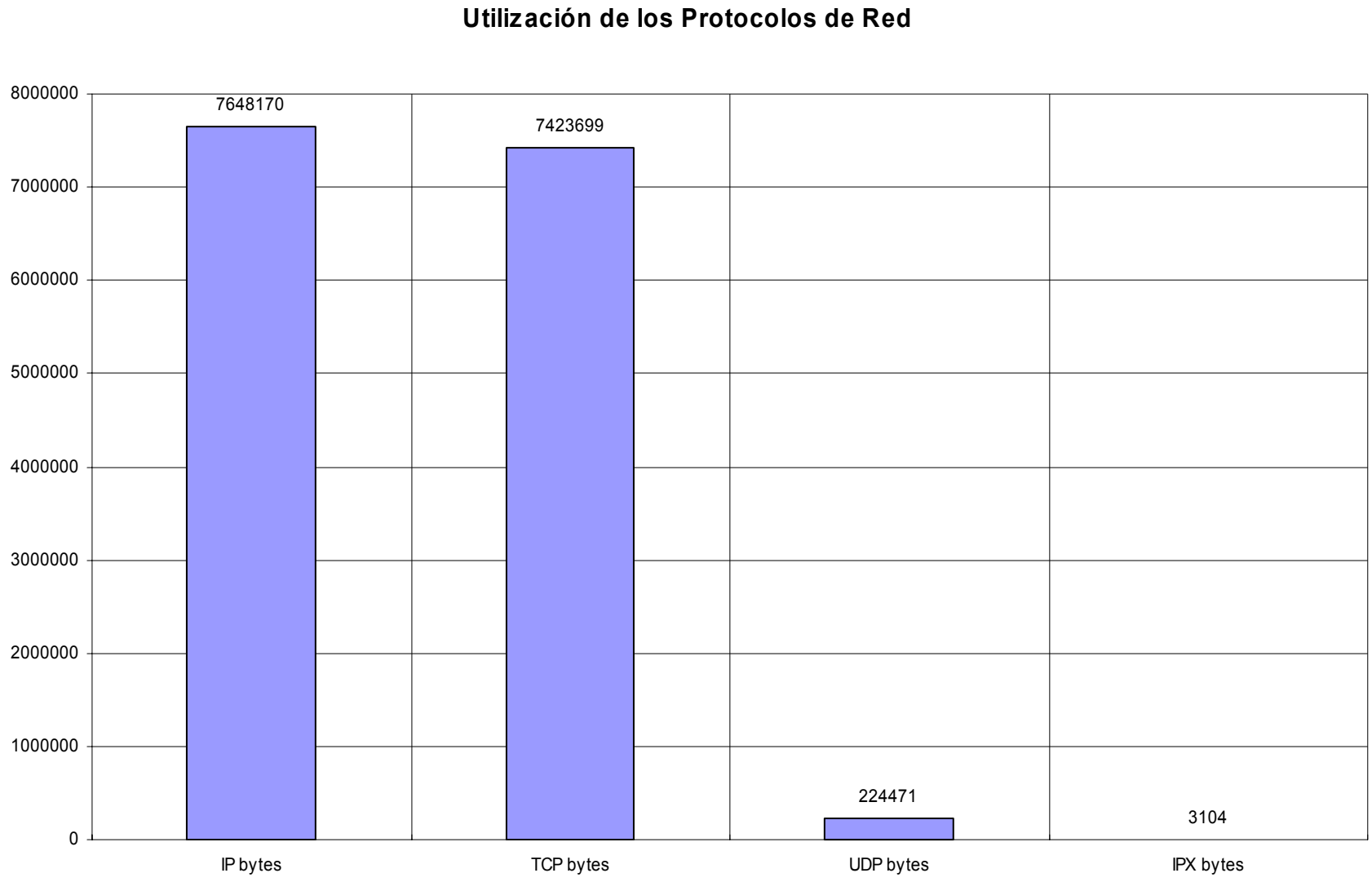



Figura 3.7 Utilización de el protocolo TCP/IP

- Subredes de servidores: el tráfico generado por las solicitudes de todas las subredes provoca una saturación en momentos pico.

- Servidores y Workstations: la mayor parte de servidores y estaciones de trabajo se encuentran en una subred (10.0.173.0), por lo que su tráfico en general se logra aislar de las demás subredes. Pero hay servidores que requieren ser consultados y requeridos por varios usuarios desde otras subredes, por lo que el tráfico es excesivo.

- Seguridad de información: el direccionamiento de la red es otorgado dinámicamente en la mayoría de la red, por lo que cualquier computadora de cualquier área puede tomar una dirección IP de la subred que el servidor tenga disponible. Pero hay áreas específicas que manejan información confidencial, por lo que su tráfico no está aislado de toda la red.

- Seguridad de red: en el mundo de la información la seguridad es un punto importante para el buen funcionamiento de la red. Se tienen algunos filtros en el *router* que nos ayudan de los ataques externos. Pero como está comprobado, la mayor parte de los ataques son por usuarios internos que aprovechan cualquier debilidad para atacar, borrar o extraer información.

- *Backbone:* el crecimiento de usuarios y equipos que día a día utilizan los recursos de la red e Internet, y aplicaciones que demandan mayor ancho de banda, hace que el equipo central que es la espina dorsal de la red se encuentre cercano a la saturación.

- *Router*: la utilización de aplicaciones de Internet es cada vez más usado por los usuarios lo que provoca saturación en memoria y procesamiento del *router*. Esto sumado con los nuevos proyectos en los que se está trabajando, como son Internet2 e IPv6.

## 3.5 Propuesta de Solución

De acuerdo con el análisis de la red obtenido anteriormente y de la problemática actual de El Colegio, se hace una propuesta de solución que se engloba en los siguientes puntos:

- Explotar las capacidades que ofrece la tecnología de conmutación (*switching*) sobre la red LAN conmutada de la Institución.

- La creación de redes virtuales (VLANs) para la segmentación del tráfico que se genera de las diferentes áreas y dominios en la infraestructura actual de la red de El Colegio.

- La seguridad en la información es parte fundamental, por lo que se propone la adecuación específica del *Firewall* para robustecer la seguridad entre las VLANs que se generen.

- El ruteo es muy importante para la comunicación entre VLANs por lo que se tiene que implementar un *router*. Para esta propuesta la función del *router* la hará el *Firewall*, donde se habilitará el servicio de ruteo al servidor donde está instalado el *Firewall*.

- La organización de los servicios que brindan los servidores es fundamental para la distribución de tráfico que es generado en la red, por tanto la distribución de servidores dependerá de la VLAN donde se demande más los servicios de red.

- El *Backbone* es parte esencial de la red por lo cual se propone hacer una actualización por un equipo que cumpla con los nuevos requerimientos y especificaciones, principalmente para soportar la exigencia en capacidades, la

creación de la redes virtuales y al mismo tiempo poner al día un equipo que ya supera los 3 años de vida.

- Por último, en esta propuesta de solución es indispensable la adquisición de un *router*, que como se comentó en el punto anterior el equipo ya ha superado el tiempo de vida por lo que se requiere la actualización del mismo, tanto por su obsolescencia como también por los requerimientos que se necesitan para nuevos proyectos.

Los puntos antes citados engloban una solución completa para mejorar el desempeño de la infraestructura de la red que se tiene actualmente. Por lo que se requiere un plan de trabajo para su reestructuración.

La reestructuración comprende una organización más eficiente de la infraestructura de red en conjunto con los servicios que se ofrecen. Seleccionar el o los equipos que soportan en mejor medida las nuevas capacidades demandadas en el *Backbone*, haciendo énfasis en el manejo de redes virtuales.

## 3.6 Consideraciones en la Creación de VLANs

Un paso importante sobre el concepto de redes virtuales, es saber primeramente los requerimientos que debe tener una VLAN para su creación. Estos requerimientos deben ser considerados antes de saber que tipo de VLAN es la adecuada en el diseño de solución del proyecto.

Las consideraciones son las siguientes:

- Configuración de las VLANs: en el desarrollo de las VLANs representa el grado de automatización que puede tener la configuración, que depende de la forma de

agrupamiento definido. Hay tres niveles de automatización en la configuración de las VLANs:

1. Configuración Manual: Tanto la inicialización como los movimientos y los cambios son controlados por el administrador de la red. La configuración manual permite un alto grado de control. Sin embargo en grandes redes es poco práctico, anulando uno de los beneficios de las VLANs que es disminuir el tiempo que toma hacer un cambio o movimiento en la red.
2. Configuración Semiautomática: Se refiere a la opción de automatizar cualquiera de las configuraciones, cambios y/o movimientos. La configuración semiautomática podría también referirse a situaciones donde las VLANs son inicializadas manualmente, con los movimientos rastreados automáticamente.
3. Configuración automática: Un sistema que automatiza totalmente la configuración de las VLANs requiere que sus estaciones de trabajo puedan ser configuradas de forma dinámica y automática, en función de la aplicación, de la identificación del usuario o de los criterios de los administradores de red.

- Estandarización de las VLANs: debido a las definiciones de las VLANs y a las diferentes formas de manejo de los switches cada fabricante ha desarrollado su propia solución, dando como resultado que los switches de un fabricante no interoperen completamente con las VLANs de otro, obligando a los usuarios a comprar a un único proveedor.

- Ruteo entre VLANs: el ruteo es requerido para el tráfico entre las redes virtuales. El mejor desempeño de las VLANs es cuando hay poco tráfico que circule por el *router*.

- Seguridad de las VLANs: una característica de las VLANs es la de delimitar el tráfico de red LAN en un área específica (generalmente realizado por el *router*) y que no se propague a otras áreas, esto puede satisfacer algunos requerimientos de seguridad y aún reemplazar funciones de los *routers*.

# 4. DISEÑO

Una vez realizado el estudio de la red, analizada la problemática y hecha una propuesta de solución, es necesario realizar el diseño de la infraestructura de red que resuelva la problemática, que permita su crecimiento y mejore sustantivamente su desempeño.

La elaboración del diseño contempla en su solución los siguientes niveles:

- La de usuario,
- La de acceso, y
- La de *Backbone*.

El nivel de usuario, que define el acceso a los recursos de la red local y es determinado por ser fuente de origen de datos o destino de ellos; enfoca su atención en protocolos LAN, interfaces y tecnologías. En este nivel de usuario, la Institución utilizará el protocolo TCP/IP, por ser un estándar de comunicaciones entre computadoras, además de ser éste robusto y confiable.

Las interfaces son *hardware* (tarjetas de red, computadoras, cableado estructurado) y *software* (sistemas operativos y aplicaciones). Por último la tecnología que se utilizará en la red LAN de la Institución, es la *Ethernet*, por ser una tecnología de transmisión de datos de alta velocidad; además de que mantiene una tendencia evolutiva a nivel tecnológico y comercial.

El nivel de acceso, se define como el punto de ingreso del usuario a la capa *Backbone*. Típicamente los dispositivos de acceso incluyen a *routers, bridges*, *switches* o cualquier otro dispositivo que proporcione un punto focal de estandarización de interfaces, protocolos, arquitecturas, tecnologías, funciones y servicios requeridos. En éste caso específico se utilizarán *switches* para extender la red virtual y permitir la conexión directa del usuario final.

Por último, el nivel de *Backbone*, es la unión de una serie de enlaces que forman un eje de conexión principal; es la columna vertebral de la red. Es en este nivel, donde se crearán las redes virtuales o dominios lógicos (VLANs).

### 4.1.1 Dominios Lógicos (VLANs)

Los esquemas VLAN proporcionan los medios adecuados para la agrupación de usuarios en forma lógica. Sin embargo, las redes virtuales siguen compartiendo las características de los grupos de trabajo físicos, en el sentido de que todos los usuarios comparten sus dominios de *broadcast*.

Una de las cualidades de la VLAN es que los usuarios pueden ser distribuidos a través de la LAN y pertenecer al mismo grupo de trabajo lógico. Además, al poder distribuir a los usuarios en diferentes segmentos, logra como consecuencia directa, el incremento del ancho de banda en dichos grupos de usuarios.

El Colegio de México en su estructura básica esta constituida por áreas de investigación, educación y administración. Partimos de lo anterior para crear las VLANs; la razón para hacer esta división es obtener mayores beneficios para la Institución y a los administradores de la red, como: mejor administración y control de las redes virtuales, organización general del tráfico que cursa en la red, control del tipo de datos que se genera en cada una ellas, seguridad de la información de cada red virtual y delimitación por ubicación física de las áreas.

Las redes virtuales a considerar son las siguientes:

1. Profesores,
2. Estudiantes,
3. Administración,
4. Biblioteca,
5. Laboratorio.

VLAN_Profesores.- La red virtual estará formada principalmente por los centros de estudios e investigación que forman El Colegio de México, razón por la cual ésta concentra la mayor parte de los datos, aplicaciones y servicios que ofrece la Coordinación de Servicios de Cómputo a los usuarios.

VLAN_Estudiantes.- Es la red virtual que se creará para los alumnos que cursan una licenciatura, maestría, doctorado o algún otro plan de estudios que brinda El Colegio. En esta red virtual estarán concentrados datos, aplicaciones y servicios que se proporcionan a los alumnos. Y será utilizada sólo para sus intereses académicos y de investigación.

VLAN_Administración.- El área Administrativa constituye una parte fundamental de El Colegio. La información que manipula es confidencial e importante; por tal motivo se creará una red virtual que facilite la implementación de mecanismos de seguridad sobre los datos y aplicaciones.

VLAN_Biblioteca.- La Biblioteca de El Colegio está clasificada como universitaria, especializada y de investigación, abierta a maestros, investigadores y alumnos, así como a toda persona de instituciones de educación superior y de otros sectores sociales del país. Es un área que tiene autonomía, y por ello brinda servicios y aplicaciones para usuarios tanto internos como externos.

VLAN_Laboratorio.- Esta red virtual será de uso exclusivo de la Coordinación de Servicios de Cómputo, la cual será utilizada para pruebas y ejercicios relacionados con la investigación de Tecnologías de la Información.

La descripción anterior, representa a los Dominios Lógicos que serán creados para tener mejor organización y administración de la red; por consiguiente, mejor desempeño de la misma. Se crean redes virtuales para evitar que el tráfico que no corresponda a esa VLAN se propague a los demás Dominios Lógicos, y con ello mejorar los tiempos de respuesta y el acceso a los recursos de la red.

En la tabla 4.1 se muestran las VLANs que se van a crear con sus respectivas áreas asignadas:

| Nombre de la VLAN | Áreas asignadas |
|---|---|
| VLAN_Profesores | • Coordinación de Servicios de Cómputo<br>• Área de Presidencia<br>• Centro de Estudios Demográficos y de Desarrollo Urbano<br>• Centro de Estudios Económicos<br>• Centro de Estudios Históricos<br>• Centro de Estudios Internacionales<br>• Centro de Estudios de Asia y África<br>• Centro de Estudios Sociológicos<br>• Centro de Estudios Lingüísticos y Literarios<br>• Diccionario del Español de México<br>• Programa Interdisciplinario de Estudios de la Mujer<br>• Programa de Investigadores Asociados<br>• Programa de Estudios Avanzados y Desarrollo Sustentable y Medio Ambiente<br>• Programa para la Formación de Traductores<br>• Sistema de Información Geográfica<br>• Asuntos Escolares<br>• Auditorio “Alfonso Reyes” |
| VLAN_Estudiantes | • Salones<br>• Sala de Cómputo de la Planta Baja de Biblioteca<br>• Sala de Cómputo de la Coordinación de Servicios de Cómputo |
| VLAN_Administración | • Área administrativa<br>• Conmutador<br>• Dirección de Publicaciones<br>• Bodegas<br>• Sala Audiovisual<br>• Archivo Histórico<br>• Áreas de Documentación |
| VLAN_Biblioteca | • Biblioteca “Daniel Cosío Villegas” |
| VLAN_Laboratorio | • Laboratorio de la Coordinación de Servicios de Cómputo |

Tabla 4.1 Asignación de VLANs

Las áreas asignadas están organizadas en subsistemas llamados IDF´s (*Intermediate Distribution Frame*, Subsistema de Administración Intermedio). Los subsistemas se encuentran distribuidos en los niveles del edificio de El Colegio de México, como lo muestra la figura 4.1.

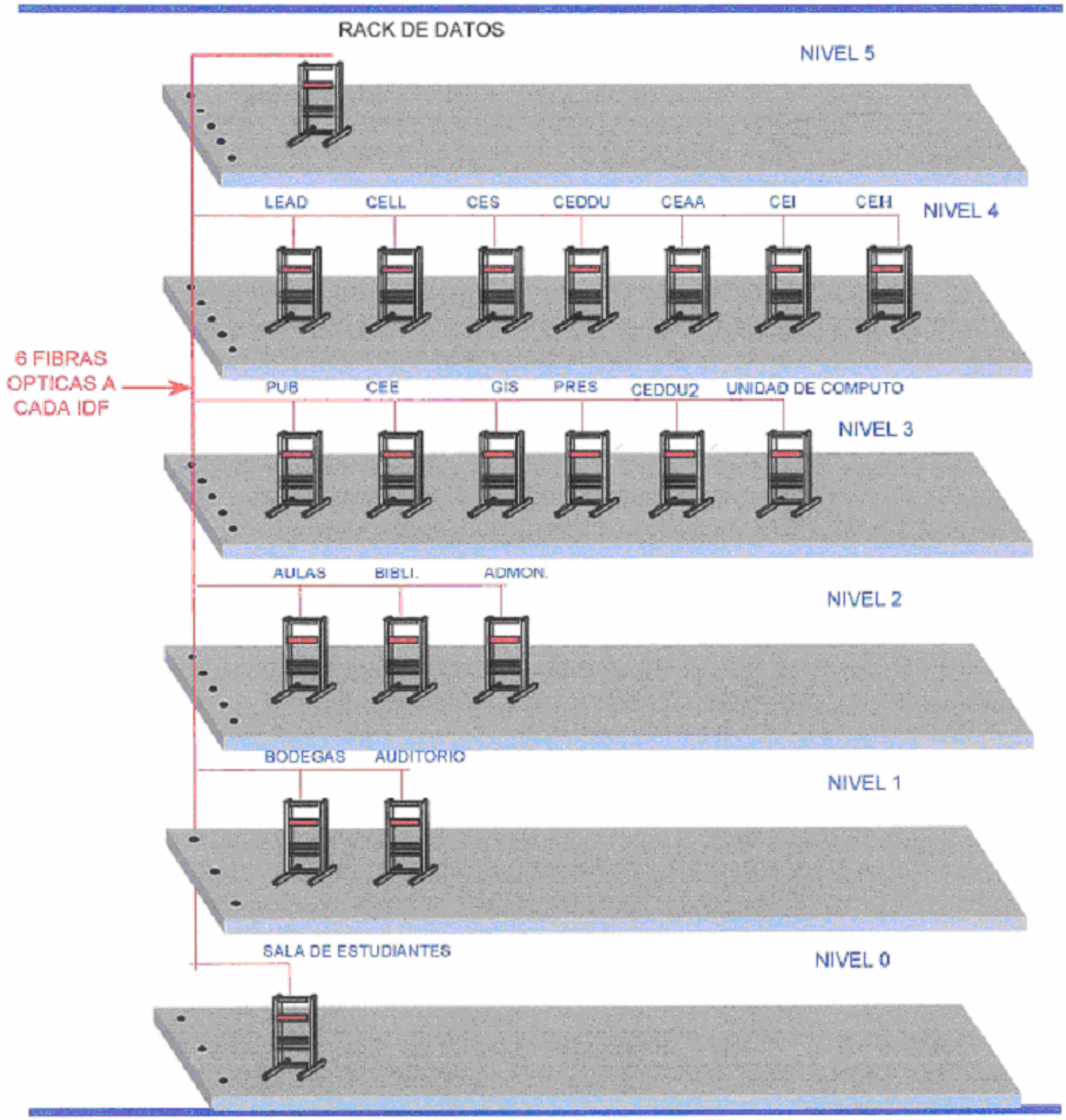



Figura 4.1 Distribución de los subsistemas en los niveles del edificio de El Colegio de México

Los subsistemas de acceso a la red dan servicio a los centros, programas, áreas administrativas y de servicio. Estos subsistemas están organizados por áreas, como lo muestra la tabla 4.2.

| No. | Nombre del IDF | Áreas que cubre |
|---|---|---|
| **1** | Estudiantes | Sala de Cómputo de la Planta Baja de Biblioteca |
| **2** | Auditorio | Auditorio “Alfonso Reyes” |
| **3** | Bodegas | Bodegas<br>Sala Audiovisual<br>Archivo Histórico<br>Áreas de Documentación |
| **4** | Administración | Área administrativa<br>Conmutador |
| **5** | Biblioteca | Biblioteca “Daniel Cosío Villegas” |
| **6** | Aulas | Salones |
| **7** | Unidad de Cómputo | Coordinación de Servicios de Cómputo<br>Diccionario del Español de México<br>Programa Interdisciplinario de Estudios de la Mujer |
| **8** | Ceddu | Dirección del Centro de Estudios Demográficos y de Desarrollo Urbano<br>Cubículos del 4° Nivel asignados al centro de estudios |
| **9** | Ceddu2 | Dirección del Centro de Estudios Demográficos y de Desarrollo Urbano<br>Programa de Investigadores Asociados |
| **10** | Presidencia | Área de Presidencia |
| **11** | Gis | Sistema de Información Geográfica<br>Asuntos Escolares<br>Sala de Cómputo de la Coordinación de Servicios de Cómputo |
| **12** | Cee | Dirección del Centro de Estudios Económicos<br>Cubículos del 4° Nivel asignados al centro de estudios |
| **13** | Publicaciones | Dirección de Publicaciones |
| **14** | Ceh | Dirección del Centro de Estudios Históricos<br>Cubículos del 4° Nivel asignados al centro de estudios |
| **15** | Cei | Dirección del Centro de Estudios Internacionales<br>Cubículos del 4° Nivel asignados al centro de estudios |
| **16** | Ceaa | Dirección del Centro de Estudios de Asia y África<br>Cubículos del 4° Nivel asignados al centro de estudios |
| **17** | Ces | Dirección del Centro de Estudios Sociológicos<br>Cubículos del 4° Nivel asignados al centro de estudios |
| **18** | Cell | Dirección del Centro de Estudios Lingüísticos y Literarios<br>Cubículos del 4° Nivel asignados al centro de estudios |
| **19** | Lead | Programa de Estudios Avanzados y Desarrollo Sustentable y Medio Ambiente<br>Programa para la Formación de Traductores |
| **20** | 5toNivel | Cubículos asignados a los Centros de Estudios |

Tabla 4.2 Áreas asignadas en los subsistemas (IDF´s).

La creación de las redes virtuales, como se mencionó anteriormente, se realizará en el *Backbone*, por lo que se necesitará configurar lógicamente para hacer la distribución de las redes virtuales. La figura 4.2 muestra las VLANs que serán creadas, con los subsistemas asignados respectivamente:

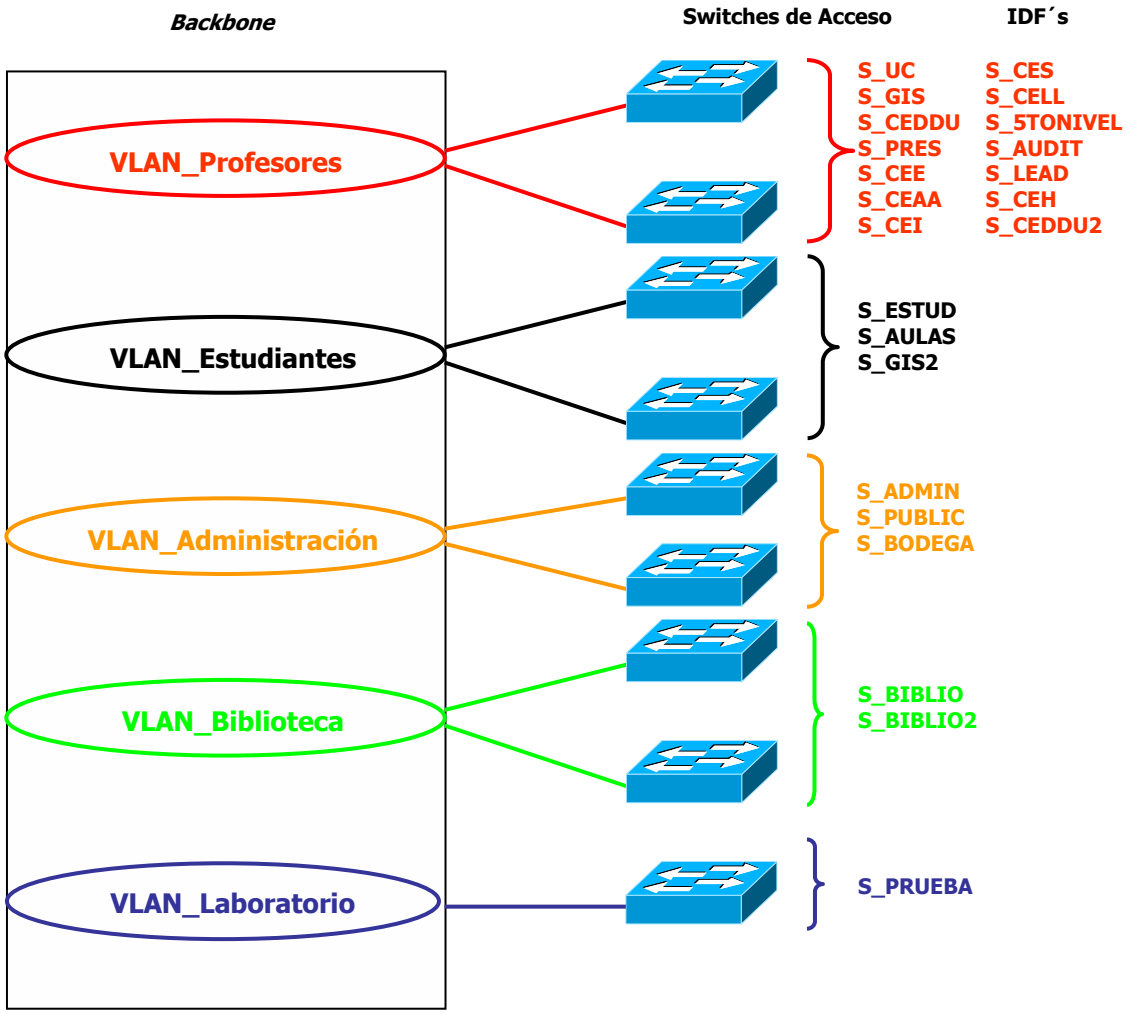



Figura 4.2 Creación de la VLANs en el *Backbone*, con la asignación de los IDF´s

Cabe mencionar la importancia de tener un sistema de cableado óptimo en su parte de distribución y asignación de puertos de acceso, para facilitar la configuración lógica de las redes virtuales. De ésta manera es factible configurar las VLANs en base a puertos en el *Backbone*.

### 4.1.2 Servicios y Aplicaciones por VLANs

Una vez que se realicen las VLANs o Dominios Lógicos, es necesario hacer una distribución de los servicios y aplicaciones para cada una de las redes virtuales. Por lo que deben estar muy bien organizados y distribuidos; esto también dependerá de quién o quienes usen más los recursos de la red.

- La VLAN de Profesores que es donde recae la mayor parte de los usuarios y son quienes más demandarán los recursos y servicios de la red. En está VLAN se encuentran los principales servicios que proporciona la Coordinación de Servicios de Cómputo: correo electrónico, servidor *web*, programas de aplicaciones, bases de datos, impresoras y datos.

- La VLAN de Estudiantes también cuenta con servicios y aplicaciones propios, que utilizan para su estudio y desarrollo conforme a sus planes de estudio. Estos servicios y aplicaciones son, básicamente, datos, programas de aplicaciones e impresoras.

- La VLAN de Administración es, igual que las anteriores, muy importante por la información que ahí se genera y se maneja. En está VLAN los principales servicios que se administrarán son: bases de datos, servidor *web* y datos.

- Los servicios que brinda la VLAN de Biblioteca son básicos en la comunidad, como el préstamo de material bibliográfico, folletos, consulta de video, catálogos, etc., para usuarios internos y externos. La Biblioteca administra su sitio *web*, los catálogos, sus bases de datos y programas específicos.

- Por último, en la VLAN de Laboratorio, será para uso de investigación y desarrollo, se utilizarán servicios y aplicaciones en base al tipo de pruebas que se necesiten, para no afectar la red que está en uso.

Con la distribución de las aplicaciones para cada uno de los Dominios Lógicos, se pretende tener mejor administración y control de los servicios, para que su tráfico se conserve “local” al grupo de trabajo y se evite el cruce de información entre el resto de las redes virtuales. La tabla 4.3 muestra los servidores con los servicios y aplicaciones que proporcionaran a cada una de las redes virtuales.

| Nombre de la VLAN | Nombre del Servidor | Servicios que proporciona |
|---|---|---|
| VLAN_Profesores | GAMA | *Domain Controller*, DHCP, DNS Primario, Datos, WINS, Impresoras, TACACS para el Acceso Remoto |
| | MEXICA | Datos, DNS Secundario |
| | DELTA | Datos, Impresoras, *Domain Controller* |
| | EPSILON | Datos, Impresoras, *Domain Controller* |
| | MERCURIO | Servidor de páginas Web |
| | HUEB | Servidor de FTP |
| | URANO | Correo Electrónico |
| | FOBOS | Antivirus de correo SMTP WEBSHIELD |
| | WODKA | Bases de Datos |
| | MEZCAL | Bases de Datos |
| | ANDROMEDA | Servidor de distribución antivirus, Datos |
| | MONRED | Monitoreo de Enlaces WAN, HP OPENVIEW, MRTG |
| | TIERRA | Servidor de correo no deseado (antispam) |
| VLAN_Estudiantes | ORION | DHCP, WINS, Impresoras, *Homes* de Estudiantes, Programas, *Domain Controller* |
| | CENTAURI | *Domain Controller*, Datos |
| VLAN_Administración | VEGA | DHCP, WINS, Impresoras |
| | XELHA | Bases de Datos |
| | JANUS | Servidor de páginas Web |
| | TRITON | Bases de Datos |
| | TEQUILA | Bases de Datos |
| | IO | Impresoras |

| Nombre de la VLAN | Nombre del Servidor | Servicios que proporciona |
|---|---|---|
| VLAN_Biblioteca | BIBLIO2 | DHCP, WINS, Impresoras, Biblioteca Digital Aplicaciones Java |
| | HANDEL | Servidor de páginas Web, Intranet, Aplicaciones |
| | VIVALDI | Servidor de bases de datos en disco compacto Impresoras |
| | CODEX | Servidor ALEPH, Catálogo Público |
| | CODEX3 | Servidor ALEPH |
| VLAN_Laboratorio | PC-Server | *Any* |
| | PC-Lab1 | *Any* |
| | PC-Lab2 | *Any* |

Tabla 4.3 Distribución de servidores para las VLANs

Es importante hacer notar que los servicios IP correspondientes a DHCP (*Dynamic Host Configuration Protocol*, Protocolo de Configuración Dinámica para los Anfitriones) y WINS (*Windows Internet Name Service*, Servicio de Nombres de Internet para Windows) serán configurados en cada VLAN para minimizar tráfico entre VLANs.

### 4.1.3 Esquema de direccionamiento

La parte de direccionamiento es esencial en esta parte del diseño para las redes virtuales, puesto que nos permitirá identificar la red virtual. Las redes con las que se contara para el desarrollo de las VLANs son las siguientes:

- 10.0.173.0/24
- 10.0.175.0/24
- 10.0.160.0/24
- 10.0.161.0/24
- 10.0.162.0/24
- 10.0.163.0/24
- 192.168.1.0/24

De estas redes, todas son Homologadas a excepción de la 192.168.1.0, que es No Homologada. Esta red No Homologada; ésta será utilizada para la VLAN de Laboratorio, que no necesariamente requiere de una red Homologada puesto que la red virtual sólo la ocuparemos para pruebas. Las redes con las que se cuenta son clase “C”, con máscara de 24 bits; es decir que tenemos 256 *hosts* por cada red, de los cuales son utilizables 254; esto se debe a que una dirección se usa para identificar la red y la otra para la dirección de *broadcast*.

En la tabla 4.4 se muestra el direccionamiento que va hacer asignado para cada una de las redes virtuales, así como las áreas que serán atendidas.

| Nombre de la VLAN | Áreas atendidas | Segmento asignado |
|---|---|---|
| VLAN_Profesores | Coordinación de Servicios de Cómputo<br>Área de Presidencia<br>Centro de Estudios Demográficos y de Desarrollo Urbano<br>Centro de Estudios Económicos<br>Centro de Estudios Históricos<br>Centro de Estudios Internacionales<br>Centro de Estudios de Asia y África<br>Centro de Estudios Sociológicos<br>Centro de Estudios Lingüísticos y Literarios<br>Diccionario del Español de México<br>Programa Interdisciplinario de Estudios de la Mujer<br>Programa de Investigadores Asociados<br>Programa de Estudios Avanzados y Desarrollo Sustentable y Medio Ambiente<br>Programa para la Formación de Traductores<br>Sistema de Información Geográfica<br>Asuntos Escolares<br>Auditorio “Alfonso Reyes” | 10.0.173.0/24<br>10.0.160.0/24<br>10.0.163.0/24 |
| VLAN_Estudiantes | Salones<br>Sala de Cómputo de la Planta Baja de Biblioteca<br>Sala de Cómputo de la Coordinación de Servicios de Cómputo | 10.0.175.0/24 |

| Nombre de la VLAN | Áreas atendidas | Segmento asignado |
|---|---|---|
| VLAN_Administración | Área administrativa<br>Conmutador<br>Dirección de Publicaciones<br>Bodegas<br>Sala Audiovisual<br>Archivo Histórico<br>Áreas de Documentación | 10.0.162.0/24 |
| VLAN_Biblioteca | Biblioteca “Daniel Cosío Villegas” | 10.0.161.0/24 |
| VLAN_Laboratorio | Laboratorio de la Coordinación de Servicios de Cómputo | 192.168.1.0/24 |

Tabla 4.4 Asignación del direccionamiento a las VLANs

Para la asignación de direcciones IP a los usuarios finales, se cuenta con un servidor exclusivo DHCP por VLAN, lo que complementa la configuración lógica general de la red LAN, excepto para la VLAN de Laboratorio, que no lo requiere.

La red 10.0.173.0/24, es utilizada para equipos de comunicaciones (*routers, switches, hubs, modems*), servidores, estaciones de trabajo e impresoras, por lo cual no está configurada en el servicio de DHCP.

La red 10.0.160.0/24 está configurada en el servidor GAMA, que tiene el servicio de DHCP para ser usadas por los usuarios de la VLAN de Profesores. La red 10.0.163.0/24 al igual que la anterior está configurada en el servidor GAMA para los clientes.

La red 10.0.175.0/24 es la asignada para la VLAN de Estudiantes, que será utilizada para sus equipos de comunicaciones, servidores, impresoras y clientes.

La red 10.0.162.0/24 es para la VLAN de Administración, y en ella también se encuentran sus equipos de comunicaciones, servidores, estaciones de trabajo, impresoras y los clientes.

La red 10.0.161.0/24 está asignada para la VLAN de Biblioteca, para los equipos de comunicaciones, servidores, estaciones de trabajo, impresoras y los clientes.

Por último la red 192.168.1.0/24 es para la VLAN de Laboratorio, que será utilizada para los equipos de prueba.

En cada una de las redes virtuales, como se mencionó anteriormente, se encuentran servidores con sus servicios y aplicaciones, motivo por el cual, deben tener un direccionamiento IP que pertenezca a la red virtual asignada.

La tabla 4.5 muestra el direccionamiento que deberán tiener los servidores para cada una de las redes virtuales.

| Nombre de la VLAN | Nombre del Servidor | Dirección IP asignado |
|---|---|---|
| VLAN_Profesores | GAMA | 10.0.173.134<br>10.0.160.1<br>10.0.163.252 |
| | MEXICA | 10.0.173.233 |
| VLAN_Profesores | DELTA | 10.0.160.250 |
| | EPSILON | 10.0.160.14 |
| | MERCURIO | 10.0.173.65 |
| | HUEB | 10.0.173.62 |
| | URANO | 10.0.173.58 |
| | FOBOS | 10.0.173.244 |
| | WODKA | 10.0.173.60 |
| | MEZCAL | 10.0.160.172 |
| | ANDROMEDA | 10.0.160.3 |
| | MONRED | 10.0.173.228 |
| | TIERRA | 10.0.173.63 |
| VLAN_Estudiantes | ORION | 10.0.175.4 |
| | CENTAURI | 10.0.175.3 |

| Nombre de la VLAN | Nombre del Servidor | Dirección IP asignado |
|---|---|---|
| VLAN_Administración | VEGA | 10.0.162.15 |
| | XELHA | 10.0.162.5 |
| | JANUS | 10.0.162.4 |
| | TRITON | 10.0.162.62 |
| | TEQUILA | 10.0.162.20 |
| | IO | 10.0.162.8 |
| VLAN_Biblioteca | BIBLIO2 | 10.0.161.9 |
| | HANDEL | 10.0.161.8 |
| | VIVALDI | 10.0.161.177 |
| | CODEX | 10.0.161.172 |
| | CODEX3 | 10.0.161.246 |
| VLAN_Laboratorio | PC-Server | 192.168.1.1 |
| | PC-Lab1 | 192.168.1.2 |

Tabla 4.5 Direccionamiento de los servidores

Por otra parte, en su sección de seguridad El Colegio cuenta con un *Firewall*, *Check Point*, el cual es necesario adaptar a los nuevos requerimientos que las redes virtuales demandan. La ubicación donde se encuentra el *Firewall* es entre el *router* y *Backbone*, como lo muestra en la figura 4.3; el motivo de esta configuración es para la protección y seguridad de la red LAN de posibles ataques de *hackers*.

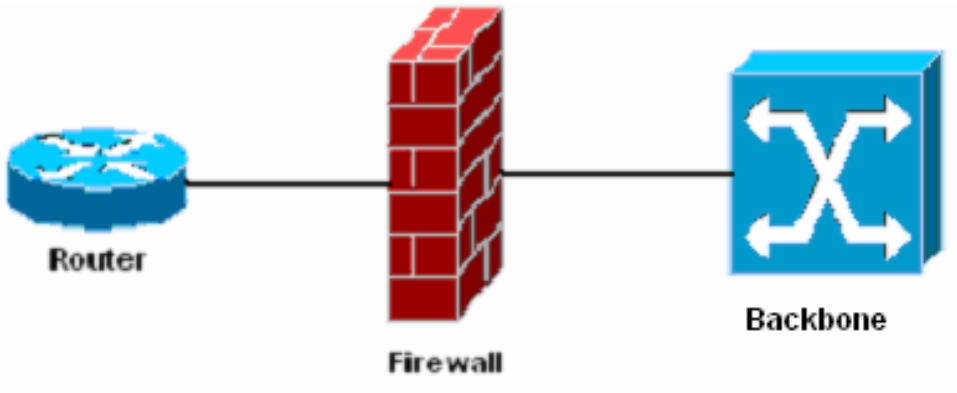



Figura 4.3 Diagrama de conexiones del *Firewall*

Partimos de esta configuración para adaptar las conexiones de las redes virtuales (creadas en el *Backbone*) con el *Firewall*. En el éste, aparte de tener incluida una tarjeta de red, se le instalarán otras dos tarjetas con cuatro puertos de red cada una; el hecho de agregar estas tarjetas de red es por el número de redes virtuales que se crearan y por un posible crecimiento de éstas en un futuro.

En estas tarjetas se hará la conexión entre las redes virtuales creadas en el *Backbone* y el *Firewall*; la conexión entre estos equipos de comunicaciones será por medio de un cable UTP por cada una de ellas. Finalmente, la conexión del *Firewall* con el *router* será también por un puerto de red del *Firewall* con el puerto *Ethernet* del *router*; igualmente será por medio de un cable UTP.

Una vez creadas las redes virtuales en el *Backbone*, se establece el direccionamiento para cada una de las interfaces de las redes virtuales con el *Firewall*; por ejemplo, el *default gateway* configurado en el *Firewall* para la VLAN de Profesores es la 10.0.173.254, 10.0.254 y 10.0.163.254; para la VLAN de Estudiantes es la 10.0.175.254; la de VLAN de Administración es la 10.0.162.254; para la VLAN de Biblioteca se tiene contemplado que sea la 10.0.161.254 y por último para la VLAN de Laboratorio el *default gateway* es la 192.168.1.254

El direccionamiento externo para el *Firewall, router* y servidores, es la red 10.0.255.0/24. La dirección IP del *Firewall* es la 10.0.255.1 y para el *router* su dirección IP en la interfaz *ethernet* es la 10.0.255.254.

La figura 4.4 muestra el direccionamiento asignado para las redes virtuales, así como para el *Firewall* y el *router*.

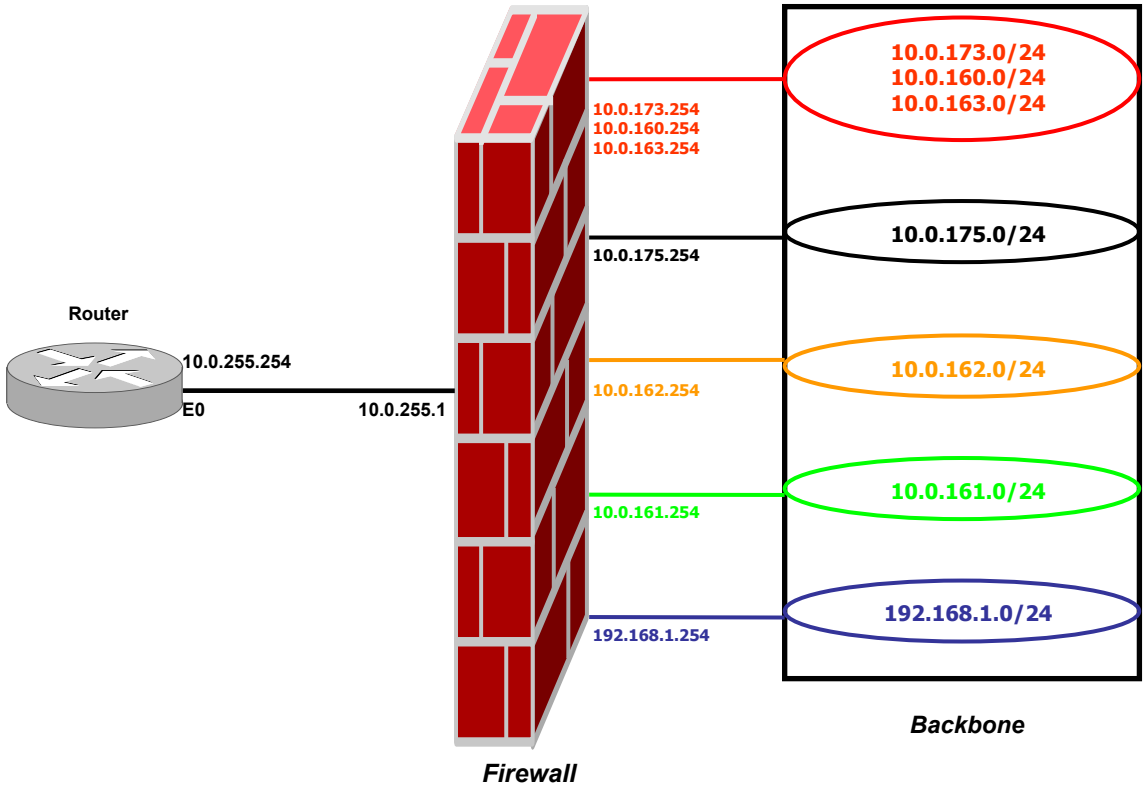



Figura 4.4 Direccionamiento asignado para las redes virtuales

### 4.1.4 Ruteo Inter-VLAN

Un punto importante en la creación de redes virtuales, es la comunicación entre VLANs. La red virtual por definición es un dominio lógico o dominio de *broadcast,* que al crearse aísla su propio tráfico de *broadcast* del resto de la red. Por lo tanto, para interconectar estos dominios lógicos y proveer los mecanismos de envío de datos entre VLANs es necesario el uso de un *router*; el cual permitirá su comunicación y mantendrá la delimitación de tráfico de *broadcast*.

En este esquema de diseño, el *Firewall* hará la función de *router* para la comunicación de las redes virtuales y también las interconectará. En este caso, el *Firewall* es un software y está implementado en un servidor con las siguientes características:

- Servidor DELL modelo *PowerEdge* 6400/700
- 2 Procesadores Pentium III de 699 Mhz cada uno
- Disco Duro de 34 GB
- Memoria RAM 1 GB
- Sistema Operativo *Windows* 2000 *Advanced Server*
- 2 tarjetas de 4 puertos de red cada uno

Una vez creadas las redes virtuales en el *Backbone* y hacer la conexión con el *Firewall*, se configurará la parte de ruteo para la comunicación entre las VLANs. El ruteo será por medio de Microsoft, que brinda una herramienta que es "*Routing and Remote Access*", y que se implementará en el sistema operativo *Windows* 2000 *Advanced Server* del *Firewall*. La seguridad de las redes virtuales también se complementará con reglas que se configuran en el *Firewall*.

La figura 4.5 muestra la comunicación que habrá entre redes virtuales por medio del *Firewall*, y éste a su vez con el *router* para la salida a Internet.

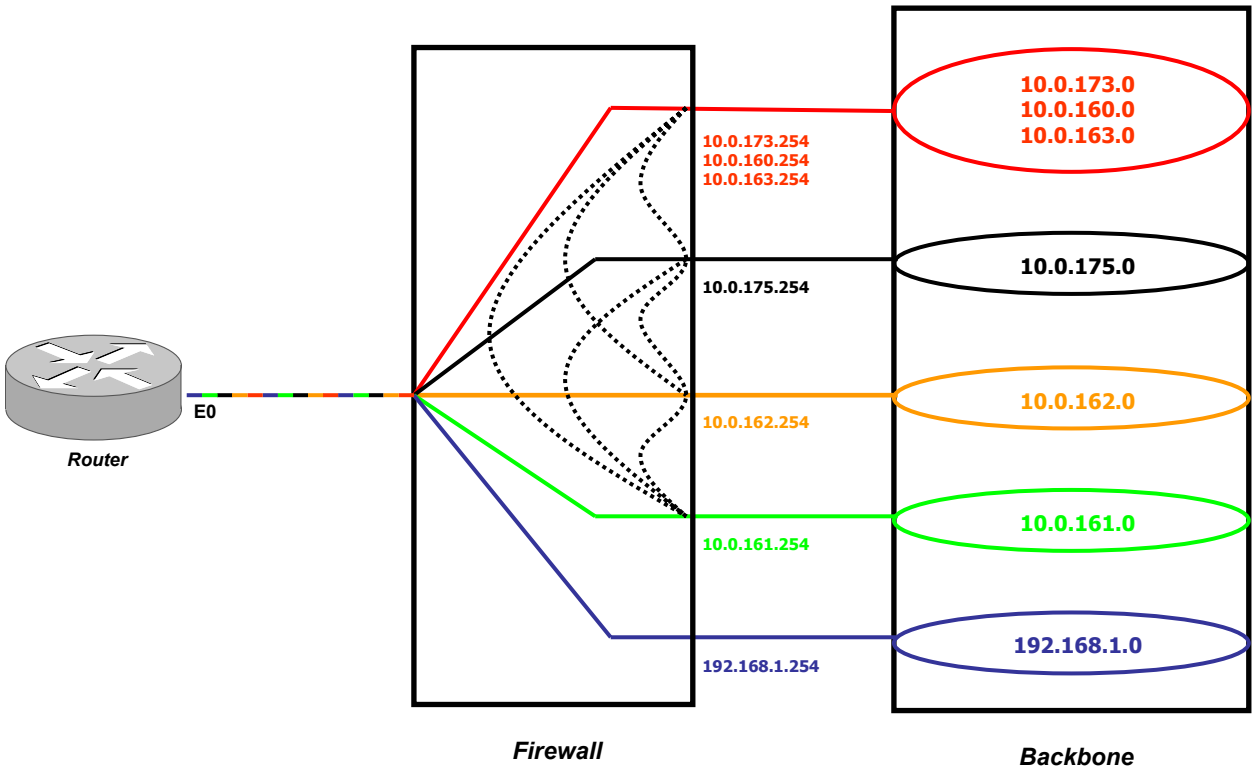



Figura 4.5 Ruteo Inter-Vlan en el *Firewall*

En este esquema de diseño, la conexión de las redes virtuales se hace por medio de un *Firewall* para dar mayor seguridad a la red LAN de El Colegio. El motivo de este diseño es para evitar ataques de los *hackers* y posibles vulnerabilidades que se puedan tener en la red.

# 5. IMPLEMENTACIÓN

La implementación es el proceso de terminación de un proyecto, por lo tanto, en éste capítulo describiremos los pasos que se llevaron acabo para la creación de las redes virtuales en el *Backbone* y la integración de éstas con el *Firewall*; así como la configuración de los equipos involucrados para la realización del proyecto.

## 5.1. Configuración de Servidores

Como paso inicial para la creación de las redes virtuales, fue necesario configurar los servidores que van a brindar los servicios que son prioritarios para los clientes en su configuración de red: DHCP, DNS y WINS; éste último servicio es para clientes que tienen instalado como sistema operativo la versión de *Windows* 95/98 de *Microsoft*.

La Tabla 5.1 describe la configuración de TCP/IP para los servidores y los servicios de red que se instalaron:

| Nombre del Servidor | Servicios | Configuración de TCP/IP | VLAN |
|---|---|---|---|
| GAMA | DNS Primario, DHCP y WINS | Host Name: gama<br>DNS suffix colmex.mx<br>IP: 10.0.173.134<br>10.0.160.1<br>10.0.163.252<br>Subnet mask: 255.255.255.0<br>Default Gateway: 10.0.160.254<br>DNS Server: 10.0.160.1<br>10.0.173.233<br>WINS Server: 10.0.160.1 | VLAN_Profesores |
| MEXICA | DNS Secundario | Host Name: mexica<br>DNS suffix colmex.mx<br>IP: 10.0.173.233<br>Subnet mask: 255.255.255.0<br>Default Gateway: 10.0.173.254<br>DNS Server: 10.0.173.233<br>10.0.160.1<br>WINS Server: 10.0.160.1 | VLAN_Profesores |
| ORION | DHCP, WINS | Host Name: orion<br>DNS suffix colmex.mx<br>IP: 10.0.175.4<br>Subnet mask: 255.255.255.0<br>Default Gateway: 10.0.175.254<br>DNS Server: 10.0.160.1<br>10.0.173.233<br>WINS Server: 10.0.175.4 | VLAN_Estudiantes |
| VEGA | DHCP, WINS | Host Name: vega<br>DNS suffix colmex.mx<br>IP: 10.0.162.15<br>Subnet mask: 255.255.255.0<br>Default Gateway: 10.0.162.254<br>DNS Server: 10.0.160.1<br>10.0.173.233<br>WINS Server: 10.0.162.15 | VLAN_Administración |
| BIBLIO2 | DHCP, WINS | Host Name: biblio2<br>DNS suffix colmex.mx<br>IP: 10.0.161.9<br>Subnet mask: 255.255.255.0<br>Default Gateway: 10.0.161.254<br>DNS Server: 10.0.160.1<br>10.0.173.233<br>WINS Server: 10.0.160.1 | VLAN_Biblioteca |

| Nombre del Servidor | Servicios | Configuración de TCP/IP | VLAN |
|---|---|---|---|
| PC-Lab | *Any* | Host Name: pc_lab<br>DNS suffix colmex2.mx<br>IP: 192.168.1.1<br>Subnet mask: 255.255.255.0<br>Default Gateway: 192.168.1.254<br>DNS Server: 10.0.255.1 | VLAN_Laboratorio |

Tabla 5.1 Configuración TCP/IP de los servidores

De esta manera, la red LAN basada en el estándar TCP/IP asignará de manera dinámica los parámetros y direcciones IP que corresponden única y exclusivamente a cada VLAN.

## 5.2. Selección de Equipo (*Backbone*)

La selección de equipo es tan importante como el diseño; es decir, si éstos no cumplen con los requerimientos que se demandan se tendrá una red con bajo desempeño y funcionalidad. El equipo debe tener flexibilidad para cubrir las expectativas y necesidades del diseño. El diseño no debe ser completamente rígido, deba ser flexible a variaciones mínimas, que permitan balancear cargas de acuerdo a características de los propios equipos.

Bajo las consideraciones anteriores, se realizó un estudio de equipos con diferentes marcas y modelos; en este estudio se evaluaron algunas características importantes como lo muestra la Tabla 5.2.

Las características que se tomaron en cuenta son las siguientes:

- *Switch Matrix* (capacidad, *non-blocking* y tipo de procesador)
- Capa del Modelo OSI (*switching*, ruteo)
- Módulos *hot swap*/redundancia
- Número y tipos de VLANs

| Características | | Marcas y Modelos de Switches | | | | |
|---|---|---|---|---|---|---|
| | | **Catalyst 6500 (Cisco) (9 Slot)** | **Passport 8600 (Nortel) (10 Slot)** | **BlackDiamond 6800 (Extreme) (8 Slot)** | **X-Pedition 8600 (Enterasys) (8 Slot)** | **BigIron 8000 (Foundry) (16 Slot)** |
| **Switch Matrix** | Capacidad | 32 Gbps/30 Mpps escalable a 256Gbps/100Mpps* | 128 Gbps/96 Mpps escalable a 256 Gbps*** | 64 Gbps/48 Mpps escalable a 128 Gbps/96 Mpps** | 32 Gbps / 30 Mpps | 64 Gbps/ 48 Mpps escalable a 256 Gbps/96 Mpps |
| | None-blocking | Solo si se tiene Supevisor Engine 2 | SI | SI | SI | SI |
| | Procesador | Procesador RISC RM7000 a 250 Mhz | PowerPC 740 con core/bus frecuencia de 266Mhz/66Mhz | Cada MSM64i tiene 2 MIPS 5000-compliant 64 bit, 133 Mhz | | PowerPC 466 Mhz |
| **Capa** | Switching (L2) | SI | SI | SI | SI | SI |
| | Ruteo (L3) | SI | SI | SI | SI | SI |
| **Hot Swap/Redundancia** | Módulos | SI | SI | SI | SI | SI |
| | Power | SI | SI | SI | SI | SI |
| | Fans | SI | SI | SI | SI | SI |
| **VLAN** | Tipos de VLAN´s | Puerto | Puerto, MAC Address, Protocolo y IP Sudnet-based | Puerto, MAC Address y Protocolo | Puertos y Protocolos | Puerto, Protocolo y Sub-red |
| | No.de VLANs | 1000 | 4,094 | 4,096 | 4,096 | 4,096 |
| **Protocolos** | Ruteo | OSPF, IGRP, Enhanced IGRP, RIP, RIP II, BGP4, IS-IS, HSRP | VRRP (Virtual Router Redundancy Protocol), RIPv1/v2, OSPFv1/v2, BGP, BGP4 | RIPv1/v2, OSPF, BGP-4. | RIPv1/v2, OSPF, BGP, BGP-4 | RIPv1/v2, OSPF, BGP, BGP-4, VRRP |
| | Red | IEEE 802.1Q,VLAN<br>IEEE 802.1p Prioridad<br>IEEE 802.1d Spanning Tree<br>IEEE 802.3<br>IEEE 802.3u Fast Ethernet<br>IEEE 802.3x Flow Control<br>IEEE 802.3z Gibabit | IEEE 802.1Q,VLAN<br>IEEE 802.1p Prioridad<br>IEEE 802.1d Spanning Tree<br>IEEE 802.3<br>IEEE 802.3u Fast Ethernet<br>IEEE 802.3z Gibabit<br>IEEE 802.3ab<br>IEEE 802.3x Flow Control | IEEE 802.1Q,VLAN<br>IEEE 802.1p Prioridad<br>IEEE 802.1d Spanning Tree<br>IEEE 802.3<br>IEEE 802.3u Fast Ethernet<br>IEEE 802.3x Flow Control<br>IEEE 802.3z Gibabit | IEEE 802.1Q,VLAN<br>IEEE 802.1p Prioridad<br>IEEE 802.1d Spanning Tree<br>IEEE 802.3<br>IEEE 802.3u Fast Ethernet<br>IEEE 802.3x<br>IEEE 802.3z Gibabit | IEEE 802.1Q,VLAN<br>IEEE 802.1p Prioridad<br>IEEE 802.1d Spanning Tree<br>IEEE 802.3<br>IEEE 802.3u Fast Ethernet<br>IEEE 802.3x Flow Control<br>IEEE 802.3z Gibabit<br>IEEE 802.3ad |
| | Multicast | IGMP, DVMRP, PIM, CGMP, GMRP | IGMPv1/v2, DVMRP, PIM | IGMPv2, DVMRPv3, PIM | IGMP, DVMRP | IGMP, DVMRP, MSDP, MBGP, PIM – Dense/Sparse |

| Características | | Marcas y Modelos de Switches | | | | |
|---|---|---|---|---|---|---|
| | | **Catalyst 6500 (Cisco) (9 Slot)** | **Passport 8000 (Nortel) (10 Slot)** | **BlackDiamond 6800 (Extreme) (8 Slot)** | **X-Pedition 8600 (Enterasys) (8 Slot)** | **BigIron 8000 (Foundry) (16 Slot)** |
| **Protocolos** | Soportados | TFTP, BOOTP, DHCP, VTP, CDP, STP, RSVP, CGMP, EIGRP, DNS. | Distributed Multi- Link Trunking (MLT), Equal Cost Multi-Path (ECMP), BOOTP, DHCP, FTP, TFTP. | Extreme Standby Router Protocol (ESRP), BOOTP, DNS Client, ICMP Router Discovery Protocol, TFTP, DHCP Relay, ICMP, DNS | Multiprotocol Interconnect over Frame Relay, PPP en HDLC Framing, PPP. | BOOTP, DNS Client, ICMP Router Discovery Protocol, PPP, TFTP, DHCP Relay, Foundry Standby Router Protocol (FSRP) |
| **Servicios** | QoS | IP precedence detection y classification, 802.1Q/802.1p detection y classification, IP Differentiated Services, Bandwidth Policing, Traffic Scheduling, Cogestion Avoidance. | DiffServ, Service provisioning using CLI, Device Manager (GUI) or Optivity Policy Services (OPS), Common Open Policy services Protocol for provisioning (COPS-PR), COPS for Resource Reservation Protocol (RSVP), IP ToS precedence, 802.1Q Virtual LAN Tagging, 802.1p User Priority Setting, Weighted Fair Queuing | Traffic Prioritization, bandwidth management y congestion control | Application Level, RSVP | Weighted Fair Queuing (WFQ), Strict Priority (SP), 802.1p queue Mapping, Type Qos Service (ToS), MAC Address, VLAN membership, IP source/destination address or subnet. |
| **Interfaces** | 10/100 BASE –TX | 384 pto | 384 ptos | 384 ptos | 240 ptos | 144 ptos |
| | 100 BASE –FX | 192 pto | 192 ptos | 224 ptos | 120 ptos | 144 ptos |
| | 1000 BASE-TX/SX/LX | 130 pto | 64 ptos | 96 ptos | 60 ptos | 48 ptos |
| **Administración y Seguridad** | | SNMPv1/v2, Telnet, CiscoWorks 2000, Cisco Rosource Manager, MIB II, RMON, RMON II, VQP, DPT, NTP, TACACS+ RADIUS, ACL, NAT. IP Permit List | 4 grupos de RMON por pto, RMON, RMON2, CLI, HTTP, RADIUS, Telnet, rlogin, MIB, MIBII SNMP, Optivity Switch Manager, Device Manager GUI and VLAN Manager, Optivity Network Configuration System (NCS) | Telnet, CLI, RMON, HTTP, SNMPv1/v2, MIB II, Simple Network Time Protocol (SNTP), RADIUS, SSH2, TACACS+ | RMON/RMON2 por pto., SNMP, CLI (Command Line Interface), MIB, MIB-2, HTTP ACLs | CLI, SNMPv1/v2, Telnet, HTTP, RMON, MIB, MIB-II TACACS/TACACS+, Radius, AAA (Authentication, Authorization and Accounting), Username/Password |

- * Solo si se tiene una Supevisor Engine 2
- ** Con otra Switching Fabric Card (MSM64i)
- ***En un Futuro

Tabla 5.2 Características de los Switches

- Protocolos (ruteo, red, *multicast*)
- Servicios (calidad de servicio)
- Número y tipos de interfaces
- Administración y seguridad

En la toma de decisión del equipo (*Backbone*) a considerar para el proyecto de tesis se contemplaron varias circunstancias, como son: las características técnicas evaluadas, costo del equipo, así como el prestigio de la marca que respalda al producto y el tiempo de vida en el mercado nacional.

Después de su análisis respectivo, se llegó a la conclusión que el equipo de la marca *Nortel* y en específico el modelo *Passport* 8600 cumple con las expectativas para el proyecto.

## 5.3. Configuración del *Backbone*

Una vez seleccionado el equipo (*Backbone*), realizado la configuración de los servidores e instalados los servicios de red correspondientes para los clientes, se procedió a la configuración de las redes virtuales en el *Backbone* (*Switch Passport 8610 de Nortel*).

El equipo *Passport* está formado por un chasis de 10 *slots*, de los cuales se ocupan 2 para los *Routing Switch Module CPU/Switch Fabric Module*. Otro *slot* es ocupado por un módulo de 48 puertos *autosensing* 10Base-T/100Base-TX *Ethernet*. Por último se tienen 3 módulos con 8 puertos cada uno de 1000Base-SX *Gigabit Ethernet*.

La configuración del *Passport* se realizó por medio de CLI (*Command Line Interface*), para lo cual se utilizaron los siguientes comandos:

*Passport-8610# config vlan <vid> create byport <sid> [name <value>]*
*Passport-8610# config vlan <vid> ports add <ports> [member <value>]*

El primer comando es para la creación de la red virtual (para nuestro diseño la VLAN será por puerto). El segundo comando es para la asignación de puertos a la respectiva VLAN.

Los comandos para la creación de la VLAN_Profesores y su asignación de puertos:

*Passport-8610# config vlan 1 create byport 1 name Profesores*
*Passport-8610# config vlan 1 ports add 1/1-1/27,1/29,1/31,7/1-7/8,8/1-8/8*

Los comandos para la creación de la VLAN_Estudiantes y su asignación de puertos:

*Passport-8610# config vlan 2 create byport 1 name Estudiantes*
*Passport-8610# config vlan 2 ports add 1/34,1/36,1/38,1/40,1/42,1/44,1/46,1/48, 9/1-9/3*

Los comandos para la creación de la VLAN_Administración y su asignación de puertos:

*Passport-8610# config vlan 3 create byport 1 name Administración*
*Passport-8610# config vlan 3 ports add 1/33,1/35,1/37,1/39,1/41,9/4-9/6*

Los comandos para la creación de la VLAN_Biblioteca y su asignación de puertos:

*Passport-8610# config vlan 4 create byport 1 name Biblioteca*
*Passport-8610# config vlan 4 ports add 1/43,1/45,1/47,9/7-9/8*

Los comandos para la creación de la VLAN_Laboratorio y su asignación de puertos:

*Passport-8610# config vlan 5 create byport 1 name Laboratorio*
*Passport-8610# config vlan 5 ports add 1/28,1/30,1/32*

Una vez realizado lo anterior se procede a guardar la configuración con el comando siguiente.

*Passport-8610# save config*

Para ver la configuración de las redes virtuales en sus diferentes presentaciones, se pueden utilizar los siguientes comandos:

*Passport-8610# show vlan info basic*

VLAN BASIC

| VLAN ID | NAME | TYPE | STG ID | PROTOCOL ID | SUBNETADDR | SUBNETMASK |
|---|---|---|---|---|---|---|
| 1 | Profesores | byPort | 1 | none | N/A | N/A |
| 2 | Estudiantes | byPort | 1 | none | N/A | N/A |
| 3 | Administración | byPort | 1 | none | N/A | N/A |
| 4 | Biblioteca | byPort | 1 | none | N/A | N/A |
| 5 | Laboratorio | byPort | 1 | none | N/A | N/A |

N/A = No Aplica

None = Ninguno

*Passport-8610# show vlan info ports*

VLAN PORT

| VLAN ID | PORT MEMBER | ACTIVE MEMBER | STATIC MEMBER | NOT_ALLOW MEMBER |
|---|---|---|---|---|
| 1 | 1/1-1/27,1/29,1/31,7/1-7/8,8/1-8/8 | 1/1-1/27,1/29,1/31,7/1-7/8,8/1-8/8 | | |
| 2 | 1/34,1/36,1/38,1/40,1/42,1/44,1/46,1/48,9/1-9/3 | 1/34,1/36,1/38,1/40,1/42,1/44,1/46,1/48,9/1-9/3 | | |
| 3 | 1/33,1/35,1/37,1/39,1/41,9/4-9/6 | 1/33,1/35,1/37,1/39,1/41,9/4-9/6 | | |
| 4 | 1/43,1/45,1/47,9/7-9/8 | 1/43,1/45,1/47,9/7-9/8 | | |
| 5 | 1/28,1/30,1/32 | 1/28,1/30,1/32 | | |

*Passport-8610# show vlan info advance*

```
================================================================================================
                                        VLAN     ADVANCE
================================================================================================
```

| VLAN ID | NAME | IF INDEX | QoS LVL | AGING TIME | MAC ADDRESS | ACTION | RESULT | USER DEFINEPID |
|---|---|---|---|---|---|---|---|---|
| 1 | Profesores | 2049 | 1 | 0 | 00:00:00:00:00:00 | none | none | 0 |
| 2 | Estudiantes | 2050 | 1 | 0 | 00:00:00:00:00:00 | none | none | 0 |
| 3 | Administración | 2051 | 1 | 0 | 00:00:00:00:00:00 | none | none | 0 |
| 4 | Biblioteca | 2052 | 1 | 0 | 00:00:00:00:00:00 | none | none | 0 |
| 5 | Laboratorio | 2053 | 1 | 0 | 00:00:00:00:00:00 | none | none | 0 |

None = Ninguno

Con los comandos antes descritos se termina la configuración de las redes virtuales en la parte del *Backbone*.

Una herramienta alterna para la creación de las redes virtuales en el equipo *Passport* es una interfase gráfica llamada "*Device Manager*". Los pasos a seguir para configurar las redes virtuales en esta forma alterna, se describe a continuación.

Se abre la aplicación *Device Manager* y aparece una ventana como lo muestra la Figura 5.1, que pedirá el nombre del dispositivo o la dirección IP (previamente configurado en el equipo para su administración), así como la comunidad de lectura y escritura.

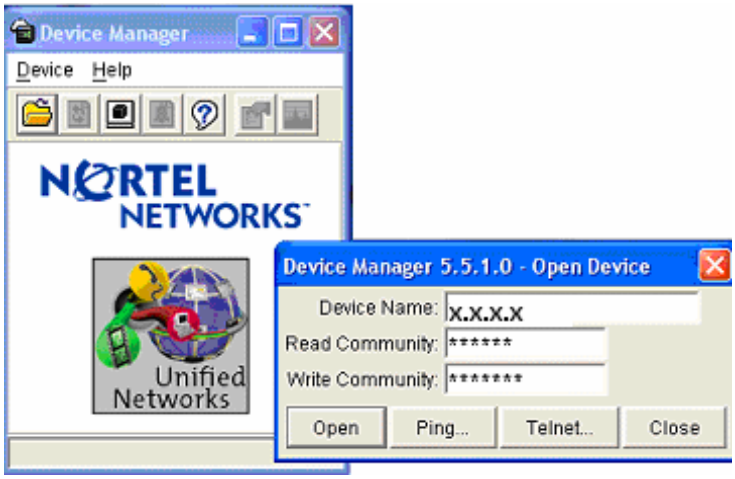



Figura 5.1 Ventana del *Device Manager*

A continuación en una pantalla como lo muestra la Figura 5.2, en la barra de menú se selecciona la parte de “VLANs..”.

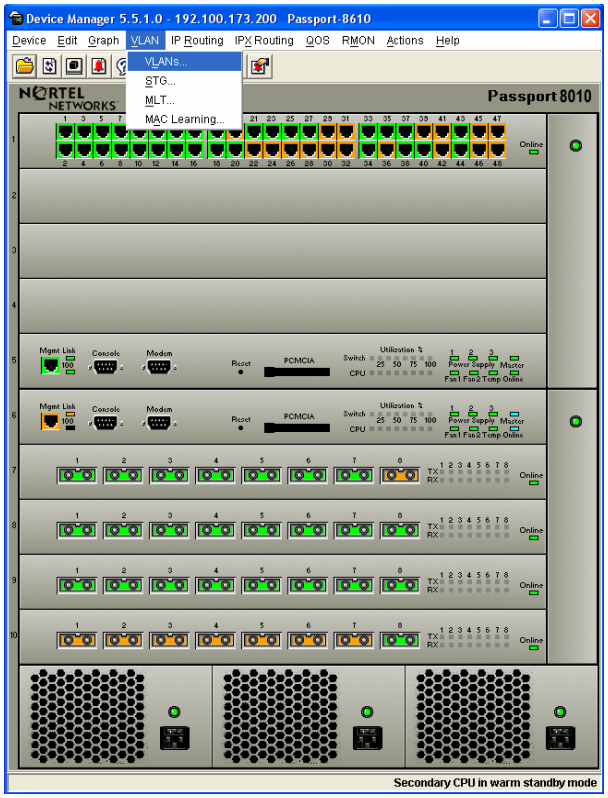



Figura 5.2 *Switch Passport* 8610

Aparece una ventana (véase Figura 5.3) donde están los parámetros de la VLAN que está por *default*; esta VLAN está formada por todos los puertos del *Switch Passport* 8610. En la creación de la VLAN_Profesores se utiliza la VLAN *default* donde se selecciona los puertos que corresponden a la red virtual: *1/1-1/27,1/29,1/31,7/1-7/8,8/1-8/8*.

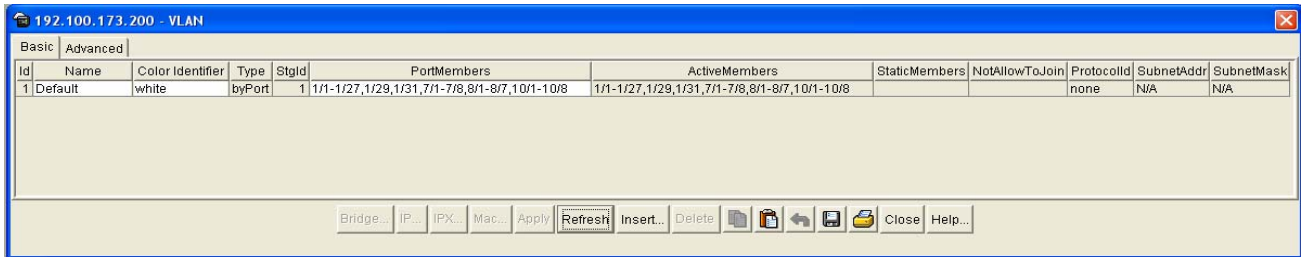



Figura 5.3 Ventana de configuración de la VLANs

La creación de la VLAN_Estudiantes se utiliza la ventana anterior (véase figura 5.3), con el botón de "*Insert..*"; aparece la ventana de la Figura 5.4, donde están los parámetros de configuración de una nueva VLAN que son Id, *name*, *color Identifier*, StgId, tipo y *PortMembers*. En *PortMembers* se selecciona los puertos correspondientes para la red virtual: *1/34,1/36,1/38,1/40,1/42,1/44,1/46,1/48,9/1-9/3*.

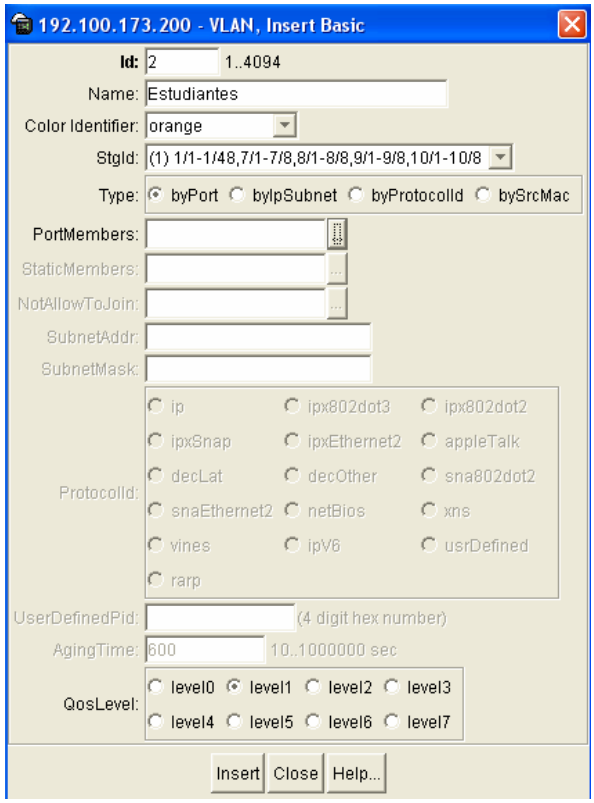



Figura 5.4 Ventana de configuración de la VLAN_Estudiantes

Para la creación de la VLAN_Administración se siguen los mismos pasos que la red virtual anterior; pero con la selección de puertos correspondientes (*1/33,1/35,1/37,1/39,1/41,9/4-9/6*) así como el Id, nombre e identificador de color; para mas detalle ver la Figura 5.5.

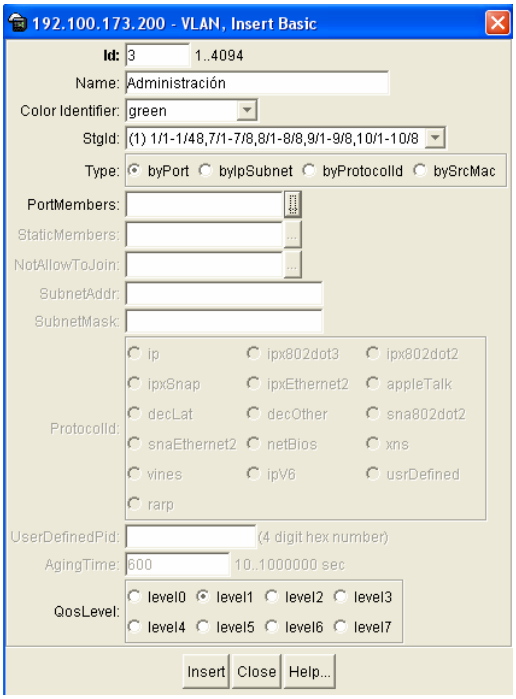



Figura 5.5 Ventana de configuración de la VLAN_Administración

La VLAN_Biblioteca es el mismo proceso que las redes virtuales anteriores, cuyos puertos son: *1/43,1/45,1/47,9/7-9/8*, el Id = 4, *color Identifier* = *blue*, *name* = Biblioteca. Para mas detalles ver la Figura 5.6.

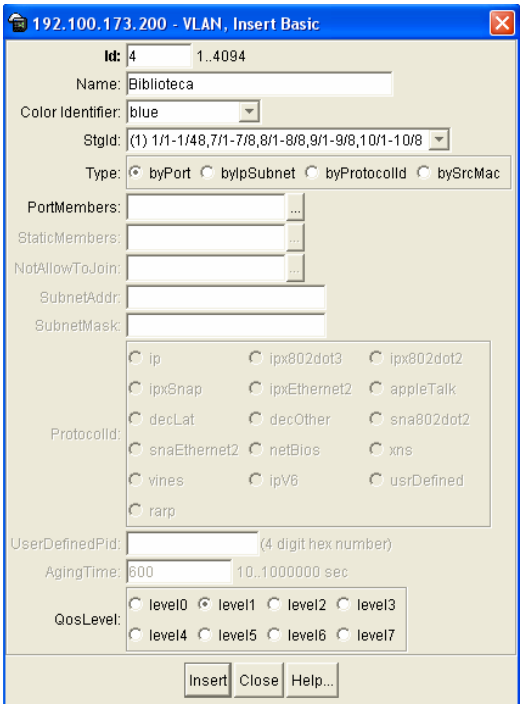



Figura 5.6 Ventana de configuración de la VLAN_Biblioteca

Por último se crea la VLAN_Laboratorio, para esta red virtual se tienen los siguientes parámetros de configuración: Id = 5, *color Identifier* = *yellow*, *name* = Laboratorio y *PortMembers* = *1/28,1/30,1/32*. Para mas detalles ver la Figura 5.7.

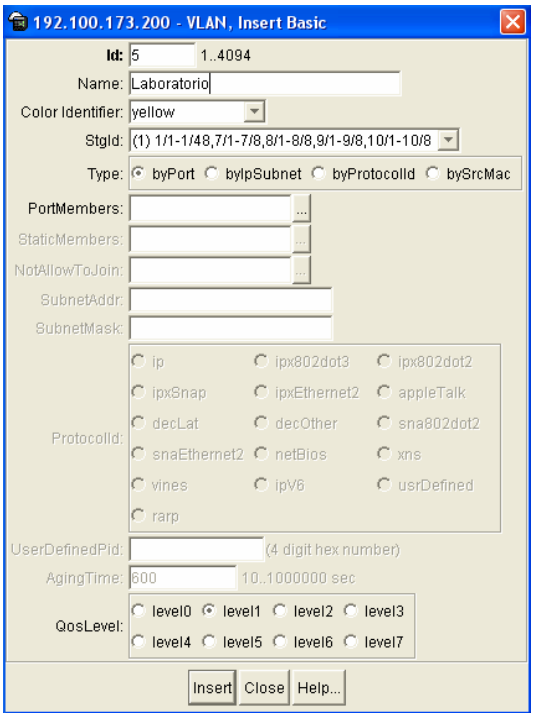
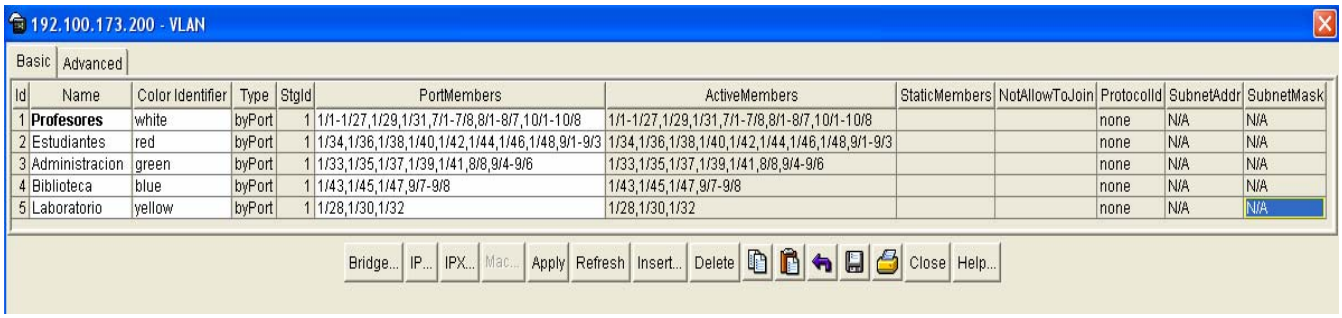



Figura 5.7 Ventana de configuración de la VLAN_Laboratorio

Finalmente se tienen las 5 redes virtuales (Profesores, Estudiantes, Administración, Biblioteca y Administración) con sus respectivas configuraciones de cada una de ellas, como se muestra la Figura 5.8.




| Id | Name | Color Identifier | Type | StgId | PortMembers | ActiveMembers | StaticMembers | NotAllowToJoin | ProtocolId | SubnetAddr | SubnetMask |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | **Profesores** | white | byPort | 1 | 1/1-1/27,1/29,1/31,7/1-7/8,8/1-8/7,10/1-10/8 | 1/1-1/27,1/29,1/31,7/1-7/8,8/1-8/7,10/1-10/8 | | | none | N/A | N/A |
| 2 | Estudiantes | red | byPort | 1 | 1/34,1/36,1/38,1/40,1/42,1/44,1/46,1/48,9/1-9/3 | 1/34,1/36,1/38,1/40,1/42,1/44,1/46,1/48,9/1-9/3 | | | none | N/A | N/A |
| 3 | Administracion | green | byPort | 1 | 1/33,1/35,1/37,1/39,1/41,8/8,9/4-9/6 | 1/33,1/35,1/37,1/39,1/41,8/8,9/4-9/6 | | | none | N/A | N/A |
| 4 | Biblioteca | blue | byPort | 1 | 1/43,1/45,1/47,9/7-9/8 | 1/43,1/45,1/47,9/7-9/8 | | | none | N/A | N/A |
| 5 | Laboratorio | yellow | byPort | 1 | 1/28,1/30,1/32 | 1/28,1/30,1/32 | | | none | N/A | N/A |

Figura 5.8 Ventana de configuración de las VLANs

## 5.4. Integración de VLANs con el *Firewall*

Una vez creadas las redes virtuales en el *Backbone,* el paso siguiente es la integración de estas con el *Firewall*. Esta integración es por medio de un cable UTP entre un puerto red en el *Passport* para cada una de las VLANs y un puerto de red en el *Firewall*. Como se mencionó anteriormente el *Firewall* tiene instaladas 2 tarjetas con 4 puertos *Ethernet* por cada una, para lo cual se utilizan 6 puertos; 5 para las redes virtuales y otra para la conexión entre el *Firewall* y el *router*.

Después de realizar las conexiones del *Passport 8610*, *Firewall* y *router*, se procede a configurar el direccionamiento en las tarjetas de red del *Firewall*. Para realizar la configuración se deben escribir los siguientes parámetros en la parte de *Internet Protocol (TCP/IP) Properties*.

Para la VLAN_Profesores son los siguientes parámetros:

| | |
|---|---|
| *IP Address* | 10.0.173.254 |
| *Subset Mask* | 255.255.255.0 |
| *IP Address* | 10.0.160.254 |
| *Subset Mask* | 255.255.255.0 |
| *IP Address* | 10.0.163.254 |
| *Subset Mask* | 255.255.255.0 |
| *DNS Server* | 127.0.0.1 |

Para la VLAN_Estudiantes son los siguientes parámetros:

| | |
|---|---|
| *IP Address* | 10.0.175.254 |
| *Subset Mask* | 255.255.255.0 |
| *DNS Server* | 127.0.0.1 |

Para la VLAN_Administración son los siguientes parámetros:

| | |
|---|---|
| *IP Address* | 10.0.162.254 |
| *Subset Mask* | 255.255.255.0 |
| *DNS Server* | 127.0.0.1 |

Para la VLAN_Biblioteca son los siguientes parámetros:

| | |
|---|---|
| *IP Address* | 10.0.161.254 |
| *Subset Mask* | 255.255.255.0 |
| *DNS Server* | 127.0.0.1 |

Para la VLAN_Laboratorio son los siguientes parámetros:

| | |
|---|---|
| *IP Address* | 192.168.1.254 |
| *Subset Mask* | 255.255.255.0 |
| *DNS Server* | 127.0.0.1 |

Los parámetros anteriores son para habilitar las conexiones de las redes virtuales. Para la comunicación con Internet se habilita otro puerto en el *Firewall*.

Para la FW-Externa son los siguientes parámetros:

| | |
|---|---|
| *IP Address* | 10.0.255.1 |
| *Subset Mask* | 255.255.255.0 |
| *Default Gateway* | 10.0.255.254 |
| *DNS Server* | 10.0.255.1 |

En la Figura 5.9 se muestran las conexiones de las redes virtuales, y la de acceso a Internet (FW-Externa).

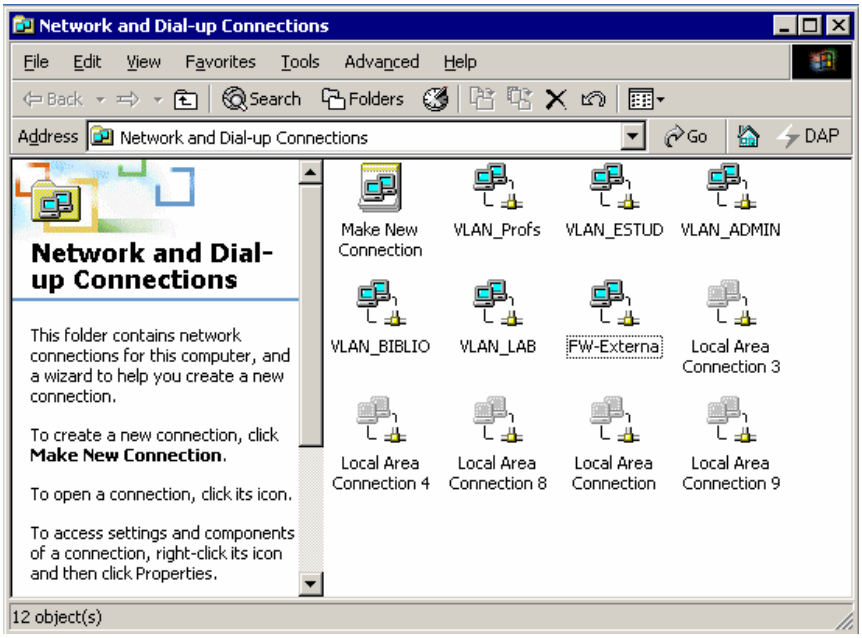



Figura 5.9 Conexiones de red

Después de configurar de las tarjetas de red en el *Firewall*, se debe habilitar y configurar el servicio de "*Routing and Remote Access*"; este servicio es parte de *Windows 2000 Advanced Server* y permite la comunicación entre las redes virtuales en conjunto con las reglas configuradas en el *Firewall*.

Para habilitar y configurar el servicio se da "*click*" en "*Routing and Remote Access*" de *Windows 2000 Advanced Server*, como se muestra en la Figura 5.10.

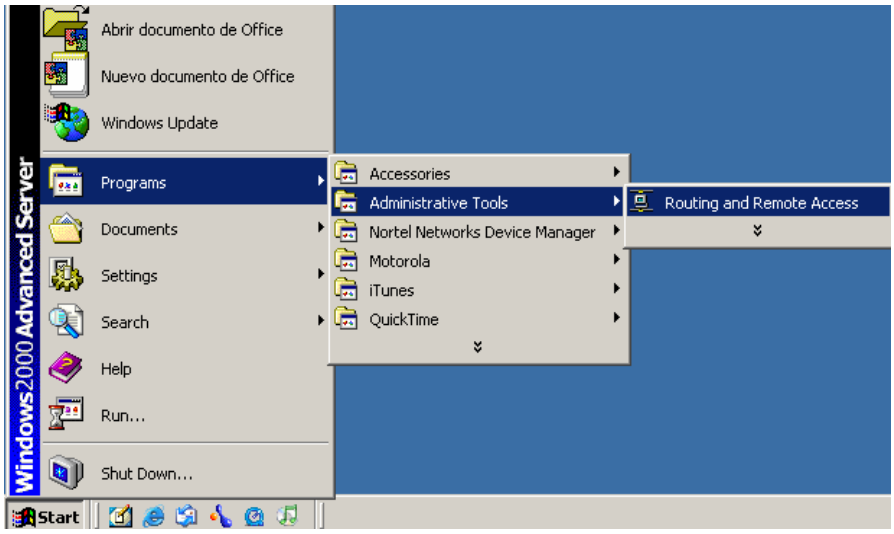



Figura 5.10 Servicio de *Routing and Remote Access*.

Posteriormente aparece una ventana en la que se habilita y configura el servicio, como lo muestra la Figura 5.11.

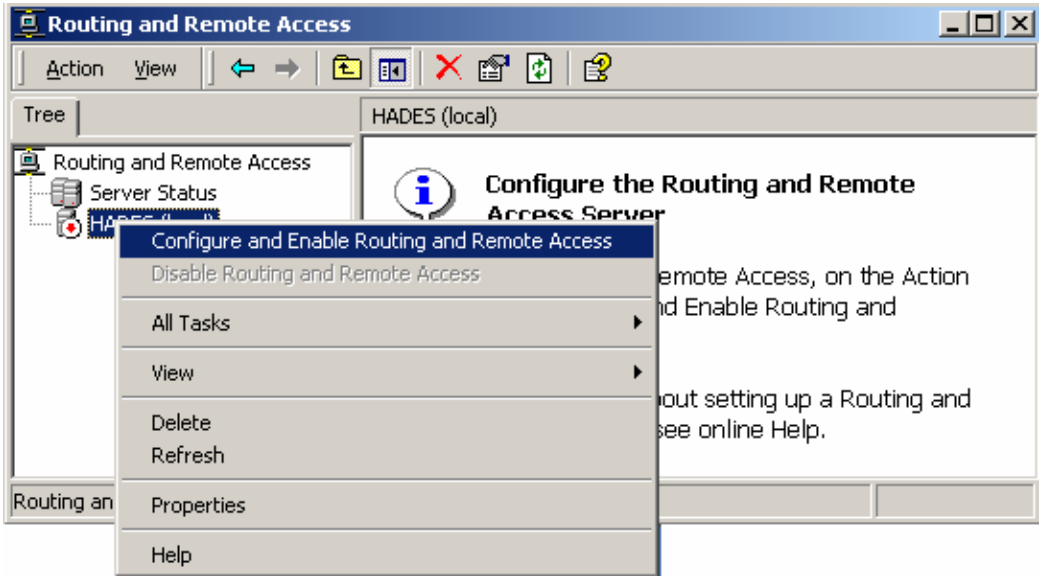



Figura 5.11 Habilitar y configurar el servicio de *Routing and Remote Access*

Una vez realizado lo anterior, se dan los pasos para la configuración del servicio con la ayuda de un asistente por medio de ventanas (véase Figura 5.12).

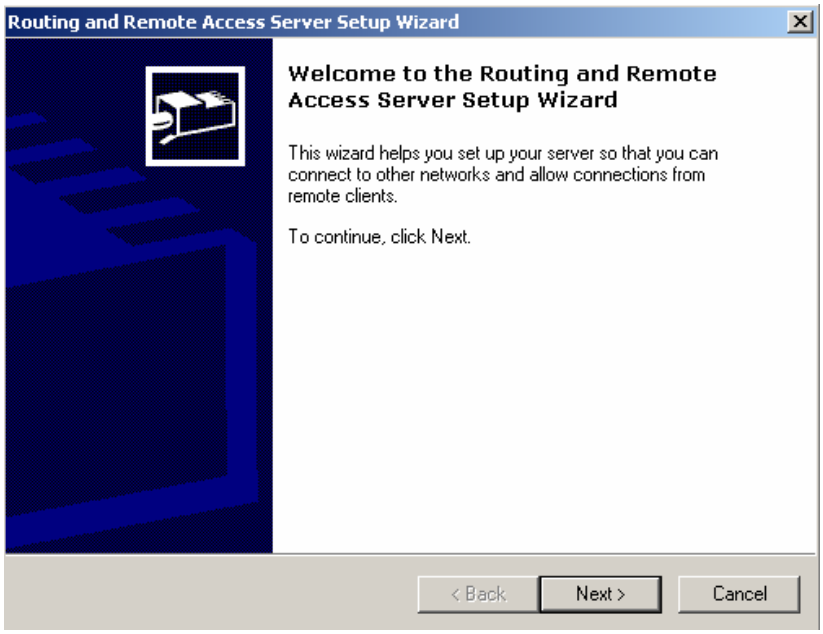



Figura 5.12 Asistente de configuración de *Routing and Remote Access*

En la ventana de la Figura 5.13, se selecciona la opción de "*Networks router*", para habilitar la comunicación con otras redes.


Figura 5.13 Configuraciones comunes *Routing and Remote Access*

La Figura 5.14 muestra los protocolos ruteados, en este caso se utiliza el protocolo TCP/IP por ser un estándar de comunicaciones entre computadoras más común, además de ser éste robusto y confiable.

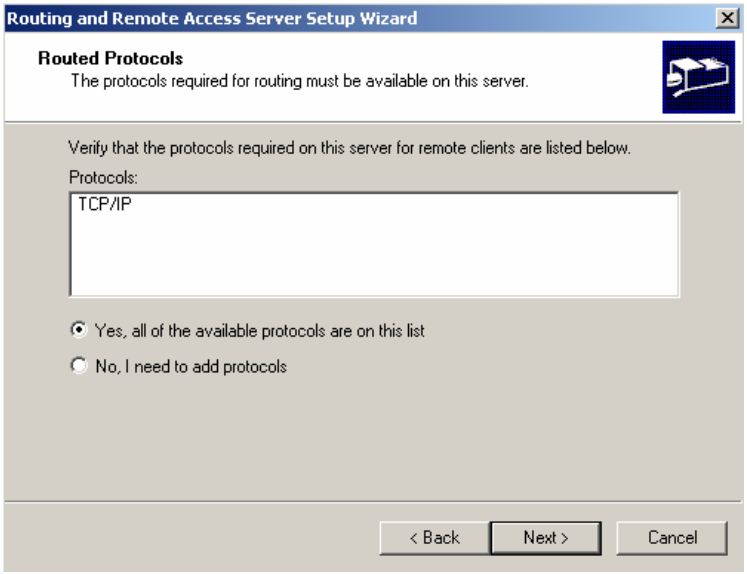



Figura 5.14 Protocolos utilizados en *Routing and Remote Access*

En la Figura 5.15 muestra la opción de habilitar una conexión de “Demand-Dial”, la cual no se habilitará por que no es necesario para nuestra configuración.

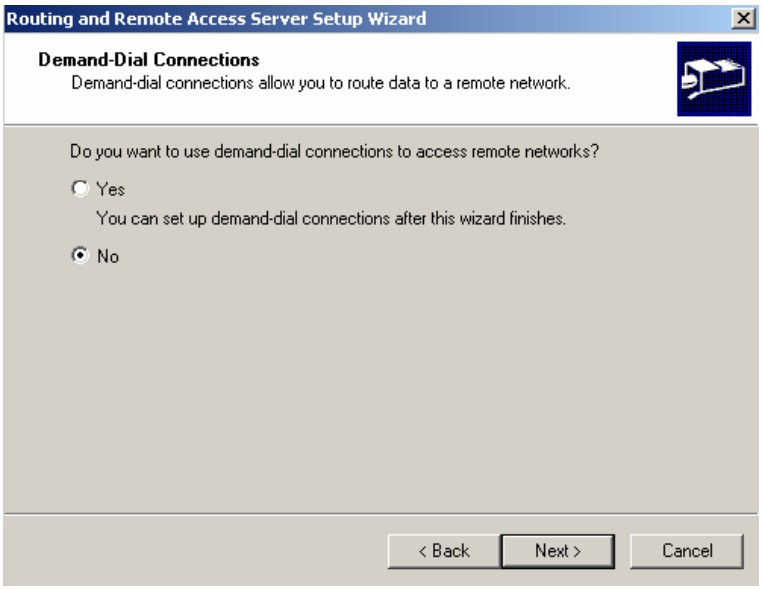



Figura 5.15 Asistente de configuración de *Routing and Remote Access*

Finalmente, la Figura 5.16 indica la terminación del asistente de configuración de *Routing and Remote Access*.

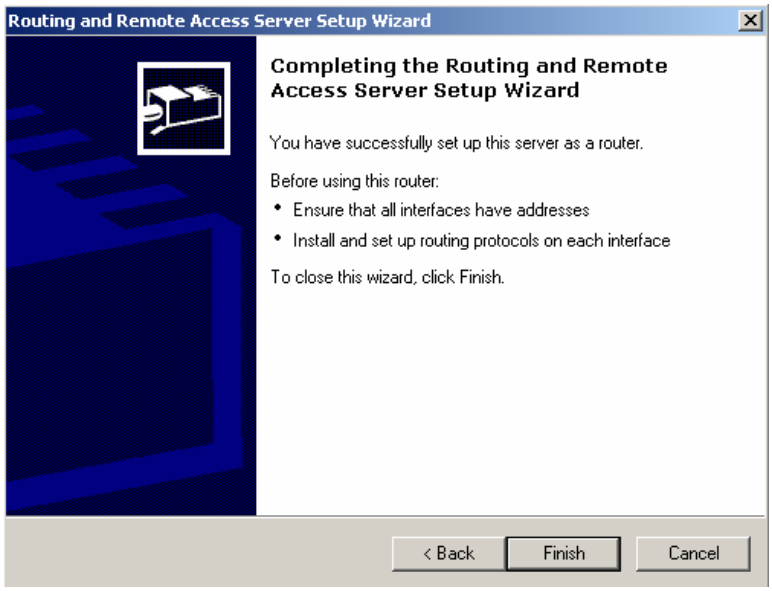



Figura 5.16 Finalización del asistente de configuración

Con lo anterior se termina la configuración de "*Routing and Remote Access*"; la Figura 5.17 muestra algunas propiedades generales de las redes virtuales para éste servicio.

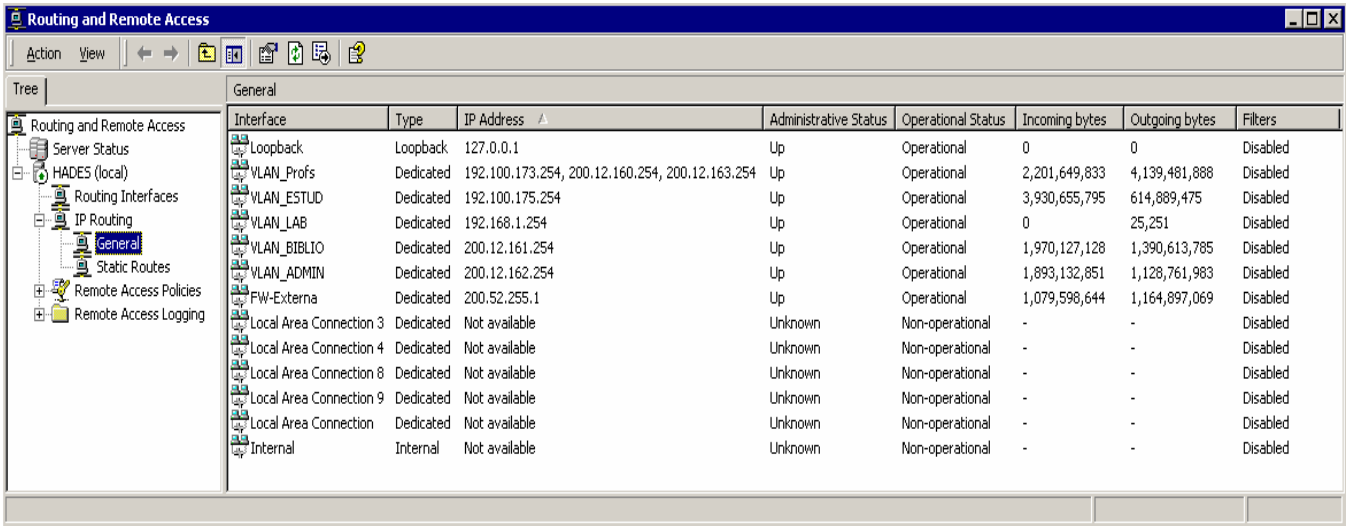



Figura 5.17 Propiedades generales de las VLANs en el *Routing and Remote Access*

## 5.5. Creación de objetos y reglas para la seguridad de las VLANs

Como se mencionó en el capítulo anterior, el *Firewall* es un *software* que está implementado en un servidor. Este software (*Check Point Next Generation Feature Pack 3*) se administra por medio de una interfaz gráfica, en la cual se generan reglas para la seguridad de las redes virtuales; las reglas se aplican a los objetos de red que son generados.

En la Tabla 5.3 se listan los objetos de red que son generados en la interfaz gráfica para posteriormente agregarlos las reglas.

| | Nombre del objeto | Descripción |
|---|---|---|
| *Nodes* | Hades | Nombre del servidor donde esta instalado el *Firewall* |
| | Defense | Servidor DNS secundario |
| | Urano | Servidor de correo electrónico |

| | Nombre del objeto | Descripción |
|---|---|---|
| *Nodes* | Fobos | Servidor de antivirus para el correo electrónico |
| | Monred | Servidor de monitoreo |
| | Biblio | Servidor del sitio web de biblioteca |
| | Codex | Servidor de ALEPH (*Automated Library Expandable Program*) |
| | Cybercop | Servidor de autenticación para equipos de comunicaciones |
| | Mercurio | Servidor del sitio web de El Colegio de México |
| | Hueb | Servidor de FTP |
| | Mezcal | Servidor de Bases de Datos |
| | Streaming | Servidor de *Streaming* |
| | Videoconferencia | Equipo de Videoconferencia |
| *Networks* | red_160 | Segmento de red (10.0.160.0) |
| | red_161 | Segmento de red (10.0.161.0) |
| | red_162 | Segmento de red (10.0.162.0) |
| | red_163 | Segmento de red (10.0.163.0) |
| | red_173 | Segmento de red (10.0.173.0) |
| | red_175 | Segmento de red (10.0.175.0) |
| *Groups* | servidores_web | Grupo donde están incluidos los servidores de sitios web y servidores que tienen instalado el IIS (*Internet Information Server*) |
| | vlan_colmex | Grupo donde están incluidos todos los segmentos de red |

Tabla 5.3 Lista de objetos de red

Creados los objetos de red, el paso siguiente es crear las reglas, por lo que es necesario conocer el origen y destino de los objetos de red, que establecen la comunicación para el intercambio de información, así como, los servicios que se darán en está comunicación y la acción se va a tomar.

La aplicación de las reglas lleva un orden descendente; es decir, el “paquete” empieza por la primera regla para verificar qué acción tomar, si no corresponde a la primera regla va con la segunda y así sucesivamente hasta llegar a la última; si el “paquete” no corresponde con ninguna regla anterior, se desecha.

Con la integración de las reglas para la seguridad de las redes virtuales queda por terminada la etapa de implementación.

# 6. ADMINISTRACIÓN DE LAS VLANs

En general, la administración de una red es un servicio que utiliza una gran variedad de herramientas, aplicaciones y dispositivos, para ayudar a los administradores de la red a supervisar y mantener funcional la infraestructura física y lógica de la red. Algunas de las herramientas que se utilizan para la administración de las redes virtuales son las siguientes:

- CLI (*Command Line Interface*, Interfaz por Línea de Comandos)
- DM (*Device Manager*, Administrador de Dispositivos)
- VLAN *Manager*

Con estas herramientas se tiene el control, configuración y monitoreo de las redes virtuales.

## *6.1 Command Line Interface*

El CLI es una herramienta de administración que proporciona métodos para configurar, administrar y monitorear funciones del *Passport* 8610, donde están generadas las redes

virtuales. Se puede acceder a CLI por una conexión directa al puerto de consola del *Passport* o remotamente utilizando *Telnet*.

Una vez realizada la conexión con el equipo, lo siguiente es conocer algunos comandos básicos para la creación, modificación y despliegue de información de las VLANs.

El comando para la creación de una VLAN es la siguiente:

*config vlan <vid> create* el parámetro vid es la VLAN ID (de 1 a 4094), la VLAN 1 es la VLAN *default*

El comando *config vlan <vid> create* incluye las siguientes opciones:

| *config vlan <vid> create* | |
|---|---|
| byipsubnet <sid> <ipaddr/mask> [name <value>] [color <value>] | Creación de una VLAN IP subnet-based.<br>• sid es el ID de un spanning tree group (1 a 25)<br>• ipaddr/mask dirección IP y la máscara<br>• name <value> nombre de la VLAN<br>• color <value> color de la VLAN (0 a 32) |
| *config vlan <vid> create* | |
| byport <sid> [name <value>] [color <value>] | Creación de una VLAN port-based.<br>• sid es el ID de un spanning tree group (1 a 25)<br>• name <value> nombre de la VLAN<br>• color <value> color de la VLAN (0 a 32) |
| byprotocol <sid> <ip\|ipx802dot3\| ipx802dot2\|ipxSnap\|ipxEthernet2\| appleTalk\|decLat\|decOther\| sna802dot2\|snaEthernet2\|netBios\| xns\|vines\|ipV6\|usrDefined\|rarp> [<pid>] [name <value>] [color <value>] | Creación de una VLAN protocol-based.<br>• sid es el ID de un spanning tree group (1 a 25)<br>• especificar protocolo ip\|ipx802dot3\|ipx802dot2\|ipxSnap\| ipxEthernet2\|appleTalk\|decLat\|decOther\|sna802dot2\| snaEthernet2\|netBios\|xns\|vines\|ipV6\|usrDefined\|rarp<br>• pid es el ID user-defined protocol en hexadecimal (0 a 65535)<br>• name <value> nombre de la VLAN<br>• color <value> color de la VLAN (0 a 32) |
| bysrcmac <sid> [name <value>] [color <value>] | Creación de una VLAN srcmac-based.<br>• sid es el ID de un spanning tree group (1 a 25)<br>• name <value> nombre de la VLAN<br>• color <value> color de la VLAN (0 a 32) |

Los comandos generales de configuración para las VLANs permiten agregar o remover puertos en la VLAN, establecer prioridad, cambiar nombre de la VLAN y mejorar otras operaciones de la VLAN.

| | |
|---|---|
| *config vlan <vid>* | el parámetro vid es la VLAN ID (de 1 a 4094) |

El comando *config vlan <vid>* incluye las siguientes opciones:

| *config vlan <vid>* | |
|---|---|
| delete | Borra la VLAN |
| name <vname> | Cambia el nombre de la VLAN |
| ports add <ports> [member <value>] | Agrega uno o mas puertos a una VLAN existente<br>• ports es una lista de puertos<br>• member <value> es el tipo de miembro del puerto. Y puede ser portmember, static o notallowed |
| ports remove <ports><br>[member <value>] | Remueve los puertos de una VLAN pero no borra la VLAN<br>• ports es una lista de puertos<br>• member <value> es el tipo de miembro del puerto. Y puede ser portmember, static o notallowed |

El comando *show vlan* muestra información de la configuración acerca de las VLANs o de una en específica, dependiendo de las opciones que a continuación se muestran.

| | |
|---|---|
| *show vlan info all [<vid>]* | muestra información general de todas las VLANs o de una en específico, donde el <vid> es el ID de la VLAN |
| *show vlan info advance [<vid>]* | muestra parámetros adicionales de una VLAN en específico o de todas, donde el <vid> es el ID de la VLAN |
| *show vlan info basic [<vid>]* | muestra la configuración básica de una VLAN en específico o de todas, donde el <vid> es el ID de la VLAN |

## *6.2 Device Manager*

El DM es un software que se proporciona con el *Passport* 8610 para la administración del equipo y con él, es posible llevar el control de las VLANs. Los requerimientos mínimos para la instalación del DM sobre plataforma Windows son los siguientes:

- Procesador Pentium o mayor a 400 Mhz
- 128 MB en RAM
- 100 MB de espacio en disco duro
- JRE (*Java Runtime Environment*) versión 1.3.0

Después de la instalación se utiliza la ventana de DM para conectarse al *Passport* 8610, para lo que se da "*click*" en *Device*, para escribir el nombre o dirección IP del dispositivo, y finalmente "*click*" en el botón *Open*; como se muestra la Figura 6.1.

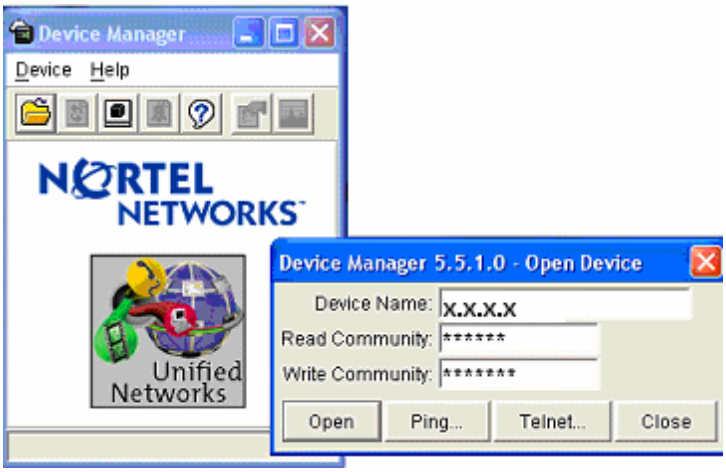



Figura 6.1 Ventana del *Device Manager*

Posteriormente se tiene la ventana de la Figura 6.2 que muestra el dispositivo, que es el *Passport* 8610, donde se ven los módulos del equipo así como el estado de los puertos. En el menú que está en la parte superior se da "*click*" en VLANs.

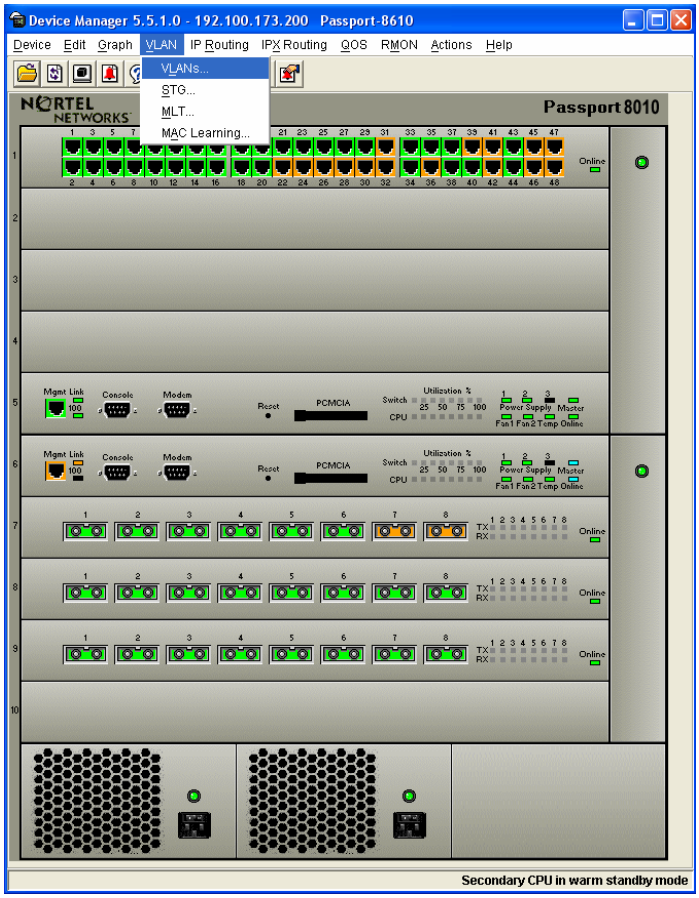
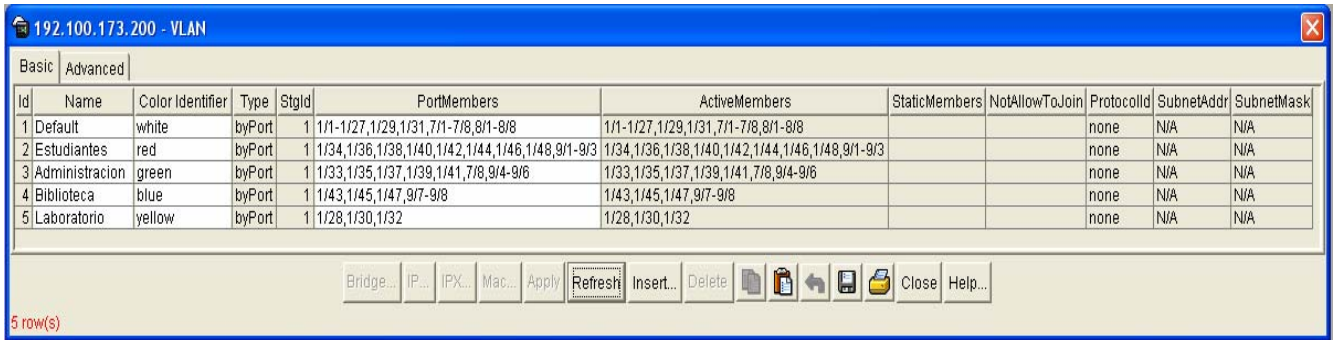



Figura 6.2 *Passport* 8610

En esta ventana (véase Figura 6.3) muestra las VLANs, así como algunas características básicas de configuración de las mismas.




| Id | Name | Color Identifier | Type | StgId | PortMembers | ActiveMembers | StaticMembers | NotAllowToJoin | ProtocolId | SubnetAddr | SubnetMask |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Default | white | byPort | 1 | 1/1-1/27,1/29,1/31,7/1-7/8,8/1-8/8 | 1/1-1/27,1/29,1/31,7/1-7/8,8/1-8/8 | | | none | N/A | N/A |
| 2 | Estudiantes | red | byPort | 1 | 1/34,1/36,1/38,1/40,1/42,1/44,1/46,1/48,9/1-9/3 | 1/34,1/36,1/38,1/40,1/42,1/44,1/46,1/48,9/1-9/3 | | | none | N/A | N/A |
| 3 | Administracion | green | byPort | 1 | 1/33,1/35,1/37,1/39,1/41,7/8,9/4-9/6 | 1/33,1/35,1/37,1/39,1/41,7/8,9/4-9/6 | | | none | N/A | N/A |
| 4 | Biblioteca | blue | byPort | 1 | 1/43,1/45,1/47,9/7-9/8 | 1/43,1/45,1/47,9/7-9/8 | | | none | N/A | N/A |
| 5 | Laboratorio | yellow | byPort | 1 | 1/28,1/30,1/32 | 1/28,1/30,1/32 | | | none | N/A | N/A |

Figura 6.3 Ventana de configuración de la VLANs

A través de esta ventana se puede modificar, agregar, borrar VLANs (véase Figura 6.4), también agregar o remover puertos; cambiar de nombre y color de las redes virtuales, así como de otras configuraciones.

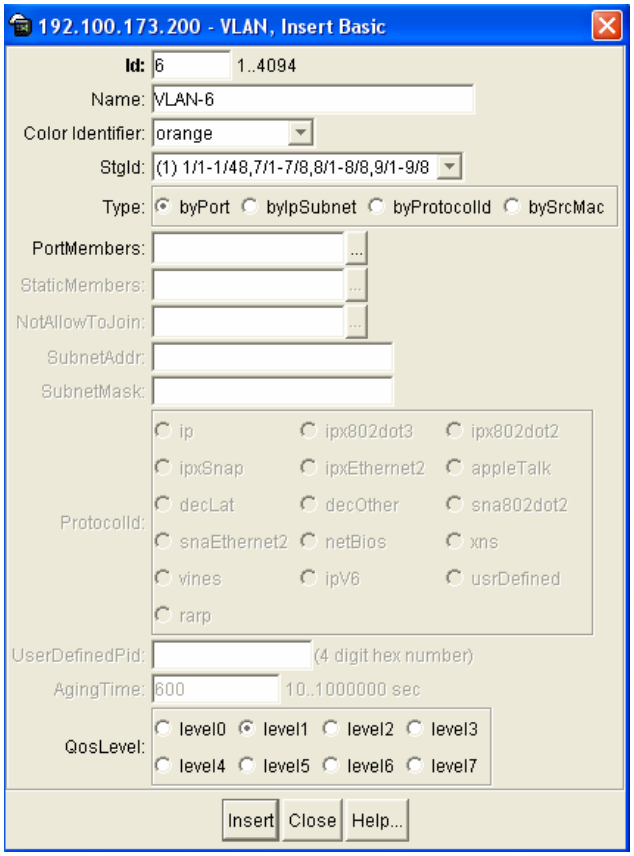



Figura 6.4 Ventana de agregar una VLAN

Con está herramienta además de tener la administración de las redes virtuales, se tiene el control, configuración y administración del equipo (*Passport* 8610).

## 6.3 VLAN *Manager*

VLAN *Manager* es una herramienta que está incluida dentro de una aplicación de administración propia del *Passport* 8610, llamada *Optivity Switch Manager* (OSM). Por lo

que es necesario instalar primero el OSM, los requerimientos mínimos para la instalación del OSM sobre plataforma Windows son los siguientes:

- Procesador Pentium o mayor a 400 Mhz
- 128 MB en RAM
- 120 MB de espacio en disco duro
- JRE (*Java Runtime Environment*) versión 1.3.0

Realizada la instalación lo siguiente es abrir la aplicación (OSM), al abrirla se muestra un icono que es el *Passport* 8610. Para abrir la herramienta de VLAN Manager se da "*click*" en *Tools* y después en VLAN *Manager* (véase Figura 6.5).

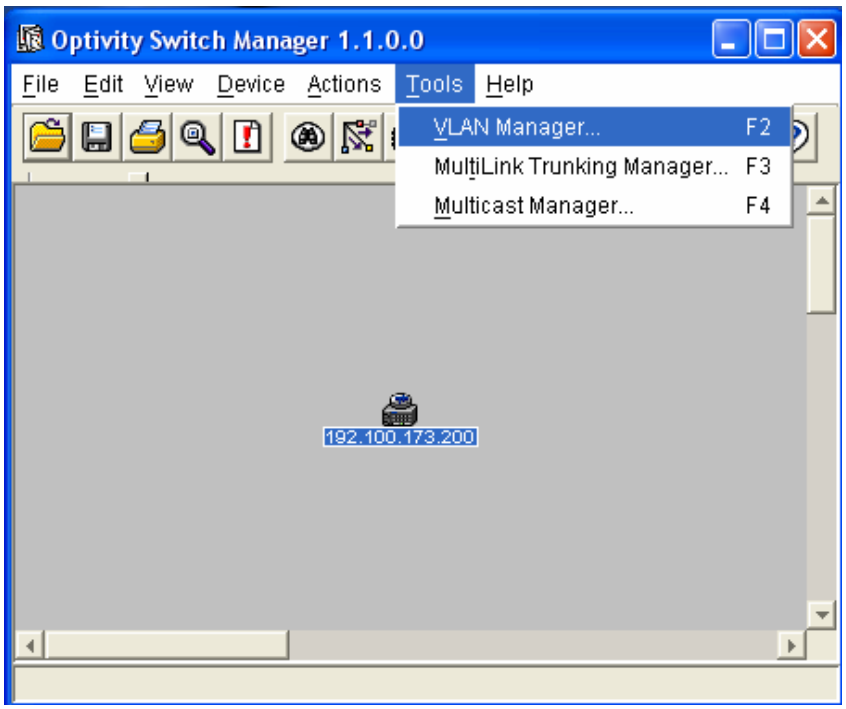



Figura 6.5 Ventana del OSM

La Figura 6.6 muestra la ventana de VLAN Manager, donde se pueden ver configuraciones y estados de las redes virtuales, entre otros detalles de configuración del *Passport* 8610. En esta ventana se puede distinguir los colores de la VLANs que fueron asignadas, así como el tipo de VLAN (puerto, subnet, protocolo y dirección MAC).

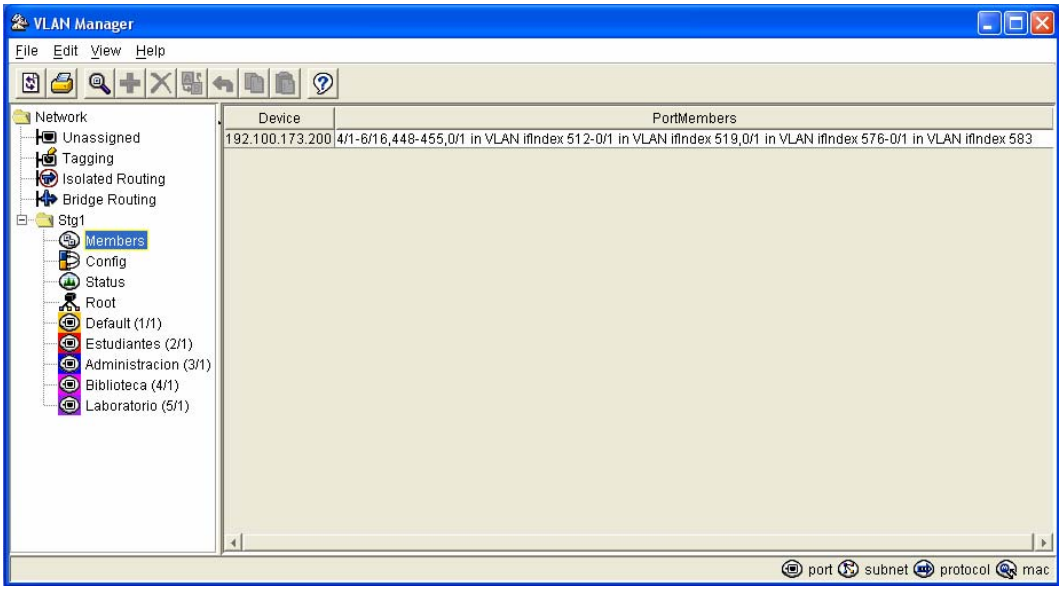



Figura 6.6 Ventana de VLAN *Manager*

Como en las otras herramientas de administración a través de VLAN *Manager* también se pueden agregar y borrar VLANs. Para agregar una VLAN se puede hacer de la siguiente manera; se selecciona el grupo de stg (*spanning tree protocol*), en "*Edit*" se selecciona insertar y aparece la ventana de la Figura 6.7.

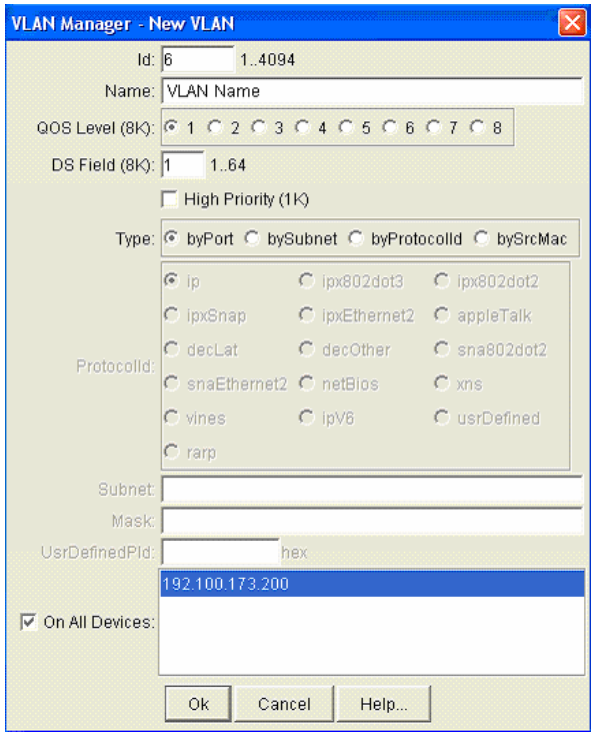



Figura 6.7 Ventana para la creación de una nueva VLAN a través de VLAN *Manager*

En está ventana están los campos para la creación de una VLAN, donde:

- "*Id*" es el identificador de la VLAN
- "*Name*" es el nombre de la VLAN
- "*QoS Level*" es el nivel de Calidad de Servicio (opcional)
- "*DS Field*" Servicios Diferenciados (opcional)
- "*High Priority*" Prioridad Alta (opcional)
- "*Type*" tipo de VLAN (*byport, bySubnet, byProtocolId, bySrcMac*)
- "*On All Devices*" seleccionar el dispositivo

Seleccionados los campos se da "*click*" en "*Ok"* para crear la VLAN. Para borrar una VLAN se selecciona primero, después, de la barra de herramientas se selecciona "*Edit"*, para posteriormente hacer "*click*" en *Delete*.

Con lo anterior, se concluye de manera general la descripción básica del conjunto de herramientas particulares para llevar a cabo la administración de las redes virtuales.

# CONCLUSIONES

Al final del presente proyecto de tesis se concluye que se cumplieron satisfactoriamente con los objetivos planteados. Esto se logró conforme a los siguientes procedimientos realizados, como son: el análisis, diseño, implementación y administración de las redes virtuales, así como con la integración de éstas con el *firewall*.

La parte de análisis fue importante, por que permitió conocer los problemas, debilidades y vulnerabilidades que existían en la red LAN; esto ayudó también para mejorar en aspectos importantes: administración, tecnología y seguridad.

La etapa de diseño fue parte base en la elaboración de la tesis por las consideraciones que se tomaron en cuenta en la creación de las redes virtuales, como fueron: el tipo de red virtual a implementar, servicios y aplicaciones por VLAN, esquema de direccionamiento, comunicación entre redes virtuales y por último la integración de las redes virtuales con el *firewall*.

Un punto también importante en el proyecto fue la selección del equipo de *Backbone,* columna vertebral en la infraestructura de red y sobre el cual se implementaron las redes

virtuales. El hecho de cambiar el equipo fue por que éste ya había cumplido su ciclo de vida de 5 años, lo que motivo la actualización del mismo y por consiguiente buscar un equipo que estuviera acorde con las nuevas tecnologías de información.

Con la implementación de las redes virtuales en El Colegio de México, los beneficios se vieron reflejados en el rendimiento de la red LAN, lo que provocó que los tiempos de respuesta fueran más rápidos en los equipos de cómputo; como son las computadoras de escritorio, servidores y equipos de comunicaciones. Adicionalmente, hubo una disminución de errores, colisiones, *broadcast* y *drops*, los cuales inundaban la red LAN de tráfico que no era necesario, lo que provocaba lentitud en la red. La disminución de errores, colisiones y drops fue al mínimo, de hecho a cero y los broadcast disminuyeron de manera considerable.

Con la integración de las redes virtuales con el *firewall* se completó una parte importante en cuanto a la seguridad en la red LAN de El Colegio, esta integración se realizó debido a posibles ataques que pudiera haber externos a la Institución. Por ello, el *firewall* como parte esencial en la seguridad de la red LAN de El Colegio de México, A.C. se conjunta a la creación y configuración de las redes virtuales.

# ANEXO

Algunos de los factores que afectan la eficiencia de una red son: cantidad de tráfico, número de nodos, tamaño de paquetes y diámetro de la red. Algunos parámetros que nos pueden ayudar para medir la eficiencia de una red es: la tasa de utilización y la tasa de colisión. La tasa de utilización es usada para indicar el comportamiento de una red, una tasa de utilización por encima del 35% pronostica problemas potenciales, es decir, que es casi óptima. La tasa de colisión mide el porcentaje de paquetes que provocan colisiones, algo menos del 10% es frecuente en redes funcionando adecuadamente.

En este anexo se integran gráficas de utilización, errores, colisiones, *broadcast* y *drops* generadas a partir de las capturas de información con el *sniffer*; realizadas en la red local de El Colegio antes y después de la implementación de las redes virtuales. En las gráficas se demuestran los resultados satisfactorios obtenidos con la creación de las VLANs.

En la Figura 7.1 se muestra la utilización de la red local antes de la creación de las redes virtuales, en ella se ve la elevada saturación de la red.

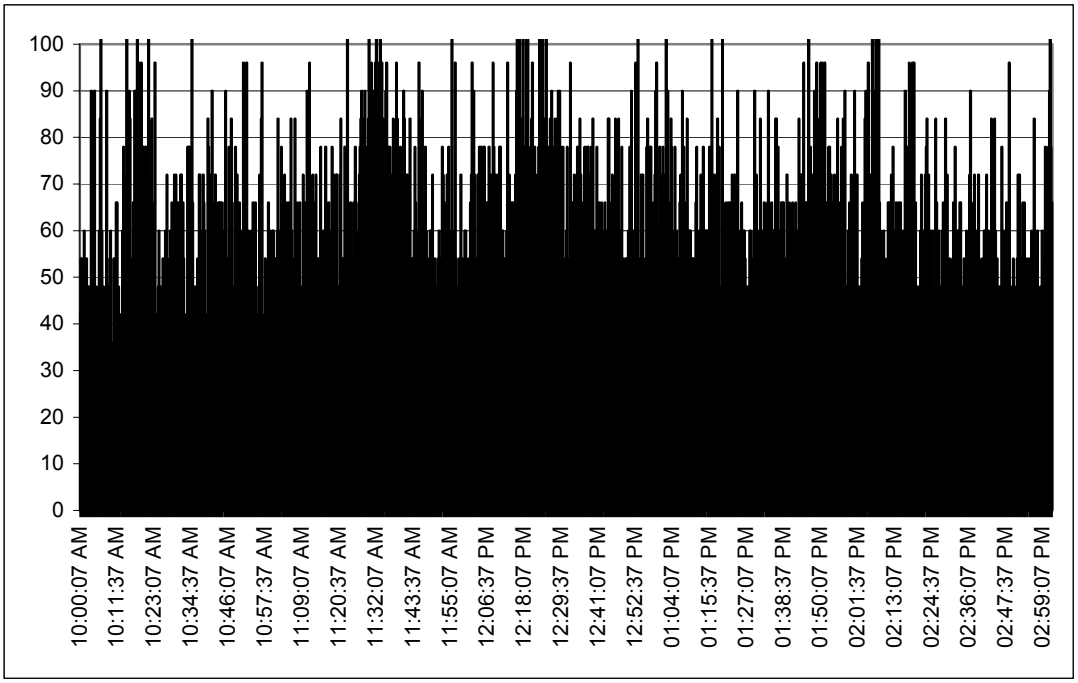



Figura 7.1 Gráfica de utilización (antes de las VLANs).

Con la creación de las redes virtuales la utilización la red se ve disminuida como lo muestra la Figura 7.2.

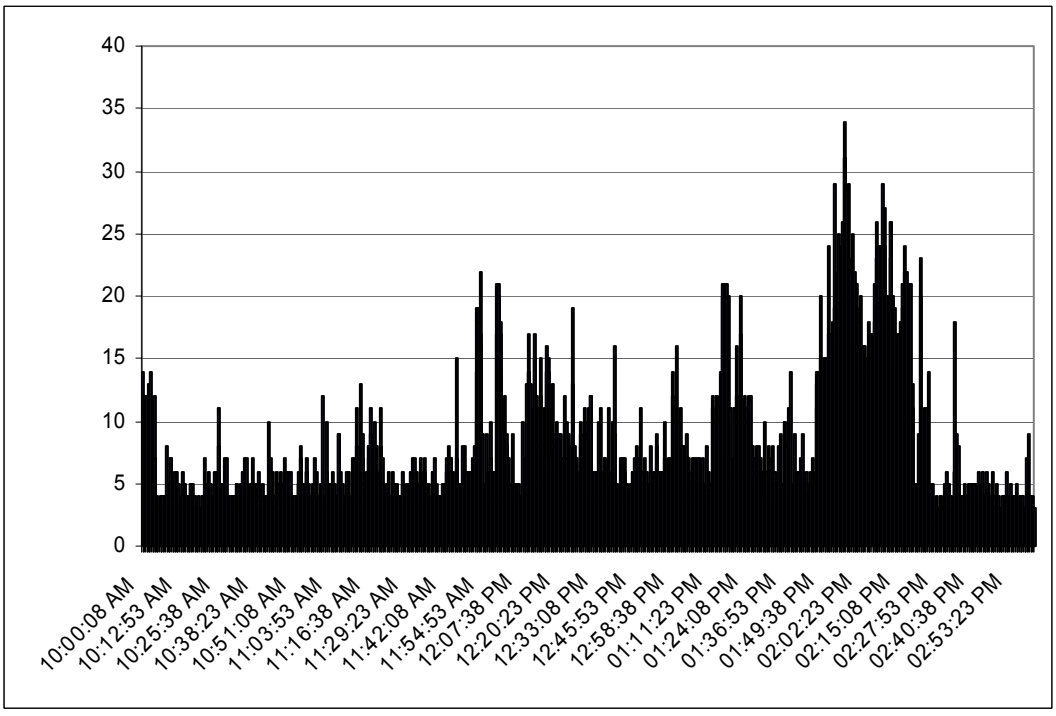



Figura 7.2 Gráfica de utilización (después de las VLANs).

Antes de la creación de las redes virtuales los errores generados en la red local eran elevados, como lo muestra la Figura 7.3.

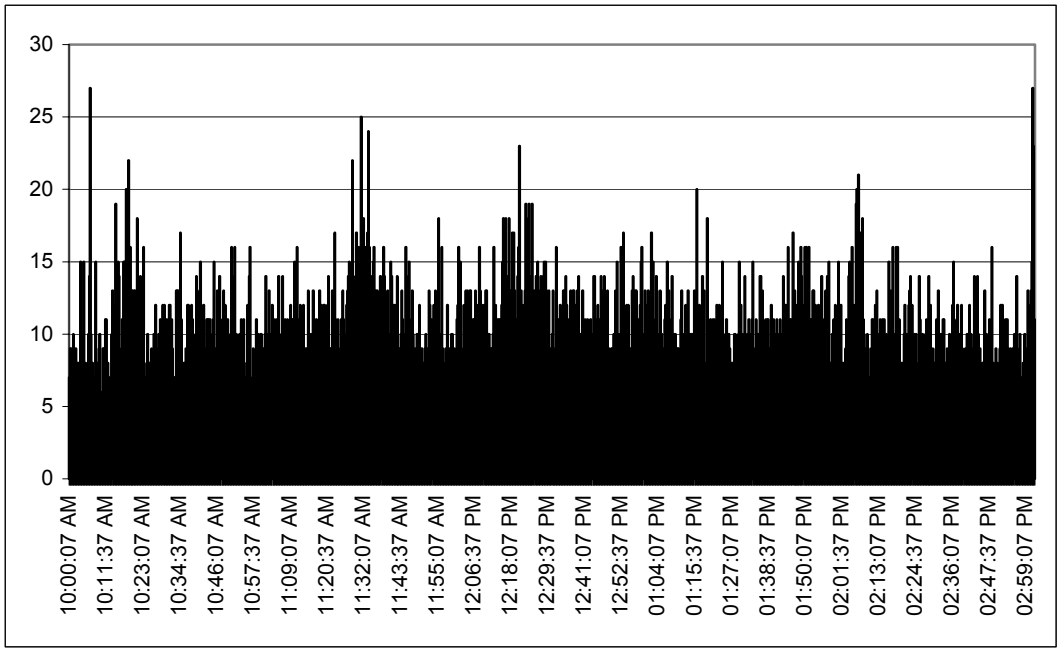



Figura 7.2 Gráfica de errores (antes de las VLANs).

Después de la creación de la VLANs los errores disminuyeron al mínimo, de hecho a cero, como lo muestra la Figura 7.4.

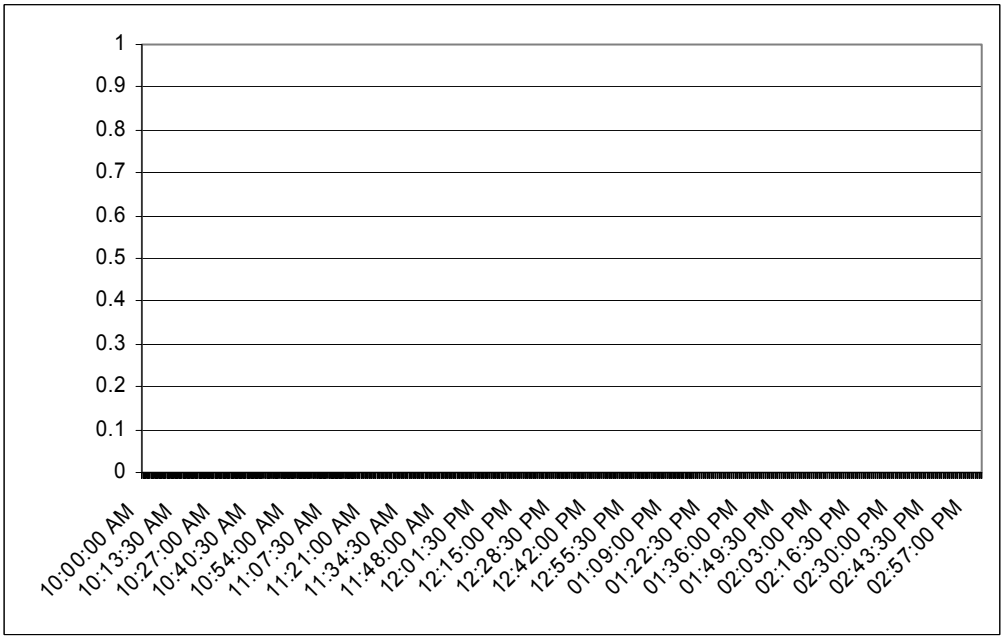



Figura 7.4 Gráfica de errores (después de las VLANs).

Con respecto a las colisiones (véase la Figura 7.5) antes de la creación de las redes virtuales, estás se generaban con un número elevado, por lo que repercutía en la red local.

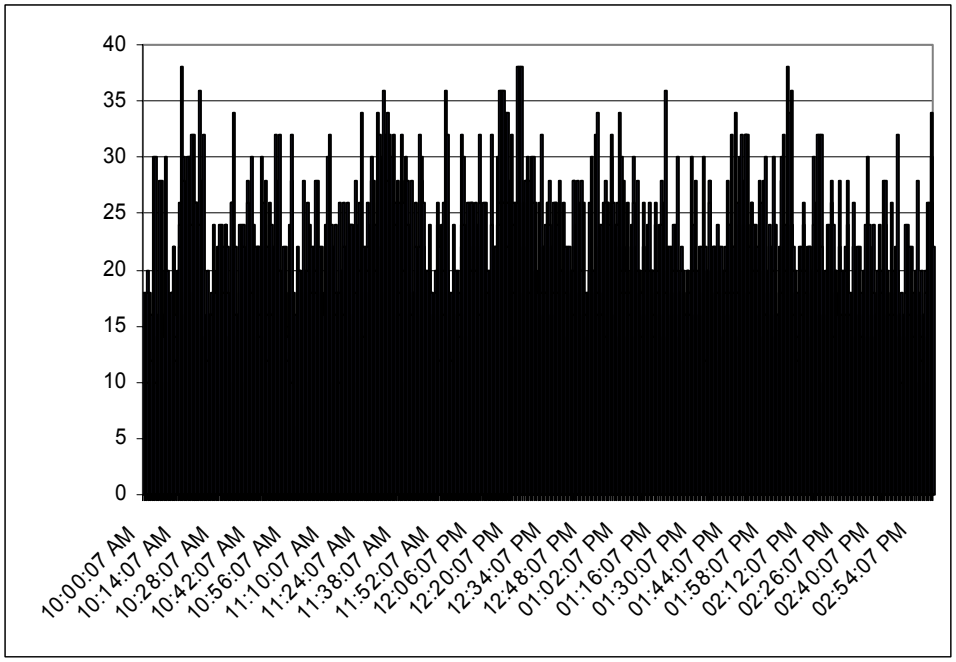



Figura 7.5 Gráfica de colisiones (antes de las VLANs).

Una vez generadas las VLANs las colisiones se redujeron a cero, como lo muestra la Figura 7.6.

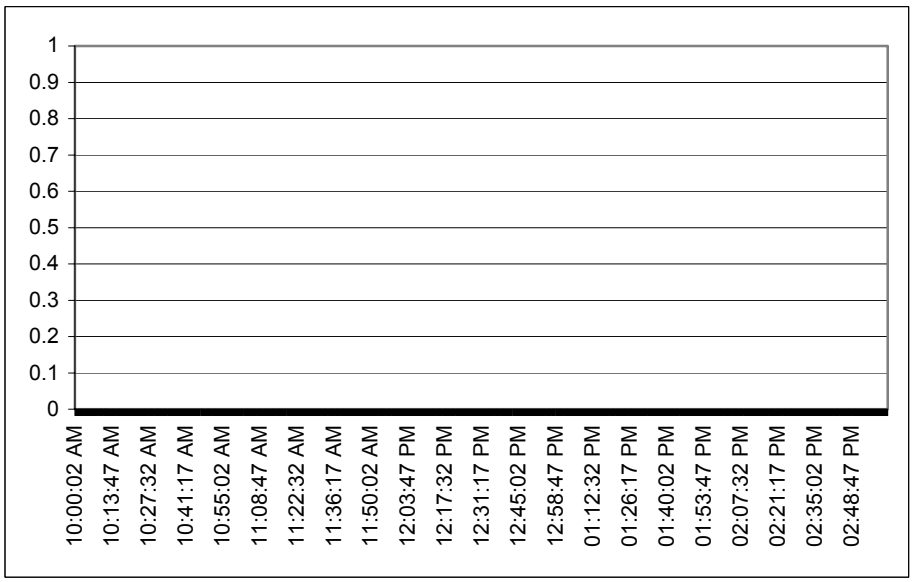



Figura 7.6 Gráfica de colisiones (después de las VLANs).

En lo que se refiere a *broadcast* que es un tráfico generado por los equipos de cómputo, eran de un número considerable antes de la creación de las redes virtuales, esto saturaba la red local; como lo muestra la Figura 7.7.

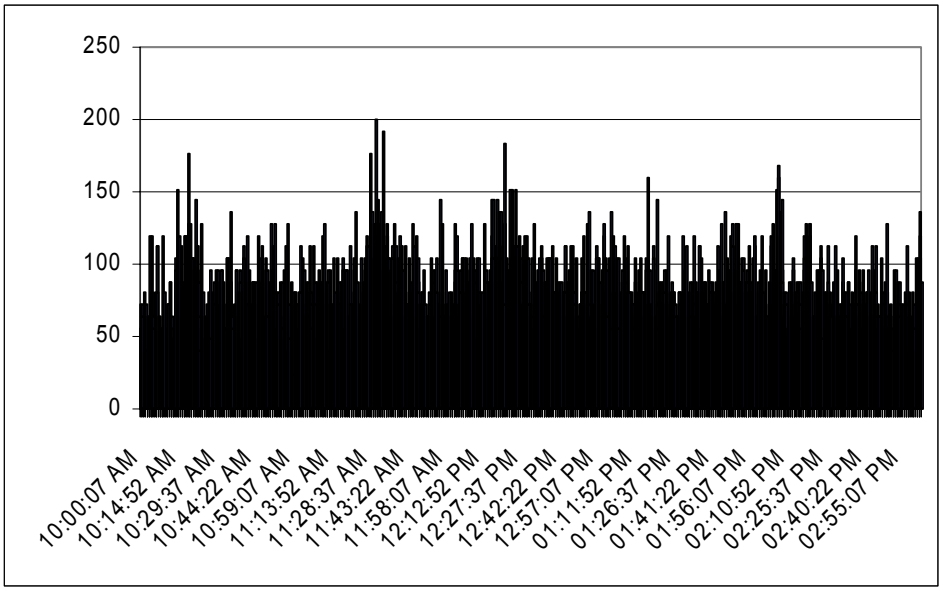



Figura 7.7 Gráfica de *broadcast* (antes de las VLANs).

Con la creación de las redes virtuales éste tipo de tráfico disminuyó considerablemente (véase Figura 7.8) en la red local, por que cada red virtual es un dominio lógico de *broadcast*.

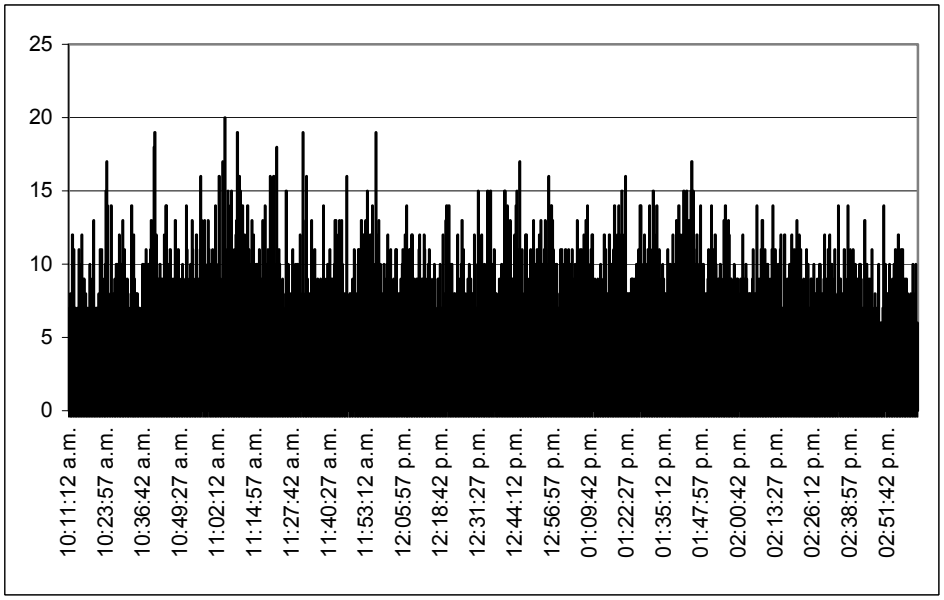



Figura 7.8 Gráfica de *broadcast* (después de las VLANs).

En lo que se refiere a *drops*, que son paquetes tirados a consecuencia de que no llegan a ser procesados o por saturación en la utilización de la red. La gráfica de la Figura 7.9 muestra el número de *drops* generados antes de la creación de las redes virtuales.

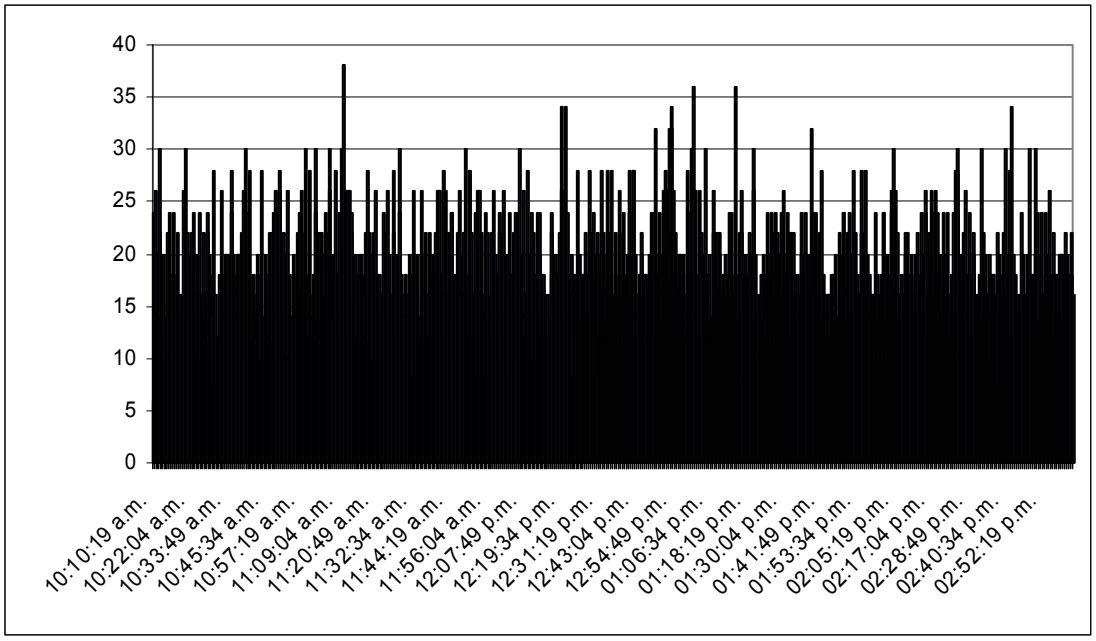



Figura 7.9 Gráfica de *drops* (antes de las VLANs).

Una vez creadas las redes virtuales el número de paquetes tirados (*drops*) fue nulo, como lo muestra la Figura 7.10

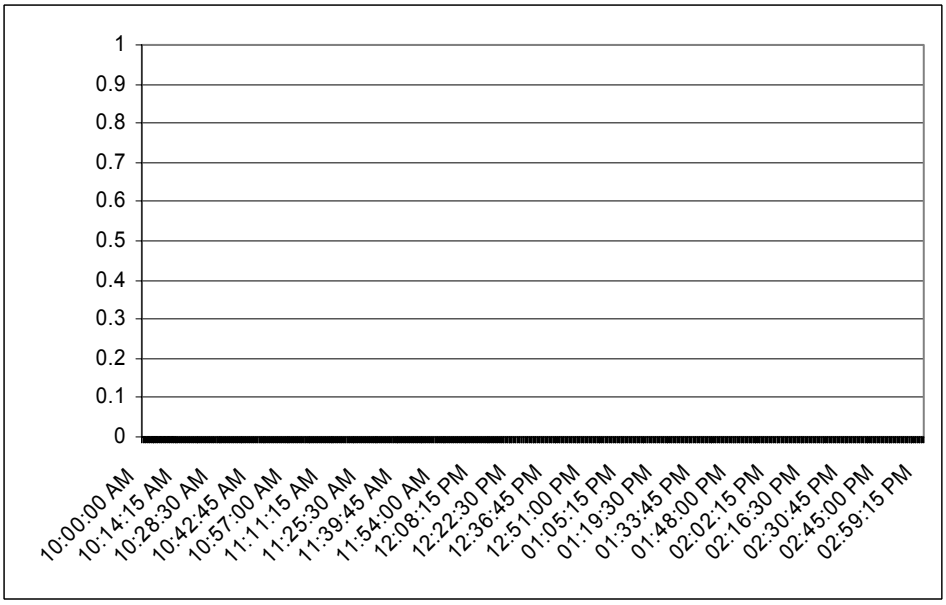



Figura 7.10 Gráfica de *drops* (después de la VLANs).

Con el resultado de las gráficas anteriores se demuestra y comprueba aún más el mejoramiento que se obtuvo y que se tiene actualmente en la red LAN de El Colegio de México, al haber implementado las redes virtuales.

# BIBLIOGRAFÍA

Ford, Merilee. Tecnologías de Interconectividad de Redes. Prentice-Hall. México, 1998.

Tanenbaum, Andrew S. Redes de Computadoras. Prentice-Hall Hispanoamérica. México, 1997.

Habraken, Joe. Routers Cisco. Pearson Educación. Madrid, 2000.

Nortel Networks. Passport 1000/8000 Configuratión and Management. Anixter. México, 2000.

UNAM, Diplomado de Telecomunicaciones, México, 2001.

García, Rafael. Guía de Seguridad. Rev. Red México 2003; 147:1-20.

García, Isabel. El Cómputo en El Colegio de México. Rev. Boletín Editorial México 2000; 87:37-43.

Redes Locales Virtuales [citado en agosto 2002]. Disponible en World Wide Web: http://www.lcc.uma.es/~eat/services/rvirtual/rvirtual.html#link1

Palet, Jordi. 1995 [citado en septiembre 2002]. Tecnología y productos de conmutación de redes. Disponible en World Wide Web: http://www.consulintel.es/Html/Tutoriales/Articulos/tecn_conm.html