Universidad Austral de Chile

Facultad de Ciencias de la Ingeniería

Escuela de Electricidad y Electrónica

Diseño e Implementación de una Red de Acceso Múltiple para Aplicaciones Educativas Virtuales en el Centro Educacional San Nicolás

Trabajo de Titulación para optar al
Título de Ingeniero en Electrónica

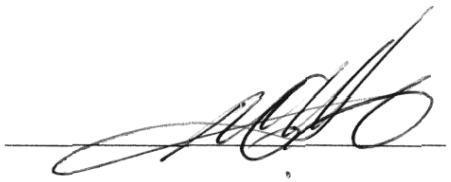
Profesor Patrocinante:
Sr. Néstor Fierro Morineaud

SERGIO ALARCÓN ACEITÓN - JAIME SÁNCHEZ RAMÍREZ

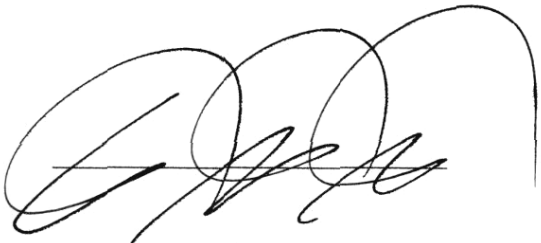
VALDIVIA

2007

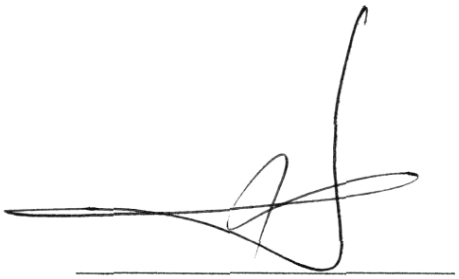
Comisión de Titulación y Fecha de Examen de Grado



Sr. Nestor Fierro Morineaud
Profesor Patrocinante



Sr. Pedro Rey Clericus.
Profesor Informante



Sr. Raúl Urra Ríos
Profesor Informante

Fecha Examen de Titulación: 17. MARZO 2008

AGRADECIMIENTOS

Todos los triunfos nacen cuando nos atrevemos a comenzar y cada paso dado es un esfuerzo que se logra gracias al cariño de nuestros seres queridos en especial la familia la cual nos entrega la energía y aliento necesario para seguir adelante y llegar a la meta.

Queremos agradecer primero a Dios por guiarnos en el camino del conocimiento y aprendizaje y a nuestros queridos Padres quienes durante todos estos años contribuyeron, gracias a su apoyo y comprensión, a concretar este triunfo.

INDICE

CAPÍTULO IV: IMPLEMENTACIÓN DEL PROYECTO

RESUMEN

Este trabajo de tesis se realizó con el propósito de investigar y aplicar conocimientos sobre redes de datos, con el fin de desarrollar un proyecto en beneficio de la comunidad escolar del Centro Educacional San Nicolás ubicada en René Schnaider en la ciudad de Valdivia, el cual no contaba con una infraestructura de red apropiada para sus alumnos y docentes.

En base a este problema se diseño e implementó un modelo de red que tiene acceso alámbrico e inalámbrico y está dividida en dos etapas: la primera corresponde al laboratorio de computadores que utilizarán los alumnos y la segunda etapa incluye el sector de la biblioteca del establecimiento.

El desarrollo de esta tesis esta contenida en cuatro capítulos: el primero describe conceptos importantes sobre redes de datos; el segundo se refiere a dispositivos vitales para el funcionamiento de una red; el tercer capítulo establece la propuesta del proyecto, en donde se indica el diseño de la red; el cuarto describe la implementación del proyecto, mencionando el trabajo en cada etapa y los elementos de hardware y software que se utilizaron.

ABSTRACT

This thesis was undertaken with the aim to investigate and apply knowledge on data networks, in order to develop a project to benefit the school community of San Nicolas Educational Center located at Rene Schnaider in the city of Valdivia, which does not he had a network infrastructure suitable for their students and teachers.

Based on this problem was designed and implemented a network model which has wireline and wireless access and is divided into two phases: the first covers the computer lab to be used by students and the second phase includes the section of the library establishment.

The development of this thesis is contained in four chapters: the first describes important concepts on data networks, while the latter refers to devices vital to the operation of a network, the third chapter provides the project proposal, which suggests the design the network, the fourth describes the implementation of the project, citing the work at every stage and the elements of hardware and software were used.

INTRODUCCIÓN

El uso del computador y de software educativo ya es parte del quehacer de muchos establecimientos educacionales en chile, los cuales son la principal fuente de acceso a computadores e Internet para los menores de 21 años y por lo tanto, representan un factor de equidad en el acceso para los sectores de menores ingresos del país.

La incorporación de la tecnología informática, multimedia e Internet en los establecimientos es una realidad y a la vez una necesidad, puesto que ayuda a mejorar la calidad de la educación ya que, en particular, permiten acceso rápido a información de dominio público y que, hoy día, abarca casi todos los campos.

Además, contribuye a la formación de alumnos y alumnas, desarrollando habilidades y los conocimientos necesarios para identificar y resolver problemas en los cuales la aplicación de la computación significa un aporte en su calidad de vida. Al mismo tiempo, se potencia la capacidad de opinar y razonar sobre sus ventajas y desventajas para su uso adecuado en el medio que lo rodea.

La computación es una asignatura que de a poco ha contribuido al mejoramiento de una política comunicacional, de modo que los niños día a día se están familiarizando

En Chile la computación en la educación está entrando en los colegios particulares, subvencionados y municipalizados. A través de programas como la Red Enlaces del Ministerio de Educación a nivel nacional, y mediante iniciativas como ‘Kidsmardt’, impulsada en conjunto por el Gobierno y la empresa privada, la gran mayoría de los niños está teniendo acceso a una nueva forma de educación, basada en las tecnologías que hoy mueven al mundo.

CAPÍTULO I: REDES DE DATOS

1.1 MODELO OSI

El modelo OSI (Open Systems Interconection) de telecomunicaciones esta basado en una propuesta desarrollada por la organización de estándares internacional (ISO), por lo que también se le conoce como modelo ISO - OSI. Su función es la de definir la forma en que se comunican los sistemas *abiertos* de telecomunicaciones, es decir, los sistemas que se comunican con otros sistemas.

El modelo OSI esta constituido por 7 capas que definen las funciones de los protocolos de comunicaciones. Cada capa del modelo representa una función realizada cuando los datos son transferidos entre aplicaciones cooperativas a través de una red intermedia.

Fig. 1.1- Capas Modelo OSI

1.1.1 Estructura del Modelo OSI

El objetivo perseguido por OSI establece una estructura que presenta las siguientes particularidades:

Estructura multinivel**:** Se diseñó una estructura multinivel con la idea de que cada nivel se dedique a resolver una parte del problema de comunicación. Esto es, cada nivel ejecuta funciones específicas.

El nivel superior utiliza los servicios de los niveles inferiores: Cada nivel se comunica con su similar en otras computadoras, pero debe hacerlo enviando un mensaje a través de los niveles inferiores en la misma computadora. La comunicación internivel está bien definida. El nivel N utiliza los servicios del nivel N-1 y proporciona servicios al nivel N+1.

Puntos de acceso: Entre los diferentes niveles existen interfaces llamadas "puntos de acceso" a los servicios.

Dependencias de Niveles: Cada nivel es dependiente del nivel inferior y también del superior.

Encabezados: En cada nivel, se incorpora al mensaje un formato de control. Este elemento de control permite que un nivel en la computadora receptora se entere de que su similar en la computadora emisora esta enviándole información. Cualquier nivel dado, puede incorporar un encabezado al mensaje. Por esta razón, se considera que un mensaje esta constituido de dos partes: Encabezado e Información. Entonces, la incorporación de encabezados es necesaria aunque representa un lote extra de información, lo que implica que un mensaje corto pueda ser voluminoso. Sin embargo, como la computadora destino retira los encabezados en orden inverso a como fueron incorporados en la computadora origen, finalmente el usuario sólo recibe el mensaje original.

Unidades de información**:** En cada nivel, la unidad de información tiene diferente nombre y estructura.

1.1.2 Niveles del Modelo OSI

Capa Física

Es la encargada de transmitir los bits de información por la línea o medio utilizado para la transmisión. Se ocupa de las propiedades físicas y características eléctricas de los diversos componentes; de la velocidad de transmisión, si esta es uni o bidireccional (simplex, duplex o flull-duplex). También de aspectos mecánicos de las conexiones y terminales, incluyendo la interpretación de las señales eléctricas.

Como resumen de los cometidos de esta capa, podemos decir que se encarga de transformar un paquete de información binaria ("Frame") en una sucesión de impulsos adecuados al medio físico utilizado en la transmisión. Estos impulsos pueden ser eléctricos (transmisión por cable); electromagnéticos (transmisión Wireless) o luminosos (transmisión óptica). Cuando actúa en modo recepción el trabajo es inverso; se encarga de transformar estos impulsos en paquetes de datos binarios que serán entregados a la capa de enlace.

Por ejemplo: este nivel define las medidas del cable coaxial Ethernet y de los conectores BNC utilizados. Otro ejemplo de estándares relativos a esta capa son RS-232 para comunicaciones serie y X.21

Capa de enlace

Proporciona servicio de envío de datos a través del enlace físico e implementa el acceso al medio mediante protocolos que manejan dos subcapas.

- **Control lógico de enlace LLC** ("Logical Link Control") define la forma en que los datos son transferidos sobre el medio físico, ejecuta el control de flujo y errores de datos.
- **Control de acceso al medio MAC** ("Medium Access Control"). Esta subcapa actúa como controladora del hardware subyacente (el adaptador de red). De hecho el controlador de la tarjeta de red es denominado a veces "MAC driver", y la dirección física contenida en el hardware de la tarjeta es conocida como dirección MAC ("MAC address"). Su principal tarea (que le proporciona el nombre -control de acceso-) consiste

en arbitrar la utilización del medio físico para facilitar que varios equipos puedan competir simultáneamente por la utilización de un mismo medio de transporte.

Además del direccionamiento local, se ocupa de la detección y control de errores ocurridos en la capa física, del control del acceso a dicha capa y de la integridad de los datos y fiabilidad de la transmisión. Para esto agrupa la información a transmitir en bloques ("Frames"), e incluye a cada uno una suma de control que permitirá al receptor comprobar su integridad. Los datagramas recibidos son comprobados por el receptor.

Capa de Red

Esta capa proporciona las especificaciones para el encaminamiento de las tramas a través de una interred, donde todos los nodos componentes de esta interred funcionan bajo el mismo protocolo que el origen y destino de los paquetes.

La búsqueda de estaciones en la red se lleva a efecto mediante la ejecución de los protocolos ARP (Addressing Resolution Protocol) y RARP (Reverse Addressing Resolution Protocol). Entre ambos resuelven el problema creando un canal directo con el protocolo MAC de la capa inferior, a objeto de mantener una tabla de relación entre direcciones físicas-lógicas de las estaciones que se encuentran en la vecindad y que han sido descubiertas por el proceso.

Asimismo, cuando se hace necesario efectuar una mantención de la red, ya sea automática o manual por parte de algún usuario, se utiliza el protocolo ICMP (Internet Control Management Protocol), el que dispone de una serie de herramientas como para saber el estado de los enlaces y trayectorias que los paquetes están siguiendo en su trayectoria origen-destino.

Capa de transporte

En este nivel se realiza y se garantiza la calidad de la comunicación, ya que asegura la integridad de los datos. Es aquí donde se realizan las retransmisiones cuando la información fue corrompida o porque alguna trama (del nivel 2) detectó errores en el formato y se requiere volver a enviar el paquete o datagrama.

El nivel de transporte notifica a las capas superiores si se está logrando la calidad requerida. Este nivel utiliza reconocimientos, números de secuencia y control de flujo.

Los protocolos TCP (Transmission Control Protocol) y UDP (User Datagram Protocol) son característicos del nivel del transporte del modelo OSI, al igual que SPX (Sequenced Packet Exchange) de Novell.

En Resumen se dice que la capa de Transporte es la integridad de datos de extremo a extremo o sea que se encarga el flujo de datos del transmisor al receptor verificando la integridad de los mismos por medio de algoritmos de detección y corrección de errores, la capa de Red es la encargada de la información de enrutador e interceptores y aquella que maneja el Hardware (HW), ruteadores, puentes, multiplexores para mejorar el enrutamiento de los paquetes.

Capa de sesión

Este nivel es el encargado de proveer servicios de conexión entre las aplicaciones, tales como iniciar, mantener y finalizar una sesión. Establece, mantiene, sincroniza y administra el diálogo entre aplicaciones remotas.

Cuando establecemos una comunicación y que se nos solicita un comando como login, estamos iniciando una sesión con un host remoto y podemos referenciar esta función con el nivel de sesión del modelo OSI. Del mismo modo, cuando se nos notifica de una suspensión en el proceso de impresión por falta de papel en la impresora, es el nivel de sesión el encargado de notificarnos de esto y de todo lo relacionado con la administración de la sesión. Cuando deseamos finalizar una sesión, quizá mediante un logout, es el nivel de sesión el que se encargará de sincronizar y atender nuestra petición a fin de liberar los recursos de procesos y canales (lógicos y físicos) que se hayan estado utilizando.

Capa de presentación

Estandariza la forma en que se presentan los datos a las aplicaciones. Se refiere a la forma en que los datos son representados en una computadora. Proporciona conversión de códigos y reformateo de datos de la aplicación del usuario.

La información es procesada en forma binaria y en este nivel se llevan a cabo las adaptaciones necesarias para que pueda ser presentada de una manera más accesible.

Capa de aplicación

En esta capa van dirigidos todos aquellos programas que prestan un directo servicio al usuario, aún siendo rutinas del sistema operativo. Existe un puerto asociado a cada una de las aplicaciones que funcionan en red. Por este puerto fluirá en ambos sentidos los datos y la información. Todos estos servicios funcionan en base a la filosofía "cliente-servidor".

Los servicios más demandados tanto en redes cerradas como abiertas, son:

Servicio de Nombre de Dominio (DNS): Cada vez que es necesario ubicar a alguien en la red IP, se piensa en un nombre, colocando en la estructura subdominio.dominio.superdominio (fci.uach.cl). Quien atiende estas consultas es el servidor DNS, que mantiene una lista de todas las peticiones que ha recibido, grabadas en un caché de direcciones, asociados los nombres a sus correspondientes números IP. Esta información proviene de los DNS de niveles superiores, que alimentan a cada servidor con el correr del tiempo.

Servicio de http: Conocido también como navegación por el espacio WEB o WWW, es un sistema que funciona en base a un cliente que funciona en la máquina del consumidor de información y que busca a un servidor que se identifica como http://www.algo.algo. Cuando lo encuentra, el servidor descarga un archivo con código HTML que el programa cliente interpreta y muestra su contenido por una ventana. Este código HTML contiene incrustaciones de otros lenguajes como JAVA, PHP, XML.etc.

Servicio de transferencia de archivos (FTP): Permite la transferencia ininterrumpida de grandes volúmenes de datos grabados en archivos, desde un programa servidor a un cliente (get) o viceversa (put). Para que ocurra esta última acción es necesario que exista una cuenta de usuario en el servidor, asociada a una contraseña, para autentificar a los usuarios.

Servicio de mensajerìa electrónica: Estos protocolos, que funciona uno para el envío y otro para la recepción, permiten a través de un programa cliente escribir mensajes cortos de texto y adjuntarle otros tipos de datos y enviárselos a alguna persona que tenga casilla electrónica. Los protocolos que funcionan son para el correo saliente SMTP y para el entrante el POP3 o IMAP. Este último normalmente, autentica al usuario antes de descargar los mensajes que están almacenados en su casilla.

Servicio de conexión remota asegurado (Virtual Private Network): Protocolo que permite utilizar una red pública o semi pública para conectarse a un servidor u otra màquina en forma segura, creando un túnel en la red pública, por donde viaja la información en forma encriptada.

Telnet: Otro terminal remoto, ha caído en desuso por su inseguridad intrínseca, ya que las claves viajan sin cifrar por la red.

1.2 MODELO TCP/IP

Es el protocolo común utilizado por todos los ordenadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Hay que tener en cuenta que en Internet se encuentran conectados ordenadores de clases muy diferentes y con *hardware* y *software* incompatibles en muchos casos, además de todos los medios y formas posibles de conexión. Aquí se encuentra una de las grandes ventajas del TCP/IP, pues este protocolo se encargará de que la comunicación entre todos sea posible. TCP/IP es compatible con cualquier sistema operativo y con cualquier tipo de *hardware*.

Este protocolo corresponde a una pila que es perfectamente coincidente con el modelo OSI en las capas 3 al 7, por lo que se dice que el TCP/IP es independiente del método de acceso que se use.

1.2.1 Capas del Modelo TCP/IP

Tal como se muestra en la siguiente ilustración, cada nivel del modelo TCP/IP corresponde a uno o más niveles del modelo de referencia Interconexión de sistemas abiertos OSI.

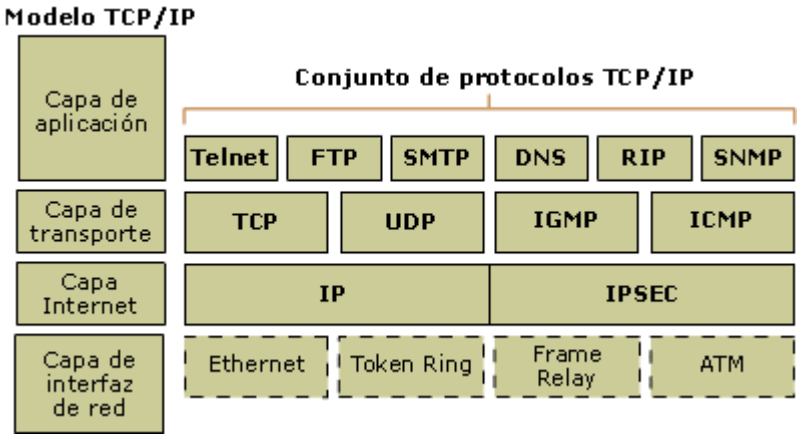


Fig. 1.2- Capas Modelo TCP/IP

Las capas que nos encontramos en el modelo TCP/IP son las siguientes:

Capa de Aplicación

En esta capa se engloban los protocolos de más alto nivel. Entre ellos se encuentran los protocolos de terminal, de transferencia de ficheros, de correo electrónico, etc. Ejemplos de protocolos que implementan las aplicaciones más conocidas son:

- NFS (Network File System) Funciona sobre UDP. Es usado en las redes locales para compartir discos en red.
- FTP: File Transfer Protocol (Protocolo de transferencia de archivos)
- HTTP: Hypertext Transfer Protocol (Protocolo de transferencia de hipertexto)
- SMTP: Simple Mail Transfer Protocol (Protocolo de transferencia de correo simple)
- DNS: Domain Name System (Sistema de nombres de dominio)
- TFTP: Trivial File Transfer Protocol (Protocolo trivial de transferencia de archivo)

Capa de Transporte

La principal tarea de la capa de transporte es proporcionar la comunicación entre un programa de aplicación y otro. Este tipo de comunicación se conoce frecuentemente como comunicación punto a punto. La capa de transporte regula el flujo de información. También, proporciona un transporte confiable, asegurando que los datos lleguen sin errores y en secuencia.

Esta capa trabaja con los siguientes protocolos:

TCP: El mejor ejemplo de este nivel es TCP, que es un protocolo orientado hacia conexión que resuelve numerosos problemas de fiabilidad para proveer una transmisión de bytes fiable, ya que se encarga de que los datos lleguen en orden, tenga un mínimo de correcciones de errores, se descarten datos duplicados, se vuelvan a enviar los paquetes perdidos o descartados e incluya control de congestión de tráfico.

UDP: Es un protocolo de datagrama sin corrección, no provee las garantías de fiabilidad y ordenamiento de TCP a los protocolos del Nivel de Aplicación y los datagramas pueden llegar en desorden o perderse sin notificación. Como consecuencia de lo anterior es que UDP es un protocolo más rápido y eficiente para tareas ligeras o sensibles al tiempo proveyendo una interfaz muy simple entre el Nivel de Red y Nivel de Aplicación.

Las aplicaciones más comunes que hacen uso de este tipo de protocolo son DNS, aplicaciones de transmisión de medios, voz sobre IP (VoIP), TFTP y juegos en línea.

Capa Internet

Esta capa tiene como objetivo enviar paquetes origen desde cualquier red en la red y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que recorrieron para llegar hasta allí. El protocolo específico que rige esta capa se denomina Protocolo Internet (IP).

En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes. Esto se puede comparar con el sistema postal. Cuando enviamos una carta por correo, no sabemos cómo llega a destino (existen varias rutas posibles); lo que nos interesa es que la carta llegue.

Capa de Acceso Red

Esta capa también se denomina capa de host a red. Es la capa que se ocupa de todos los aspectos que requiere un paquete IP para realizar realmente un enlace físico y luego realizar otro enlace físico. Esta capa incluye los detalles de tecnología LAN y WAN y todos los detalles de las capas físicas y de enlace de datos del modelo OSI.

Compuesto de protocolos como:

- Ethernet
- Wi-Fi
- Token ring
- PPP (Point-to-Point Protocol)
- SLIP (Serial Line Internet Protocol)
- FDDI (Fiber Distributed Data Interface)
- ATM (Asynchronous Transfer Protocol)
- Frame Relay
- SMDS (Switched Multi-megabit Data Services)

1.3 TIPOS DE RED

En primer lugar una red es un conjunto de dispositivos físicos "hardware" y de programas "software", mediante el cual podemos comunicar computadoras para compartir recursos (discos, impresoras, programas, etc.) así como trabajo (tiempo de cálculo, procesamiento de datos, etc.).

A cada una de las computadoras conectadas a la red se le denomina un nodo. Para transmitir información entre dos nodos cualquiera se necesita un sistema de conmutación.

1.3.1 Tipos de conmutación:

Difusión (broadcast)

Es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

Conmutación de Circuitos

El sistema telefónico plano antiguo es un típico ejemplo de éste tipo de red. Cuando el emisor marca un número, el par de hilos de cobre que lleva desde su teléfono hasta la centralita es conectado automáticamente al par que va al teléfono receptor.

Conmutación de Paquetes

El tipo de redes de comunicaciones de almacenamiento y reenvío (store-and-forward network), envía paquetes desde el origen hacia el destino. En cada nodo de cambio se encuentra un computador (halla donde varios circuitos se conectan). Los paquetes que llegan a un nodo se almacenan en la memoria del computador de ese nodo y luego son procesados por un programa que les envía hacia su destino eligiendo uno de los circuitos salientes que llevará a los paquetes a otro nodo que estará más cerca del destino que el nodo anterior.

La transmisión no es instantánea, toma pocas decenas de microsegundas hasta pocos milisegundos para encaminar los paquetes en cada nodo de la red, dependiendo del tamaño del paquete, velocidad de hardware y cantidad de tráfico. Los paquetes pueden ser encaminados hacia muchos nodos antes de que alcance su destino. Los retardos son acumulativos.

Frame Relay (o retransmisión de marcos)

Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos (“*frames*”) para datos, perfecto para la transmisión de grandes cantidades de datos.

La técnica Frame Relay se utiliza para un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un costo menor.

1.3.2 Lan (Redes Locales)

La red de área local (LAN) es aquella que se expande en un área relativamente pequeña. Comúnmente se encuentra dentro de un edificio o un conjunto de edificios contiguos. Asimismo, una LAN puede estar conectada con otras LAN a cualquier distancia por medio de una línea telefónica y ondas de radio.

Las LAN, sin embargo, no son necesariamente simples de planificar, ya que pueden unir muchos centenares de ordenadores y pueden ser usadas por muchos miles de usuarios. El desarrollo de varias normas de protocolos de red y medios físicos han hecho posible la proliferación de LAN's en grandes organizaciones multinacionales, aplicaciones industriales y educativas.

Las redes locales son capaces de transmitir datos a velocidades muy altas, algunas inclusive más rápido que por línea telefónica, pero las distancias son limitadas. Generalmente estas redes transmiten datos a 10 megabits por segundo (Mbps). En comparación, Token Ring opera a 4 y 16 Mbps, mientras que FDDI y Fast Ethernet a una velocidad de 100 Mbps o más. Cabe destacar que estas velocidades de transmisión no son caras cuando son parte de la red local.

Características principales:

- Capacidad de transmisión comprendida entre 1 Mbps y 1 Gbps.
- Incrementan la eficiencia y productividad de los trabajos de oficinas al poder compartir información.
- Las tasas de error son menores que en las redes WAN.
- Tecnología broadcast (difusión) con el medio de transmisión compartido. La simplicidad del medio de transmisión que utiliza (cable coaxial, cables telefónicos y fibra óptica).
- La facilidad con que se pueden efectuar cambios en el hardware y el software.
- Posibilidad de conexión con otras redes.

Los objetivos de este tipo de redes son:

- Asegurar la compatibilidad de productos de diferentes empresas conectados a la misma.
- Permitir la comunicación de nodos baratos y que ella también sea barata.
- Estar estructurada en niveles para que un cambio en un nivel no afecte a los demás niveles. Es decir, deben ser flexibles. La adición o supresión de nodos ha de ser fácil de llevar a cabo.
- Las características físicas deben cumplir los siguientes objetivos funcionales: Transparencia de los datos para que los niveles superiores puedan usar cualquier combinación de bits para ser enviados por la red.

1.3.3 Wan (Redes de Área Extensa)

Una Wan o red punto a punto es, como lo implica su nombre, una red que se extiende a larga distancia. Las redes extendidas son posibles gracias al extenso cableado de líneas telefónicas, torres de retransmisión de microondas y satélites que abarcan todo el globo terráqueo.

Se conoce además como un sistema de comunicación que interconecta redes computacionales (LAN) que están en distintas ubicaciones geográficas. Los enlaces atraviesan áreas públicas locales, nacionales o internacionales, usando en general como medio de transporte la red pública telefónica.

Al tener que recorrer una gran distancia sus velocidades son menores que en las LAN aunque son capaces de transportar una mayor cantidad de datos.

Las Redes de Área Extensa son mucho más complejas, porque deben enrutar correctamente toda la información proveniente de las redes conectadas a ésta.

Entre las WAN más grandes se encuentran: ARPANET, creada por la Secretaría de Defensa de los Estados Unidos y que se convirtió en lo que actualmente es la WAN mundial: Internet.

Características principales:

- Posee máquinas dedicadas a la ejecución de programas de usuario (hosts)
- Una subred, donde conectan varios hosts.
- División entre líneas de transmisión y elementos de conmutación (enrutadores)
- Usualmente los routers son computadores de las subredes que componen la WAN.

1.3.4 Man (Red de Área Metropolitana)

Otro tipo de red que se aplica en las organizaciones es la red de área metropolitana o MAN (Metropolitan Área Network), una versión más grande que la LAN y que normalmente se basa en una tecnología similar a ésta y su distancia de cobertura es mayor a 4kmts.

Puede cubrir un grupo de oficinas de una misma corporación o ciudad, esta puede ser pública o privada y no contiene elementos de conmutación, los cuales desvían los paquetes por una de varias líneas de salida potenciales.

Teóricamente, una MAN es de mayor velocidad que una LAN, pero diversas tesis señalan que se distinguen por dos tipos de red MAN. La primera de ellas se refiere alas de tipo privado, las cuales son implementadas en zonas de campus o corporaciones con edificios diseminados en un área determinada. Su estructura facilita la instalación de cableado de fibra óptica.

El segundo tipo de redes MAN se refiere a las redes públicas de baja velocidad, las cuales operan a menos de 2 Megabits por segundo en su tráfico como Frame Relay, ISDN (Integrated Services Digital Network; Red Digital de Servicios Integrados), Tl- E 1, entre otros.

Las redes de área metropolitana tienen muchas y variadas aplicaciones, las principales son:

- Interconexión de redes de área local (LAN)
- Interconexión de centralitas telefónicas digitales (PBX y PABX)
- Interconexión ordenador a ordenador
- Transmisión de video e imágenes
- Pasarelas para redes de área extensa (WAN)

1.3.5 VPN (Red Privada Virtual)

Una red privada virtual (*Virtual Private Network*) es una red privada que permite conectar diferentes puntos remotos entre si, así como equipos móviles y oficinas desde cualquier parte del mundo a través de Internet y, además, facilita el acceso a nuevas tecnologías como la Telefonía IP o el Vídeo IP.

Conectar sitios múltiples juntos sobre el Internet es generalmente menos costoso que los circuitos dedicados alquiler con opción a compra. Un riesgo al usar el Internet como medio del transporte es el riesgo de la interceptación de los datos al lado de los partidos desautorizados. Cuando los datos se mueven a través del Internet, debe ser considerado conocimiento público.

Un VPN (red privada virtual) soluciona ese problema. Un VPN es un túnel cifrado entre dos puntos finales que garantiza la confidencialidad de la información, así mismo las políticas de seguridad del sistema impedirán que personas no autorizadas tengan acceso a la VPN.

1.3.5.1 Tipos de VPN

Básicamente existen tres arquitecturas de conexión VPN:

VPN de acceso remoto

Este es quizás el modelo más usado actualmente y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones, etc.) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura "dial-up" (módems y líneas telefónicas), aunque por razones de contingencia todavía conservan sus viejos módems.

VPN sitio-a-sitio

Este esquema se utiliza para conectar oficinas remotas con la sede central de organización. El equipo central vpn, que posee un vinculo a Internet permanente, acepta las conexiones vía Internet provenientes de los sitios y establece el "túnel" vpn. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicional, sobre todo en las comunicaciones internacionales.

VPN Interna

Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red Lan (Red de área local) de la empresa.

Muchos de los ataques son ejecutados desde el interior de las corporaciones, por los que una VPN interna elimina la posibilidad de que un usuario o invitado malintencionado logre acceder al servidor principal sin tener los permisos necesarios. Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de RRHH habilitado pueda acceder a la información.

Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

1.4 RED ALÁMBRICA

Las redes alámbricas son redes cuyo medio de transmisión es a través de cables, los cuales pueden ser:

1.4.1 Cable coaxial

Se llama así porque su construcción es de forma coaxial. La construcción del cable debe ser firme y uniforme, porque si no es así, no se tiene el funcionamiento adecuado. Este conexionado está estructurado por los siguientes componentes de adentro hacia fuera de la siguiente manera:

Un núcleo de cobre sólido: o de acero con capa de cobre, o bien de una serie de fibras de alambre de cobre entrelazadas dependiendo del fabricante.

Una capa de aislante: que recubre el núcleo o conductor, generalmente de material de polivinilo, este aislante tiene la función de guardar una distancia uniforme del conductor con el exterior.

Una capa de blindaje metálico: generalmente cobre o aleación de aluminio entretejido cuya función es la de mantenerse lo mas apretado posible para eliminar las interferencias.

Por último, tiene una capa final de recubrimiento, de color negro en caso del cable coaxial delgado o amarillo en el caso del cable coaxial grueso, este recubrimiento normalmente suele ser de vinilo, xelón o polietileno uniforme para mantener la calidad de las señales.

1.4.2 Cable Par trenzado

Es de los más antiguos en el mercado y en algunos tipos de aplicaciones es el más común. Consiste en dos alambres de cobre o a veces de aluminio, aislados con un grosor de 1mm aproximadamente. Los alambres se trenzan con el propósito de reducir la interferencia eléctrica de pares similares cercanos. Los pares trenzados se agrupan bajo una cubierta común de PVC (Policloruro de Vinilo) en cables multipares de pares trenzados (de 2, 4, 8, hasta 300 pares).

Un ejemplo de par trenzado es el sistema de telefonía, ya que la mayoría de aparatos se conectan a al central telefónica por medio de un par trenzado. Actualmente, se han convertido en un estándar en el ámbito de las redes LAN como medio de transmisión en las redes de acceso a usuarios. A pesar que las propiedades de transmisión de cables de par trenzado son inferiores, y en especial la sensibilidad ante perturbaciones extremas, a las del cable coaxial, su gran adopción se debe al costo, su flexibilidad y facilidad de instalación, así como las mejoras tecnológicas constantes introducidas en enlaces de mayor velocidad, longitud, etc.

El cable Par trenzado tiene dos categorías:

- Apantallado
- No Apantallado

1.4.3 Fibra Óptica

Son filamentos de vidrio (compuestos de cristales naturales) o plástico (cristales artificiales), del espesor de un pelo (entre 10 y 300 micrones). Llevan mensajes en forma de haces de luz que realmente pasan a través de ellos de un extremo a otro, donde quiera que el filamento vaya (incluyendo curvas y esquinas) sin interrupción.

Las fibras ópticas se caracterizan por una pérdida de transmisión realmente bajas, una capacidad extremadamente elevada de transporte de señales, dimensiones mucho menores que los sistemas convencionales, instalación de repetidoras a lo largo de las líneas, una mayor resistencia frente a interferencias, etc.

El cable de fibra óptica se divide en tres categorías:

- Monomodo
- Multimodo
- Multimodo graduado

1.4.4 Protocolos

Los protocolos de red son normas que permiten a los ordenadores comunicarse. Un protocolo define la forma en que los ordenadores deben identificarse entre si en una red, la forma en que los datos deben transitar por la red, y cómo esta información debe procesarse una vez que alcanza su destino final.

Aunque cada protocolo de la red es diferente, todos pueden compartir el mismo cableado físico. Este concepto es conocido como "independencia de protocolos," lo que significa que dispositivos que son compatibles en las capas de los niveles físicos y de datos permiten al usuario ejecutar muchos protocolos diferentes sobre el mismo medio físico.

Actualmente, los protocolos más comúnmente utilizados en las redes son: Ethernet, Token Ring y ARCNET. Cada uno de estos esta diseñado para cierta clase de topología de red y tienen ciertas características estándar.

1.4.4.1 Ethernet

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

Es, sin lugar a dudas, la tecnología más extendida y de mayor difusión en todo el mundo para la implementación de redes de área local. Actualmente es el protocolo más sencillo y es de bajo costo. Utiliza la topología de "Bus" lineal.

Fue diseñado originalmente por Digital, Intel y Xerox por lo cual, la especificación original se conoce como Ethernet DIX. Posteriormente en 1.983, fue formalizada por el IEEE como el estándar Ethernet 802.3.

A partir de 2001 Ethernet alcanzó los 10 Gbps lo que dio mucha más popularidad a la tecnología. Dentro del sector se planteaba a ATM como la total encargada de los niveles superiores de la red, pero el estándar 802.3ae (Ethernet Gigabit 10) se ha situado en una buena posición para extenderse al nivel WAN.

En el apartado 1.6 de este capitulo se menciona en mas detalle este tema, en donde se describe su estructura y las características que definen su funcionamiento.

1.4.4.2 Token Ring

El protocolo de red IBM es el Token ring o estándar IEEE 802.5, el cual se basa en la topología de anillo. Se distingue más por su método de transmitir la información que por la forma en que se conectan las computadoras.

Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación del anillo. No hay una computadora host central que guarde todos los datos. Las comunicaciones fluyen en una sola dirección alrededor del anillo. En esta topología los datos se distribuyen con un orden preestablecido.

Los datos en Token-Ring se transmiten a *4 ó 16Mbps*, depende de la implementación que se haga. Todas las estaciones se deben de configurar con la misma velocidad para que funcione la red. Cada computadora se conecta a través de cable Par Trenzado ya sea blindado o no a un concentrador llamado MAU (Media Access Unit/Unidad de acceso Multiestación), y aunque la red queda físicamente en forma de estrella, lógicamente funciona en forma de anillo por el cual da vueltas el Token. En realidad el MAU es el que contiene internamente el anillo y si falla una conexión automáticamente la ignora para mantener cerrado el anillo.

La MAU es un concentrador de dispositivos en estrella. La MAU permite establecer la topología física en estrella a partir del anillo lógico.

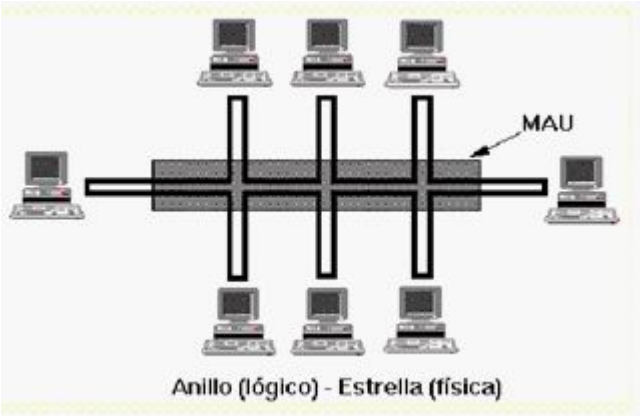


Fig. 1.3- Topología Token Ring

Funcionamiento:

Token Ring esta basado en una teoría MAC (media access control) denominada Token Passing -paso de testigo-.

- *Token Passing* es el método utilizado por Token Ring para acceder al medio físico. Sirve para determinar que nodo en el anillo puede transmitir frames (tramas) en determinado momento.

La idea básica del protocolo es muy simple, cuando un nodo tiene datos para transmitir debe apropiarse de un token libre (debe pedir la palabra). La apropiación se hace modificando un bit en el segundo byte del token.

El *token* es un patrón especial de bits (un frame "pequeño") usado para acceder al anillo. Su formato consta de tres bytes:

- **Delimitador de inicio (SDEL)**: 8 bits (1 byte) que informan donde comienza el frame de token
- **Control de acceso (AC)**: 8 bits (1 byte), sirve como método de control para ganar el acceso a la red. (tres bits indican la prioridad, tres se utilizan para reservación, uno es el "token bit" y otro es el "monitor bit")

- **Delimitador de finalización (EDEL)**: 8 bits (1 byte), informan donde termina el frame de token.

Si un nodo no tiene información para transmitir, debe pasar el token a la siguiente estación. El nodo que "tenga" el token puede transmitir frames (puede hablar). Los nodos pueden apropiarse del token por un tiempo máximo.

Mientras el token esté siendo "ocupado", las otras estaciones deben permanecer inactivas para evitar colisiones dentro de la red (deben permanecer en silencio mientras quien tiene la palabra habla).

Una vez terminada la transmisión, el token vuelve a quedar libre y puede ser utilizado por otra estación (cede la palabra a quien quiera hablar).

Mientras el frame esté moviéndose en la red, no habrá token en la red. El frame circula en la red hasta que llegue a la estación destino, quien hace una copia del contenido del frame para pasarlo a las capas superiores, pero no retira el frame de la red.

El frame sigue en la red hasta que regrese a la estación que lo transmitió para que ella misma lo retire de la red.

Token ring es una red determinística: es posible calcular exactamente el máximo tiempo que transcurrirá antes que otra estación vuelva a transmitir.

Token ring es ideal para aplicaciones donde el retardo (delay) deba predecirse con exactitud (por ejemplo, ambientes de automatización de fabricas).

Características:

- Topología: anillo lógico, estrella física.
- Toda la información viaja en una sola dirección a lo largo del círculo formado por el anillo.

- El anillo no representa un medio de difusión sino que una colección de enlaces punto a puntos individuales.
- Cada estación se conecta a otras.
- Cada nodo siempre pasa el mensaje, si este mensaje es para él, entonces lo copia y lo vuelve a enviar.
- Número máximo de nodos por red 260.
- El arreglo tiene un bit de verificación, a simple vista, este mecanismo podría parecer menos fuerte que el mecanismo usado para la topología en caso de fallas.
- En la implementación es posible diseñar anillos que permitan saltar a un nodo que este fallando.
- Resultan más caras que las ethernet, pero son más estables.

Ventajas:

- No requiere de enrutamiento.
- Requiere poca cantidad de cable.
- Fácil de extender su longitud, ya que el nodo esta diseñado como repetidor, por lo que permite amplificar la señal y mandarla mas lejos.

Desventajas:

- Altamente susceptible a fallas.
- Una falla en un nodo deshabilita toda la red (esto hablando estrictamente en el concepto puro de lo que es una topología de anillo).
- El software de cada nodo es mucho más complejo

1.4.4.3 Arcnet

Es conocida como un arreglo de redes estrella, es decir una serie de redes estrella que se comunican entre sí, cada una de las estaciones de trabajo de este tipo de red pueden estar conectadas a una distancia máxima de 1200 metros con respecto al servidor de la red, esta distancia equivale a casi el triple de la permitida por la red tipo estrella

Las estaciones ArcNet utilizan un esquema de pase por testigo para acceder a la red. Sin embargo, el testigo no circula en un anillo físico, sino lógico. Cada estación tiene asignado un número y el testigo pasa a cada estación en el orden numérico correcto, aunque las estaciones no estén conectadas en ese orden

Debido a que tiene un costo bajo y es muy fácil de instalar es el hardware de red más utilizado en redes pequeñas, aunque cada vez se usa menos. Sin embargo, por su velocidad y las distancias que soporta, es ideal para redes medias.

Aunque existe una versión de esta red que utiliza topología bus, la más conocida utiliza topología de estrella distribuida. Soporta una velocidad de 2.5 Mbit/s suficiente para redes de tamaño medio.

Funcionamiento:

El funcionamiento de esta red se basa en unos módulos denominados RIM (Resource Interface Module, módulo interfase de dispositivo) que controlan la actividad de la red, liberando de esta tarea a los demás dispositivos conectados. Los RIM están formados por cuatro componentes básicos:

- Un controlador que contiene básicamente un chip y memoria RAM
- Un reloj que sincroniza las operaciones.
- Una interfase de enlace que conecta el controlador con la línea de transmisión.
- Una interfase con el procesador, que contiene los controladores del bus y los decodificadores de direcciones.

Las estaciones están conectadas por medio de un cable coaxial, a un RIM, el cual esta conectado a un puerto a través de un HUB, este hace las veces de amplificador de señal.

Características principales:

- Velocidad máxima de transmisión: 2.5 Mbps.
- Medios de transmisión soportados:
  Cable coaxial (configuración en estrella)
  Cable coaxial (configuración en bus)
- Topología en estrella. También es posible la topología en bus. Emplean el mismo tipo de cableado y resulta muy sencillo la combinación de ambas topologías en una sola red.
- Es la red con el hardware más barato.
- Esquema de acceso al medio: “Token Passing”
- Número máximo de nodos en la red: 255
- Los adaptadores de red son RIM (*Resource Interface Module***).**

1.4.5 Topología

La topología o forma lógica de una red se define como la forma de tender el cable a estaciones de trabajo individuales; por muros, suelos y techos del edificio. Existe un número de factores a considerar para determinar cual topología es la más apropiada para una situación dada.

1.4.5.1 Anillo

Consiste de un cable que interconecta los nodos formando un anillo o circulo. La señal viaja en una dirección y no requiere de terminadores ya que los nodos son los encargados de depurar la información que viaja en el cable.

El acceso al medio de la red es otorgado a una computadora en particular en la red por un "token".

El término de “token” se explica con más detalle en el apartado anterior, en donde se describe el funcionamiento de la red Token Ring.

Fig. 1.4- Topología anillo

Ventajas:

- Es posible realizar el enlace mediante fibra óptica por sus características de unidireccionalidad, con las ventajas de su alta velocidad y fiabilidad.

Desventajas:

- Si se rompe una conexión, se cae la red completa
- Es difícil localizar los fallos
- La reconfiguración de la red es complicada, puesto que incluir un ordenador màs en la red implica variar el nodo anterior y posterior de varios nodos de la red.

1.4.5.2 Estrella

La red se une en un único punto, normalmente, se compone de un dispositivo central (el hub) o a un conmutador de paquetes (swicth en inglés) y un conjunto de terminales o computadoras conectadas. En una red en estrella, los mensajes pasan directamente desde un nodo al dispositivo central, el cual gestiona la redistribución de la información a los demás nodos.

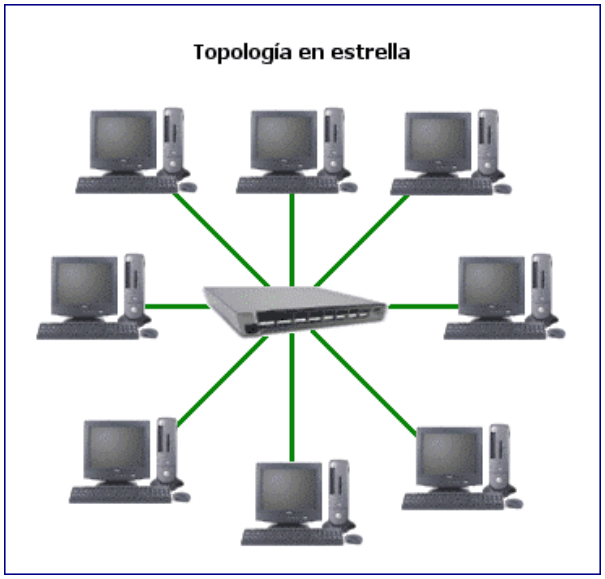


Fig. 1.5- Topología estrella

Ventajas:

- El fallo de un nodo no causa problemas de funcionamiento al resto de la red.
- La detección y localización de averías es sencilla.
- Es posible conectar terminales no inteligentes, ya que el nodo central tiene capacidad de proceso.

Desventajas:

- La avería del nodo central supone la inutilización de la red.
- Se necesitan longitudes grandes de cableado, ya que dos estaciones cercanas entre sí, pero distantes del nodo centra, requieren cada una un cable que las una a éste.
- Poseen limitaciones en cuanto a expansión (incremento de nodos), dado que cada canal requiere una línea y una interfaz al nodo principal.
- La carga de red es muy elevada en el nodo central, por lo cual éste no se puede utilizar más que como servidor o controlador.
- No soporta cargas de tráfico elevadas por sobrecarga del nodo central.

1.4.5.3 Bus

La topología de bus tiene todos sus nodos conectados directamente a un cable central, llamado el bus o *backbone* y no tiene ninguna otra conexión entre nodos.

Los nodos en una red de "bus" transmiten la información y esperan que ésta no vaya a chocar con otra información transmitida por otro de los nodos. Si esto ocurre, cada nodo espera una pequeña cantidad de tiempo al azar, después intenta retransmitir la información.

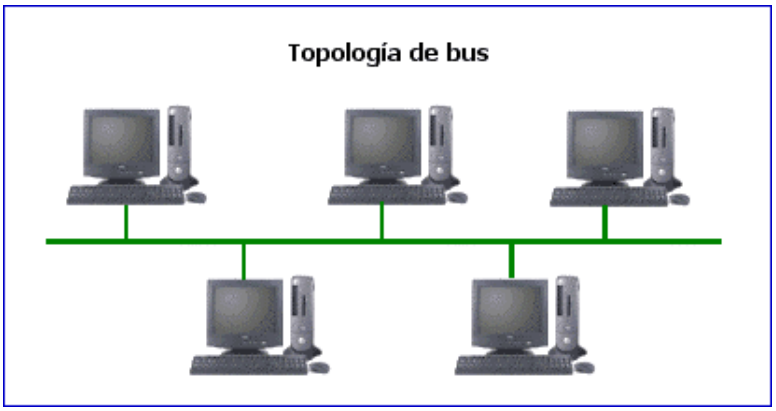


Fig. 1.6- Topología bus

Ventajas:

- Simplicidad en el cableado, ya que no se acumulan montones de cables en torno al nodo.
- Hay una gran facilidad de ampliación, y se pueden agregar fácilmente nuevas estaciones o ampliar la red añadiendo una nueva línea conectada mediante un repetidor.
- Existe una interconexión total entre los equipos que integran la LAN.

Desventajas:

- Un fallo en una parte del cableado detendría el sistema, total o parcialmente, en función del lugar en que se produzca. Además, es muy difícil localizar las averías en esta topología. Sin embargo, una vez localizado el fallo, al desconectar de la red la parte averiada ya no interferiría en la instalación.

- Todos los nodos han de ser inteligentes, ya que han de manejar el medio de comunicación compartido.
- Debido a que la información recorre el bus bidireccionalmente hasta encontrar su destino, la posibilidad de que sea interceptada por usuarios no autorizados es superior a la existente en una red de estrella.

1.4.5.4 Híbridas

Las redes híbridas usan una combinación de dos o más topologías distintas de tal manera que la red resultante no tiene forma estándar.

Anillo en estrella

En esta topología los equipos están conectados a un componente central al igual que en una red en estrella. Sin embargo, estos componentes están enlazados para formar una red en anillo.

Esta topología se utiliza con el fin de facilitar la administración de la red.

"Bus" en estrella

Es una variante de la topología en bus. En este caso la red es un "bus" que se cablea físicamente como una estrella por medio de concentradores.

Tiene una gran facilidad de expansión, siendo la colocación de nuevos nodos o ramas sencilla. Además, la detección de problemas es relativamente sencilla, ya que se pueden desconectar estaciones o ramas completas hasta localizar la avería.

Sin embargo, existe una dependencia a la línea principal, y los fallos en una rama provocan la caída de todos los nodos que cuelgan de la rama o subrayas.

1.5 REDES INALÁMBRICAS

Las redes inalámbricas son redes cuyos medios físicos no son cables de cobre de ningún tipo. Están basadas en la transmisión de datos mediante ondas de radio, microondas, satélites o infrarrojos.

Al igual que las redes tradicionales cableadas se clasifican en tres categorías:

- WAN/MAN
- LAN
- PAN

En los siguientes ítems de este apartado se acotará el tema solo para redes de área local (LAN).

1.5.1 Wlan

Una red de área local inalámbrica (WLAN) es un sistema de comunicación de datos flexible que puede reemplazar o extender una red de área local cableada (LAN) para ofrecer funcionalidad adicional.

Como mínimo, el punto de acceso recibe, almacena y transmite los datos entre la red inalámbrica y la red alambrada. Uno de estos dispositivos puede soportar un grupo pequeño de usuarios (hasta 30 por punto de acceso) dentro de un rango promedio de 30 a 100 metros.

Los usuarios finales acceden a la red a través de adaptadores inalámbricos, implementados en tarjetas PC para computadoras portátiles (Laptops), adaptadores ISA o PCI para computadoras de escritorio (Desktops) o mediante adaptadores totalmente integrados en asistentes personales digitales (PDA, por las siglas de Personal Digital Assistant). Los adaptadores WLAN proporcionan la interfaz entre el sistema operativo de red del cliente y las ondas electromagnéticas por conducto de la antena.

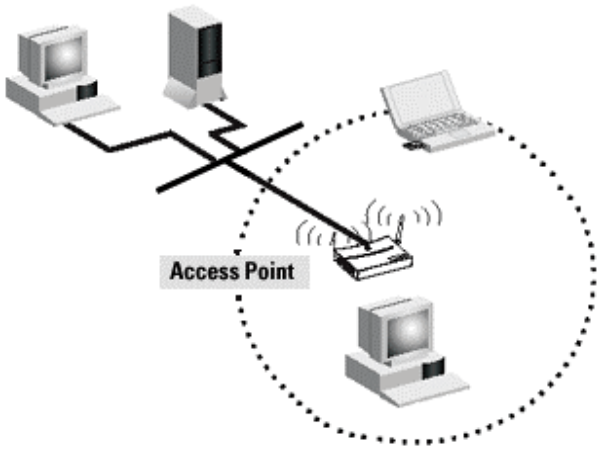


Fig. 1.7- Red Inalámbrica Wlan

Los sistemas WLAN utilizan para su funcionamiento las siguientes bandas de frecuencia:

- 902-928 Mhz
- 2.400-2.483 Ghz
- 5725-5850 Ghz

Estas bandas de frecuencia, llamadas bandas ISM, estaban anteriormente limitadas a instrumentos científicos, médicos e industriales. Esta banda, a diferencia de la ARDIS y MOBITEX, está abierta para cualquiera y se pueden usar libremente.

Ventajas y Desventajas:

Las principales ventajas que presentan las redes WLAN son su libertad de movimientos, sencillez en la reubicación de terminales y la rapidez consecuente de instalación. La solución inalámbrica resuelve la instalación de una red en aquellos lugares donde el cableado resulta inviable, por ejemplo en edificios históricos o en grandes naves industriales, donde la realización de canaletas para cableado podría dificultar el paso de transportes, así como en situaciones que impliquen una gran movilidad de los terminales del usuario o la necesidad de disponer de vías alternativas por motivos de seguridad.

Los inconvenientes que tienen las redes de este tipo se derivan fundamentalmente de encontrarnos en un periodo transitorio de introducción, donde faltan estándares, hay dudas que algunos sistemas pueden llegar a afectar a la salud de los usuarios, no está clara la obtención de licencias para las que utilizan el espectro radioeléctrico y son muy pocas las que presentan compatibilidad con los estándares de las redes fijas.

El costo de instalación y mantenimiento de una WLAN es generalmente menor al correspondiente a una LAN alámbrica, por dos razones:

- Elimina el costo generado por el tendido del cableado y las actividades asociadas de mantenimiento y reparación.
- Simplifica movimientos de la infraestructura, crecimientos y cambios, por consiguiente, disminuye los costos generados durante estas actividades.

1.5.2 Estándar Wlan IEEE 802.11

La promoción de normas que regula la operación de la red de área local inalámbrica se inició con el estándar 802.11, desarrollado en 1997 por el Instituto de Instituto de Ingeniería Eléctrica y Electrónica (IEEE). Este estándar base permitió la transmisión de datos hasta 2 Mbps. Con el pasar del tiempo, dicho estándar fue ampliado, a través de extensiones las cuales son reconocidas por la incorporación de una carta al estándar 802.11 original, incluyendo el 802.11a y el 802.11b.

El estándar IEEE 802.1 1 extiende el principio del acceso múltiple sensible a la portadora (CSMA) utilizado por la tecnología Ethernet (IEEE 802.3) para adecuarse a las características de la comunicación sin hilos.

1.5.2.1 Estándares del 802.11

802.11 Estándar WLAN original. Soporta de 1 Mbps a 2 Mbps.

802.11a Estándar WLAN de alta velocidad para banda de 5 Ghz. Soporta 54 Mbps.

802.11b Estándar WLAN para banda de 2.4 Ghz. Soporta 11 Mbps.

802.11e Dirige los requerimientos de calidad de servicio para todas las interfaces de radio WLAN del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE).

802.11f Define la comunicación del punto de inter-acceso para facilitar las múltiples redes WLAN distribuidas por los diferentes fabricantes.

802.11g Establece una técnica de modulación adicional para banda de 2.4 Ghz. Propuesta para ofrecer velocidades hasta 54 Mbps.

802.11h Define el manejo de espectro de banda de 5 Ghz para uso en Europa y en Asia Pacífica.

802.11i Dirige las actuales debilidades de seguridad para los protocolos de autenticación y encriptación. El estándar comprende los protocolos 802.1X, TKIP y AES.

Características del 802.11b

La 802.11b utiliza la misma frecuencia de radio que el tradicional 802.11 (2.4Ghz). El problema es que al ser ésta una frecuencia sin regulación, se podían causar interferencias con hornos microondas, teléfonos móviles y otros aparatos que funcionan en la misma frecuencia. Sin embargo, si las instalaciones 802.11b están a una distancia razonable de otros elementos, estas interferencias son fácilmente evitables. Además, los fabricantes prefieren bajar el coste de sus productos, aunque esto suponga utilizar una frecuencia sin regulación. En espacios abiertos los alcances pueden llegar a 120 m (a 11 Mbit/s) y 460 m (a 1 Mbit/s).

La técnica de modulación empleada es CCK (Complementary Code Keying), codificando cada símbolo con 4 bits a velocidades de 1,375 MBd. Dado que CCK es una técnica DSSS, existe compatibilidad con los productos 802.11 originales simplemente reduciendo las velocidades de funcionamiento a 1 ó 2 Mbit/s. Posteriormente, un segundo esquema de codificación llamado PBCC (Packet Binary Convolutional Code) fue incluido para mejorar el alcance en el caso de tasas de 5,5 y 11 Mbit/s, ya que proporciona una ganancia de codificación de 3 Db.

Ventajas:

- Bajo costo.
- Rango de señal muy bueno y difícil de obstruir.

Desventajas:

- Baja velocidad máxima.
- Soporte de un número bajo de usuarios a la vez.
- Produce interferencias en la banda de 2.4GHz.

Características del 802.11g

Entre 2002 y 2003 ha aparecido un nuevo estándar denominado 802.11g. Este nuevo estándar intenta aprovechar lo bueno de cada uno de los estándar 802.11a y 802.11b. La 802.11g permite velocidades de hasta 54 Mbps y utiliza la banda de frecuencia de 2.4Ghz.

Además, al trabajar en la misma frecuencia, la 802.11g es compatible con la 802.11b, por lo que puntos de acceso 802.11g pueden trabajar en redes 802.11b y viceversa.

Este estándar utiliza tecnología OFDM, implementando al mismo tiempo las modalidades 802.11b y, de manera opcional, CCK-OFDM y PBCC-22.

Ventajas:

- Velocidad máxima alta.
- Soporte de muchos usuarios a la vez.
- Rango de señal muy bueno y difícil de obstruir.

Desventajas:

- Alto costo.
- Produce interferencias en la banda de 2.4GHz.

1.5.2.2 Técnicas de Transmisión

Existen dos técnicas para distribuir la señal convencional en un espectro de propagación equivalente (espectro ensanchado).

DSSST: Tecnología de espectro ensanchado de secuencia directa

Técnica en donde la portadora está modulada por un código de dispersión de alta velocidad y una corriente de datos de información. La secuencia del código de alta velocidad es el causante directo del ensanchamiento de la señal transmitida y reduce la densidad de potencia espectral (es decir, el nivel de potencia en cualquier frecuencia dada).

En este método el flujo de bits de entrada se multiplica por una señal de frecuencia mayor, basada en una función de propagación determinada. El flujo de datos original puede ser entonces recobrado en el extremo receptor correlacionándolo con la función de propagación conocida. Este método requiere un procesador de señal digital para correlacionar la señal de entrada.

La señal resultante tiene un espectro muy parecido al del ruido, de tal forma que a todos los radiorreceptores les parecerá ruido menos al que va dirigida la señal.

El estándar IEEE 802.11 ha definido dos tipos de modulación para la técnica de espectro ensanchado por secuencia directa (DSSS), la modulación DBPSK (Differential Binary Phase Shift Keying) y la modulación DQPSK (Differential Quadrature Phase Shift Keying), que proporcionan una velocidad de transferencia de 1 y 2 Mbps respectivamente. La técnica de DSSS podría compararse con una multiplexación en frecuencia.

FHSST: Tecnología de espectro ensanchado de saltos de frecuencia

La tecnología de espectro ensanchado por salto en frecuencia (FHSS) consiste en transmitir una parte de la información en una determinada frecuencia durante un intervalo de tiempo llamada dwell time e inferior a 400 ms. Pasado este tiempo se cambia la frecuencia de emisión y se sigue transmitiendo a otra frecuencia. De esta manera cada tramo de información se va transmitiendo en una frecuencia distinta durante un intervalo muy corto de tiempo.

El número de saltos por segundo es regulado por cada país, así, por ejemplo, Estados Unidos fija una tasa mínima de saltas de 2.5 por segundo.

La portadora está modulada por información codificada convencionalmente, originando una dispersión convencional de la energía de RF alrededor de la misma. La frecuencia de la portadora no es constante, sino que varia a intervalos fijos controlada por la secuencia de codificación.

Este método es una técnica en la cual los dispositivos receptores y emisores se mueven sincrónicamente en un patrón determinado de una frecuencia a otra, brincando ambos al mismo tiempo y en la misma frecuencia predeterminada. Como en el método de secuencia directa, los datos deben ser reconstruidos en base del patrón de salto de frecuencia. Este método es viable para las redes inalámbricas, pero la asignación actual de las bandas ISM no es adecuada, debido a la competencia con otros dispositivos, como por ejemplo las bandas de 2.4 y 5.8 Mhz que son utilizadas por hornos de Microondas.

El estándar IEEE 802.11 define la modulación aplicable en este caso. Se utiliza la modulación en frecuencia FSK (Frequency Shift Keying), con una velocidad de 1Mbps ampliable a 2Mbps. La técnica FHSS seria equivalente a una multiplexación en frecuencia.

1.5.3 Topología

Existen dos métodos de comunicación vía inalámbrica, los cuales son:

1.5.3.1 Modo Ad Hoc

También denominadas WLANs independientes, es el medio de comunicación por el cual uno se conecta a otro dispositivo suponiendo crear una red imaginaria entre dos equipos de cómputo, no existe un punto de acceso y la comunicación es uno a uno “Peer to Peer”.

La configuración más simple de una WLAN conecta un conjunto de PCs con adaptadores inalámbricos. Cuando dos o más de estos equipos están dentro del rango de alcance de sus adaptadores pueden establecer una red independiente. Estas redes generalmente no requieren administración o preconfiguración alguna.

Esta topología es práctica en lugares en los que pueden reunirse pequeños grupos de equipos que no necesitan acceso a otra red. Ejemplos de entornos en los que podrían utilizarse redes inalámbricas ad hoc serían un domicilio sin red con cable o una sala de conferencias donde los equipos se reúnen con regularidad para intercambiar ideas.

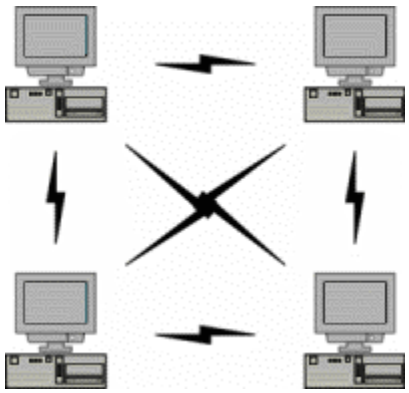


Fig. 1.8- Topología modo Ad Hoc

Funcionamiento:

En esta red sólo hay dispositivos inalámbricos presentes. Muchas de las operaciones que controlaba el punto de acceso, como la señalización y la sincronización, son controladas por una estación. La red ad hoc no disfruta todavía de algunos avances como retransmitir tramas entre dos estaciones que no se oyen mutuamente.

1.5.3.2 Modo Infraestructura

En este modo, cada cliente wireless envía su información a un Punto de Acceso, que la hace llegar al destino adecuado.

Los Puntos de Acceso permiten aumentar la cobertura de la red wireless, dado que los equipos clientes se comunican con él y no directamente entre sí, y por su condición de equipos fijos ubicados en zonas estratégicas y con antenas de más calidad, ofrecen una mayor cobertura y mejor fiabilidad del enlace. Además, existe la posibilidad de instalar varios Puntos de Acceso que actúen como repetidores para cubrir áreas mayores permitiendo el roaming de usuarios entre ellos.

Los Puntos de acceso actúan normalmente como bridge entre la red cableada y la red inalámbrica, lo que permite el acceso de los clientes wireless a los servicios de la red, aunque también pueden ofrecer servicios más avanzados, como servidores DHCP, asi como la posibilidad del empleo de herramientas de seguridad y control de acceso a la red wireless.

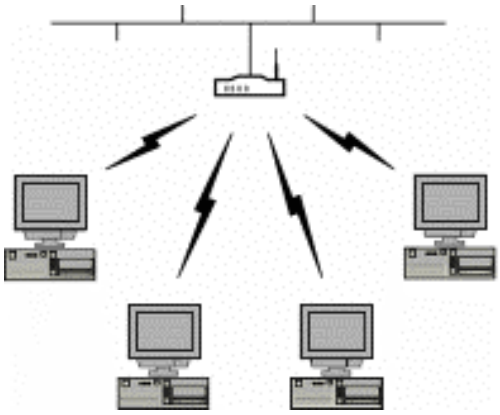


Fig. 1.9- Topología modo Infraestructura

Funcionamiento:

El portátil o dispositivo inteligente, denominado "estación" en el ámbito de las redes LAN inalámbricas, primero debe identificar los puntos de acceso y las redes disponibles. Este proceso se lleva a cabo mediante el control de las tramas de señalización procedentes de los puntos de acceso que se anuncian a sí mismos o mediante el sondeo activo de una red específica con tramas de sondeo.

La estación elige una red entre las que están disponibles e inicia un proceso de autenticación con el punto de acceso. Una vez que el punto de acceso y la estación se han verificado mutuamente, comienza el proceso de asociación.

La asociación permite que el punto de acceso y la estación intercambien información y datos de capacidad. El punto de acceso puede utilizar esta información y compartirla con otros puntos de acceso de la red para diseminar la información de la ubicación actual de la estación en la red.

El acceso a la red se administra mediante un protocolo que detecta las portadoras y evita las colisiones. Las estaciones se mantienen a la escucha de las transmisiones de datos durante un período de tiempo especificado antes de intentar transmitir (ésta es la parte del protocolo que detecta las portadoras). Antes de transmitir, la estación debe esperar durante un período de tiempo específico después de que la red está despejada.

Esta demora, junto con la transmisión por parte de la estación receptora de una confirmación de recepción correcta, representa la parte del protocolo que evita las colisiones. Observar que, en la modalidad de infraestructura, el emisor o el receptor es siempre el punto de acceso.

Dado que es posible que algunas estaciones no se escuchen mutuamente, aunque ambas estén dentro del alcance del punto de acceso, se toman medidas especiales para evitar las colisiones. Entre ellas, se incluye una clase de intercambio de reserva que puede tener lugar antes de transmitir un paquete mediante un intercambio de tramas "petición para emitir" y "listo para emitir", y un vector de asignación de red que se mantiene en cada estación de la red. Incluso aunque una estación no pueda oír la transmisión de la otra estación, oirá la transmisión de "listo para emitir" desde el punto de acceso y puede evitar transmitir durante ese intervalo.

La sincronización entre las estaciones de la red se controla mediante las tramas de señalización periódicas enviadas por el punto de acceso. Estas tramas contienen el valor de reloj del punto de acceso en el momento de la transmisión, por lo que sirve para comprobar la evolución en la estación receptora. La sincronización es necesaria por varias razones relacionadas con los protocolos y esquemas de modulación de las conexiones inalámbricas.

1.5.4 Seguridad de una Red

1.5.4.1 Seguridad Red WiFi

Las redes WiFi pueden ser abiertas o cerradas. En una red abierta, cualquier ordenador cercano al punto de acceso puede conectarse a Internet a través de él, siempre que tenga una tarjeta WiFi incorporada, claro. En la red cerrada el ordenador detectará una red inalámbrica cercana disponible, pero para acceder habrá que introducir la contraseña.

Es más complicado, en las redes cableadas, conectarse de forma ilegítima, habría que conectarse físicamente mediante un cable. Sin embargo en las redes inalámbricas donde la comunicación se realiza mediante ondas de radio, esta tarea resulta más sencilla. Para poder proteger una red WiFi se tiene que acceder a la configuración del Router o Punto de Acceso inalámbrico, además de configurar Windows o el Software correspondiente. A continuación se indican los métodos para proteger una red WiFi:

Cambiar la contraseña de administrador

Los routers wifi se configuran con un sencillo menú al que se llega abriendo una página web. Aquí hay que introducir la contraseña que indica el fabricante para poder entrar. La contraseña viene en los manuales de instrucciones de los routers, por lo que es muy importante no perderlos, aunque a priori parezca que el usuario no tiene nada que operar sobre el router.

Por desgracia, cualquier persona con unos mínimos conocimientos puede hacer lo mismo y configurar el router a su antojo. Un simple cambio de contraseña es una medida importante de protección.

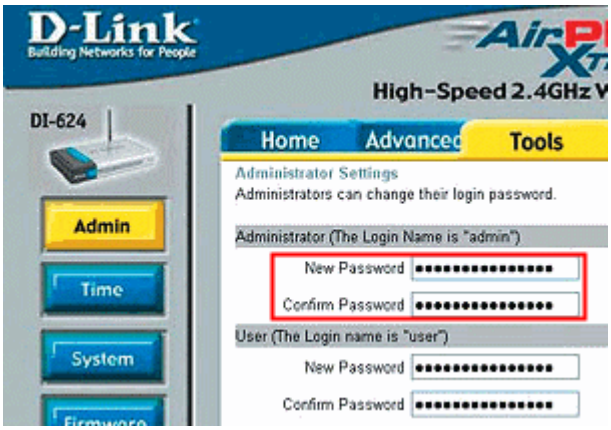


Fig. 1.10- Ventana para cambiar contraseña

Conviene, no obstante, elegir bien la contraseña. Las palabras completas como 'Alberto' o 'ferrocarril' pueden descubrirse por medio de fuerza bruta (prueba y error). Las palabras combinadas en código alfanumérico, con números como 'anto69mired' son más seguras

Modificar el SSID

El SSID es el nombre de la red y si alguien la conoce, es más sencillo descubrirla y conectarse a ella. Los fabricantes normalmente comercializan sus Routers inalámbricos con el mismos SSID genérico, de esta forma los intrusos pueden adivinar fácilmente cual es el nombre y registrarse. Por lo tanto, hay que escoger un nombre con el que se denominará la red.

Desactivar el broadcasting SSID

Otro método que no es 100% seguro pero ayuda a mantener segura una red es desactivar la difusión (o broadcast) del SSID. Así, los intrusos verían que la red no está en uso. Sin embargo, no es un método muy confiable debido a que hay ocasiones aún con el SSID desactivado en que ciertas conexiones, específicamente intentos de acceso a la red, difunden el SSID en marcos de respuesta a la conexión.

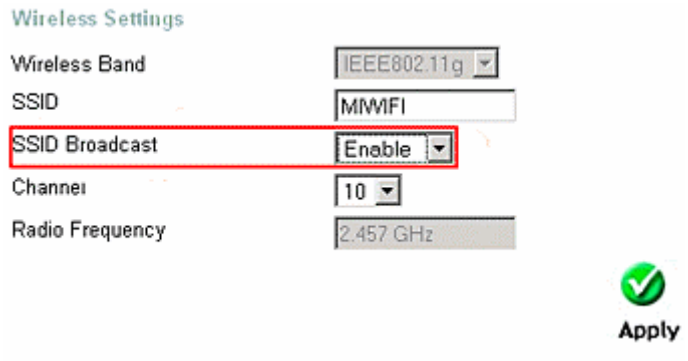


Fig. 1.11- Ventana para desactivar el SSID

Encriptación WEP/WPA

WEP (*Wired Equivalent Privacy),* es la màs conocida y usada, utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red. Esto genera varios inconvenientes. Por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

Se basa en claves de 64 ó 128 bits, hay casos en que fabricantes ofrecen cifrados de 40 bits y de 104 bits.

WAP *(WiFi Protected Access)*, surgió como alternativa segura y eficaz al WEP. Sus principales características son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

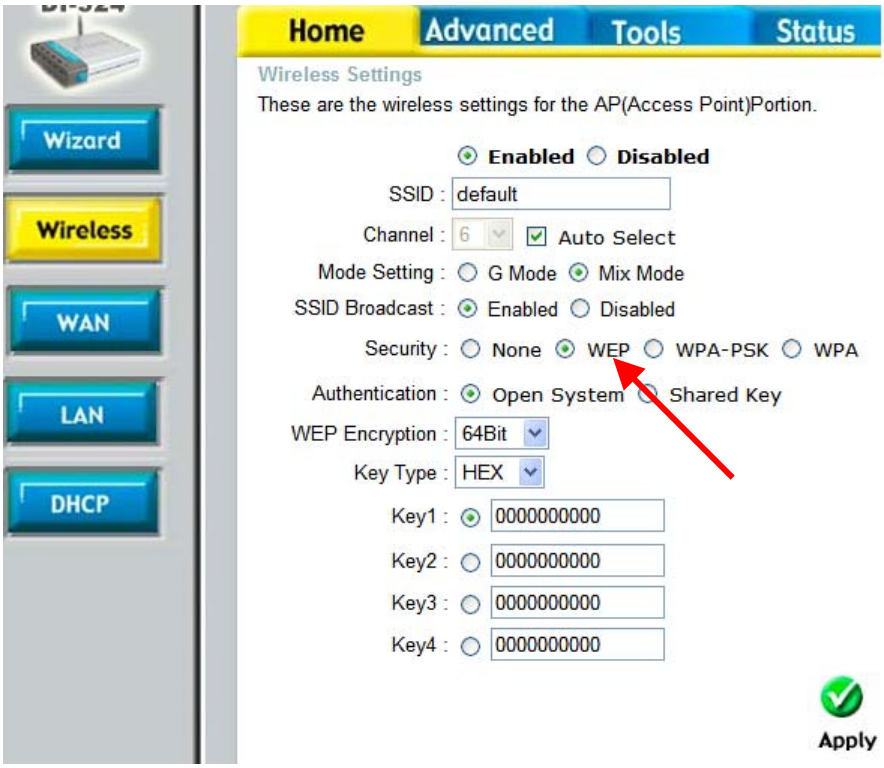


Fig. 1.12- Ventana para elegir tipo de encriptación

Filtrado de dirección MAC

MAC (Media Access Control) es un número identificador de 48 bits que se le otorga a cada tarjeta o interfaz de red, router inalámbrico u otro dispositivo con capacidad para conexión de red.

El filtrado de direcciones MAC es una técnica desarrollada para que en una red inalámbrica solo se puedan conectar aquellas tarjetas de red y/o dispositivos que posean las direcciones MAC que el usuario programó para conectarse a través de la puerta de enlace, impidiendo que otros dispositivos que no se hayan programado puedan entrar.

Últimamente recientes muestras por expertos han demostrado que este no es un método efectivo debido a que:

- Los usuarios deben ingresarse de forma manual
- Las direcciones de los usuarios se deben actualizar con frecuencia
- Se puede realizar una captura de una dirección MAC de un equipo de la red dando acceso libre a la red a intrusos, los cuales pueden hacer que una dirección MAC intrusa pueda identificarse como perteneciente a la red.
- Si algun equipo con acceso a la red y/o el punto de acceso se roba, el responsable podrá tener acceso a la red
- Al no brindar protección ni a la red ni al usuario para confirmar la conexión de un usuario no cumple con los estándares IEEE 802.1X.

Desactivar el servidor DHCP

El servidor DHCP integrado en el enrutador distribuye las direcciones IP siempre a cada PC. Por lo tanto, otro método para detener a los intrusos es limitar el número de direcciones IP al número de ordenadores que realmente se posee.

Si se decide mantener activado el DHCP, restringiendo el rango de direcciones que asigna, se tiene que modificar los valores “Start IP Address”, en donde se debe introducir la primera dirección que debe asignar el servidor, y “End IP Address”, en donde se debe indicar dónde termina el conjunto de direcciones que puede asignar el router, es decir, la última IP válida.

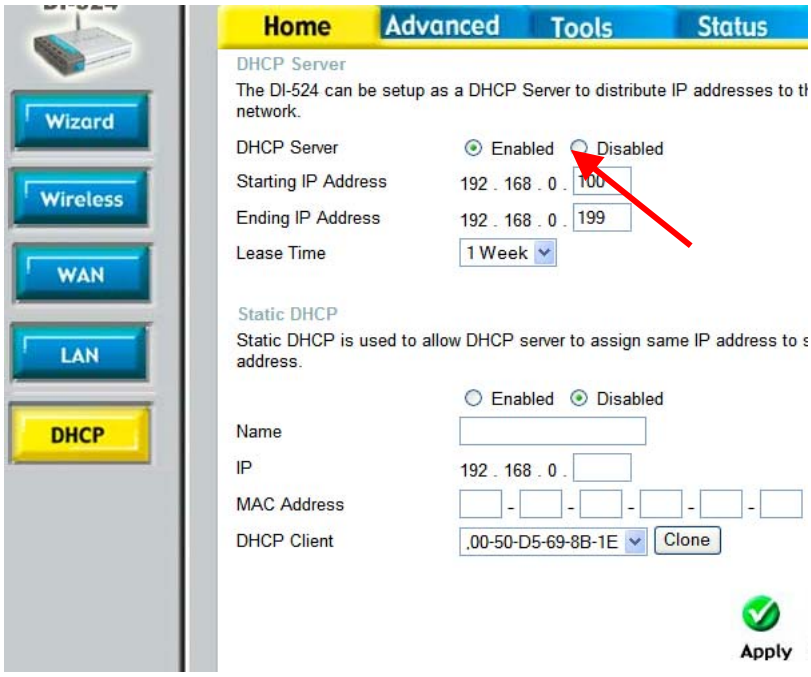


Fig. 1.13- Ventana para desactivar DHCP

Para desactivar el servidor DHCP y configurar todas las direcciones de los dispositivos manualmente, hay que marcar la casilla “Disable DHCP Server”, de este modo se evitará que el router conceda a un equipo externo los datos de conexión de la red. Sin embargo, esto implica que se tendrá que introducir la dirección IP, la puerta de enlace y los DNS directamente a mano en cada PC.

1.5.4.2 Seguridad en Internet: Firewall

Un Firewall es un sistema, o conjunto de ellos, ubicado entre dos redes y que ejerce la política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

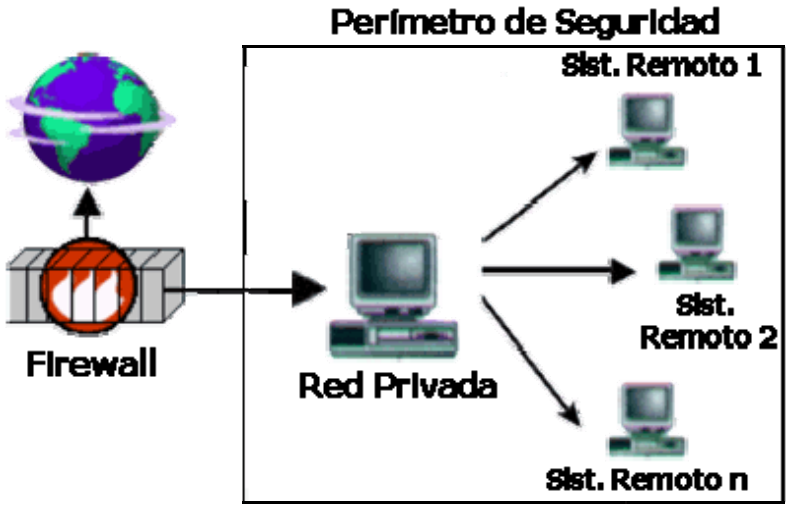


Fig. 1.14- Perímetro de seguridad

El Firewall sirve de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Funcionamiento:

El funcionamiento elemental, es que cualquier paquete de datos, que circule entre nuestra maquina y el exterior (red), es filtrado por el firewall, de acuerdo a unas normas con el cual le hemos configurado, y de acuerdo a esas normas, permitirá o no, la entrada/salida de esos mismos datos.

Básicamente, y depende de los firewall la configuración del mismo viene dada por permisos adjudicados a programas (con los puertos que usen), o bien a servicios usados por estos, por lo que si damos paso libre a un programa, generalmente, estaremos dando paso a todos los datos que circulen de y hacia ese programa, independientemente del puerto que tenga abierto y de que los datos sean "maliciosos" o no (una especial atención a esto), el firewall, permite o no el trafico de datos, pero NO chequea el contenido de los mismos, de ahí la importancia del tandem firewall-antivirus.

Normalmente, cuando instalamos un firewall, este nos rechaza cualquier tipo de trafico, al cerrarnos todos los puertos de la maquina, progresivamente, según vayamos usando los programas o servicios del sistema que necesitemos, el firewall nos dará un mensaje de alerta, indicándonos que tal servicio o programa esta intentando acceder a la red, o de la red a nuestra maquina, y nos preguntara las pautas a seguir en ese y en los siguientes intentos de conexión.

Un firewall lleva a cabo tres funciones para proteger su red:

• Bloquea los datos entrantes que pueden contener el ataque de un “hacker”
• Oculta la información acerca de la red, haciendo que todo parezca como si el tráfico de salida se originara del firewall y no de la red. Esto también se conoce como NAT (Network Address Translation)
• Filtra el tráfico de salida, con el fin de restringir el uso de Internet y el acceso a localidades remotas

Características y funciones adicionales de un Firewall

Además de las capacidades de seguridad estándares, se ha integrado una gran cantidad de características y funciones adicionales a los productos de firewall. Entre estas figuran: soporte para servidores públicos de Web y correo electrónico, por lo general llamada zona desmilitarizada (DMZ), filtración de contenido, soporte de encriptación de VPN y de antivirus.

Firewalls con zona desmilitarizada (DMZ): Una zona desmilitarizada (DMZ) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa, es decir: los equipos locales (hosts) en la DMZ no pueden conectar con la red interna.

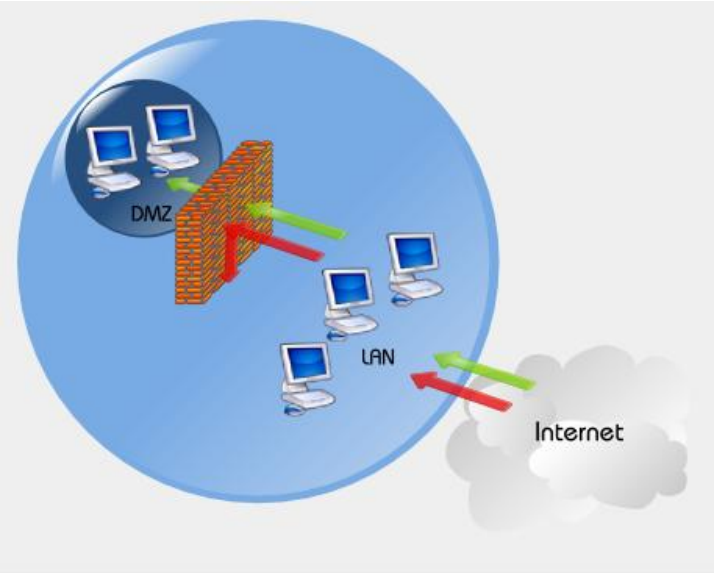


Fig. 1.15- Zona desmilitarizada (DMZ)

La decisión de optar por un firewall con DMZ debe basarse en la cantidad de usuarios externos que acceden a la red y la frecuencia con la que lo hacen. Un firewall con DMZ crea un área de información protegida ("desmilitarizada") en la red. Los usuarios externos pueden ingresar al área protegida, pero no pueden acceder al resto de la red. Esto permite a los usuarios externos acceder a la información que usted quiere que vean, pero previene que obtengan información no autorizada.

Filtración de contenido: Un filtro de sitios Web o filtro de contenido extiende las capacidades del firewall para bloquear el acceso a ciertos sitios Web. Usted puede usar esta función adicional para asegurarse de que sus empleados no accedan contenido inapropiado, como por ejemplo, material pornográfico o racista. Esta funcionalidad le permite definir categorías de material inadecuado y obtener un servicio que lista miles de sitios Web que incluyen dicho tipo de material. Como siguiente paso, puede escoger si quiere bloquear totalmente el acceso a estos sitios o permitir su uso, pero manteniendo un registro del mismo. Tal servicio debe actualizar automática y regularmente la lista de sitios Web que no pueden ser accedidos.

Protección a través de antivirus: Todos debemos preocuparnos seriamente por las amenazas de los virus, uno de los esquemas más nocivos de "hacking" de computadoras.

Los usuarios pueden dañar rápidamente toda una red si, inadvertidamente, bajan material desconocido o diseminan virus peligrosos en las redes. Empresas de todo tipo y tamaño han perdido enormes cantidades de dinero, debido al impacto negativo en la productividad y los costos de reparación de la red causados por un virus.

Los firewalls no están diseñados para remover o limpiar virus. No obstante, pueden ayudar a detectarlos, lo cual es un factor esencial de cualquier plan de protección contra virus.

Es importante observar que el firewall sólo puede proteger la red a partir del dispositivo de WAN al cual está conectado. Un servidor de acceso remoto o una PC con un módem puede servir como puerta de acceso a la red, el cual puede burlar las medidas de seguridad del firewall. Lo mismo puede ocurrir cuando un empleado introduce un diskette infectado con un virus en su PC. El lugar más apropiado para instalar el software antivirus es en la PC de cada usuario. No obstante, un firewall puede contribuir a la detección de virus, exigiendo que cada usuario que ingrese a Internet o baje correo electrónico, utilice, como mínimo, la última versión del software antivirus.

1.6 ETHERNET

Una Red Ethernet es un tipo particular de cableado de red más un grupo de especificaciones de señalización que cubren las capas 1 (Física) y 2 (Enlace) del modelo OSI. Fue formalizada por el IEEE como el estándar Ethernet 802.3.

En una configuración Ethernet, los equipos están conectados mediante cable coaxial o de par trenzado ("Twisted-pair") y compiten por acceso a la red utilizando un modelo denominado CSMA/CD ("Carrier Sense Multiple Access with Collision Detection"), el cual se describe en el apartado 1.6.4

Ethernet utiliza tres conceptos esenciales para su operatividad:

- La difusión.
- El direccionamiento Ethernet.
- Trama Ethernet.

1.6.1 Difusión o Broadcast

La *difusión* o broadcast hace que una trama Ethernet se difunda por todo el medio de comunicación, llegando a cada tarjeta conectada (al cable) sin necesidad de reproducir la misma transmisión nodo por nodo; sin embargo, sólo la tarjeta con la *dirección Ethernet* que coincide con la Dirección indicada en la trama la aceptará, el resto simplemente la ignorará.

Una cantidad inapropiada de estos mensajes de difusión (broadcast) provocara un bajo rendimiento en la red, una cantidad exagerada (tormenta de broadcast) dará como resultado el mal funcionamiento de la red hasta tal punto de poder dejarla completamente congestionada.

1.6.2 Direccionamiento Ethernet

El direccionamiento Ethernet hace que una tarjeta sea única en la red y corresponde a la dirección física de la tarjeta.

Cada tarjeta de red o NIC tiene un número de identificación (dirección) de 6 bytes que es único en el mundo y no se repite y se denomina MAC ("Media Access Control"). Esta dirección está contenida en el hardware de la tarjeta o adaptador de red y no puede/debe ser alterado.

Por ejemplo, cuando un host A quiere conocer la dirección Ethernet de otro host B conectado a su misma red, envía un mensaje ARP (protocolo de encaminamiento capa3) de petición en modo 'broadcast' (dirección Ethernet destino = FF:FF:FF:FF:FF:FF). En dicho mensaje ARP repite su dirección Ethernet, ya presente en la cabecera Ethernet, en el cuerpo del mensaje (dir. Ether. Origen) e indica su dirección IP (dir. IP origen). Rellena dir. IP destino con la dirección IP de B y deja dir. Ether. destino como FF:FF:FF:FF:FF:FF. B, al recibir este paquete (lo cual ocurrirá siempre que su tarjeta tenga habilitada la recepción de tramas broadcast), responde con un mensaje ARP de respuesta. Esta vez el mensaje irá dirigido directamente a A en lugar de ser difundido.

La máquina A tomará nota de la información obtenida, apuntando la correspondencia de direcciones IP-Ethernet de B en una caché, con lo cual se evitarán futuras peticiones para

mensajes IP dirigidos a la misma máquina. Por otra parte, B, al recibir la petición de A, tomará nota en su caché de la dirección Ethernet de esta máquina, si no la tenía ya almacenada.

La caché mantiene una lista de las direcciones obtenidas por las sucesivas peticiones y respuestas recibidas. Se suele implementar un tiempo vida (TTL, *time to live*) para cada entrada de la caché, borrándose dicha entrada cuando su tiempo de vida expira. Esto fuerza un cierto refresco en las cachés de los hosts de una red, de forma que entradas no usadas o incorrectas acaban siendo eliminadas.

1.6.3 Trama Ethernet

Todo lo que circula por una red Ethernet lo hace a través de una *Trama Ethernet*; ésta vendría a ser el medio de transporte de todos los protocolos que se definen en las capas superiores. Las tramas son el formato en que los datos son encapsulados para poder ser transmitidos al medio físico.

La trama Ethernet es de una longitud variable pero no es menor a 64 octetos ni rebasa los 1518 octetos (encabezado, datos y CRC). Como en todas las redes de conmutación de paquetes, cada trama Ethernet contiene un campo con la información de la dirección de destino. La figura muestra que la trama Ethernet contiene la dirección física de la fuente y también la dirección física del destino.

Preámbulo	Destino	Fuente	Tipo	Datos	CRC
8 octetos	6 octetos	6 octetos	2 octetos	64-1500 octetos	4 octetos

Fig. 1.16- Trama Ethernet

Además de la información para identificar la fuente y el destino, cada trama transmitida a través de Ethernet contiene un *preámbulo*, *un campo de tipo*, *un campo de datos* y una *Cyclic Redundancy Check* (verificación por redundancia cíclica o CRC, por sus siglas en inglés). El preámbulo consiste en 64 bits que alternan ceros y unos para ayudar a la sincronización de los nodos de recepción.

El CRC de 32 bits ayuda a la interfaz a detectar los errores de transmisión: el emisor computa el CRC como una función de los datos de la trama y el receptor computa de nuevo el CRC para verificar que el paquete se ha recibido intacto.

El campo de tipo de trama contiene un entero de 16 bits que identifica el tipo de datos que se están transfiriendo en la trama. Desde el punto de vista de Internet, el campo de tipo de trama es esencial porque significa que las tramas de Ethernet se *autoidentifican*.

Cuando una trama llega a una máquina dada, el sistema operativo utiliza el tipo de trama para determinar que módulo de software de protocolo se utilizará para procesar la trama. La mayor ventaja de que las tramas se autoidentifiquen es que éstas permiten que múltiples protocolos se utilicen juntos en una sola máquina y sea posible entremezclar diferentes protocolos en una sola red física sin interferencia. Por ejemplo, uno podría tener un programa de aplicación que utiliza protocolos de Internet, mientras otro utiliza un protocolo experimental local. El sistema operativo utiliza el campo de tipo de una trama entrante para decidir cómo procesar el contenido. Veremos que los protocolos TCP/IP utilizan tramas Ethernet autoidentificables para hacer una selección entre varios protocolos.

Una red Ethernet es una red de banda base, o sea que provee un único canal de comunicación sobre el medio físico (cable), de forma que solo puede usarlo un dispositivo a la vez.

Esta tecnología realiza varias funciones que incluyen empaquetado y desempaquetado de los datagramas; manejo del enlace; codificación y decodificación de datos, y acceso al canal. El manejador del enlace es responsable de vigilar el mecanismo de colisiones, escuchando hasta que el medio de transmisión está libre antes de iniciar una transmisión (solo un usuario utiliza la transmisión cada vez -Banda base-). El manejo de colisiones se realiza deteniendo la transmisión y esperando un cierto tiempo antes de intentarla de nuevo.

El largo dominio de Ethernet se debe principalmente a un buen equilibrio entre velocidad, coste y facilidad de instalación.

1.6.4 CSMA/CD

El concepto básico del protocolo CSMA/CD ("Carrier Sense Multiple Access with Collision Detection") utilizado en Ethernet es muy sencillo: todas las estaciones se dedican a escuchar si hay transmisiones en la línea. La estación que desea transmitir lo hace cuando detecta que el canal está desocupado. Este procedimiento se llama detección de potadora (CS, carrier sensing), y la estrategia de acceso que en este caso se aplica es el esquema CSMA (acceso múltiple con detección de portadora). Las estaciones están fìsicamente separadas entre sí y es probable que dos o más estaciones detecten al mismo tiempo que el canal está desocupado, y por tanto empiecen a transmitir, causando colisiones. Una vez que las estaciones detectan una colisión, transmiten una señal de bloqueo especial, notificando a las otras estaciones que ha ocurrido una colisión y que aborten sus transmisiones.

Cada segmento de una red Ethernet (entre dos router, bridges o switches) constituye lo que se denomina **dominio de tiempo de colisiones** o **dominio de colisiones** Ethernet.

Se supone que cada bit permanece en el dominio un tiempo máximo ("Slot time") de 25.6 µs (algo más de 25 millonésimas de segundo), lo que significa que en este tiempo debe haber llegado al final del segmento.

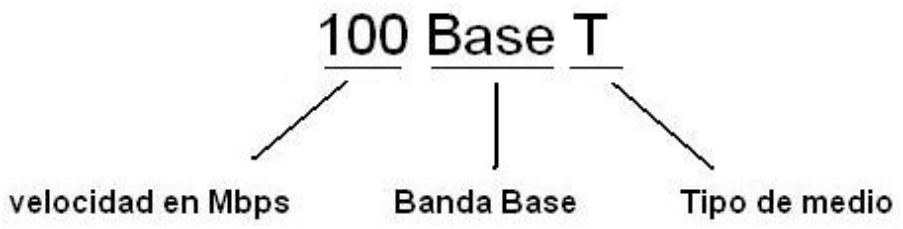
Si en este tiempo la señal no ha salido del segmento, puede ocurrir que una segunda estación en la parte del segmento aún no alcanzado por la señal, pueda comenzar a transmitir, puesto que su detección de portadora indica que la línea está libre, dado que la primera señal aún no ha alcanzado a la segunda estación. En este caso ocurre un acceso múltiple MA ("Multiple Access") y la colisión de ambos datagramas es inevitable

En la operación de una red Ethernet se considera normal una cierta tasa de colisiones, aunque debe mantenerse lo más baja posible. En este sentido una red normal debe tener menos de un 1% de colisiones en el total de paquetes transmitidos (preferiblemente por debajo del 0.5%). Para realizar este tipo de comprobaciones es necesario contar con analizadores adecuados.

1.6.5 Tipos de Ethernet

Según el tipo de cable, topología y dispositivos utilizados para su implementación podemos distinguir varios tipos de Ethernet:

En primer lugar existe una convención utilizada en los estándares Ethernet, y está denotada por tres partes:



Tecnología	Velocidad de transmisión	Tipo de cable	Distancia máxima	Tipología
10Base2	10 Mbps	Coaxial	185 m	Conector T
10BaseT	10 Mbps	Par Trenzado	100 m	Hub o Switch
10BaseF	10 Mbps	Fibra óptica	2000 m	Hub o Switch
100BaseT4	100Mbps	Par Trenzado (categoría 3UTP)	100 m	Half Duplex(hub) y Full Duplex(switch)
100BaseTX	100Mbps	Par Trenzado (categoría 5UTP)	100 m	Half Duplex(hub) y Full Duplex(switch)
100BaseFX	100Mbps	Fibra óptica	2000 m	No permite el uso de hubs
1000BaseT	1000Mbps	4 pares trenzado	100 m	Full Duplex (switch)

		(categoría 5UTP)		
1000BaseSX	1000Mbps	Fibra óptica (multimodo)	550 m	Full Duplex (switch)
1000BaseLX	1000Mbps	Fibra óptica (monomodo)	5000 m	Full Duplex (switch)

Tabla 1.1- Tipos de Ethernet

Ethernet incluye tres principales categorías:

10 Mbps Ethernet: Especificaciones LAN que operan a 10 Mbps sobre cable coaxial.

100 Mbps Ethernet: Especificación LAN, también conocida como "FAST ETHERNET", que opera a 100 Mbps sobre cable par trenzado.

En su momento el prefijo *fast* se le agregó para diferenciarlas de la Ethernet regular de 10 Mbps. Fast Ethernet no es hoy por hoy la más rápida de las versiones de Ethernet, siendo actualmente Gigabit Ethernet y 10 Gigabit Ethernet las más veloces.

En su momento dos estándares de IEEE compitieron por el mercado de las redes de área local de 100 Mbps. El primero fue el IEEE 802.3 100BaseT, denominado comercialmente Fast Ethernet, que utiliza el método de acceso CSMA/CD con algún grado de modificación, cuyos estándares se anunciaron para finales de 1994 o comienzos de 1995. El segundo fue el IEEE 802.12 100BaseVG, adaptado de 100VG-AnyLAN de HP, que utiliza un método de prioridad de demandas en lugar del CSMA/CD. Por ejemplo, a la voz y vídeo de tiempo real podrían dárseles mayor prioridad que a otros datos. Esta última tecnología no se impuso, quedándose Fast Ethernet con casi la totalidad del mercado

Existen tres tipos de Fast Ethernet:

- 100BaseTX usado con cable CAT 5 UTP
- 100BaseFX usado con fibra óptica
- 100BaseT4 el cual utiliza dos cables extras para usarse con cable UTP CAT 3.

1000 Mbps Ethernet: Especificación LAN, también conocida como Gigabit Ethernet, que opera a 1000 Mbps (1 Gbps) sobre fibra óptica y cable par trenzado.

Gigabit Ethernet (1000 Mbps Ethernet) es una extensión del estándar IEEE 802.3. Gigabit Ethernet está construído sobre el mismo protocolo de Fast Ethernet pero incrementa la velocidad en 10 veces sobre Fast Ethernet.

En 1999, la IEEE probó la especificación 802.3ab, también conocida como 1000BaseT, que define Gigabit Ethernet (GE) corriendo sobre cable de cobre, es decir Gigabit Ethernet puede correr sobre el cable de cobre categoria 5, pero también corre sobre fibra óptica monomodo y multimodo.

También GE es más fácil de implementar y mucho más es mucho más rápido que otras tecnologías como ATM o FDDI.

Un nuevo estándar de GE acaba de ser aprobado por la IEEE, el IEEE 802.3ae opera a 10 Gigabits. Este estándar es una actualización directa de las dorsales de GE, es especificado sólo para fibra óptica y es full duplex. Las interfaces ópticas proveen opciones para fibras monomodo de hasta 40 Km y para fibras multimodo a distancias máximas de 300 metros. Este nuevo estándar utiliza la misma arquitectura de los anteriores estándares Ethernet (arquitectura, software y cableado).

1.6.6 Conmutador Ethernet

Un conmutador Ethernet, realiza el encaminamiento de tramas Ethernet, que para lo cual debe construir la tabla de encaminamiento, para ello realiza un proceso de aprendizaje de direcciones. Este consiste en escuchar todas las tramas recibidas en un puerto dado y para cada una de ellas extraer la dirección origen y si no existe una entrada en la tabla de encaminamiento para esta dirección, añadirla con puerto de salida aquel en el que hemos recibido la trama. De este modo, la trama de encaminamiento se construye de un modo automático.

A pesar del proceso de aprendizaje, es posible que al conmutador le llegue una trama con una dirección destino para la cual no existe ninguna entrada en la tabla de encaminamiento. En este

caso el conmutador la transmite por todos los puertos excepto por aquel en el que recibió. En este proceso se conoce como inundación y garantiza que la trama llegará a destino.

Tanto el proceso de encaminamiento como el de aprendizaje suponen realizar una búsqueda en la tabla de encaminamiento. En la siguiente tabla se muestra un ejemplo de una sencilla tabla de encaminamiento. En el caso de que tengamos una trama con dirección destino 00-07-b3-5c-11-c0, la búsqueda nos dice que debemos transmitirla por el puerto 1. Como se observa la búsqueda en la tabla se realiza sobre todos los bits de la dirección. Esta es una diferencia fundamental con la búsqueda realizada en otros protocolos en los que la estructura de la dirección se utiliza para optimizar el proceso. Este es el caso por ejemplo de los routers IP para los que se han propuesto numerosos algoritmos de búsqueda sobre la tabla de encaminamiento. El hecho de que en Ethernet la búsqueda se realiza sobre todos los bits de la dirección y que para una dirección destino hay sólo una posible entrada en la tabla nos permite el uso de memorias CAM para la implementación de las tablas de encaminamiento.

Dirección Destino	Puerto de Salida
00-07-b3-5c-11-c0	1
00-07-e9-1a-0c-53	3
00-06-5b-87-8b-97	2
08:00:20:d9:d1:40	4
00-06-5b-57-04-43	1

Tabla 1.2- Tabla de encaminamiento

Las tramas son recibidas en un puerto del conmutador y normalmente tras su procesado se transmiten por otro puerto de este hacia su destino. Por cada puerto el conmutador debe realizar las funciones de nivel físico que permiten convertir las señales eléctricas u ópticas recibidas en los bits que forman las tramas Ethernet. Estas funciones son muy dependientes del medio de transmisión utilizado y están recogidas en diferentes estándares IEEE 802.3. Una vez recuperada la trama, esta pasa al nivel de control de acceso al medio (MAC) que comprueba la validez del campo de redundancia (FCS) y si ha habido errores descarta la trama. En caso contrario la almacena en un buffer.

Una vez que la trama ha sido recibida y almacenada correctamente, el conmutador en función de sus características puede realizar una clasificación de la trama por diversos motivos como el marcado de la etiqueta de red de área local virtual, la asignación de prioridad a la trama para implementar mecanismos de calidad de servicio o el filtrado de acuerdo a una lista de control de acceso para implementar mecanismos de seguridad.

En la mayoría de los casos, la clasificación se hace en base no solamente a las direcciones de origen y destino Ethernet sino que es necesario incluir campos de niveles superiores (nivel 3 en adelante) como las direcciones IP o los puertos TCP. Esto hace que el proceso de clasificación sea complejo.

1.6.6.1 Tipos de Conmutadores

Las redes de área local pueden llegar a conectar miles de dispositivos, en estos casos de grandes redes, se hace necesaria una estructura jerárquica.

Esta jerarquía da lugar a diferentes tipos de conmutadores diseñados específicamente para cada nivel de la jerarquía. En el nivel mas bajo (ver figura) encontramos los conmutadores de *desktop* a los que se conectan directamente los ordenadores de los usuarios en el caso de una red micro segmentada o repetidores que dan acceso a varios usuarios que comparten un único puerto del conmutador.

En el siguiente nivel están los conmutadores de *workgroup* o departamento a los que están conectados los servidores del departamento y conmutadores del nivel inferior.

Los conmutadores de *campus* son los que conectan distintos departamentos que pueden estar físicamente en el mismo o en diferentes edificios y dan acceso a los servidores comunes o varios departamentos. En el último nivel están los dispositivos que conectan las diferentes sedes de la organización, normalmente mediante redes WAN.

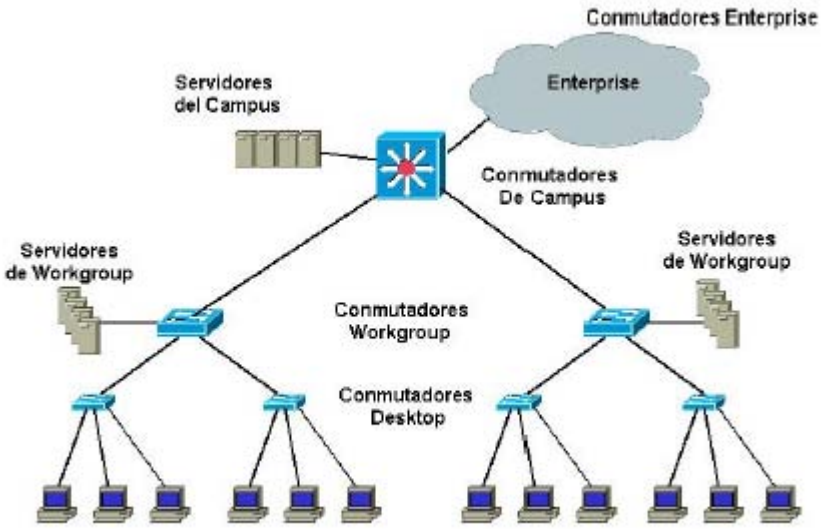


Fig. 1.17- Jerarquía de conmutadores

Los requisitos que deben cumplir los conmutadores son distintos en cada nivel de la jerarquía y se pueden analizar en términos de números de puertos, y su velocidad, lo medios físicos soportados, el tamaño de la tabla de encaminamiento y el soporte de ciertas características como las redes VLAN, mecanismos de seguridad, etc.

1.7 DIRECCIÓN IP

El protocolo de red IP utiliza direcciones formadas por números de 32 bits. Se le debe asignar un número único a cada máquina del entorno de red. Hay algunos rangos de direcciones IP que han sido reservadas para redes privadas. De cualquier modo, los números para los sitios en Internet los asigna una autoridad central, el Network Information Center (NIC).

Las direcciones IP se separan en cuatro números de ochos bits llamados octetos. Por ejemplo, quark.physics.groucho.edu tiene una dirección IP:

0x954C0C04 que se escribe como 149.76.12.4.

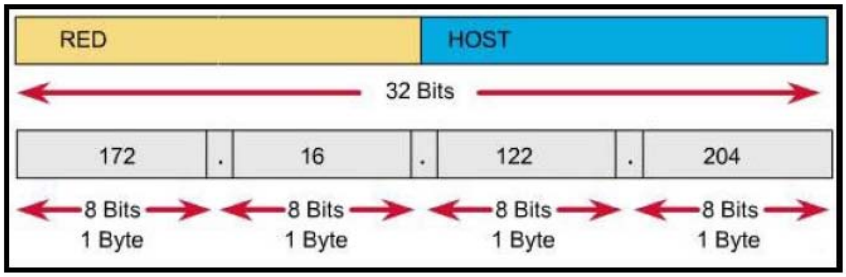


Fig. 1.18- formato dirección IP

Este formato se denomina normalmente notación de puntos divisorios. Otra razón para usar esta notación es que las direcciones IP se dividen en un número de red, que es contenido en el octeto principal, y un número de puesto (host) que es contenido en el resto. Cuando se solicita al NIC una dirección IP, no se le asignará una dirección para cada puesto individual que pretenda usar. En cambio, se le otorgará un número de red y se le permitirá asignar todas las direcciones IP válidas dentro de ese rango para albergar puestos en su red de acuerdo con sus preferencias.

1.7.1 Clasificación de direcciones IP

Las direcciones IP se clasifican en:

Direcciones IP públicas. Son visibles en todo Internet. Un ordenador con una IP pública es accesible (visible) desde cualquier otro ordenador conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.

Direcciones IP privadas (reservadas). Son visibles únicamente por otros hosts de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los puestos de trabajo. Los ordenadores con direcciones IP privadas pueden salir a Internet por medio de un router (o proxy) que tenga una IP pública. Sin embargo, desde Internet no se puede acceder a ordenadores con direcciones IP privadas.

Cada host conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el host. En el caso de Internet, no puede haber dos ordenadores con 2 direcciones IP (públicas)

iguales. Pero sí podríamos tener dos ordenadores con la misma dirección IP siempre y cuando pertenezcan a redes independientes entre sí (sin ningún camino posible que las comunique).

A su vez, las direcciones IP pueden ser:

Direcciones IP estáticas (fijas). Un host que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas para evitar duplicar una misma dirección dentro de la subred.

Direcciones IP dinámicas. Un host que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem. Los proveedores de Internet utilizan direcciones IP dinámicas debido a que tienen más clientes que direcciones IP.

1.7.2 Clases de direcciones IP

La comunidad de Internet originalmente definió cinco clases de direcciones para acomodar redes de diferentes tamaños. Para uso convencional se utilizan solo tres de las cinco clases definidas por la IETF (http://www.ietf.org). Las distintas clases definen qué bits de la dirección identifican las redes y cuales los hosts. También queda definido el número posibles de redes de esa clase y, en cada una de ellas, el número de hosts.

Clase A.

Las direcciones clase A son asignadas para redes muy grandes. El bit de más alto orden siempre està en “0”. Los siguientes siete bits completan el identificador de red. Luego, los restantes 24 bits quedan para combinaciones que identifican los hosts en la red, menos dos. Estas redes permiten 127 redes y 16.777.214 hosts en cada una de ella.

Clase B.

Las direcciones de clase B son asignadas a redes de mediano a gran tamaño. Los dos bits de orden más alto son siempre iguales a "10". Los siguientes 14 bits identificarán las distintas redes. Los restantes 16 bits servirán para identificar los hosts. Esto permite 16.384 redes distintas y cada una de ellas con 65.534 hosts.

Clase C.

Son utilizable para direccional pequeñas redes. Los tres bits de mayor orden estará siempre puestos en 110. Los siguientes 21 bits completan el identificador de red. Los ocho restantes permiten identificar los hosts. Esto permite obtener 2.097.157 redes y 254 hosts por cada una.

Clases D y E

Las clases D y E no se asignan a hosts. Las direcciones de clase D se utilizan para la multidifusión, y las direcciones de clase E se reservan para uso futuro.

En la siguiente tabla se indica el espacio de direccionamiento en cada una de las tres clases comercialmente utilizable de redes IP.

Clase	**Nº redes**	**Nº Hosts**	**Rango inicial**
A	127	16.717.214	1.0.0.0
B	16.384	65.534	128.0.0.0
C	2.097.157	254	192.0.0.0

Tabla 1.3- Clases de direccionamiento IP

1.7.3 Concepto de IPv4 e Ipv6

La creación de Ipv6 no es solo causa de la escasez de direcciones Ipv4, sino que además se añaden nuevas características y se mejoran las existentes. Sobre Ipv4 las tablas de rutas de los routers se están haciendo gigantescas, tanto el multi-homing como la movilidad son tareas excesivamente complejas.

Las nuevas necesidades del usuario no pueden ser satisfechas de forma sencilla: seguridad, movilidad y calidad de servicio (QoS) entre otras. De todas estas razones, la única que no tiene alternativa sobre Ipv4 es el agotamiento de direcciones.

Ipv4 soporta 4.294.967.296 (232) direcciones de red diferentes, un número inadecuado para dar una dirección a cada persona del planeta, y mucho menos para cada coche, teléfono, PDA o tostadora; mientras que Ipv6 soporta 340.282.366.920.938.463.463.374.607.431.768.211.456 (2128 ó 340 sextillones) direcciones, cerca de 4,3 × 1020 (430 trillones) direcciones por cada pulgada cuadrada (6,7 × 1017 ó 670 mil billones direcciones/mm2) de la superficie de La Tierra

Las principales características nuevas que aporta el Ipv6 frente al Ipv4 son:

Aumento de las capacidades de direccionamiento

Ipv6 incrementa el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a más niveles de direccionamiento jerárquico. Estos 128 bits suponen 340 cuatrillones de direcciones con lo que incluso cada grano de arena del planeta podría tener su propia dirección IP.

Soporte mejorado para las Extensiones y Opciones

Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos y mayor flexibilidad para introducir nuevas opciones en el futuro.

Capacidad de Etiquetado de Flujo

Se agrega una nueva capacidad para permitir el etiquetado de paquetes que pertenecen a “flujos” de tráfico particulares, para lo cuál, el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en “tiempo real”.

Capacidades de Autenticación y Privacidad

En Ipv6 se especifican extensiones para utilizar autenticación, integridad de los datos, y confidencialidad de los datos.

CAPÍTULO II: DISPOSITIVOS DE RED

2.1 HUB (*o Concentrador)*

Es un dispositivo el cual nos sirve para realizar una red compartida. El propósito principal del hub es regenerar y retemporizar las señales de la red. El hub también se denomina un repetidor diseccionado. Las razones por las que se usan los hubs son crear un punto de conexión central para los medios de cableado y aumentar la confiabilidad de la red, es por ello que se le denomina concentrador. La red se hace más confiable debido a que si falla un cable o algún puerto del hub, la red no se interrumpe. Opera en la capa física del modelo OSI.

Su funcionamiento es relativamente simple pues recibe una trama de Ethernet, por uno de sus puertos, y la repite por todos sus puertos restantes sin ejecutar ningún proceso sobre las mismas.

Un Hub funciona a la velocidad del dispositivo más lento de la red. El Hub no tiene capacidad de almacenar nada. Por lo tanto si un ordenador que emite a 100 megabit le trasmitiera a otro de 10 megabit algo se perdería el mensaje.

Sus principales características son:

- Se trata de un armario de conexiones donde se centralizan todas las conexiones de una red, es decir un dispositivo con muchos puertos de entrada y salida.
- No tiene ninguna función aparte de centralizar conexiones.
- Se suelen utilizar para implementar topologías en estrella física, pero funcionando como un anillo o como un bus lógico.
- Un hub sólo permite operar en modo Half-Duplex

Tipos de Hubs:

- **Hubs activos***:* permiten conectar nodos a distancias de hasta 609 metros, suelen tener entre 8 y 12 puertos y realizan funciones de amplificación y repetición de la señal. Los más complejos además realizan estadísticas. Toman energía desde un suministro de alimentación para regenerar las señales de red

- **Hubs pasivos***:* son simples armarios de conexiones. Permiten conectar nodos a distancias de hasta 30 metros. Generalmente suelen tener entre 8 y 12 puertos. Sólo dividen la señal entre múltiples usuarios, simplemente permiten que uno o más hosts se conecten al mismo segmento de cable.

- **Hubs inteligentes** tienen puertos de consola, es decir se pueden programar para administrar el tráfico de red.

2.2 SWICTH (o Conmutador)

Un switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento de la red, problemas de congestión y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la salida de tramas, reducir tiempo de espera y actualmente el costo por puerto tiende a bajar (costo económico). Opera generalmente en la capa 2 del modelo OSI (también existen de capa 3 y últimamente multicapas), reenvía las tramas en base a la dirección MAC.

Se puede pensar en cada puerto de switch como un micropuente; este proceso se denomina microsegmentación. De este modo, cada puerto de switch funciona como un puente individual y otorga el ancho de banda total del medio a cada host.

El Switch conoce los ordenadores que tiene conectados a cada uno de sus puertos (enchufes). Cuando en la especificación del un “switch” leemos algo como “8k MAC address table” se refiere a la memoria que el “switch” destina a almacenar las direcciones.

Un “switch” cuando se enchufa no conoce las direcciones de los ordenadores de sus puertos, las aprende a medida que circula información a través de él. Con 8k hay más que suficiente. Por cierto, cuando un “switch” no conoce la dirección MAC de destino envía la trama por todos sus puertos, al igual que un HUB (“Flooding”, inundación). Cuando hay más de un ordenador conectado a un puerto de un “switch” este aprende sus direcciones MAC y cuando se envían información entre ellos no la propaga al resto de la red, a esto se llama filtrado.

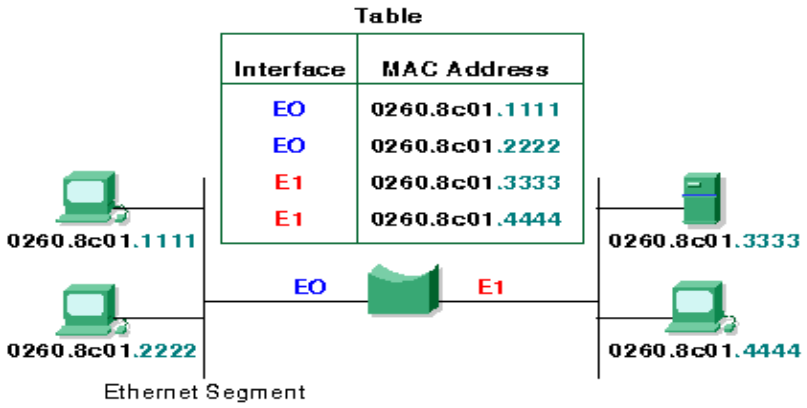


Fig. 2.1- Tabla direcciones MAC

Segmentación de tráfico**:**

Hay dos motivos fundamentales para dividir una LAN en segmentos. El primer motivo es aislar el tráfico entre segmentos, y obtener un ancho de banda mayor por usuario, al crear dominios de colisión más pequeños. Si la LAN no se divide en segmentos, las LAN cuyo tamaño sea mayor que un grupo de trabajo pequeño se congestionarían rápidamente con tráfico y colisiones y virtualmente no ofrecerían ningún ancho de banda.

Al dividir redes de gran tamaño en unidades autónomas, los switches ofrecen varias ventajas: reduce el tráfico que experimentan los dispositivos en todos los segmentos conectados ya que sólo se envía un determinado porcentaje de tráfico; amplían la longitud efectiva de una LAN, permitiendo la conexión de estaciones distantes que anteriormente no estaban permitidas.

Existe otro dispositivo llamado “Puente” que comparte los atributos más importantes del Swith, sin embargo, existen varias diferencias entre ellos. Los switches son significativamente más veloces porque realizan la conmutación por hardware, mientras que los puentes lo hacen por software y pueden interconectar las LAN de distintos anchos de banda. Una LAN Ethernet de 10 Mbps y una LAN Ethernet de 100 Mbps se pueden conectar mediante un switch. Estos pueden soportar densidades de puerto más altas que los puentes. Algunos switches soportan la conmutación por el método cut- through, que reduce la latencia y las demoras de la red mientras que los puentes soportan sólo la conmutación de tráfico de guardar y enviar (store-and-forward). Por último, los switches reducen las colisiones y aumentan el ancho de banda en los segmentos de red ya que suministran un ancho de banda dedicado para cada segmento de red.

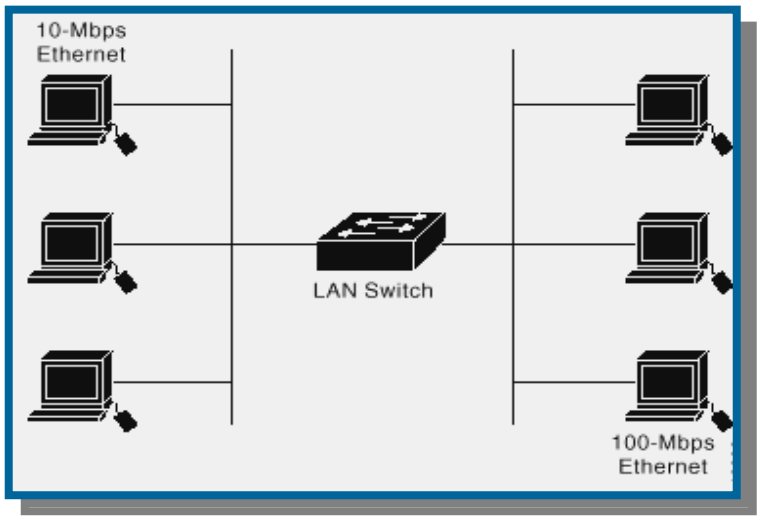


Fig. 2.2- Segmentación de red

Un Switch permite operación Full-Duplex, doblando el Ancho de Banda posible y reduciendo las perdidas por colisiones.

2.3 ROUTER

Los routers trabajan en el nivel de red del modelo de referencia OSI. Esto significa que pueden conmutar y encaminar paquetes a través de múltiples redes. Realizan esto intercambiando información específica de protocolos entre las diferentes redes. Los routers leen en el paquete la información de direccionamiento de las redes complejas teniendo acceso a información adicional.

Funcionamiento:

La primera función de un router, la más básica, es saber si el destinatario de un paquete de información está en nuestra propia red o en una remota. Para determinarlo, el router utiliza un mecanismo llamado “máscara de subred”. La máscara de subred es parecida a una dirección IP (la identificación única de un ordenador en una red de ordenadores, algo así como su nombre y apellido) y determina a que grupo de ordenadores pertenece uno en concreto. Si la máscara de subred de un paquete de información enviado no se corresponde a la red de ordenadores de por ejemplo, nuestra oficina, el router determinará, lógicamente que el destino de ese paquete está en alguna otra red.

La elección de la mejor ruta para garantizar la llegada de los paquetes con el menor retardo depende fundamentalmente de tres criterios:

- Saturación de tráfico (en cada uno de los enlaces del router)
- Dirección de destino del paquete
- Priorización del tráfico hacia determinados destinos.

Los routers mantienen sus propias tablas de encaminamiento, normalmente constituidas por direcciones IP; también se pueden incluir las direcciones de los hosts si la arquitectura de red lo requiere.

Para determinar la dirección de destino de los datos de llegada, las tablas de encaminamiento incluyen:

- Todas las direcciones de red conocidas.
- Instrucciones para la conexión con otras redes.
- Los posibles caminos entre los routers.
- El coste de enviar los datos a través de estos caminos.

Dado que los routers sólo leen paquetes diseccionados de red, no permiten pasar datos corruptos a la red. Por tanto, al no permitir pasar datos corruptos ni tormentas de difusión de datos, los routers implican muy poca tensión en las redes.

Los routers no ven la dirección del nodo de destino, sólo tienen control de las direcciones de red. Los routers pasarán información sólo si conocen la dirección de la red. Esta capacidad de controlar el paso de datos a través del router reduce la cantidad de tráfico entre las redes y permite a los routers utilizar estos enlaces de forma más eficiente que los bridges.

La utilización de un esquema de direccionamiento basado en router permite a los administradores poder dividir una gran red en muchas redes separadas, y dado que los routers no pasan e incluso controlan cada paquete, actúan como una barrera de seguridad entre los segmentos de la red. Esto permite reducir bastante la cantidad de tráfico en la red y el tiempo de espera por parte de los usuarios.

Tipos de routers:

Los tipos principales de routers son:

Estático: Los routers estáticos requieren un administrador para generar y configurar manualmente la tabla de encaminamiento y para especificar cada ruta.

Dinámico: Los routers dinámicos se diseñan para localizar, de forma automática, rutas y, por tanto, requieren un esfuerzo mínimo de instalación y configuración. Son más sofisticados que los routers estáticos, examinan la información de otros routers y toman decisiones a nivel de paquete sobre cómo enviar los datos a través de la red.

Características de los dos tipos de routers:

Routers estáticos	**Routers dinámicos**
Instalación y configuración manual de todos los routers	Configuración manual del primer router. Detectan automáticamente redes y routers adicionales.
Utilizan siempre la misma ruta, determinada a partir de una entrada en la tabla de encaminamiento	Pueden seleccionar un ruta en función de factores tales como coste y cantidad del tráfico de enlace.
Utilizan una ruta codificada (designada para manejar sólo una situación específica), no necesariamente la ruta más corta.	Pueden decidir enviar paquetes sobre rutas alternativas.
Se consideran más seguros puesto que los administradores especifican cada ruta	Pueden mejorar la seguridad configurando manualmente el router para filtrar direcciones específicas de red y evitar el tráfico a través estas direcciones.

Tabla 2.1- Tipos de Routers

En Internet hay miles de routers que trabajan, junto con el nuestro, para buscar el camino más rápido de un punto a otro. Si tenemos un router en nuestra conexión a Internet, este buscará el router óptimo para llegar a un destinatario, y ese router óptimo, buscará a su vez el siguiente óptimo para llegar al destinatario. Digamos que es un gran trabajo en equipo.

Tanto los routers medianos como los más sofisticados permiten configurar què información deseamos que pueda entrar o salir de nuestro PC o red. En caso de que deseemos ampliar las posibilidades de control deberemos añadir un dispositivo llamado Firewall (cortafuegos).

2.4 ANTENAS

Las antenas de redes inalámbricas WLAN se pueden dividir en tres tipos:

2.4.1 Antenas direccionales (o directivas)

Orientan la señal en una dirección muy determinada con un haz estrecho pero de largo alcance. Una antena direccional actúa de forma parecida a un foco que emite un haz concreto y estrecho pero de forma intensa (más alcance).

Las antenas Direccionales "envían" la información a una cierta zona de cobertura, a un ángulo determinado, por lo cual su alcance es mayor, sin embargo fuera de la zona de cobertura no se "escucha" nada, no se puede establecer comunicación entre los interlocutores.

El alcance de una antena direccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor.

Fig. 2.3- Antena directiva

2.4.2 Antenas Omnidireccionales

Orientan la señal en todas direcciones con un haz amplio pero de corto alcance. Si una antena direccional sería como un foco, una antena omnidireccional sería como una bombilla emitiendo luz en todas direcciones pero con una intensidad menor que la de un foco, es decir, con menor alcance.

Las antenas Omnidireccionales "envían" la información teóricamente a los 360 grados por lo que es posible establecer comunicación independientemente del punto en el que se esté. En contrapartida el alcance de estas antenas es menor que el de las antenas direccionales.

El alcance de una antena omnidireccional viene determinado por una combinación de los dBi de ganancia de la antena, la potencia de emisión del punto de acceso emisor y la sensibilidad de recepción del punto de acceso receptor. A mismos dBi, una antena sectorial o direccional dará mejor cobertura que una omnidireccional.

Fig. 2.4- Antena omnidireccional

2.4.3 Antenas sectoriales

Son la mezcla de las antenas direccionales y las omnidireccionales. Las antenas sectoriales emiten un haz más amplio que una direccional pero no tan amplio como una omnidireccional. La intensidad (alcance) de la antena sectorial es mayor que la omnidireccional pero algo menor que la direccional. Siguiendo con el ejemplo de la luz, una antena sectorial sería como un foco de gran apertura, es decir, con un haz de luz más ancho de lo normal.

Para tener una cobertura de 360º (como una antena omnidireccional) y un largo alcance (como una antena direccional) deberemos instalar o tres antenas sectoriales de 120º ó 4 antenas sectoriales de 80º. Las antenas sectoriales suelen ser más costosas que las antenas direccionales u omnidireccionales.

Fig. 2.5- Antena sectorial

2.4.4 Apertura vertical y apertura horizontal

La apertura es cuanto se "abre" el haz de la antena. El haz emitido o recibido por una antena tiene una abertura determinada verticalmente y otra apertura determinada horizontalmente.

En lo que respecta a la apertura horizontal, una antena omnidireccional trabajará horizontalmente en todas direcciones, es decir, su apertura será de 360º. Una antena direccional oscilará entre los 4º y los 40º y una antena sectorial oscilará entre los 90º y los 180º.

La apertura vertical debe ser tenida en cuenta si existe mucho desnivel entre los puntos a unir inalámbricamente. Si el desnivel es importante, la antena deberá tener mucha apertura vertical. Por lo general las antenas, a más ganancia (potencia por decirlo de algún modo) menos apertura vertical. En las antenas direccionales, por lo general, suelen tener las mismas aperturas verticales y horizontales.

CAPÌTULO III: PROPUESTA DEL PROYECTO

3.1 DESCRIPCIÓN DEL PROYECTO

El cambio producido por el avance de la tecnología en el área informática y de telecomunicaciones es tan profundo, que hoy es posible utilizar servicios impensados años atrás, como la consulta de bases de datos remotas ubicadas en computadoras a miles de kilómetros, la transferencia "instantánea" de documentos, video conferencia en tiempo real, correo electrónico, acceso a enciclopedias y muchos más, estos ya coexisten con otros servicios tradicionales como la telefonía y el fax. Técnicamente la infraestructura básica permitirá brindar los múltiples servicios de redes y gestión de información a todas las dependencias del establecimiento, además de permitir su ingreso en la red mundial Internet mediante múltiples conexiones a Internet.

El Centro Educacional San Nicolás es el establecimiento elegido para realizar, diseñar e implementar el trabajo de investigación, dando la posibilidad de desarrollar un proyecto que cumplirá con dos objetivos fundamentales, el primero establece la necesidad real del establecimiento educacional de contar con una infraestructura de red adecuada para desarrollar sus actividades de enseñanza, y el segundo otorga la oportunidad de aplicar conocimientos teóricos de ingeniería en el desarrollo de una infraestructura de red con soporte para aplicaciones virtuales. De esta forma, se integra un proyecto de Ingeniería y una comunidad educativa, en pro de un entorno de desarrollo y crecimiento con responsabilidad social.

3.2 ESTUDIO TÈCNICO

3.2.1 Tamaño del Proyecto: etapa 1 sala de computación.

Descripción física del laboratorio de computación

El establecimiento debe otorgar un espacio físico para a implementación del laboratorio, considerando la cantidad de alumnos que lo ocupará, la cantidad de estaciones de trabajo, el espacio y el mobiliario que se necesita para instalar todos los componentes del laboratorio: tales

como computadores, impresoras, pizarrón, telón, proyector y el lugar donde se colocaran los equipos de red.

De acuerdo a nuestra experiencia, podemos recomendar una sala de computación, que a nuestro modo de ver correspondería a una situación ideal. Se debe considerar que cada estación de trabajo puede ser compartida por a lo más dos alumnos (recomendable sólo para alumnos de enseñanza básica), lo optima es una estación por alumnos, pero puede no estar al alcance del presupuesto. Además cada curso tiene a lo menos 30 alumnos y entonces se implementará el laboratorio con un mínimo de 15 estaciones de trabajo, ya que esto está directamente relacionado con la cantidad de alumnos de cada curso.

Además se debe considerar que la sala debe estar administrada por una persona, la cual deberá realizar las siguientes tareas:

- Monitoreo del uso de los Recursos: el administrador debe mantener las estaciones de trabajo libre de virus y basura informática (archivos y programas que no se ocupen, o que no sean de índole educativo), generar respaldos de archivos fundamentales y al menos, realizar una limpieza semanal de los equipos.
- Mantener bitácora del Equipamiento: esto ayudará a determinar soluciones proactivas en caso de problemas repetitivos de algunos componentes de hardware de la sala de computación, un ejemplo de bitácora es la siguiente

FORMULARIO INDIVIDUAL DE EQUIPAMIENTO

ESPECIFICACIONES GENERALES

NOMBRE DEL EQUIPO	FECHA DE INGRESO

COMPONENTES DEL EQUIPO

MARCA CPU	NRO. SERIE CPU	FECHA DE COMPRA	TIEMPO DE GARANTIA

PROVEEDOR CPU	GUIA DE DESPACHO/FACTURA

MARCA MONITOR	NRO. SERIE MONITOR	FECHA DE COMPRA	TIEMPO DE GARANTIA

SERIE TECLADO	SERIE MOUSE	TARJETA DE RED	OTROS

SOFTWARE ASOCIADO

WINDOWS NT SERVER	
WINDOWS 95	
OFFICE 97 PROFESSIONAL	
ANTIVIRUS	
SOFTWARE ADMINSTRATIVO	

SOFTWARE EDUCACIONAL

BITACORA DE INCIDENTES

FECHA	DESCRIPCION DEL PROBLEMA	FECHA SOLUCION	DESCRIPCION SOLUCION

Fig. 3.1- Formulario individual de equipamiento

- Mantener inventario de los recursos: esta información facilita la adquisición de partes y piezas en caso de que alguno de los componentes de hardware falle.
- Establecer restricciones: el administrador controlará la información que se desea tener a disposición de profesores, alumnos y apoderados.

3.2.2 Descripción de las estaciones de trabajo

Dimensiones de cada estación: 1x0.6 mtrs. Estas estaciones se han definido acorde al espacio mínimo utilizado para el trabajo de dos alumnos frente a una misma estación, de esta manera cada uno de ellos se encontrará cómodamente sentado y además tendrá espacio para ubicar su cuaderno y útiles.

Espacio entre una estación y otra: 0.4 mtrs. Se considera este espacio como mínimo para el libre tránsito de los alumnos que ingresan y se retiran de las estaciones, es decir, ubicarse para sentarse sin problema.

Espacio total ocupado por cada estación: 1 mtrs. Es la suma del espacio usado por la estación de trabajo y el espacio considerado para el acceso de los alumnos a la estación de trabajo.

Distribución: se recomienda distribuir las estaciones de trabajo de manera que los alumnos queden cómodamente ubicados y distribuidos en forma de “U”, ya que esto permite ahorrar en implementación del cableado y la construcción de los muebles, este tipo de distribución se presenta en el siguiente flujo grama espacial:

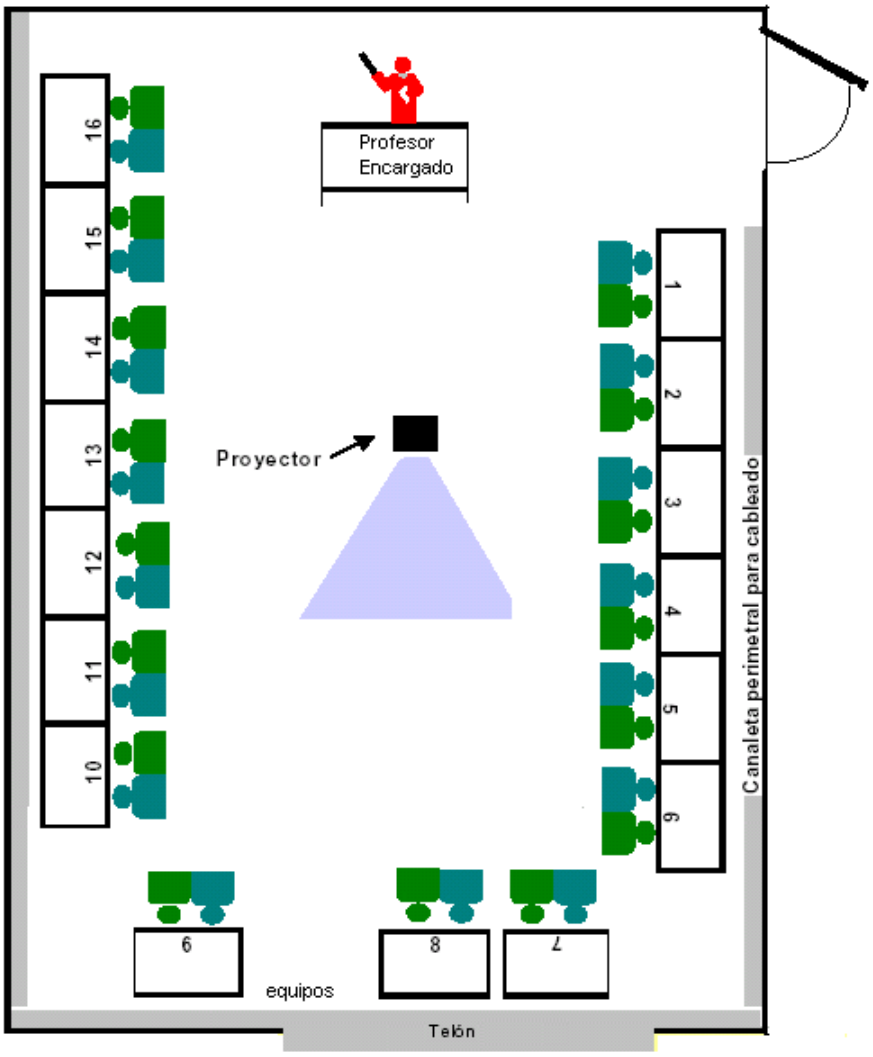


Fig. 3.2- Distribución de estaciones de trabajo

3.2.3 Proveedores de Hardware

Se proveerá de insumos y productos de hardware de empresas mayoristas que se dedican a este rubro, entre las cuales están:

- Refly Chile, importador mayorista en computadores reacondicionados de fábrica
- PC Factory Empresa mayorista de productos e insumo
- Computer Center: Empresa minorista de productos, insumos y reparaciones computacionales

- Minicentro, importador de productos e insumos computacionales
- Electrocom, importador de productos e insumos eléctricos

3.2.4 Mano de Obra

Para realizar la adaptación de la sala, construcción de muebles y su respectiva instalación se requiere de un maestro carpintero cuyo costo esta considerado en la planilla administrativa del colegio (ya que este cuenta con un maestro carpintero), sin embargo para la realización del cableado eléctrico, el cableado estructurado y configuración de equipos se requiere de personal altamente capacitado para realizarlo, que para el caso de este proyecto, lo realizaron los alumnos tesistas Sergio Alarcón y Jaime Sánchez .

Costos de la mano de obra:

- Los costos de realizar una instalación de tendido eléctrico estructurado por estación (canalización y enchufes para un equipo) es de $8.000.
- Los costos de implementar un cableado de red estructurado y certificación por estación (tendido de red, y caja de punto de red) es de $ 20.000
- La configuración de cada equipo de red (router y swicht) tiene un costo de : 10:000
- La configuración y programación de cada estación de trabajo tiene un costo de : $10.000

3.3 ESTUDIO DE FACTIBILIDAD

3.3.1 Factibilidad Técnica

En la actualidad se pueden encontrar variados equipos y dispositivos de red adecuados para implementar cualquier tipo de red de datos, esto se debe a que la relación entre plataformas de hardware, sistemas operativos y redes de comunicación de datos no sólo es muy estrecha, sino que cada uno de ellos se fundamenta en el otro, mediante un proceso de integración, generando así una distribución funcional de recursos que permite optimizar la conectividad de cada usuario

de la red, esto es razón por el cual se considera que el proyecto de implementación de red es fundamental para la aplicación práctica y es viable desde el punto de vista técnico.

Como la red a implementar presenta un diseño operacional no complejo, mas aún ésta se presenta distribuida en 2 zonas de red, por lo que la canalización en los edificios a intervenir con el cableado no tendrá mayor costo y menos necesidad de perforar ni cambiar las estructuras existentes debido a que los edificios presentan canalización entre el hormigón, facilitando el cableado , además no se necesitará personal técnico externo para su mantención, puesto que existirá, permanentemente, un profesor del área de computación que podrá solucionar problemas típicos de PC`s y redes.

3.3.2 Factibilidad Económica

Como todo proyecto de diseño de una red, al implementarlo, siempre tiene implicado costos, tales como mano de obra para realizar el cableado, diseño de muebles para las estaciones de trabajo, adquisición de equipos, configuración y mantención, pero todo esto surge a partir de la necesidad de compartir los diversos recursos informáticos, entre distintos sectores de un lugar, es decir, suministrar los diversos servicios de red a cualquier punto o puesto de trabajo ubicado en un edificio, por lo que se justifica que la implementación de la red tendrá costo.

Sin embargo, el costo que generará la implementación del diseño de red propuesto, es relativamente bajo, ya que el hardware que requerirá la red será adquirido en una empresa de venta de equipos reacondicionados. Además la institución en la cual se implementará cuenta con recursos necesarios para realizar el proyecto, es por este motivo y de acuerdo a lo antes mencionado se considera que económicamente el proyecto es factible de realizarlo.

3.4 DISEÑO DE LA RED DE ACCESO MÚLTIPLE

3.4.1 Principios para la Arquitectura de red

Para proponer una arquitectura de red es necesario comprender los requerimientos mínimos necesarios que se necesitan para construir un sistema integrado de conectividad, es por esto que se sugieren los siguientes aspectos técnicos generales que debería poseer la arquitectura de la red, estos son:

- La Arquitectura principal de red se desarrolla con el objetivo de entregar soporte interactivo de información, esto significa que debe ser capaz de entregar conectividad a alta velocidad, por lo consiguiente se debe diseñar esta estructura principal para soportar múltiples usuarios conectados simultáneamente integrando puntos de acceso cableados e inalámbricos.
- Para dar integridad, flexibilidad y expansión al troncal de red, se propone usar un equipo distribuidor profesional switch Ethernet que proporcione rapidez en conectividad permanente a 100Mbps a todos los usuarios conectados al sistema, cable categoría 5e de baja perdida y una conexión de Internet de 1Mbps
- Para establecer parámetros de control de acceso, administrar el flujo de información a través de un enlace de Internet y direccionar usuarios conectados al sistema se debe utilizar un equipo Router con capacidad WLan integrado lo que permitirá cubrir gran parte del espacio físico con señal de conectividad inalámbrica.

3.4.2 Arquitectura de Red Existente

El establecimiento se ha divido en dos zonas de red principales; la primera zona esta constituida por salas y laboratorios, incluyendo la sala de computación, la segunda se destaca por integrar oficinas administrativas, biblioteca (segundo piso) y oficinas de recepción, inspectoría y UTP (primer piso). En la oficina administrativa (secretaria) se encuentra el nodo de conexión a Internet, el cual permite conectar mediante cableado no estructurado toda la segunda Zona, sin embargo, están conectados solo los equipos administrativos y el PC de biblioteca. Entre estas

zonas de red no existe conexión debido a que se encuentran a una distancia superior a 100 mtrs, por lo que se propone tener 2 conexiones a Internet para poseer 2 enlaces permanentes.

La arquitectura de red existente en la primera zona del establecimiento se desarrollo en base a un proyecto enlaces, el cual consiste en una pequeña red de 6 puntos de conexión de computadores, sin conexión a Internet, sin embargo la implementación de esta red proporcionaba un punto de conexión en la sala de profesores, ubicada a unos 40 mtrs de la red principal, punto que esta operativo lo que facilitará cubrir de mejor manera parte del establecimiento en el diseño definitivo de la red.

A partir de la información recolectada y posteriormente analizada, se comenzó a desarrollar el prototipo de red, para esto se requieren diferentes tipos de dispositivos para la red alámbrica e inalámbrica.

3.4.3 Primera Etapa: Proyección Laboratorio computación

Esta zona se caracterizará por concentrar gran numero de puntos de acceso, debido a que se encuentra la sala de computación, para esta se sugiere utilizar un multiplicador switch de 48 bocas que permitirá abastecer y proyectar la capacidad de puntos de conexión a la red con 100 Mbps en esta sala y con una conexión a Internet de 2Mbps. Para asignar direcciones IP se necesita de un Router con capacidad inalámbrica configurado para entregar direccionamiento usando DHCP, además este equipo deberá proporcionar conectividad inalámbrica a 54Mbps en un radio de 100 mtrs, esto permite cubrir las salas de clases con señal inalámbrica y dar conectividad a gran parte del establecimiento. En el siguiente esquema se puede apreciar la arquitectura de red para la sala de computación:

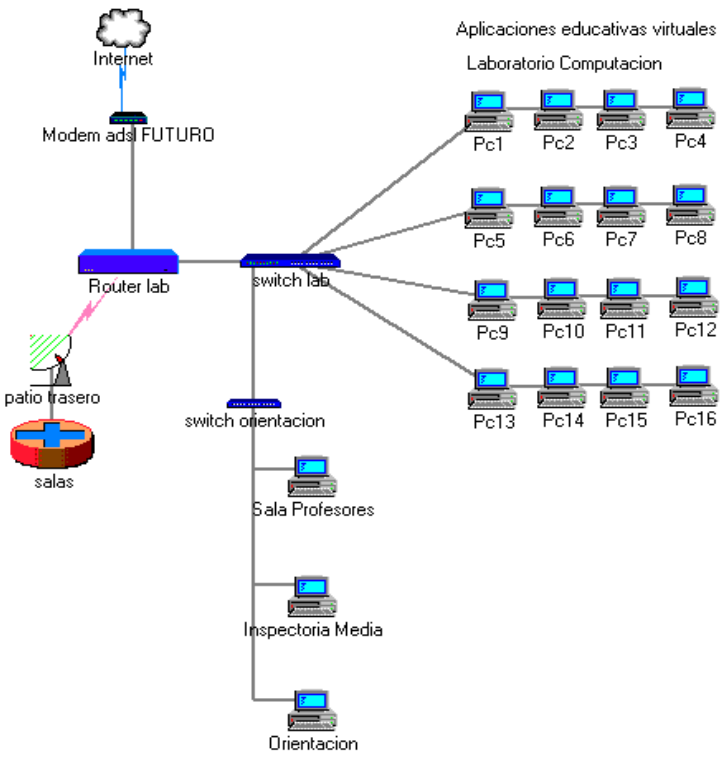


Fig. 3.3- Arquitectura de red de Sala de computación

3.4.4 Segunda Etapa: Proyección Edificio Biblioteca

En esta etapa se requiere estructurar el cableado existente y optimizar la conexión a Internet de 300Kbps a 1Mbps, además para asignar direcciones IP se debe utilizar un Router con Wlan integrado que permitirá cubrir la zona que no puede abarcar el Router de la sala de computación, de esta manera se da conexión inalámbrica en oficinas administrativas, biblioteca y salas de clases. Para mejorar el funcionamiento de biblioteca se proyecta instalar estaciones de trabajo (PC`s) que permitan el desarrollo de una referencia electrónica.

Para implementar referencia electrónica se sugiere instalar un switch de 16 bocas a 100Mbps y estructurar el cableado cat5 para los puntos de acceso distribuidos en biblioteca. La arquitectura que deberá poseer esta zona de red es la siguiente:

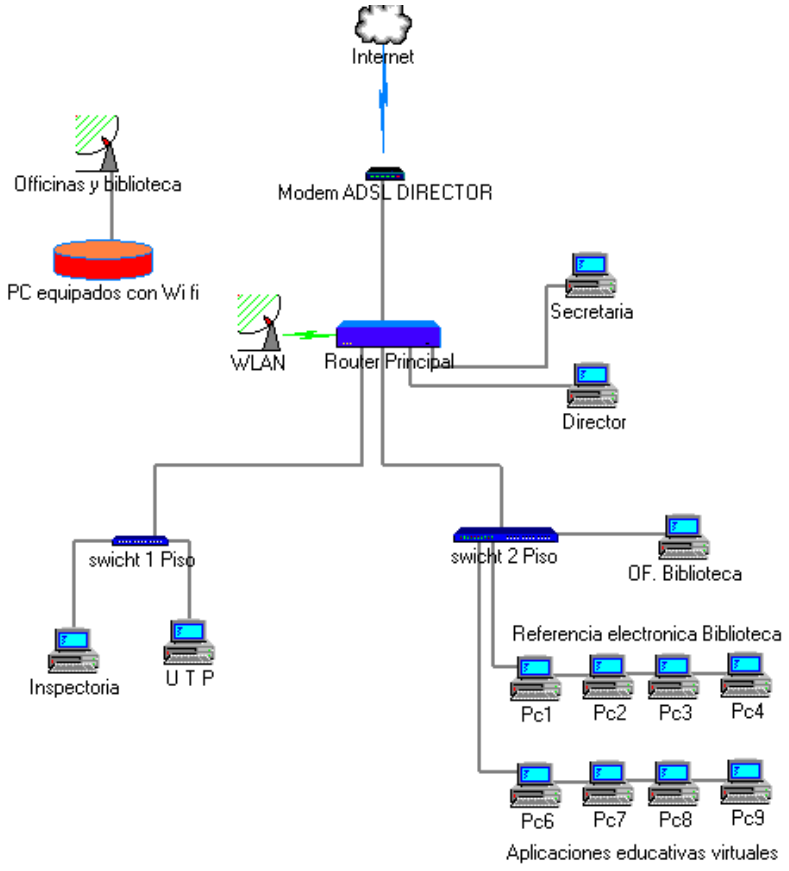


Fig. 3.4- Arquitectura de Red Edificio Biblioteca

3.5 APLICACIONES VIRTUALES

Las complejidades que se perciben de los sistemas de información constituyen un impedimento para que los usuarios los adopten ampliamente. La convergencia entre la computación y las comunicaciones han impulsado un crecimiento continuo, pero tal crecimiento obliga a encontrar nuevas formas de entregar y administrar la información. Esto significa generar un nuevo concepto, la virtualización, que se puede utilizar para ofrecer a los usuarios finales sistemas que sean tan fáciles de usar como el equipo electrónico de consumo.

Las plataformas virtuales prometen hacer que los PC del futuro sean más autónomas, confiables y seguras, convirtiéndolas en una herramienta casi imperceptible en nuestra vida cotidiana y por sobre todo en torno al aprendizaje. La virtualización de plataformas es un habilitador clave de los nuevos modelos de uso diseñados para hacer de estas metas una realidad.

La virtualización se define como la creación de un sistema de cómputo dividido de forma lógica que se ejecuta sobre una plataforma presente. Aunque la virtualización se ha aplicado al almacenamiento y a los servidores, el concepto de virtualización se extiende para incluir todas las capas de la plataforma; desde las aplicaciones y el software operativo hasta los componentes, procesadores e interconexiones de la plataforma.

Los usuarios perciben las plataformas virtuales como si fueran sistemas físicos, desde este punto de vista, las plataformas virtuales ofrecen una técnica extremadamente sólida y de fácil transporte que ocultan la complejidad a los usuarios y a la vez mejoran la seguridad del sistema.

En este sentido, la virtualización es una forma para crear sistemas menos complejos, entrega más seguridad a los sistemas, las redes y las aplicaciones gracias a la separación de las aplicaciones potencialmente vulnerables y de otras plataformas virtuales.

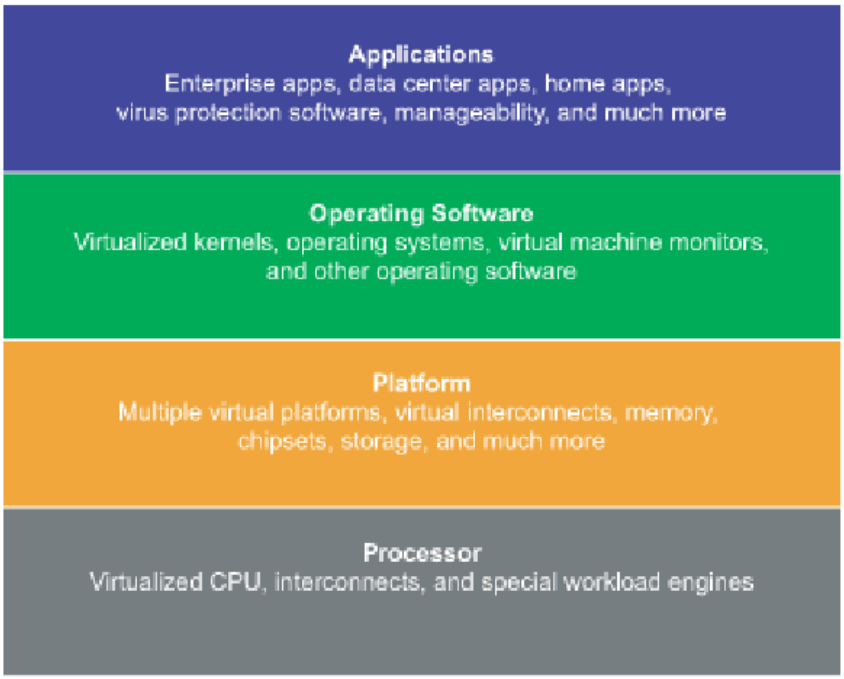


Fig.3.5- Niveles de representación de aplicaciones virtuales

Tal como se ve en la figura la virtualización está incorporada a cada capa del sistema de cómputo del PC, desde las aplicaciones hasta los componentes, las interconexiones y los procesadores de la plataforma.

Por lo anterior, vemos que variados sistemas pueden transformarse en plataformas virtuales, es por esto que abarcaremos en esta investigación solo aquellas plataformas virtuales dedicadas al aprendizaje y enseñanza, como aplicación a la implementación de la red con acceso múltiple.

3.5.1 Enciclopedias Virtuales

Una enciclopedia virtual es recopilación de información de diferentes temas que se presentan en variados formatos, en general, se utiliza lenguaje java para facilitar el diseño de las plataformas que permitan una mejor operabilidad por parte del usuario y fácil acceso a la información contenida, un ejemplo de ello es Wikipedia (www.wikipedia.org), que en un diseño de enciclopedia virtual tipo pagina Web permite mediante un buscador encontrar fácilmente la información almacenada en dicho servidor, a continuación vemos una imagen de lo que es Wikipedia:

Fig. 3.6- Bienvenida Enciclopedia Wikipedia

Como se observa, esta plataforma virtual es amigable, dado a que permite acceder rápidamente a la información deseada. Existen otras plataformas virtuales, tales como:

- UNCYCLOPEDIA (uncyclopedia.org): La enciclopedia creada en enero del 2005, fue traducida recientemente al español e invita a “escribir sobre el tema que quieras e introducir el artículo.

- ICARITO (www.icarito.cl): La enciclopedia nacional, en formato virtual, que permite encontrar todos los temas relacionadas con las tareas escolares. La información se encuentra ordenada por temas o si lo prefieres se puede utilizar el buscador que posee.
- CIBERNETICA (www.encyberpedia.com):Todo pero realmente todo lo que se busque se encuentra en esta enciclopedia virtual. Está en inglés y contiene mucha información para aumentar tu conocimiento en los diferentes temas que circulan en la red y el mundo.
- BRITÁNICA (www.britannica.com): Esta enciclopedia británica es la más completa de su estilo, con la última información de los sucesos más importantes en la historia mundial que van sucediendo. Se puede buscar toda la información y se encuentra en inglés.

3.5.2 Google Earth

Una de las plataformas virtuales relacionadas con la ubicación de lugares y representación geográfica, es Google Earth, aplicación que se ocupará regularmente en las sala de computación (primera etapa del proyecto). Esta plataforma virtual en línea requiere de un programa principal que se instala en el computador, y este mediante una conexión a Internet de banda ancha demanda al servidor Google, gran cantidad de imágenes y animaciones que requiere bajar para presentar en forma definitiva una imagen de la zona que se requiera visualizar.

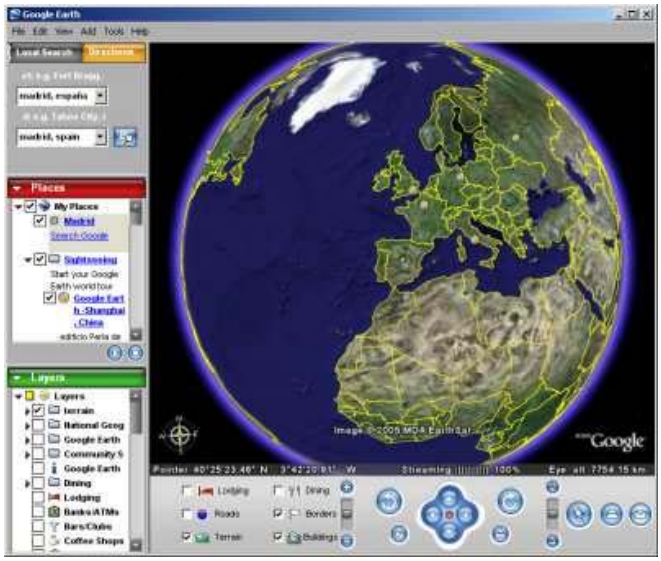


Fig. 3.7- Ventana Principal Google Earth

La interfaz es amigable y permite buscar los lugares mediante coordenadas o simplemente haciendo un zoom en la zona de la tierra que se desea explorar, su visualización puede ser plana o tridimensional (esta función permite observar relieve) como vemos en la siguiente figura:

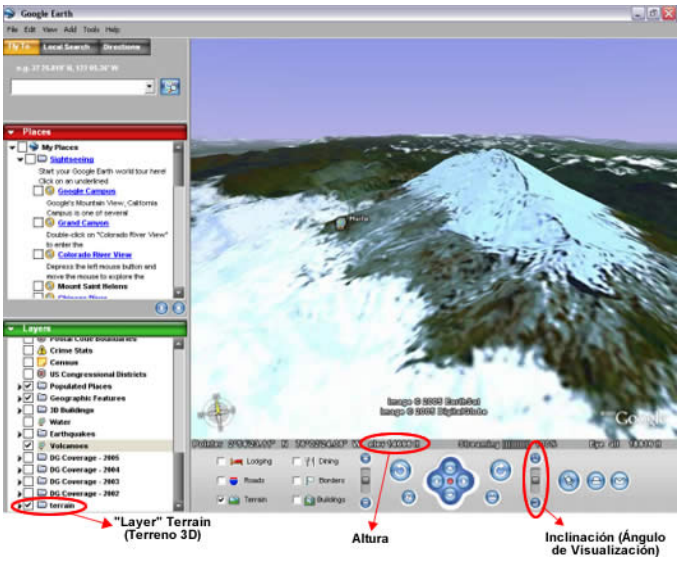


Fig. 3.8- Visualización tridimensional

Google Earth posee las siguientes funciones:

- Observar la Tierra en tres dimensiones y rotar la vista.
- Visualizar paisajes y ciudades en cualquier rincón del planeta, cambiar de un lugar a otro o de un continente a otro.
- Observar e identificar tipos o formas de relieve en cualquier lugar del mundo (volcanes, cordilleras, valles, picos, etc.) y conocer la medida exacta de su altura sobre el nivel del mar.
- Cambiar el ángulo de visualización de un territorio para poder observarlo en perspectiva.
- Conocer las coordenadas de cualquier punto de la Tierra con solo ubicar el ratón sobre el sitio.
- Marcar sitios e imágenes de interés y compartir información sobre ellos con otros usuarios.

Esta aplicación permitirá a los alumnos que están en la carrera “Técnico de nivel medio en servicios de turismo” complementar y consolidar sus conocimientos sobre lugares turísticos y geográficos del planeta.

3.5.3 Grupos

En primer lugar MSN Groups son pequeñas comunidades de usuarios en las que se publican mensajes, se charla y se comparten ideas. Permite publicar fotos digitales en un álbum de fotos en línea o ver las fotos ya publicadas por otros usuarios.

Esta aplicación permitirá a los docentes publicar mensajes para sus alumnos. Desde el propio programa se inicia sesión en el sistema, los alumnos se autentificaran como usuario de dicho grupo para así utilizar los elementos que entrega esta aplicación.

Fig.3.9- Ventana Principal MSN Groups Centro Educacional San Nicolás

CAPITULO IV: IMPLEMENTACION DEL PROYECTO

4.1 PRIMERA ETAPA: laboratorio computación

La implementación estimada de la primera etapa consistente en la sala de computación y puntos de red anexos se realizó en un 80% aproximadamente, estructurando óptimamente el troncal principal que brinda conectividad de red y que permitirá construir en corto plazo la proyección de la red propuesta. Se instaló un router Belkin que permitirá acceso a Internet mediante protocolo IEEE 802.11b/g (Wifi) en forma mixta. Respecto a la LAN cableada se utilizó el protocolo IEEE 802.3 o Ethernet debido a su extensión y escalabilidad.

La red construida esta representada en el siguiente diagrama.

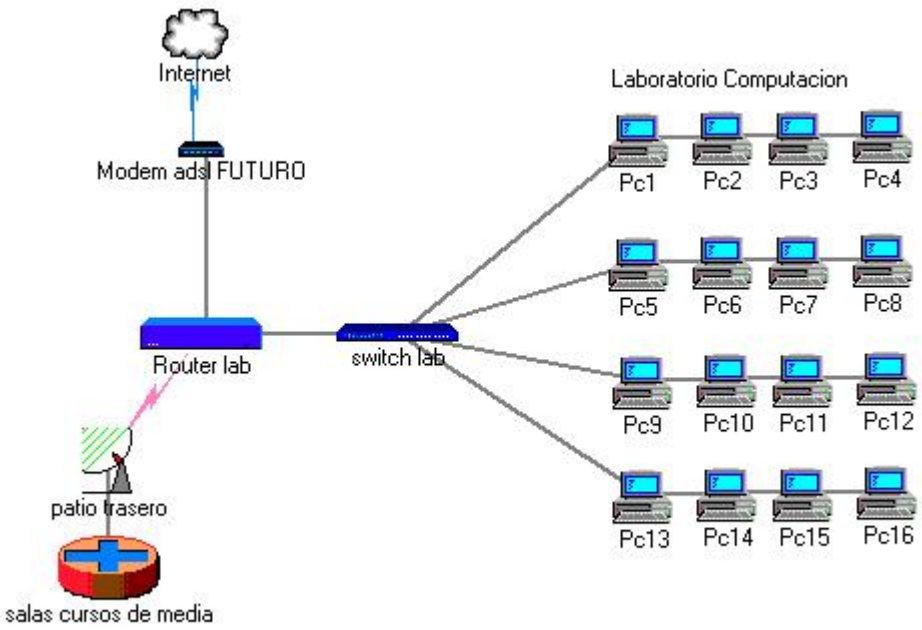


Fig. 4.1- Estructura de red, 1º etapa implementada

Respecto al sistema de cableado se aplicó la norma EIA/TIA 568B. En primera instancia, se realizó el tendido de tuberías y canalización que permitirían el cableado estructurado de la red y energía, para esto se utilizó 30 Mtrs de tubería (1,5 pulg. De diámetro), 130 Mtrs de cable UTP Cat. 5, 15 terminales hembra RJ45, 50 conectores RJ45, y 16 cables UTP Cat. 5 de 3 Mtrs, 12 cajas de 3 enchufes, 20 Mtrs cables Rojo, Verde, Negro respectivamente.

Fig. 4.2- Tendido de tubería para el cable UTP y energía.

La construcción del cableado eléctrico y de red tardo 5 días, tiempo durante el cual se construían los muebles, y posteriormente, éstos se ubicaron en la sala permitiendo la instalación de cada uno de los PC, el resultado de la obra se aprecia en el siguiente cuadro:

Fig. 4.3- Laboratorio computación

4.2 SEGUNDA ETAPA: Edificio Biblioteca

Esta etapa se implemento en un 50%, en lo que se consideró la instalación cableada del primer piso correspondiente a Inspectoría y Utp, en donde se instaló un swicht con norma IEEE 802.3 o Ethernet para así brindar una distribución óptima de recursos de red, y adicionalmente se instaló, en el segundo piso, un router Dlink con soporte a la norma IEEE 802.11b/g en forma mixta que permitirá tener acceso a Internet mediante WiFi.

Debido a que la vialidad económica de realizar cableado estructurado o de instalar tarjetas inalámbricas salía casi lo mismo se tomo la decisión de comprar dispositivos inalámbricos para cada PC. La instalación de cables y conectores se rigió según el estándar EIA/TIA 568B.

En el siguiente cuadro se representa la red implementada.

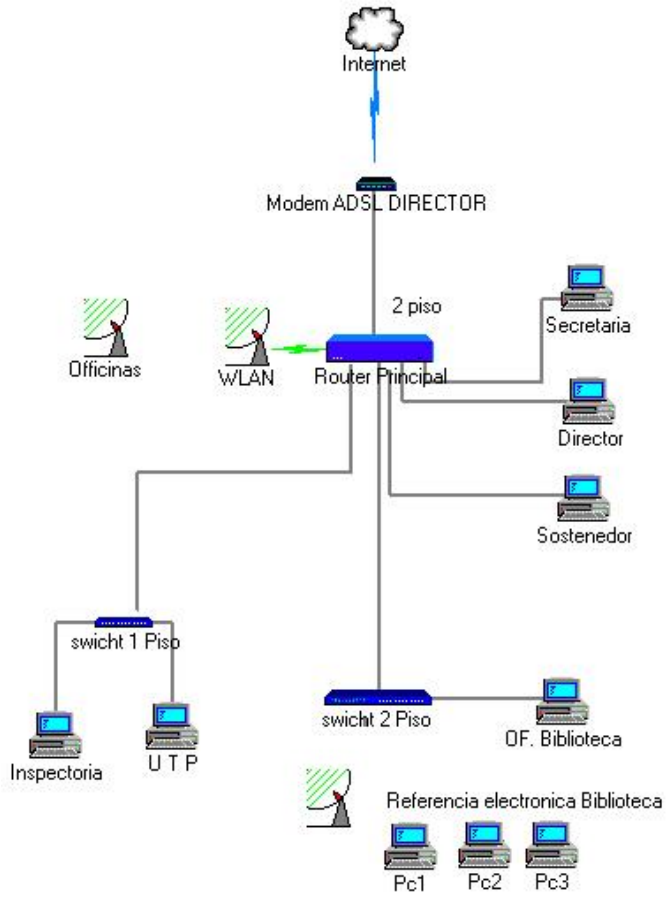


Fig. 4.4- Estructura de red, 2º etapa implementada

4.3 DIRECCIONAMIENTO IP

Primera Etapa

Para el direccionamiento se habilito DHCP en el Router Belkin del Laboratorio de computación, el configurado para asignar direcciones IP es desde 192.168.2.1 hasta 192.168.2.199.

Equipo	Dirección Ip
Router	192.168.2.1
Pc1	192.168.2.2
Pc2	192.168.2.3
Pc3	192.168.2.4
Pc4	192.168.2.5
Pc5	192.168.2.6
Pc6	192.168.2.7
Pc7	192.168.2.8
Pc8	192.168.2.9
Pc9	192.168.2.10
Pc10	192.168.2.11
Pc11	192.168.2.12
Pc12	192.168.2.13
Pc13	192.168.2.14
Pc14	192.168.2.15
Pc15	192.168.2.16
Director Pc 1	192.168.2.17
Director PC2	192.168.2.18

Tabla 4.1- Direcciones IP laboratorio computación

Segunda Etapa

De igual modo para el direccionamiento de las estaciones de trabajo en biblioteca y oficinas administrativas se habilito DHCP en el Router Dlink configurado para entregar direcciones a los usuarios desde la 192.168.0.2 hasta 192.168.0.199, el cual asigno las siguientes direcciones:

Equipo	Dirección Ip
Router	192.168.0.1
Secretaria	192.168.2.2
OF. Sost.	192.168.2.3
OF. Director	192.168.2.4
Of. Utp	192.168.2.5
Of. Inspectoria	192.168.2.6
Biblioteca	
PC1	192.168.2.8
PC2	192.168.2.9
PC3	192.168.2.10

Tabla 4.2- Direcciones IP edificio biblioteca

En el caso de la red Wi-fi (1º y 2º etapa) el usuario que desee conectarse a ella el router asignara alguna dirección disponible en el rango.

4.4 ANÁLISIS USANDO ETHEREAL

A continuación se muestra el análisis efectuado a la red de la primera y segunda etapa, en donde se capturaron paquetes de información y los protocolos involucrados, para esto se utilizó el software Ethereal.

Primera etapa: Sala computación

En esta tabla se aprecia la captura de paquetes realizada en la sala de computación. En esta se observa cada protocolo y el % de paquetes en referencia al total.

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes
⊟ Frame	100,00%	1254	285027	0,007	0	0
⊟ Ethernet	100,00%	1254	285027	0,007	0	0
⊟ Logical-Link Control	13,72%	172	11180	0,000	0	0
Spanning Tree Protocol	11,32%	142	8520	0,000	142	8520
⊟ Internetwork Packet eXchange	2,39%	30	2660	0,000	0	0
NetBIOS over IPX	1,20%	15	1470	0,000	15	1470
IPX Routing Information Protocol	0,80%	10	610	0,000	10	610
Name Management Protocol over IPX	0,40%	5	580	0,000	5	580
⊟ Internet Protocol	75,44%	946	265885	0,007	0	0
⊟ User Datagram Protocol	40,67%	510	74619	0,002	0	0
⊟ NetBIOS Datagram Service	2,39%	30	6561	0,000	0	0
⊟ SMB (Server Message Block Protocol)	2,39%	30	6561	0,000	0	0
⊟ SMB MailSlot Protocol	2,39%	30	6561	0,000	0	0
Microsoft Windows Browser Protocol	2,39%	30	6561	0,000	30	6561
NetBIOS Name Service	28,23%	354	37067	0,001	354	37067
Domain Name Service	5,74%	72	6688	0,000	72	6688
Bootstrap Protocol	4,23%	53	24234	0,001	53	24234
Data	0,08%	1	69	0,000	1	69
⊟ Transmission Control Protocol	34,37%	431	190996	0,005	165	9530
⊟ Hypertext Transfer Protocol	21,21%	266	181466	0,005	249	169679
Line-based text data	1,04%	13	5947	0,000	13	5947
Unreassembled Fragmented Packet	0,32%	4	5840	0,000	4	5840
Internet Group Management Protocol	0,40%	5	270	0,000	5	270
Address Resolution Protocol	10,05%	126	7362	0,000	126	7362
⊟ Internetwork Packet eXchange	0,80%	10	600	0,000	0	0
IPX Routing Information Protocol	0,80%	10	600	0,000	10	600

Fig. 4.5-Ventana de captura de paquetes.

Del total de trafico capturado el 75.44% son paquetes de información con protocolo IP y el 34.37% pertenecen a paquetes TCP.

La siguiente ventana muestra el diálogo de las estaciones de trabajo (address A) de la sala de computación con el resto de la red (address B), lo cual se manifiesta con el envío de broadcast.

Cada PC del laboratorio, al momento de conectarse a la red, transmite un broadcast o paquete de información, lo cual se ve representado en este cuadro, en donde se puede apreciar las direcciones IP de cada host y la cantidad de paquetes que transmite.

Ethernet Conversations

Address A	Address B	Packets ˆ	Bytes	-> Packets	-> Bytes	<- Packets	<- Bytes
192.168.2.1	192.168.2.16	506	198051	248	150517	258	47534
192.168.199.18	Spanning-tree-(for-bridges)_00	142	8520	142	8520	0	0
192.168.2.14	Broadcast	67	6958	67	6958	0	0
192.168.2.13	Broadcast	50	5594	50	5594	0	0
192.168.2.3	Broadcast	49	5534	49	5534	0	0
192.168.2.12	Broadcast	44	5067	44	5067	0	0
192.168.2.16	Broadcast	41	5514	41	5514	0	0
192.168.2.2	Broadcast	40	4470	40	4470	0	0
192.168.2.7	Broadcast	39	4384	39	4384	0	0
192.168.2.11	Broadcast	39	4384	39	4384	0	0
192.168.2.5	Broadcast	35	3842	35	3842	0	0
192.168.2.15	Broadcast	34	3782	34	3782	0	0
192.168.2.10	Broadcast	31	3312	31	3312	0	0
192.168.2.8	Broadcast	27	3022	27	3022	0	0
192.168.2.4	Broadcast	26	2898	26	2898	0	0
192.168.2.9	Broadcast	25	2742	25	2742	0	0
192.168.2.1	Broadcast	25	13690	25	13690	0	0
192.168.2.6	Broadcast	24	2682	24	2682	0	0
192.168.2.16	01:00:5e:00:00:16	5	270	5	270	0	0
192.168.199.18	Broadcast	3	180	3	180	0	0
192.168.2.10	192.168.2.1	2	131	0	0	2	131

Fig. 4.6-Ventana de captura de paquetes ethernet.

Segunda etapa: Edificio Biblioteca

Para la segunda etapa se efectuó el mismo análisis de captura. Se aprecia que el 71.03% del total corresponde a tramas con protocolo IP, y el 28.97% pertenece a datos no provenientes de Internet.

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes
⊟ Frame	100,00%	145	44455	0,002	0	0
⊟ Ethernet	100,00%	145	44455	0,002	0	0
⊟ Internet Protocol	71,03%	103	38050	0,002	103	38050
Transmission Control Protocol	13,10%	19	1254	0,000	19	1254
⊟ User Datagram Protocol	15,86%	23	5151	0,000	0	0
Hypertext Transfer Protocol	15,17%	22	4904	0,000	22	4904
⊟ NetBIOS Datagram Service	0,69%	1	247	0,000	0	0
⊟ SMB (Server Message Block Protocol)	0,69%	1	247	0,000	0	0
⊟ SMB MailSlot Protocol	0,69%	1	247	0,000	0	0
Microsoft Windows Browser Protocol	0,69%	1	247	0,000	1	247
Data	28,97%	42	6405	0,000	0	0

Fig. 4.7-Ventana de captura de paquetes.

4.5 ANALISIS DE SEÑAL USANDO NETSUMBLER

A continuación se describe el análisis efectuado a la señal WiFi de la primera y segunda etapa, en donde con la ayuda del software NetStumbler se evaluó la recepción de intensidad de la señal inalámbrica, la cual es graficada en función del tiempo.

Con respecto a la transmisión de señal, los routers que se utilizaron cumplen con la norma IEEE 802.11 que fija el nivel máximo de potencia permitido:

- 100 mW. Potencia Máxima Radiada. En interior de inmuebles (+20dBm)
- 5 mW. Potencia Máxima Radiada. En exterior de inmuebles (+7dBm)

Primea etapa: laboratorio Computación

Para el análisis de la señal en esta etapa se escogió una sala ubicada a 15 mtrs aproximadamente con respecto al transmisor, debido que el fabricante del dispositivo estima que la propagación "indoors" de la señal es 20 mtrs.

El resultado obtenido se visualiza en el siguiente gráfico:

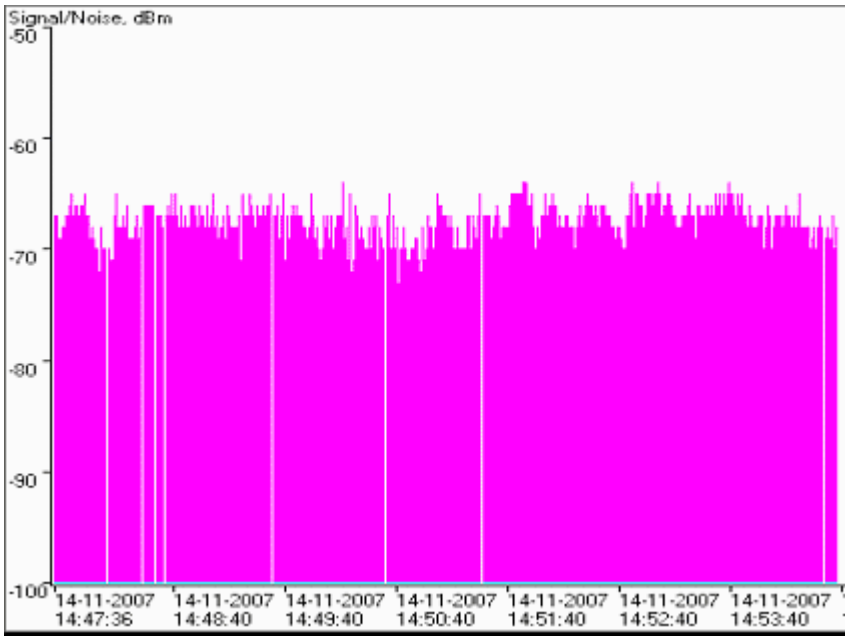


Fig. 4.8-Señal capturada en sala de clases.

Se observa que la señal es estable y no existen variaciones bruscas en su amplitud, posee una magnitud de -66 dBm aproximadamente y si se considera que un receptor común WiFi tiene sensibilidad de unos -84 dBm a 11Mbps entonces la señal recibida es 18 dB superior al mínimo necesario, por lo tanto se concluye que el acceso a Internet podría haberse establecido a la velocidad máxima posible. En este caso se cumple con la norma IEEE 802.11b.

Nota: La sensibilidad de recepción de una señal WiFi suelen manejarse valores de -80 dBm a -96 dBm.

Segunda Etapa: Edificio biblioteca

De igual modo se capturó la intensidad de la señal WiFi en el edificio de biblioteca, en donde el router se ubica en el segundo piso, a diferencia de la primera etapa, en donde el transmisor se encontraba en el primer nivel. Por este motivo se registró una señal menos intensa que la anterior, debida que se produce una atenuación por efecto del diseño estructural del edificio (material de cemento).

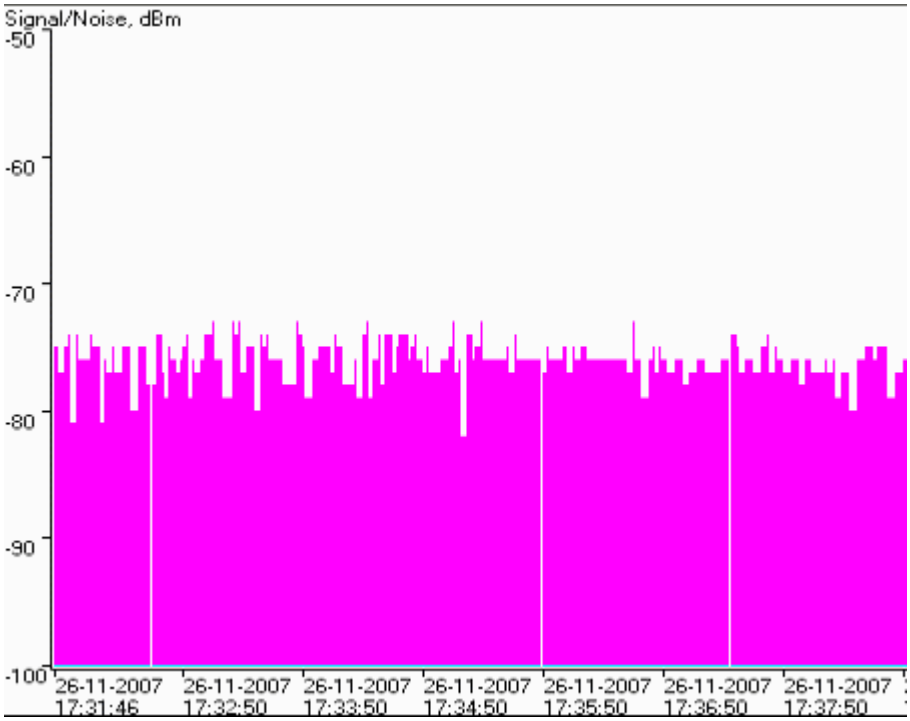


Fig. 4.9-Señal capturada en edificio biblioteca.

Se aprecia una señal estable en el tiempo, ya que no presenta variaciones bruscas en su amplitud. Se registró una magnitud de -74 dBm, y al igual que en el caso anterior, si se considera que un receptor WiFi tiene sensibilidad de unos -84 dBm a 11Mbps entonces la señal recibida es 10 dB superior al mínimo necesario, por lo tanto se concluye que el acceso a Internet podría haberse establecido a la velocidad máxima posible. En este caso se cumple con la norma IEEE 802.11b.

4.6 HARDWARE USADO

Estaciones de trabajo

Debido al uso que tendrá esta red se utilizaron computadores reacondicionados que poseen parte de la última tecnología, ya que solamente se necesitaron estaciones de trabajo que cumplan con los requerimientos mínimos para desarrollar las actividades diarias en el colegio.

Computador	Marca: IBM Factor: Desktop
CPU	Pentium III 1000 Mhz Fsb: 133Mhz
Ram	128 Mb , 133 Mhz
HDD	15 Gb 5400 rpm
Óptico	48 X
Puertos	LPT1, com1,com2, 2xUSB,2 mini din, VGA, Sonido, Red 100 Mb/s
Monitor	Compaq, IBM, Sony de 17" pantalla plana con Protector de radiación integrado
Otros	Teclado compatible y Maus Óptico fujitel

Tabla 4.3- Características técnica de estaciones de trabajo

Fig. 4.10- Computador de laboratorio.

Router

Se utilizaron dos router, para la primera y segunda etapa respectivamente. Cada uno es un router ADSL de fácil conexión, configuración y mantenimiento. Va a permitir que con una sola cuenta de acceso a Internet, puedan conectarse todos los puestos de la LAN a la red pública.

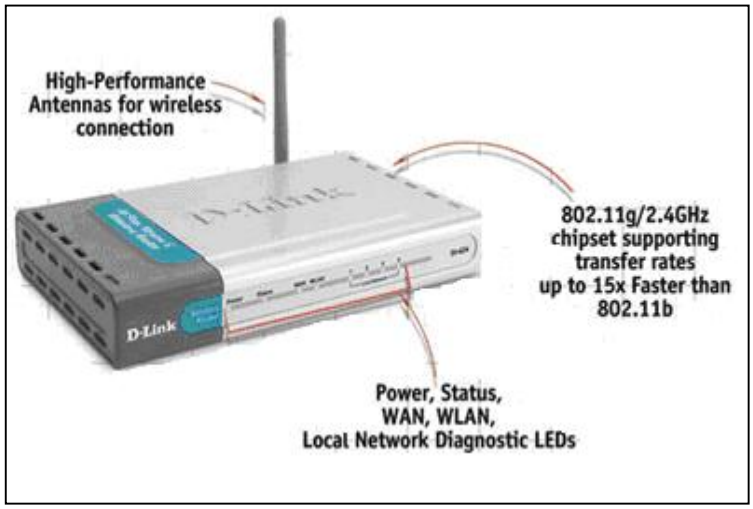


Fig. 4.11- Router primera etapa

Fig. 4.12- Router segunda etapa

Para las estaciones de trabajo será totalmente transparente la conexión con Internet, ya que en el momento que necesiten cualquier servicio de ésta, será el router el encargado de interconectar nuestra LAN con el resto del mundo.

Swicht

En el proyecto se usó un concentrador de 45 tomas RJ45 para la conexión de los distintos nodos y estaciones de trabajo en la etapa de la sala de computación. Este swicht es un equipo reacondicionado del fabricante Dell modelo Power connect serie 3048 que satisface todos lo requerimientos y que permitirá expandir la implementación de la sala de computación lograda en este trabajo. A continuación se aprecia el swicht funcionando:

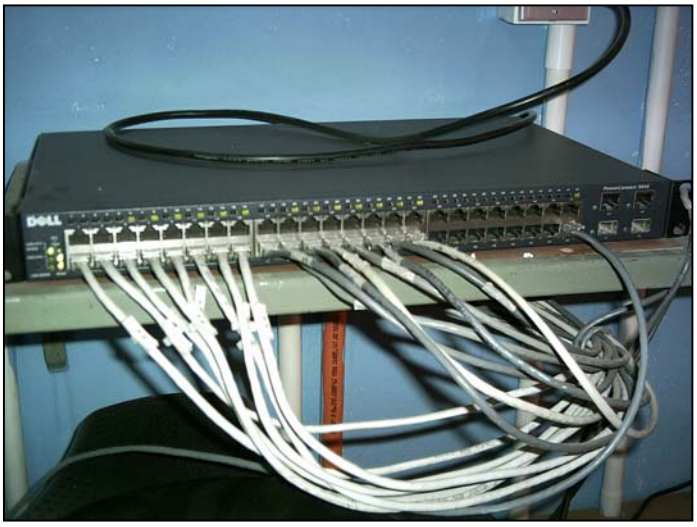


Fig. 4.13- Swicht primera etapa

Módulos hembra nivel 5

En el mercado existen varios tipos de módulos de conexión con sus respectivos conectores. Sin embargo se escogió un modelo de categoría 5.

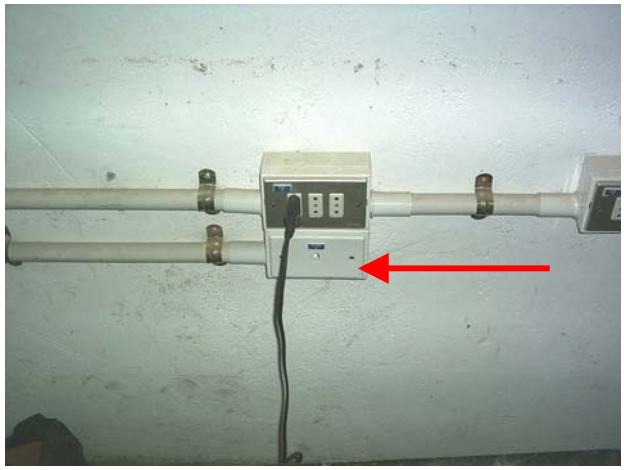


Fig. 4.14- Módulo hembra nivel 5

Conectores RJ-45

Para el presente proyecto se eligió un conector RJ-45 macho de categoría 5 y de la calidad suficiente para que permita contactos seguros.

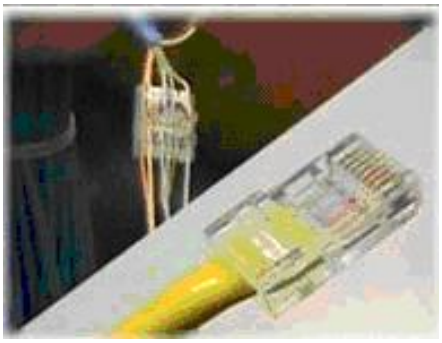


Fig. 4.15- conector RJ45

Cableado

Para el cableado se utilizó el cable par trenzado Nivel Nº 5 sin apantallar. (Cable UTP) debido a sus características de velocidad y costo.

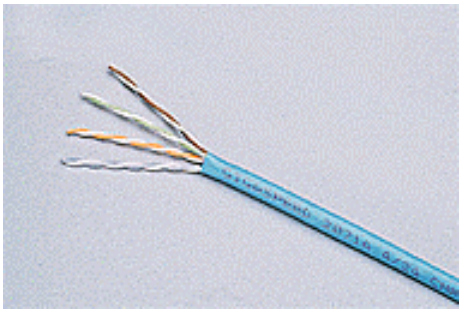


Fig. 4.16- Cable UTP nivel 5

Herramientas adicionales

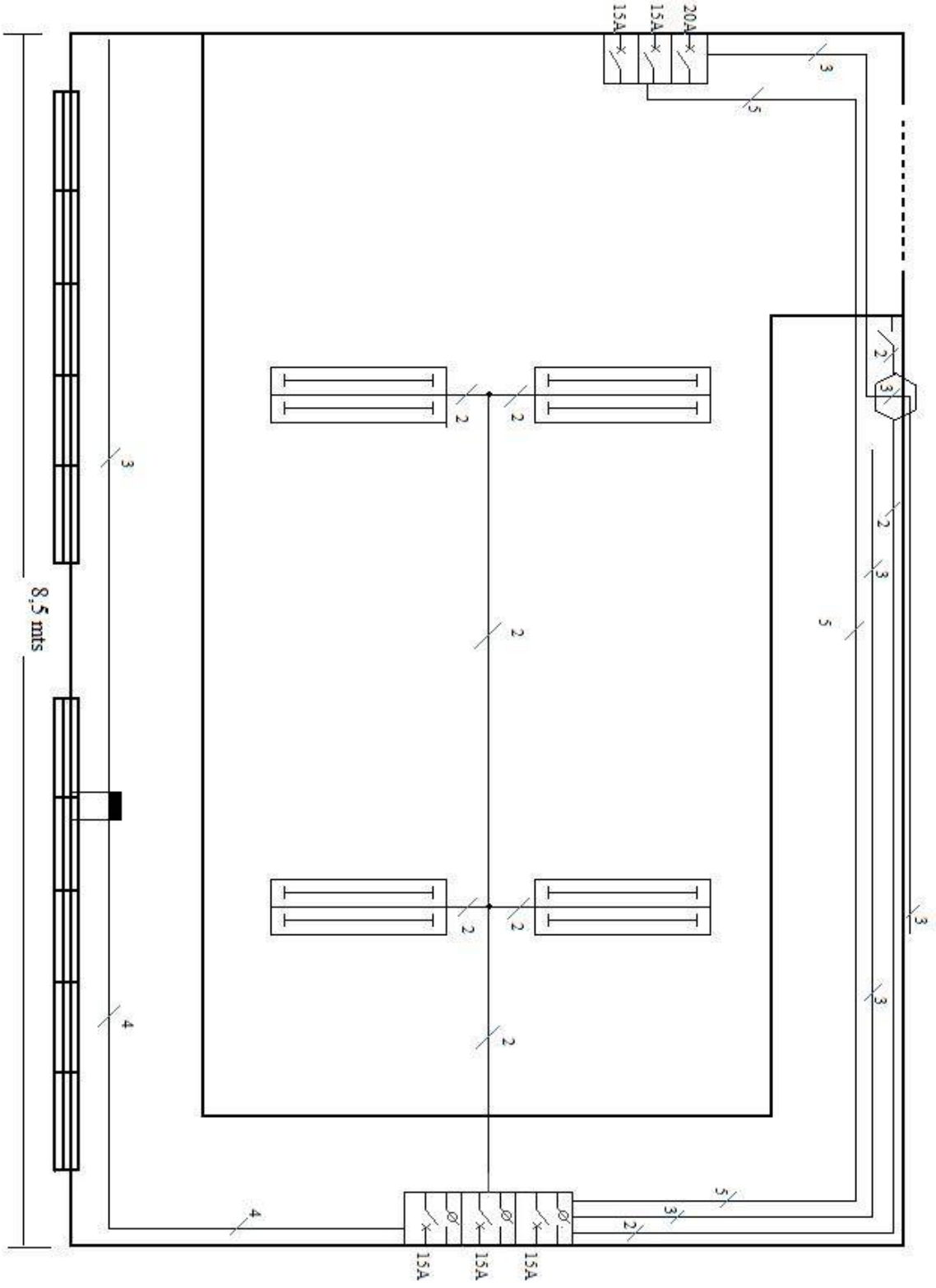
Punch Tool:

Se utilizó esta herramienta para fijar los cables a los conectores RJ45 macho, en donde se inserta a presión cada hilo conductor, de modo que cada punta metálica rompa el plástico y logren hacer buen contacto.

Fig. 4.17- Herramienta Punch Tool.

4.7 PLANO ELÉCTRICO SALA DE COMPUTACIÓN

En el siguiente plano se representa las disposiciones de la instalación eléctrica de la sala de computación.



4.8 PARÁMETRO ELÉCTRICOS SALA COMPUTACIÓN

A continuación se dan a conocer los parámetros eléctricos que fueron medidos en la sala de computación una vez implementada:

Parámetro por PC	**Valor**
Potencia consumida	120 W
Corriente	0,6 A
Voltaje entregado	220 V (50 hz)
Parámetros generales de la sala	
Potencia conectada	1KW
Corriente	16ª
Protecciones	
Barras de Tierra con impedancia de	28 ohms
3 Automático instalado	15ª
3 Automático instalado	10ª
3 diferenciales	10ª

Tabla 4.4- Parámetros eléctricos sala computación

CONCLUSIONES

Al momento de diseñar una red implica tener algunas consideraciones físicas y lógicas, en primera instancia hay que evaluar el entorno y lugares donde se extenderán las distintas conexiones, de este modo se logra determinar la ruta adecuada para el cableado de la red. Además, un aspecto fundamental en el diseño de una red es la cantidad de datos que pueden transmitirse a través de la red, por lo que deber poseer un ancho de banda apropiado.

El laboratorio de computación y el resto de infraestructura de red implementada significan un apoyo y complemento a las actividades académicas de los alumnos y docentes, quienes podrán aprovechar los recursos y utilidades que otorga Internet, lo cual constituye en la actualidad una herramienta de enseñanza integrada en cualquier establecimiento de educación. Adicionalmente esto representa para el Centro de Educación San Nicolás un importante paso en su modernización en el uso de las TIC y promoción de su establecimiento como alternativa educacional.

Se comprendió la relación de las distintas capas del modelo OSI con respecto a la funcionalidad y prestaciones de algunos dispositivos de red, por ejemplo; el switch opera en la capa2 (capa de enlace), envía paquetes en base a las direcciones MAC de los host, por otro lado en la capa 3 (capa de red) se utiliza el router el cual se encarga de encaminar o enrutar los diferentes caminos que puede existir desde una red LAN a la WAN, entre otras cosas. En síntesis, el switch opera únicamente en una red LAN en cambio el router es un dispositivo de mayor cobertura de red y por ende posee mayores funciones.

La red de datos implementada ofrece una cobertura inalámbrica en todo el recinto educacional debido que existen dos transmisores WiFi que cubren la primera y segunda zona respectivamente, esto se suma al tipo de construcción del establecimiento, el cual no produce el fenómeno de Jaula de Faraday. Este efecto se genera cuando existe gran cantidad de material metálico en la estructura de un edificio, lo cual provoca que el campo electromagnético en el interior se desvanezca, sin desaparecer.

Por ultimo, este proyecto de tesis y su respectiva implementación significó una satisfacción personal por haber puesto conocimientos y conceptos de ingeniería a beneficio de una comunidad escolar y docente. Además, representó un desafío desde el punto de vista técnico y lógico, pues no se contaba con experiencia alguna sobre modelamiento de red.

BIBLIOGRAFÍA

[1] Schwartz, Misha, "**Redes de Telecomunicaciones: protocolos, modelado y análisis"**, Addison-Wesley Iberoamericana, Buenos Aires, 1994.

[2] David Muñoz Rodríguez, "**Sistemas Inalámbricos de comunicación Personal"**, Alfaomega, México, 2002.

[3] Stallings, William, "**Comunicaciones y redes de computadores",** Prentice Hall, Madrid, 2000.

[4] Denis Ricardo Cortes Peredo, Alvaro Andrés Vera Schafer, "**Estudio e implementación de Red Multifuncional**", UACH, Valdivia, 2004.

[5] Black, Uyless, "**Redes de computadoras: protocolos, normas e interfases",** Alfaomega Ra-Ma, Santafé de Bogotá, 1999.

Web:

www.stumbler.net
www.earth.google.com
www.redes.com
www.ieee802.org/11
www.wlana.com/learn/80211.htm
www.guw.cl (medición señales wifi)
www.subtel.cl
www.wifichile.cl

ANEXOS

A1. TABLA DE COSTO

La inversión total, para llevar a cabo la implementación del proyecto, fue asumido por el establecimiento educacional San Nicolás.

En primera instancia se efectuó la compra de los componentes que se mencionan en la siguiente tabla:

Detalle	Cant.	Precio	Total
COMPUTADOR REACONDICIONADO IBM NETVISTA PIII 1000	12	$ 50,413	$ 604,956
COMPUTADOR REACONDICIONADO HP VECTRA PIII 1000 MHZ	3	$ 49,579	$ 148,737
TARJETA USB INALAMBRICA	4	$ 16.500	$ 66.000
ROUTER D-LINK WIRELESS 108G DI-624 4 PUERTAS	1	$ 41,077	$ 41,077
SWITCH 16 PUERTAS 10/100 DELL REACONDICIONADO	1	$ 20.000	$ 20.000
SWITCH 48 PUERTAS 10/100 DELL REACONDICIONAD	1	$ 33,605	$ 33,605
MONITOR REACONDICIONADO SVGA 17" GRADO A B EIGE P/P	15	$ 20,160	$ 302,400
TECLADO ESPAÑOL FUJITEL PS2 BEIGE MODELO 2282P	15	$ 2,674	$ 40,11
MOUSE FUJITEL OPTICO PS2 986 NEGRO PLATA	15	$ 3,114	$ 46,710
CABLE PODER 220 VOLT 3 PIN TIPO NACIONAL	30	$ 790	$ 23,700
SERVCIO DE EMBALAJE	30	$ 2,527	$ 75,810

SUBTOTAL	$1,353,605
DSCUENTO 10%	$135,360
NETO	$1,218,244
I.V.A	$231.466
TOTAL(1)	**$1.449.711**

Posteriormente se efectuó una segunda compra que incluye los siguientes elementos:

Detalle	**Cantidad**	**Precio**	**Total**
Cable red	150 mtrs	$200/mt	$30.000
Conectores	40	$50	$2.000
Caja chuki	20	$250	$5.000
Tubos de PVC	30 mtrs	-	$60.000
Elementos eléctricos	-	-	$ 50.000
Conectores hembra	20	$500	$10.000
Inmobiliario	-	-	$120.000
Computador AMD 2G	5	$160.000	$800.000

TOTAL(2)	**$1.077.000**

Total(1)	$1.449.711
Total(2)	$1.077.000
TOTAL	**$2.526.711**

El costo total que generó la implementación del proyecto fue por un monto de **$2.526.711.**

En la tabla de costo no se consideró el monto de la mano de obra que asciende a un total de $648.000, según lo especificado en el apartado 3.2.4 del Estudio Técnico, debido que la implementación del proyecto fue efectuado por los mismos alumnos tesistas como parte de su trabajo, lo cual significó un importante ahorro de inversión para el establecimiento.

A continuación se muestra el monto total de cada tarea efectuada en la implementación del proyecto.

Tarea por equipo	**Nº equipos**	**Total**
canalización y enchufes	16	$128.000
tendido de red, y caja de punto de red	16	$320.000
configuración y programación	16	$160.000
configuración router y switch	4	$40.000
TOTAL		$648.000

A2. Introducción al Cableado Estructurado

El cableado estructurado está diseñado para usarse en cualquier cosa, en cualquier lugar, y en cualquier momento. Elimina la necesidad de seguir las reglas de un proveedor en particular, concernientes a tipos de cable, conectores, distancias, o topologías. Permite instalar una sola vez el cableado, y después adaptarlo a cualquier aplicación, desde telefonía, hasta redes locales Ehernet o Token Ring.

El cableado estructurado recibe nombres distintos para cada tipo de aplicación, aunque popularmente se generaliza y se le conoce con el nombre de P.D.S. Los nombres reales son:

- P.D.S. Sistemas de Distribución de Locales
- I.D.S. Sistemas de Distribución de Industria
- I.B.S.Control de Seguridad y Servicios

Un sistema de cableado estructurado es físicamente una red de cable única y completa. Con combinaciones de alambre de cobre (pares trenzados sin blindar UTP), cables de fibra óptica bloques de conexión, cables terminados en diferentes tipos de conectores y adaptadores.

Otro de los beneficios del cableado estructurado es que permite la administración sencilla y sistemática de las mudanzas y cambios de ubicación de personas y equipos. Tales como el sistema de cableado de telecomunicaciones para edificios que presenta como característica saliente de ser general, es decir, soporta una amplia gama de productos de telecomunicaciones sin necesidad de ser modificado.

La norma garantiza que los sistemas que se ejecuten de acuerdo a ella soportarán todas las aplicaciones de telecomunicaciones presentes y futuras por un lapso de al menos diez años. Esta afirmación Puede parecer excesiva, pero si se tiene en cuenta que entre los autores de la norma están precisamente los fabricantes de estas aplicaciones.

Elementos principales de un cableado estructurado:

- Cableado Horizontal
- Cableado del backbone
- Cuarto de telecomunicaciones
- Cuarto de entrada de servicios

A3. Estándares

Todo el cableado estructurado está regulado por estándares internacionales que se encargan de establecer las normas comunes que deben cumplir todos las instalaciones de este tipo. Las reglas y normas comentadas en secciones anteriores están sujetas a estas normas internacionales.

Existen tres estándares:

- ISO/IEC-IS11801 que es el estándar internacional,
- EN-50173 que es la norma europea y
- ANSI/EIA/TIA-568A que es la norma de EE.UU.

Éste último es el más extendido aunque entre todas ellas no existen diferencias demasiado significativas.

Todas ellas se han diseñado con el objeto de proporcionar las siguientes utilidades y funciones:

- Un sistema de cableado genérico de comunicaciones para edificios comerciales.
- Medios, topología, puntos de terminación y conexión, así como administración, bien definidos.
- Un soporte para entornos multiproveedor multiprotocolo.
- Instrucciones para el diseño de productos de comunicaciones para empresas comerciales
- Capacidad de planificación e instalación del cableado de comunicaciones para un edificio sin otro conocimiento previo que los productos que van a conectarse.

La normativa aceptada en Chile es la dictada por la EIA/TIA, con las normas que se indican en la tabla siguiente:

NORMA	SIGNIFICADO
TIA/EIA 569	Normas de edificios comerciales para espacios y vías de telecomunicaciones.
TIA/EIA 607	Requerimientos de puestas a tierra para telecomunicaciones en edificios comerciales
TIA/EIA 568A	Normas de cableado para telecomunicaciones en edificios comerciales
TIA/EIA 606	Normas de administración para infraestructura de telecomunicaciones en edificios comerciales
TIA/EIA TSB-67 UTP	Pruebas de desempeño para sistemas finales.
TIA/EIATSB-72	Guía de instalación para fibra óptica centralizada.
TIA/EIA TSB-75	Pràcticas adicionales para cables horizontales en oficinas abiertas.
TIA/EIA 568 A1	Especificaciones para los retardos en la propagación.

Tabla A1- Normativa en Chile

A4. Norma ANSI/TIA/EIA-568-A,

La norma central que especifica un género de sistema de cableado para telecomunicaciones es la norma **ANSI/TIA/EIA-568-A**, "Norma para construcción comercial de cableado de telecomunicaciones". Esta norma fue desarrollada y aprobada por comités del Instituto Nacional Americano de Normas (ANSI), la Asociación de la Industria de Telecomunicaciones (TIA), y la Asociación de la Industria Electrónica, (EIA) La norma establece criterios técnicos y de

rendimiento para diversos componentes y configuraciones de sistemas. Además, hay un número de normas relacionadas que deben seguirse con apego.

La norma ANSI/TIA/EIA-568-A publicada en Octubre de 1995 amplio el uso de Cable de Par Trenzado (UTP) y elementos de conexión para aplicaciones en Redes de Area Local (LAN) de alto rendimiento. La edición de la ANSI/TIA/EIA-568-A integra los Boletines Técnicos de Servicio TSB 36 y TSB 40A los cuales prolongan el uso de Cable de Par Trenzado (UTP) en un ancho de banda de hasta 100 Mhz.

Esto permite el uso de Modo de Transferencia Asincrona (ATM), Medio Físico Dependiente del Par Trenzado (TP-PMD), 100Base-Tx y otras 100 Mbps o transmisiones superiores sobre UTP.

Alcance:

La norma EIA/TIA 568A específica los requerimientos mínimos para el cableado de establecimientos comerciales de oficinas. Se hacen recomendaciones para:

- Las topología
- La distancia máxima de los cables
- Parámetros de medios de comunicación que determinan el rendimiento
- Las tomas y los conectores de telecomunicaciones.

Se pretende que el cableado de telecomunicaciones especificado soporte varios tipos de edificios y aplicaciones de usuario. Se asume que los edificios tienen las siguientes características:

- Una distancia entre ellos de hasta 3 km
- Un espacio de oficinas de hasta 1,000,000 m2
- Una población de hasta 50,000 usuarios individuales

A5. Cable RJ-45, Par trenzado o CableUTP

Hay 5 categorías de cable UTP (1 a 5), cada una de ellas posee velocidades de transmisión y características propias. Cuanto mayor es el número de categoría, mayor es la velocidad de transmisión soportada por el cable. También cuanto mayor es el número de categoría, mayor es el número de vueltas de sus conductores a lo largo del cableado (están trenzados o retorcidos). La categoría de cable UTP que soporta mayores velocidades de transmisión, además de ser la más moderna y usada actualmente es la 5, esta categoría es la que conviene usar hoy en día, pues sus costos han descendido mucho y están al alcance de cualquier uso que se le quiera dar, inclusive los instaladores de cableado la usan para hacer las instalaciones telefónicas.

Durante la instalación del cableado no es conveniente usar cables y conectores (hembra y macho) de diferentes categorías, pues el rendimiento de la instalación será equivalente al de la categoría de menor performance, debido a que ésta hace de cuello de botella para las demás. El número de categoría al que pertenece el cable UTP viene especificado en su cubierta plástica externa. Por ejemplo, en un cable de categoría 4, aparecerá regularmente a lo largo de éste, la inscripción “CAT 4”. Las principales características de las categorías del cable UTP son:

- **Categoría 1:** Se utiliza para transmitir voz en instalaciones telefónicas.
- **Categoría 2:** Es el cable UTP más económico que hay para la transmisión de datos en la red.
- **Categoría 3:** Es usado en antiguas redes Ethernet y Token Ring. Soporta velocidades de hasta 10 Mbps (Megabits por segundo) en redes Ethernet 10 BaseT.
- **Categoría 4:** Se usa en redes Ethernet y (Token Ring de 16 Mbps). La máxima velocidad de transmisión soportada es de 20 Mbps.
- **Categoría 5:** Es más moderno y costoso. El 50 % de las redes de área local “LAN” actuales lo utilizan. Puede usarse en el ámbito de las Categorías anteriores. Exige que la longitud máxima sin trenzar no supere los 13 milímetros. Soporta arquitecturas Ethernet, Fast Ethernet, Atm, Token Ring. La máxima velocidad de transmisión soportada es de 100 Mbps.

Categoría 5, 6 ó 7: Cualquiera de estas tres Categorías constituyen una mejora de la categoría anterior (la 5) y pueden transmitir datos a 1 Gbps (Gigabits por segundo).

El cable UTP tipo5 se refiere a que dicho cable se compone de 8 hilos conductores de cobre. Es un cable compuesto desde fuera hacia dentro, de una funda de plàstico habitualmente de color gris, tras la cual se encuentran 8 hilos de cobre cubiertos de una funda plàstica cada uno y entrelazados en pares dando dos vueltas y media por pulgada (De ahì su nombre Par trenzado).

No es para garantizar el funcionamiento de una aplicación específica. Es el equipo que se le conecte el que debe usar o no todo el Bw permitido por el cable.

Cuando se certifica una instalación en base a la especificación de “Categoría 5” se lo hace de Punta a Punta y se lo garantiza por escrito.

Los parámetros eléctricos que se miden son:

- Atenuación en función de la frecuencia (dB)
- Impedancia característica del cable (Ohms)
- Acoplamiento del punto más cercano (NEXT-db)
- Relación entre Atenuación y Crostalk (ACR-db)
- Capacitación (pf/m)
- Resistencia en DC (Ohms/m)
- Velocidad de propagación nominal (% en relación C)

Las figuras siguientes muestran cómo se deben conectar los pares de cables de acuerdo a la norma 568A y 568B.

	Posición en que se deben insertar los conductores del cable UTP a los conectores plug RJ-45(macho)							
Convención	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
568A	Blanco con rayas Verde	Verde	Blanco con rayas Naranja	Azul	Blanco con rayas Azul	Naranja	Blanco con rayas Café	Café
568B	Blanco con rayas Naranja	Naranja	Blanco con rayas Verde	Azul	Blanco con rayas Azul	Verde	Blanco con rayas Café	Café

Tabla A2- Posición del cable UTP a los conectores RJ-45 macho

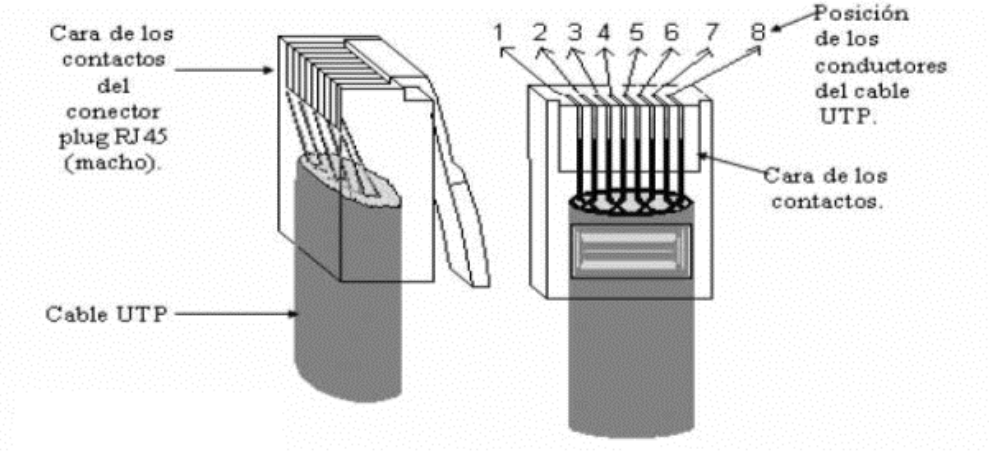


Fig. A1- Posición del cable UTP

A6. Especificaciones IEEE 802.11

En 1997, el Instituto de Ingeniería Eléctrica y Electrónica (Institute of Electrical and Electronics Engineers, IEEE) adoptó la norma 802.11 para los dispositivos inalámbricos que funcionan en la banda de frecuencia de 2,4 GHz. Esta norma incluye disposiciones para tres tecnologías de radio: espectro ensanchado de secuencia directa, espectro ensanchado de saltos de frecuencia e infrarroja. En 1999, el IEEE modificó la norma 802.11 para admitir los dispositivos de secuencia directa que funcionan a velocidades de hasta 11 Mbits/seg. El IEEE ratificó esta norma como norma 802.11b. Los dispositivos que cumplen con la norma 802.11b son compatibles hacia atrás con los dispositivos de secuencia directa 802.11 de 2,4 GHz (que funcionan a 1 ó 2 Mbits/seg). Los canales de frecuencia disponibles varían por dominio de regulación y/o país.

Para 802.11b, hay un solo modelo de radio que se utiliza en todo el mundo.

A continuación se muestra las asignaciones del canal 802.11b.

ID de canal	**World (GHz)**
1	2.412
2	2.417
3	2.422
4	2.427
5	2.432
6	2.437
7	2.442
8	2.447
9	2.452
10	2.457
11	2.462

Tabla A3- Asignaciones de canal 802.11b

También en 1999, el IEEE modificó la norma 802.11 para admitir los dispositivos que funcionan en la banda de frecuencia de 5 GHz. A esta norma se le conoce como norma 802.11a. Los dispositivos que cumplen con la norma 802.11a no son compatibles con los dispositivos 802.11 ni 802.11b de 2,4 GHz. Los radios que cumplen con la norma 802.11a usan una tecnología de radio denominada Multiplexión por división ortogonal de frecuencia (Orthogonal Frequency

Division Multiplexing, OFDM) para alcanzar velocidades de datos de hasta 54 Mbits/seg. Los canales de frecuencia disponibles varían por dominio de regulación y/o país.

Los dispositivos 802.11g operan en la banda de frecuencias 2,4 GHz por medio de una OFDM (multiplexión por división ortogonal de frecuencias) para lograr velocidades de datos de hasta 54 Mbits/ seg. Además, los dispositivos 802.11g son compatibles en forma regresiva con los dispositivos 802.11b. Los canales de frecuencia varían por dominio de regulación y/o país. Los canales 802.11b/g disponibles varían por dominio de reglamentación y/o país. Para 802.11b/g, hay dos modelos: un modelo FCC y un modelo ETSI/MKK (para Europa y Japón). Algunos países restringen la operación de 802.11b/g a bandas de frecuencia específicas. La interfaz de web y CLI siempre presentará los canales disponibles dependiendo del dominio de regulación de las tarjetas. A continuación se muestra las asignaciones del canal 802.11b/g que varían de país a país.

ID de canal	**FCC (GHz)**	**ETSI/MKK (GHz)**
1	2.412	2.412
2	2.417	2.417
3	2.422	2.422
4	2.427	2.427
5	2.432	2.432
6	2.437	2.437
7	2.442	2.442
8	2.447	2.447
9	2.452	2.452
10	2.457	2.457(1)
11	2.462	2.462(1)
12	—	2.467(1)
13	—	2.472(1)

Tabla A4- Asignaciones del canal 802.11b/g

Nota 1: Francia está restringida a estos cuatro canales.

El nivel máximo de potencia permitido no puede sobrepasar el valor de 100 mW (+20 dBm) de Potencia Isotrópica Radiada Equivalente (PIRE). Por otro lado, a nivel nacional, la nota de utilización UN-85 del Cuadro Nacional de Atribución de Frecuencias (CNAF) recoge las normas de uso de la banda de frecuencias de 2.400 a 2.483,5 MHz destinada para uso común.

A7. Ethereal

Ethereal es un analizador de protocolos, utilizado para solucionar problemas de red, análisis, desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos

Todos los administradores de red necesitan tarde o temprano una herramienta que pueda capturar paquetes de la red y analizarlos. En el pasado, estas herramientas eran muy caras, propietarias, o ambas cosas. Sin embargo, con la llegada de Ethereal, todo eso ha cambiado.

Aspectos importantes de Ethereal:

- Es mantenido bajo la Licencia GPL.
- Trabaja tanto en modo promiscuo como en modo no promiscuo.
- Puede capturar datos de la red o leer datos almacenados en un archivo (de una captura previa).
- Tiene una interfaz muy flexible.
- Capacidades de filtrado muy ricas.
- Soporta el formato estándar de archivos tcpdump.
- Reconstrucción de sesiones TCP.
- Se ejecuta en más de 20 plataformas (Linux, Windows, *BSD, Mac OS X, Solaris, etc.).
- Soporta más de 480 protocolos. Puede leer archivos de captura de más de 20 productos

Además, como todo el código fuente de Ethereal está gratuitamente disponible, es muy fácil añadir nuevos protocolos a Ethereal, así como módulos, o modificar el código fuente.

NOTA: Los analizadores de protocolo también son llamados analizadores de paquetes , “packet sniffer” o simplmente sniffer (del inglés “olfateador”).

Uso de Ethereal

Este programa puede hacerse a través del menú de invocación del ambiente gráfico o desde una terminal Unix si no existe la opción en el menú.

En la ventana principal de Ethereal se reconoce tres áreas de despliegue:

Resumen de paquetes capturados, un paquete por línea; uno de ellos ha sido seleccionado como paquete actual (dando clic sobre la línea del paquete). Al desplazarse en la lista y cambiar el paquete actual se actualizan las otras dos ventanas, donde se despliegan en dos formatos diferentes el contenido del paquete.

Detalles de encabezado de protocolos para el paquete seleccionado; los encabezados pueden abrirse (clic en +) para ver mayor detalle, o cerrarse (clic en -) para ocupar sólo una línea.

Datos cruzados del paquete, representación hexadecimal y ASCII del encabezado del paquete seleccionado en el campo del medio.

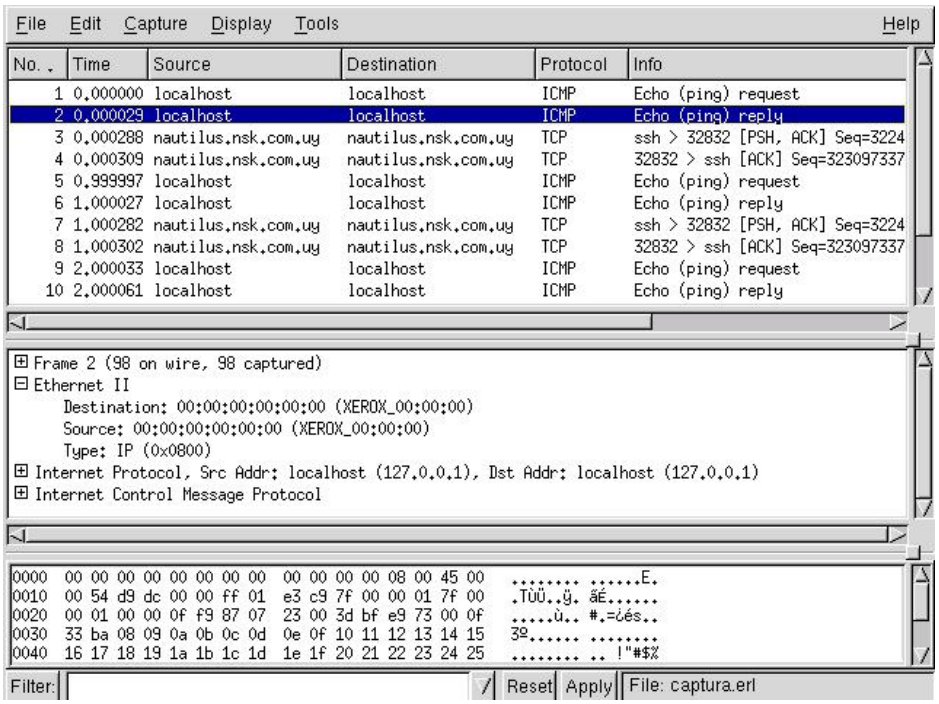


Fig. A2- Filtrado de protocolos

Para iniciar la captura de datos, elegir las opciones de menú Capture: Start (capturar, comienzo). En la ventana de opciones de captura, hay que fijarse al menos la interfaz sobre la que se quiere realizar la captura. Los nombres varían según los sistemas operativos; la interfaz lo (loopback) permite enviar y recibir paquetes en la propia máquina.

Para capturar en un archivo debe indicarse su nombre en el cuadro “Capture file(s)” de la ventana de Opciones de Captura (Capture: Start abre esta ventana).

Estos archivos pueden ser examinados luego con el propio Ethereal mediante la opciòn de menú File: Open. El tráfico ya capturado puede grabarse en un archivo eligiendo File: Print (Archivo: Imprimir); esta opción graba en formato legible (texto).

La ventana de estado muestra en tiempo real la cantidad de paquetes capturados, en total y de algunos tipos corrientes. La situación de captura se mantiene hasta que se presiona el botón Stop. Luego de unos instantes aparecen los paquetes capturados, tal cual se ve en la imagen de la ventana principal. Si se activó la opción de actualizar lista de paquetes en tiempo real (“Update list of packets in real time”) estos se visualizan a medida que son capturados.

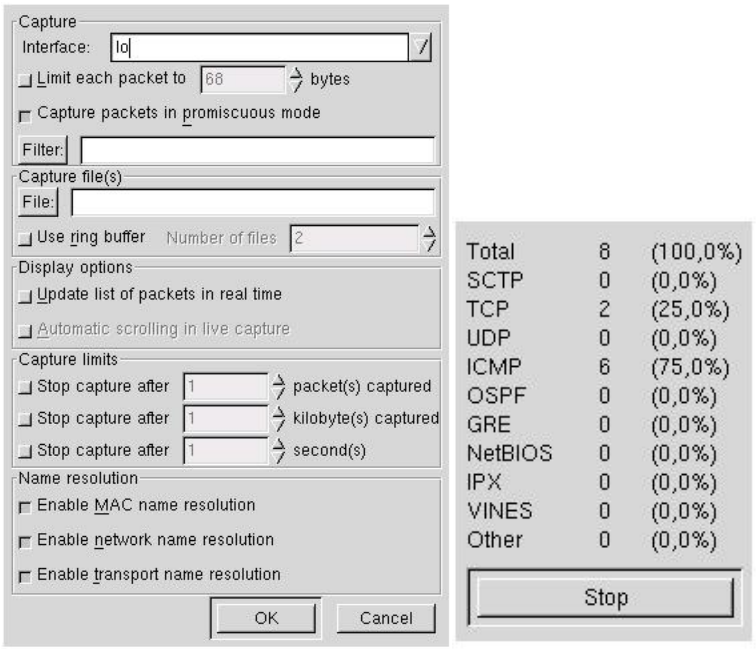


Fig. A3- Opciones y Estado de captura de Ethereal

A8. Network Stumbler

La principal función del software Network Stumbler es tomar control de una tarjeta inalámbrica (Wlan) y usarla como antena para captar todas las señales que se pueden recibir, esto lo realiza dando un inicio de cero para poder monitorear todo tipo de redes.

Es bastante útil para detectar y listar redes. Tiene diferentes características entre ellas la posibilidad de graficar la potencia de la señal. Es muy útil para detectar Puntos de Acceso al observar los niveles de potencia de la red.

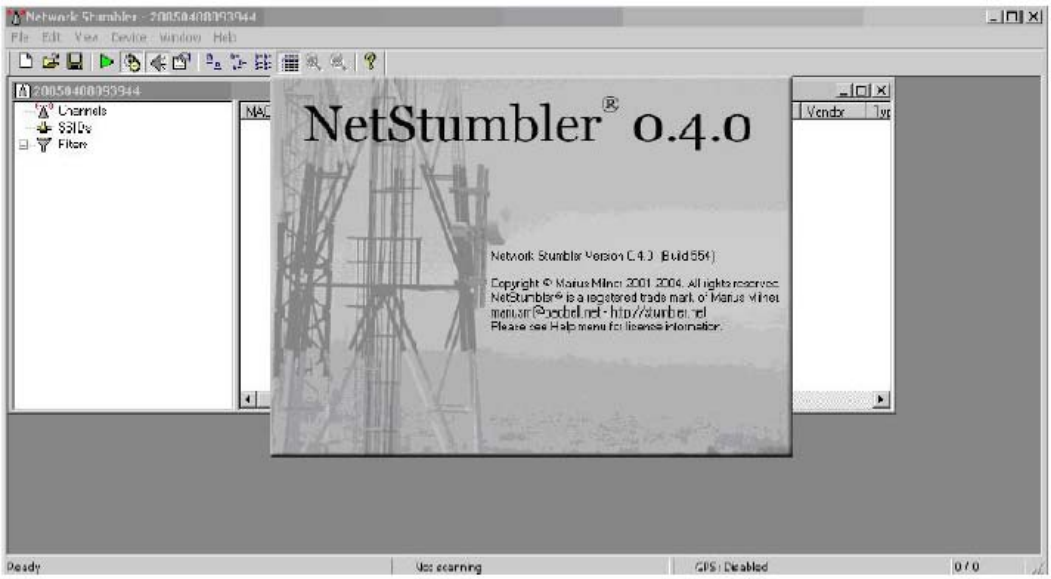


Fig. A4- Bienvenida del NetStumbler

Este programa posee las siguientes funciones:

- Verificar que nuestra red esté bien configurada
- Estudiar la cobertura o señal que tenemos en diferentes puntos de nuestro domicilio de nuestra red.
- Detectar otras redes que pueden causar interferencias a la nuestra.
- Orientar antenas direccionales cuando se desea hacer enlaces de larga distancia, o simplemente para colocar la antena o tarjeta en el punto con mejor calidad de la señal.
- Sirve para detectar puntos de acceso no autorizados.
- Sirve para WarDriving, es decir, detectar todos los APs que están alrdedor.

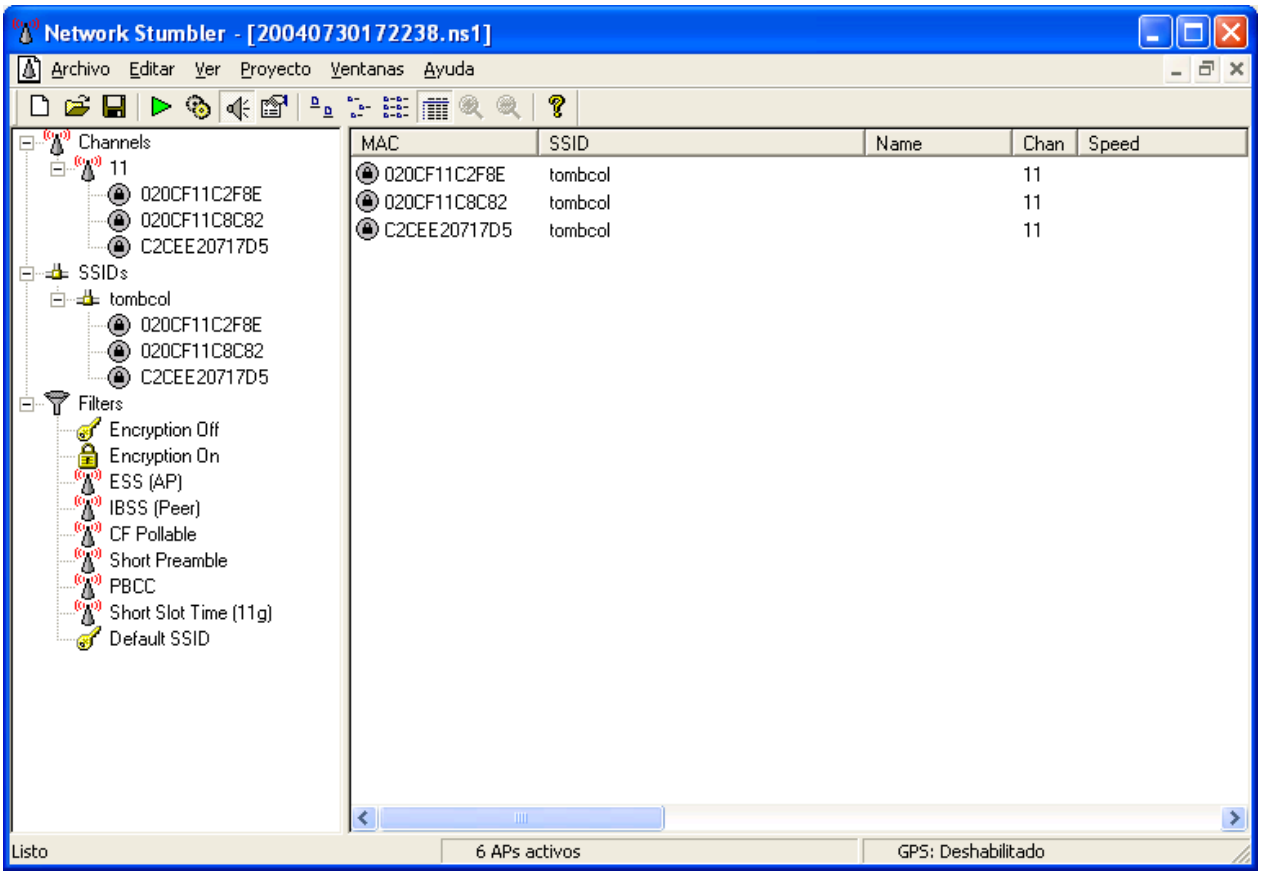


Fig. A5- Pantalla principal de Network Stumbler

A continuación se mencionan algunas características del entorno de este programa:

Icono circular: En la primera columna podéis observar un pequeño icono circular o disco. Cuando en el interior del mismo hay un candado significa que el punto de acceso usa algún tipo de encriptación. El icono también cambia de color para indicar la intensidad de la señal, de la forma siguiente:

- Gris: No hay señal.
- Rojo: Señal pobre o baja.
- Naranja: Señal regular o mediana.
- Amarillo: Señal buena.
- Verde claro: Muy buena señal.
- Verde oscuro: La mejor señal.

MAC: dirección del AP.

SSID: nombre de la red.

Name: es el nombre del AP. Esta columna generalmente está en blanco porque NetStumbler solo detecta el nombre de los APs Orinoco o Cisco.

Chan: Indica el canal por el que transmite el punto de acceso detectado. Un asterisco (*) después del número del canal significa que estás asociado con el AP. Un signo de suma (+) significa que estuviste asociado recientemente con el AP. Y cuando no hay ningún carácter significa que has localizado un AP y no estas asociado a él.

Speed: Indica la velocidad, los Mbps máximos que acepta esa red (11, 22.54…).

Vendor: indica el fabricante, lo detecta a partir de los tres primeros pares de caracteres de la dirección MAC. No importa lo muestra, porque la base de datos que usa no contiene todos los fabricantes. En este caso se debe poner Fake, que no es el nombre de ningún fabricante.

Type: Tipo de red (AP-infraestructura, o ad-hoc).

Encrypton: encriptación, se suele equivocar y algunas WPA las detecta como WEP, acrónimo de Wired Equivalency Privacy. Es un mecanismo de seguridad vulnerable pero muy extendida entre los puntos de acceso comerciales.

SNR: Acrónimo de Signal Noise Ratio. Es la relación actual entre los niveles de señal y ruido para cada punto de acceso.

Signal+: Señal (MAX), muestra el nivel máximo de señal que ha sido detectado para un punto de acceso.

Noise: Ruido, muestra el nivel de ruido actual para cada punto de acceso.

SNR+: muestra el nivel máximo que ha tomado el factor SNR para cada punto de acceso

IP Adress: indica la dirección IP en la que se encuentra la red, aunque solo la muestra en el caso de estar conectados a la misma.

Latitude, Longitude, Distance: si se está usando GPS nos indica la posición estimada.

First Seen: la hora a la que la red fue detectada por primera vez.

Last Seen: la hora a la que la red fue detectada por última vez.

Signal: el nivel de señal actual en dB.

Noise: el nivel de ruido en dB. No está soportado por todas las tarjetas, por lo que si pone -100 es que no detecta ruido, pero no quiere decir que no lo haya sino que no lo soporta.

Gráfica Señal a Ruido

En la parte izquierda de la pantalla se puede pinchar en alguna MAC de las redes que detecta el programa y entonces aparecerá un gráfico como este:

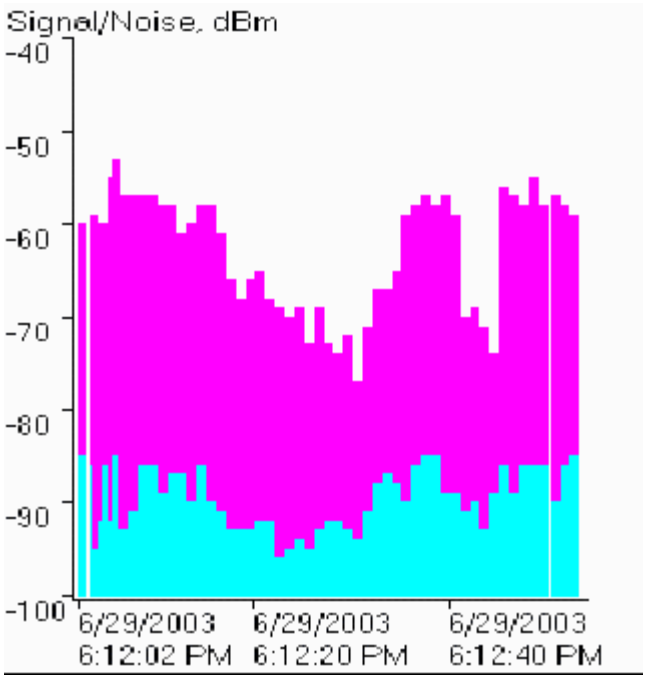


Fig. A6- Gráfica Señal a Ruido

Los datos que aparecen en el gráfico dependen de la tarjeta que se tenga. La zona verde indica el nivel de señal. A mayor altura, mejor señal. La zona roja (si esta soportado por la tarjeta) indica el nivel de ruido. A mayor altura, mayor ruido.

El espacio entre la altura de la zona roja y verde es el **SNR.**

Para ver cual es el **SNR** (Signal Noise Ratio), es decir la diferencia entre la señal y el ruido se puede usar la pantalla principal; o calcularlo mirando la gráfica.

Hay que tener en cuenta que el valor del ruido (noise) si no lo detecta esta a -100, lo que no quiere decir que no haya ruido sino que puede ser que la tarjeta no sea capaz de detectar el ruido.

Hay muchas tarjetas con las cuales Netstumbler usa el controlador NDIS 5.1 y este controlador no muestra el ruido.

El SNR es igual a SIGNALL-NOISE;

Ejemplo: si signal=-70 y NOISE=-100 el valor de SNR (que este es normalmente positivo) será -70-(-100)= 30 dB.

En la gráfica de arriba, observamos que si tiene una signal=-60 y noise=-85 el valor de SNR es -60-(-85)=25 dB.

GLOSARIO

ADSL

ADSL son las siglas de Asymmetric Digital Subscriber Line (Línea de Abonado Digital Asimétrica). Consiste en una línea digital de alta velocidad apoyada en el par trenzado de cobre que lleva la línea telefónica convencional o línea de abonado.

ARP

(Address Resolution Protocol). Protocolo de resolución de dirección. Protocolo usado por una computadora para correlacionar una dirección IP con una dirección de hardware. Las computadoras que llaman el ARP difunden una solicitud a la que responde la computadora objetivo.

ATM

(Asynchronous Transfer Mode) Modo de Transferencia Asíncrona. Sistema de transferencia de información de conmutación de paquetes de tamaño fijo con alta carga, utilizados en banda ancha para aprovechar completamente una línea y soporta velocidades de hasta 1,2 GB. También es conocido como Paquete rápido.

Bridge

Puente. Dispositivo que pasa todos los mensajes de una red a otra sin distinguir a cuál red pertenece el destino del mensaje.

Banda base

Tecnología de comunicaciones que utiliza una frecuencia portadora única y requiere que las estaciones conectadas a la red participen en cada transmisión.

Bit

Dígito binario, unidad mínima de información de los dos estados 0/1. Abreviación de Binary Digit que puede ser 0 o 1. Es la unidad básica de almacenamiento y proceso de una computadora. 8 bits = 1 byte.

Backbone

Se refiere a las principales conexiones troncales de Internet. Está compuesta de un gran número de router comerciales, gubernamentales, universitarios y otros de gran capacidad interconectados que llevan los datos entre países, continentes y océanos del mundo.

Caché

Es un conjunto de datos duplicados de otros originales, con la propiedad de que los datos originales son costosos de acceder, normalmente en tiempo, respecto a la copia en el caché. Cuando se accede por primera vez a un dato, se hace una copia en el caché; los accesos siguientes se realizan a dicha copia, haciendo que el tiempo de acceso aparente al dato sea menor.

Datagrama

Paquetes de datos que se transfieren en una conexión.

DBi

Ganancia relativa de una antena, con respecto a un radiador isotrópico.

Full duplex

Permite transmitir en ambas dirección, pero simultáneamente por el mismo canal. Existen dos frecuencias una para transmitir y otra para recibir. El caso más típico es la telefonía, donde el transmisor y el receptor se comunican simultáneamente utilizando el mismo canal, pero usando dos frecuencias.

FDDI

(Fiber Digital Device Interface) Dispositivo Interface de Fibra Digital. Topología de red local en doble anillo y con soporte físico de fibra óptica. Alcanza velocidades de hasta 100 Mbps y utiliza un método de acceso al medio basado en paso de testigo (token passing). Alcanza una distancia máxima de 100 kilómetros, con un número máximo de repetidores de 100 y un número máximo de estaciones permitidas de 500.

Jaula de Faraday

El efecto jaula de Faraday provoca que el campo electromagnético en el interior de un conductor en equilibrio sea nulo, anulando el efecto de los campos externos. Esto se debe a que, cuando el conductor sujeto a un campo electromagnético externo, se polariza de manera que queda cargado positivamente en la dirección en que va el campo electromagnético, y cargado negativamente en el sentido contrario. Puesto que el conductor se ha polarizado, este genera un campo eléctrico igual en magnitud pero opuesto en sentido al campo electromagnético, luego la suma de ambos campos dentro del conductor será igual a 0.

Half duplex

Permite transmitir en ambas direcciones; sin embargo, la transmisión puede ocurrir solamente en una dirección a la vez. Tanto transmisor y receptor comparten una sola frecuencia. Un ejemplo típico de half-duplex es el radio de banda civil (CB) donde el operador puede transmitir o recibir, no pero puede realizar ambas funciones simultáneamente por el mismo canal.

Hacking

Acción de piratear sistemas informáticos y redes de telecomunicación.

ICMP

Componente de los protocolos TCP/IP que realiza las funciones de control y administración de transacciones.

Modulación

Es el proceso de colocar la información contenida en una señal, generalmente de baja frecuencia, sobre una señal de alta frecuencia**.**

MAU

Dispositivo utilizado en topologías de estrella física para generar un círculo lógico. Todos se conectan a él, y él asigna quién tiene el Token Passing o derecho de transacción.

NAT

Proceso de conversión de IP (Protocolo Internet) que permite a una red con direcciones privadas tener acceso a información de Internet.

Latencia

Es el tiempo o lapso necesario para que un paquete de información se transfiera de un lugar a otro. La latencia, junto con el ancho de banda, son determinantes para la velocidad de una red.

OFDM

La Multiplexación por División de Frecuencias Ortogonales (OFDM), también llamada modulación por multitono discreto (DMT), es una modulación que consiste en enviar la información modulando en QAM o en PSK un conjunto de portadoras de diferentes frecuencias.

Proxy

El Proxy es un servidor de que conectado normalmente al servidor de acceso a la WWW de un proveedor de acceso va almacenando toda la información que los usuarios reciben de la WEB, por tanto, si otro usuario accede a través del Proxy a un sitio previamente visitado, recibirá la información del servidor Proxy en lugar del servidor real.

PHP

Es un lenguaje de programación muy potente que, junto con html, permite crear sitios web dinámicos. Php se instala en el servidor y funciona con versiones de Apache, Microsoft IIs, Netscape Enterprise Server y otros.

PPP

(Point to Point Protocol - Protocolo Punto a Punto). Protocolo de nivel de enlace para hacer conexión entre dos puntos (dos computadoras o nodos). Permite conectar computadoras utilizando cable serial, línea telefónica, teléfono celular, enlace de fibra óptica, etc. Generalmente es empleado para establecer la conexión a Internet desde un usuario al proveedor de Internet a través de un módem telefónico.

RARP

(Reverse Address Resolution Protocol - Protocolo de Resolución de Dirección de Retorno). Protocolo de bajo nivel que asigna direcciones IP a ordenadores desde un servidor en una red.

Roaming

Capacidad de un dispositivo de moverse desde una zona de cobertura hacia otra, sin pérdida de la conectividad.

Slot Time

Ranura de tiempo. Intervalo de tiempo continuamente repetido o un periodo de tiempo en el que dos dispositivos son capaces de interconectarse.

Simplex duplex

Es aquella que ocurre en una dirección solamente, deshabilitando al receptor de responder al transmisor. Normalmente la transmisión simplex no se utiliza donde se requiere interacción

humano-máquina. Ejemplos de transmisión simplex son: La radiodifusión (broadcast) de TV y radio.

SLIP

(Serial Line Internet Protocol) Protocolo que permite transferir paquetes TCP/IP, permite sólo transmisión asíncrona, direcciones IP, no tiene detección de errores y está menos optimizado que el PPP.

SMDS

Servicio de conmutación de paquetes de alta velocidad sin conexiones que extiende el desempeño tipo LAN mas allá de las instalaciones del suscriptor.

Los objetivos primordiales son proporcionar interfaces de alta velocidad con los sistemas de los clientes y desligar las operaciones SMDS del equipo del cliente. Este trabajo lo haría el CPE (equipo presente en las instalaciones del cliente que hará las veces de ruteador).

Trama o paquete de datos

Todo tipo de información que es transferida por Internet está dividida en paquetes pequeños de información. Cada paquete posee una estructura y tamaño diferente dependiendo del protocolo que lo utilice.

VoIP

(Voice over Internet Protocol, voz sobre Internet). Enrutamiento de conversaciones de voz sobre Internet u otra red basada en el protocolo IP.

X.21

Protocolo usado en las redes telefónicas digitales para voz y datos en transmisión síncrona Full Duplex.

XML

Son las siglas de Extensible Markup Language, una especificación/lenguaje de programación diseñado especialmente para los documentos de la web. Permite que los diseñadores creen sus propias etiquetas, permitiendo la definición, transmisión, validación e interpretación de datos entre aplicaciones y entre organizaciones.