UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES ARAGÓN

REDES INALÁMBRICAS SOLUCIÓN DE CONECTIVIDAD PARA RED LOCAL, RED UNAM E INTERNET DENTRO DE LA ENEP ARAGÓN.

T E S I S

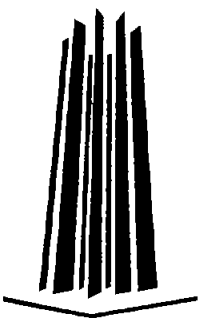
QUE PARA OBTENER EL TITULO DE:

INGENIERO EN COMPUTACIÓN

P R E S E N T A N:

JUAN MANUEL ARELLANO OROZCO

FR ANCISCO MARTINEZ CRUZ



ASESOR: ING. VICTOR RAÙL VELASCO VEGA

MÉXICO

2005

Autorizo a la Dirección General de Bibliotecas de la UNAM a difundir en formato electrónico e impreso el contenido de mi trabajo recepcional.

NOMBRE: Juan Manuel Arellano Orozco

FECHA: 23-Nov-2004

FIRMA:

Autorizo a la Dirección General de Bibliotecas de la UNAM a difundir en formato electrónico e impreso el contenido de mi trabajo recepcional.

NOMBRE: Francisco Martínez Cruz

FECHA: 23/Nov/2004

FIRMA:

Dedicatoria

A la enfermera (cuando se necesitó), maestra (en su mas amplia extensión de la palabra), cuidadora y cómplice, por esos días de desvelo y horas de dedicación para hacerme salir adelante en esta vida. Gracias mamá.

A mi amiga, confidente y entrenadora por darme ánimos en esos momentos difíciles. Gracias Maribel.

Dr. Jaime Orozco ya que gracias a tu persistencia he logrado llegar a esta meta.

A toda la Familia Orozco por todo su apoyo incondicional ya que en mi formación todos participaron de una manera u otra.

Al Ing. Víctor Velasco por la ayuda y apoyo para la realización de esta tesis y así como por las enseñanzas recibidas.

Al Dpto. de Informática de la ENEP Aragón por soportarme y apoyarme ya que gran parte de la realización de este proyecto ellos estuvieron presentes.

Gracias Marce.

A todo el equipo que me ayudo a salir adelante, que gracias a ellos estoy aquí.

"*Caminante no hay camino se hace*
camino al andar".
Antonio Machado

Juan Manuel

Dedicatoria

A mis Padres José Refugio y Graciela

Por todo su apoyo, comprensión, sacrificios, consejos, confianza y amor que siempre me han brindado, porque siempre han estado conmigo en las buenas y en las malas, porque por ustedes termine una carrera, por todo eso y mucho mas. Gracias los quiero mucho.

A mi Hermano Sergio

Por todos esos momentos que compartimos juntos, por creer en mi y porque siempre que te he necesitado has estado conmigo. Te quiero mucho y espero ser un buen ejemplo para ti.

A mi Esposa Lucina

Amor gracias por todo tu apoyo y comprensión, por estar conmigo en todo momento además de motivarme día a día a terminar este trabajo, te amo.

A mi Hija Carolina

Hija aunque todavía no tienes conocimiento de las cosas, has sido una gran motivación en mi vida para seguir adelante, por eso a ti también te dedico esta tesis te amo bebe.

Al Ingeniero Victor

Por todos esos consejos que tanto me han ayudado, por esos días de trabajo, por confiar en mi y por aceptar ser mi asesor de tesis. Gracias Inge.

A todos mis amigos y compañeros de trabajo

Gracias a todos porque de cada uno de ellos he aprendido algo, Everardo, Agustín, Alberto, Christian, Heriberto, Ernesto, Eric, Carlos, Luis, Manuel, Eduardo, Victor y Fernanda.

A los Ingenieros

Juan Gastaldi Pérez, Roberto Blanco Bautista, Marcelo Pérez Medel, y al Lic. Alberto Ibarra Rosas, por tomarse el tiempo de revisar este trabajo. Gracias.

Francisco Martínez Cruz

CONTENIDO

	PAG.
Introducción	I
Objetivos	II
1 Conceptos Generales de Redes	1
1.1 Definición de red	1
1.2 El modelo de referencia OSI	1
1.2.1 Nivel Físico	2
1.2.2 Nivel de enlace de datos	3
1.2.3 Nivel de red	4
1.2.4 Nivel de transporte	6
1.2.5 Nivel de sesión	7
1.2.6 Nivel de presentación	8
1.2.7 Nivel de aplicación	9
1.3 Tipos de redes	10
1.3.1 Red de Área Local (LAN, Local Area Network)	10
1.3.2 Red de Área Metropolitana (MAN, Metropolitan Área Network)	11
1.3.3 Red de Área Ancha (WAN, Wide Área Network)	12
1.4 Topologías	13
1.4.1 Topología en bus	13
1.4.2 Topología en anillo	14
1.4.3 Topología en estrella	15
1.4.4 Topología en árbol	16
1.5 Métodos de acceso al cableado (Protocolos de Contienda)	17
1.5.1 Contienda simple	18
1.5.2 Acceso múltiple por detección de portadora (CSMA)	18
1.5.3 CSMA / CD	19
1.5.4 Llamada selectiva (Polling)	19
1.5.5 Token passing (pase de testigo)	20
1.6 Arquitectura de las redes locales	21
1.6.1 Ethernet	21
1.6.2 Token ring	23
1.6.3 Arcnet	25
2 Redes Inalámbricas	27
2.1 WLAN	27
2.2 Normas IEEE 802 para LAN.	28
2.3 Norma IEEE 802.11. Redes Inalámbricas.	29
2.4 Mecanismos de Seguridad.	32
2.5 Porque usar una red inalámbrica	35
2.5.1 Áreas críticas	36
2.6 Medios de transmisión	38
2.6.1 Infrarrojo	38
2.6.2 Banda Angosta	39
2.6.3 Espectro Extendido	39
2.6.4 Que no es espectro extendido	40
2.7 Como funciona una WLAN	40

2.8 Configuración de una WLAN 41
2.9 Cobertura 43
2.10 Rendimiento 43

3 Infraestructura actual de la Red en Aragón 45

3.1 Introducción 45
3.2 Biblioteca 47
3.3 Edificio de Gobierno 49
3.4 Edificio A1 (Servicios Escolares) 52
3.5 Centro de Cómputo 53
3.6 Edificio A12 (Posgrado) 54
3.7 Edificio A5 (Área del CAE) 55
3.8 Edificio del Centro Tecnológico 56
3.9 Edificio A4 (Fundación UNAM y Revisión de Estudios) 57
3.10 Laboratorio L3 58
3.11 Otras Áreas 60
3.12 Monitoreo de la Red 62
3.13 Seguridad 63
3.13.1 Limitando la propagación de RF 63
3.13.2 Autentificación de llave compartida 65
3.13.3 WEP 66
3.13.4 Firewall y Router 67

4 Conexión Inalámbrica en Áreas aisladas de la ENEP Aragón 70

4.1 Edificio del CLE 70
4.2 Instalación del Access Point modelo 2311 WLAN 72
4.2.1 Aplicaciones 72
4.2.2 Procedimientos para instalar un AP 2311 73
4.3 Configuración del Access Point 76
4.4 Características de los AP 77
4.5 Especificación del Hardware del AP 78
4.6 Departamento de Adquisiciones 79
4.7 Laboratorios de Ingeniería L1, L2 y L4 81
4.8 Módulo de Extensión Universitaria 84
4.9 Instalación del AP 2411 WLAN 86

5 Futuro de la red en la ENEP Aragón 89

5.1 Panorama en la red de la Enep Aragón 89
5.2 Corto Plazo 91
5.3 Mediano Plazo 92
5.3.1 Crear VPN´S 93
5.3.2 Protocolos usados en las VPN´S 95
5.4 Largo Plazo 101
5.4.1 Internet2 101

Conclusiones 105

Glosario de términos 106

Bibllografía 115

Introducción

Debido a la gran evolución dentro del campo de las computadoras ha sido necesario el empleo de nuevas tecnologías que faciliten la comunicación entre ellas, una de estas tecnologías es la inalámbrica.

Es por eso que en el presente trabajo se muestra el uso de esta tecnología como una herramienta auxiliar para la ampliación de una red existente cableada, así como sus ventajas, aplicaciones, beneficios de su empleo en áreas donde no es práctico o es imposible instalar cables, ya sea por cuestiones estéticas o porque el medio físico no lo permite.

Cabe hacer notar que esta investigación se llevó a cabo en la ENEP Aragón, debido a la falta de conectividad en diferentes áreas académico-administrativas del plantel, las cuales necesitaban estar conectadas a la red.

Este trabajo lo dividimos en 5 capítulos los cuales describimos brevemente a continuación:

Capítulo 1: Conceptos Generales de Redes. Aquí se hace una introducción a lo que son las redes así como los conceptos generales que se manejan dentro del empleo de las redes como son las topologías, la arquitectura, los protocolos y el modelo OSI.

Capítulo 2: Redes Inalámbricas. Aquí damos una explicación de lo que son las redes inalámbricas, así como los estándares que se utilizan, las diferentes formas de configuración, los tipos de transmisión y su funcionamiento.

Capítulo 3: Infraestructura Actual de la Red en Aragón. Aquí se describe cual es la situación actual de la red, cuales son los segmentos de esta, así como las áreas que pertenecen a cada segmento, también explicamos una de las herramientas que se utilizan para monitorear la red.

Capítulo 4: Conexión inalámbrica en áreas aisladas de la ENEP Aragón. En esta parte se explica cuales son las áreas donde se emplea la tecnología inalámbrica, para realizar la conexión con áreas donde ya se tiene acceso a la red cableada, así como la forma de instalar y configurar un Access Point.

Capítulo 5: Futuro de la red en la ENEP Aragón. Por último se propone un proyecto de cómo puede ir actualizándose la red tanto a corto como mediano y largo plazo hasta llegar a estar en un estado óptimo, así como también la implementación de Internet 2.

Es así como damos comienzo a este trabajo que esperamos sea de utilidad para todos aquellos que requieran información sobre la conexión inalámbrica existente hasta este momento en la ENEP Aragón.

Objetivo Principal

Poder enlazar las áreas Académico-Administrativas del plantel que no cuentan con acceso a red, Internet y Red UNAM. Mediante el uso de tecnología inalámbrica.

Objetivos Específicos

- Conectar el edificio del Centro de Lenguas Extranjeras el cual no cuenta con acceso a la red, con el Centro de Cómputo de forma inalámbrica y así poder dar acceso a la red de la ENEP Aragón.

- Enlazar el Módulo de Extensión Universitaria con el Edificio de Gobierno. Igualmente mediante tecnología inalámbrica.

- Conectar el Departamento de Adquisiciones y Servicios Generales por medio de una antena externa con la Biblioteca para que puedan tener acceso a la red, y de esta manera puedan realizar sus transacciones.

- Efectuar el acceso a red UNAM de los laboratorios de Ingeniería L1, L2 y L4 mediante el Edificio L3.

- Crecer en servicios de Red en las diversas áreas del plantel evitando el uso de direcciones IP fijas, sustituyéndolas por direcciones IP dinámicas.

- Proporcionar acceso a Internet a las áreas antes mencionadas con el fin de poder consultar información actualizada sobre algún tema en específico, además de brindar acceso al correo electrónico.

CAPÍTULO I

CONCEPTOS GENERALES DE REDES

1.1.- Definición de una Red

Es un sistema de comunicación entre computadoras que permite compartir recursos tanto de software como periféricos.

1.2.- El modelo de referencia OSI

Las comunicaciones de red tienen muchos niveles y pueden ser difíciles de entender incluso para el administrador de red experto. El modelo de referencia de Interconexión de Sistemas Abiertos (Open Systems Interconnection u OSI) es un concepto teórico que separa las comunicaciones de red en siete niveles diferentes, tal y como se muestra en la (Figura 1). Cada computadora de la red utiliza una serie de protocolos para realizar las funciones asignadas a cada nivel. El conjunto de niveles forma lo que se conoce como pila de protocolos. En la parte más alta de la pila está la aplicación que demanda un recurso localizado en cualquier otro sitio de la red y en la parte más baja, medios de transmisión, como los cables, que conectan las computadoras entre sí y forman la red.

Figura 1

El modelo de referencia OSI se desarrollo en dos proyectos independientes por la Organización Internacional de Normalización (ISO International Organization for Standardization) y el Comité Consultivo Internacional Telefónico y Telegráfico (CCITT Comité Consultatif International Telephonique et Telegraphique), que se conoce ahora como Sector de Estandarización en Telecomunicaciones de la Unión Internacional de Telecomunicaciones (ITU-T).Cada uno de estos organismos desarrolló su propio modelo de

siete niveles, pero se combinaron ambos proyectos en 1983, dando como resultado un documento denominado "El modelo básico de referencia para Interconexión de sistemas abiertos" que publicó ISO como ISO 7498 e ITU-T como X.200.

1.2.1.- Nivel Físico

El nivel físico del modelo OSI define el medio físico utilizado para transmitir los datos de una computadora a otra. El tipo más común de medio de transmisión utilizado en redes es el cable eléctrico de cobre, aunque el cable de fibra óptica se está volviendo cada vez más popular. Existen también un cierto número de implementaciones del nivel físico inalámbricas, que usan ondas de radio, radiación infrarroja, luz láser, microondas y otras tecnologías. El nivel físico incluye el tipo de tecnología utilizado para transportar los datos, el tipo de equipo que implementa esa tecnología, las especificaciones de instalación del equipo y la naturaleza de las señales que codifican los datos transmitidos. (Figura 2).

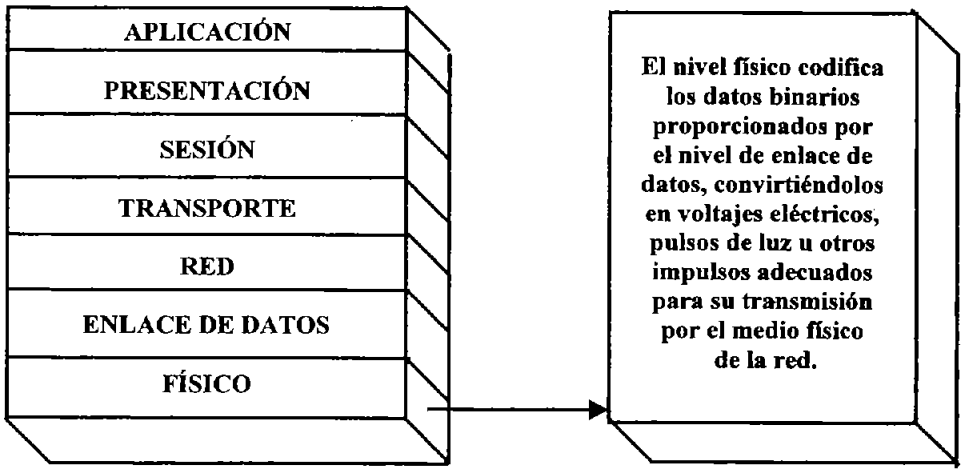


Figura 2

Hasta aquí sólo hemos hablado del cableado, pero el cable propiamente dicho no es el único elemento del nivel físico. Los estándares utilizados para crear una red, definen también cómo instalar el cable, incluyendo la longitud máxima de los segmentos y la distancia desde las fuentes de alimentación. Los estándares especifican que tipo de conectores utilizar para unir los cables, el tipo de tarjeta de red para instalar en la computadora y el tipo de concentrador para unir las computadoras en topología de estrella. Finalmente el estándar especifica el modo en que la tarjeta de red debe convertir los datos generados por la computadora en impulsos eléctricos que se puedan transmitir por el cable. De esta forma podemos ver que el nivel físico abarca mucho más que sólo el tipo de cable.

El principal componente activo en una instalación del nivel físico es el transceptor, éste se encuentra en las tarjetas de red, en los concentradores-repetidores y en otros dispositivos.

Como su propio nombre indica, el transceptor está encargado de recibir y transmitir señales por el medio físico de la red. En redes que usan cable de cobre, el transceptor es un dispositivo eléctrico que toma los datos binarios recibidos del protocolo de enlace de datos y los convierte en señales de diversos voltajes. A diferencia de los demás niveles de la pila de protocolos, el nivel físico no se ocupa para nada del significado de los datos que está transmitiendo. El transceptor simplemente convierte los ceros y unos en voltajes, pulsos de luz, ondas de radio o algún otro tipo de señal, pero ignora completamente los paquetes, tramas, direcciones, e incluso el sistema que va a recibir la señal.

Las señales generadas por el transceptor pueden ser analógicas o digitales. La mayor parte de redes de datos usan señales digitales, pero algunas tecnologías inalámbricas usan transmisiones de radio analógicas para llevar los datos. Las señales analógicas van variando gradualmente entre dos valores, formando el tipo de onda sinusoidal, mientras que las transiciones digitales son inmediatas y absolutas.

1.2.2.- Nivel de enlace de datos

El protocolo del nivel de enlace de datos es un intermediario entre la red física y la pila de protocolos de la computadora. (Figura 3). Un protocolo de enlace de datos incluye los tres siguientes elementos:

- El formato de la trama que encapsula los datos del nivel de red.
- El mecanismo que regula el acceso al medio de transmisión compartido.
- Especificaciones para la instalación del nivel físico de la red.

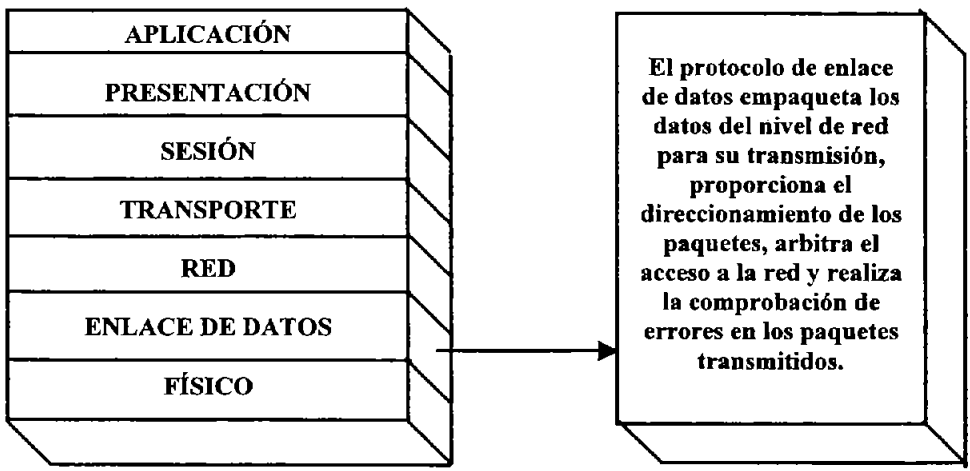


Figura 3

El encabezado y la cola con los que el protocolo de enlace de datos envuelve los datos del nivel de red, constituyen la corteza exterior de la trama que se transmite por la red. En esencia, esta trama es el sobre que lleva el paquete de datos hasta su siguiente destino y por tanto proporciona la información básica de direccionamiento necesaria para que el paquete llegue a su destino. Además los protocolos de enlace de datos incluyen habitualmente un mecanismo de detección de errores y un indicador que especifica el protocolo de red que debe usar el sistema receptor para procesar los datos incluidos en el paquete.

El encabezado del protocolo de enlace de datos contiene la dirección de la computadora que envía el paquete y de la que lo tiene que recibir. La dirección utilizada en este nivel es la dirección hardware, o dirección MAC, que en la mayor parte de los casos, viene codificada de fábrica en la interfaz de red de cada computadora. En redes Ethernet y Token Ring, las direcciones tienen una longitud de 6 bytes, de los cuáles los 3 primeros los asigna el Institute of Electrical and Electronic Engineers (IEEE), y los 3 siguientes los asigna el propio fabricante.

El control de acceso al medio es el proceso por medio del cuál el protocolo de enlace de datos arbitra el acceso al medio de transmisión. Para que la red funcione efectivamente, cada una de las computadoras que comparten un cable u otro medio debe tener la posibilidad de transmitir sus datos de un modo regular. Este es el motivo principal por el que los datos que se van a transmitir se dividen en paquetes. Si las computadoras transmitieran todos sus datos en un flujo continuo, podrían monopolizar la red por periodos de tiempo prolongados.

El protocolo de enlace de datos además del encabezado, incluye una cola a continuación del campo de datos. Esta cola contiene un campo denominado Secuencia de Comprobación de Tramas (FCS, Frame Check Séquence) que utiliza el sistema receptor para detectar errores ocurridos durante la transmisión. Con este fin, el sistema que transmite el paquete realiza una cuenta sobre la totalidad de la trama denominada Comprobación de Redundancia Cíclica (CRC) e incluye el resultado en el campo FCS. Cuando el paquete alcanza su siguiente destino, el sistema receptor realiza el mismo proceso y compara el resultado con el valor del campo FCS. Si los valores no corresponden se deduce que el paquete se ha deteriorado durante el tránsito y se elimina.

1.2.3.- Nivel de red

El protocolo del nivel de red es el principal portador, desde el origen hasta el destino, de los mensajes generados en el nivel de aplicación. Esto significa que a diferencia del protocolo de enlace de datos que sólo se ocupa de que el paquete llegue a su próximo destino en la red local, el protocolo de red es responsable de todo el camino recorrido por el paquete, desde el sistema de origen hasta el destino final. Este protocolo acepta datos del nivel de transporte y los encapsula en un datagrama, añadiendo su propio encabezado, el cuál contiene la dirección del sistema de destino que identifica al destinatario final del paquete. (Figura 4). Además de la función de direccionamiento, los protocolos del nivel de red realizan también las siguientes funciones:

- Enrutamiento
- Fragmentación
- Comprobación de errores
- Identificación del protocolo del nivel de transporte

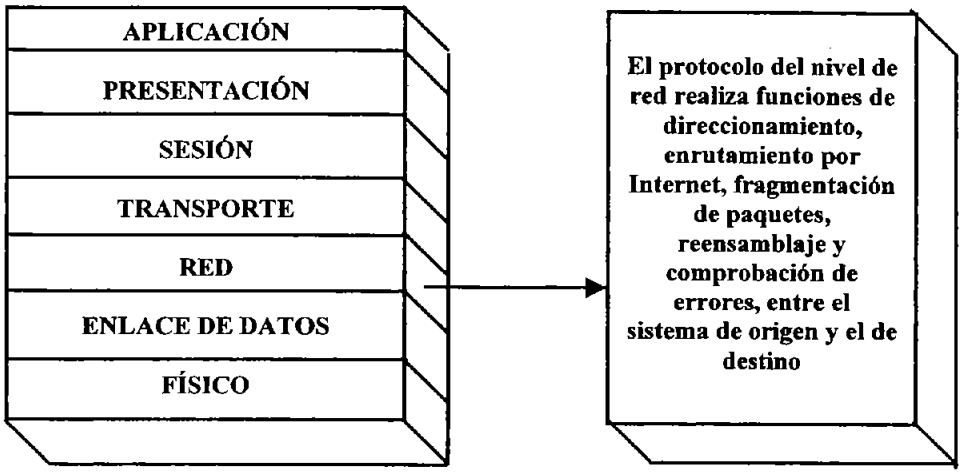


Figura 4

Los protocolos del nivel de red utilizan diferentes sistemas de direccionamiento para identificar el destino final de un paquete. El protocolo más popular del nivel de red, el Protocolo de Internet (IP Internet Protocol), proporciona su propio espacio de direcciones de 32 bits, que identifica tanto la red en que reside el sistema de destino como el sistema mismo.

El nivel de red define dos tipos de computadoras que pueden participar en una transmisión de paquetes: sistemas terminales e intermedios. El terminal es aquel que genera y transmite el paquete o bien el destinatario final. El intermedio es un enrutador o conmutador que conecta dos o más redes y reenvía paquetes de camino a sus destinos. En los sistemas terminales, los siete niveles de la pila de protocolos están involucrados en la creación o en la recepción del paquete. Pero en los intermedios los paquetes llegan al sistema y suben por la pila de protocolos sólo hasta el nivel de red. El cuál elige una ruta para el paquete y lo pasa al enlace de datos para su empaquetamiento y transmisión en el nivel físico.

Como los enrutadores pueden conectar redes que usan diferentes protocolos de enlace de datos, algunas veces es necesario que los sistemas intermedios dividan los datagramas en fragmentos para transmitirlos. Dependiendo de los protocolos de enlace de datos utilizados por los sistemas intermedios, los fragmentos de un datagrama pueden a su vez ser fragmentados, y éstos no se reensamblan hasta que alcanzan su destino final.

1.2.4.- Nivel de transporte

Una vez alcanzado el nivel de transporte, el proceso de llevar los paquetes a su destino ha dejado de ser una preocupación. La unidad de datos del nivel de transporte está formada por un encabezado y por un campo de datos recibido del nivel de aplicación. A su vez, el nivel de red encapsula esta unidad de datos formando un datagrama. Una de las principales funciones del protocolo de transporte es identificar tanto el proceso de nivel superior que generó el mensaje en el sistema de origen, como el que recibirá el mensaje en el sistema de destino. Por ejemplo, los protocolos de transporte del conjunto TCP/IP utilizan en sus encabezados números de puerto para identificar servicios de niveles superiores. Otras funciones que puede realizar el nivel de transporte son la detección y la corrección de errores, el control de flujo, el asentamiento de recepción de paquetes y otros servicios con conexión. (Figura 5).

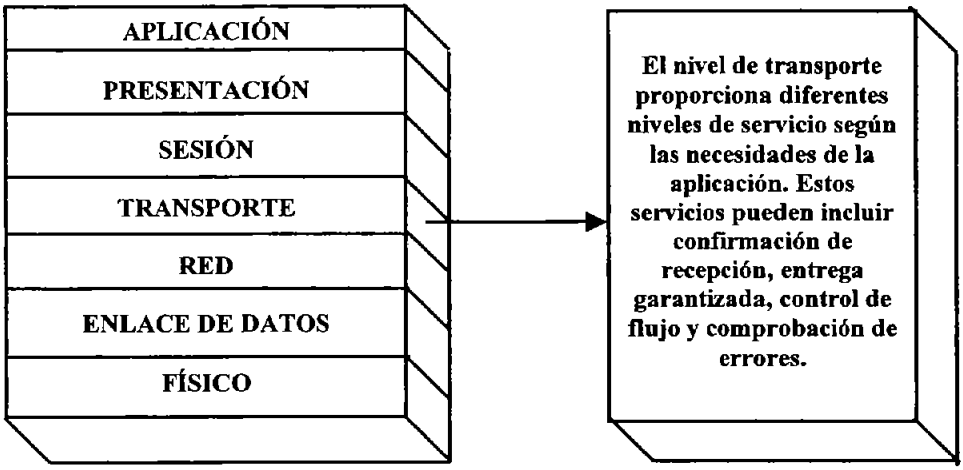


Figura 5

La selección de un protocolo de transporte depende de las necesidades de la aplicación que genera los mensajes y de los servicios ya proporcionados por los protocolos de nivel inferior. El documento OSI define las siguientes 5 clases teóricas de protocolos de transporte:

- **TP0** Sin funciones adicionales. Se supone que los protocolos de nivel inferior ya proporcionan todos los servicios que necesita la aplicación.
- **TP1** Corrección de errores señalados. Proporciona la capacidad de corregir errores detectados por los protocolos de nivel inferior.
- **TP2** Multiplexación. Incluye códigos que identifican el proceso que generó el paquete y el que lo procesará en su destino, permitiendo que un único medio de transmisión transporte el tráfico de múltiples aplicaciones.

- **TP3** Corrección de errores señalados y multiplexación. Combina los servicios proporcionados por las clases TP1 y TP2.
- **TP4** Servicio completo con conexión. Incluye detección y corrección de errores, control de flujo y otros servicios.

Los protocolos de transporte con conexión están diseñados para llevar grandes cantidades de datos, pero estos datos se deben dividir en segmentos para que quepan en paquetes individuales. La segmentación de los datos y la numeración de los segmentos es un elemento crítico del proceso de transmisión, que además hace posible funciones como la corrección de errores. El proceso de enrutamiento, realizado en el nivel de red, es dinámico, durante el curso de una transmisión es posible que los segmentos tomen diferentes rutas hacia el destino y que lleguen en un orden diferente al que se enviaron. La numeración de segmentos posibilita que el sistema receptor los reensamble a su orden original. También que notifique al emisor que determinados paquetes no llegaron o se han deteriorado. En consecuencia el emisor tiene la posibilidad de retransmitir solamente los segmentos que falten sin tener que repetir la transmisión entera. Otra de las funciones del protocolo de transporte con conexión es el control de flujo, que es un mecanismo por el que el sistema receptor puede notificar al emisor que disminuya la velocidad de transmisión si no quiere arriesgarse a saturar al receptor y perder datos.

1.2.5.- Nivel de sesión

En este nivel no hay protocolos independientes que operen exclusivamente en el nivel de sesión. En cambio, la funcionalidad del nivel de sesión está incorporada en diversos protocolos, cuyas funciones caen también en la jurisdicción de los niveles de presentación y aplicación. (Figura 6). NetBIOS (Network Basic Input/Output System, o Sistema Básico de Entrada y Salida de Red) y NetBEUI (NetBIOS Extended User Interface, o Interfaz de Usuario Extendido de NetBIOS) son dos de los mejores ejemplos de estos protocolos.

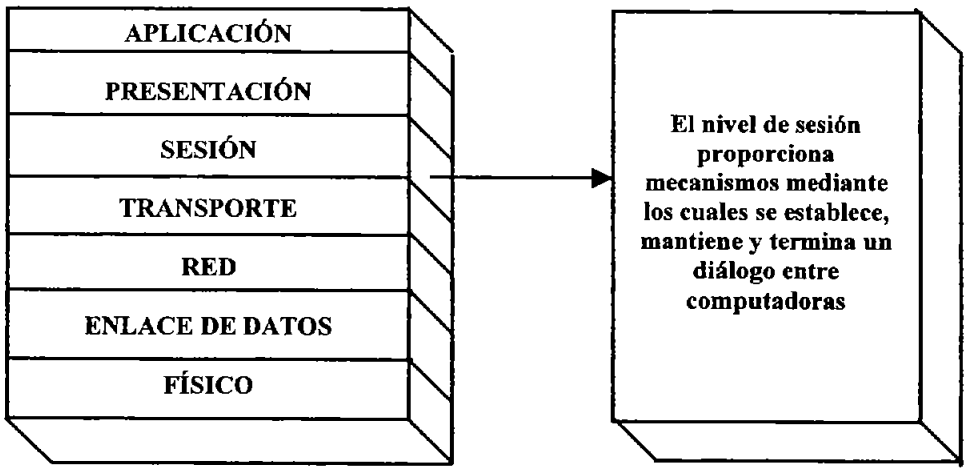


Figura 6

El nivel de sesión no se ocupa necesariamente de la seguridad, ni del proceso de inicio de sesión de red, como su nombre parece indicar. En su lugar, las principales funciones de este nivel están relacionadas con el intercambio de mensajes (diálogo) entre los dos sistemas terminales.

Los dos servicios más importantes atribuidos al nivel de sesión son el control del diálogo y la separación del diálogo. El control del diálogo es el medio por el que los dos sistemas inician, intercambian mensajes y finalmente terminan, asegurando que cada sistema ha recibido los mensajes que le correspondían. La separación del diálogo es el proceso de insertar un marcador, llamado punto de comprobación, dentro del flujo de datos que circula entre dos sistemas, de modo que se pueda evaluar el estado de las dos máquinas en el mismo instante.

1.2.6.- Nivel de presentación

El nivel de presentación funciona principalmente como un servicio de paso a través, en el sentido de que recibe primitivas de nivel de aplicación y emite duplicados de esta primitiva al nivel de sesión, usando el Punto de Acceso del Servicio de Presentación (PSAP, Presentation Service Access Point) y el Punto de Acceso del Servicio de Sesión (SSAP, Session Service Access Point). Todo lo dicho en la sección anterior sobre aplicaciones que utilizan los servicios del nivel de sesión, implica en realidad la utilización del servicio de paso a través del nivel de presentación, porque para un proceso de cualquier nivel del modelo OSI, le es imposible comunicarse directamente con otro nivel que no esté inmediatamente por encima o por debajo. (Figura 7).

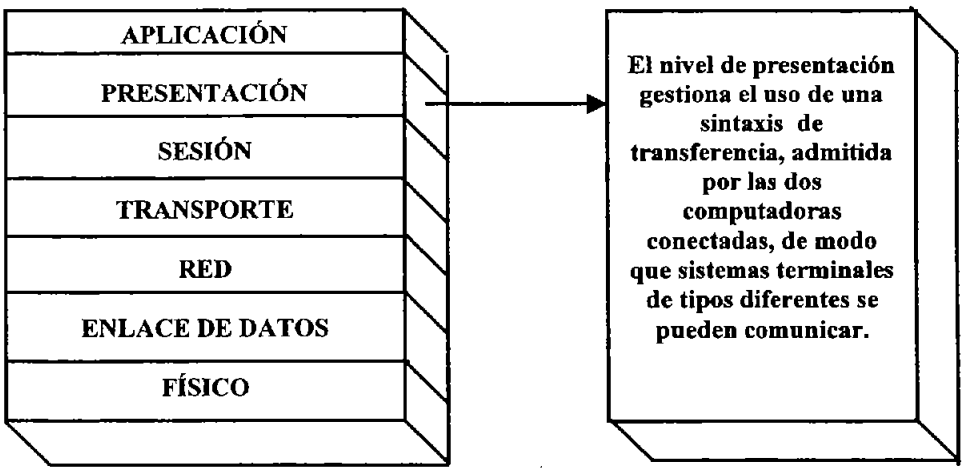


Figura 7

Mientras que las funciones básicas de las primitivas no cambian cuando pasan a través del nivel de presentación, pueden experimentar un proceso crucial de traducción, y de hecho ésta es la función principal del nivel.

1.2.7.- Nivel de aplicación

Como nivel superior de la pila de protocolos, el nivel de aplicación constituye el origen y destino último de todos los mensajes transmitidos por la red. todos los procesos analizados en las secciones previas son iniciados por una aplicación que demanda acceso a un recurso localizado en un sistema de la red. Sin embargo, los procesos del nivel de aplicación no son necesariamente sinónimos de las aplicaciones mismas. (Figura 8).

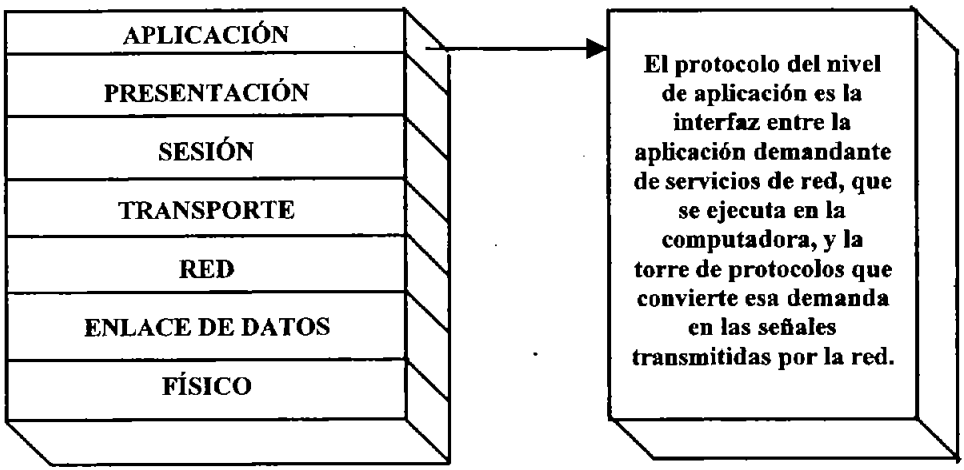


Figura 8

Cuando se ejecuta un cliente de FTP, la aplicación misma es inseparable del protocolo del nivel de aplicación que usa para comunicarse con la red. Otros protocolos íntimamente ligados a las aplicaciones que los usan son los siguientes:

- DHCP Protocolo de configuración dinámica de host
- FTP Protocolo básico de transferencia de archivos
- DNS Sistema de nombres de dominio
- NFS Sistema de archivos de red
- RIP Protocolo de información de enrutamiento
- BGP Protocolo de pasarela de borde

1.3.- Tipos de Redes

Las redes de computadoras de acuerdo a su extensión geográfica se clasifican de la siguiente manera: Red de Área Local LAN (Local Area Network), Red de Área Metropolitana MAN (Metropolitan Area Network), Red de Área Amplia WAN (Wide Area Network).

1.3.1.- Red de Área Local LAN (Local Area Network).

Es una red que permite compartir información y recursos con la característica de que la distancia entre las computadoras debe ser pequeña, esto es normalmente una LAN pertenece a una sola organización y se encuentra localizada en un solo edificio. (Figura 9) Los elementos que integran una red LAN son:

- Computadoras
- Periféricos
- Servidor
- Concentrador
- Tarjeta de interfase
- Cableado
- Sistema operativo de red

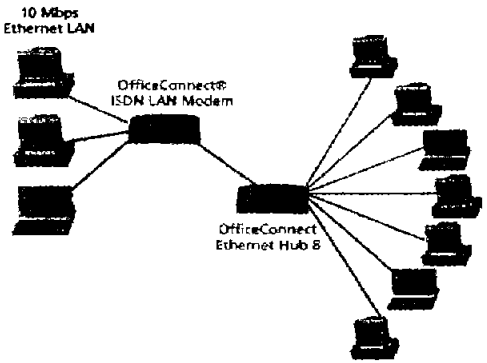


Figura 9

1.3.2.- Red de Área Metropolitana (MAN Metropolitan Area Network)

Una MAN es la conexión de redes locales y equipos periféricos que cubren un área superior a los 100 km, cuya velocidad es mayor a los 50 Mbps. Y dentro de las redes que enlaza, une desde 500 estaciones de trabajo en adelante. (Figura 10)

Este tipo de red puede ser privada o pública, los elementos que integran una red MAN además de los ya mencionados en las redes LAN son:

- Bridges
- Gateway
- Ruteadores

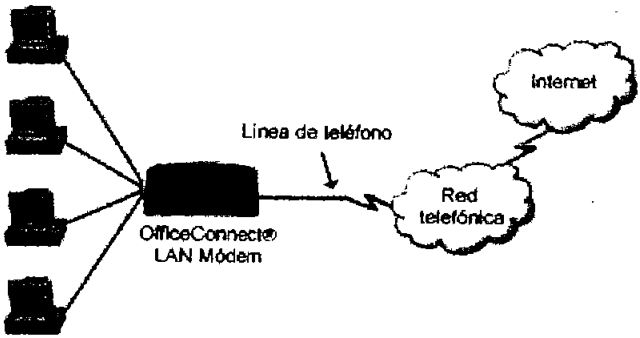


Figura 10

1.3.3.- Red de Área Amplia (WAN Wide Area Network)

Es una red comúnmente compuesta por varias redes Man y Lan interconectadas, pero con la característica de que la distancia entre las computadoras es amplia (de un país a otro o de un continente a otro) este tipo de redes se encuentran conectadas por medio de fibra óptica o por enlaces aéreos como satélites. (Figura 11). Los elementos que integran este tipo de redes son:

- Computadoras
- Periféricos
- Servidor
- Concentrador
- Tarjeta de interfase
- Cableado
- Sistema operativo de red
- Bridges
- Gateway
- Ruteadores

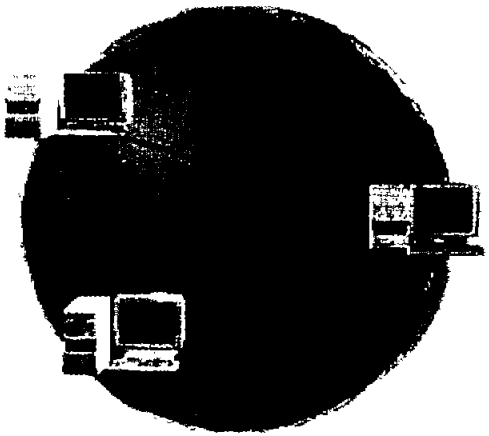


Figura 11

1.4.- Topologías

La topología de una red, se refiere a la forma de cómo va el cable de un nodo a otro, se puede ver como un "plano" del cableado.

Las estaciones de trabajo de una red se comunican entre sí mediante una conexión física y el objetivo de la topología es buscar la forma más económica y eficaz de conectarlas, para evitar los tiempos de espera en la transmisión de los datos, permitir un mejor control de la red y permitir de forma eficiente el aumento de las estaciones de trabajo:

Las topologías más comunes son:

- Topología en bus o lineal
- Topología en anillo
- Topología en estrella
- Topología en árbol

1.4.1.- Topología en bus

En esta topología todos los nodos comparten el mismo canal de comunicaciones; toda la información circula por ese canal y cada estación recoge la información que le corresponde, esta topología es muy conveniente para las redes debido a su bajo costo, pero está limitado en cuanto a la distancia, ya que no puede sobrepasar los 2000 metros de longitud.
(Figura 12)

La principal desventaja de la topología en bus radica en el hecho de que normalmente sólo hay un canal de comunicación para dar servicio a todos los dispositivos de la red.

Consecuentemente en el caso de una falla del canal de comunicación se paraliza toda la red.

Para que las señales no reboten dentro del bus, se utiliza un componente llamado terminador el cual es colocado en cada extremo del cable para absorber las señales libres.

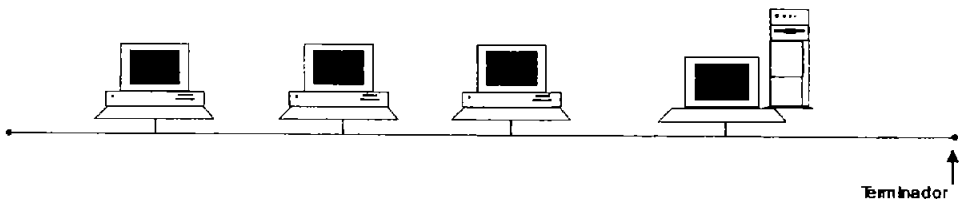


Figura 12

1.4.2.- Topología en anillo

En esta topología todas las estaciones están conectadas entre sí formando un anillo, de forma que cada estación sólo tiene conexión con otras dos. En las primeras redes de este tipo los datos se movían en una única dirección, de manera que todas las informaciones tenían que pasar por todas las estaciones hasta llegar a la de destino, donde se quedaban.

Las redes más modernas disponen de dos canales y transmiten en direcciones diferentes por cada uno de ellos. (Figura 13).

Este tipo de redes permite aumentar o disminuir el número de estaciones sin dificultad, pero a medida que aumenta el flujo de información, será menor la velocidad de respuesta de la red.

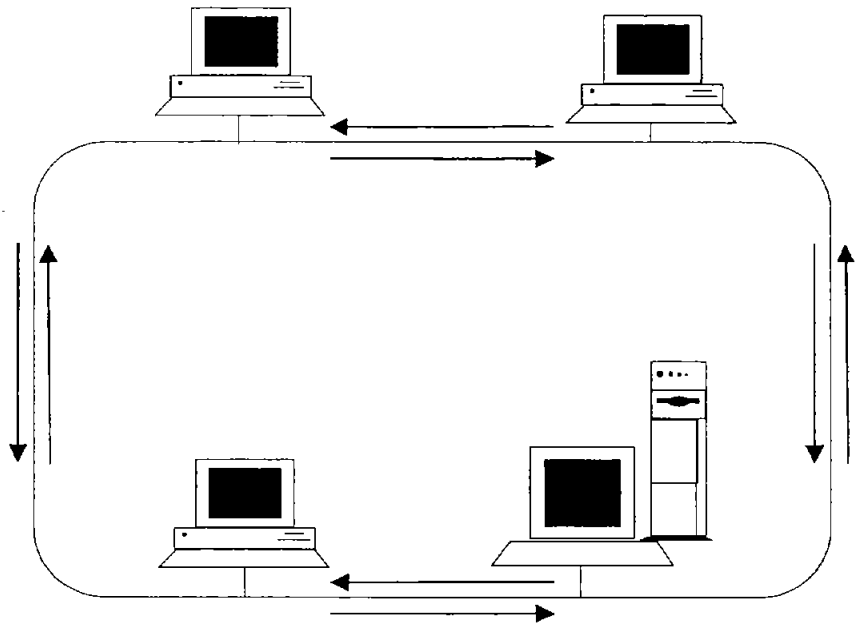


Figura 13

1.4.3.- Topología en estrella

En esta topología todas las estaciones se comunican entre sí a través de un dispositivo central Hub o Concentrador (Figura 14). Esto es todos los mensajes son enviados al concentrador para su reenvió a otros nodos. El uso de este controlador central para llevar a cabo todas las transferencias de información simplifica la estructura de los nodos, así el usar este controlador nos proporciona los medios de conectar más máquinas en la red sin grandes cambios en su estructura.

El fallo en un nodo de la red no repercute en el comportamiento global de la red, sólo afectará al tráfico relacionado con este nodo. En el caso de una falla en el medio de comunicación, sólo quedaría fuera de servicio el nodo afectado. El problema sería mayor si la falla estuviera en el HUB ya que todas las estaciones serían afectadas.

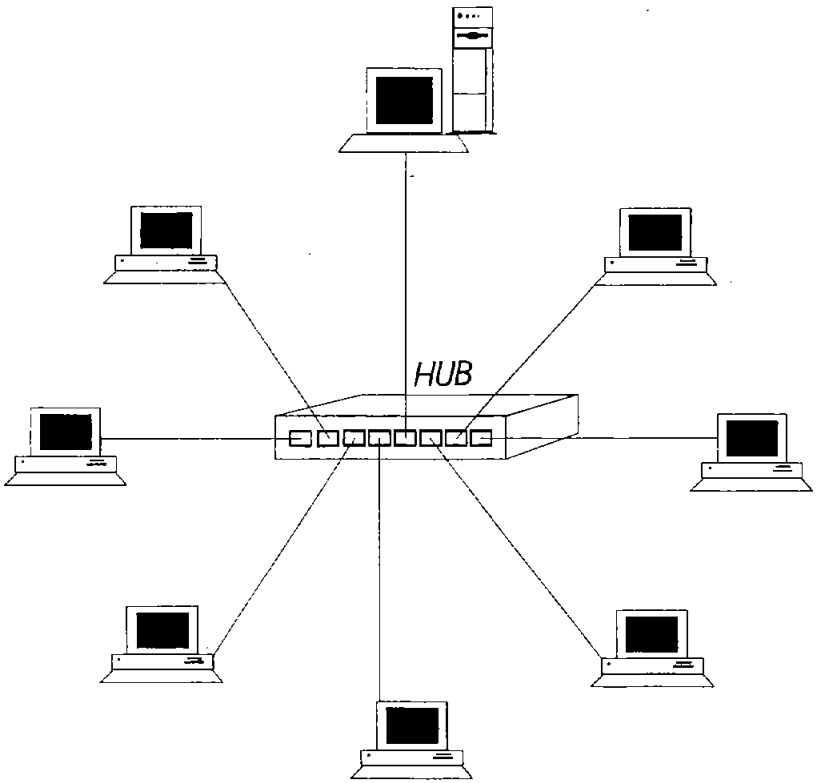


Figura 14

1.4.4.- Topología en árbol

En esta topología se tiene en el primer nivel (el más alto), el control de tareas y la resolución de los errores. En muchos casos se distribuyen dichos controles hacia los nodos inferiores para que a su vez tengan el control de los nodos que quedan debajo de ellos, y de esta manera no saturen el nodo maestro. (Figura 15)

Una de las desventajas que presenta es la formación de cuellos de botella en determinados momentos, con lo que puede verse considerablemente disminuida su fiabilidad.

Dependiendo de donde se quieran anexar nodos, puede o no afectarse a algunos de los que ya existan, por lo que no es recomendable redes con crecimiento a futuro. La comunicación entre nodos distantes puede provocar congestionamiento.

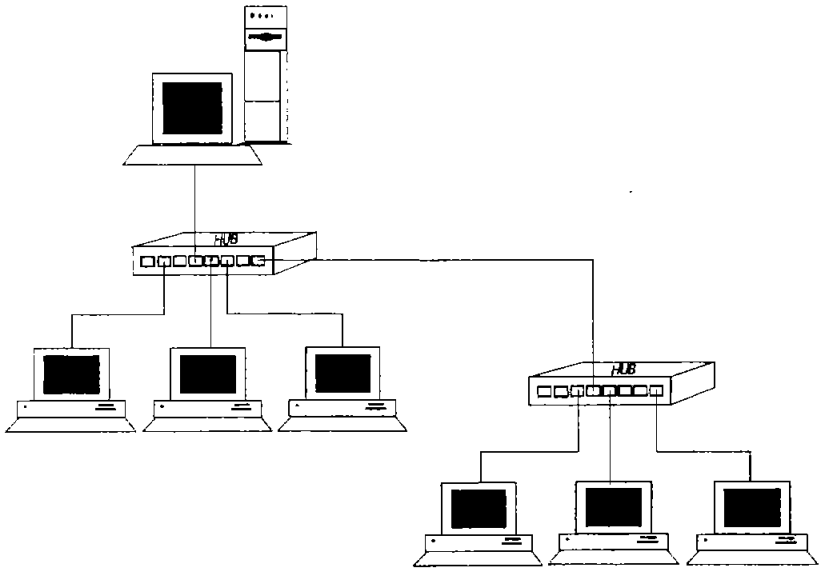


Figura 15

1.5.- Métodos de acceso al cableado (Protocolos de Contienda)

Estos métodos muestran como un nodo puede acceder a un sistema de cableado, los sistemas de cableado lineales pueden utilizar el método de detección de portadora, mientras que los sistemas en anillo o estrella pueden utilizar un método de pase de testigo. Una vez que la placa accede al cable comienza a enviar paquetes de información a otros nodos.

El proceso de transmisión de datos con lleva una serie de procedimientos que van desde el nivel físico hasta la presentación de la información en un formato determinado. Aunque todos ellos son fundamentales, veremos el nivel de enlace, que es el encargado del control de la comunicación.

Toda comunicación se puede dividir en tres fases: establecimiento de la comunicación, transferencia de la información y terminación. La forma de establecer y finalizar la comunicación depende de cómo estén conectadas las dos estaciones de trabajo (a través de un cable por el puerto serie o paralelo, a través de una línea punto a punto, a través de un módem, por la red telefónica, o mediante una tarjeta de red).

La forma de controlar la transferencia de la información depende exclusivamente del protocolo que se utilice, y deberá realizar las siguientes funciones:

- Sincronización de la comunicación.
- Control de los errores de transmisión.
- Coordinación de la comunicación.
- Recuperación ante los fallos que se produzcan.

Cuando se ha de transmitir una determinada información, ésta se distribuirá en bloques de una longitud determinada, dispuestos en un orden determinado y con un control de errores que permitirá comprobar que todos y cada uno de los bits enviados sean iguales a todos y cada uno de los bits recibidos. De esta forma, si se produjera un error en uno de los bloques, únicamente sería necesario volver a transmitir dicho bloque, sin necesidad de repetir toda la transmisión.

Entre los protocolos más adecuados se encuentran:

- Contienda Simple.
- Acceso múltiple por detección de portadora (CSMA).
- Acceso múltiple por detección de portadora con detección de colisiones (CSMA/CD).
- Llamada selectiva (polling).
- Paso de testigo (token passing).

1.5.1.- Contienda Simple

En este protocolo todas las estaciones comparten el mismo canal de transmisión y los mensajes se envían a través de dicho canal; las estaciones responden únicamente a los mensajes que incluyen su dirección y el resto los ignoran; mientras no reciban un mensaje que incluya su dirección, se encuentran en estado de espera, pero escuchando el canal de transmisión.

Por tanto, se pueden dar dos situaciones: que las estaciones se encuentren transmitiendo datos o que se encuentren en estado de espera.

Una estación envía los bloques de datos sin fijarse si el canal está disponible o no. Cuando un bloque de una estación coincide con el de otra, se produce una colisión y ambos se destruyen automáticamente. Si el bloque llega a su destino, la estación receptora envía un mensaje indicando que lo ha recibido. Si la estación emisora, después de un tiempo aleatorio, no ha recibido este mensaje, vuelve a repetir la transmisión del bloque y así sucesivamente hasta que haya finalizado la transmisión de datos.

Este tipo de protocolo no se utiliza en redes con cargas medias o altas, ya que se estarían produciendo colisiones constantemente y el rendimiento de la red sería muy bajo y con tiempos de espera muy grandes.

1.5.2.- Acceso Múltiple por Detección de Portadora (CSMA)

En este protocolo también se utiliza un único canal, pero una estación no transmite hasta que la línea está libre. Para ello, la estación emisora se pone a la escucha, en una frecuencia secundaria, para saber si hay otra estación que esté enviando algún bloque de datos.

Mientras se encuentra a la escucha, puede actuar de dos maneras distintas:

- Escuchar continuamente a la espera de que quede libre y entonces transmitir (detección continua de portadora).

- Escucha si el canal está ocupado. Si lo está, deja la transmisión un tiempo aleatorio y después vuelve a intentarlo (detección no continua de portadora).

Cuando la línea está libre, envía el bloque de datos y además, otra señal en la frecuencia secundaria para avisar a las demás estaciones de que la línea está ocupada.

Una vez transmitido el bloque de datos, la estación espera hasta recibir el mensaje de que la estación receptora ha recibido el bloque. Si no lo recibe o recibe una señal negativa, la estación supone que se ha producido una colisión (por haber iniciado dos estaciones emisoras un envió simultáneamente), espera un tiempo aleatorio y vuelve a enviar el bloque de datos.

Por tanto, se pueden dar tres situaciones: que las estaciones se encuentren transmitiendo datos, que se encuentren en estado de espera o que se encuentren escuchando la línea.

Este protocolo permite una mejora en comparación con el de contienda simple si la carga es baja o media y la red tiene una longitud pequeña, ya que entonces el tiempo que tarda la señal en propagarse es pequeño, y el riesgo de que dos estaciones decidan enviar bloques de datos simultáneamente y colisionen será bajo.

1.5.3.- Acceso Múltiple por Detección de Portadora con Detección de Colisiones (CSMA/CD)

El método de detección de portadora se utiliza fundamentalmente en los sistemas de cableado lineales. Antes de comenzar a transmitir, un nodo comprueba si el cable está siendo usado. Transmite a través de todo el cable, todos los otros nodos lo detectan y determinan si la transmisión está destinada a ellos, si no lo está, la rechazan. Si dos nodos emiten a la vez, se produce una colisión anulándose ambas emisiones; los nodos esperan un cierto tiempo aleatorio, para reducir la probabilidad de volver a colisionar y vuelven a transmitir. A medida que aumenta el tráfico en la red el rendimiento disminuye debido a las colisiones que obligan a efectuar retransmisiones. Sin embargo, las pruebas publicadas muestran que esta caída de rendimiento es mínima a menos que estén conectados cientos de nodos.

1.5.4.- Llamada selectiva (polling)

Para poder utilizar este protocolo, se necesita que la red disponga de dos tipos de estaciones: la estación principal y las secundarias.

Cada estación secundaria dispone de una zona de almacenamiento temporal, donde envía el bloque de datos que desea transmitir.

La estación principal comprueba en cada una de las secundarias si alguna tiene algún bloque de datos para transmitir. Si en alguna de ellas encuentra uno, se autoriza a dicha estación para que lo transmita de forma inmediata o al cabo de un determinado tiempo. Si no tiene ningún bloque de datos, pasa a revisar la estación siguiente, y así sucesivamente.

Los bloques de datos se pueden enviar de dos formas distintas:

- Pasando por la estación principal, la cual los reenvía a la estación destino.
- Enviándolos directamente a la estación destino.

Se puede indicar que el control sobre las estaciones secundarias tenga el mismo nivel de prioridad para todas o que las estaciones que cuentan con mayor actividad tengan una prioridad más alta. También se puede indicar que las estaciones que no estén activas no tengan control por parte de la estación principal.

Este tipo de protocolo cuenta con algunas ventajas con respecto a los de contienda:

- La longitud de los bloques es superior.
- Soporta un volumen mayor de carga en la red.
- Permite trabajar con longitudes de red mayores.

1.5.5.- Token Passing (Pase de testigo)

Este protocolo hace circular continuamente un grupo de bits (testigo) por la red. Este testigo está formado por una cabecera, un campo de datos y un campo final.

Cuando una estación quiere transmitir, ha de esperar a que llegue hasta ella el testigo vacío. En ese momento le añade unos datos, quedando el testigo formado por: la cabecera, la dirección destino, la dirección origen, el camino que ha de seguir para llegar a su destino y el bloque de datos, y lo envía a su destino.

Si la estación no desea transmitir, pasa el testigo vacío a la siguiente estación y así sucesivamente. El testigo ocupado llega a la estación destino, que recoge el bloque de datos, pone una marca en el testigo indicando si lo acepta o lo rechaza por venir con errores y lo devuelve a la estación que lo ha enviado.

Cuando llega a la estación que lo envió, ésta vuelve a enviarlo si llega con la marca de rechazado, envía el siguiente bloque de datos o vacía el testigo para que pase a la estación siguiente.

Este protocolo cuenta con bastantes ventajas:

- Elimina por completo el riesgo de colisiones.
- Puede emplear mensajes muy largos
- El volumen de carga es bastante alto
- El tamaño de la red puede ser grande

Está recomendado para redes con volumen de carga medio o alto y para una longitud media o grande de la red.

El método de pase de testigo se utiliza normalmente con las redes en anillo, o las que se comportan como anillos. El concepto de "testigo" se utiliza para definir como una estación de trabajo puede acceder al cable. Cuando una estación de trabajo está preparada para transmitir, debe esperar a que esté disponible.

1.6.- Arquitectura de las Redes Locales

Hay distintos tipos de redes locales, pudiéndose realizar múltiples combinaciones distintas al seleccionar el tipo de cableado, la topología, el tipo de transmisión e incluso los protocolos utilizados. Estos factores van a determinar la arquitectura de la red local.

Sin embargo, de todas las posibles soluciones hay tres que ya están establecidas y que, al mismo tiempo, cuentan con una gran difusión dentro del mundo de las redes locales:

- **Ethernet**
- **Token Ring**
- **Arcnet**

1.6.1.- Ethernet

Esta red fue desarrollada por Xerox Corporation para enlazar un grupo de microcomputadores que estaban distribuidos por los laboratorios de investigación de Palo Alto en California, para poder intercambiar programas y datos, así como compartir los periféricos.

Ethernet puede resumirse brevemente como un bus, con una distancia máxima de 2,500 m y una velocidad de 10 mbps sobre cable en banda base, con un número máximo de 1024 estaciones de trabajo, y una longitud de cable de un segmento de 500 m (10base5) o 180m (10base2). Como todas las redes que trabajan en banda base, la transmisión es de naturaleza half–duplex, es decir, sólo una estación puede transmitir en un tiempo dado.

El protocolo que soporta Ethernet es CSMA/CD (Carrier Sense Múltiple Access with Collision Detection). Acceso Múltiple por Detección de Portadora con Detección de Colisiones.

Con este protocolo cada estación está a la escucha de cualquier señal que haya sido previamente enviada por otra estación antes de emprender cualquier acción. Si la red está activa, la estación pospone su intento de transmisión. Por el contrario si la red está inactiva, la estación transmite pero continua a la escucha durante la transmisión para detectar la presencia de otras señales. Si la estación durante este tiempo de transmisión detectara a otra estación que a su vez ha iniciado la transmisión se produciría una colisión.

En un principio se creó para ser utilizada con cable coaxial de banda base, aunque actualmente se pueden utilizar otros tipos de cable.

Si se utiliza cable coaxial grueso, se pueden tener hasta cuatro tramos de cable (unidos con repetidores) y las computadoras se conectan al cable por medio de transceptores.

Se pueden conectar computadoras en tres tramos únicamente, con un máximo de 100 estaciones en cada tramo.

La conexión de Ethernet al cable coaxial se denomina transceptor, tanto 10base5 como 10base2 se refieren a el como MAU (Médium Attachment Unit) unidad de acceso al medio, aunque este dispositivo en el caso de 10base2 esté incorporado en la propia tarjeta de red. (Figura 16).

De la misma manera 10base5 llama al cable entre el transceptor y la tarjeta adaptadora de red, cable AUI (Attachment Unit Interfaz). 10base2 no requiere un cable AUI.

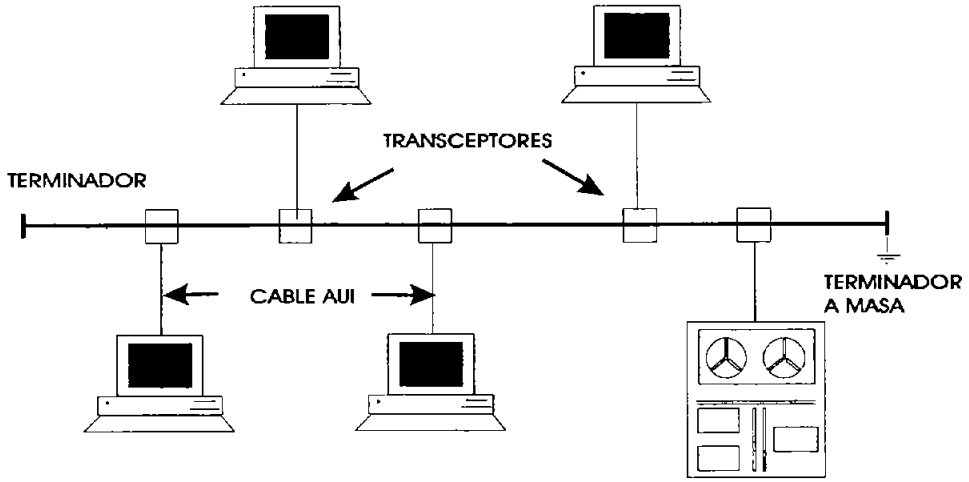


Figura 16

Todas las estaciones tienen asignada una dirección de 48 bytes, que permite que cuando se cambia de lugar una estación no haya posibilidad de conflictos, y por tanto se puede reconfigurar completamente la red local con unos mínimos cambios en el sistema operativo.

Si se utiliza cable coaxial fino, no es necesario utilizar transceptores, pudiéndose conectar el cable a la computadora por medio de una conexión BNC en forma de T. El número máximo de tramos es de cinco, y la longitud máxima de cada tramo es de 185m. (Figura 17).

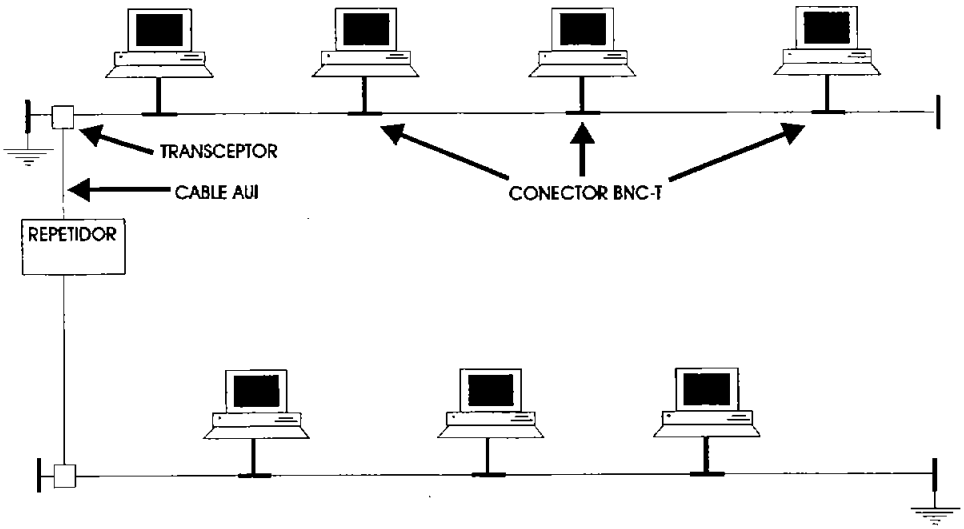


Figura 17

1.6.2.- Token Ring

Esta arquitectura de red fue creada por IBM en Octubre de 1985, aunque anteriormente había comercializado dos tipos de redes locales: una red de banda base a 375 kilobaudios y para un máximo de 64 computadores y una red de banda ancha a 2 megabaudios para un máximo de 72 computadores.

Emplea una topología de anillo con protocolo de paso de testigo y se puede utilizar cable de par trenzado, cable coaxial y fibra óptica.

Los datos se transmiten a una velocidad de 4 megabaudios pudiéndose conectar hasta un máximo de 8 computadores y a una distancia máxima de 350 metros en cada unidad de acceso multiestación (MAU) si se utiliza con cable coaxial (si se utiliza con fibra óptica, puede llegar hasta una velocidad de 16 magabaudios).

No obstante, como se pueden conectar hasta 12 unidades de acceso multiestación, el número de computadores conectados y la distancia máxima pueden aumentar considerablemente.

La red Token-Ring se adhiere al estándar IEEE 802.5 y está actualmente soportada por un número importante de fabricantes, entre ellos, IBM, Proteon, Racore, Gateway Communications, 3 COM, D-LINK. El comité IEEE 802.5 se formó en 1980, anunciando después IBM y Texas Instruments un acuerdo para desarrollar conjuntamente un juego de chips que implementará Token Ring. Este acuerdo culminó en 1985 con el juego de chips TMS380 compuesto de cinco componentes.

Arquitectura Token Ring

El componente básico de la red en anillo es un dispositivo denominado MAU (Multistation Access Unit) Unidad de Acceso Multiestación o también WC (Wire Concentrador) Concentrador de Cableado. Este dispositivo es el punto central de conexión de los nodos de la red. (Figura 18).

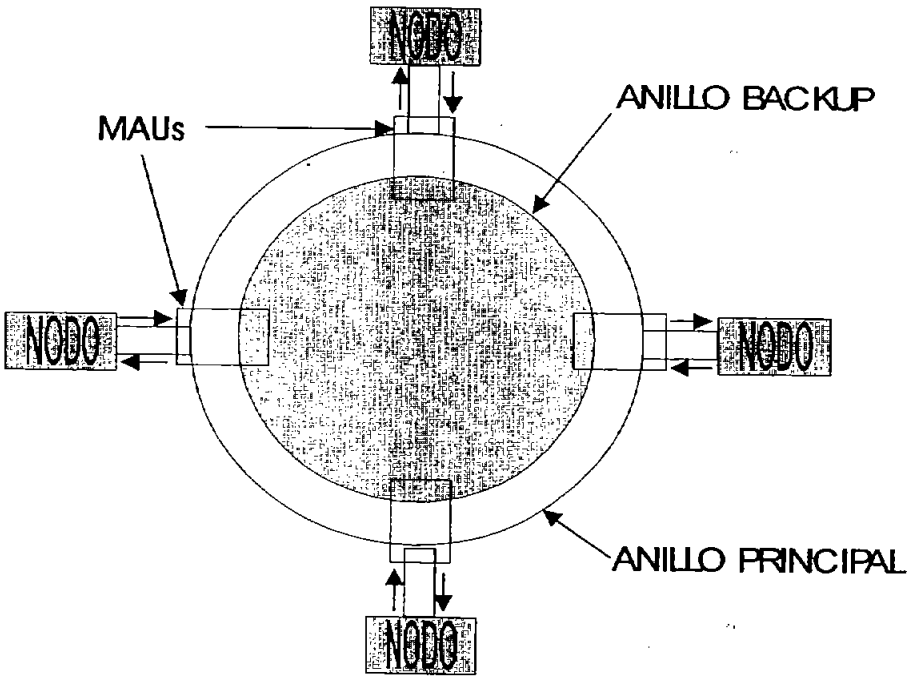


Figura 18

1.6.3.- ARCNet

ARCNet – Attached Resource Computer Network es uno de los sistemas de redes existentes más antiguos. Fue desarrollado en 1977 por Datapoint Corporation, Arcnet ha llegado a ser uno de los sistemas de hardware para redes más populares en el mundo, estimándose en un 25% su penetración en el mercado de redes. Según NOVELL más de la mitad de instalaciones en todo el mundo sobre Netware están usando hardware Arcnet.

¿Por qué una red que ni siquiera lleva el sello de homologación de los IEEE es tan popular? Hay varias e importantes razones para ello: su fiabilidad, flexibilidad y facilidad de instalación, funcionamiento y facilidad de localización de averías.

Hay un consenso general entre los revendedores de redes e instaladores diciendo que Arcnet es la red mas fácil de instalar y de diagnosticar sus averías. Los controladores Arcnet (tarjetas adaptadoras de red) muy raramente causan problemas y lo que es más importante debido a su topología de estrella, es muy fácil aislar secciones de la red para su diagnóstico.

ARCNet con sus 2.5 Mbps de velocidad no es la red más rápida disponible, pero su protocolo de token – passing proporciona un funcionamiento muy razonable que no se degrada bajo un tráfico pesado, como ocurriría con una red Ethernet CSMA/CD.

La topología estándar para ARCNet es en estrella, aunque también puede usarse en bus o una combinación de ambas a la que podemos denominar de estrella distribuida con las estaciones conectadas a un dispositivo central Concentrador (Hub).

Existen dos tipos de Hubs para ARCNet, activos y pasivos. Un hub activo es una unidad con su propia alimentación que actúa como un dispositivo de distribución y amplificador de señal. En cambio un hub pasivo sólo distribuye la señal sin amplificarla, y sólo tiene 4 puertos de conexión, para 4 tarjetas de red ARCnet. (Figura 19).

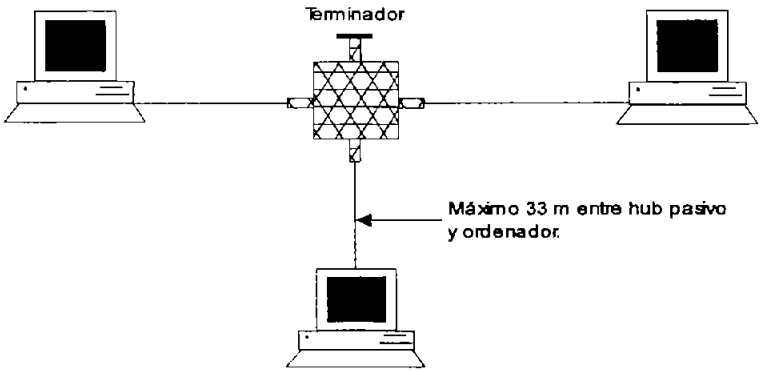


Figura 19

Los hubs activos pueden tener entre 2 y 64 puertos. Si utilizamos hubs activos como repetidores de señal, una red ARCNet puede llegar a tener una distancia máxima de 6,000 metros entre nodos.

ARCNet transmite todas las señales a través de toda la red simultáneamente. Esto se debe a que usa una topología de bus lógico, donde todos los dispositivos comparten el mismo cable. haciendo posible que todo dispositivo de red puede hablar y oír a todos. En el diseño de Token-Ring esto no es posible, ya que las estaciones sólo pueden hablar a las que están directamente conectadas.

Este tipo de arquitectura comenzó siendo un sistema de proceso distribuido de Datapoint.

Es una red en banda base que utiliza una topología mixta estrella / bus con protocolo de paso de testigo.

Transmite a una velocidad de 2.5 mega baudios y todos los computadores han de estar conectados a un concentrador, HUB activo. La distancia máxima entre el computador y el HUB activo no puede sobrepasar los 650 metros.

No obstante, se puede conectar mas de un HUB activo, por lo que el número máximo de estaciones puede llegar a ser de 255.

CAPÍTULO II

REDES INALÁMBRICAS

2.1.- WLAN

WLAN son las siglas en inglés de Wireless Local Area Network (Red de Área Local Inalámbrica). Es una red inalámbrica la cual podemos considerar como un sistema de comunicación de datos flexible muy utilizado como alternativa a la LAN cableada o como una extensión de ésta. Utiliza tecnología de radio frecuencia que permite mayor movilidad a los usuarios. Últimamente han ido ganando adeptos y se empieza a consolidar como una tecnología madura y robusta que permite resolver varias de las restricciones derivadas de la utilización de medios físicos en las redes locales convencionales.

Actualmente cobran cada vez mas sentido, desde el momento en que los usuarios necesitan ser más móviles. Las redes inalámbricas, permiten su conexión a la red de datos sin necesidad de llevar molestos cables y tener que encontrar un punto de red al cual conectarse. Basta una computadora portátil y una tarjeta de red inalámbrica, para que el usuario pueda moverse con su equipo a distintas salas de reuniones, vestíbulos, salones de clase etc.

Las redes inalámbricas ofrecen toda una serie de ventajas sobre las cableadas como:

- Gran flexibilidad dentro del área de cobertura.
- Posibilidad de construir redes sin infraestructura ni planeación previa.
- Robustez frente a contingencias.
- Elimina los problemas del cableado

Pero también cuenta con algunos inconvenientes como pueden ser:

- Velocidad generalmente menor que las cableadas.
- Regulaciones nacionales, licencias etc.
- Mayores problemas de seguridad.
- Costo de los equipos generalmente mayor.

Ante la existencia de dispositivos WLAN de diferentes fabricantes, se hizo necesaria la existencia de recomendaciones (contenidas en los estándares), para permitir a los productos de estas firmas, una operación adecuada entre sí y que, además, se cumpliera con un mínimo establecido de calidad y funcionalidades.

Los estándares WLAN iniciaron con el estándar 802.11, desarrollado en 1997, por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE). Estos estándares permiten transmisiones de datos de hasta 2 Mbps, transferencias que han sido mejoradas con el paso del tiempo. Las extensiones a estas reglas se reconocen con la adición de una letra al estándar original.

2.2.- Normas IEEE 802 para LAN

Los comités 802 del IEEE se concentran principalmente en la interfaz física relacionada con los niveles físicos y de enlace de datos del modelo de referencia OSI de la ISO.

Entre los productos que siguen las normas 802 se incluyen tarjetas de interfaz de red, bridges, routers y otros componentes utilizados para crear LANs de par trenzado y cable coaxial.

Tabla de normas del estándar 802 IEEE

802.1	Da una introducción al conjunto de normas y define las primitivas de interfaz, para interconexión de redes.
802.2	Describe la parte superior de la capa de enlace que utiliza el protocolo LLC.
802.3	Describe la norma CSMA/CD.
802.4	Describe la norma token bus.
802.5	Describe la norma token ring.
802.6	Red de Área Metropolitana MAN
802.7	Grupo asesor para técnicas de banda ancha
802.8	Grupo asesor para técnicas de fibra óptica.
802.9	Redes integradas para voz y datos.
802.10	Seguridad de red.
802.11	Redes inalámbricas.
802.12	LAN de acceso de prioridad bajo demanda (100VG-Any LAN).

Tabla 1

Como podemos ver en la tabla 1 todo el estándar 802 se refiere a redes pero en este momento el estándar que nos interesa y que veremos más a fondo es el 802.11 el cual se refiere a las Redes Inalámbricas y define la velocidad de transmisión así como el tipo de modulación y la frecuencia en la cual puede transmitir.

2.3.- Norma IEEE 802.11: Redes inalámbricas.

Originalmente cuando se creó el estándar en 1997 por la IEEE sólo se estableció que las transmisiones de datos fueran de hasta 2 Mbps, pero por las necesidades de tener una mayor velocidad y mejor rendimiento de las redes inalámbricas se fueron haciendo modificaciones y mejoras hasta llegar a todas las variaciones con las que contamos actualmente. En la tabla 2 se muestran las diferentes especificaciones de los estándares.

Estándar	Descripción
802.11	Estándar WLAN original. Soporta de 1 a 2 Mbps.
802.11a	Estándar WLAN de alta velocidad en la banda de los 5GHz. Soporta hasta 54 Mbps.
802.11b	Estándar WLAN para la banda de 2.4GHz. Soporta 11 Mbps.
802.11e	Está dirigido a los requerimientos de calidad de servicio para todas las interfaces IEEE WLAN de radio.
802.11f	Define la comunicación entre puntos de acceso para facilitar redes WLAN de diferentes proveedores.
802.11g	Establece una técnica de modulación adicional para la banda de los 2.4GHz. Dirigido a proporcionar velocidades de hasta 54 Mbps.
802.11h	Define la administración del espectro de la banda de los 5GHz. Para su uso en Europa y en Asia Pacífico.
802.11i	Está dirigido a abatir la vulnerabilidad actual en la seguridad para protocolos de autentificación y de codificación. El estándar abarca los protocolos 802.1X, TKIP (Protocolo de Llaves Integras, Seguras Temporales) y AES (Estándar de Encriptación Avanzado).

Tabla 2

De los estándares anteriores el más utilizado es el 802.11b el cual fue ratificado por el IEEE en julio de 1999, y opera en un ancho de banda que abarca las frecuencias dentro del rango de 2.4 a 2.497GHz. Del espectro de radio. El método de modulación que utiliza es el DSSS (Modulación de Secuencia Directa de Espectro Extendido) usando CCK (Modulación por Cambios de Código Complementarios), lo cual le permite alcanzar una velocidad máxima de hasta 11 Mbps.

La especificación 802.11a también fue ratificada en Julio de 1999 pero los productos se hicieron disponibles en el mercado hasta el año 2001, de tal forma, que su despliegue no fue tan amplio como sucedió con 802.11b. El 802.11a opera con frecuencias que van desde los 5.15 a los 5.875GHz. El método de modulación que utiliza es el OFDM (Multiplexación por División de Frecuencias Ortogonales), el cual hace posible que se alcancen velocidades de hasta 54 Mbps.

El 802.11a representa la próxima generación de tecnología LAN inalámbrica para empresas, con ventajas sobre soluciones actuales. A velocidades de 54 Mbps y mayores es más rápido que cualquier otra solución sin licencia. Además el 802.11a brinda una mayor velocidad en toda el área de cobertura.

Dada su capacidad se puede ocupar el 802.11a para aplicaciones que comprenden video, voz y la transmisión de imágenes y ficheros grandes. O para dar soporte a áreas con numerosos usuarios que no necesitan demasiado ancho de banda, como por ejemplo, para navegar por Internet.

Por último el 802.11g opera en la banda de los 2.4GHz, por lo que si es compatible con Wi-Fi y 802.11b, pero a diferencia de éste último que tan solo alcanza los 11 Mbps, con 802.11g podemos alcanzar los 54 Mbps. La modulación que se utiliza es OFDM y CCK.

Como hemos visto la frecuencia más utilizada por los estándares es la de 2.4Ghz. Debido a que dicha frecuencia es libre en prácticamente todos los países del mundo, ya que se trata de una frecuencia reservada para la investigación, educación o sanidad.

Sin embargo en muchos países algunas frecuencias dentro de los 2.4Ghz. están reservadas para que solamente las puedan usar el ejército o los gobiernos.

Es por eso que hay que ser cuidadoso al hacer las compras del equipo ya que podemos adquirir determinados productos que tengan cerrados algunos canales los cuales utilizan las frecuencias que están reservadas en ese país.

En la tabla 3 podemos ver una lista de la relación entre los canales y la frecuencia de esta manera podemos saber exactamente que frecuencia utiliza cada canal.

Relación entre canal y frecuencia	
[illegible]	[illegible]
1	2.412 Ghz
2	2.417 Ghz
3	2.422 Ghz
4	2.427 Ghz
5	2.432 Ghz
6	2.437 Ghz
7	2.442 Ghz
8	2.447 Ghz
9	2.452 Ghz
10	2.457 Ghz
11	2.462 Ghz
12	2.467 Ghz
13	2.472 Ghz
14	2.484 Ghz

Tabla 3

En la tabla 4 podemos ver los canales disponibles dependiendo de cada país.

Países y Canales	
[illegible]	[illegible]
Europa (ETSI)	1 - 13
USA (FCC)	1 - 11
Francia	10 - 13
Japón	1 - 14

Tabla 4

2.4.- Mecanismos de seguridad

En los inicios de la tecnología inalámbrica, los procedimientos y mecanismos de seguridad eran tan débiles que podía ganarse acceso con relativa facilidad hacia redes WLAN de compañías desde la calle.

Existe el término "wardriving", que se refiere a la acción de recorrer una ciudad para buscar la existencia de redes inalámbricas y ganar acceso a ellas. En la actualidad, existen técnicas más sofisticadas y complejas, las cuales fortalecen los inconvenientes de los mecanismos WLAN y ayudan a mantener la confidencialidad y resistencia ante los ataques dirigidos hacia este tipo de redes.

El estándar inalámbrico 802.11 original incorpora encriptación y autentificación WEP (Privacidad Equivalente a Cable).

Sin embargo, en el 2001 se publicaron artículos que comunicaban las deficiencias que enfrentaba dicho mecanismo. Al interceptar y decodificar los datos transmitidos en el aire, y en cuestión de horas en una red WLAN con tráfico intenso, la clave WEP puede ser deducida y se puede ganar acceso no autorizado.

Esta situación desencadenó una serie de acciones por parte del IEEE y de la industria para mejorar la seguridad en las redes de tecnología inalámbrica.

La seguridad WLAN abarca dos elementos:

- El acceso a la red.
- La protección de los datos (autentificación y encriptación, respectivamente).

Las violaciones a la seguridad de la red inalámbrica, generalmente, vienen de los puntos de acceso no autorizados, aquéllos instalados sin el conocimiento de los administradores de la red, o que operan con las funcionalidades de protección deshabilitadas (que es la configuración por omisión en los dispositivos inalámbricos).

Estos "hoyos" en la seguridad, pueden ser aprovechados por personal no autorizado (hackers), que en caso de que logren asociarse con el punto de acceso, ponen en riesgo no únicamente la infraestructura inalámbrica, sino también la red alámbrica a la cual se conecta si es el caso.

La tabla 5 contiene los mecanismos de seguridad usados en redes WLAN, así como las ventajas y desventajas de cada uno de ellos.

Mecanismo de seguridad	Descripción
Especificación original 802.11	Utiliza tres mecanismos para proteger las redes WLAN: • SSID (Identificador de Servicio): es una contraseña simple que identifica la WLAN. Los clientes deben tener configurado el SSID correcto para acceder a la red inalámbrica. El uso del SSID como método único de control de acceso a la infraestructura es peligroso, porque típicamente no está bien asegurado; comúnmente el punto de acceso está configurado para distribuir este parámetro en su señal guía (beacon). • Filtrado con dirección MAC (Control de Acceso al Medio) restringe el acceso a computadoras cuya dirección MAC de su adaptador está presente en una lista creada para cada punto de acceso en la WLAN. Este esquema de seguridad se rompe cuando se comparte o se extravía el adaptador inalámbrico. • WEP (Privacidad Equivalente a Cable): es un esquema de encriptación que protege los flujos de datos entre clientes y puntos de acceso como se especifica en el estándar 802.11. Aunque el soporte para WEP es opcional, la certificación Wi-Fi exige WEP con llaves de 40 bits. El estándar recomienda dos esquemas para definir las llaves WEP. En el primer esquema, un conjunto de hasta cuatro llaves establecidas es compartido por todas las estaciones (clientes y puntos de acceso). El problema con estas llaves es que cuando se distribuyen ampliamente, la seguridad se ve comprometida. En el segundo esquema cada cliente establece una relación de llaves con otra estación. Este método ofrece una alternativa más segura, porque menos estaciones tienen las llaves, pero la distribución de las mismas se dificulta con el incremento en el número de estaciones.
802.1X	• Para contrarrestar los defectos de la seguridad WEP, el IEEE creó el estándar 802.1X. Se trata de un mecanismo de seguridad diseñado para proporcionar acceso controlado entre dispositivos inalámbricos clientes, puntos de acceso y servidores.

	• Emplea llaves dinámicas en lugar de llaves estáticas usadas en la autentificación WEP, y requiere de un protocolo de autentificación para reconocimiento mutuo. Es necesario un servidor que proporcione servicios de autentificación remota de usuarios entrantes (RADIUS, Servicio Remoto de Autentificación de Usuarios Entrantes).
WPA (Wi-Fi Protected Access)	• Contiene los beneficios de encriptación del protocolo de integridad de llave temporal (TKIP, Protocolo de Llaves Integras –Seguras– Temporales). TKIP fue construido tomando como base el estándar WEP, además está diseñado y analizado con detalle por importantes criptógrafos para reforzar la protección ofrecida en las redes WLAN. • También emplea 802.1X como método de autentificación en conjunto, con uno de los protocolos EAP estándar disponibles. EAP (Protocolo de Autentificación Extensible) es un protocolo punto a punto que soporta múltiples métodos de autentificación. • Debido a que la tecnología WLAN se basa en transmisión sobre ondas de radio, con cobertura en áreas que pueden ser ambientes públicos o privados, se han tomado en cuenta importantes consideraciones acerca de la seguridad en la red; las actividades están dirigidas por la especificación de seguridad WPA (Acceso de Protección Wi-Fi) desarrollada por el IEEE en conjunto con la alianza Wi-Fi. • Esta especificación proporciona una mayor encriptación de datos para corregir las vulnerabilidades de seguridad WEP, además de añadir autentificación de usuarios que no se habían contemplado.

Tabla 5

2.5.- Por que usar una red Inalámbrica.

En general los motivos que impiden la utilización del cable para la unión de segmentos o dispositivos de red pueden dividirse en dos grupos bien diferenciados. Por un lado, tenemos aquellas situaciones en las cuales, debido a los accidentes naturales o a las normativas que rigen el cableado no es posible el tendido de cables para completar la infraestructura de enlace físico de nuestra red.

Por otro lado, la complejidad de las actuales organizaciones y las crecientes necesidades en cuanto a disponibilidad y movilidad de sus trabajadores, demandan soluciones más acordes con el nuevo estilo de los negocios.

En el primer caso, indudablemente se hace del todo necesario la búsqueda de tecnologías alternativas que posibiliten el enlace, según el tráfico de información y la distancia, se requerirá de un sistema u otro.

Por el contrario, en el segundo caso, y a medida que crecen las capacidades de los medios informáticos, se precisa la creación de entornos de trabajo en grupo para dar cabida a la creciente demanda de servicios. Según los objetivos a cumplir y la rapidez de su puesta en marcha, éstos podrán tener una infraestructura más o menos duradera, como en caso de tener que dar soporte a convenciones, estar ocupando sedes provisionales o sufrir con relativa frecuencia profundos cambios en la organización de la red.

Para entender mejor la necesidad de este tipo de redes, plantearemos un problema común en cualquier empresa provista de una infraestructura informática de cierto calibre. No es extraño que nuestra hipotética empresa disponga de una oficina arrendada y sus correspondientes puestos de trabajo, acomodados según la estructura inicial del tendido de cable. Debido a la buena marcha del negocio nos vemos en la necesidad de ampliar el número de empleados y consecuentemente el número de estaciones de trabajo. Para ello, será necesario realizar una ampliación de la red.

Entre los muchos inconvenientes que surgen durante el tendido del cable, seguramente el menor de todos será el que tengan que soportar nuestros trabajadores ante la incomodidad de los trabajos de reacondicionamiento del entorno.

Y si después de todo este esfuerzo nuestros directivos deciden cambiar la sede a otro edificio por sus mejores condiciones económicas o situación estratégica, toda la inversión realizada en la adecuación de la infraestructura se perderá.

Pues bien, la adopción de una red inalámbrica puede evitar estos inconvenientes y algunos más, con el atractivo adicional de tener una conexión inmediata y móvil. Este argumento es más habitual de lo que pueda parecer a primera vista, siendo fruto de pormenorizados estudios. Según los informes realizados por compañías especializadas, un nodo de red, por norma general, se reubica por lo menos una vez cada dos años, sin considerar la gran cantidad de nodos que se agregan durante ese período.

Esta reestructuración lleva consigo un considerable gasto que puede dividirse en un 40 por ciento de mano de obra, un 30 por ciento de cableado y conectores, y el otro 30 por ciento restante en pérdida de la productividad debido al tiempo en que estará inactivo el sistema. Por si este desalentador panorama no fuera suficiente, y retomando el ejemplo anterior, el tiempo invertido en su instalación sobrepasa con creces al tiempo necesario para la instalación de una red inalámbrica, y no digamos ya si en el tendido del cable debe realizarse procurando reducir al máximo el impacto sobre la estética de la oficina.

En definitiva, las redes inalámbricas pueden usarse en multitud de lugares y situaciones como en la creación de redes temporales (exposiciones, ferias, certámenes, etc) o para enlazar edificios cercanos permanentemente. Igualmente, son útiles en el control de procesos en compañías como actualizar inventarios desde la misma planta de producción o en la creación de puntos móviles de ventas y atención al cliente.

Ejemplos de uso: ventas al pormenor, almacenes, manufacturación, etc, de modo que se transmite la información en tiempo real a un procesador central. Cada día se reconocen más este tipo de redes en un amplio número de negocios y se augura una gran extensión de las mismas y altas ganancias.

Es clara la alta dependencia en los negocios de la redes de comunicación. Por ello la posibilidad de compartir información sin que sea necesario buscar una conexión física permite mayor movilidad y comodidad.

Asímismo la red puede ser más extensa sin tener que mover o instalar cables.

2.5.1.- Áreas críticas

Para hacer frente a las necesidades de conexión, existen cuatro áreas críticas que los sistemas de conectividad inalámbrica deben cumplir:

- **Altos rendimientos.** El mundo LAN cableado ya ha alcanzado las velocidades de 100 Mbps (Fast Ethernet) y 1.000 Mbps (Gigabit Ethernet), y muy pronto llegará a 10.000 Mbps (10 Gigabit Ethernet). Al mismo tiempo, la potencia de la informática móvil y la riqueza de los contenidos en red no paran de crecer rápidamente. Por ello, todos los esfuerzos de la industria y los cuerpos de estandarización deben ir hacia la ampliación de la capacidad de las WLAN y evitar que se conviertan en un cuello de botella.

- **Movilidad.** Aunque siempre han existido los usuarios móviles, sólo ahora pueden estar conectados mientras se desplazan. Puesto que la mayoría de los actuales sistemas de hardware y software se diseñaron para usuarios fijos, dotar de la suficiente inteligencia a los sistemas de red inalámbricos es una cuestión crítica a la hora de dar soporte a estos usuarios móviles, a fin de que estén conectados sin interrupciones del servicio.

- **Seguridad.** Dado que la transmisión de señales inalámbricas no puede ser limitada enteramente al espacio privado de una empresa, las WLAN han de contar con sistemas de seguridad fiables y sencillos.

- **Gestión.** Para garantizar el rendimiento, la movilidad y la seguridad, es fundamental proporcionar las herramientas apropiadas para configurar estas opciones, monitorear las redes inalámbricas y localizar los problemas así como darles solución a los problemas.

2.6.- Medios de Transmisión.

Existen varias tecnologías utilizadas en redes inalámbricas. El empleo de cada una de ellas depende mucho de la aplicación. Cada tecnología tiene sus ventajas y desventajas. A continuación se listan las más importantes en este género.

- Infrarrojo (Infrared)
- Banda Angosta (Narrowband)
- Espectro Extendido (Spread Spectrum)

2.6.1.- Infrarrojo.

Los sistemas de comunicación por infrarrojo utilizan muy altas frecuencias, justo abajo del espectro de la luz visible para transportar datos. Como la luz, el infrarrojo no puede penetrar objetos opacos, ya sea directamente (línea de vista) o indirectamente (tecnología difundida/reflectiva). El alto desempeño del infrarrojo directo es impráctico para usuarios móviles pero su uso es recomendable para conectar dos redes fijas. La tecnología reflectiva no requiere línea de vista pero está limitada a cuartos individuales en zonas relativamente cercanas. Se utilizan en redes personales de área reducida y ocasionalmente en LAN's específicas. No es práctico para redes de usuarios móviles por lo que únicamente se implementa en subredes fijas. Los sistemas de difusión IR no requieren línea de visión pero las células están limitadas a habitaciones individuales. La siguiente figura muestra un transreceptor. (Figura 20).

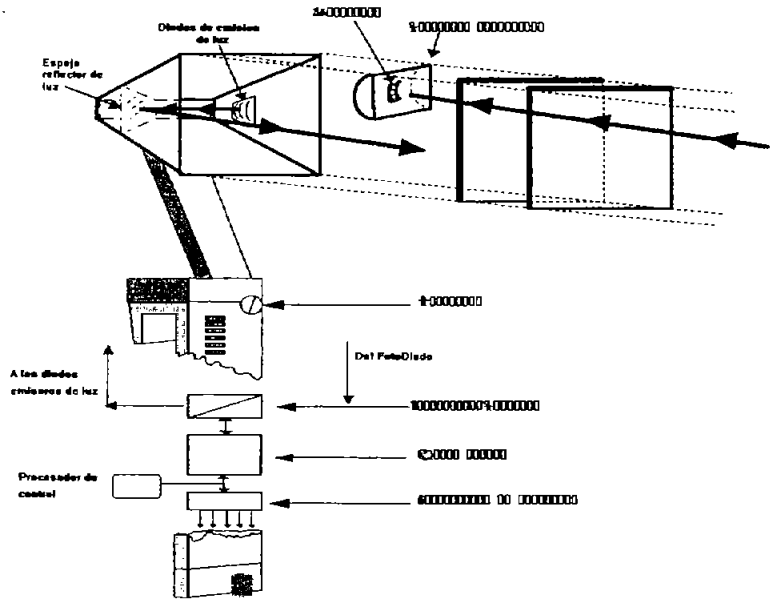


Figura 20

2.6.2.- Banda Angosta.

Un sistema de radio de banda angosta transmite y recibe información en una radio frecuencia específica. La banda amplia mantiene la frecuencia de la señal de radio tan angostamente posible para pasar la información. El cruzamiento no deseado entre canales es evitado al coordinar cuidadosamente diferentes usuarios en diferentes canales de frecuencia.

En un sistema de radio la privacidad y la no-interferencia se incrementan por el uso de frecuencias separadas de radio. El radio receptor filtra todas aquellas frecuencias que no son de su competencia ya que su uso requiere de la autorización del organismo regulador, en el caso norteamericano, una vez que una cierta banda de frecuencias es asignada a un usuario, ella no puede ser asignada a ningún otro usuario dentro de un radio de 30 km. lo cual es impráctico si se tienen muchos usuarios.

2.6.3.- Espectro Extendido.

Es el usado por la mayor parte de los sistemas sin cable. La gran mayoría de los sistemas inalámbricos emplean la tecnología de Espectro Extendido (Spread Spectrum), una tecnología de banda ancha desarrollada por los militares estadounidenses que provee comunicaciones seguras, confiables y de misión critica.

La tecnología de Espectro Extendido está diseñada para intercambiar eficiencia en ancho de banda por confiabilidad, integridad y seguridad. Es decir, más ancho de banda es consumida con respecto al caso de la transmisión en banda angosta, pero el 'trueque' [ancho de banda/potencia] produce una señal que es en efecto más fuerte y así más fácil de detectar por el receptor que conoce los parámetros de la señal de espectro extendido que está siendo difundida.

Si el receptor no está sintonizado a la frecuencia correcta, una señal de espectro extendido se miraría como ruido en el fondo. Otra característica del espectro disperso es la reducción de interferencia entre la señal procesada y otras señales no esenciales o ajenas al sistema de comunicación.

Hay dos tipos de tecnología en banda ancha:

- Frecuencia esperada (FHSS: Frecuency-Hopping Spread Spectrum): utiliza una portadora de banda estrecha que cambia la frecuencia a un patrón conocido por transmisor y receptor. Tanto receptor como receptor están debidamente sincronizados comunicándose por un canal que está cambiado a cada momento en frecuencia. FHSS es utilizado para distancias cortas, en aplicaciones por lo general punto a multipunto, donde se tienen una cantidad de receptores diseminados en una área relativamente cercana al punto de acceso.

- Secuencia directa (DSSS: Direct-Sequence Spread Spectrum): se genera un patron de bits redundante por cada bit transmitido. Estos bits redundantes son llamados "chipping code". Cuanto mayor sea esta secuencia, mayor es la probabilidad de reconstruir los datos originales (también se requiere mayor ancho de banda). Incluso si uno o más bits son perturbados en la transmisión, las técnicas implementadas en radio pueden reconstruir los datos originales sin necesidad de retransmitir. Para un receptor cualquiera DSSS es un ruido de baja potencia y es ignorado. DSSS se utilizará comúnmente en aplicaciones punto a punto.

2.6.4.- Qué no es espectro extendido

Conviene tener presente que existen equipos que utilizan estas mismas frecuencias y que producen una energía de radiofrecuencia, pero que no transmiten información. Estos equipos tienen aplicaciones Industriales, Científicas y Médicas (ICM) y en particular dichos equipos operan en otras bandas de frecuencia [902-908 MHz; 2,400-2,500 MHz y 5,525-5,875 MHz]. Ejemplos de estos equipos son: limpiadores domésticos de joyería, humidificadores ultrasónicos, calefacción industrial, hornos de microondas, etc.

2.7.- Cómo funciona una WLAN.

Se utilizan ondas de radio o infrarrojos para llevar la información de un punto a otro sin necesidad de un medio físico. Las ondas de radio son normalmente referidas a portadoras de radio ya que éstas únicamente realizan la función de llevar la energía a un receptor remoto. Los datos a transmitir se superponen a la portadora de radio y de este modo pueden ser extraídos exactamente en el receptor final. Esto es llamado modulación de la portadora por la información que está siendo transmitida. De este modo la señal ocupa más ancho de banda que una sola frecuencia. Varias portadoras pueden existir en igual tiempo y espacio sin interferir entre ellas, si las ondas son transmitidas a distintas frecuencias de radio. Para extraer los datos el receptor se sitúa en una determinada frecuencia ignorando el resto. En una configuración típica de LAN sin cable los puntos de acceso (transceiver) conectan la red cableada de un lugar fijo mediante cableado normalizado. El punto de acceso recibe la información, la almacena y transmite entre la WLAN y la LAN cableada. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

El punto de acceso (o la antena conectada al punto de acceso) es normalmente colocado en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada. El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, vía una antena.

La naturaleza de la conexión sin cable es transparente al sistema del cliente.

2.8.- Configuración de la WLAN

Pueden ser simples o complejas. La más básica se da entre dos ordenadores equipados con tarjetas adaptadoras para WLAN, de modo que pueden poner en funcionamiento una red independiente siempre que estén dentro del área que cubre cada uno. Esto es llamado red de igual a igual.

Cada cliente tendría únicamente acceso a los recursos de otro cliente pero no a un servidor central. Este tipo de redes no requiere administración o preconfiguración. (Figura 21).

Figura 21

Instalando un Punto de Acceso (APs) se puede doblar el rango al cual los dispositivos pueden comunicarse, pues actúan como repetidores. Desde que el punto de acceso se conecta a la red cableada cualquier cliente tiene acceso a los recursos del servidor y además actúan como mediadores en el tráfico de la red en la vecindad más inmediata. Cada punto de acceso puede servir a varios clientes, según la naturaleza y número de transmisiones que tienen lugar. Existen muchas aplicaciones en el mundo real con entre 15 y 50 dispositivos cliente en un solo punto de acceso. (Figura 22).

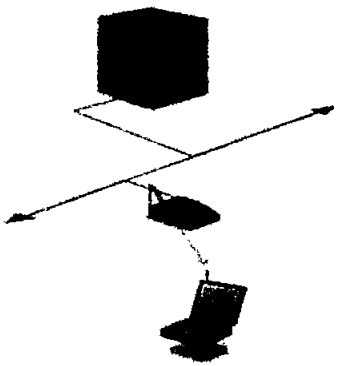


Figura 22

Los puntos de acceso tienen un rango finito, del orden de 150m en lugares cerrados y 300m en zonas abiertas. En zonas grandes como por ejemplo un campus universitario o un edificio es probablemente necesario más de un punto de acceso. La meta es cubrir el área con células que solapen sus áreas de modo que los clientes puedan moverse sin cortes entre un grupo de puntos de acceso. Esto es llamado "roaming". (Figura 23).

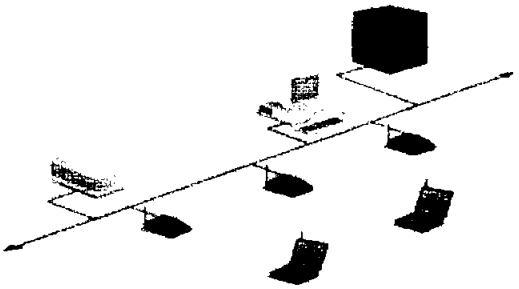


Figura 23

Para resolver problemas particulares de topología, el diseñador de la red puede elegir usar un Punto de Extensión (EPs) para aumentar el número de puntos de acceso a la red, de modo que funcionan como tales pero no están enganchados a la red cableada como los puntos de acceso. Los puntos de extensión funcionan como su nombre indica: extienden el rango de la red retransmitiendo las señales de un cliente a un punto de acceso o a otro punto de extensión. Los puntos de extensión pueden encadenarse para pasar mensajes entre un punto de acceso y clientes lejanos de modo que se construye un "puente" entre ambos. (Figura 24).

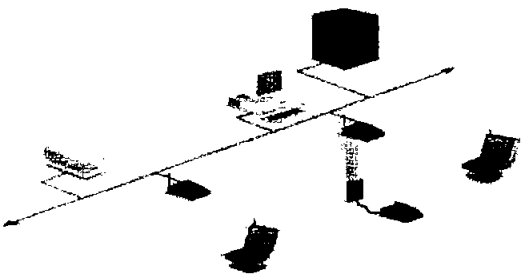


Figura 24

Uno de los últimos componentes a considerar en el equipo de una WLAN es la antena direccional. Por ejemplo: se quiere una Lan sin cable a otro edificio a 1Km de distancia. Una solución puede ser instalar una antena en cada edificio con línea de visión directa. La antena del primer edificio está conectada a la red cableada mediante un punto de acceso. Igualmente en el segundo edificio se conecta un punto de acceso, lo cual permite una conexión sin cable en esta aplicación. (Figura 25).

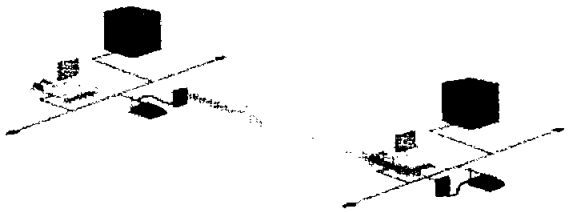


Figura 25

2.9.- Cobertura

La distancia que pueden alcanzar las ondas de Radiofrecuencia (**RF**) o de Infrarojos (**IR**) es en función del diseño del producto y del camino de propagación, especialmente en lugares cerrados. Las interacciones con objetos, paredes, metales, e incluso la gente, afectan a la propagación de la energía. Los objetos sólidos bloquean las señales de infrarrojos, esto impone límites adicionales. La mayor parte de los sistemas de redes inalámbricas usan RF porque pueden penetrar la mayor parte de lugares cerrados y obstáculos. El rango de cobertura de una Lan inalámbrica típica va de 30m. a 100m. Puede extenderse y tener posibilidad de alto grado de libertad y movilidad utilizando puntos de acceso (microcélulas) que permiten "navegar" por la Lan.

2.10.- Rendimiento

Depende de la puesta a punto de los productos así como del número de usuarios, los factores de propagación (cobertura, diversos caminos de propagación), y del tipo de sistema inalámbrico utilizado. Igualmente depende del retardo y de los cuellos de botella de la parte cableada de la red.

Para la más comercial de las redes inalámbricas los datos que se tienen hablan de un rango de 1.6 Mbps. Los usuarios de Ethernet o Token Ring no experimentan generalmente gran diferencia en el funcionamiento cuando utilizan una red inalámbrica. Éstas proporcionan suficiente rendimiento para las aplicaciones más comunes de una Lan en un puesto de trabajo, incluyendo correo electrónico, acceso a periféricos compartidos, acceso a Internet, y acceso a bases de datos y aplicaciones multiusuario. Como punto de comparación una Lan inalámbrica operando a 1.6 Mbps es al menos 30 veces más rápida.

2.11.- Bluetooth

Los primeros pasos en el largo camino que ha significado el desarrollo de la tecnología Bluetooth sucedieron en 1994, cuando la compañía Ericsson Mobile Communications decidió investigar la viabilidad de desarrollar un radio, de bajo costo y corto alcance, que sirviera de interfase entre los teléfonos móviles y sus accesorios. La idea consistía en construir un pequeño radio y colocarlo dentro de un teléfono celular y una computadora portátil para reemplazar el cable que hasta ese momento era indispensable para conectar ambos aparatos. En febrero de 1998 fue creado el Grupo Especial de Interés (SIG, por sus siglas en inglés). Actualmente son nueve de las empresas más importantes del mundo (3Com, Ericsson, IBM, Intel, Agere Systems, Microsoft, Motorola, Nokia y Toshiba) quienes forman el grupo promotor dentro del consorcio Bluetooth, formado por cerca de 1,900 fabricantes de todos los sectores que colaboran conjuntamente en el desarrollo e implantación de la nueva tecnología.

Bluetooth es un transmisor de radiofrecuencia muy pequeño que permite conectar entre sí todo tipo de dispositivos electrónicos (teléfonos, ordenadores, impresoras, faxes, etc). Cualquier aparato Bluetooth puede asumir la función de un "maestro" o un "esclavo", dependiendo del escenario de aplicación. Para hacer posible la comunicación, Bluetooth emplea el Salto de Frecuencias de Espectro Libre (Frecuency Hopping Spread Spectrum). Para hacer realidad la comunicación entre múltiples aparatos Bluetooth, todos deben estar sincronizados en la misma frecuencia. El aparato "maestro" es quien establece la secuencia y los "esclavos" se sincronizan con él.

La potencia de transmisión es de hasta 100 mW. La distancia nominal de enlace va desde los 10 cm a 10 metros, pudiéndose alcanzar hasta los 100 metros incorporando la potencia necesaria. El transmisor está integrado en un pequeño microchip de 9x9 milímetros y opera en una frecuencia de banda global de 2.4 GHz (utilizada en muchos países para usos médicos y científicos) que asegura la compatibilidad universal y no requiere licencia para operar en ella.

Los dispositivos que incorporan Bluetooth se reconocen y hablan de la misma forma que lo hace un ordenador con su impresora. El canal permanece abierto y no requiere la intervención directa y constante del usuario cada vez que se quiere enviar algo. La tasa binaria es de hasta 1Mb/s, utilizándose para transmitir paquetes de pequeña longitud y un salto de frecuencia muy rápido. Esto reduce el efecto de interferencias con otros dispositivos y mejora la transmisión. El transmisor permite enviar voz y datos a una velocidad máxima de 700 Kb/seg. y consume un 97% menos de energía que un teléfono móvil. Además, es inteligente: cuando el tráfico de datos disminuye el transmisor adopta el modo bajo de consumo de energía.

La tecnología inalámbrica Bluetooth emplea una banda de frecuencias disponible en todo el mundo (2,4 GHz) para asegurar la compatibilidad en todos los países. En dos palabras: la tecnología Bluetooth libera los periféricos digitales y convierte los cables en cosa del pasado.

CAPÍTULO III

INFRAESTRUCTURA ACTUAL DE LA RED EN ARAGÓN

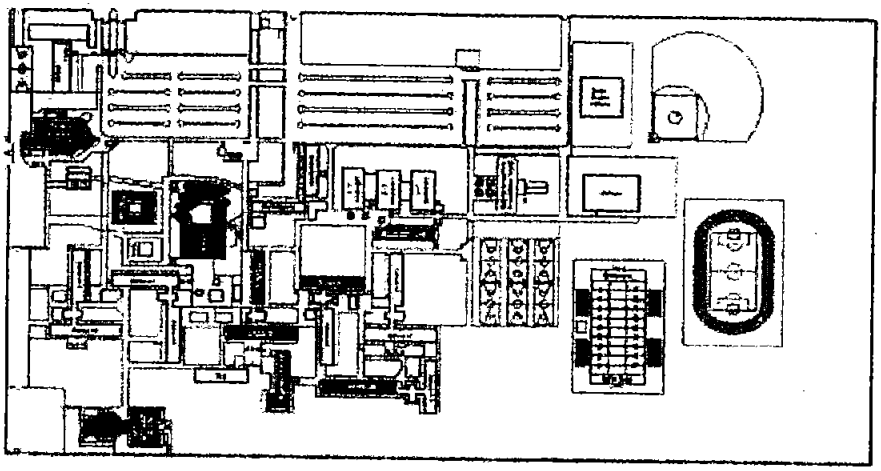
3.1.- Introducción

La base medular (actualmente) de la Red local de cómputo de la ENEP Aragón está compuesta por cable par trenzado, cabe mencionar que la entrada y salida de la señal es a través de un enlace tipo E1, el cual nos enlaza a CU, dicha conexión se encuentra ubicada en el edificio de mantenimiento y a partir de este punto la señal se reparte vía fibra óptica a nueve edificios. En la tabla 6 se describen cuales son estos edificios así como el segmento de red al que están conectados.

	Edificio	Segmento de Red
1.	Biblioteca	132.248.44
2.	Gobierno	132.248.44
3.	Servicios Escolares (ubicado en el edificio A1)	132.248.44
4.	Centro de Cómputo	132.248.145
5.	Posgrado (ubicado en el edificio A12)	132.248.145
6.	CAE (ubicado en el edificio A5)	132.248.173
7.	Centro Tecnológico	132.248.173
8.	Fundación UNAM y Revisión de Estudios (ubicados en el edificio A4)	132.248.173 y 44
9.	Laboratorio de Eléctrica y Electrónica (ubicado en el L3)	132.248.173

Tabla 6

En el mapa 1 se muestran los diferentes segmentos de la red así como los edificios a los cuales pertenece, el color azul representa el segmento 44, el color café el segmento 145 y el color verde el segmento 173. También se muestra en el diagrama 1 la situación actual de la red en la Enep Aragón.



Mapa 1

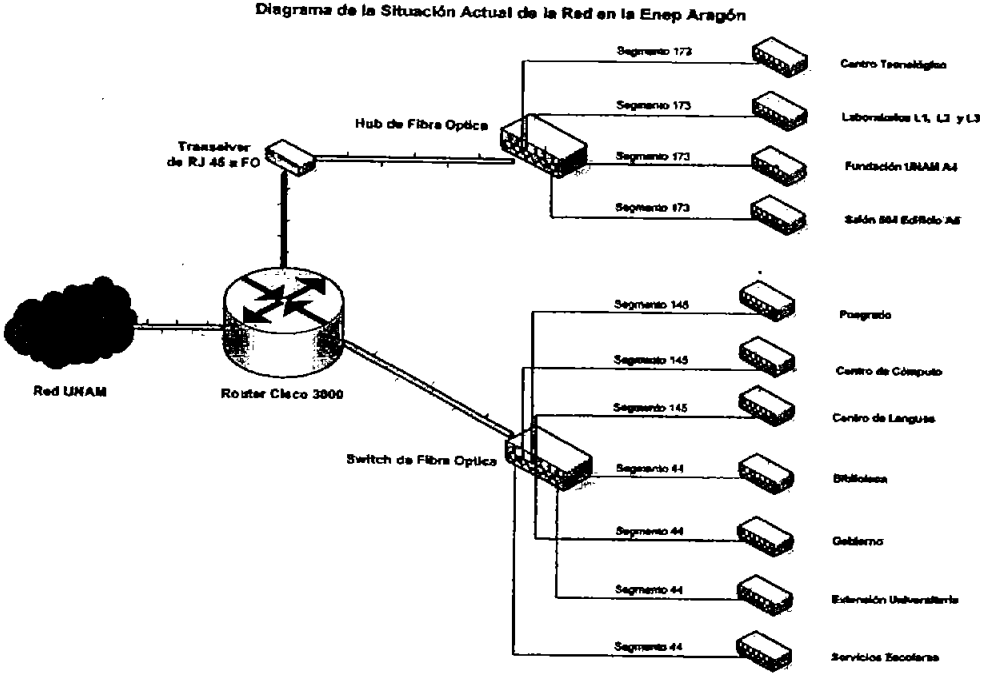


Diagrama 1

3.2.- Biblioteca

Ésta es la encargada de resguardar todo el acervo bibliográfico de la escuela, así como de brindar un servicio de catálogo en línea lo cual permite a los alumnos poder localizar fácilmente cualquier publicación que pertenezca al acervo de la UNAM. También cuenta dentro de sus instalaciones con tres salas de cómputo, las cuales pertenecen a Fundación UNAM estas salas proporcionan los siguientes servicios: Acceso a Internet, Cursos de Cómputo, Escáner, Impresiones en Plotter y Láser. (Figura 26 y 27).

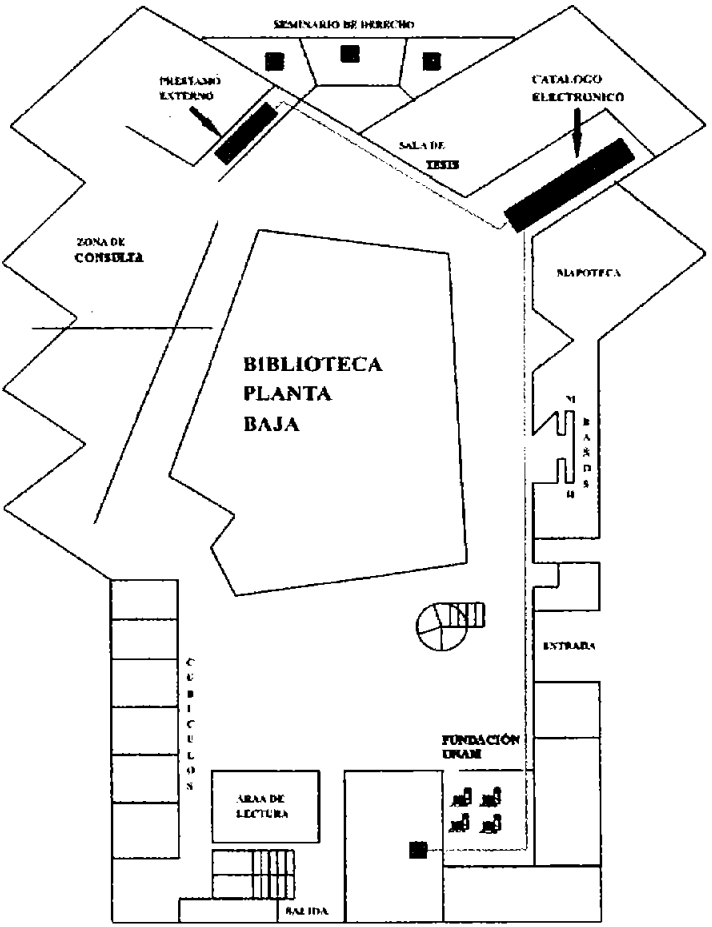


Figura 26

La señal de red llega a través de una fibra óptica la cual viene del Edificio de Mantenimiento y llega a un transceiver el cual convierte la señal a par trenzado y de ahí se deriva a seis concentradores los cuales alimentan toda la biblioteca.

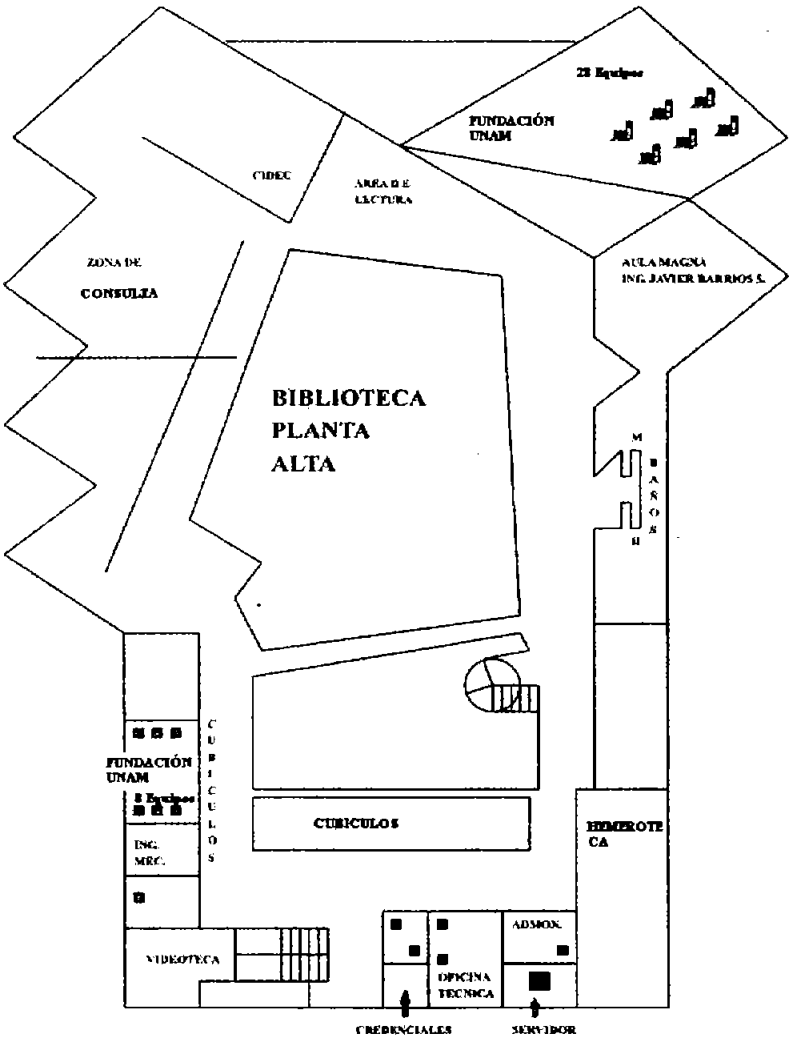


Figura 27

3.3.- Edificio de Gobierno

Es importante mencionar que anteriormente este edificio tenía una infraestructura de cable coaxial, la cual generaba bastantes problemas en el manejo de información y en la comunicación con otras áreas, es por eso que a partir de la construcción del segundo nivel de este edificio se decidió instalar el cableado estructurado en sus tres niveles que son los siguientes:

- Planta Baja: Se localizan todas las jefaturas de carrera las cuales son las encargadas de manejar toda la información relacionada con los alumnos. (Figura 28).

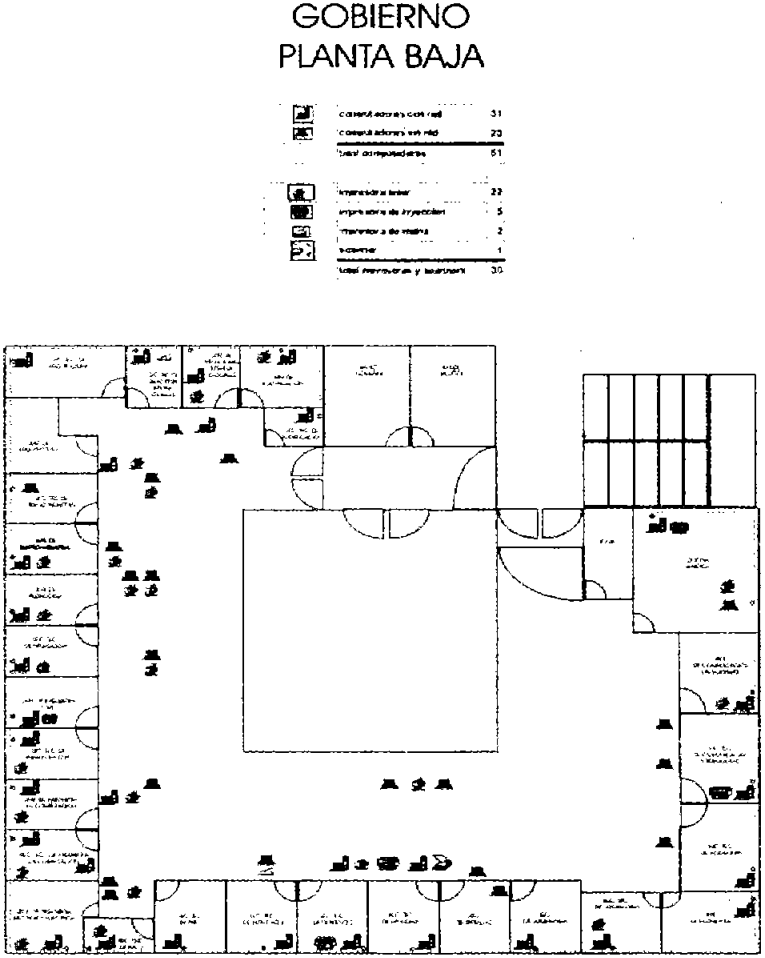


Figura 28

- Primer Piso: En este piso se encuentra la Dirección, la Secretaría General y Particular, estas oficinas son críticas debido a la importancia de ellas. Las Jefaturas de División, Unidad Académica y la Coordinación de Apoyo a la Comunidad, siendo éstas las áreas encargadas de controlar el ámbito académico de la escuela. (Figura 29).

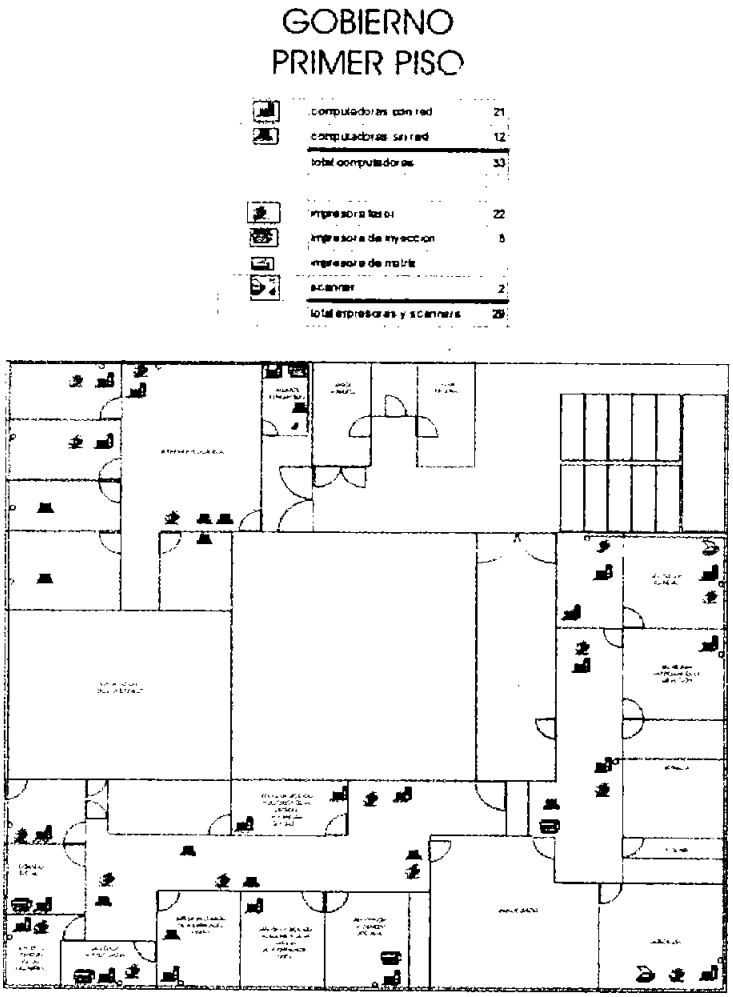


Figura 29

- Segundo Piso: Aquí se ubican la Unidad Administrativa (encargada del manejo administrativo de todo el plantel), Servicio Social, Personal, Unidad de Planeación y la Unidad de Sistemas y Servicios de Cómputo. (Figura 30).

GOBIERNO
SEGUNDO PISO

	computadoras con red	60
	computadoras sin red	18
	total computadoras	78
	impresora laser	23
	impresora de inyeccion	9
	impresora de matriz	2
	scanner	1
	total impresoras y scanners	35

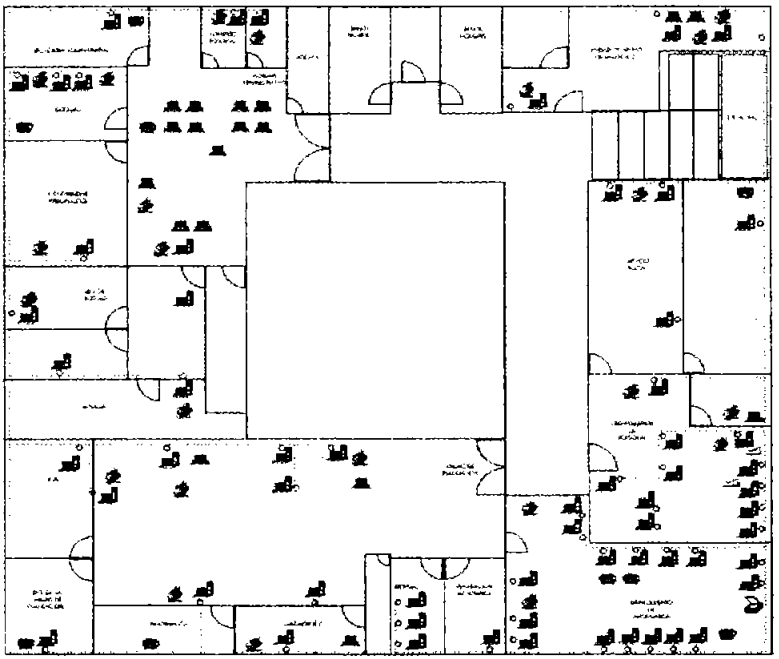


Figura 30

3.4.- Edificio A1 (Servicios Escolares)

En este edificio se encuentran ubicadas las oficinas de Servicios Escolares, esta área es la encargada de realizar la transmisión en línea de la información contenida en las actas de calificaciones, las inscripciones, trámites de titulación, así como todo tipo de trámite escolar que necesiten llevar a cabo los alumnos y ex alumnos del plantel, para poder realizar este tipo de trámites es necesaria la conexión a la red, la cual es a través de una conexión de Fibra Óptica que sale del edificio de Mantenimiento y llega a un transceiver el cual tiene como función recibir la señal de fibra y convertirla a señal de cable par trenzado, después de éste se conecta a un concentrador marca 3Com de 24 puertos que es el que distribuye la señal a toda el área. (Figura 31 y 32).

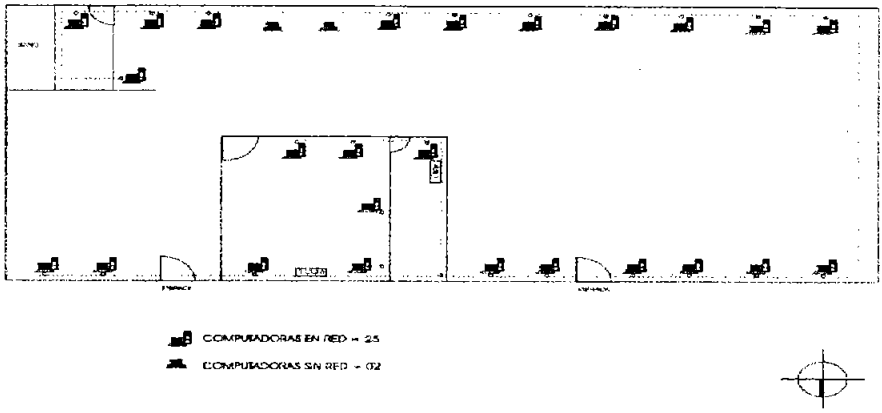


Figura 31

Figura 32

3.5.- Centro de Cómputo

Aquí se proporcionan servicios de Internet, correo electrónico aparte de otros servicios a los alumnos y académicos de esta escuela. Para ello se cuenta con 8 salas, una para profesores y las demás para los alumnos, (Figura 33). En cada sala se tiene instalado un concentrador, y éstos a su vez llegan a un switch, el cual se enlaza con el transceiver que es a donde llega la fibra óptica que viene del edificio de mantenimiento.

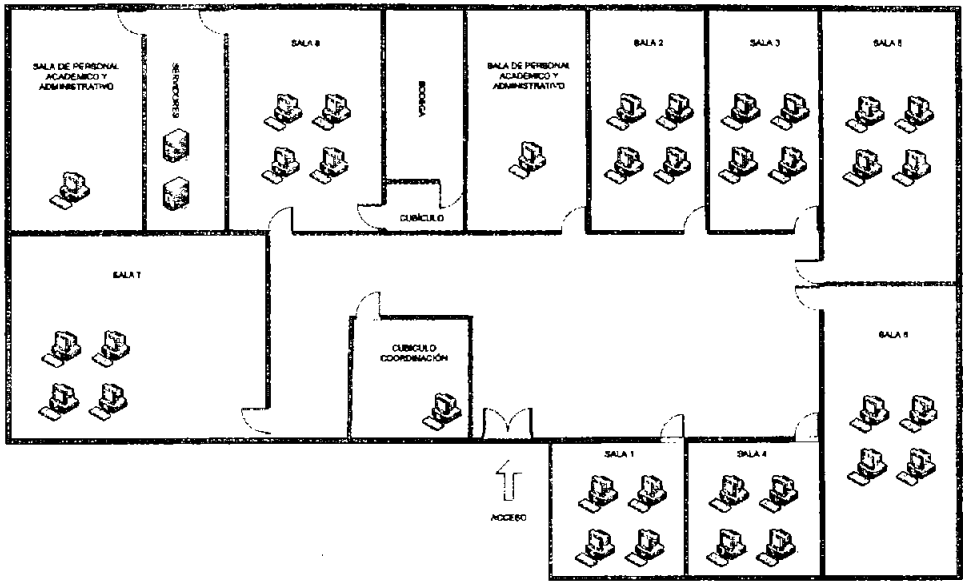


Figura 33

- La sala 1 cuenta con 20 Equipos Pentium IV con 128 Mb. de Ram y DD.de 40 Gb.
- La sala 2 cuenta con 19 Equipos Pentium III con 128 Mb. de Ram y DD. de 9 Gb.
- La sala 3 tiene 28 Equipos Pentium II con 64 Mb. de Ram y DD. de 6 Gb.
- La sala 4 tiene 10 Equipos Pentium III con 128 Mb. de Ram y DD. de 10 Gb. También cuenta con 15 Equipos Pentium IV con 512 Mb. de Ram y DD. de 80 Gb.
- La sala 5 tiene 19 Equipos Pentium I con 32 Mb. de Ram y DD. de 2 Gb.
- La sala 6 cuenta con 20 Equipos Pentium IV con 256 Mb. de Ram y DD. de 40 Gb.
- La sala 7 cuenta con 20 Equipos Pentium IV con 256 Mb. de Ram y DD. de 40 Gb.
- La sala 8 tiene 7 equipos Pentium III con 64 Mb. de Ram y DD. de 10 Gb.

3.6.- Edificio A 12 (Posgrado)

Este edificio lo ocupa la Unidad de Posgrado, en la planta baja se encuentran ubicadas las oficinas académico-administrativas que se encargan del manejo de dicha área (Figura 34).

En el segundo piso se encuentra ubicado el laboratorio de Cómputo que es donde se imparten los cursos en línea de posgrado. Este edificio anteriormente era uno de los más problemáticos debido a que utilizaba cable coaxial como medio de comunicación, además esta red no tenía las especificaciones técnicas necesarias para una red LAN, actualmente esta red ha sido reestructurada y ya se instaló cable Par Trenzado, para lograr tal fin es necesario el uso de dos concentradores uno ubicado en planta baja y otro en el segundo piso, además de un transceiver para poder lograr la conexión con el cable de fibra óptica que esta conectada al edificio de Mantenimiento.

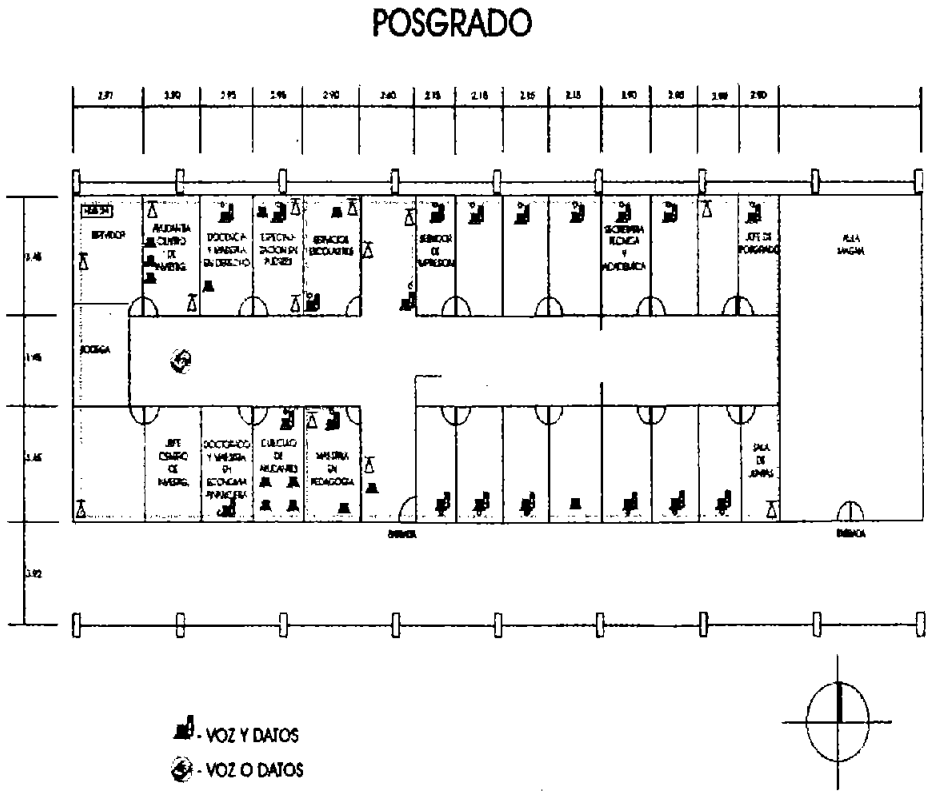


Figura 34

3.7.- Edificio A5 (Área del CAE).

Este Centro ofrece servicios de Internet para alumnos de la carrera de Ingeniería en Computación, así como cursos extracurriculares, para ofrecer estos servicios existen 3 aulas con 15 computadoras cada una. (Figura 35 y 36). Para poder suministrarle el servicio de red se cuenta con 3 concentradores conectados en cascada (2 de 16 puertos y 1 de 24 puertos), y un transceiver que es el que convierte la señal de fibra óptica a par trenzado, dicha fibra (como en otras áreas) viene del Edificio de Mantenimiento y pasa por el edificio A4 hasta llegar a este lugar.

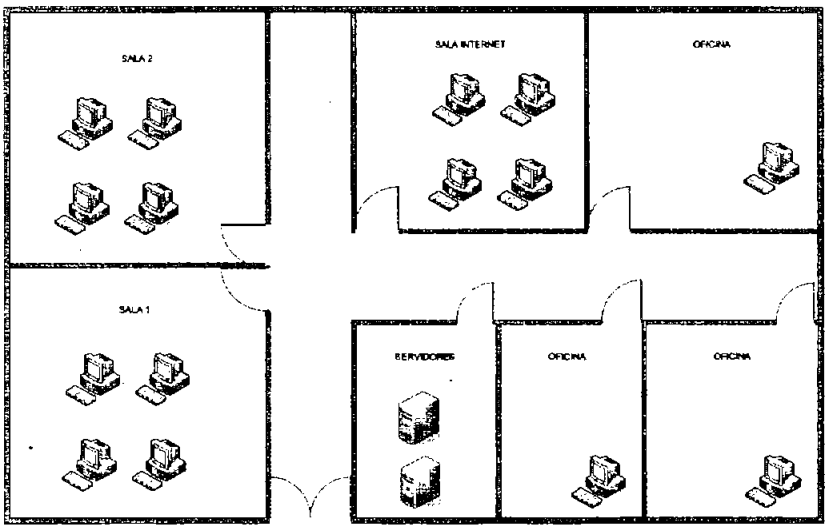


Figura 35

Figura 36

3.8 .- Edificio del Centro Tecnológico

Cabe mencionar que este edificio es una de las construcciones más recientes dentro de la ENEP Aragón, (Figura 37). Es por ello que cuenta con una de las mejores infraestructuras de red dentro del plantel. Tiene cableado estructurado en todo el edificio así como un panel de "ponchado" en la planta baja del edificio reduciendo así en gran medida el cascadeo entre los concentradores, además de contar con un concentrador de 24 puertos en cada nivel. Del edificio de mantenimiento llegan 4 pares de fibra óptica dos de entrada/salida y dos que se encuentran libres.

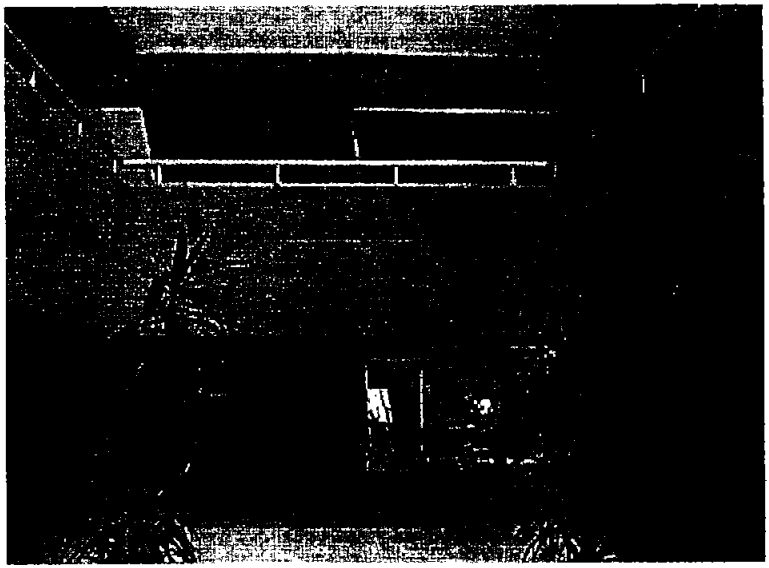
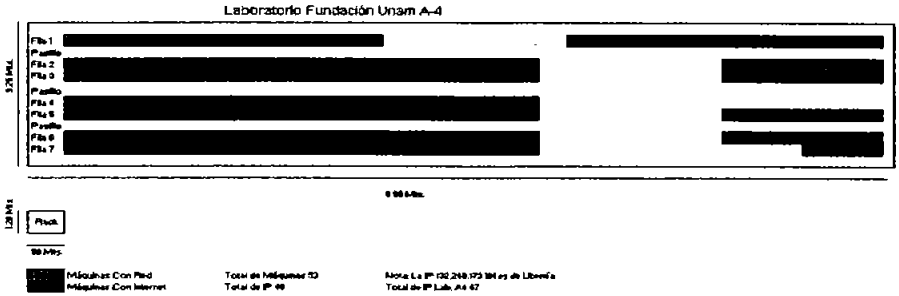


Figura 37

3.9 .- Edificio A4 (Fundación UNAM y Revisión de Estudios)

En este salón se brindan servicios de acceso a Internet a los alumnos del plantel, cuenta con aproximadamente 40 equipos de cómputo, la conexión es a través de fibra óptica que llega directamente del edificio de Mantenimiento a un convertidor que hace el puente a dos concentradores marca 3Com modelo SuperStack (1 de 40 puertos y otro de 24 puertos) ubicados en sala de firmas. (Figura 38).

Con lo que respecta a Revisión de Estudios esta área se encarga de verificar que el alumno haya terminado satisfactoriamente el plan de estudios de su carrera, para lograr este objetivo se requiere de una conexión a CU, la cual es proporcionada mediante un cable par trenzado que viene del área de Servicios Escolares y llega a un concentrador ubicado en esta área.



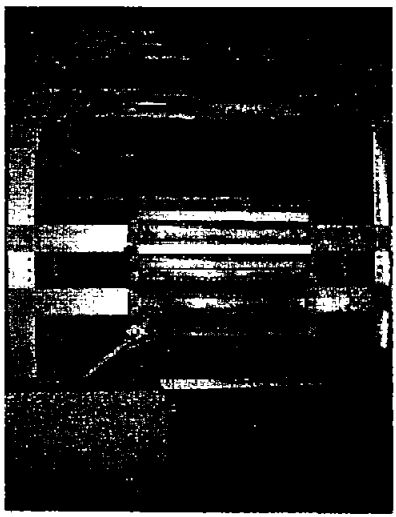


Figura 38

3.10.- Laboratorio L-3

En este edificio se concentran los laboratorios del área Eléctrica y del área Electrónica, así como cubículos, los cuales cuentan con equipo de cómputo conectado a la red y son utilizados para uso académico por profesores para la consulta de correo electrónico y también para la investigación.

Cabe hacer notar que este es el único laboratorio que cuenta con servicio de red. Como en los demás edificios la señal de Red UNAM llega por fibra óptica del edificio de Mantenimiento por un par de hilos Tx y Rx para transmisión y recepción, son recibidos por un transceiver que a su vez envía la señal a un concentrador y este distribuye la señal respectiva a todo el edificio. (Figura 39, 40 y 41).

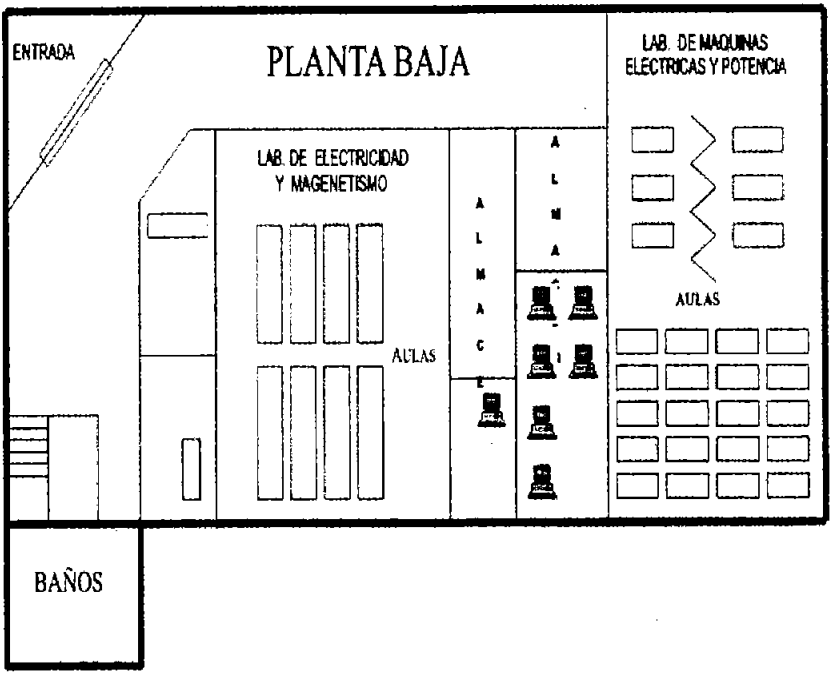


Figura 39

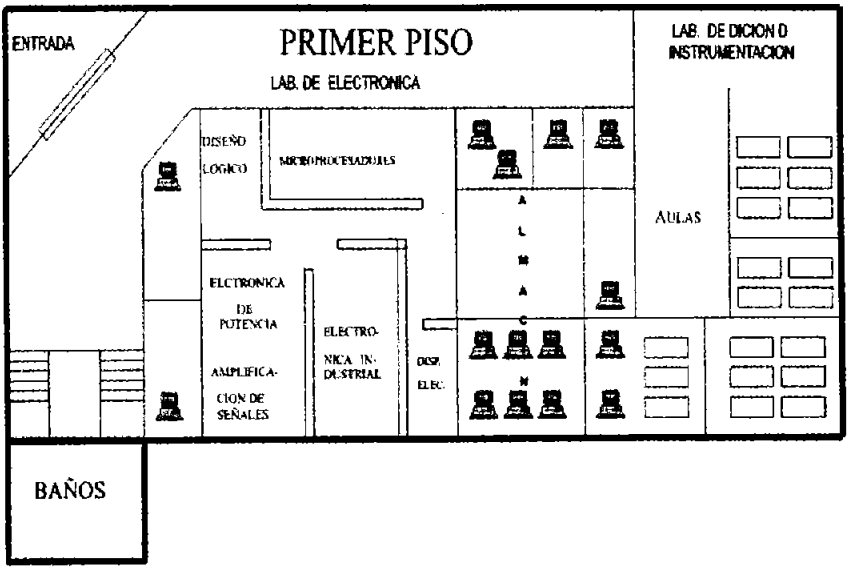


Figura 40

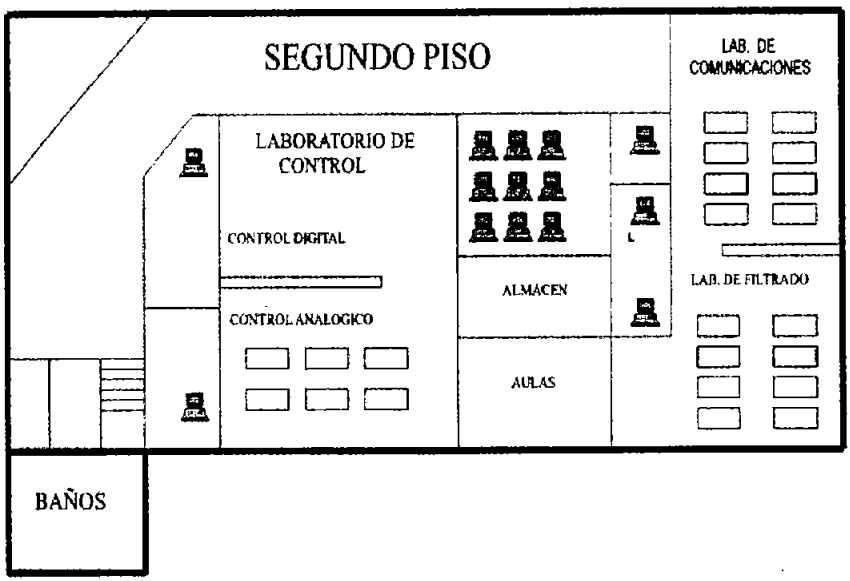


Figura 41

3.11.- Otras áreas

Hasta este momento sólo se describieron los edificios que cuentan con conexión de fibra óptica, pero además de estos también existen otras áreas que cuentan con red pero no están conectados por medio de FO, tal es el caso de los Talleres de Ciencias Sociales (Radio, Redacción y Televisión), éstos están conectados mediante cable par trenzado a un concentrador que se encuentra ubicado en el Taller de Radio y de aquí se enlaza al Departamento de Difusión, de este último Departamento se conecta al Centro de Cómputo que como ya vimos tiene salida mediante Fibra Óptica.

Cabe hacer mención que en el edificio de Servicios Generales es donde se encuentra ubicada la acometida de los servicios de fibra óptica, los módems de RF y el Gateway los cuales nos permiten enlazarnos con la red de Telecomunicaciones de la UNAM. (Figuras 42, 43, y 44).

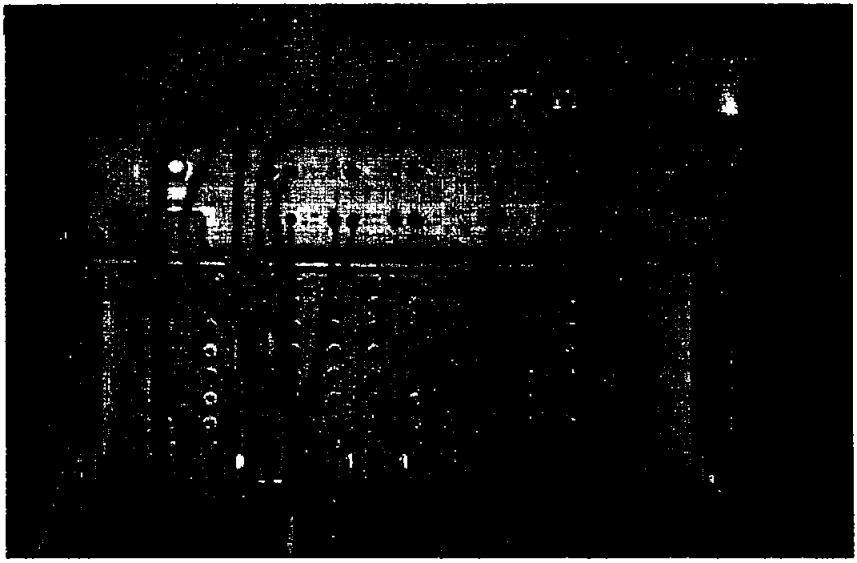


Figura 42

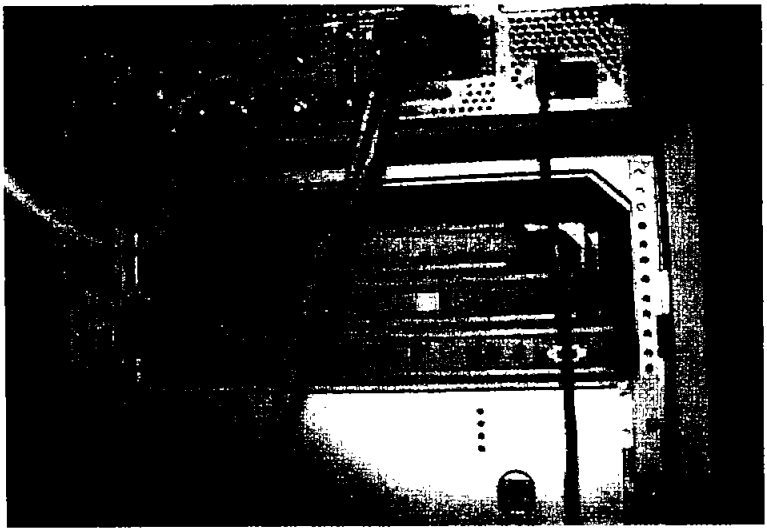


Figura 43

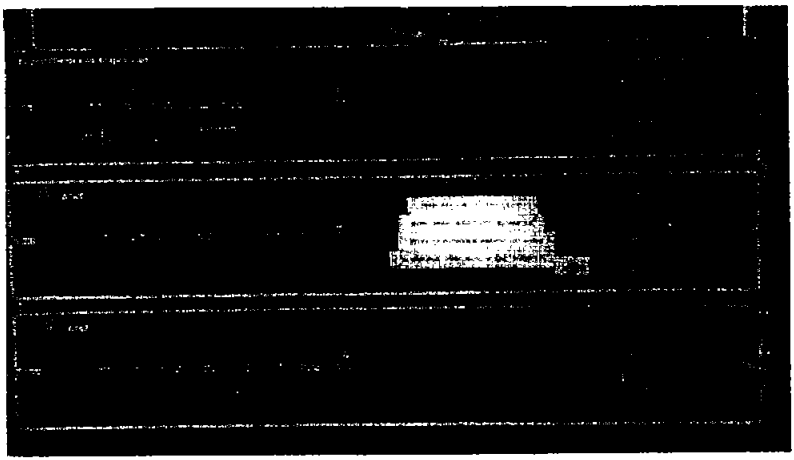


Figura 44

3.12.- Monitoreo de la Red

Como se vio en este capítulo la red del campus está dividida en tres segmentos y para poder analizar el comportamiento de éstos se necesita de programas especializados en el monitoreo de red, un ejemplo de estos programas es: 3Com Network supervisor este programa es de la compañía 3Com entre sus ventajas permite ver el comportamiento de los equipos de la red que estén conectados a un dispositivo 3Com como pueden ser un concentrador o un Switch.

Dicho programa tiene la opción de reportar el estado actual de un segmento o toda la red así como el tráfico que genera una máquina, y los conflictos existentes en la misma.

En la siguiente (Figura 45) se muestra el programa cuando empieza a revisar y a buscar todos los dispositivos que se encuentran conectados en la red.

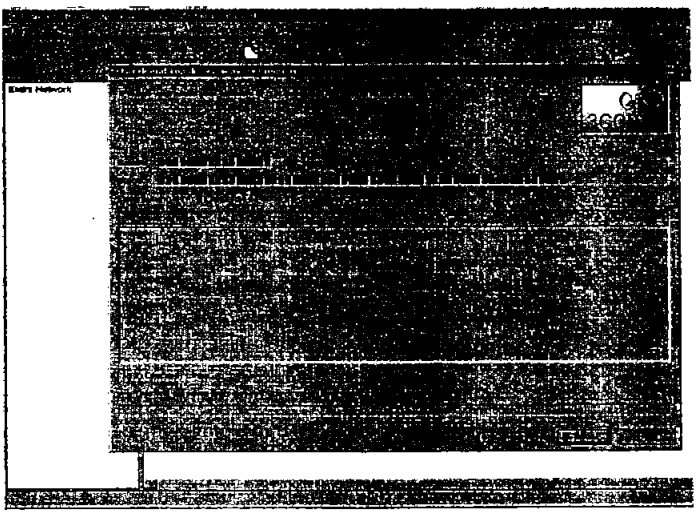


Figura 45

En cuanto el programa termina de escanear toda la red en este caso el segmento 44 nos pone un recuadro en donde aparecen todos los equipos encontrados por ejemplo encontró un switch modelo 3300 y nos pone todos los equipos conectados a el identificados con su número de IP.

Ahora si podemos hacer un análisis sobre un equipo en particular como se muestra en la (Figura 46).

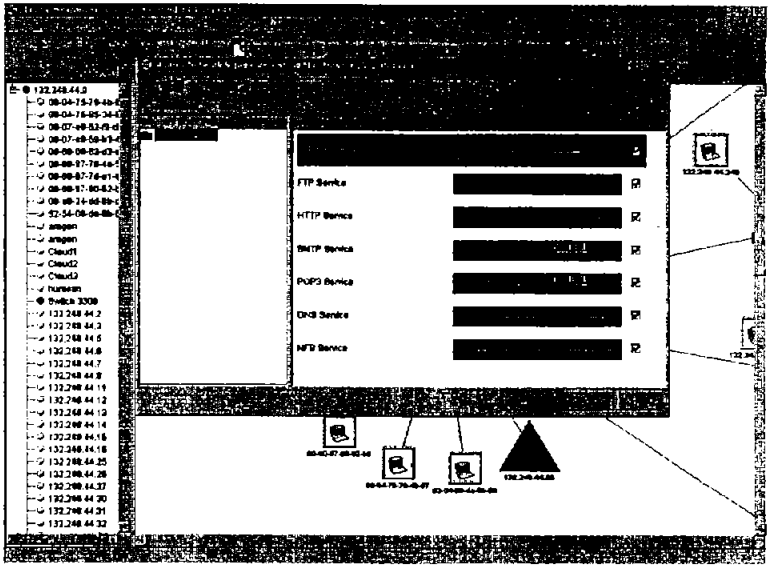


Figura 46

3.13.- Seguridad

El estándar IEEE 802.10 contiene varias características de seguridad, tales como los modos de autentificación del sistema abierto y de llave compartida, el Identificador del Juego de Servicios (Service Set Identifier-SSID), y el Equivalente a Privacidad Cableada (Wired Equivalent Privacy-WEP). Cada una de estas características provee diferentes grados de seguridad que serán revisados a continuación. También se revisa información de cómo las antenas RF pueden ser usadas para limitar, y en algunas instancias darle forma a la propagación WM.

3.13.1.- Limitando la Propagación de RF

Antes de que se implemente cualquier otra medida de seguridad, es importante considerar las implicaciones de la propagación de RF por los APs en una red inalámbrica. Escogidas de una forma inteligente, la combinación adecuada de transmisor/antena puede ser una herramienta efectiva que ayudará a limitar el acceso a la red inalámbrica al área única pretendida de cobertura. Escogidas de forma poco inteligente, pueden extender la red más allá del área pretendida hacia un estacionamiento o más lejos.

Las antenas omnidireccionales tienen un área de cobertura de 360 grados, mientras que las antenas direccionales limitan la cobertura a áreas mejor definidas (Figura 47).

La ganancia de la antena típicamente es medida en dBi[1] y está definida como el incremento de la potencia que la antena agrega a la señal RF.

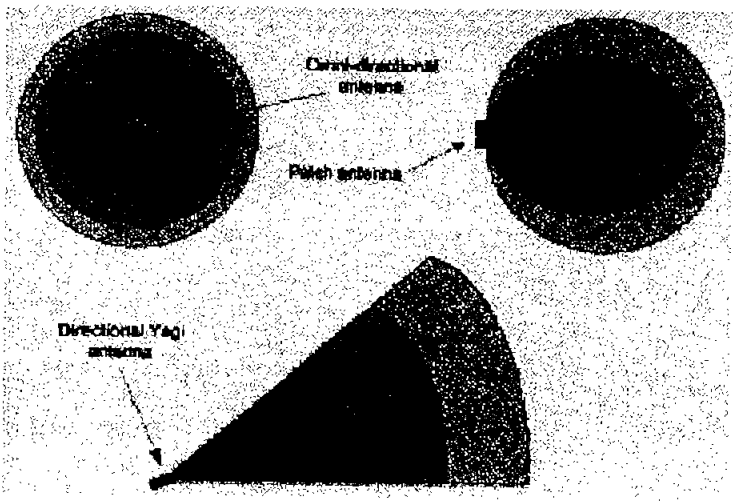


Figura 47

Debido a que los productos actuales 802.11 hacen uso de la banda sin licencia ISM (Industrial, Scientific, and Medical) de 2.4 Ghz, están sujetas a las reglas promulgadas por la FCC en 1994 para uso de espectro distribuido. Estas reglas especifican que cualquier antena vendida con un producto debe ser probada y aprobada por un laboratorio de la FCC. Para evitar que los usuarios utilicen de forma incorrecta o ilegal antenas con productos 802.11, la FCC.

En los Estados Unidos, la FCC define el máximo de Potencia Efectiva Isotrópica Radiada (Effective Isotropic Radiated Power - EIRP) de una combinación transmisor / antena como 36 dBm, donde EIRP = potencia del transmisor + ganancia de la antena-perdida del cable.

Esencialmente, esto significa que mientras la potencia del transmisor aumenta, la ganancia de la antena debe disminuir para permanecer abajo del máximo legal de 36 dBm. Por ejemplo un transmisor del 100mW equivale a 20 dBm. Este transmisor combinado con una antena de 16 dBi produce un total de 36 dBm, que es el límite legal. Para incrementar la ganancia de la antena, estaríamos legalmente obligados a reducir la potencia del transmisor. En la práctica, la mayor parte de las combinaciones transmisor / antena vendidas juntas están por debajo del máximo permitido por la FCC de 36 dBm.

[1] dBi está definida en referencia a una antena teóricamente isotrópica (propagación perfectamente esférica).

Las implicaciones de todo esto son que las combinaciones del poder del transmisor / ganancia de la antena están estrictamente reguladas y limitan el área que legalmente puede ser cubierta por un solo AP. Cuando esté diseñando una WLAN, es importante llevar a cabo un reconocimiento a fondo del lugar y considerar los patrones de propagación RF de las antenas que se vayan a usar y la potencia efectiva de la combinación transmisor/antena.

También como la banda ISM está esencialmente abierta para ser usada por cualquier persona sin licencia, es importante considerar la posibilidad de la negación de servicio (Denial Of Service - DOS) de otras fuentes benignas tales como teléfonos inalámbricos de 2.4 Ghz.

3.13.2.- Autentificación de Llave Compartida

Autentificación de llave compartida (Figura 48). Está basada en el hecho de que ambas estaciones tomando parte en el proceso de autentificación tiene la misma llave "compartida". Se asume que esta llave ha sido trasmitida a ambas estaciones a través de un canal seguro que no es WM. En implementaciones típicas, esto podría ser configurado manualmente en la estación cliente y en el AP. El primero y el cuarto frame de autentificación de llave compartida son similares a aquellos encontrados en sistemas de autentificación abierta. La diferencia es que en el segundo y el tercer frame, la estación de autentificación recibe un paquete de texto que es un reto (creado usando el Generador de Números Pseudo Aleatorios de WEP- Pseudo Random Number Generador PRNG) desde el AP, lo encripta usando la llave compartida, y luego lo manda de regreso al AP. Si después de la desencripción, el texto de reto es igual, entonces la autentificación de un sentido es exitosa. Para obtener la autentificación mutua, el proceso se repite en la dirección opuesta. El hecho de que la mayor parte de los ataques hechos contra WLAN's 802.11b están basados en capturar la forma encriptada de una respuesta conocida hace de esta forma de autentificación una elección pobre. Les da a los atacantes exactamente la información necesaria para derrotar la encripción WEP y es por lo que la llave de autentificación compartida nunca es recomendada. Es mejor utilizar la autentificación abierta, la cual permitirá la autentificación sin la llave WEP correcta. Se mantendrá seguridad limitada porque la estación no estará preparada para enviar o recibir información de forma correcta con una llave WEP no válida.

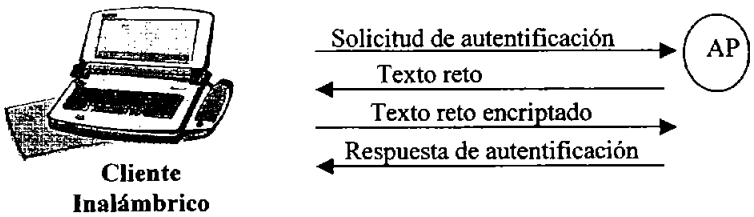


Figura 48

3.13.3.- WEP

Como lo define el IEEE, WEP está diseñado para proteger a usuarios de una WLAN de espías casuales y su intención es tener las siguientes propiedades:

- **Encriptación razonablemente fuerte.** Depende de la dificultad de recuperar la llave secreta a través de un ataque de fuerza bruta. La dificultad crece con el tamaño de la llave.

- **Auto-sincronización.** No hay necesidad de lidiar con los paquetes perdidos. Cada paquete contiene la información requerida para desencriptarlo.

- **Eficiente.** Puede ser implementado en software de forma razonable.

- **Exportable.** Limitar el largo de la llave conlleva a una mayor posibilidad de exportar más allá de las fronteras de los Estados Unidos.

El algoritmo WEP esencialmente el algoritmo criptográfico RC4 de Data Security Inc. es considerado un algoritmo simétrico porque utiliza la misma llave para cifrar y para descifrar la Unidad de Información de Protocolo (PDU) de texto plano. Para cada transmisión el texto plano es XOR con una llave pseudo aleatoria para producir texto cifrado. El proceso es invertido para la desencriptación.

El algoritmo funciona de la siguiente manera:

- Se asume que la llave secreta ha sido distribuida en la estación de transmisión y recepción por algún medio seguro.
- En la estación de transmisión, la llave secreta de 40 bits es concatenada con el Vector de Inicialización (IV) de 24 bits para producir la semilla para la entrada hacia el PRNG WEP.
- La semilla es pasada al PRNG para producir un stream (keystream) de octetos pseudo aleatorios.
- El texto plano PDU es XOR con la keystream pseudo aleatoria para producir el texto cifrado PDU.
- El texto cifrado PDU se concatena con el IV y transmitido por el WM.
- La estación receptora lee el IV y lo concatena con la llave secreta, produciendo la semilla que pasa al PRNG.
- El PRNG del receptor deberá producir un keystream idéntico al usado por la estación de transmisión, de tal forma que cuando XOR con el texto cifrado, el texto plano original PDU sea producido.

Vale la pena mencionar que el texto plano PDU también está protegido con CRC para prevenir manejo aleatorio del texto cifrado en tránsito. Desafortunadamente, la especificación no incluye ninguna regla relacionada con el uso del IV, excepto que dice que el IV podrá ser cambiado "tan frecuentemente como cualquier MPDU."

La especificación sin embargo si pone sobre aviso a los implementadores a considerar los peligros de una pobre administración del IV. Esto es en parte responsable de la facilidad con la que algunas implementaciones WEP son comprometidas.

3.13.4.- Firewall y Router

Una de las medidas que se han tenido que tomar en la ampliación y seguridad de la red Aragón ha sido la implementación de Router y Firewall en diferentes áreas, esto es debido a que las direcciones ya están muy reducidas, además de poder reducir el tráfico de la misma.

Pero vamos a verlo por separado, primero que es un Firewall o cortafuegos. (Figura 49). Es un sistema de defensa que se basa en la instalación de una "barrera" entre tu PC y la Red, por la que circulan todos los datos. Este tráfico entre la Red y tu PC es autorizado o denegado por el firewall (la "barrera"), siguiendo las instrucciones que le hayamos configurado.

Aunque un firewall se compone de equipos y programas, estos quedan un poco lejos para el usuario doméstico, así que lo que vamos a explicar es un programa (entre los muchos que hay) que realiza las funciones descritas.

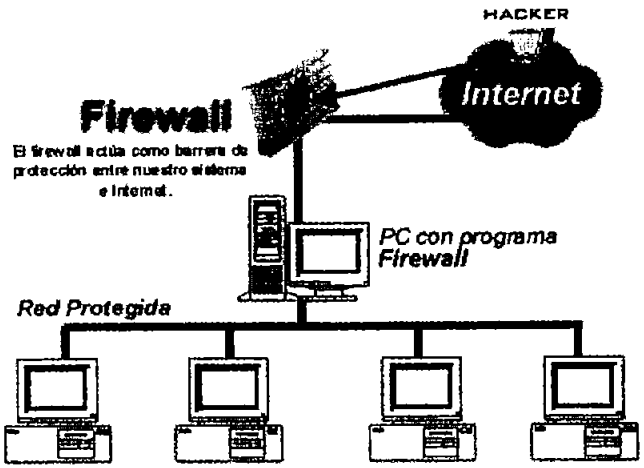


Figura 49

El funcionamiento de este tipo de programas se basa en el "filtrado de paquetes". Todo dato o información que circule entre nuestro PC y la Red es analizado por el programa (firewall) con la misión de permitir o denegar su paso en ambas direcciones (Internet-->PC ó PC--->Internet).

Esto es muy importante, ya que si autorizamos un determinado servicio o programa, el firewall no va a decirnos que es correcto o incorrecto, o incluso, que siendo correcto los paquetes que están entrando o saliendo, éstos pueden contener datos maliciosos para nuestro sistema o la Red, por lo que hay que tener cuidado en las autorizaciones que otorguemos.

Como ejemplo de esto último podemos poner el Correo Electrónico, si autorizamos en nuestro firewall a que determinado programa de Correo acceda a Internet, y al recibir nuestros mensajes viene un adjunto con un virus tipo gusano, el firewall no nos va a defender de ello, ya que le hemos autorizado a que ese programa acceda a la Red.

Lo que si va a hacer es que si al ejecutar el adjunto, el gusano intenta acceder a la Red por algún puerto que no esté previamente aceptado por nosotros, no lo va a dejar propagarse. Ahora bien, si hace uso por ejemplo del mismo cliente de correo, si va a propagarse. La misión del firewall es la de aceptar o denegar el trafico, pero no el contenido del mismo.

Un firewall funciona, en principio, DENEGANDO cualquier tráfico que se produzca cerrando todos los puertos de nuestro PC. En el momento que un determinado servicio o programa intente acceder a Internet o a nuestro PC nos lo hará saber. En ese momento podremos aceptar o denegar dicho tráfico.

Una buena política debería ser, ante la duda, no aceptar nunca cualquier acceso hasta comprobar que es necesario para un correcto funcionamiento del servicio que deseamos usar y no es potencialmente peligroso para el sistema.

Con la instalación de un firewall conseguiremos hacer nuestro sistema mucho menos vulnerable a intrusiones.

Un **router** o **enrutador** es un dispositivo de interconexión de redes de computadoras que opera en la capa 3 (nivel de red) del modelo OSI.

Este dispositivo interconecta segmentos de red o redes enteras. Hacen pasar paquetes de datos entre redes tomando como base la información de la capa de red.

Los routers toman decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirigen los paquetes hacia el segmento y el puerto de salida adecuados.

Los routers toman decisiones basándose en la densidad del tráfico y la velocidad de la conexión (ancho de banda, o *bandwidth*).

En el siguiente ejemplo se muestra cómo funciona un router. (Figura 50).

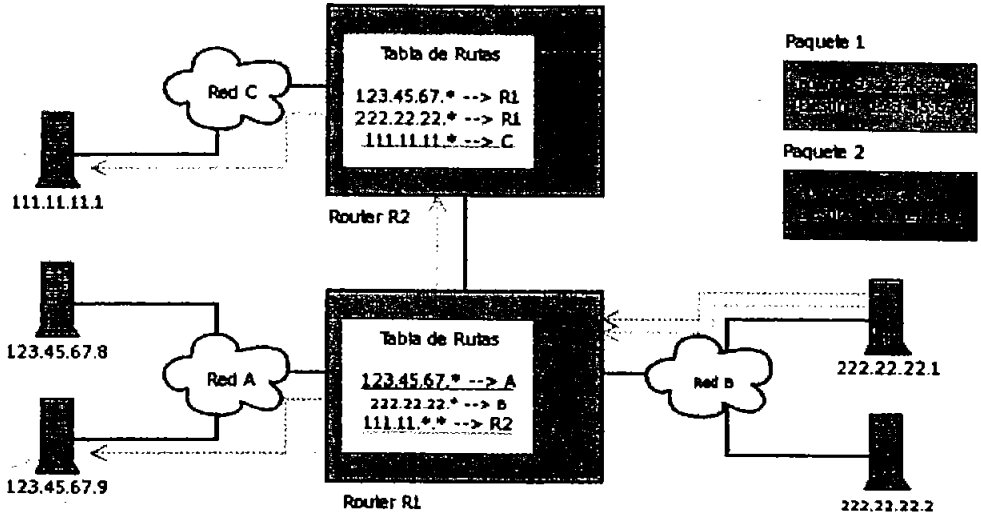


Figura 50

Aquí se muestran 3 redes IP interconectadas por 2 routers. La computadora con el IP 222.22.22.1 envía 2 paquetes, uno para la computadora 123.45.67.9 y otro para 111.11.11.1 A través de sus tablas de enrutamiento configurados previamente, los routers pasan los paquetes para la red con el rango de direcciones que corresponde al destino del paquete.

El contenido de las tablas de rutas está simplificado, en realidad se utilizan máscaras de red para definir las subredes interconectadas. Los **broadcast**, o difusiones, se producen cuando una fuente envía datos a todos los dispositivos de una red. En el caso del protocolo IP, una dirección de broadcast es una dirección compuesta exclusivamente por números unos (1) en el campo del host: 255.255.255.255.

En redes IP, el ruteo tiene dos tipos de direccionamiento, el estático que debe ir con dispositivos individuales y configurarlo con una dirección IP y el direccionamiento dinámico que puede ser ARP, BOOTstrop y DHCP. El ARP pertenece al conjunto de TCP IP, éste permite que una computadora descubra la dirección MAC del ordenador que está asociado con una dirección IP.

CAPÍTULO IV

CONEXIÓN INALÁMBRICA EN ÁREAS AISLADAS DE LA ENEP ARAGÓN

Como se mencionó en el capítulo II (Redes Inalámbricas) este tipo de red se utiliza cuando no se puede establecer una red alambrada debido a múltiples factores como pueden ser lugares donde no se permite la instalación de cables ya sea por ser lugares inaccesibles o debido a circunstancias geográficas. Otro de los usos es el de poder ampliar una red existente, en este caso es lo que se va a realizar, es decir, ampliar una red alambrada.

4.1.- Edificio del CLE

Como primer proyecto a realizar tenemos el edificio del CLE, el cuál se encuentra ubicado en la parte posterior de la escuela entre el Centro Tecnológico, los Edificios A1 y A2, y el Edificio de Talleres de Ciencias Sociales y Centro de Cómputo, en este Edificio se encuentran ubicadas las siguientes áreas académico-administrativas:

- Centro de Educación Continua: Es la encargada de actualizar y capacitar en forma permanente a los alumnos y egresados así como a la comunidad externa en general, en los distintos campos del conocimiento incrementando la calidad de profesionalización de los egresados de la institución, mediante la impartición de diplomados, seminarios, cursos, etc.

- Centro de Investigación: Es el área donde se encuentran los cubículos de los profesores de carrera, así como dos salones de cómputo los cuales son utilizados por los maestros para preparar sus clases y realizar proyectos de investigación.

- Centro de Lenguas Extranjeras: Este centro se encarga de apoyar a las áreas académicas del plantel en la formación integral de los estudiantes y de la comunidad universitaria en general, a través de la impartición de cursos tales como: inglés, francés, italiano, alemán, portugués, latín, japonés y ruso.

- Bolsa de Trabajo: Su objetivo principal es establecer una comunicación con empresas públicas y privadas, con el propósito de conocer las ofertas de trabajo y canalizar a los aspirantes en los diferentes empleos.

- Salón rojo : Aquí se llevan a cabo exámenes profesionales, impartición de clases así como el escrutinio de los votos cuando hay elecciones en el plantel, por lo que se tiene que capturar la información en línea.

Como estas áreas son muy importantes, necesitan integrarse tanto a la red local de la escuela así como contar con acceso a Internet, por lo que se tuvo que analizar cual sería la mejor alternativa para poder conectar este edificio a la red.

Para lograr esto primero se tuvo que ver cuáles eran las instalaciones más cercanas al edificio del CLE y que contaran con acceso a la red, en este caso el Centro de Cómputo es el edificio más cercano que cumple con los requisitos, así que será al que nos enlacemos. El siguiente paso es determinar cual será la forma de conexión, debido a su ubicación, a las irregularidades del suelo, así como a la zona verde que hay a su alrededor se determinó que sería muy complicado conectarlos mediante un cable, así que se optó por la conexión inalámbrica.

Para poder llevar a cabo la conexión inalámbrica y lograr que el CLE contará con acceso a la red y a Internet, se tuvieron que realizar los siguientes procedimientos:

- Se tuvo que instalar una red local en el edificio del CLE, esta red se diseñó de forma estructurada usando cable par trenzado UTP nivel 5 y utilizando un concentrador 16 puertos por cada piso, de esta manera quedaron tres concentradores además de un general, el cuál nos sirve para enlazar los tres niveles.

- Una vez que ya se tenía la red en el CLE se conectó un Access Point modelo 2311 marca Ansel, el cual se configuró como esclavo (véase manual de instalación) al concentrador general para poder establecer la conexión inalámbrica en este edificio.

- En el Centro de Cómputo se instaló otro Access Point (de las mismas características que el anterior para evitar problemas de incompatibilidad además éste se configuró como maestro) para poder completar la conexión inalámbrica y a su vez establecer el enlace con la red local de la escuela. (Figura 51).

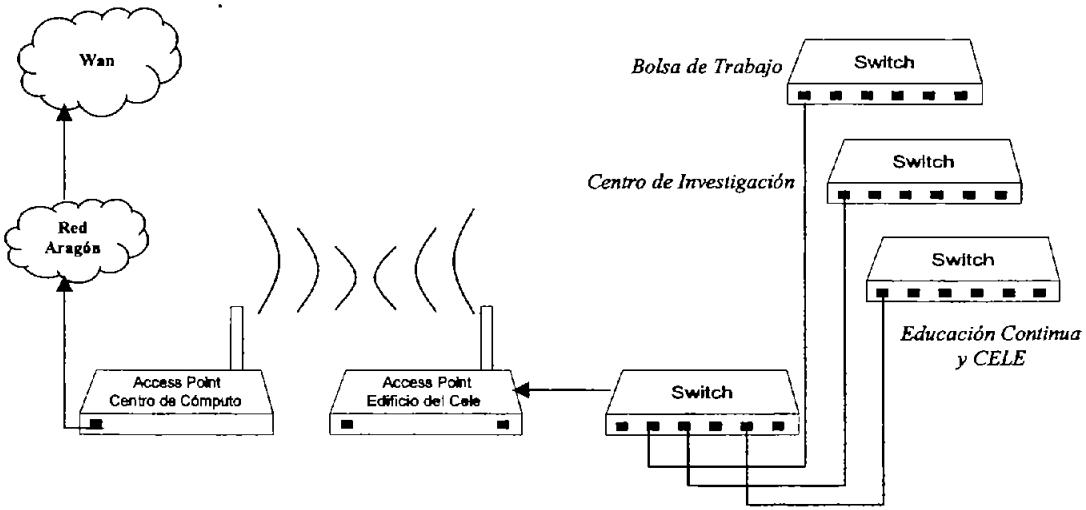


Figura 51

4.2.- Instalación del Access Point modelo 2311WLAN

El AP 2311 es un dispositivo electrónico el cual nos permite establecer enlaces entre redes alambradas, así como también realizar conexiones entre dispositivos de red inalámbricos. Un simple AP provee de conexión a computadoras siempre y cuando cuenten con tarjeta inalámbrica y se encuentren dentro de su área de cobertura.

4.2.1.- Aplicaciones

I. Acceso remoto a la red de información corporativa como es el correo electrónico, transferencia de archivos y emulación de terminal.

II. En áreas difíciles de cablear como son los edificios históricos o viejos, instalaciones de asbesto y en áreas donde sea difícil el cableado.

III. Áreas donde se cambien con frecuencia como son: vendedores, fabricantes y bancos donde frecuentemente arreglan el lugar de trabajo o cambian de oficinas.

IV. Redes temporales para proyectos especiales: es el caso de espectáculos, exhibiciones y sitios donde se necesiten temporalmente en un corto tiempo. Vendedores, aerolíneas y compañías de envío que necesiten computadoras adicionales para periodos cortos. Auditores que requieran sitios especiales.

V. Acceso a base de datos para trabajadores móviles como son doctores, enfermeras, vendedores, administrativos que necesiten accesar la base de datos mientras se mueven en su área de trabajo.

VI. Usuarios SOHO (Pequeñas oficinas u oficinas en casa por sus siglas en inglés) los usuarios SOHO necesitan una instalación fácil y rápida de una pequeña red de computadoras.

VII. Lan soporta las mismas opciones de configuración de red del legado ethernet.

VIII. La Lan está definida por el comité de la IEEE bajo el estándar 802.11

IX. La Lan puede ser configurada como:

1. Ad-Hoc para departamentos o redes Lan SOHO
2. Infraestructura para empresas
3. Interconexión Lan punto a punto

4.2.2.- Procedimientos para instalar un AP 2311

Al adquirir un AP por lo regular viene con lo siguiente:

- Un Access Point
- Una antena dipolo (algunos AP no tienen esta antena porque la tienen de forma interna)
- Un adaptador (9V/1.11A)
- Un CD

Instalación del Hardware

- Un puerto RJ 45 para conectarlo a la red ethernet 10 baseT
- Atornillar la antena dipolo en el conector SMA del AP
- Conectar el cable de alimentación del AP

Instalación del Software

A continuación describimos los pasos a seguir para instalar el software del AP en una computadora. Ver (Figura 52, 53, 54, 55 y 56).

1. Encender la computadora e iniciar Windows.
2. Insertar el CD con los controladores.
3. Teclee D:\AP\Utility\setup.exe para iniciar la instalación.
4. Siga las instrucciones del asistente para terminar el proceso de carga.

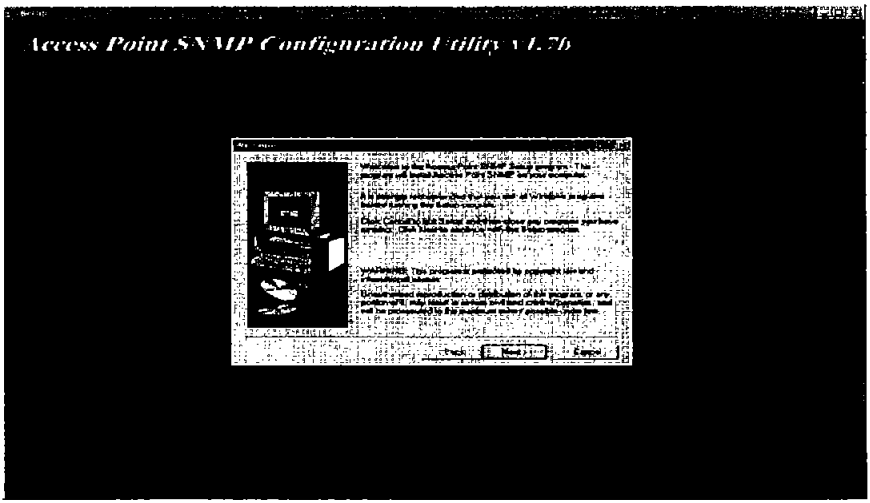


Figura 52

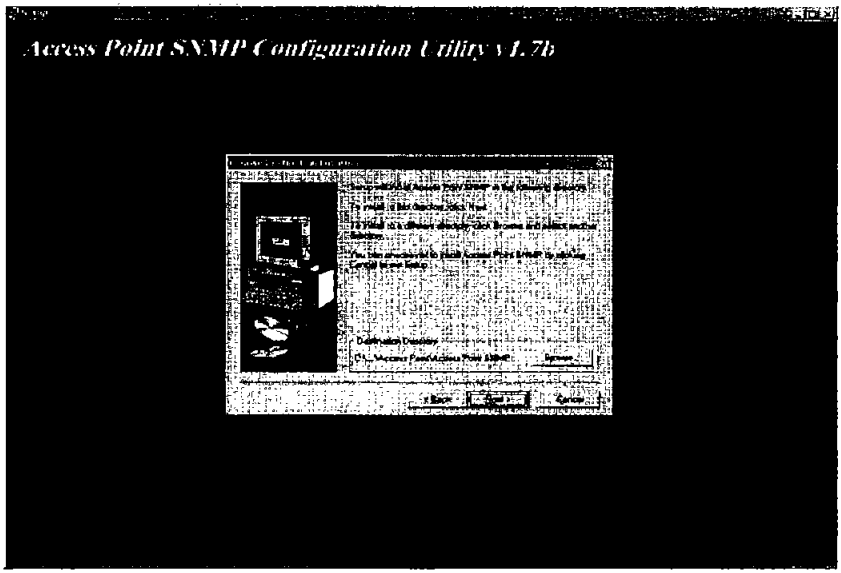


Figura 53

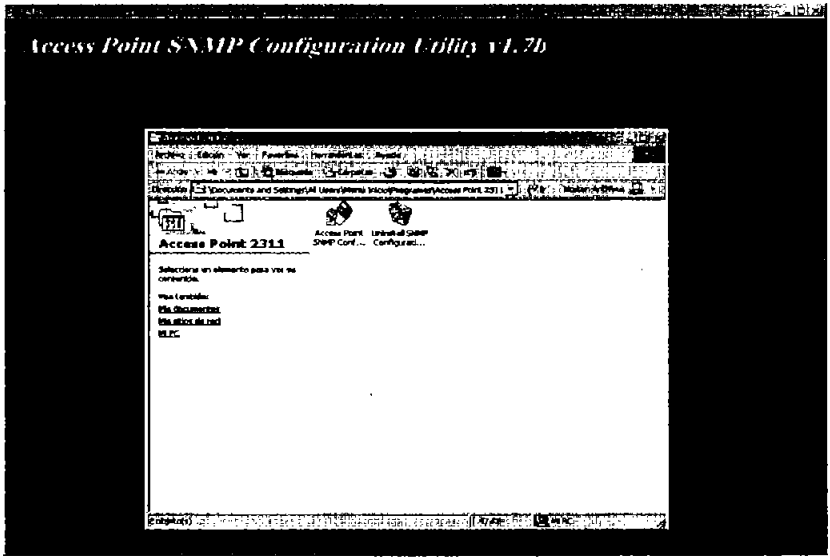


Figura 54

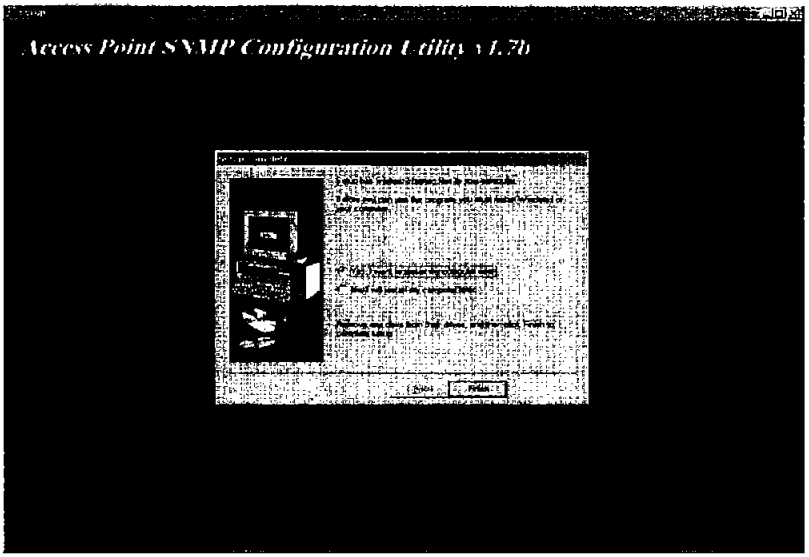


Figura 55

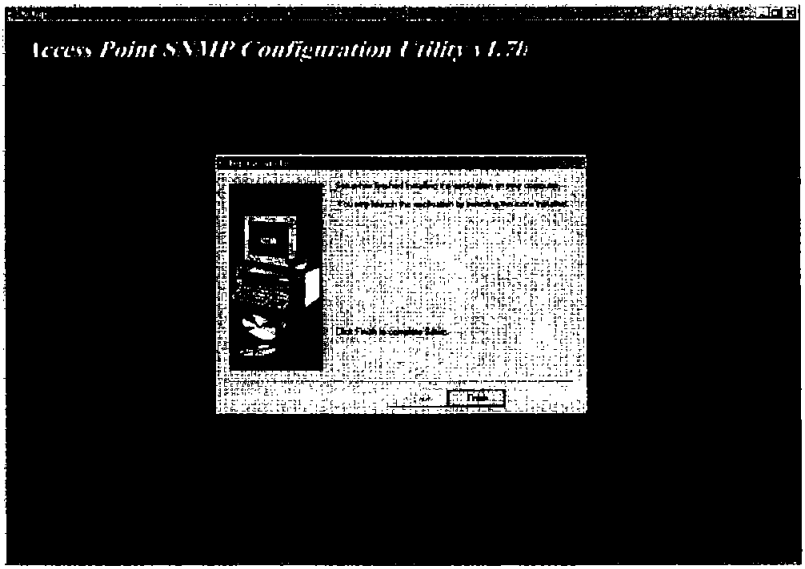


Figura 56

4.3.- Configuración del Access Point

Después de que se ha instalado el software del AP WLAN usted debe empezar la configuración de éste. Primero se debe conectar un cable UTP con configuración "cruzado" entre el AP y la computadora donde se instaló el software de configuración, no olvide conectar el cable de alimentación del Access Point.

- Inicie el programa de utilidad AP WLAN desde el fólder "Utilidad del AP WLAN"
- Presione sobre el campo "búsqueda" bajo el menú AP en el programa de utilidad para buscar los AP's que se encuentren en la red.
- Si el AP es detectado, el programa de utilidad mostrará la información del AP como se muestra en la siguiente (Figura 57).

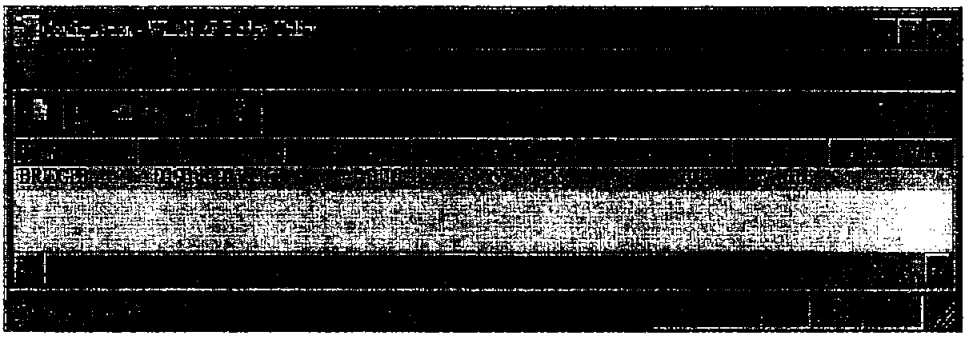


Figura 57

Presione dos veces sobre el AP que desee, posteriormente aparecerá una caja de diálogo para que se le asigne un IP temporal al AP ya que de fábrica al AP no se le asigna un IP. (Figura 58).

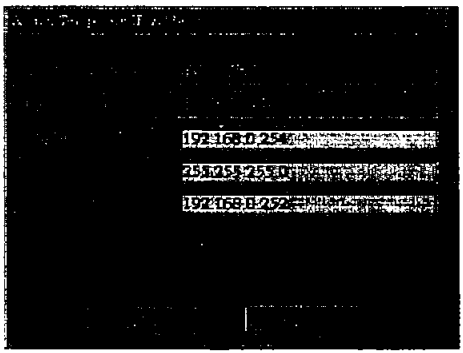


Figura 58

Ahora hay que asignar al AP, una dirección IP, máscara de subred y una puerta de enlace correctamente, al terminar presionar el botón OK para que surtan efecto los cambios de forma temporal. Observe que cuando llena la dirección IP del AP usted debe asignarle al AP una dirección que se encuentre dentro del mismo rango así como la subred en que esté configurada su PC.

1. Presione dos veces sobre el AP que aparece en la tabla, la utilidad lo ligará automáticamente con la "página de inicio" del AP mediante el navegador de su PC.

2. Introduzca como nombre de usuario "Default" y clave se acceso "WLAN_AP" presione el botón login. (Figura 59). Ahora entrará al programa de configuración del AP en donde usted puede modificar los parámetros del mismo, ver el estado y la información de él.

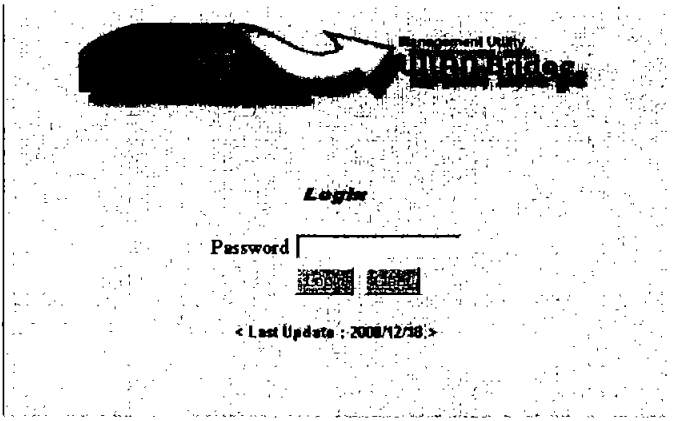


Figura 59

De esta manera tendremos ya instalado y configura nuestro AP.

4.4.- Características de los AP

- Compatible con IEEE 802.11 DSSS (Espectro extendido de secuencia directa), con velocidades de 11/5.5/2/1 Mbps.
- Llave WEP inalámbrica de 64 o 128 bits (opcionales para encriptación y seguridad de datos).
- Soporte completo para 802.11 y autentificación de clave
- Manejo del AP bajo navegadores web estándar.
- Capacidad de Roaming.
- Conectividad para ethernet 802.3, 10 baseT y redes Lan de PC's existentes
- Asignación dinámica de dirección IP vía DHCP o asignación de IP estático Vía utilería del AP.

- Actualización de firmware vía transferencia FTP.

4.5.- Especificación del Hardware del AP

Radio:	Cumple con los estándares IEEE 802.11 y WECA
Banda de Frecuencia:	De 2400 a 2483.5 Mhz (para USA, Canadá y ETSI) De 2400 a 2497 Mhz (para Japón)
Tipo de Modulación:	CCK, BPSK y QPSK
Canales de operación:	Cumple con IEEE 802.11 - 11 canales (USA y Canadá) - 13 canales (ETSI) - 14 canales (Japón)
Tecnología de radio:	DSSS (Espectro extendido de secuencia directa)
Transferencia de datos:	1/2/5.5/11 Mbps
Potencia de Salida:	➢ 13 dBm
Sensibilidad de recepción:	Mín –76 dBm para 11 Mbps Mín –80 dBm para 5.5/2/1 Mbps
Tipo de Antena:	Antena externa, interna y aérea.
Interfase de conexión	Ethernet IEEE 802.3 en 10 baseT
Conector:	RJ 45
LED:	Encendido, liga Ethernet, actividad Ethernet, liga de conexión y actividad.
Fuente de energía:	Un adaptador de CA (CA 100~240 V 50/60 Hz, Salida de CD 9 V/1.11)
Certificaciones:	FCC inciso 15 ETSI 300.328 ARIB STD33 & T66

4.6.- Departamento de Adquisiciones

Como Segundo proyecto a realizar tenemos el Departamento de Adquisiciones, el cual se encuentra ubicado en la parte frontal de la escuela entre los edificios de Biblioteca, Servicios Generales y Laboratorio L1.

Este departamento es el encargado de adquirir todo el material que requiere la escuela para su adecuado funcionamiento, mismo que tiene que darse de alta para llevar un control de todo el material asignando un número de inventario, anteriormente este procedimiento se realizaba en Ciudad Universitaria por lo que se tardaba más de ocho días en trámites administrativos debido a esto se solicito conectar este Departamento a la Red UNAM, para poder realizar la captura en línea con los servidores de Proveeduría, y así agilizar los trámites de esta área.

Después de realizar un estudio para ver cuál sería la forma idónea de conectar este departamento a la red, tenemos que existe un estacionamiento enfrente del edificio así como áreas verdes, debido a estas dificultades se optó por una conexión inalámbrica, dentro de este mismo estudio se vio que el edificio más cercano con acceso a red y con la infraestructura adecuada es la Biblioteca, por lo que se tiene que hacer la conexión con este edificio mediante el siguiente procedimiento:

1. En la Biblioteca se conecta un Access Point (modelo 2311 en forma de maestro) a la red local.

2. En el Departamento de Adquisiciones se instaló una red local de par trenzado UTP nivel 5 y un concentrador de 8 puertos.

3. Una vez terminada la instalación, se conectó a un nodo del concentrador el otro Access Point (con las mismas características que el anterior pero con la configuración de esclavo) para poder dar salida a la red pero debido a los problemas mencionados anteriormente, y debido a que existe demasiada interferencia de señal (esto es causado por una subestación eléctrica y una bomba hidráulica) se tuvo que conectar una antena externa (Figura 60) al Access Point para hacer que la señal se amplificara y de esta forma pudiera llegar sin ningún problema al edificio de la Biblioteca.

Figura 60

En el siguiente diagrama muestra la forma en que quedó la conexión inalámbrica del Departamento de Adquisiciones con la Biblioteca. (Figura 61).

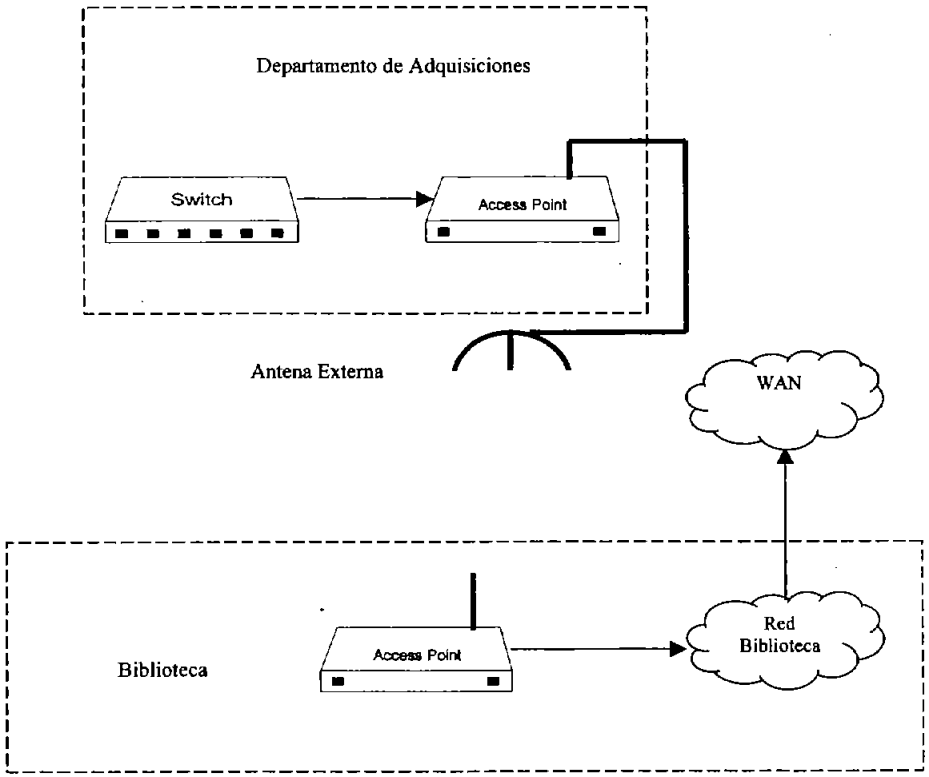


Figura 61

4.7.- Laboratorios de Ingeniería L1, L2 y L4

Como tercer proyecto a realizar tenemos los laboratorios de Ingeniería los cuales son el L1, L2 y L4. Estos no cuentan con acceso a red, así que tenemos que ver cuál será la mejor forma de conectarlos ya que se encuentran en la parte posterior del plantel.

Es necesario que se conecten a la red ya que en estos laboratorios hay varios cubículos de profesores los cuales requieren del servicio, así como también realizan investigaciones y es necesario que cuenten con acceso a Internet y correo electrónico para poder enviar y recibir información. El L1 es de Diseño y manufactura el L2 de Hidráulica y el L4 de Ingeniería Civil.

El edificio L3 es un laboratorio de Ingeniería que también se encuentra ubicado en la zona de los otros laboratorios pero a diferencia de éstos, éste si cuenta con acceso a la red y es el edificio más cercano, así que será este laboratorio el que utilizaremos para poder conectar los demás laboratorios a la red.

El enlace directo será entre el L3 y el L2 ya que quedan exactamente de frente, la forma de conectarlos será mediante un AP 2311, pero debido a que hay áreas verdes entre los edificios y están un poco separados, utilizaremos 2 antenas externas para que no se pierda la señal y tengan un buen enlace, éstas se conectarán a los AP y se colocarán a los costados de los laboratorios. De la siguiente manera:

- Se creo una red local en el Laboratorio L1 y otra en el Laboratorio L4 dejando puertos disponibles en los switches, para después conectar la liga que saldrá del L2.

- En el laboratorio L3 se conecta un AP (modelo 2311 en forma de maestro) a la red local. Pero le conectamos una antena externa para amplificar la señal y que ésta llegue sin ningún problema al L2 (Figura 62).

- En el laboratorio L2 se instaló otro AP 2311 pero como esclavo el cual lo conectamos a un concentrador que alimenta la red local, también este AP tiene conectada una antena externa (Figura 63).

- Del concentrador que se instaló en el L2, sacamos dos ligas o enlaces hacia los laboratorios L1 y L4 para dar salida a éstos.

- Así quedaron conectados los laboratorios L1, L2 y L4 con el L3.

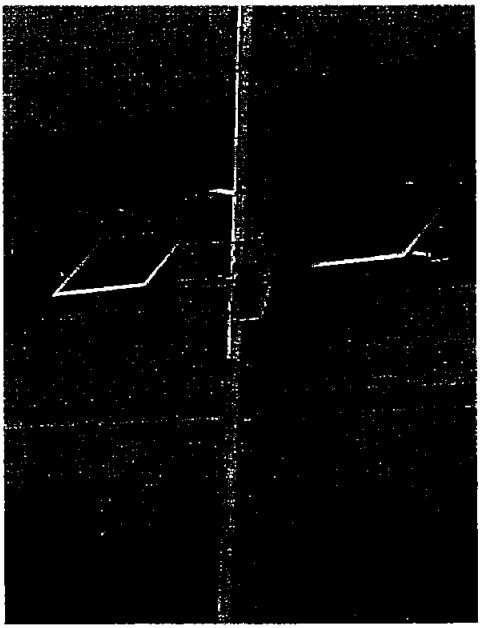


Figura 62

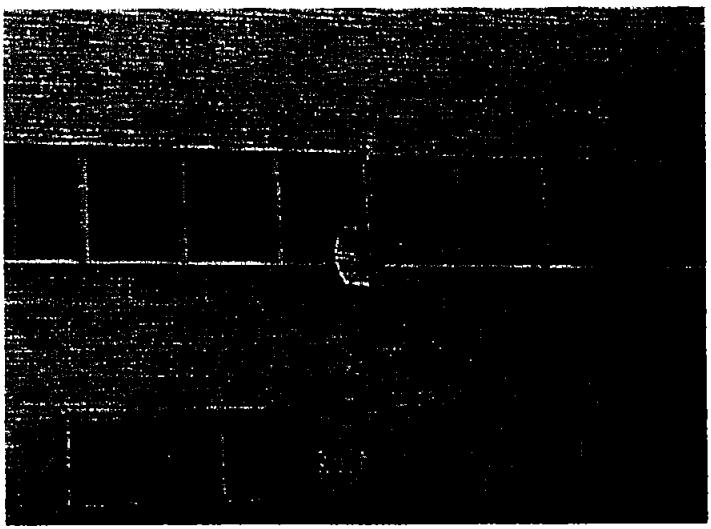


Figura 63

El diagrama de conexión quedo de la siguiente manera (Figura 64).

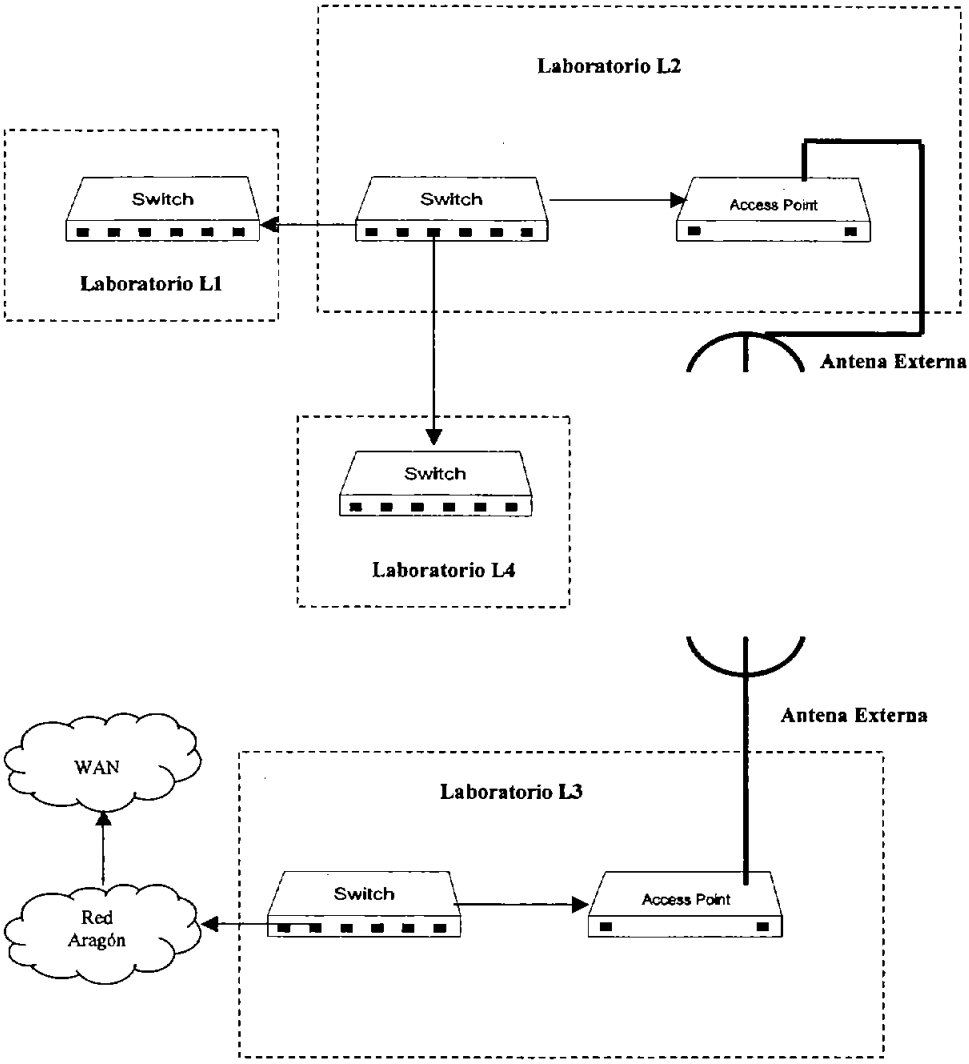


Figura 64

4.8.- Módulo de Extensión Universitaria.

Como cuarto proyecto a realizar se tiene el Módulo de Extensión Universitaria (Figura 65). Ubicado en la entrada del plantel, entre la Clínica Odontológica Aragón, el comedor y los estacionamientos de académicos y alumnos, así como una zona de áreas verdes. Aquí se encuentran ubicadas varias oficinas administrativas pertenecientes a la Unidad de Extensión Universitaria entre las cuales podemos mencionar:

- La Jefatura de esta Unidad: Su función es la de promover y coordinar los eventos académicos, culturales y administrativos que coadyuven a la formación de los estudiantes.

- Departamento de Intercambio Académico y Vinculación: Es el encargado de fomentar y apoyar el intercambio entre la UNAM y las universidades e instituciones científicas y culturales tanto nacionales como extranjeras, así como concertar los acuerdos y convenios de carácter académico entre el plantel y otras instituciones, además de proporcionar información a la comunidad universitaria sobre becas cursos, seminarios y otros apoyos que ofrecen organismos internacionales, instituciones y fundaciones.

- Actividades Culturales: Organiza y promueve las diversas actividades de tipo cultural y artístico que permiten ampliar las posibilidades educativas del estudiante.

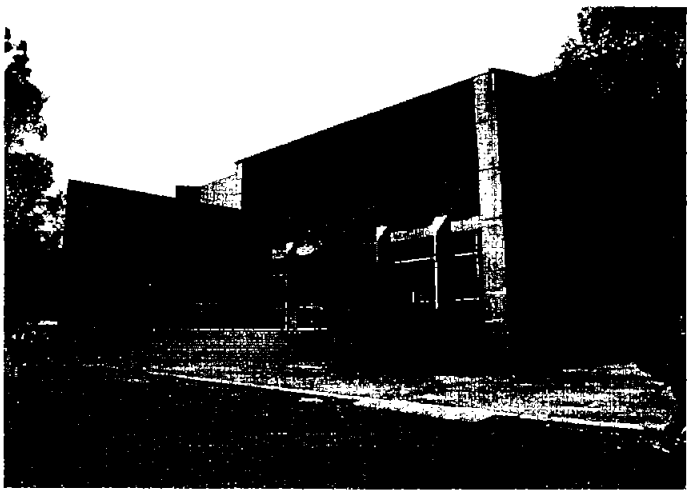


Figura 65

Debido a la información que se maneja en esta Unidad es de suma importancia que se cuente con acceso a Internet, es por ello que se tuvo que analizar la forma de poder conectar esta área a la red, debido a su ubicación y a la problemática que rodea este edificio, se optó por una conexión inalámbrica entre este Módulo y el Edificio de Gobierno el cual es el más cercano y con la infraestructura necesaria para brindar el acceso a red. La instalación se llevó a cabo de la siguiente manera:

1. Se instaló una red local de 6 nodos , utilizando cable par trenzado UTP nivel 5 y un concentrador de 8 puertos.

2. Se conectó un Access Point modelo 2411 al concentrador de la red ubicada dentro de la Unidad. El cual se configuró como esclavo (véase manual de instalación Access Point 2411).

3. En el Edificio de Gobierno se conectó otro Access Point modelo 2411 con el fin de poder establecer el enlace entre ambos edificios. Éste se configuró como maestro.

En el siguiente diagrama se muestra como está físicamente realizado el enlace. (Figura 66).

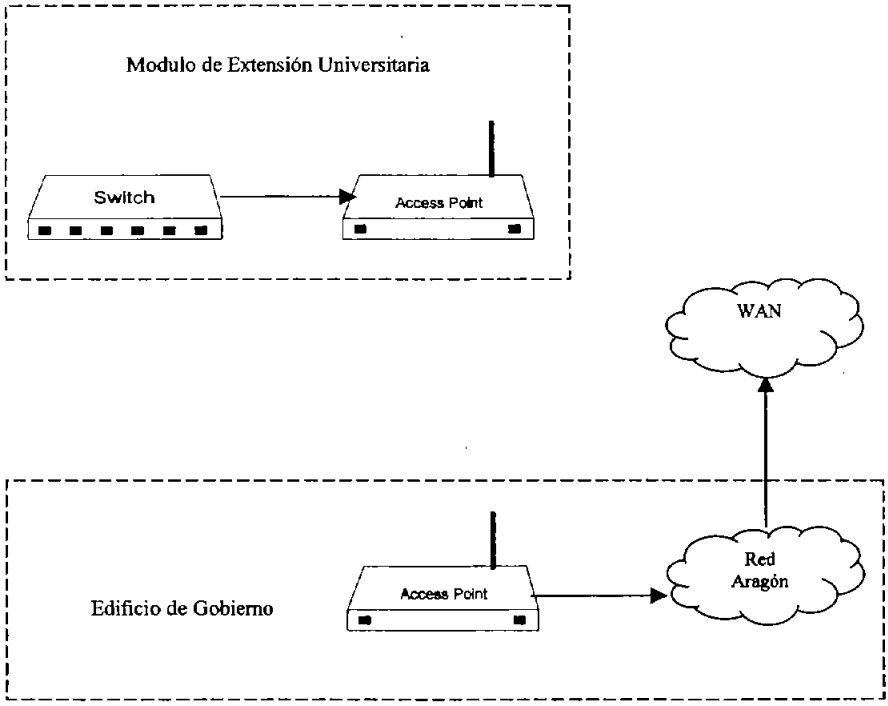


Figura 66

4.9.- Instalación del Access Point modelo 2411 WLAN

Al igual que el modelo 2311 el AP 2411 también se tiene que instalar su software en la computadora donde lo vamos a configurar, hay que ejecutar el archivo Setup.exe y seguir las indicaciones en pantalla. (Figura 67 y 68).

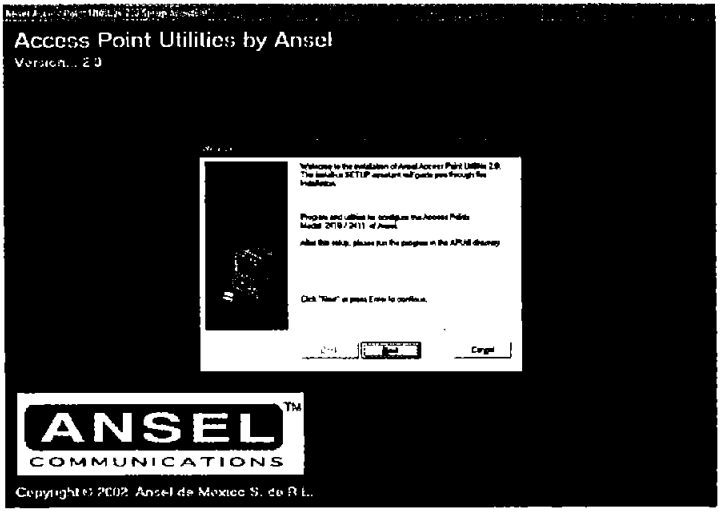


Figura 67

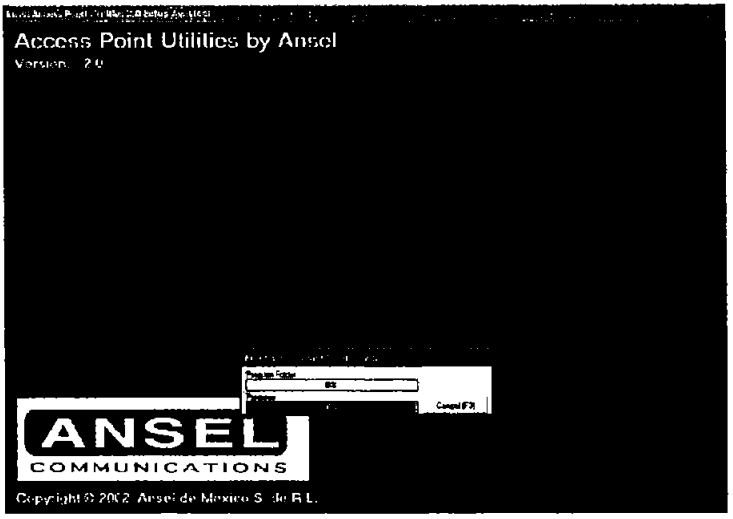


Figura 68

Al terminar de instalar el software hay que ejecutar AP Configuration para poder ver los AP que tenemos conectados en nuestra red y así modificar sus parámetros o simplemente revisarlos. (Figura 69 y 70).

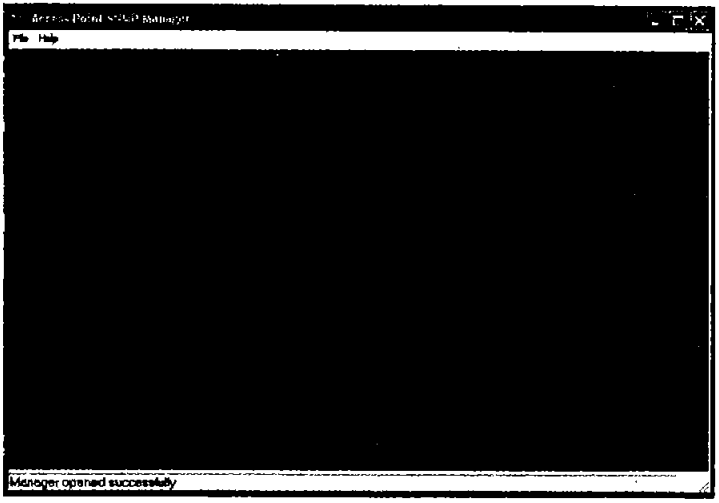


Figura 69

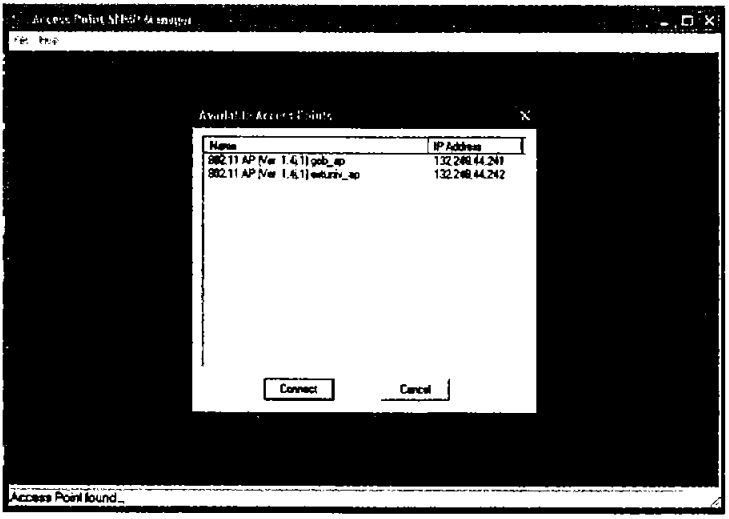


Figura 70

Ahora nos vamos a la opción File y ahí elegimos Find Access Point en este caso encontramos dos AP uno que está conectado en el Módulo de Extensión Universitaria y el otro en el Edificio de Gobierno, la información que nos proporciona el software es el nombre del AP y su dirección IP.

Desde aquí ya podemos revisar que estén funcionando adecuadamente así como modificar su configuración.

CAPÍTULO V

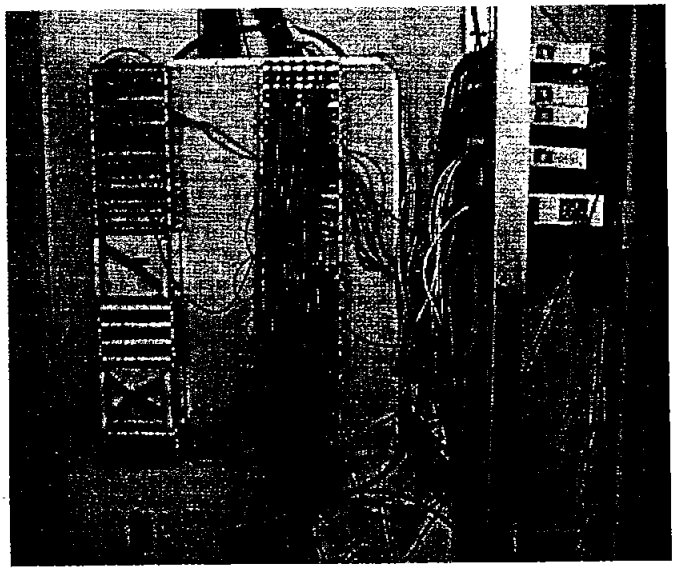
FUTURO DE LA RED EN LA ENEP ARAGÓN

5.1.- Panorama en la red de la Enep Aragón.

En la actualidad la red de la Enep Aragón se encuentra en decadencia ya que el equipo con el que se cuenta en estos momentos es obsoleto respecto a la nueva tecnología existente.

Esto quiere decir que se encuentra funcionando con concentradores existentes desde 1996 este es uno de los principales problemas ya que estos equipos están casi totalmente desapareciendo del mercado por tal motivo se cuenta con poco soporte técnico y hace que su mantenimiento sea cada vez más problemático y costoso debido a que las refacciones son cada vez mas difíciles de conseguir, además estos concentradores son muy lentos y no permiten agilizar el tráfico en la red.

No solo los concentradores están en malas condiciones sino también el cableado con el que se cuenta está funcionando bajo esquemas fuera de la normatividad establecida ya que se han hecho muchos cambios debido al crecimiento que ha tenido la escuela en materia de equipo de cómputo. (Figura 71).



Situación Actual

Figura 71

También la fibra óptica no se está aprovechando al máximo debido a que los concentradores de fibra con los que se cuenta actualmente sólo pueden transmitir a una velocidad máxima de 10 Mbps. Por tal motivo actualmente la Fibra óptica sólo sirve como un medio de comunicación entre diversos puntos remotos pero sin disfrutar de las ventajas que ésta es capaz de brindar. Ya que la fibra es capaz de transmitir a 100 ó a 1000 Mbps. Con un switch de fibra adecuado. (Figura 72).

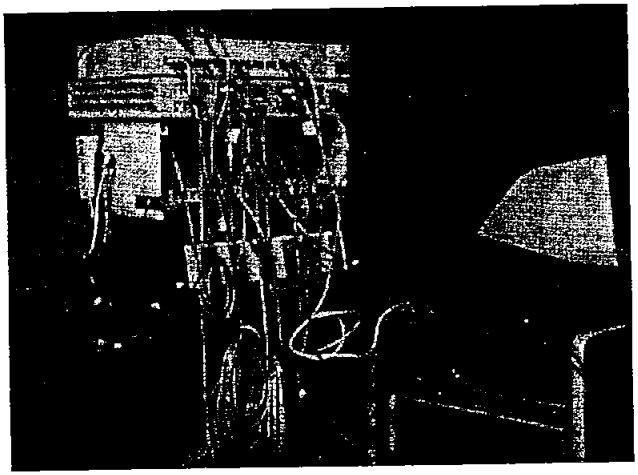


Figura 72

En cuanto equipo de cómputo cabe señalar que aunque existen todavía algunas computadoras obsoletas en la escuela, la gran mayoría son equipos recientes Pentium III y Pentium IV, los cuales periódicamente se están actualizando para un dar un mejor servicio en todas las áreas.

Debido a todos estos detalles que existen actualmente en la red, es necesario hacer una reestructuración planeando y creando programas y/o estrategias para el mantenimiento y mejora de la red así como para la ampliación de la misma, tanto a corto, como mediano y largo plazo.

En la tabla 7 se muestra una proyección a 3 años de lo que creemos es mas necesario para llegar a una reestructuración total de la Red de la Enep Aragón y así ir avanzando paso a paso hasta llegar al nivel óptimo.

Futuro de la Enep Aragón en el Área de Comunicaciones.

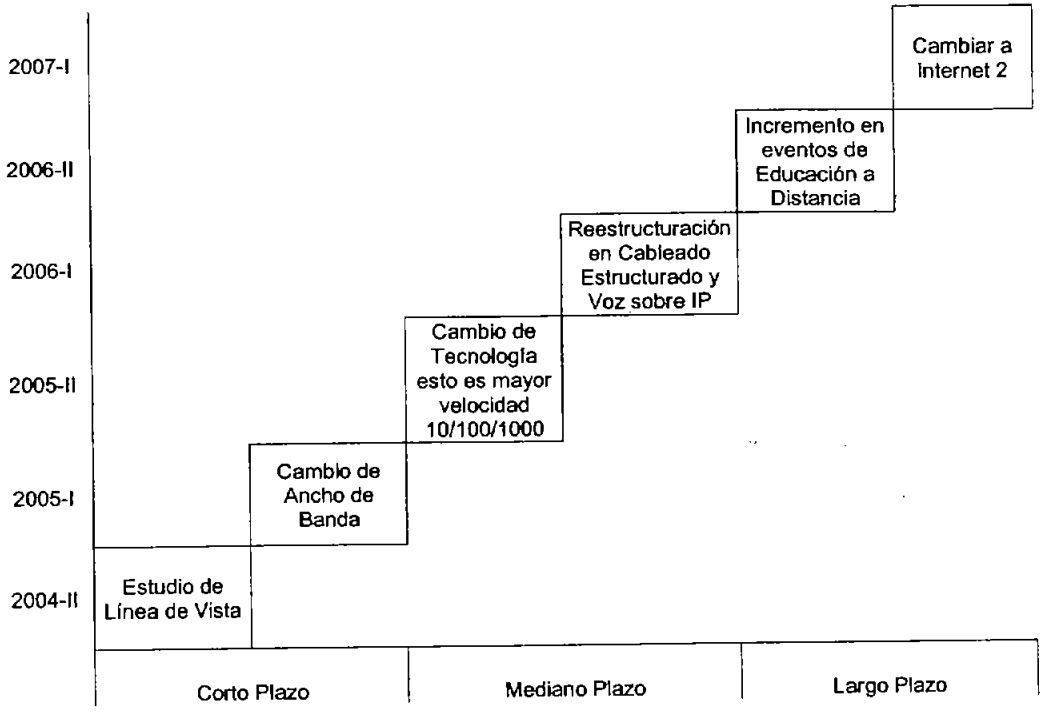


Tabla 7

5.2.- Corto plazo.

En el corto plazo se tiene que hacer un estudio de línea de vista, esto es un análisis de todos los cambios que son necesarios para mejorar el rendimiento de la red así como todo lo necesario para su reestructuración.

Primeramente tenemos que pensar en tener un ancho de banda mayor ya que en la actualidad sólo se cuenta con un enlace E1, esto le corresponde a DGSCA, tienen que hacer una licitación para hacer los cambios necesarios esto es un concurso para cambiar los equipos de comunicaciones por unos más actuales que nos brinden una salida mayor esto es un ancho de banda mejor el cual soporte a todo el equipo de cómputo que requiere de un acceso a Red UNAM e Internet.

Estos cambios traerían beneficios en toda la Red de la Enep Aragón en cuanto a salida a Internet se refiere pero también se requiere de una comunicación rápida y confiable dentro del plantel esto es la red interna, para esto se necesitan hacer unos cambios tanto en el

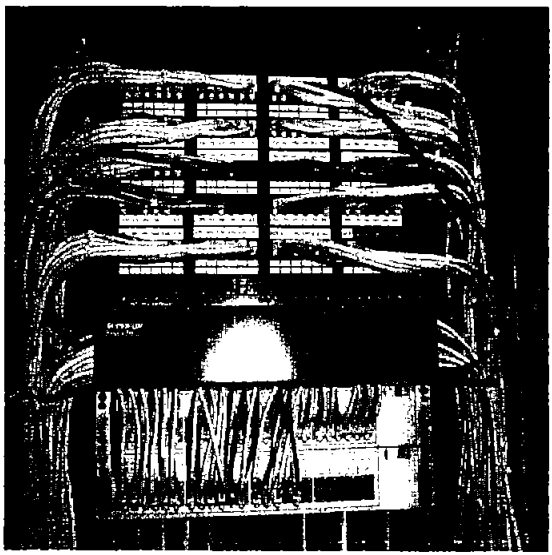
cableado como en los aparatos que están funcionando actualmente (Hubs) todo esto lo vemos en lo que es a mediano plazo.

5.3.- Mediano plazo.

En este caso vamos a proponer algunos cambios de lo que se puede hacer para optimizar el funcionamiento de la red de datos de la Enep Aragón.

- Actualizar la tecnología con la que se trabaja, esto es hacer una migración de los concentradores que actualmente transmiten a 10 Mbps. sustituirlos por switches que transmiten a 10/100/1000 Mbps.

- Mejorar el cableado existente por uno estructurado que permita mayor flexibilidad para resolver rápidamente posibles fallas en el sistema de comunicación, mejor desempeño de la red, así como incorporar a futuro nuevas tecnologías (voz por el mismo cableado de datos). (Figura 73).



Situación Deseable

Figura 73

Para mejorar el cableado existente se proponen los siguientes elementos:

- Patch panel.
- Organizadores Horizontales.
- Organizadores Verticales.
- Scaneo de servicios para verificar funcionamiento.

También será necesario que en algunos equipos de cómputo se cambien las tarjetas de red de 10 Mbps por tarjetas 10/100 Mbps. Aunque los nuevos equipos ya cuentan con dichas tarjetas

5.3.1.- Crear VPN´S

Otro de los planes que se necesitan implementar dentro de la Red es el uso de las VPN's (Redes Privadas Virtuales), una Virtual Private Network es un sistema para simular una red privada sobre una red pública. (Figura 74).

La idea es que la red pública sea "vista" desde dentro de la red privada como un cable lógico que une las dos o más redes que pertenecen a la red privada.

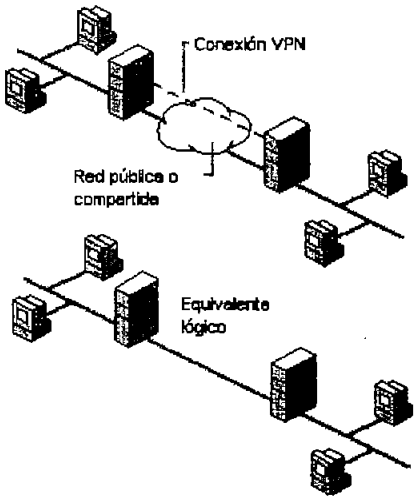


Figura 74

Las VPNs también permiten la conexión de usuarios móviles a la red privada, tal como si estuvieran en una LAN dentro de una oficina de la empresa donde se implementa la VPN. Esto resulta muy conveniente para personal que no tiene lugar fijo de trabajo dentro de la empresa, como podrían ser vendedores, ejecutivos que viajan, personal que realiza trabajo desde el hogar, etc.

La forma de comunicación entre las partes de la red privada a través de la red pública se hace estableciendo túneles virtuales entre dos puntos para los cuales se negocian esquemas de encriptación y autentificación que aseguran la confidencialidad e integridad de los datos transmitidos utilizando la red pública.

Como se usan redes públicas, en general Internet, es necesario prestar debida atención a las cuestiones de seguridad, que se aborda a través de estos esquemas de encriptación y autentificación y que se describirán luego.

La tecnología de túneles ("Tunneling") es un modo de transferir datos en la que se encapsula un tipo de paquetes de datos dentro del paquete de datos de algún protocolo, no necesariamente diferente al del paquete original. Al llegar al destino, el paquete original es desempaquetado volviendo así a su estado original. En el traslado a través de Internet, los paquetes viajan encriptados.

Las técnicas de autentificación son esenciales en las VPNs, ya que aseguran a los participantes de la misma que están intercambiando información con el usuario o dispositivo correcto. La autentificación en VPNs es conceptualmente parecido al logeo en un sistema como nombre de usuario y contraseña, pero con necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autentificación usados en VPN están basados en un sistema de claves compartidas.

La autentificación es llevada a cabo generalmente al inicio de una sesión, y luego aleatoriamente durante el curso de la misma, para asegurar que no exista algún tercer participante que se haya intrometido en la conversación. La autentificación también puede ser usada para asegurar la integridad de los datos. Los datos son procesados con un algoritmo de hashing para derivar un valor incluido en el mensaje como checksum. Cualquier desviación en el checksum indica que los datos fueron corruptos en la transmisión o interceptados y modificados en el camino.

Ejemplos de sistemas de autentificación son Challenge Handshake Authentication Protocol (CHAP) y RSA.

Todas las VPNs tienen algún tipo de tecnología de encriptación, que esencialmente empaqueta los datos en un paquete seguro. La encriptación es considerada tan esencial como la autentificación, ya que protege los datos transportados de la poder ser vistos y entendidos en el viaje de un extremo a otro de la conexión. Existen dos tipos de técnicas de encriptación que se usan en las VPN: encriptación de clave secreta, o privada, y encriptación de clave pública.

En la encriptación de clave secreta, se utiliza una contraseña secreta conocida por todos los participantes que necesitan acceso a la información encriptada. Dicha contraseña se utiliza tanto para encriptar como para desencriptar la información. Este tipo de encriptación posee el problema que, como la contraseña es compartida por todos los participantes y debe mantenerse secreta, al ser revelada, debe ser cambiada y distribuida a los participantes, con lo cual se puede crear de esta manera algún problema de seguridad.

La encriptación de clave pública implica la utilización de dos claves, una pública y una secreta. La primera es enviada a los demás participantes. Al encriptar, se usa la clave privada propia y la clave pública del otro participante de la conversación.

Al recibir la información, ésta es desencriptada usando su propia clave privada y la pública del generador de la información. La gran desventaja de este tipo de encriptación es que resulta ser más lenta que la de clave secreta.

En las VPNs, la encriptación debe ser realizada en tiempo real. Por eso, los flujos encriptados a través de una red se realizan utilizando encriptación de clave secreta con claves que son solamente buenas para sesiones de flujo.

El protocolo más usado para la encriptación dentro de las VPNs es IPSec, que consiste en un conjunto de proposals del IETF que delinean un protocolo IP seguro para IPv4 y IPv6. IPSec provee encriptación a nivel de IP.

El método de túneles, como fue descrita anteriormente, es una forma de crear una red privada. Permite encapsular paquetes dentro de paquetes para acomodar protocolos incompatibles. Dentro de los protocolos que se usan para la metodología de túneles se encuentran Point-to-Point Tunneling Protocol (PPTP), Layer-2 Fowarding Protocol (L2FP) y el modo túnel de IPSec.

5.3.2.- Protocolos utilizados en las VPNs

PPTP: Point-to-Point Tunneling Protocol fue desarrollado por ingenieros de Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft, y ECI Telematics para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual.

Como protocolo de túnel, PPTP encapsula datagramas de cualquier protocolo de red en datagramas IP, que luego son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP, como Internet.

PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en Internet para tener la misma autentificación, encriptación y los mismos accesos de LAN como si marcaran directamente al servidor. En vez de marcar a un modem conectado al servidor RAS, los usuarios se conectan a su proveedor y luego "llaman" al servidor RAS a través de Internet utilizando PPTP.

Existen dos escenarios comunes para este tipo de VPN:

- El usuario remoto se conecta a un ISP que provee el servicio de PPTP hacia el servidor
- El usuario remoto se conecta a un ISP que no provee el servicio de PPTP hacia el servidor RAS y, por lo tanto, debe iniciar la conexión PPTP desde su propia máquina cliente.

Para el primero de los escenarios, el usuario remoto establece una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS.

Para el segundo escenario, el usuario remoto se conecta al ISP mediante PPP y luego "llama" al servidor RAS mediante PPTP. Luego de establecida la conexión PPTP, para cualquiera de los dos casos, el usuario remoto tendrá acceso a la red corporativa como si estuviera conectado directamente a la misma.

La técnica de encapsulamiento de PPTP se basa en el protocolo Generic Routing Encapsulation (GRE), que puede ser usado para realizar túneles para protocolos a través de Internet. La versión PPTP, denominada GREv2, añade extensiones para temas específicos como Call Id y velocidad de conexión.

El paquete PPTP está compuesto por un header de envío, un header Ip, un header GREv2 y el paquete de carga. El header de envío es el protocolo enmarcador para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, frame relay, PPP. El header IP contiene información relativa al paquete IP, como pueden ser, direcciones de origen y destino, longitud del datagrama enviado, etc. El header GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor. Por último, el paquete de carga es el paquete encapsulado, que, en el caso de PPP, el datagrama es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros. (Figura 75).

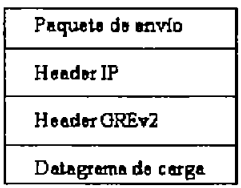


Figura 75

Para la autentificación, PPTP tiene tres opciones de uso: CHAP, MS-CHAP y aceptar cualquier tipo, inclusive texto plano. Si se utiliza CHAP, standard en el que se intercambia un "secreto" y se comprueba ambos extremos de la conexión coincidan en el mismo, se utiliza la contraseña de Windows NT, en el caso de usar este sistema operativo, como secreto. MS-CHAP es un standard propietario de Microsoft y resulta ser una ampliación de CHAP. Para la tercer opción, el servidor RAS aceptará CHAP, MS-CHAP o PAP (Password Autenthication Protocol), que no encripta las contraseñas.

Para la encriptación, PPTP utiliza el sistema RC4 de RSA, con una clave de sesión de 40 bits.

IPSec: Trata de remediar algunas fallas del IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP).

Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión. Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación. Por autenticidad se entiende la validación de remitente de los datos. Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

AH: Provee autentificación, integridad y protección a repeticiones pero no así confidencialidad. La diferencia más importante con ESP es que AH protege partes del header IP, como las direcciones de origen y destino.

ESP: Provee autentificación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header.

AH sigue al header IP y contiene diseminaciones criptográficas tanto en los datos como en la información de identificación. Las diseminaciones pueden también cubrir las partes invariantes del header IP. El header de ESP permite rescribir la carga en una forma encriptada. Como no considera los campos del header IP, no garantiza nada sobre el mismo, sólo la carga.

Una división de la funcionalidad de IPSec es aplicada dependiendo de dónde se realiza la encapsulación de los datos, si es la fuente original o un gateway. El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los headers de seguridad son antepuestos a los de la capa de transporte, antes de que el header IP sea incorporado al paquete. En otras palabras, AH cubre el header TCP y algunos campos IP, mientras que ESP cubre la encriptación del header TCP y los datos, pero no incluye ningún campo del header IP.

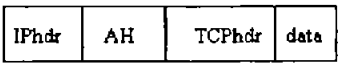
El modo de túnel es usado cuando el header IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un gateway. En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el header IP entre los extremos, agregando al paquete un header IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del gateway.

Los enlaces seguros de IPSec son definidos en función de Security Associations (SA). Cada SA está definido para un flujo unidireccional de datos y generalmente de un punto único a otro, cubriendo tráfico distinguible por un selector único. Todo el tráfico que fluye a través de un SA es tratado de la misma manera. Partes del tráfico puede estar sujeto a varios SA, cada uno de los cuales aplica cierta transformación. Grupos de SA son denominados SA Bundles. Paquetes entrantes pueden ser asignados a un SA específico por los tres campos definitorios: la dirección IP de destino, el índice del parámetro de seguridad y el protocolo de seguridad. El SPI puede ser considerado una cookie que es repartido por el receptor del SA cuando los parámetros de la conexión son negociados.

El protocolo de seguridad debe ser AH o ESP. Como la dirección IP de destino es parte de la tripleta antes mencionada, se garantiza que este valor sea único.

Un ejemplo de paquete AH en modo túnel es:

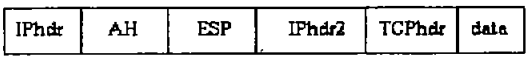
Un ejemplo de paquete AH en modo transporte es:



Como ESP no puede autentificar el header IP más exterior, es muy útil combinar un header AH y ESP para obtener lo siguiente:

Este tipo de paquete se denomina Transport Adjacency.

La versión de entunelamiento sería:



Sin embargo, no es mencionado en las RFC que definen estos protocolos. Como en Transport Adjacency, esto autenticaría el paquete completo salvo algunos pocos campos del header IP y también encriptaría la carga. Cuando un header AH y ESP son directamente aplicados como en esta manera, el orden de los header debe ser el indicado. Es posible, en el modo de túnel, hacer una encapsulación arbitrariamente recursiva para que el orden no sea el especificado.

L2TP: Layer-2 Tunneling Protocol (L2TP) facilita el entunelamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos corran.

El escenario típico L2TP, cuyo objetivo es la creación de entunelar marcos PPP entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local. (Figura 76).

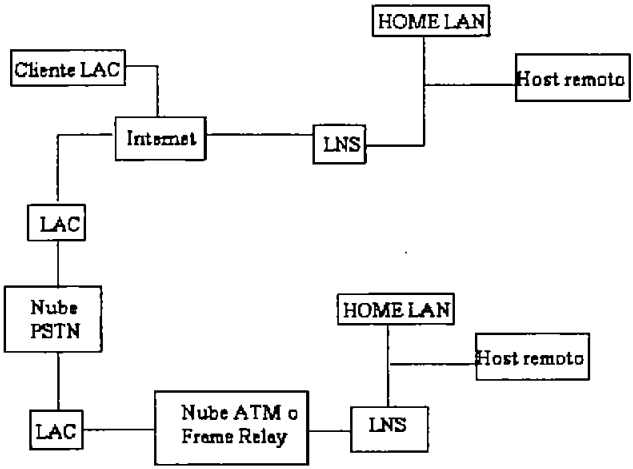


Figura 76

Un L2TP Access Concentrator (LAC) es un nodo que actúa como un extremo de un túnel L2TP y es el par de un LNS. Un LAC se sitúa entre un LNS y un sistema remoto y manda paquetes entre ambos. Los paquetes entre el LAC y el LNS son enviados a través del túnel L2TP y los paquetes entre el LAC y el sistema remoto es local o es una conexión PPP. Un L2TP Network Server (LNS) actúa como el otro extremo de la conexión L2TP y es el otro par del LAC. El LNS es la terminación lógica de una sesión PPP que está siendo puesta en un túnel desde el sistema remoto por el LAC. Un cliente LAC, una máquina que corre nativamente L2TP, puede participar también en el túnel, sin usar un LAC separado. En este caso, estará conectado directamente a Internet. El direccionamiento, la autentificación, la autorización y el servicio de cuentas son provistos por el Home LAN's Management Domain.

L2TP utiliza dos tipos de mensajes: de control y de datos. Los mensajes de control son usados para el establecimiento, el mantenimiento, el borrado de los túneles y las llamadas, Utilizan un canal de control confiable dentro de L2TP para garantizar el envío. Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel. La siguiente figura muestra la relación entre los marcos PPP y los mensajes de control a través de los canales de control y datos de L2TP. (Figura 77).

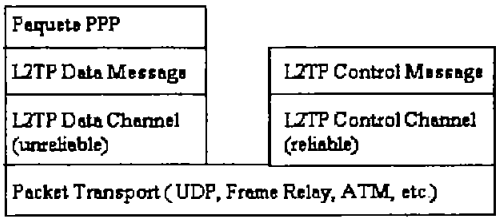


Figura 77

Los marcos PPP son enviados a través de un canal de datos no confiable, encapsulado primero por un encabezado L2TP y luego por un transporte de paquetes como UDP, Frame Relay o ATM. Los mensajes de control son enviados a través de un canal de control L2TP confiable que transmite los paquetes sobre el mismo transporte de paquete.

Se requiere que haya números de secuencia en los paquetes de control, que son usados para proveer el envío confiable en el canal de control. Los mensajes de datos pueden usar los números de secuencia para reordenar paquetes y detectar paquetes perdidos.

Al correr sobre UDP/IP, L2TP utiliza el puerto 1701. El paquete entero de L2TP, incluyendo la parte de datos y el encabezado, viaja en un datagrama UDP. El que inicia un túnel L2TP toma un puerto UDP de origen que esté disponible, pudiendo ser o no el 1701 y envía a la dirección de destino sobre el puerto 1701. Este extremo toma un puerto libre, que puede ser o no el 1701, y envía la respuesta a la dirección de origen, sobre el mismo puerto iniciador. Luego de establecida la conexión, los puertos quedan estáticos por el resto de la vida del túnel.

En la autentificación de L2TP, tanto el LAC como el LNS comparten un secreto único. Cada extremo usa este mismo secreto al actuar tanto como autenticado como autenticador.

Sobre la seguridad del paquete L2TP, se requiere que el protocolo de transporte de L2TP tenga la posibilidad de brindar servicios de encriptación, autentificación e integridad para el paquete L2TP en su totalidad. Como tal, L2TP sólo se preocupa por la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los puntos extremos del túnel, no entre los extremos físicos de la conexión.

Una vez que ya se han visto dos diferentes tecnologías útiles para la ampliación y robustecimiento de las comunicaciones de voz y datos se verán las diferentes áreas que hasta la fecha no cuentan con servicio de red:

5.4.- Proyectos a largo plazo

5.4.1.- Internet 2

Se busca que en un futuro se pueda implementar el servicio de Internet 2 en la totalidad de la red de la UNAM incluyendo la Enep Aragón, pero ¿qué es el Internet 2?

El Internet 2 o también llamado I2 es el proyecto más importante sobre el desarrollo tecnológico de Internet. Con la iniciativa del grupo NGI en 1996, 34 de las principales Universidades de USA se reunieron con el espíritu de crear una nueva red e inician el proyecto Internet 2. En la actualidad son más de 200 Universidades afiliadas al proyecto solamente en Estados Unidos.

El objetivo del I2 es investigar, diseñar e implantar una red de alta velocidad, esto es que soporte las necesidades de las nuevas aplicaciones de educación e investigación, tales como:

- Educación a Distancia
- Bibliotecas Digitales
- Telemedicina
- Astronomía
- Ciencias de la Tierra
- Robótica
- Supercómputo compartido

Aquí en México fue hasta 1999 que se crea la CUDI (Corporación Universitaria del Desarrollo de Internet). Entre sus principales participantes están:

- UNAM
- IPN
- UAM
- ITESM
- UANL
- UAT
- UdeG
- UDLA
- CICESE

En la actualidad la CUDI cuenta con 70 instituciones académicas integradas al proyecto I2 en México. Su objetivo es el de dotar a la Comunidad Científica y Universitaria de México de una red de telecomunicaciones que le permita crear una nueva generación de investigadores, proporcionándoles nuevas y mejores herramientas que les permitan desarrollar aplicaciones científicas y educativas de alta tecnología a nivel mundial.Actualmente el Backbone de I2 en México lo proporciona Telmex con enlaces de la ciudad de México a Guadalajara, Tijuana, Monterrey y Cd. Juárez, y Avantel tiene

enlaces de la Cd. de México a Monterrey y de ahí a Reynosa. Todas estas conexiones transmiten a 155 Mbps. (Figura 78).

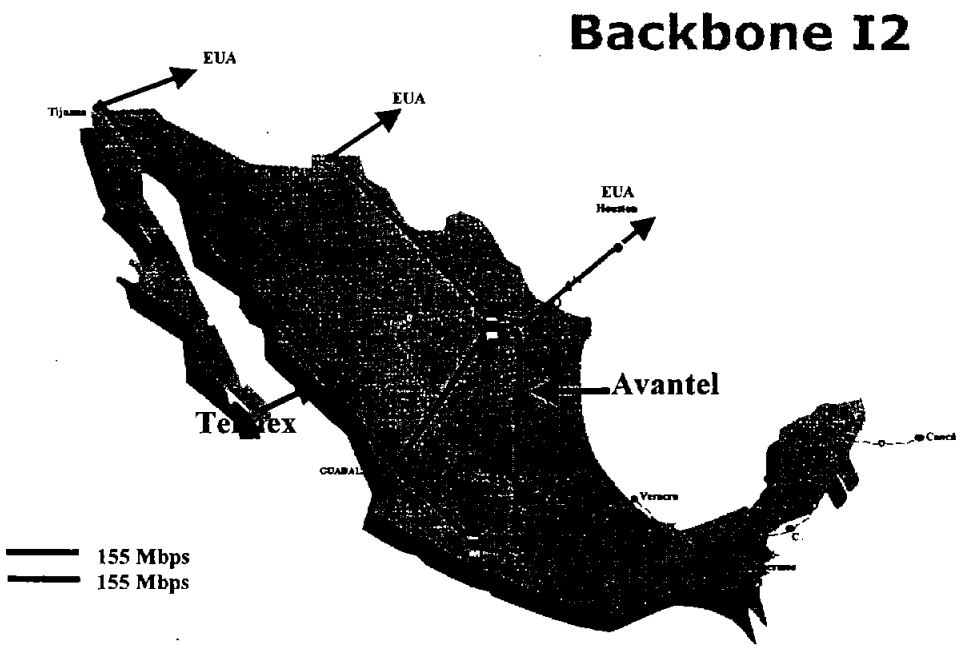


Figura 78

Dentro de la UNAM el I2 como fase inicial e inmediata se buscó fortalecer la infraestructura del backbone hacía una mas robusta con tecnologías de vanguardia que permitieran soportar con alto nivel de control, calidad y disponibilidad las aplicaciones de investigación y académicas de alta demanda dentro de la UNAM.

Se tiene un proyecto Backbone GigabitEthernet cuyo objetivo es hacer una reestructuración y actualización de la red de datos de la UNAM, implementando un Backbone (Figura 79) que sea capaz de soportar de forma óptima todos los servicios de datos, voz y video sobre IP y aplicaciones emergentes que lo demanden, además de ser suficientemente flexible para permitir su crecimiento cuando lo requiera.

De esta forma se busca ubicar a la Red UNAM como una de las redes académicas más robustas y de alta calidad de operación en el mundo. Todo esto beneficiará el soporte de aplicaciones multimedia como son:

- VoIp (voz sobre IP)
- Video

También se beneficiará el soporte al dar un menor tiempo de respuesta a fallas, una mejor calidad de servicio, actualización en el equipo así como un crecimiento.

Con todo esto también se buscará la integración de las dependencias con proyectos que demanden capacidades de I2. Además del uso óptimo de los recursos basado en la Ingeniería de tráfico la cual consiste en procesos de control del comportamiento del tráfico en los medios físicos y lógicos de la red para optimizar recursos y controlar el desempeño de la red. Y no solamente en el ancho de banda.

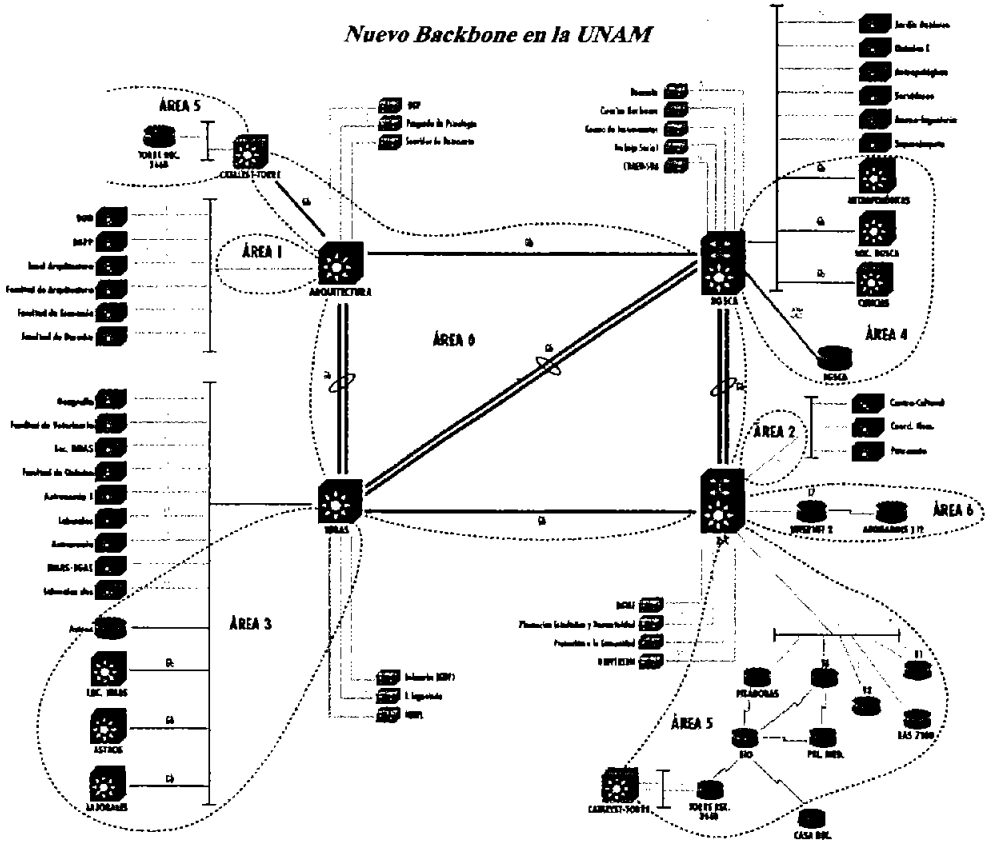


Figura 79

Así se espera que en un futuro llegue lo que es el I2 a la ENEP Aragón y con él todos los beneficios y ventajas que se han visto. En la (figura 80) se muestra cómo se realizaría el enrutamiento lógico del tráfico dentro de la red. Por un lado quedaría la red actual con el enlace a Internet y por otro lado lo que sería ya el I2.

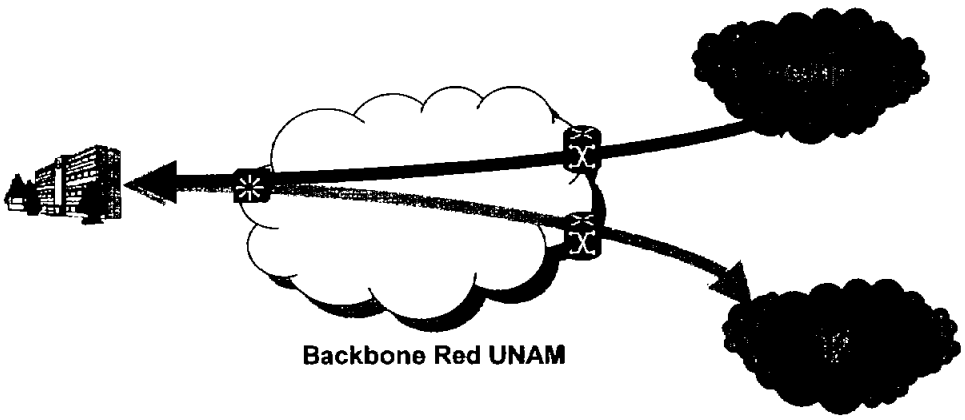


Figura 80

También existen otros proyectos en desarrollo para el I2 uno de ellos es el CAESAR (Connecting all European and South American Researchers). Y el proyecto CLARA (Cooperación Latino Americana de Redes Avanzadas).

Existen otras redes del tipo I2 entre las más importantes se encuentran:

- ABILENE (Estados Unidos)
- CANARIE (Canadá)
- DANTE (España)
- TERENA (España)
- APAN (Asia-Pacífico)
- RENATER (Francia)
- REUNA (Chile)
- RETINA (Argentina)
- CERNET (China)
- SIGAREN (Singapur)
- CRNET (Costa Rica)

Conclusiones

La presentación de este trabajo no es más que la documentación de un proceso que se llevó a cabo en la ENEP Aragón, mediante el cuál se implementó la tecnología inalámbrica con la finalidad de poder enlazar las diferentes áreas que se encuentran ubicadas en el plantel de una forma rápida, segura y además que no contaban con acceso a red.

Así mismo se cumplió con los objetivos planteados como fue enlazar las áreas académico - administrativas que no contaban con acceso a red e Internet. Mediante el uso de tecnología inalámbrica.

Como consecuencia se beneficiaron diferentes áreas en el Edificio del Centro de Lenguas Extranjeras entre éstas destacan:

Centro de Lenguas (con 5 computadoras en red)
Educación Continua (con 5)
Profesores de carrera primer piso (con 27)
Profesores de carrera planta baja (con 17)
Bolsa de trabajo (con 2)
Salón Rojo (con 1)

Obteniendo como resultado un total de 57 computadoras conectadas y un beneficio en investigación a los profesores de carrera, Intercambio de información a los profesores de Idiomas y el acceso de bolsa de trabajo a empresas que otorgan oportunidades de empleo a los alumnos de la ENEP.

Cabe mencionar la automatización del Departamento de Adquisiciones vía Internet efectuando sus transacciones en línea para registro de inventarios y pago a proveedores. Servicios Generales y Superintendencia de Obras obtuvo como resultado la publicación de bases de concursos de obra vía Internet tales como el estacionamiento de profesores y otras actividades del plantel.

Se logró finalmente el enlace de los laboratorios de Ingeniería que son L1, L2, y L4 teniendo como consecuencia que los estudiantes y profesores del área de Ing. Mecánica y de Ing. Civil consultaran información de su plan curricular beneficiando aproximadamente a 2000 usuarios.

También cabe mencionar que se pusieron routers para evitar usar tantas direcciones IP fijas ya que con las que se cuenta actualmente no son suficientes debido a que sólo se tienen 3 segmentos y en el plantel tenemos un aproximado de 1100 computadoras. De esta manera se usaron hasta 254 IP Dinámicas ocupando una sola IP fija.

Finalmente podemos mencionar que la tecnología inalámbrica está en pleno desarrollo y que poco a poco se irán alcanzando mayores velocidades de transferencia que van desde los 54 Mbps hasta los 125 Mbps y en un futuro hasta 1 Gb. Así como también su costo será menor debido a que cada día son más usuarios los que optan por usar esta tecnología.

Glosario de términos

802.11b
IEEE 802.11b es una norma de redes inalámbricas creada por el Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Electricistas y Electrónicos) (IEEE).

"Access point" o Punto de acceso.
El dispositivo físico, similar a un hub, permite al usuario acceder a una red inalámbrica.

Ancho de banda
Una medida de la capacidad de transmisión de información dentro de una red. Las señales de video, por ejemplo, ocupan más ancho de banda que el texto para transmitirse en una red. El ancho de banda es un tema importante para los administradores de redes.

Bridge
Dispositivo hardware ó software utilizado para conectar dos redes o dividir una red sobrecargada en dos ramas separadas.

BSS
Cuando un punto de acceso está conectado a una red alambrada y a un conjunto de dispositivos inalámbricos, se denomina Basic Service Set (Conjunto de Servicio Básico) (BSS). Un Extended Service Set (Conjunto de Servicio Extendido) (ESS) es un conjunto de dos o más BSS que forman una subred sencilla. Véase ESS ID.

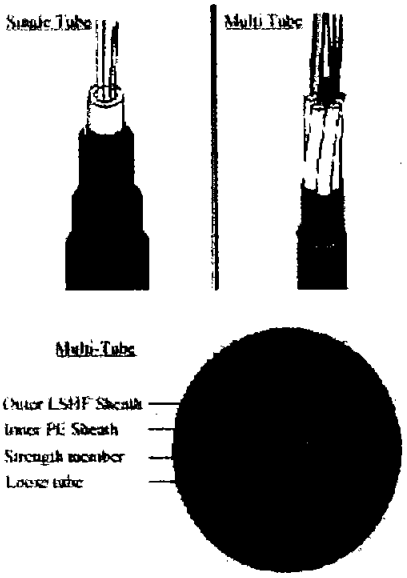
Cable RJ-45, Par Trenzado ó UTP
Estas formas de denominación se refieren a la misma tecnología de cableado. La primera hace referencia a la normativa del cable propiamente dicho, la segunda a su nombre y la tercera al nombre técnico que utilizan los conectores usados en este tipo de cableado.
Cuando nos referimos a este cable y utilizamos "el apellido" Tipo 5, nos referimos a que dicho cable se compone de 8 hilos conductores de cobre. Existen otros Tipos, como el 3 compuesto de 4 hilos ó el Tipo 1, pero que con la incorporación de nuevas tecnologías han caído en desuso.
Es un cable compuesto, de fuera a dentro, de una funda de plástico, habitualmente de color gris, tras la cual se encuentran 8 hilos de cobre cubiertos de una funda plástica y entrelazados en pares dando dos vueltas y media por pulgada. (De ahí su nombre Par Trenzado).
Para la utilización de este tipo de cableado es necesario instalar un concentrador para que haga la función de repartidor de señales, por eso se denomina topología en estrella.
La distancia máxima utilizada en este tipo de cable es de 105 metros entre la tarjeta de red y el concentrador.

Cable STP, FTP ó RJ-49
No es mas que una derivación de la anterior estructura de cableado, incluyendo una platina de metal de separación entre la capa plástica de protección del cable y de los hilos.
No es ni mejor ni peor que el anterior cable, simplemente su utilización será recomendada en determinados entornos en detrimento del RJ-45 ó UTP.

Cable de Fibra Óptica

Cada vez mas utilizado este tipo de cableado, por su flexibilidad, manejabilidad y distancias que soporta. Se compone de dos hilos conductores, transmisión y recepción, de señal óptica. La distancia máxima que soporta es de 2 Km.

Todavía es una filosofía de cableado cara y costosa de grimpar, pues un error en el grimpaje del conector y habría que tirar el latiguillo de cable, pero se va imponiendo con mayor fuerza, se utiliza principalmente para Servicios de Datos ya que su ancho de banda y alta velocidad es ideal para ese propósito.



Aunque hay muchos tipos diferentes de Cables de Fibra Optica en cables para datos nos concentraremos en 62.5/ 125 Loosetube. Los números 62.5/ 125 se refiere al tamaño de la Fibra (Micrones) y Loosetube se refiere al tipo de construcción usado en el cable.

Existen variados cables Loosetube, tanto en cuanto a su construcción como a la cantidad de fibras.

En general se emplean dos tipos; un solo tubo ó multitubo. En el tipo de un solo tubo solo todas las fibras se incluyen dentro de un solo tubo de diámetro de 5.5mm reforzados longitudinalmente en sus paredes. Esta construcción simple proporciona un nivel alto de aislamiento de las fibras de fuerzas exteriores mecánicas. Los cables multitubo ofrecen capacidades de fibras más altas y construcciones más complejas a veces requeridas en ambientes más hostiles. Pequeños tubos reforzados(3mm) se encuentran dentro de un tubo reforzado mayor. Cada tubo menor puede contener hasta 8 fibras.

Cable coaxial, biaxial y triaxial

Cable multiconductor no apareado

Cable multiconductor apareado

Cable de fibra óptica

Como características adicionales de los cables coaxiales tenemos:

- Su costo es moderado.
- Soporta velocidades de transmisión alta.
- Inmune a interferencias eléctricas, en condiciones normales.
- Buena tolerancia de fallas.

Concepto	Par Trenzado No Apantallado	Par Trenzado Apantallado	Coaxial	Fibra Optica
Tecnología Ampliamente Probada	Si	Si	Si	Si
Ancho de Banda	Medio	Medio	Alto	Muy Alto
Hasta 20 Mhz	Si	Si	Si	Si
Hasta 100 Mhz	Si (*)	Si	Si	Si
27 Canales video	No	No	Si	Si
> 50 canales video	No	No	No	Si
Canal Full Duplex	Si	Si	Si	Si
Distancias medias	100 m 65 Mhz	100 m 67 Mhz	500 (Ethernet)	2 km (Multi.) 100 Km. (Mono.)
Inmunidad Electro- magnética	Limitada	Media	Media	Alta
Seguridad	Baja	Baja	Media	Alta
Coste	Bajo	Medio	Medio	Alto

(*) UTP Categoría 5

Conector BNC

Es el conector utilizado cuando se utiliza cable coaxial. Como ya hemos dicho, la malla de cable coaxial y el hilo central están separados, así que es muy importante que a la hora de grimpar este conector al cable dichos hilos se hallen separados.

Conector RJ-45
Se utiliza con el cable UTP. Está compuesto de 8 vías con 8 "muelas" que a la hora de grimpar el conector pincharán el cable y harán posible la transmisión de datos. Por eso será muy importante que todas la muelas queden al ras del conector.

Conector RJ-49
Igual que el anterior, pero recubierto con una platina metálica para que haga contacto con la que recubre el cable STP.

DHCP
Dynamic Host Configuration Protocol (Protocolo de Configuración de Anfitrión Dinámica) (DHCP) es un procedimiento que siguen los ordenadores de una red para identificarse entre sí y asegurarse de que la información se transfiere correctamente.

Dirección IP (estática y DHCP)
Identifica una computadora determinada dentro de una red para las otras computadoras. Una dirección IP es similar a la dirección de una casa. En un barrio, cada casa tiene una dirección única; en una red cada computadora debe tener una dirección única. Hay dos tipos de direcciones IP: estáticas y DHCP.
Una dirección estática es donde alguien se conecta físicamente a una computadora y define la dirección IP para esa computadora. Una dirección estática no cambia a menos que alguien físicamente la cambie.
Las direcciones DHCP (protocolo de configuración dinámica de host) son asignadas dinámicamente desde un servidor que contiene un grupo de direcciones. El servidor presta a la computadora una de las direcciones disponibles por una cantidad específica de tiempo. Una vez agotado este tiempo específico, la computadora renueva el préstamo o solicita una dirección IP nueva.

DSSS.
Acrónimo de "Direct Sequence Spread Spectrum", sistema de transmisión de datos usado por las redes sin hilos.

drive-by hacking.
Técnica de hacking que localiza redes Wireless mediante un portátil o PDA mientras se conduce. De esta manera es relativamente fácil localizar gran número de redes en poco tiempo.

Dúplex completo
Transmisión simultánea de datos en ambas direcciones.

ESID.
Identificador del punto de acceso, es un nombre del tipo mi_red_sin_hilos, utilizado por los clientes para conectarse a el.

SSID
Significa Service Set Identifier (Identificador de Conjunto de Servicio) – simplemente - es el mismo nombre de la red que está conectada al punto de acceso

ESS ID
ESS ID (Extended Service Set-Identificador de Servicio Extendido) es una identificación asignada al punto de acceso con el que se conecta la tarjeta Wi-Fi inalámbrica. Los dispositivos inalámbricos que se conectan al punto de acceso deben usar el mismo ESS ID. El ESS ID puede tener un máximo de 32 caracteres, y distingue entre mayúsculas y minúsculas.

Frag Threshold (Umbral Frag)
La fragmentación se utiliza para mejorar la eficacia o transmitir ficheros grandes (paquetes) por una red inalámbrica. Cuando el Umbral Frag. está habilitado, los ficheros grandes se tienen que dividir antes de que se transmitan y reensamblen en el punto de acceso. El valor de fragmentación se puede fijar entre 256 y 1500.

Gatekeeper
El gatekeeper (GK) es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales H.323, gateways y MCUs. El GK puede también ofrecer otros servicios a los terminales, gateways y MCUs, tales como gestión del ancho de banda y localización de los gateways o pasarelas.

H.323
Es una familia de estándares definidos por el ITU para las comunicaciones multimedia sobre redes LAN. Está definido específicamente para tecnologías LAN que no garantizan una calidad de servicio (QoS). Algunos ejemplos son TCP/IP e IPX sobre Ethernet, Fast Ethernet o Token Ring. La tecnología de red más común en la que se están implementando H.323 es IP (Internet Protocol).

Hotspot.
Área geográfica a la que da cobertura un punto de acceso, para puntos de acceso normales este área suele cubrir un radio de 100 metros. Un Hotspot puede ser: nuestra oficina, un aeropuerto, una sala de convenciones, etc.

HUB (Concentrador)
Es un dispositivo hardware utilizado en las redes de cableado UTP ó STP para conformar una red LAN. Realmente lo que hace es repartir la señal y lanzarlo a lo largo del cable a todas las estaciones de la red. Denominamos a este tipo de red de "estrella", puesto que en vez de una línea continua de cable se utiliza una por estación de trabajo. Hay dos tipos de concentradores: estándar y conmutador.
Un concentrador estándar comparte ancho en banda entre todos los puertos. Por ejemplo, si tiene un concentrador estándar de ocho puertos de 100 Mps, todos sus puertos compartirán el ancho de banda de 100 Mps.

Con un concentrador conmutador, cada puerto recibe una cantidad determinada de ancho de banda. Por ejemplo, si tiene un concentrador estándar de ocho puertos de 100 Mps, cada puerto recibe un ancho de banda completo de 100 Mps.

MAC Address (Dirección MAC)
(Media Access Control) Dirección de Control de Acceso a Medios (MAC), una dirección de hardware que identifica de modo individual un punto de acceso, la tarjeta LAN inalámbrica o cualquier otro dispositivo de la red.

MCU (Multipoint Control Units)
La Unidad de Control Multipunto está diseñada para soportar la conferencia entre tres o más puntos, bajo el estándar H.323, llevando la negociación entre terminales para determinar las capacidades comunes para el proceso de audio y vídeo y controlar la multidifusión.

Modo Ad-Hoc
El modo Ad-Hoc hace posible que los dispositivos inalámbricos se comuniquen directamente entre sí, eliminando la necesidad de un punto de acceso o una conexión a una red alámbrica. El modo Ad-Hoc también se denomina modo peer-to-peer o Basic Service Set (Conjunto de Servicio Básico) independiente (IBSS). Véase MODO DE INFRAESTRUCTURA.

Modo de infraestructura
En modo de infraestructura, la red inalámbrica consta, como mínimo, de un punto de acceso conectado a la infraestructura de red alámbrica y un grupo de estaciones finales inálambricas. Véase el modo Ad-Hoc.

Navegador
Un programa de software que proporciona un medio para enviar y recibir información desde una red. Cuando se configura PelcoNet para visualizar imágenes de video a través de una computadora personal, se puede utilizar un navegador comercial, como Internet Explorer. Cuando se configura PelcoNet con los monitores CCTV de Pelco en una configuración de caja a caja, PelcoNet no utiliza un navegador comercial.

Puerta de entrada predeterminada
Es la dirección IP del ruteador, que se necesita para enviar información o señales de video desde una red a otra.

Red
Computadoras conectadas para compartir información. La red es como una ciudad y las computadoras son como las casas que la conforman. Hay dos tipos de redes: LAN y WAN.

Red Ad Hoc.
Conexión punto a punto entre dos ordenadores mediante tarjetas inalámbricas, no es necesario disponer de un punto de acceso.

Red Ethernet
Así denominamos al tipo de arquitectura que soporta nuestra red. En concreto la arquitectura ETHERNET utiliza una topología lineal (en bus), es decir, la información pasa en todo momento por todos los puntos de conexionado utilizando el método de acceso por detección de portadora con detección de colisiones (CSMA/CD). La velocidad de transmisión es de 10 Mbps.

Fast Ethernet
Su topología y forma de transmisión de la información es igual que la anterior, su única diferencia es que la velocidad de transmisión es de 100 Mbps.

Red Intranet
Una red privada de computadoras que utilizan tecnología basada en la web que le permite compartir información entre personas dentro de una compañía. Normalmente esta información es confidencial para la compañía y el público general no puede acceder a las intranets.

Red LAN
Red de área local; varias computadoras conectadas para compartir información. La información compartida podría incluir correo electrónico, archivos e impresoras. Una red LAN es como un barrio.

Red WAN
Es el acrónimo de "Wireless Local Area Network" Red de área amplia; varias redes LAN conectadas, normalmente a grandes distancias, para compartir información. Una red LAN es como todos los barrios de una ciudad, no confundir con LAN o WAN.

Ruteador
Un ruteador es un dispositivo que conecta dos redes. El ruteador lee la dirección de destino de la información enviada en una red y la envía al siguiente paso de su ruta.

Repeater ó Repetidor
Dispositivo hardware externo utilizado en redes coaxiales para modular y amplificar la señal que transporta dicha estructura de cableado.

RTCP (Real Time Control Protocol).
Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

RTS Threshold (Umbral RTS)
Umbral de solicitud de envío (Umbral RTS) es una petición de permiso para transmitir datos a un punto de acceso. Al activar esta opción, se evita que los datos de dos dispositivos inalámbricos lleguen al punto de acceso al mismo tiempo (colisionen). Si dos transmisiones inalámbricas colisionan en el punto de acceso, se perderán los datos de cada transmisión.

La colisión de transmisiones ocurre normalmente cuando dos dispositivos inalámbricos se encuentran al alcance del mismo punto de acceso, pero no al alcance el uno del otro. De hecho, se mantienen ocultos entre sí.

Cuando se activa el Umbral RTS, el dispositivo inalámbrico envía un mensaje de Solicitud de envío al punto de acceso antes de transmitir datos. El punto de acceso devuelve al dispositivo inalámbrico un mensaje de Clear to Send (Preparado para enviar), confirmando el tiempo reservado para la transmisión. Al mismo tiempo, el punto de acceso notifica a todos los demás dispositivos inalámbricos dentro del mismo alcance que aplacen la transmisión.

La configuración por defecto del Umbral RTS es Inhabilitado. El habilitar el Umbral RTS carga la red y afecta negativamente su rendimiento.

Servidor
Una computadora y su software que proporciona algún servicio a otras computadoras conectadas a ésta a través de una red.

SOHO
El término "SOHO" (pequeña oficina / casa oficina) es usada actualmente para diferentes tipos de aplicaciones. Las definiciones originales ANSI / EIA / TIA - 570 para cableado categoría 3 cableado pasado de moda y la inclinación común es un requerimiento para una infraestructura simple de servicio múltiple que puede ser manejado para muchas aplicaciones posibles, incluyendo datos, teléfono y CATV de acuerdo a los estándares, requiere un ancho de banda de 862 MHZ en Europa 855 MHZ en USA y 765 MHZ en Japón.

Con objeto de manejar las altas frecuencias en un cable balanceado (twisted - pair) junto con señales de frecuencia más bajos (e.g. data y teléfono) dos requerimientos mayores deben ser cumplidos:

- Las diferentes señales no deben interferir la una con la otra.
- Ninguna resonancia debería ser observada hasta la frecuencia más alta utilizada.

El cable horizontal TERA SOLUCION fue diseñado para cumplir estos dos requerimientos hasta 1.200 MHZ, suministrando un verdadero sistema de cableado de múltiple servicio para SOHO y para alguna otra aplicación variada usarse hasta 1.200 MHZ.

Transceiver ó Transceptor
Con estas dos palabras se denomina a un convertidor de medio, o lo que es lo mismo, a un aparato cuya función es la convertir un tipo de cable en otro. Por ejemplo, un TRANSCEIVER de FIBRA OPTICA nos convierte la señal de AUI a Fibra óptica.

VPN
(Redes Privadas Virtuales), una Virtual Private Network (VPN por sus siglas en inglés) es un sistema para simular una red privada sobre una red pública, por ejemplo, Internet.

Warchalking.
Sistema de símbolos utilizado por hackers. Mediante una combinación de señalaes escritas en los muros de los edificios, se informa de la existencia de una red inalámbrica y de su nivel de seguridad.

WEP.
Acrónimo de "Wired Equivalent Privacy" sistema de encriptacion de datos usado por los sistemas inalámbricos (40-bit o 128-bit), no es seguro y fácilmente violable.

WiFi.
Estándar que hace referencia al protocolo IEEE802.11b, gestionado por el Wireless Ethernet Compatibility Alliance. El sello WiFi nos garantiza la compatibilidad entre productos, de distintos fabricantes, con dicha certificación.

WISP.
Acrónimo de "Wireless Internet Service Provider", proveedor de acceso a Internet sin hilos. En estos momentos no existen proveedores de este tipo pero poco a poco van surgiendo iniciativas, la mayoria libres, para ofrecer cobertura Wireless en núcleos urbanos.

WEP Encryption (Encriptación WEP)
WEP (Wired Equivalent Privacy-Privacidad Equivalente Alámbrica) es un protocolo de seguridad para redes de área local inalámbricas (WLAN) definido en la norma 802.11b. WEP ha sido diseñado para proporcionar el mismo nivel de seguridad que tienen las LAN alámbricas.

Bibliografía

1. Zacker, Craig
Manual de Referencia de Redes
McGraw-Hill,España, 2001, 1046 p.

2. Hillar Gaston C.
Redes, Diseño, actualización y reparación
Editorial Hasa Argentina, 2004, 237 p.

3. Manual de Referencia Tarjeta inalámbrica LAN PC
USA, 2000, 44 p.

4. Manual de Referencia Acces Point Mod. 2311
USA, 1999, 40 p.

5. Manual de Referencia Acces Point Mod. 2411
USA, 1999, 40 p.

6. Tere Parnell ; tr. Ricardo de Cordoba Herralde
Guia lan times de redes de alta velocidad
Madrid; México: Interamericana McGraw Hill : Osborne, c1997
335 p

7. Michael J. Palmer ; traducción Manuel Delgado Cañizares
Redes de computadoras: una guía práctica
Mexico: Thomson Learning, c2001
482 p

8. Uyless black
Redes de computadoras: Protocolos, normas e interfaces
México: Macrobit : Ra-Ma, c1990
421 p

9. Jerry fitzgerald ; vers. en español, Sergio Manzanares Basurto y Hugo villa Gómez Velásquez
Comunicación de datos: Conceptos básicos, diseño y seguridad
México: Limusa, 1992
790 p

10. José Félix Rabago
Introducción a las redes locales
Madrid: Anaya Multimedia, 1996
251 p

11. Jesús García Tomas, Santiago Ferrando Girón, Mario Piattini Velthuis
Redes de alta velocidad
Madrid: Ra-ma, c1997
267 p.

Direcciones de Internet

1. http://tiny.uasnet.mx/prof/cln/ccu/mario/REDES/node39.html
2. http://www.baquia.com/com/20030117/bre00004.html
3. http://www.casadomo.com/canal_comunicaciones.asp?TextType=1430
4. http://www.computerworld.com.mx/redes-telecom/otras/laswlan802.htm
5. http://www.idg.es/dealer/impart.asp?clave=149421
6. http://www.pve.unam.mx/alerta/#3
7. http://www.wi-fi.org