



**UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO**

**FACULTAD DE ESTUDIOS SUPERIORES
ARAGÓN**

**“IMPLEMENTACIÓN DE REDES
INALÁMBRICAS EMPRESARIALES”**

T E S I S

QUE PARA OBTENER EL TÍTULO DE :
INGENIERO EN COMPUTACIÓN
P R E S E N T A N :

ABEL BECERRIL FAJARDO

CARLOS ANDRÉS SÁNCHEZ FLORES

ASESOR: ING. RODOLFO VÁZQUEZ MORALES



MÉXICO

2005

m. 346814



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

AGRADECIMIENTOS

Con agradecimiento y cariño

A mis padres

Sr. Abel Becerril Gil

Sra. Gloria Fajardo Zuñiga

*A mis hermanos universitarios Pedro y Cynthia,
a mi tía Glafira y a todos aquellos que me apoyaron
para cumplir este objetivo.*

Abel

*Agradezco a todas las personas que hicieron posible
concluir este trabajo de tesis, en especial a mi familia
que siempre me apoyó, a mis revisores por su tiempo
y sus valiosas opiniones, pero sobre todo a Dios
que me permitió llegar a este momento de mi vida.*

Carlos Andrés

*Con nuestro agradecimiento a la FES Aragón
A nuestros profesores y compañeros*

*Hacemos patente nuestro especial agradecimiento
al Ing. Rodolfo Vázquez Morales asesor de esta Tesis,
por su gentil apoyo y tiempo cedido para el desarrollo de la misma.*

ÍNDICE DE CONTENIDO

Objetivo General	IV
Justificación	V
Introducción	VI

Capítulo 1. Redes inalámbricas **Pág.**

1.1 ¿Qué es una red?	1
1.1.1 ¿Cómo funciona?	1
1.2 Clasificación de redes	4
1.2.1 Redes de conexión alámbrica	4
1.2.2 Redes de conexión inalámbrica	5
1.2.3 Distribución Geográfica	7
1.2.4 Topología Física	7
1.3 Redes WLAN	10
1.4 Topología de redes WLAN	12
1.5 Tecnología WLAN	14
1.5.1 Dispositivos de comunicación inalámbrica	14
1.5.2 Mecanismos de seguridad y configuración WLAN	15
1.5.2.1 Opciones de Seguridad para WLAN	15
1.5.2.2 Opciones de de configuración	16

Capítulo 2. El modelo OSI y su aplicación inalámbrica

2.1 ¿Qué es el modelo OSI?	17
2.2 Capas del modelo OSI	17
2.2.1 Capa de aplicación	21
2.2.2 Capa de presentación	21
2.2.3 Capa de sesión	22
2.2.4 Capa de transporte	23
2.2.5 Capa de red	24
2.2.6 Capa de enlace de datos	25
2.2.7 Capa física	25
2.3 Capas del modelo OSI que son modificadas por medios Inalámbricos	26

Capítulo 3. Tecnología de redes LAN y WLAN

3.1 Tecnologías de redes LAN	28
3.1.1 ARCnet	28
3.1.2 Token Ring	29
3.1.3 Ethernet	30

3.1.4 FDDI y CDDI-----	32
3.2 Tecnologías de redes WLAN-----	33
3.2.1 WLAN 802.11-----	34
3.2.2 WLAN 802.11b-----	34
3.2.3 WLAN 802.11g-----	34
3.2.4 WLAN 802.11a-----	35
3.2.5 Otras tecnologías-----	35
3.2.6 ¿Qué tecnología utilizar?-----	36
3.2.7 Compatibilidad de Wi-Fi-----	37
3.3 Wi-Max-----	37
3.4 Tecnología Bluetooth-----	39

Capítulo 4. Conformación y planeación de una red

4.1 Equipo-----	41
4.1.1 Estaciones de trabajo-----	41
4.1.2 Servidores-----	41
4.1.3 Periféricos-----	42
4.2 Conectividad-----	43
4.2.1 Tarjetas de interfaz a red-----	43
4.2.2 Medio de comunicación-----	44
4.2.3 Dispositivos de conectividad-----	45
4.2.3.1 Hub-----	45
4.2.3.2 Switch-----	45
4.2.3.3 Router-----	45
4.2.3.4 Puente-----	46
4.2.3.5 Repetidores-----	46
4.2.3.6 Modems-----	46
4.2.3.7 Firewall-----	46
4.2.4 Direccionamiento IP-----	48
4.2.4.1 Clasificaciones de IP-----	48
4.2.4.2 Estructura de IP-----	49
4.2.4.3 Clases de IP-----	49
4.2.4.4 Direcciones IP especiales y reservadas-----	51
4.2.4.5 DNS-----	52
4.2.4.6 Puertos y sus protocolos-----	53
4.3 Software-----	56
4.3.1 Sistemas operativos de red-----	56
4.3.2 Arquitecturas de los sistemas operativos más utilizadas-----	60
4.3.2.1 Arquitectura punto a punto-----	60
4.3.2.2 Arquitectura cliente servidor-----	61
4.4 Etapas para implementar un proyecto de red-----	61
4.4.1 Análisis de una red-----	62
4.4.2 Factores que intervienen en la planeación de una red-----	64
4.4.3 Elementos que intervienen en el diseño de una red-----	65
4.4.4 Implementación-----	66

Capítulo 5. Implementación de una red WLAN empresarial.

5.1 Método para implementar una red LAN empresarial-----	67
5.1.1 Etapa de planteamiento de problema-----	67
5.1.2 Etapa de análisis planeación y diseño-----	68
5.1.2.1 Infraestructura de la empresa-----	68
5.1.2.2 Características, ubicación de los equipos y requerimientos de los usuarios-----	72
5.1.2.3 Evaluación de alternativas tecnológicas-----	75
5.1.2.4 Arquitectura de red-----	78
5.1.2.5 Configuración de la arquitectura de red-----	85
5.1.2.6 Opciones de crecimiento-----	89
5.1.2.7 Presupuesto-----	89
5.1.3 Implementación de red-----	89
5.1.4 Configuración y seguridad de red-----	94
5.1.5 Prueba de red-----	109
Conclusión-----	110
Bibliografía-----	111
Direcciones Electrónicas-----	112
Glosario-----	115
Anexo A-----	122
Anexo B-----	126
Anexo C-----	130

OBJETIVO GENERAL

El objetivo de esta tesis es proporcionar los conceptos fundamentales que nos permitan entender el funcionamiento de una red de una manera clara y precisa. Así mismo, dotarnos de herramientas necesarias para poner en marcha una red empresarial inalámbrica de un modo práctico, fácil y seguro, utilizando los métodos y tecnologías precisos que nos garanticen su buen funcionamiento.

JUSTIFICACIÓN

Este trabajo estará dirigido principalmente a los estudiantes universitarios que tengan conocimientos de computación y estén interesados en las redes de cómputo inalámbricas y en la implementación de ellas.

Sabemos que las computadoras han venido a revolucionar a la humanidad, ya que se han convertido en una herramienta muy importante para el desarrollo de todo tipo de actividades empresariales. Las redes de cómputo han aumentado la productividad increíblemente, ya que le han dado a las computadoras un alcance jamás pensado. Un ejemplo de ello es Internet, la red más grande de computadoras que existe actualmente y que se extiende por todo el mundo, la cual nos provee de varios recursos que nos han venido a facilitar la vida y el trabajo.

La mayoría de nosotros hemos utilizado el Internet para diferentes objetivos, ya sea para obtener información de cualquier tipo, enviar correos electrónicos, para comunicarnos con familiares y amigos, obtener imágenes, comunicación por audio y video, así como diferentes utilidades que nos brinda la red. Por lo que consideramos que es muy importante para todas aquellas personas que se quieran dedicar a la implementación y administración de redes, tener conocimientos sólidos que puedan garantizar la funcionalidad de la misma.

La productividad es un elemento importante para toda empresa, explotar todos los recursos al máximo para obtener un mayor beneficio es sin duda el objetivo primordial. Las redes vienen a incrementar la productividad y sacar el máximo provecho de los recursos que ofrecen.

Sin duda, las redes son muy importantes para cualquier empresa, por lo que el desarrollo de nuevas formas de comunicación es parte del futuro. Es de vital importancia conocer aspectos teóricos y técnicos que hacen posible que las redes funcionen, ya que sólo así podemos solucionar problemas de una manera profesional y certera. Por lo que vale la pena abarcar el tema de "*Implementación de redes inalámbricas empresariales*", esperando que sea de utilidad para aquellas personas que lleguen a tener este material en sus manos.

Nuestra intención es aportar los conocimientos aprendidos durante la carrera así como la experiencia profesional obtenida hasta el momento, abarcando una problemática particular y aplicando un método resolutivo que nos ayude a solucionarla. Sabemos que este material será de gran ayuda para futuras generaciones.

TESIS CON
FALLA DE ORIGEN

INTRODUCCIÓN

La tecnología inalámbrica ha tomado gran importancia en los últimos años, diariamente nuevos productos aparecen en el mercado ofreciendo nuevas opciones donde el cable no puede llegar. Los módems inalámbricos, ruteadores inalámbricos, puntos de acceso y wireless, son un ejemplo de las opciones que podemos contemplar, dependiendo de nuestras necesidades.

Es muy fácil poder utilizar y configurar dispositivos inalámbricos. Que nuestra computadora forme parte de una red, ya no es tan complicado, podemos realizar nuevas redes caseras únicamente adquiriendo las tarjetas que nos permitan comunicarnos con los otros equipos con los que contamos. No necesitamos invertir en una infraestructura cableada que nos genere un gran gasto de instalación, ni tampoco romper con un buen ambiente estético del hogar u oficina.

La explotación de recursos informáticos es primordial para toda organización, el poder obtener información y acceder a recursos que nos ofrecen las redes, es de vital importancia en estos tiempos de globalización.

Sin duda uno de los retos a futuro de las redes inalámbricas será el de comunicarnos donde quiera que nos encontremos, ofreciéndonos el nivel de movilidad más alto.

Es importante mencionar que las redes inalámbricas, son un concepto relativamente nuevo, por lo que es necesario contar con técnicos e ingenieros especializados, que conozcan del tema que sean capaces de montar redes seguras y funcionales. Sabemos que últimamente los sistemas operativos se han vuelto muy amigables al igual que el concepto de Wireless, cualquier persona con conocimientos básicos en computación, puede instalar un controlador e incluso una tarjeta inalámbrica. El problema surge, en que no siempre se hace de forma adecuada y que no se utilizan los niveles de seguridad.

Por este motivo es fundamental conocer del tema, convirtiéndose en el objetivo de la tesis, el dotarnos de conocimientos y técnicas que nos ayuden a montar una red empresarial inalámbrica. El presente trabajo está dividido en 5 capítulos los cuales nos llevarán de la mano para obtener las bases y conocimientos necesarios para solucionar una problemática particular, así mismo justificar cada uno de los capítulos que la conforman.

El primer capítulo se titula “ Redes inalámbricas” en el cual definimos lo que es una red, ¿cómo funciona?, mencionamos las principales clasificaciones que existen. Se abarcan temas básicos sobre redes inalámbricas, contemplando sus ventajas y desventajas, mencionamos las nuevas clasificaciones de topología lógica que se utilizan para WLAN y sus diferencias, además de contemplar algunas configuraciones importantes que no existían en las redes puramente cableadas. Buscamos principalmente que el lector se vaya involucrando con el tema.

El segundo capítulo es sobre “El modelo OSI”, el cual es parte fundamental para el diseño, implementación y mantenimiento de redes de todo tipo. Sabemos que el modelo es complicado de abarcar, pero buscamos presentarlo de una manera sencilla, explicando cada una de las 7 etapas que lo conforman y haciendo hincapié en las capas que se ven modificadas cuando de redes inalámbricas hablamos.

El tercer capítulo es sobre “Tecnologías de redes LAN y WLAN”. Definimos algunas tecnologías que han aparecido a lo largo de los años referente a las redes de área local y que han adquirido una gran importancia. Se verán más definidamente lo que son las tecnologías inalámbricas y cada una de las normas donde se apoyan, realizándose una comparación entre cada una de ellas, para saber en que casos nos conviene más una que otra. Terminaremos abarcando bluetooth, como tecnología complementaria a WLAN, dedicada a dispositivos con niveles de transferencia de datos inferiores.

El cuarto capítulo trata sobre “Conformación y planeación de una red” abarcaremos los elementos generales que conforman una red, dentro de ellos veremos aspectos teóricos y técnicos que nos serán de gran ayuda para entender su funcionamiento.

Una vez entendido su funcionamiento y los elementos, el paso siguiente es planear una red empresarial, para ello buscaremos todos los elementos que debemos de considerar para montar una red exitosamente, aplicando una guía de procedimiento que nos ayude a considerar el mayor número de variables que pueden surgir durante el proyecto, para así poder realizar una correcta planeación y un buen diseño.

Y en el último capítulo titulado “Implementación de una red WLAN empresarial” retomaremos todos los conocimientos generados hasta el momento para poder aplicarlos en una empresa en particular. Se atiende una propuesta de un montaje de red de la empresa Isatem de México S.A., explicaremos cada una de las etapas que debemos de seguir para llevar a cabo este proyecto apoyándonos en nuestro criterio y experiencia profesional, para que así podamos construir una red WLAN segura y funcional, que aproveche los recursos al máximo.

Sin duda el último capítulo, es la prueba de fuego para todo lo antes dicho, es muy importante decir que los casos varían y que son muy particulares entre sí, ya que cada uno de ellos es único, por lo que se recomienda hacer un diseño para cada caso. Hay aspectos que no se ven modificados de una experiencia a otra, el secreto está en detectar que podemos aplicar y que no. Sabiendo eso podemos ahorrarnos tiempo en los nuevos proyectos.

Ahora bien, es momento de comenzar con los capítulos esperando que sean de utilidad para todos aquellos interesados en el funcionamiento de redes inalámbricas y su implementación.

Capítulo 1. Redes Inalámbricas

Las redes sin duda han venido a revolucionar la manera en que se comparte la información, a quien de nosotros no le ha pasado, que el compañero de la escuela o del trabajo nos entrega un disquete con una información importante, llegamos a nuestro hogar, insertamos el disco y nos encontramos que el disquete se dañó en el transcurso del viaje, por lo que no podemos ver dicha información. Afortunadamente las cosas han cambiado, basta con llamarle por teléfono y decirle que nos envíe la información a nuestro correo electrónico, nos conectamos a Internet y la recibimos en nuestro buzón.

El caso anterior es un ejemplo simple de cómo las redes han facilitado el acceso a la información. Empecemos el capítulo definiendo lo ¿Qué es una red? y ¿Cómo funciona?, para tener así un concepto general y poderlo aplicar en el aspecto inalámbrico.

1.1 ¿Qué es un red?

Una red es una manera de conectar varias computadoras entre sí, para que exista una comunicación que comparta información y recursos. Cabe aclarar que no solamente se pueden conectar computadoras, se puede poner toda clase de dispositivos que se quieran compartir, un ejemplo de ello son impresoras, máquinas industriales, elementos de medición y de control.

Podemos encontrar redes homogéneas como lo es la red de telefonía local o una red de oficina, donde interactúan dispositivos del mismo tipo. Pero lo cierto es que en la actualidad las redes se están convirtiendo en heterogéneas, es decir que podemos involucrar diferentes dispositivos o mecanismos a una red, no sólo equipo de cómputo, ahora nos podemos enlazar con teléfonos móviles, agendas electrónicas, manejar máquinas industriales, movimientos de cajeros bancarios, utilizar robots e instrumentos científicos de monitoreo, entre otros.

1.1.1 ¿Cómo funciona?

Ahora bien, sabemos que el objetivo de una red es compartir información, pero es muy importante mencionar las técnicas que se utilizan para que exista una comunicación entre nodos o equipos.

La técnica más importante es la conmutación, no importa si es una red inalámbrica o alámbrica, se trata de regular el flujo de información y comunicar a cada una de las estaciones de trabajo.

Si hablamos de una red cableada, es fundamental la conmutación entre nodos, ya que en caso contrario la forma en que se enlazarían los mismos, sería de la siguiente manera:

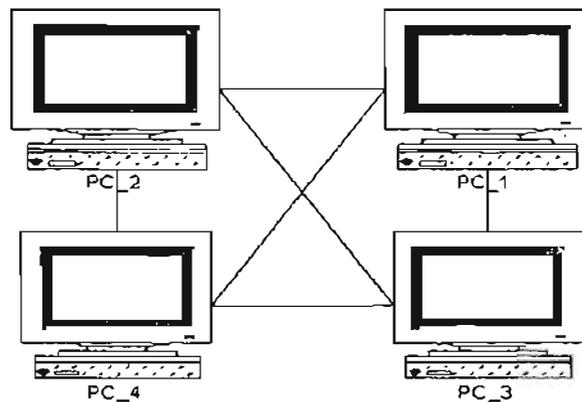


Fig.1,1 Conexión sin conmutación.

El número de conexiones representadas en la figura 1,1 está dado por $n(n-1)/2$, es decir, que cada uno de los dispositivos debe tener una conexión con todos los nodos. Podemos predecir que entre mayor número de nodos, mayor será las conexiones cableadas que debemos montar, por lo que no es nada práctico utilizar este tipo de enlace. Sin embargo, si hablamos de redes inalámbricas la idea no es tan descabellada, debido a que no utilizamos cables y nos ahorramos los enredos, podemos comunicarnos directamente con cada uno de los nodos sin necesidad de intermediarios.

Veamos algunos tipos de conmutación que se utilizan para realizar los enlaces entre nodos:

Conmutación de circuitos. Es un tipo de comunicación en la cual se establece un camino dedicado entre dos estaciones. Después de que se termina una sesión el canal es liberado para poder ser utilizado por otros usuarios¹. Un ejemplo típico de ello es la telefonía tradicional, en la cual no podemos tener una conversación con más de dos usuarios al mismo tiempo. Por último, es necesario agregar que el que realiza la llamada es el que determina el destino. En el siguiente diagrama se muestra la conmutación de circuitos donde las líneas remarcadas muestran el canal dedicado:

¹ <http://www.eveliux.com/telecom/cpswitching.html>

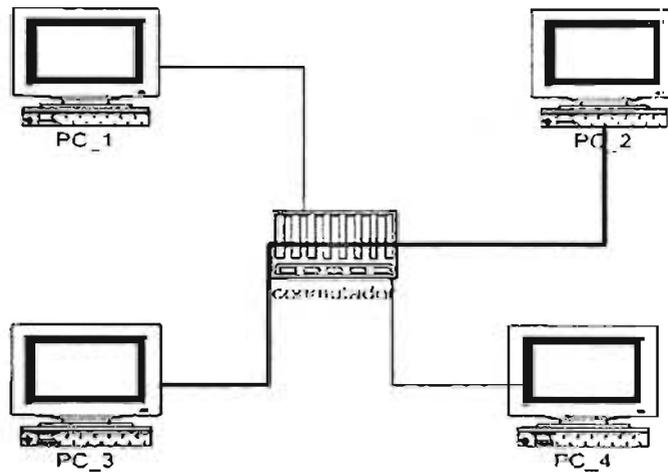


Fig. 1,3 Conmutación de circuitos.

Conmutación de mensajes. Este método de comunicación transmite un mensaje de un nodo a otro, donde es almacenado y verificado, libera el tramo anterior para que pueda ser utilizado por otro mensaje. Para poder pasar al siguiente nodo tiene que esperar que esté libre para poder transmitir la información y así sucesivamente hasta llegar al destino. Es importante tener en cuenta que el mensaje debe de tener la dirección del origen y del destino, ya que de lo contrario se perdería.²

Una de las ventajas de la conmutación mensajes es que en términos de recursos de línea ó disponibilidad de red, resulta menos costosa, sin embargo los retrasos de tiempo llegan a ser más grandes al igual que la memoria temporal que se necesita para almacenar los mensajes.

En el siguiente diagrama podemos ver un ejemplo de este tipo de conmutación, en donde se muestra uno de los posibles caminos que puede tomar un mensaje del origen al destino.

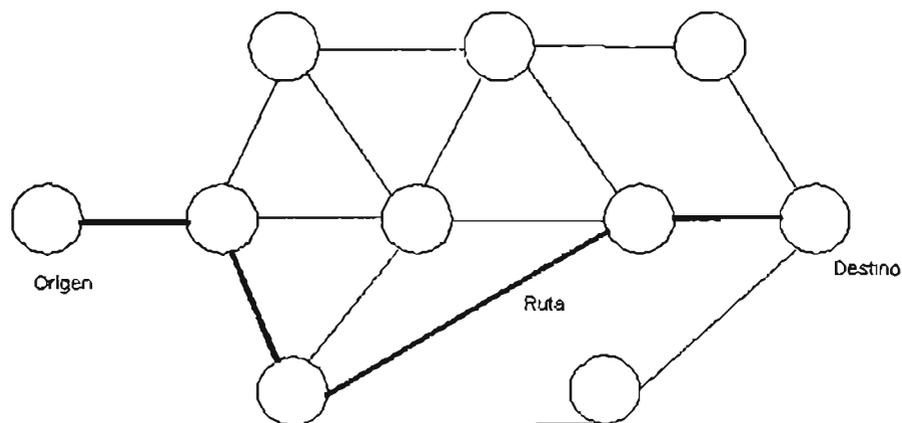


Fig.1,4 Conmutación de mensajes.

² Sograft, *Redes LAN*, CD-ROM Guía Intervisual, México, 2004.

Conmutación de paquetes. Esta forma de transmitir los datos, se ha convertido en un estándar cuando se trata de conectar computadoras, no importa si los datos llegan de forma alámbrica o inalámbrica. La información que se va a enviar se fragmenta en pequeños paquetes que son transmitidos de forma individual del origen al destino. Este método es muy parecido al anterior, sólo que los paquetes son más pequeños, por ello no se necesita una gran cantidad memoria temporal y el tráfico de red es más fluido.³

Es importante tener en cuenta que el paquete debe de tener la siguiente información para poder llegar a su destino y desfragmentar el mensaje original:

- Dirección del destino.
- Número de paquete.
- Información para detectar posibles errores.

Una de las ventajas de esta técnica es que requiere de menos capacidad de almacenamiento intermedio entre los nodos y el tiempo de transmisión es menor, los recursos de transmisión se aprovechan mejor.

1.2 Clasificación de redes

Las redes de computadora suelen tener varias clasificaciones, entre las más importantes que podemos mencionar se encuentran las que se especifican por su área geográfica, topología y el tipo de conexión.

1.2.1 Redes de conexión alámbrica

Las redes alámbricas son aquellas que utilizan un medio físico para comunicarse con los demás miembros de la red. Entre los principales medios físicos de comunicación, tenemos los siguientes:

Par Trenzado. Este medio físico de comunicación conocido como UTP (Unshielded Twisted Pair) es utilizado tanto para la transmisión de señales analógicas como para la transmisión de señales digitales, es muy similar al cable telefónico que usualmente conocemos. Es quizá el medio alámbrico de transmisión más utilizado ya que es de bajo costo y su instalación es rápida y fácil. El cable está compuesto por alambres de cobre revestidos cada uno con plástico utilizado como aislante, asimismo los alambres se agrupan en pares dentro de un tubo de plástico que los protege. El nombre de par trenzado viene precisamente porque los pares

³ loc. cit.

que se forman están trenzados, esto con el fin de protegerlos de la diafonía, que es la señal inducida por conductores eléctricos cercanos.⁴

Cable coaxial. El cable coaxial es otro de los medios de transmisión más conocidos en el terreno de las telecomunicaciones. Es un conductor eléctrico en forma de tubo que contiene un segundo conductor en el centro. El conductor externo es una malla, envuelta en una capa plástica que lo protege. La malla está tejida alrededor del hilo conductor interno el cual también está separado por una capa aislante.⁵

La estructura del cable tiene dos efectos sobre la transmisión. Por una parte, se elimina totalmente la diafonía o probabilidad de que intervengan otras señales electromagnéticas. Por otro lado, se aumenta en forma considerable el ancho de banda, lo que permite transmitir un buen volumen de información.

Fibra Óptica. La fibra óptica está compuesta por una fibra de vidrio flexible y ligera en forma de hilo entre 5 y 80 micras por el que viaja un rayo de luz. Un diodo o láser es el encargado de transmitir la luz a través de la fibra. Al llegar a su destino, un fototransistor convierte nuevamente el haz de luz en señales útiles.

Una de las ventajas de la fibra óptica es que es inmune a las interferencias electromagnéticas, ya que no existe posibilidad de diafonía debido a que los rayos de luz no son afectados, así mismo proporciona un gran ancho de banda y su baja atenuación permite distancias mayores entre repetidores.

1.2.2 Redes de conexión inalámbricas

Las redes inalámbricas no utilizan un medio físico de conexión que una a las máquinas de extremo a extremo, el aire se convierte en el medio de transporte de las ondas de radio, micro ondas y enlaces satelitales, existe otra tecnología alternativa de corto alcance, que utiliza infrarrojos, la cual veremos también a continuación:

Enlaces de radio. Los enlaces de radio generalmente tienen un alcance limitado debido a los límites de disponibilidad de frecuencias para transmitir en cierta zona, ocasionalmente llegan a ocurrir interferencias. Estas ondas de radio son omnidireccionales, esto es que se propagan en todas direcciones. Sin embargo, cuando se transmite de forma adecuada, los enlaces de radio son muy útiles en aplicaciones de redes inalámbricas de área local.⁶

Micro-ondas. La micro-onda es una señal de radio de muy alta frecuencia, pero tiene la particularidad de viajar en línea recta. Para la transmisión se utilizan

⁴ <http://www.saulo.net/pub/redes/>

⁵ *loc. cit.*

⁶ *loc. cit.*

antenas parabólicas, tanto la antena emisor como la antena receptor deben estar alineadas cuidadosamente para el correcto funcionamiento de la red, aproximadamente la distancia entre repetidores no debe exceder de unos 80 kms.⁷

Las principales ventajas que tiene un enlace de micro-ondas son:

- Los enlaces son inmunes a interferencias de otras transmisiones radiales.
- Se obtiene una gran calidad a grandes distancias.

Las principales desventajas son las siguientes:

- Son afectadas por fenómenos ambientales que deterioran la calidad de la señal, como la lluvia que causa atenuación debido a que la longitud de onda de la micro-ondas es similar a las gotas de lluvia, por lo que estas absorben la energía de la señal.
- Hay desviación de señal (deflexión) debido a los cambios atmosféricos como presión, temperatura y humedad.
- También está lo que se le conoce como propagación múltiple que es cuando un cuerpo interfiere en la señal principal y ésta es rebotada.

Infrarrojos. Los infrarrojos son ondas direccionales de corta distancia Esta tecnología inalámbrica es muy utilizada en redes de área local, en computadoras portátiles resultan una buena opción, aunque la velocidad puede ser inferior que si se utilizará una red de par trenzado. La señal que se utiliza normalmente tiene una longitud de onda de 870 nm y permite la transmisión de datos entre 4 y 16 Mbps a distancias de hasta 24 metros, siempre y cuando exista una línea de vista entre las estaciones, ya que las ondas son incapaces de atravesar paredes, bloqueándose la transmisión.⁸

Satélites. Como su nombre lo dice, este tipo de comunicación utiliza como recurso principal los satélites que giran alrededor de la tierra, dichos satélites funcionarán como los enlaces para que se lleve a cabo la transmisión. Para establecer un enlace, una estación debe transmitir una señal hasta el satélite y éste se encargará de transmitirla de regreso a la tierra. El costo del uso de satélites dependerá de las necesidades que se requieran en la comunicación; si se requiere difundir la información a varias estaciones, si se requiere comunicación a diferentes distancias etc.⁹

⁷ *loc. cit.*

⁸ Rosenbluet Arturo, *Introducción a la tecnología de redes*, México, 2000, p.20

⁹ *loc. cit. p.21*

1.2.3 Distribución geográfica

Dentro de la clasificación de distribución geográfica tenemos tres tipos de redes que describimos a continuación:

Las redes LAN. Son el tipo de red que la mayoría de gente conoce, vienen de las siglas en inglés (Local Area Network) es decir, redes de trabajo de área local, las cuales abarcan áreas relativamente pequeñas, con esto queremos decir que cubren áreas menores a un kilómetro, aunque actualmente la distancia ya no suele ser un parámetro a evaluar, se entiende que son redes que generalmente se instalan en oficinas, en edificios o campus, incluso en nuestro hogar, en donde el medio de comunicación está dedicado 100% a la transmisión de la información dentro de la organización, independientemente de la distancia o cobertura de la red. Las redes LAN contienen uno o más servidores que se conectan con otros dispositivos; estaciones de trabajo, impresoras, módems y que a su vez interactúan con un sistema operativo. En lo que respecta a la velocidad son redes muy rápidas, generalmente el rango de velocidad está dado en 10 Mbps en instalaciones viejas, 100 Mbps en la mayoría de organizaciones y 1 Gbps en corporativos de vanguardia.

Una red MAN (Metropolitan Area Network, Redes de Área Metropolitana). Pueden ser una extensión de una red LAN, o puede ser una conexión de varias redes LAN por lo que utiliza una tecnología muy similar que la última. Estas son redes geográficamente más grandes, como una ciudad o dos poblaciones cercanas.

Redes WAN (Wide Area Network, Redes de área extensa). Son redes establecidas en una extensa área geográfica, son redes punto a punto que interconectan ciudades, países y continentes. Contienen una mayor cantidad de información que una LAN o MAN, aunque la velocidad de transmisión suele ser menor.

1.2.4 Topología Física

Según su topología, las redes cableadas se pueden clasificar en Estrella, Anillo, Bus e Híbridas. Por topología se entenderá, como la forma física en que se conectan los elementos que integran la red, principalmente las computadoras y los nodos de la red.

Estrella. En este tipo de conexión existe un nodo central principal, al cual se conectan los equipos ó computadoras en forma de radio. El nodo central será el elemento que administre y organice la información, toda la red dependerá del correcto funcionamiento de este nodo, por lo que tiene que ser el elemento más seguro. Su principal ventaja es que permite desconectar fácilmente a un equipo que

falla, asimismo se pueden aumentar el número de equipos sin que se afecte el funcionamiento de la red.¹⁰

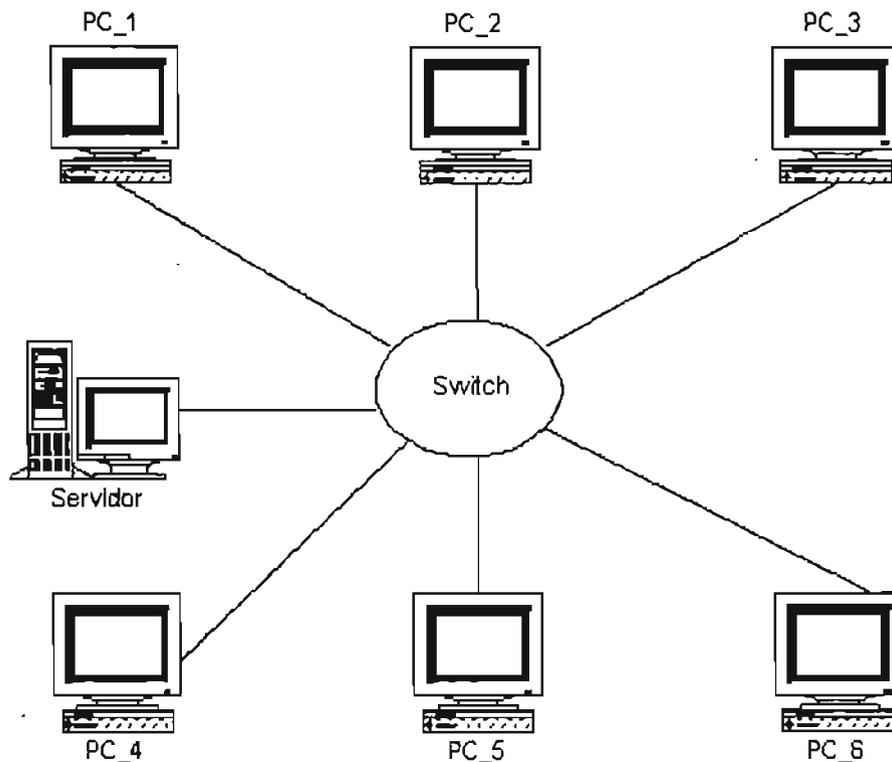


Fig. 1,5 Red en estrella.

Bus. En esta topología todos los nodos que componen la red están unidos linealmente por un Bus o cable. Cada estación está conectada en un mismo canal de comunicación donde circula toda la información en forma bidireccional, sólo existe un enlace, pero cada estación tomará la información que le corresponda o que le sea dirigida. En este tipo de conexión hay que tener cuidado con el cableado principal, ya que si fallara ocasionaría que el sistema dejará de funcionar por completo, por otro lado si un equipo se avería, el funcionamiento del resto de la red no se ve afectado. Añadir nuevas terminales supone detener por tramos la actividad de la red, pero suele ser rápido y sencillo.

La red en Bus necesita incluir en ambos extremos, terminadores, que son dispositivos que controlaran los rebotes de señal que puedan surgir en el canal.¹¹

¹⁰ http://www.htmlweb.net/redes/topologia/topologia_2.html

¹¹ *op. cit.*

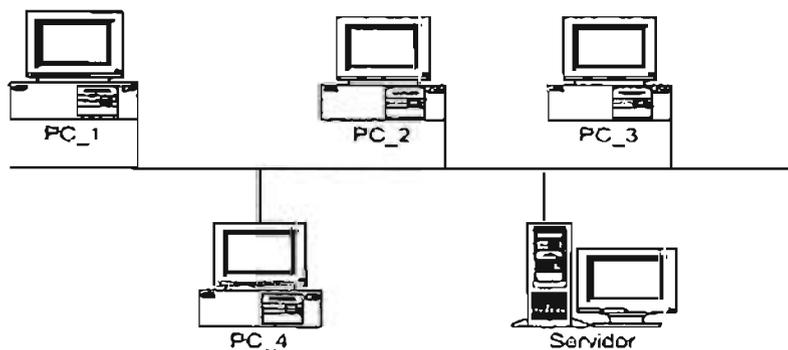


Fig.1,6 Red en bus.

Anillo. Esta topología como su nombre lo indica está formada por una red en forma de un anillo, cada estación se conecta en forma serial una tras otra, hasta que finalmente la última estación se conecta a la primera. La información se transfiere en un sólo sentido de un nodo a otro a través del anillo hasta alcanzar destino. Los nodos participan por igual, de manera que la carga de trabajo se distribuye equitativamente.

En esta topología de anillo resulta más complicado hacer cambios que en una red bus o estrella. Cuando se agrega o quita un nodo del anillo queda dividido temporalmente deteniendo el flujo de datos. Los nodos que fallan obstaculizan la comunicación, por lo que deben ser puenteados y separados.¹²

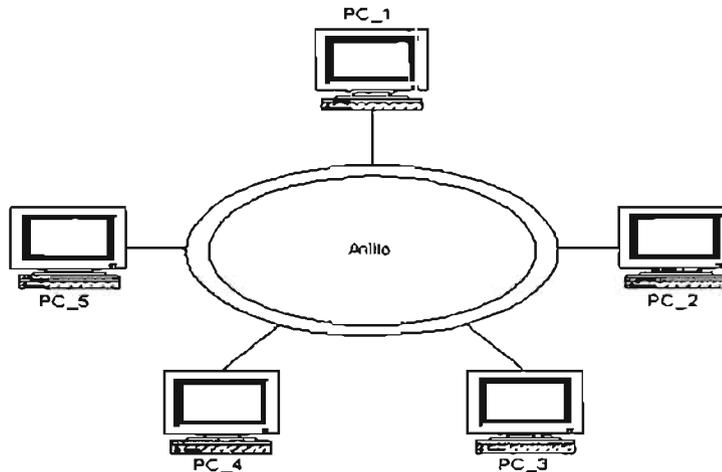


Fig.1,7 Red en anillo.

Híbridas. Por último, mencionaremos las redes híbridas, las cuales están compuestas por una combinación de las topologías anteriores. Un ejemplo de ello, es la red tipo árbol, la cual se compone de dos o más redes en estrella.

¹² *op.cit.*

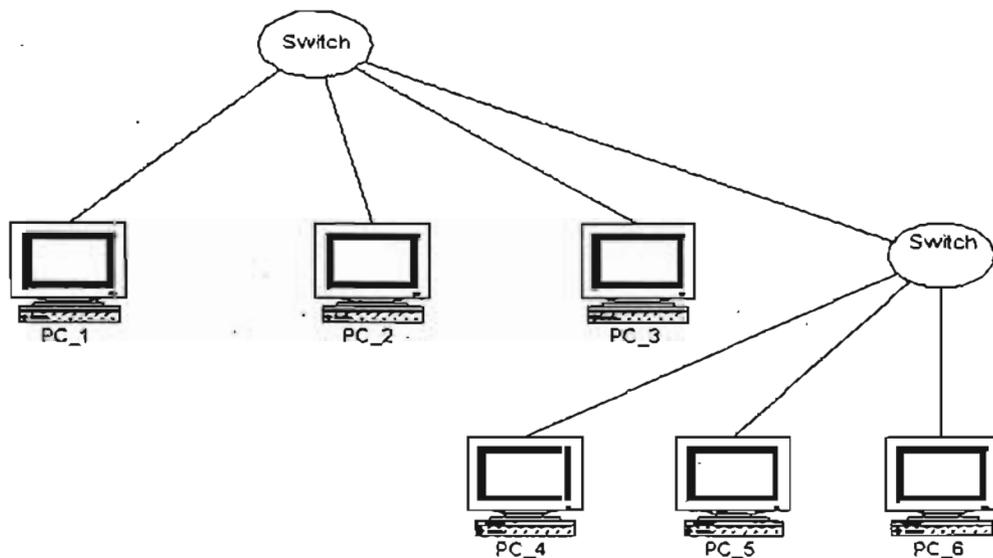


Fig.1,8 Red en árbol.

1.3 Redes WLAN

Las redes WLAN, tienen el mismo objetivo que las redes LAN convencionales, el cual es compartir información y recursos dentro de una empresa u organización. Sin embargo, la diferencia se encuentra cuando la comparamos una con otra, es decir, que se busca rebasar las limitaciones del cable, para dar origen a una nueva tecnología de comunicación que cumpla con las necesidades de las empresas.

Las redes WLAN, son un sistema de comunicación que transmite y recibe datos utilizando ondas electromagnéticas, proporciona una conectividad inalámbrica de igual a igual entre los distintos nodos de red, por lo que es una alternativa muy flexible que les permite a los usuarios una movilidad que con el cable no existía.

Es claro que las empresas han encontrado en las redes una solución a sus necesidades administrativas, el crecimiento de las redes en los últimos años ha sido muy grande. Podemos predecir que las redes inalámbricas serán una solución viable en la creación de nuevas redes de cómputo.

Abarquemos algunas de las ventajas principales que encontraremos al usar las redes WLAN.

Movilidad. Los usuarios que formen parte de la red, podrán moverse de lugar sin complicaciones. Esto favorece a todos aquellos que tengan máquinas portátiles, ya que podrán estar en la sala de juntas, en el comedor e incluso en el baño, si su trabajo es mucho. Por lo que se genera una mayor productividad y comodidad.

Facilidad de instalación. La instalación es muy fácil evitando realizar perforaciones en muebles, paredes y techos, con lo que el daño a las instalaciones es mínimo. Es ideal para aquellas empresas que se encuentran en lugares rentados y no quieren invertir en una infraestructura cableada que sólo podrán utilizar en ese lugar.

Creación de redes temporales. Con el uso de dispositivos inalámbricos, se pueden crear redes temporales de una forma rápida y sencilla, ideal para eventos y proyectos temporales.

Expansión de redes. Con las redes inalámbricas, podemos extender una red existente y llegar a lugares poco accesibles para el cable.

Costo de instalación bajo. Debido a que no requieren de una gran infraestructura cableada, el costo de instalación es mínimo.

Analicemos ahora sus desventajas:

Costo alto de dispositivos Inalámbricos. Las tarjetas inalámbricas son más caras. Sin embargo, el costo total se hace más flexible debido a que su instalación es más barata.

Cobertura limitada. Los dispositivos inalámbricos nos brindan una cobertura pequeña no mayor a 200 metros, pero suficiente para crear una red WLAN.

Velocidad. La velocidad inalámbrica alcanzada hasta el momento es aproximadamente la mitad que ofrece un cable UTP de categoría 5, que transmite datos a 100 Mbps.

Seguridad. Se debe tener mucho cuidado cuando se utilizan tarjetas inalámbricas, ya que las ondas electromagnéticas llegan más allá de las paredes que delimitan a la empresa. Sin son instaladas sin un sistema de encriptación, la información puede llegar a personas ajenas, que le pueden dar mal uso a la información.

1.4 Topología de redes WLAN

Las redes LAN inalámbricas han dejado de tener una clasificación dentro de las topologías físicas, debido a que los equipos pueden estar acomodados aleatoriamente, sin que esto intervenga en su funcionamiento, ya no es relevante clasificar a los equipos en estrella, anillo o lineal. La topología lógica se sigue aplicando en las redes WLAN, básicamente son dos tipos las que se utilizan, en estrella y en malla. La topología en estrella utiliza un punto de acceso donde todos los equipos deberán de comunicarse, para acceder a la red. Veamos la siguiente figura:

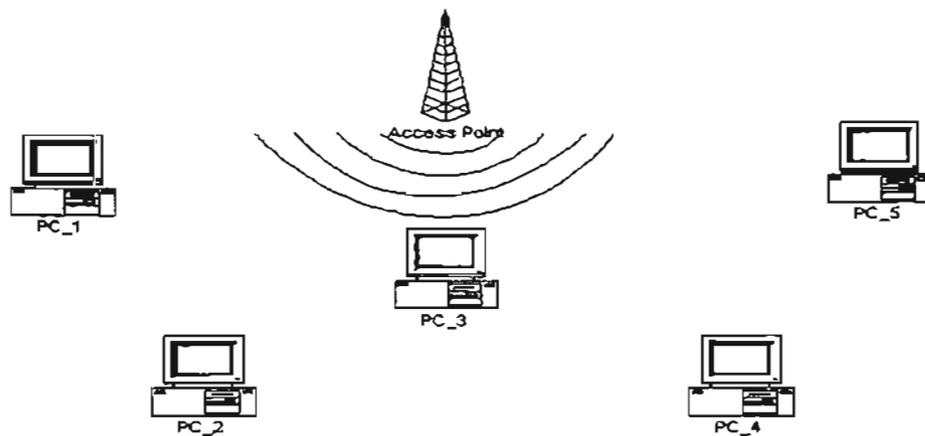


Fig. 1,9 Topología lógica en estrella.

Sin embargo, aunque se trata de una topología lógica en estrella el término ya no es utilizado, ahora es conocido como infraestructura, debido a que esta configuración sigue utilizando cableado para poder acceder a los recursos de red que no cuenten con tarjetas inalámbricas, como impresoras y computadoras que no cumplen con los requerimientos inalámbricos.

Una topología de infraestructura puede extender una red LAN con cable existente, para incorporar dispositivos inalámbricos mediante una estación base, denominada punto de acceso. El punto de acceso se encarga de unir la red LAN inalámbrica con la red LAN con cable, además de ser un controlador central, coordinando la transmisión y recepción de múltiples dispositivos inalámbricos dentro de una extensión específica; la extensión y el número de dispositivos dependen del estándar de conexión inalámbrica que utilice el fabricante. En la modalidad de infraestructura, puede haber varios puntos de acceso para poder abarcar una zona grande o un único punto de acceso si se trata de una zona pequeña. Es ideal para su uso en oficinas.¹³

¹³ <http://www.infinitum.d2g.com/index.html>

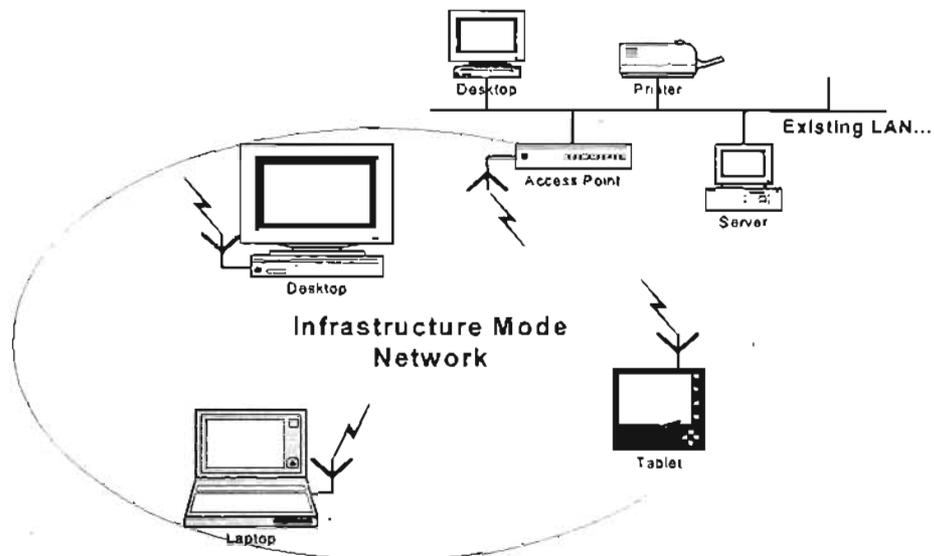


Fig. 1,10 Red de la modalidad de infraestructura.

La topología ad hoc viene a resucitar a la topología en malla, debido a que cada una de las máquinas se pueden comunicar con otras directamente, sin necesidad de intermediarios. Los propios dispositivos crean una red LAN y no existe un controlador central, ni un punto de acceso como en la anterior. Esta topología es la ideal para pequeños grupos que utilicen redes improvisadas o temporales, como una sala de juntas o el mismo hogar.¹⁴

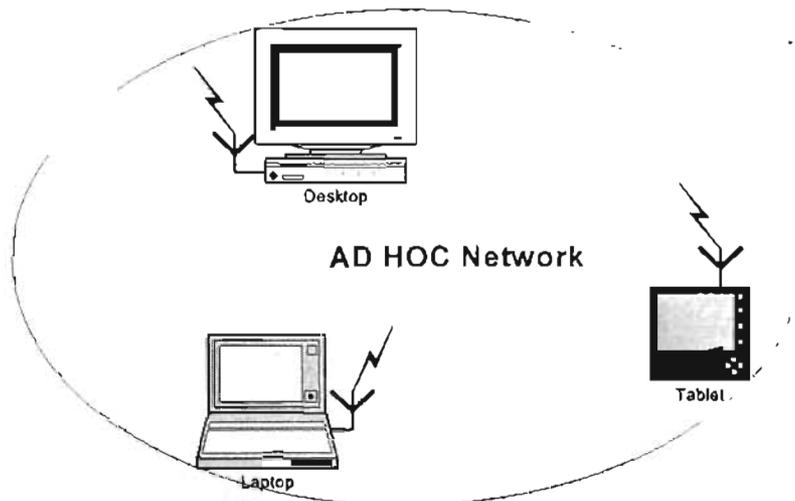


Fig. 1,11 Red ad hoc.

Combinando las nuevas generaciones de software y soluciones par a par inteligentes. Las redes inalámbricas ad hoc pueden permitir a los usuarios móviles,

¹⁴ op.cit

colaborar y participar en juegos de equipo muy interesante, transfiriendo archivos o comunicarse de algún otro modo mediante sus PC o dispositivos inteligentes sin cables.

1.5 Tecnología WLAN

La tecnología inalámbrica actual ha tenido grandes avances en los últimos años, además los costos se han vuelto más accesibles permitiendo que este tipo de red llegue casi a cualquier entorno, como el hogar, pequeñas y medianas empresas, grandes industrias, instalaciones de uso temporal o construcciones donde no se permite el cableado. Por lo que no dudamos que en un futuro cercano, las redes inalámbricas desplacen completamente a las redes cableadas.

Las redes inalámbricas han alcanzado un gran desarrollo en lo que respecta a la tecnología de radio frecuencia conocida como WiFi, que se encuentra regulada por IEEE y tiene como referencia la norma 802.11. Al mismo tiempo varias empresas del mundo han creado una alianza para certificar a los productos que salen al mercado, garantizado así una interoperabilidad entre los distintos fabricantes.

Más adelante, en el capítulo 3, abarcaremos detalladamente los distintos apartados de la norma 802.11, primero que nada definamos algunos conceptos importantes de debemos de conocer sobre la tecnología WLAN.

1.5.1 Dispositivos de comunicación inalámbrica

Punto de acceso (Access Point): Es un dispositivo que nos permite centralizar la comunicación inalámbrica, conectando a los diferentes equipos como lo haría un hub de una red cableada, encargándose de repartir los paquetes de información y haciéndolos llegar a su destino. Otra de las funciones importantes es que da conectividad a una red cableada, haciendo que los equipos inalámbricos se enlacen con los equipos cableados, como miembros de una sola red.

Tarjetas WIFI o Wireless. Estas tarjetas nos permiten comunicarnos con el punto de acceso y con otras tarjetas, utilizando una interfase de red, la cual es capaz de enviar y recibir datos por medio de radio frecuencia. Tiene el mismo fin de una tarjeta de enlace de una red cableada. Existen en el mercado varios formatos, como el PCMCIA que se utiliza en portátiles, PCI en computadoras personales y USB que se usa en ambos casos. Aunque actualmente los productos portátiles son lanzados al mercado con wireless integrados.

Conmutadores Wireless. Al igual que en las redes LAN, también existen conmutadores de red para wireless, encargándose de monitorizar las ondas de radio midiendo el rendimiento en tiempo real y reajustando las potencias de emisión, cuentan con un software donde nos permite situar los puntos de acceso

tomando en cuenta el grosor y el tipo de material que se utiliza para dividir las oficinas y cubículos.

Antenas. Los Dispositivos inalámbricos deben de contar con una antena receptora-transmisora que nos servirá para poder establecer un enlace de comunicación, recordemos que las tarjetas wireless utilizan ondas de radio que viajan omnidireccionalmente y deben de ser capturadas por las antenas, dependiendo de la distancia que se requiera cubrir se obtendrá la altura de la antena.

1.5.2 Mecanismos de seguridad y configuración de las WLAN

Otros conceptos importantes que debemos conocer en las tarjetas Wifi, son los de seguridad y de configuración. Los más importantes son los siguientes:

1.5.2.1 Opciones de seguridad

Se puede pensar que las WLAN son más inseguras que las redes alámbricas, ya que el medio físico para la transmisión de datos son las ondas electromagnéticas. Quizá es muy fácil que un hacker detecte una red inalámbrica, mas no le es tan fácil entrar a dicha red. Actualmente los modos de encriptación que se utilizan para una inalámbrica son los siguientes:

WEP (Wired Equivalent Privacy, Privacidad equivalente a cable). Wep provee de seguridad, encriptando los datos que viajan sobre la ondas radioelectricas en las dos capas más bajas del modelo OSI (capa física y capa de enlace), como veremos en el siguiente capítulo.

La encriptación se puede ajustar a 64 bits, ó a 128 bits, obviamente entre mayor número de bits, mayor seguridad. Debemos de tener en cuenta que todas las estaciones de trabajo que necesiten comunicarse deben de utilizar la misma clave para poder cerrar la llave de encriptación. Actualmente ya hay niveles de encriptación de 152, 256 y hasta de 512 bits, que utilizan algunas Instituciones que requieren de una seguridad Máxima.

WPA (Wi-Fi Protected Access, Acceso de Protección Wi-Fi). WPA viene a ser el sustituto de WEP, ya que actualmente aunque todavía es funcional, se ha mostrado vulnerable. En WPA la cadena ASCII que se introduce es una clave que sirve de punto inicial para que se genere una clave en constante rotación, de forma que cada paquete de información lleva una clave completamente diferente a las anteriores. WPA necesita que todos los dispositivos sean compatibles con este sistema. Si uno de los adaptadores inalámbricos no está preparado, la red entera se encriptará utilizando el antiguo WEP.

1.5.2.2 Opciones de configuración

Modo PS (Power Saving): Esta opción nos permite ahorrar energía en la batería para cuando los equipos portátiles no utilicen la red.

Channel. Cuando un grupo de computadoras se conectan a través de radio, es necesario que utilicen un canal de comunicación, el cual debe ser el mismo para todos los miembros de la red. De la misma manera cuando se utiliza un punto de acceso, es recomendable configurar la tarjeta de red en modo automático, para que utilicen el canal del punto de acceso más cercano. Debemos de dejar claro que esta configuración dependerá del tamaño de red y de las instalaciones en particular, ya que se puede adecuar de un modo óptimo en el lugar de la implementación haciendo las pruebas correspondientes.

Tx Rate. El término se refiere a la velocidad de enlace, aunque se ajusta automáticamente se puede modificar manualmente. Es recomendable dejarla automática, ya que forzarla a niveles superiores no significa un aumento en la velocidad de la red. Dependiendo del fabricante y de los requerimientos se ajustara la velocidad de enlace.

En este primer capítulo, hemos visto los conceptos necesarios para conocer de forma general los dispositivos que involucran a una red Inalámbrica. Así mismo, mencionamos las topologías, seguridad, ventajas y desventajas que tiene el uso de esta tecnología en el manejo de recursos e información.

Capítulo 2. *El Modelo OSI y su aplicación inalámbrica.*

Ahora que ya tenemos una idea más clara de lo que son las redes de computadora y de algunos conceptos básicos vistos en el capítulo 1, nos podemos adentrar más en este interesante tema de la conexión de computadoras. Sin duda, el modelo OSI es uno de los pilares importantes en la creación de redes, pues en él se establecen los estándares de comunicación que hacen posible conectar equipos de distintos fabricantes.

Debemos de tener presente que el modelo OSI se creó mucho antes de que apareciera el concepto inalámbrico, pero debido a su estructura muy bien planeada nos sirve como referencia para el análisis de redes inalámbricas. Abarquemos algunos datos importantes que nos ayudaran a entender mejor la importancia de este modelo.

2.1 *¿Qué es el modelo OSI?*

El modelo OSI fue implementado por la Organización Internacional de Normas (ISO), que se ocupa de la elaboración de recomendaciones internacionales a partir de propuestas de los países miembros. La ISO está dividida en diferentes áreas y su objetivo es crear estándares y sobre todo la normalización, que tiene como función proteger a los usuarios o consumidores contra monopolios por parte de las compañías que fabrican un producto u ofrecen diferentes tipos de servicio.

La ISO define a un sistema informático como el conjunto de una o más computadoras, el software asociado, los periféricos, el medio de transmisión y en general todos los elementos necesarios para el manejo de información. De acuerdo a ISO, un sistema abierto es un sistema capaz de interconectarse con otros de acuerdo a ciertas normas establecidas, entonces se entenderá que OSI (Interconexión de sistemas abiertos) se ocupa del intercambio de información entre sistemas abiertos y cuyo objetivo es la definición de un conjunto de normas que permitan a dichos sistemas cooperar entre sí.¹⁵

2.2 *Capas del Modelo OSI*

El modelo OSI está dividido en 7 capas ó niveles ordenados jerárquicamente, los cuales son las siguientes:

¹⁵ Stallings, William. *Comunicaciones y redes de computadores*. Prentice Hall, México 2000, p 18.

- Nivel de aplicación
- Nivel de presentación
- Nivel de sesión
- Nivel de transporte
- Nivel de red
- Nivel de enlace de datos
- Nivel físico

Cada una de las capas debe realizar funciones específicas utilizando para ello únicamente los servicios de la capa inferior. Como sabemos, en toda red existe un emisor y un receptor, la comunicación se realiza entre dos terminales así que existirá un grupo equivalente de capas, 7 para cada una de ellas. Cada capa se comunicará con su capa similar en el extremo opuesto a través de reglas ó lo que es lo mismo a través de protocolos. En el modelo OSI queda definido que la comunicación entre capas sólo ocurra al mismo nivel, esto es el nivel 7 del emisor con el nivel 7 del receptor, el nivel 6 con el nivel 6 y así sucesivamente.

Llevemos este funcionamiento de comunicación a la vida cotidiana, imaginemos a una empresa que tiene distintos departamentos, tomemos dos de ellos como ejemplo. Digamos que el departamento de ventas, se quiere comunicar con el departamento de compras, ya que es necesario surtir un producto que se terminó. Como se trata de una empresa imaginaria, pongamos tres niveles a cada departamento y comuniquémoslo con el otro departamento para que se tome una decisión importante, que es la compra del producto. Tomemos como referencia la siguiente figura:

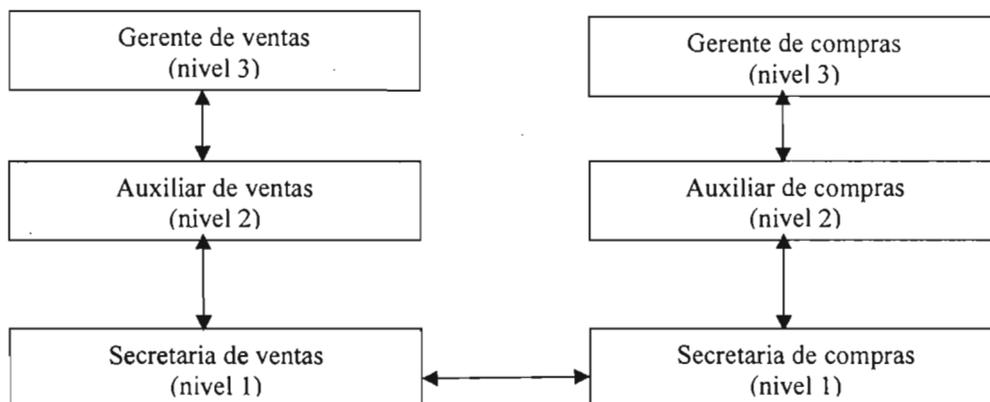


Figura 2,1. Niveles de una empresa imaginaria.

Como podemos ver, en la figura se ejemplifica un protocolo de comunicación de una determinada empresa. Retomando lo anterior, si queremos que el departamento de ventas se comunique con el departamento de compras para adquirir un producto, se haría de la siguiente manera:

- 1) El gerente de ventas da una orden a su auxiliar para que sea entregado un requerimiento al departamento de compras.
- 2) El auxiliar de ventas realiza el requerimiento y lo entrega a su secretaria.
- 3) La secretaria lo lleva al departamento de compras.
- 4) La secretaria de compras lo recibe y se lo pasa a su jefe.
- 5) El auxiliar de compras lo evalúa y se lo pasa a su jefe.
- 6) El Gerente de compras toma la decisión final y si procede, se realiza la orden de compra.

Nos damos cuenta que la información va pasando de nivel a nivel, hasta llegar a la persona adecuada que tiene el poder de tomar la decisión. Un ejemplo no valido sería, que la secretaria de ventas le diga al auxiliar de compras que falta un producto, pues rompe con el protocolo de comunicación, además de que es arriesgado tomar una decisión tan a la ligera. De igual manera, la secretaria no le interesa si la información que entregó es válida o no, sólo se preocupa por entregarla y se deja que el homologo de cada capa la interprete de acuerdo a su trabajo.

El siguiente cuadro muestra como se divide el modelo OSI en 7 niveles:

Emisor Receptor	Paquete	Receptor Emisor	nivel
Aplicación	C7 Datos	Aplicación	7
Presentación	C7 C6 Datos	Presentación	6
Sesión	C7 C6 C5 Datos	Sesión	5
Transporte.	C7 C6 C5 C4 Datos	Transporte.	4
Red	C7 C6 C5 C4 C3 Datos	Red	3
Enlace	C7 C6 C5 C4 C3 C2 Datos	Enlace	2
Físico	C7 C6 C5 C4 C3 C2 Datos	Físico	1

Fig. 2,2 Niveles del modelo OSI.

Ahora veamos como viaja la información a través de las distintas capas. Cuando se realiza una transmisión de información los datos fluyen desde las capas de mayor jerarquía hacia las de menor jerarquía y contrariamente cuando se realiza una recepción de información los datos viajan de las capas inferiores a las superiores. Por ejemplo, si en el emisor generamos información en el nivel de aplicación (7) ésta tendrá que descender por el resto de los niveles hasta llegar al nivel físico (1) y posteriormente llegará al nivel físico(1) del receptor, para de ahí

ascender hasta el nivel de aplicación (7). En la siguiente figura se muestra el flujo de información.

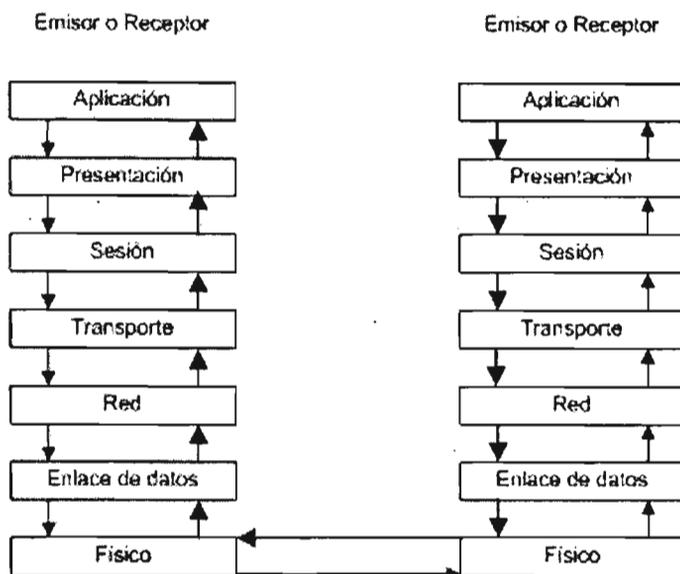


Fig. 2,3 Flujo de datos entre niveles.

Es importante recalcar que cada nivel es independiente y que cada uno de los mismos tiene que comunicarse únicamente con su nivel correspondiente, aunque tienen que atravesar por los niveles que se encuentran a su paso. Pero ¿Cómo saben los niveles que los datos son para ellos? pues muy fácil, en la emisión cada uno de los niveles va añadiendo a los datos a transmitir, la información de control relativa a su nivel o encabezados, de forma que los datos originales van siendo recubiertos por capas de control, en contraparte, en la recepción, según se vaya ascendiendo del nivel 1 al 7, se van dejando en cada nivel los datos añadidos por el nivel equivalente del lado de la emisión y así, hasta que quedan únicamente los datos que se querían transmitir desde una nivel específico.¹⁶

Los paquetes de datos suelen recibir nombres diferentes dependiendo del nivel de fragmentación que se tengan. En la capa física se habla de cadenas de bits, en la de enlace se habla de tramas; en la capa de red, paquetes o data gramas; en las capas de transporte se habla de segmentos. Aunque todos los términos se refieren a lo mismo, es importante tenerlos en cuenta.

El intercambio de información entre capas se realiza en términos de unidad de datos de protocolo (PDU's). Cada PDU ó paquete de información está compuesto de dos partes; por la información de control del protocolo (PCI) o encabezado y por la unidad de datos de servicio (SDU) que son servicios suministrados por las capas vecinas. Por ejemplo, la capa de enlace recibe un

¹⁶ Vallejos Soto, Antonio. *Sistemas microinformáticos y redes LAN*. Marcombo. México 1997, pp 248,249

servicio de la capa física, ya que envía las tramas de datos en secuencias de unos y ceros por un medio de transmisión, que puede ser un cable.

Analicemos ahora cada una de las capas que conforman el Modelo OSI para tener un concepto más detallado del mismo.

2.2.1 Capa de Aplicación

La capa de aplicación es la más cercana al usuario ya que está relacionada con las funciones de más alto nivel, proporcionando un soporte para las aplicaciones y actividades del sistema. Las aplicaciones no son otra cosa que los programas que utilizamos para desarrollar una actividad específica, una hoja de texto por poner un ejemplo. También se encarga de suministrar servicios de red a las aplicaciones, definiendo los protocolos utilizados por estas, un ejemplo de ello es el correo electrónico.

La capa de aplicación es el medio por el cual el usuario accede a la comunicación por red, mediante el entorno OSI, proporcionando los procedimientos precisos para ello. Los procesos de las aplicaciones se comunican entre sí por medio de entidades de aplicación propias, estando controladas por protocolos específicos de la capa de aplicación; que a su vez utiliza los servicios de la capa de presentación, que como podemos ver en la figura 2,3, se encuentra debajo de ella.

Es la única capa que no proporciona servicios a ninguna otra capa del modelo OSI, sólo a las aplicaciones que se encuentran fuera del modelo (procesadores de texto, hojas de calculo, navegadores, etc.)

Por último, la capa de aplicación establece la disponibilidad de diversos elementos que deben de participar en la comunicación, sincronizando las aplicaciones que cooperan entre sí y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.¹⁷

2.2.2 Capa de Presentación

La capa de presentación suministra servicios a la capa de aplicación, garantizando que la información enviada pueda ser entendida y utilizada por la capa de aplicación del receptor, estableciendo el argumento sintáctico del dialogo. La sintaxis se refiere al formato que los datos son transmitidos.

La tarea principal de este nivel es aislar a las capas inferiores de formatos de datos con los que trabajan las aplicaciones (ASCII), transformando estos formatos

¹⁷ <http://www.htmlweb.com>

particulares en un formato común para ser enviado por la red, de manera que los datos puedan ser entendidos correctamente de emisor a receptor.¹⁸

También es responsable de la obtención y liberación de la conexión de sesión cuando existen varias alternativas disponibles.

Para que la capa de presentación pueda cumplir con su función, debe realizar las siguientes operaciones:

- Traducir de entre varios formatos de datos a un formato en común, estableciendo las reglas de sintaxis de la información transmitida. Para ello, los datos son codificados de un formato local un estándar de red y viceversa.
- Definir la estructura que tienen los datos para ser transmitidos, estableciendo la información de control para la coordinación o semántica.
- Definir el código a usar para representar la cadena de caracteres y aplicar a los datos procesos criptográficos cuando sea necesario.
- Dar un formato a la información para poder visualizarla en pantalla o poder imprimirla.

2.2.3 Capa de sesión

La capa de sesión proporciona servicios a la capa de presentación, creando el medio necesario para que las capas de presentación, la del emisor y la del receptor se comuniquen entre sí, sincronizando el dialogo y el intercambio de datos¹⁹. Las principales funciones son:

- Iniciar y finalizar sesiones entre emisor y receptor.
- Administrar la sesión, si la comunicación falla por una causa ajena al usuario, restaurará la sesión desde un punto seguro, garantizando así que no exista alguna pérdida de datos. Pero si la comunicación no logra restablecerse, se deberá de terminar la sesión de una manera ordenada, recuperando todas sus funciones y evitando problemas en el sistema.
- Establecer las reglas o protocolos, para sincronizar el intercambio de datos entre capas de presentación homólogas.

¹⁸ *loc. cit.*

¹⁹ *op.cit*

- Lograr una transferencia de datos eficiente.
- Obtener un registro de problemas de sesión, al igual que de las capas de presentación y aplicación.
- Manejar tokens. Los tokens son muestras o señales que se utilizan para controlar o validar la comunicación entre los usuarios.
- Realizar checkpoints. Los cuales son puntos de recuerdo en la transferencia de datos que son necesarios para la recuperación de sesiones perdidas.

2.2.4 Capa de transporte

La capa de transporte proporciona servicios a la capa de sesión, realizando la transferencia de datos. Para ello, los datos son divididos en segmentos, que posteriormente son reensamblados en la capa homóloga del receptor.

Mientras que en las capas de aplicación, presentación y sesión están relacionadas con las aplicaciones del usuario o software, las cuatro capas inferiores restantes se encargan del transporte de datos.

La capa de transporte es la primera que se comunica directamente con su homóloga receptora, ya que la comunicación de los niveles anteriores es del tipo máquina a máquina.

El nivel de transporte, como su nombre lo indica, es el encargado de transportar los datos de una forma segura entre los distintos nodos de la red. Para ello, se establecen circuitos virtuales, que son encargados de proporcionar un servicio confiable mediante el uso de sistemas de detección y recuperación de errores.²⁰

Los circuitos virtuales son las conexiones que se establecen dentro de una red. Los paquetes de datos viajan por estas vías hasta llegar al nodo destino.

Las funciones principales son:

- Incluir controles de integración entre los usuarios de la red para prevenir pérdidas de datos o doble procesamiento de transmisiones.
- Controlar el flujo de las transacciones y el direccionamiento de los procesos de máquina a procesos de usuario.

²⁰ *op.cit*

- Asegurar que los datos se reciban completamente y en el orden adecuado, realizando un control de origen a destino.
- Aceptar los datos del nivel de sesión para fragmentarlos en unidades más pequeñas.
- Realizar funciones de control y numeración de los segmentos para su envío.
- Reensamblar los segmentos en el nodo destino.
- Garantizar la transferencia de información a través de la red.

2.2.5 Capa de red

Como hemos venido señalando la capa de red proporciona sus servicios a la capa de transporte, proporcionando una conectividad y seleccionando la mejor ruta para realizar la transmisión de datos. Es responsable de la conmutación y encaminamiento de la información, proporcionando los procedimientos adecuados para la transmisión de datos entre origen y destino.²¹

La capa de red debe de conocer la forma en que están conectadas las máquinas para determinar la ruta más adecuada para la transmisión de datos.

Las principales funciones son:

- Dividir los segmentos de la capa de transporte en unidades más complejas, denominadas paquetes, en los cuales son asignadas direcciones lógicas del receptor.
- Conocer la topología de la red, y manejar el caso donde las máquinas sean de distintas redes geográficamente distintas.
- Encaminar la información por la red tomando como referencia las direcciones del paquete.
- Aplicar los métodos de conmutación y enrutamiento para que los paquetes fluyan en los dispositivos intermedios.(routers)
- Enviar los paquetes de nodo a nodo usando los circuitos virtuales.
- Ensamblar los paquetes en el nodo destino.

²¹ *op.cit*

Los routers son dispositivos que se encargan de encaminar los paquetes de datos desde el origen hasta el nodo destino, buscando la mejor ruta para llevar a cabo la comunicación.

2.2.6 Capa de enlace de datos

La capa de enlace proporciona sus servicios a la capa de red, suministrando un tránsito de tramas de datos confiables por el enlace físico. Se ocupa del direccionamiento físico, del acceso a la topología de red, notificación de errores, la entrega ordenada de datos y el control de flujo.²²

La principal misión es hacer de la comunicación un medio libre de errores, para ello se realizan las siguientes funciones:

- Establecer los medios necesarios para una comunicación eficiente entre emisor y receptor
- Agregar una secuencia de bits al principio y al final de los paquetes de datos, controlando el flujo de datos en una trama, las cuales están formadas por cientos de bytes.
- Sincronizar el envío de tramas y los errores que puedan surgir. Los códigos cíclicos redundantes, son los encargados de enviar acuses de recibo para evitar la pérdida de datos y tramas repetidas.
- Regular la velocidad de tráfico de datos.
- Controlar el flujo de tramas equivocadas que pertenecen a otros usuarios mediante protocolos que sincronizan el envío y la recepción.
- Manejar el acceso de los datos al medio físico o inalámbrico.

2.2.7 Capa Física

Por último, la capa física proporciona sus servicios a la capa de enlace de datos, definiendo las especificaciones eléctricas y mecánicas para realizar la transmisión. También activa las funciones que administran el enlace físico entre sistemas finales, relacionando la agrupación de circuitos físicos o inalámbricos a través de los cuales los bits son transmitidos.²³

²² *op.cit*

²³ *op.cit*

La misión primordial de esta capa es transmitir los bits por un canal de comunicación, de manera que cuanto el emisor los envíe lleguen sin alteraciones al receptor.

Sus principales funciones las podemos resumir en:

- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión) que se van a usar en la transmisión de los datos por los medios físicos. En el caso de medios inalámbricos hay que definir, las frecuencias o los canales en que viajarán los datos.
- Transmitir el flujo de bits a través del medio.
- Garantizar la conexión
- Especificar cables, conectores y componentes de enlace inalámbrico.

Este nivel reconoce únicamente los bits que son transmitidos, no tiene la capacidad de darles una interpretación.

2.3 Capas del modelo OSI que son modificadas por los medios inalámbricos

Ahora que analizamos el modelo OSI nos damos cuenta que las redes inalámbricas se diferencian de las redes convencionales principalmente en las dos capas inferiores, es decir, que la capa física y la capa de enlace presentan cambio importantes, las capas superiores no se ven modificadas por el cambio de tecnología.

En la capa física, los cables son sustituidos por el aire, en el cual viajan ondas de radio frecuencia que se encargan de transportar los datos de un extremo a otro. Las bandas de frecuencia están en un rango de 2,4 GHz. a 5 GHz. que utilizan las principales marcas en el mercado.

En la capa de enlace, las tarjetas convencionales con conectores de cable son sustituidas por tarjetas inalámbricas, que cuentan con su propio método de transmisión de datos. Lo ideal en este tipo de redes es que la señal debe de viajar por el aire con un mínimo de interferencia, para ello existen dos técnicas utilizadas: la secuencia directa y el salto de frecuencia.

En la primera técnica, la información es mezclada con un patrón aleatorio de bits con una frecuencia mayor, que se basa en una función de propagación determinada, cuando llega la señal al receptor, los datos originales son recuperados aplicándoles nuevamente la función de propagación conocida. Sólo aquel receptor

que tenga la misma función de propagación será capaz de regenerar la información enviada.

La segunda técnica, el emisor y el receptor se sincronizan en un patrón determinado, brincando de una frecuencia a otra, en ambos extremos al mismo tiempo, como en el método de secuencia directa los datos originales son recuperados en el receptor en base al patrón de salto de frecuencia.

Por último, para cerrar el capítulo ejemplificaremos un dispositivo inalámbrico dentro del modelo OSI. El punto de acceso funciona en la capa física y en la capa de enlace de datos, realizando la tarea de un hub encargándose de brindar acceso a las computadoras que conforman la red. Como se ve en el cuadro de la figura 2,4, donde se remarcan las capas que se involucran en el funcionamiento del access point.

Capa de aplicación
Capa de presentación
Capa de sesión
Capa de transporte
Capa de red
Capa de enlace de datos
Capa física

Fig. 2,4 Capas que utiliza el access point dentro del modelo OSI.

Capítulo 3. Tecnologías de redes LAN y WLAN

En este capítulo abarcaremos las principales tecnologías de red que han surgido a través de los años y que han adquirido una gran importancia, debido a la manera en la que operan y a la manera en que comparten la información.

Se verán las normas IEEE en que se apoyan cada una de las tecnologías dando mayor énfasis a la 802.11 y sus derivaciones, que son las que utilizan las redes WLAN. Sin duda, nos será de gran utilidad para escoger la mejor tecnología que cumpla con las necesidades requeridas por las empresas.

3.1 Tecnologías de las redes LAN

Las redes LAN son básicamente redes de computadoras utilizadas por alguna organización u empresa donde el medio de comunicación está dedicado a la transmisión de información dentro de la misma, con el fin de compartir recursos físicos ó lógicos principalmente datos. Para que se lleve a cabo ello, existen varias tecnologías que se han utilizado desde su aparición hasta la fecha, en este apartado se entenderá específicamente como tecnología a la interfase de red y a su forma de operar por su protocolo físico de red.

3.1.1 ARCnet

Esta tecnología de red surgió en los años 70's empleando como medio de transmisión cable coaxial, aunque es un estándar aceptado por la industria no tiene un número en IEEE. La velocidad de transferencia de datos es de 2.5 Mbps y 25 Mbps, utiliza una topología lógica de estrella y así mismo utiliza el protocolo polling (poleo) protocolo físico mediante el cual la comunicación se realiza a través de una pregunta-respuesta, del servidor hacia cada uno de los nodos. El se mantiene preguntando constantemente a cada estación de trabajo mediante una comunicación exclusiva y por turno si desea transmitir información, en caso afirmativo, la atiende y al terminar prosigue con otra a su interrogatorio permanente.²⁴

En su tiempo ARCnet fue muy utilizada para la implantación de redes LAN, sin embargo ha caído en desuso debido a su baja velocidad, pues las redes Ethernet ofrecen una velocidad de 10Mbps hasta 1 Gbps.

²⁴ <http://www.saulo.net/pub/redes/>

3.1.2 Token Ring

La red token ring fue implementada por IBM en 1982, es reconocida por la IEEE en 1985 en su apartado 802.5, se distingue por el método de transmitir información empleando el método de acceso Token passing.

Se utiliza un token o ficha virtual que va pasando de computadora a computadora. Cuando una computadora desea realizar una transmisión debe de esperar que le llegue un token vacío, cuando esto pasa puede realizar su envío de datos, el receptor recibe la información y regresa el token a la computadora que se la envió, junto con un acuse de recibido, en este momento queda liberado el token para que pueda ser utilizado por otro nodo de la red. Sin duda es una manera muy segura y ordenada de enviar información, evitando posibles colisiones. El problema consiste en el tiempo de espera para recibir el token, debido a que sólo hay uno.²⁵

La velocidad de transmisión de este tipo de red es de 4 Mbps ó 16 Mbps. Lo importante es que todas las estaciones deben de estar configuradas a la misma velocidad para que funcione. Las computadoras se conectan a un concentrador por medio de un cable en forma de estrella, aunque lógicamente funciona en forma de anillo, debido a que el token se va rolando entre todas las computadoras.

El concentrador que se utiliza en este tipo de red se le conoce como MAU (Unidad de múltiple acceso), tiene la capacidad de soportar de 72 hasta 260 nodos. Es claro que esta tecnología es eficiente en redes pequeñas y medianas, el medio de transmisión empleado es cable coaxial.

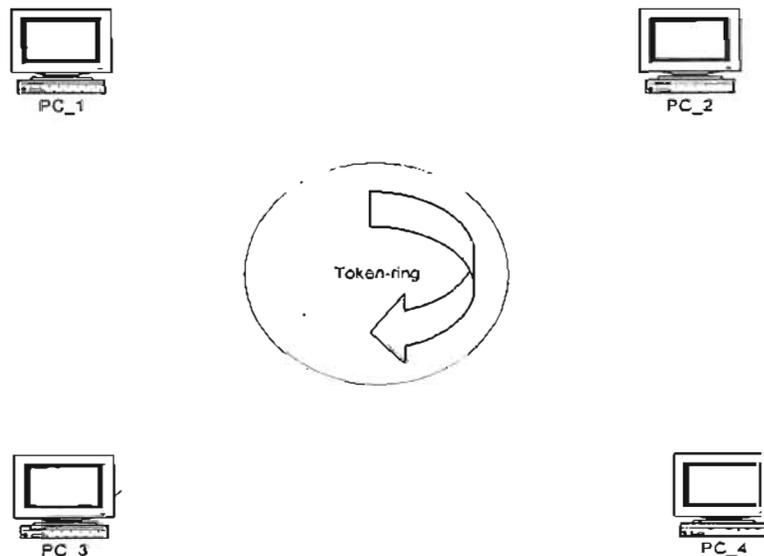


Fig. 3,1 Flujo de datos en token ring.

²⁵ http://www.htmlweb.net/redes/topologia/topologia_4.html

Las redes Token ring siguen existiendo, aunque actualmente es muy difícil encontrarlas. A pesar de ser una red con un funcionamiento lógico eficiente hoy en día la tendencia sigue siendo hacia Ethernet y sus derivaciones.

3.1.3 Ethernet

Es la tecnología de red más utilizada actualmente en el mundo y es la única de interés para los entornos LAN. Resulta muy eficiente para transportar tráfico esporádico y pesado a velocidades muy elevadas. Su topología física es en bus ó estrella y su topología lógica es en bus. Es un estándar aceptado por IEEE en su norma 802.3, fue diseñada originalmente para funcionar a 10 Mbps, aunque con el paso del tiempo se ha ido perfeccionando y alcanza velocidades de 100 Mbps(802.3u) hasta 1 Gbps(802.3z). El tipo de cable utilizado para esta tecnología, es el tipo telefónico ó el conocido como par trenzado.

El origen de este método de acceso, fue en la Universidad de Hawai en los años setentas, el cual utiliza el protocolo físico CSMA/CD (Carrier Sense and Multiple Access with Collision Detection), Método de Acceso Múltiple con Detección de Portadora y Detección de Colisiones. Con este protocolo, cualquier nodo transmite y espera a que se le confirme que la información fue recibida correctamente, de otra forma, se detecta la posible colisión, cada estación espera un tiempo a que el canal esté desocupado y la información se transmite nuevamente.

Una colisión se produce cuando dos máquinas escuchan para saber si hay tráfico en red, no detectan nada y transmiten de forma simultánea. En este caso, ambas transmisiones se dañan y las estaciones deben volver a transmitir más tarde. Las máquinas poseen mecanismos de detección de las colisiones y algoritmos de postergación²⁶ que determinan el momento de retransmisión de tramas que han sido destruidas.

Las redes Ethernet son broadcast, lo que significa que cada máquina puede ver todas las tramas, aunque la información no sea para ellas. Por lo que cada máquina examina las tramas que circulan por la red para determinar si la información les pertenece. De ser así, las tramas pasan por cada una de las capas que especifica el protocolo y se procesan. Si no es el caso, las tramas son ignoradas.²⁷

Ethernet tiene las siguientes características:

- Utiliza un canal único de transmisión para todas las estaciones, por que sólo una lo puede usar en cada momento, CSMA/CD es un protocolo por demanda.

²⁶ Nota: Se genera un tiempo de espera aleatorio en las dos máquinas para iniciar la retransmisión de tramas.

²⁷ http://www.htmlweb.net/redes/topologia/topologia_3.html

Cabecera Ethernet	Cabecera IP (20 bytes)	Cabecera TCP/IP (20 bytes)	Trama de datos	Checksum Ethernet
-------------------	------------------------	----------------------------	----------------	-------------------

Fig. 3,3 Formato general de trama Ethernet.

3.1.4 Redes FDDI Y CDDI

Las redes FDDI Y CDDI manejan el principio básico de las redes Token ring, con algunas variaciones, utilizan el mismo método de acceso, el Token passing. La diferencia más importante se encuentra en que FDDI utiliza fibra óptica y CDDI utiliza cobre, ambas con velocidades de 100Mbps. Actualmente FDDI es la más utilizada de las dos por lo que explicamos a continuación sus principales características, las redes FDDI (Fiber Distributed Data Interface, Interfaz de Datos Distribuida por Fibra) surgieron a mediados de los años ochenta, se caracterizan por tener una topología física de anillo y estrella con una topología lógica de anillo con doble token, uno transmitiendo en el sentido de las manecillas del reloj y la otra en dirección contraria. La velocidad ofrecida por esta arquitectura 100 Mbps, es sobre una distancia del anillo de hasta 300 metros, soportando un total de hasta 1000 estaciones conectadas.²⁹

Los dos anillos de la FDDI son conocidos con el nombre de primario y secundario. El anillo primario o principal se usa para la transmisión de datos, mientras que el anillo secundario se usa generalmente como respaldo.

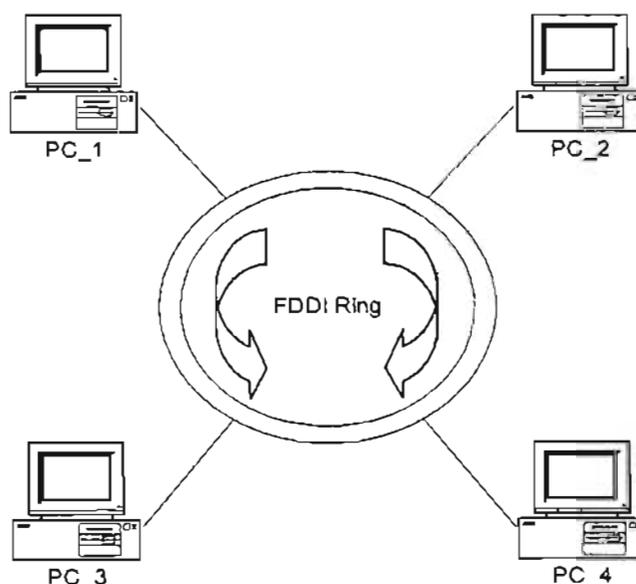


Fig. 3,5 Arquitectura FDDI.

²⁹ http://www.htmlweb.net/redes/topologia/topologia_5.html

En la figura anterior podemos observar los dos anillos que conforman la arquitectura FDDI y los dos sentidos en el que fluye la información. Existen dos tipos de terminales, las de clase B; que son conectadas al anillo primario, y las de clase A, que goza de estar conectada a los dos anillos.

Como se menciona, la característica más importante de FDDI, es la utilización de fibra óptica. Los cables ópticos ofrecen grandes ventajas en seguridad y velocidad, debido a que la fibra es inmune a las interferencias eléctricas y el rendimiento de velocidad es mayor, comparado con cable de cobre.

3.2 Tecnologías de redes WLAN

Al igual que las redes LAN, las redes WLAN son redes que comparten información entre sí, con la diferencia de que se utiliza el aire como medio de comunicación en lugar de los cables, proporcionando una conectividad de igual a igual entre los distintos nodos de la red.

Las redes WLAN encuadran en el estándar 802 en su apartado 11. En el capítulo anterior vimos que las redes inalámbricas son contempladas en las capas más bajas del modelo OSI, lo que garantiza que funcionen utilizando la familia de protocolos TCP/IP para su comunicación debido a que el protocolo está por arriba de la tecnología.

Debemos saber que las primeras redes inalámbricas que se utilizaron fueron enlaces infrarrojos que surgieron en el año de 1979, con lo que podemos considerarlo el punto de partida de las redes LAN sin cable.

En 1985 se autorizó el uso de la banda de frecuencia gratuita llamada ICM (Industria, Científica y Médica) utilizada por algunos dispositivos del área industrial, científica y médica. Esta decisión hizo posible que las redes WLAN salieran de los laboratorios para llegar al mercado. Su historia es reciente de no más de 15 años. En 1989 se forma el comité encargado del establecimiento de la norma 802.11 original, pero fue hasta 1994 cuando aparece el primer borrador, sin embargo en 1999 es cuando se da por finalizada la norma.³⁰

En los últimos años las redes Wi-Fi han empezado a tomar fuerza en México, pero el crecimiento no se compara con el de Estados Unidos, donde no parecen temerle a las nuevas tecnologías y han invertido en centros de convenciones, hoteles, restaurantes y casetas telefónicas para laptops. Por ello, podemos decir que en México no se tiene un total conocimiento de las ventajas que puede ofrecer las redes Inalámbricas.

³⁰ <http://www.eveliux.com/articulos/estandareswlan.html>

3.2.1 WLAN 802.11

En 1997, IEEE corroboró el estándar 802.11 para WLAN que alcanzaba una velocidad de 2.4 Mbps, con una modulación de señal de espectro expandido por secuencia directa (DSSS), sin embargo también contempla la opción de espectro expandido por salto de frecuencia (FHSS) en la banda de 2.4 GHz. Se definió también el funcionamiento y la interoperabilidad de las redes inalámbricas.

En las estaciones de trabajo inalámbricas no se pueden detectar las colisiones como se contempla en las redes cableadas, el método de acceso al medio es CSMA/ CA, el cual escucha el medio y verifica si está disponible, minimiza el riesgo de colisión por medio de un retardo aleatorio, usado antes de escuchar el medio y de transmitir la información.

3.2.2 WLAN 802.11b

Unos años más tarde en 1999 se aprobó el estándar 802.11b para redes WLAN empresariales, con una velocidad de 11 Mbps y tiene una cobertura interior de 50 m y exterior de 150 m, su alcance es óptimo para su uso en oficinas y zonas residenciales. Pertenecen a la banda ICM en la frecuencia de 2.4 GHz, con una modulación del tipo DSSS, que le permite una mayor velocidad.³¹

Una de las ventajas que puede tener el uso de esta tecnología es que cuenta con un mecanismo de velocidades múltiples para el control de acceso al medio, con ello podemos intercambiar la velocidad utilizada de 11, 5.5, 2 y 1 Mbps, esto en función de la distancia e interferencia. Las estaciones de trabajo más lejanas pueden conectarse a velocidades menores con el fin de que la señal llegue óptimas condiciones. Es importante señalar que entre más frecuencia de operación tengamos, obtendremos mayor velocidad, pero estaremos reduciendo la cobertura de la red. Ya que la señal se vuelve más directa hacia un sólo punto cuando aplicamos más frecuencia.

3.2.3 WLAN 802.11g

Esta tecnología fue aprobada por IEEE en el año 2003, en el estándar 802.11g, el cual es compatible con la 802.11b, sin embargo la velocidad es duplicada a 22 Mbps y se puede acelerar hasta los 54 Mbps, compitiendo con las nuevas tecnologías que prometen velocidades elevadas.³²

Utiliza una modulación OFDM y/o CCK que puede coexistir perfectamente con normas anteriores, con una cobertura de interior de 30 metros y una exterior de 50 metros.

³¹ *loc. cit*

³² <http://www.monografias.com/trabajos14/wi-fi/wi-fi.shtml#REDES>

3.2.4 WLAN 802.11a

En 1999 se ratificó el estándar 802.11^a, aunque los productos empezaron a salir al mercado internacional a mediados del 2002, utilizan una modulación OFDM que alcanza una velocidad de 54 Mbps con una frecuencia de 5 Ghz, aunque con una cobertura menor que la tecnología 802.11b, que alcanza 30 metros en interiores y 50 metros en exteriores.

El uso de puntos de acceso ayudan a extender al doble la cobertura si se encuentra en un punto medio. Aunque en Europa esta banda no está disponible, en otros países como Estados Unidos, Canadá, Japón, Australia y México, se puede utilizar sin ningún problema. Aunque el costo de los dispositivos inalámbricos es mayor, permite un mayor número de usuarios y una comunicación menos expuesta a interferencias que la hacen más confiable. Actualmente existe una variación la 802.11^a turbo que puede llegar hasta una velocidad de 125 Mbps.³³

3.2.5 Otras tecnologías

Existen más normas de IEEE que involucran a las redes WLAN, pero son de escaso interés práctico para las personas que se dedican a la instalación de ellas, debido a que es muy difícil encontrarlas en el mercado mexicano. A continuación mencionamos algunas de ellas:

802.11e. Está dirigida 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.

802.11h. Define la administración del espectro de la banda de los 5GHz para su uso en Europa y en Asia Pacífico.

802.11i. Está dirigida a abatir la vulnerabilidad actual en la seguridad para protocolos de autenticación y de codificación. El estándar abarca los protocolos 802.1X, TKIP (Protocolo de Llaves Integras-Seguras-Temporales) y AES(Estándar de Encriptación Avanzado).³⁴

³³ *loc. cit*

³⁴ Material de apoyo del diplomado redes inalámbricas impartido por la Facultad de Ingeniería 2004.

3.2.6 ¿Qué tecnología utilizar?

Para que nosotros podamos instalar alguna tecnología primeramente debe estar en el mercado para poder adquirirla, seguidamente tenemos que analizar los requerimientos de la empresa, el número de computadoras, su estructura y su información técnica de los dispositivos inalámbricos. Ello nos ayudará a tomar la decisión más adecuada.

En el siguiente cuadro mostramos una comparación de las tecnologías más importantes, debido a que son las más utilizadas y comerciales hasta el momento.

Parámetro	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g
Frecuencia	5 Ghz.	2,4 Ghz.	2,4 Ghz.
Espectro disponible	300 Mhz.	83.5 Mhz.	83.5 Mhz
Modulación	OFDM	DSSS/CCK	DSSS/OFDM
Ancho de banda por canal	20 Mhz.	22 Mhz.	22 Mhz.
Número de canales utilizables	6 canales	3 canales	3 canales
Cobertura Interior / Exterior	30/50 metros	50/150 metros	30/50 metros
Usuarios simultáneos	64	32	50
Potencia	200 mW, 1 W y 4 W	1 mW.	200 mW, 1 W y 4 W

Fig. 3, 6 Tabla de comparación de estándares 802.11a, b y g.

La cobertura es muy importante para escoger la tecnología de acuerdo al lugar donde se realizará la instalación, para ello el siguiente cuadro pone a prueba la tecnología con algunas barreras que puede tener el área del montaje.

Tipo de área	Barreras	Longitud confiable	Longitud probable	Rango de porcentajes de pérdida de longitud con una referencia de 120 metros.
Áreas abiertas	Vista directa	120 metros	200 metros	0 %
Áreas semiabiertas	Madera Plástico Sintético Tabla roca.	30 metros	50 metros	58 % a 75 %
Área cerrada	Ladrillo Techos	15 metros	25 metros	79 % a 87.5 %
Área obstruida	Metal concreto	0	10 metros	91 % a 100%

Fig. 3,7 Cobertura en distintas áreas con barreras.

Por último, compararemos las principales tecnologías de redes, respecto a su tiempo de instalación, contemplando un número de 20 máquinas, donde podemos ver que las redes WLAN son más rápidas de instalar.

	Token Ring	Ethernet	WLAN
Colocación de tuberías y cableado	2 semanas	2 semanas	No necesario a menos que sea infraestructura.
Configuración y pruebas de red.	1- 2 días	1 día	8 horas
Colocación de computadoras.	7 horas	7 horas	2 horas

Fig. 3,8 Tiempos aproximados de instalación de tecnologías LAN.

3.2.7 Compatibilidad Wi-Fi

Los líderes de la industria crean la WECA (Wireless Ethernet Compatibility Alliance), una alianza para la Compatibilidad Ethernet Inalámbrica, con el objetivo de certificar la interoperabilidad de los productos de redes inalámbricas 802.11b y promoverlos para la empresa y el hogar. Para indicar la compatibilidad entre dispositivos inalámbricos, tarjetas de red o puntos de acceso de cualquier fabricante, se les incorpora el logo "Wi-Fi" (estándar de Fidelidad Inalámbrica), que garantiza que los equipos con esta marca, pueden funcionar en las redes sin ningún problema.

Aunque está garantizada la compatibilidad de los dispositivos Wi-Fi de los distintos fabricantes, es recomendable utilizar una misma marca de dispositivos, para realizar los enlaces en la red, ya que ello nos garantiza un mayor desempeño y mejor monitoreo de red.

3.3 Wi-Max

Esta tecnología es el futuro de las redes inalámbricas, que busca dar una mayor cobertura que Wi-Fi, convirtiendo las señales de voz y datos en ondas de radio que pueden tener un alcance hasta de 50 kilómetros en su primera versión. El enlace es punto a punto con una velocidad de más de 100 Mbps, siempre y cuando exista visión directa entre emisor y receptor. Se utilizan varias frecuencias que van desde los 10 hasta 66 Ghz.

El nivel de cobertura rompe con los alcances que posee actualmente las redes Wi-fi creadas para WLAN. La tecnología Wi-Max está pensada para crear redes WMAN y se basa en la norma 802.16 de IEEE.

La primera publicación de Wi-max fue en el año 2002, en marzo del 2003 se ratificó una nueva versión llamada 802.16^a y opera en una banda de frecuencia entre los 2 y 11 Ghz, posee un rango de cobertura entre 40 y 70 kilómetros. Es válida para enlaces punto a punto y punto a multipunto, ya que no requiere de una línea de visión directa como la primera versión, pero con una velocidad menor.

Se habla de que esta tecnología puede salir al mercado a mediados del 2007 para ser incorporada en los equipos portátiles y que los usuarios se puedan comunicar en cualquier parte de la ciudad, sin contar los subterráneos del metro por razones obvias. Debido a que Wi-max no ha salido al mercado, le ha permitido que el estándar se desarrolle conforme a un ciclo muy bien establecido, que garantice un buen desempeño y la estabilidad. En el siguiente cuadro realizamos una comparación entre Wi-fi y Wi-Max.

Características	Wi-fi (802.11)	Wi-Max (802.16)
Alcance	Optimizada para usuarios en un rango de 150 metros. Se añaden puntos de acceso y antenas de ganancia para mayor cobertura	Alcance de hasta 70 kms. Sin problemas de nodo oculto.
Cobertura	Optimizada para ambientes interiores, con docenas de usuarios simultáneos.	Optimizada para ambientes exteriores (árboles, edificios y usuarios distribuidos en un amplio radio. Soporta el estándar para técnicas avanzadas de antena y malla.
Escalabilidad	Canal amplio y estable, ideal para interiores (20 Mhz) La velocidad decrece conforme se vayan agregando usuarios a la red.	Canal con ancho de banda flexible de 1.5 a 20 Mhz. Acceso múltiple y eficiente.
Velocidad	11 a 54 Mbps	124 Mbps

Fig. 3,9 Diferencias entre Wi-fi y Wi-Max.

Es claro que Wi-Max no busca remplazar a Wi-Fi, sólo busca llenar los vacíos tecnológicos que Wi-fi no ha podido cubrir. Las dos tecnologías pueden llegar a convivir sin ningún problema, complementándose una con otra, por lo que se requiere de puntos de acceso que las hagan interactuar.

3.4 Tecnología Bluetooth

Bluetooth es una tecnología utilizada para conectividad inalámbrica de corto alcance, de no más de 10 metros, entre los distintos dispositivos tales como teléfonos celulares, teclados, máquinas de fax, computadoras de escritorio y portátiles, bocinas, proyectores, impresoras, etc. El principal mercado es la transferencia de datos y voz entre periféricos y computadoras personales, las velocidades de operación van de 1 a 2 Mbps.

El enfoque de Bluetooth es el de evitar el uso de cables y aportar una sencillez en el uso de dispositivos, sólo basta acercarnos físicamente para que la tecnología funcione. Con el simple hecho de acercar la Palm al ordenador podemos realizar la sincronización automáticamente, actualizando nuestra agenda y nuestros correos electrónicos. Sin embargo, esta tecnología no sólo se queda en la oficina, llega también a los hogares, realizando una automatización en el encendido y apagado de luz, el manejo de persianas, el uso de bocinas inalámbricas y de auriculares inalámbricos para el walkman.³⁵

En los automóviles se empieza a utilizar bluetooth, para abrir puertas, quitar seguros, abrir la cajuela, nivelar suspensiones e incluso encender el coche sin estar dentro.

Como podemos darnos cuenta, esta tecnología no está direccionada para interconectar redes, más bien a interconectar periféricos y dispositivos de enlace, por lo que podemos decir que es complementaria a WLAN, muchas veces se confunde ya que utiliza ondas de radiofrecuencia de 2.4 Ghz en la misma banda del estándar IEEE 802.11, aunque por su aceptación no descartamos que próximamente bluetooth llegue a las tarjetas de red.

Por último, en marzo del 2002 se hizo la estandarización de bluetooth en la norma 802.15.1 de IEEE, algunos dispositivos anteriores no pueden convivir con la norma 802.11b, debido a que ambos interferían entre sí. El nuevo estándar establecido ya no tiene ese problema, además permite una mayor validez y soporte en el mercado.

El conocer las tecnologías existentes, nos permitirá seleccionar adecuadamente los dispositivos más apropiados que nos ayudarán a cubrir las necesidades de la empresas donde realicemos proyectos de redes inalámbricas.

³⁵ <http://www.zonablueetooth.com/documentacion.htm>

Capítulo 4. Conformación y planeación de una red.

Sabemos que para montar una red inalámbrica, debemos de conocer los elementos que conforman la misma, por ello mencionamos los aspectos más importantes que hacen posible que una red funcione haciendo hincapié que los conceptos pueden ser empleados tanto para una red inalámbrica como para una alámbrica. En primer lugar mencionamos los grupos más importantes que conforman una red; Equipos, Conectividad y Software. Por otro lado, una vez conocidos dichos elementos, debemos pasar al siguiente paso, la planeación de una red, si esta etapa se realiza lo más profesional posible, evitaremos contratiempos que puedan surgir a la hora del montaje.

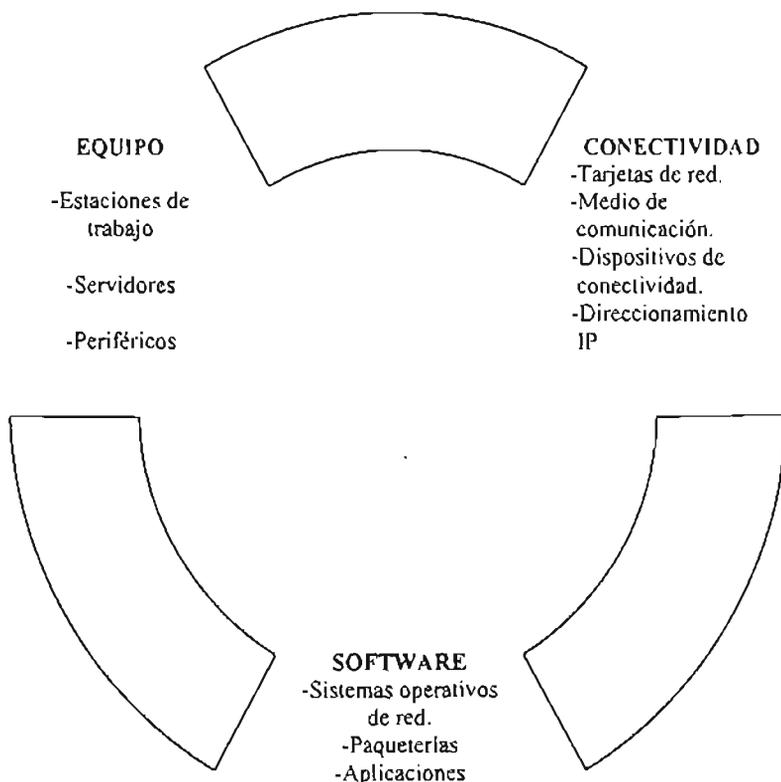


Fig. 4,1 Grupos que conforman una red.

4.1 Equipo

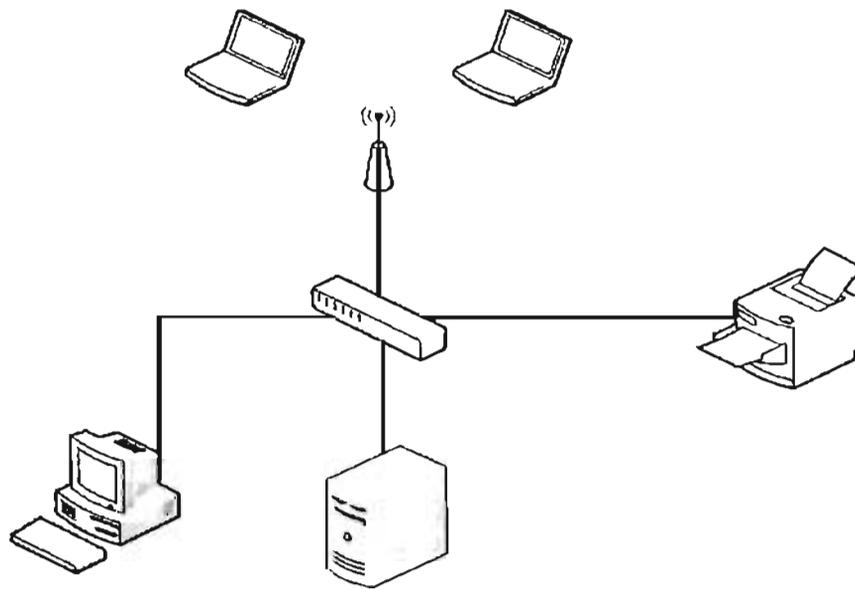


Fig. 4,2 Equipos principales de una red.

4.1.1 Estaciones de trabajo

Las computadoras son conocidas en el ámbito de las redes como estaciones de trabajo, pues nos sirven para realizar un sin fin de tareas en nuestro trabajo. Sin embargo, al conectarse a la red no pierden su capacidad de funcionar de manera independiente; podemos trabajar sin conexión. Sin embargo, cuando una computadora acceda a la red incrementa su funcionalidad, ya que podemos utilizar todos los recursos que estén disponibles, como por ejemplo imprimir en la impresora láser a color del jefe, si nuestra impresora de matriz no funciona.

4.1.2 Servidores

Las características y configuración de una computadora para que sea posible definirla como Servidor, están en función de los requerimientos particulares del caso, generalmente se entiende como servidor a un equipo robusto tanto en hardware como en software.

El servidor provee de recursos a los demás nodos de la red. Los recursos pueden ser impresoras, unidades de disco, unidades de almacenamiento. No hay que olvidar que un servidor también puede considerarse como un programa de software (servidor DNS, servidor DHCP, servidor Web etc.) y no sólo como un elemento físico.

Aunque es posible adaptar un servidor a casi cualquier actividad específica, los más comunes son los siguientes:

Servidores de bases de datos.

Los servidores de bases de datos distribuyen el procesamiento de la información entre una aplicación, que es ejecutada en la estación de trabajo cliente, y el manejador de bases de datos que se ejecuta en el servidor. Con esto se reduce, además de la carga de procesamiento del servidor, el tráfico de la red. Estos servidores pueden manejar las bases de datos de dos maneras, bases de datos centralizadas y bases de datos distribuidas.

Servidores de impresión.

La función de este tipo de servidores es la de administrar los recursos de impresión, dentro de la red, de manera eficiente. Generalmente se tiene al servidor conectado directamente al dispositivo de impresión, dicho servidor se encarga de recibir las peticiones de impresión de las demás estaciones de la red y de mandarlas a la impresora.

Servidores Proxy

Un servidor Proxy es un programa de software que se instala en un único ordenador de la red local, y que permite que varios ordenadores de la misma red puedan compartir un mismo acceso a Internet o conexión a Internet de manera simultánea.³⁶

El servidor Proxy da servicio a todos los ordenadores de una red local, sean éstos Windows, UNIX ó Novell. Permite la interconexión de redes heterogéneas.

Hablando del servidor como un equipo físico dentro de la red, tenemos que la clasificación más importante es la siguiente:

El Servidor o servidores puede ser de dos tipos: ***Dedicado o No dedicado***

- El dedicado se utiliza exclusivamente para administrar los recursos físicos y lógicos de la red.
- El no dedicado además de administrar los recursos físicos y lógicos de la red, funciona como Estación de Trabajo

4.1.3 Periféricos

Cuando hablamos de periféricos entendemos que se habla de cualquier recurso de hardware a explotar dentro de la red. Impresoras, escaners, unidades de respaldo, dentro de los más importantes.

³⁶ <http://www.mundofree.com/juanpablo/xarxes/gg.html>.

Hoy en día un concepto que está tomando fuerza es la telefonía sobre IP, que consiste en empaquetar la voz en datagramas IP, esto implica que la voz pueda viajar sobre un red de computadora, en un canal dedicado o en Internet. La voz puede ser obtenida desde un micrófono conectado a la placa de sonido de la PC, o bien desde un teléfono común: existen gateways (dispositivos de interconexión) que permiten intercomunicar las redes de telefonía tradicional con las redes de datos. De hecho, el sistema telefónico podría desviar sus llamadas a Internet para que, una vez alcanzado el servidor más próximo al destino, esa llamada vuelva a ser traducida como información analógica y sea transmitida hacia un teléfono común por la red telefónica tradicional. Se pueden mantener conversaciones teléfono a teléfono. Hoy en día existen, teléfonos IP y hubs telefónicos distribuidos por Cisco.

4.2 Conectividad

A continuación abarcamos los elementos de conectividad más utilizados hasta hoy en día: tarjetas de interfaz, medio de comunicación, dispositivos de conectividad y el direccionamiento IP.

4.2.1 Tarjetas de interfaz a red

En el capítulo anterior se definieron las tecnologías propias de las redes LAN y WLAN, entendimos que la tecnología va ligada con la interfase de red. Ahora, si definimos una interfase de red de manera práctica, tenemos que para que una estación pueda conectarse a la red es necesario que cuente con un adaptador de red o tarjeta de interfaz, las cuales son adaptadas a una ranura de expansión, o también hay dispositivos externos que son conectados en el puerto serial, paralelo o USB.

En la siguiente figura podemos ver algunos tipos de tarjetas de red alámbricas comerciales en la actualidad:

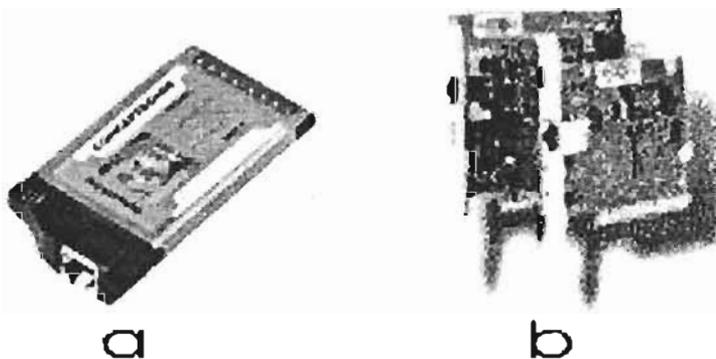


Fig. 4,3 Tarjetas de red 10/100 Mbps.

La tarjeta tipo a, es utilizada por las computadoras portátiles; la conocida como PCMCIA. Las tipo b, son conectadas en la ranura de expansión PCI.

Wireless

Complementando lo dicho anteriormente en el aspecto inalámbrico decimos que el Wireless es una tarjeta de enlace como las anteriores, pero con la diferencia que nos permite interconectar estaciones de trabajo a una red de una manera inalámbrica.

En la siguiente figura mostramos la tarjeta Wireless:

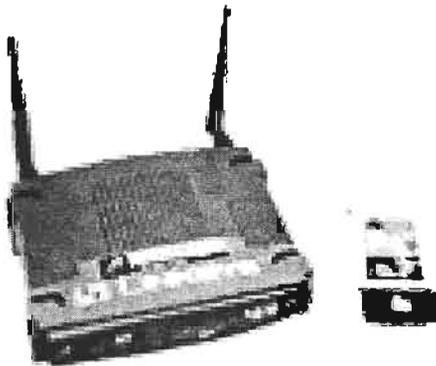


Fig. 4,4 Wireless.

4.2.2 Medio de comunicación

Como vimos en el capítulo 1, existen los medios de comunicación guiados y no guiados, dentro de la parte inalámbrica tenemos como medio, el aire, dentro de la parte alámbrica, el cable es el medio más utilizado en el transporte de datos. A continuación se muestran las categorías existentes en el cable par trenzado:

Categoría	velocidad	comentario
1	1 Mbps	Se usa en la transmisión de voz solamente.
2	4 Mbps	Se usa para la transmisión de datos a baja velocidad
3	10 Mbps	Se usa en la transmisión de datos en redes ethernet a una frecuencia de 16 Mhz.
4	16 Mbps	Se usa en transmisión de datos en redes Token Ring a una frecuencia de 20 Mhz,
5	100 Mbps	Se usa en la transmisión de datos en redes ethernet rápidas a una frecuencia de de 100 Mhz.
6	1 Gbps	Transmisión de datos en redes de de alta velocidad y su frecuencia es de 200 Mhz.

Fig. 4,5 Categorías de par trenzado.

4.2.3 Dispositivos de conectividad

Otro aspecto importante que necesitamos conocer son los dispositivos de conectividad, los cuales nos permiten extender la red e incrementar el número de nodos utilizados, sabemos que dentro de la parte inalámbrica el *access point* es nuestro elemento principal de conectividad, pero no nos podemos olvidar de otros dispositivos que nos pueden ayudar en un momento dado a expandir una red:

4.2.3.1 Hub

Pertenece a la capa física. Son dispositivos que conectan múltiples estaciones de trabajo o nodos, utilizando un sólo bus en su interior, la velocidad de transmisión es la misma en cada uno de los nodos con la variante que hay un mayor riesgo de colisión ya que un hub no tiene varios buses como lo es en un switch.

4.2.3.2 Switch

Es un dispositivo que pertenece a la capa de enlace de datos ó de nivel 2 del modelo OSI, por lo que trabaja con direcciones físicas, su principal función es segmentar físicamente a una red con el fin de que se distribuya el tráfico por varios buses, reduciendo así el número de colisiones en la red, así mismo los diferentes buses pueden transmitir a diferentes velocidades por ejemplo 10 y 100Mbps.

La diferencia entre el hub y el switch es que los switches toman decisiones basándose en las direcciones MAC y los hubs no toman ninguna decisión. Como los switches son capaces de tomar decisiones, así hacen que la LAN sea mucho más eficiente. Los switches hacen esto "conmutando" datos sólo desde el puerto al cual está conectado el host correspondiente. A diferencia de esto, el hub envía datos a través de todos los puertos de modo que todos los hosts deban ver y procesar (aceptar o rechazar) todos los datos. Esto hace que la LAN sea más lenta. A primera vista los switches parecen a menudo similares a los hubs. Tanto los hubs como los switches tienen varios puertos de conexión (pueden ser de 8, 12, 24 o 48 puertos).

4.2.3.3 Router

Es un dispositivo que pertenece a la capa de red o de nivel 3 del modelo OSI, trabaja con direcciones lógicas y se encarga de generar la ruta ó de tomar el mejor camino que seguirá cada paquete de información de un nodo origen a un nodo destino, Los enrutadores o routers a parte de dividir el tráfico, pueden interconectar diferentes redes. Un router no sólo puede ser un componente físico en hardware, también puede ser un componente en software.³⁷

³⁷ *loc. cit*

Un router identifica dos tipos de direcciones:

- 1) Direcciones únicas de red. (IP)
- 2) Direcciones de los dispositivos de cada red

En general, los dos aspectos fundamentales para un ruteador son:

- Obtener información sobre los ruteadores adyacentes y las redes remotas
- Escoger la ruta más adecuada para llegar al destino

4.2.3.4 Puente

Dispositivo perteneciente a la capa de enlace de datos, los puentes al igual que los routers interconectan redes pero a nivel de direcciones físicas, unen redes heterogéneas esto es que pueden conectar diversas tecnologías ó diferentes protocolos físicos. Los puentes también tienen la particularidad de que pueden duplicar distancias.

4.2.3.5 Repetidores

Los repetidores son dispositivos para interconectar segmentos de red, lo cual permite que dichos segmentos sean tratados como uno solo. Un repetidor recibe señales de un segmento anterior de la red, las amplifica y las retransmite al segmento siguiente, funcionan en la capa física y son utilizados para extender la cobertura geográfica de una red con el fin de no perder atenuación. Los repetidores físicamente extienden el alcance de una red regenerando señales (bits) de un medio de transmisión cualquiera y retransmitiéndolas.

4.2.3.6 Modems

Son dispositivos que modulan y demodulan señales en un medio de transmisión, es decir, convierten los números binarios de una computadora en señales eléctricas para que puedan viajar por la capa física. Hay modems analógicos y módems digitales ambos utilizando una línea telefónica como es el caso del modem de alta velocidad ADSL u otros pueden utilizar otro medio como es el caso del Cable Modem. Un módem se puede conectar a la PC a través de un puerto USB, un ethernet ó por medio de un slot PCI.

4.2.3.7 Firewall

Se puede decir que un firewall es un router, este router nos protege contra ataques exteriores a nuestra red en el caso de que estemos uniendo dos redes diferentes o que tengamos salida a Internet. Un firewall es un elemento que filtra el tráfico entre redes, puede ser un dispositivo físico o un software sobre un sistema operativo. Se establecen reglas de filtrado con las que se decide si una conexión

determinada puede establecerse o no. Incluso puede irse más allá y realizarse modificaciones sobre las comunicaciones, como el NAT.

En el siguiente esquema se muestra uno de los ejemplos funcionales utilizando algunos de los dispositivos de conectividad mencionados, ya que todo dependerá de nuestras necesidades. El esquema muestra una conexión de una red LAN con acceso a Internet.

Como se menciona anteriormente, la parte alámbrica sigue siendo operativa, principalmente cuando utilizamos routers para interconectar redes.

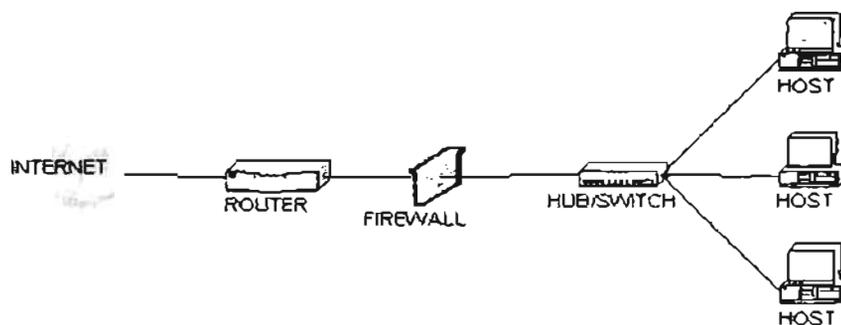


Fig. 4,6 Conexión alámbrica de una red LAN con acceso a Internet.

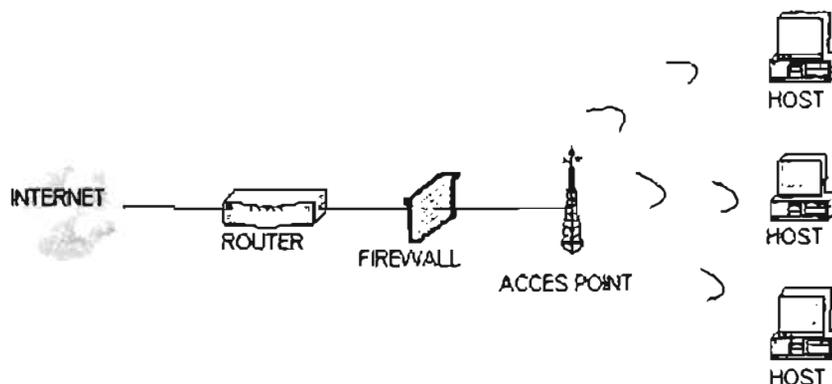


Fig 4, 7 Conexión inalámbrica de una red LAN con acceso a Internet.

4.2.4 Direccionamiento IP

Como sabemos, la familia de protocolos TCP/IP sigue siendo la familia más utilizada hoy en día en la comunicación de redes LAN, WLAN y WAN, por lo que el direccionamiento IP nos resulta importante. Para que la información llegue a cada máquina es necesario el uso de una dirección IP, con el fin de que exista un control en la comunicación.

4.2.4.1 Clasificación de direcciones IP

Una dirección IP es un identificador que tiene cada máquina dentro de la red, la cual debe ser única, es decir, distinta a todas las demás, no puede haber dos ordenadores con la misma dirección. Las direcciones IP se clasifican en:

Direcciones IP públicas. Son las utilizadas por los servidores dentro de Internet, para que toda computadora conectada pueda tener acceso a la información y servicios que ofrece el Internet. Por lo tanto, para que nosotros podamos acceder a Internet, nuestra máquina debe de contar con una IP de este tipo.

Un ejemplo práctico es la dirección 132.248.10.7, que pertenece al portal de la Universidad Nacional Autónoma de México. Podemos comprobarlo, accediendo al explorador y escribiendo la dirección.

Direcciones IP privadas. Son utilizadas por las redes privadas, únicamente son visibles por las computadoras que pertenecen a la misma red. Las empresas las usan para manejar información interna y privada. Por lo tanto, no es posible tener acceso a estas redes por medio de Internet. Sin embargo, las estaciones pueden acceder a Internet mediante un servidor o router con una IP pública.

Dentro de estas clasificaciones existes dos tipos de IP, las estáticas y las dinámicas. Expliquemos cada una de ellas:

Direcciones IP estáticas. Se dice que una estación tiene una IP estática cuando se conecta a la red con la misma dirección, es decir, se configura y es fija. Los servidores de Internet utilizan este tipo de dirección con el fin de que siempre se encuentren disponibles ante los usuarios.

Direcciones IP dinámicas. Una estación tiene una IP dinámica cuando a la hora de conectarse utiliza un IP distinta, es decir, que cada vez que inicie sesión dentro de la red, la IP se asigna automáticamente. Los proveedores de Internet utilizan estas direcciones, para ofrecerlas a sus usuarios, ya que es difícil que se conecten todos al mismo tiempo. Eso garantiza un mejor aprovechamiento de las direcciones públicas, puesto que son caras y no son muchas.

La dirección 200.65.102.119 es un ejemplo de IP pública dinámica, es utilizada en estos momentos por la computadora para conectarse a Internet, es asignada automáticamente por el servidor de Prodigy Internet por poner algún ejemplo.

4.2.4.2 Estructura de la IP

Las direcciones IP están formadas por 32 bits que se agrupan en 4 secciones separadas por un punto de la forma A.B.C.D, donde cada letra tiene un rango de 0 a 255.

Veamos un ejemplo:

01000001 00001010 00000010 00000011

Podemos ver que esta dirección está agrupada en 4 octetos de 8 bits y representada en decimal sería 129.10.2.3. Si queremos saber el número de direcciones totales que podemos formar con 32 bits, lo hacemos de la siguiente manera:

El 2 lo elevamos a la potencia 32, esto nos da un resultado de 4,294,967,296.

Como podemos ver en el cálculo, el número de direcciones supera los 4,000 millones, aunque no todas son validas para asignarlas a las estaciones. El número de IP's, dependerá del tamaño de la red, es decir, el total de computadoras que la conformen.

4.2.4.3 Clases de IP

Las direcciones IP están divididas en 5 clases, las cuales analizaremos en el siguiente cuadro:

Clase	Formato R= Red H = host	Número de redes	Total de host por red	Rango de direcciones por red	Máscara de red.
A	R.H.H.H	128	16,777,214	de 0.0.0.0 a 127.0.0.0	255.0.0.0
B	R.R.H.H	16,384	65,534	de 128.0.0.0 a 191.255.0.0	255.255.0.0
C	R.R.R.H	2,097,152	254	de 192.0.0.0 a 223.255.255.0	255.255.255.0
D	Grupo			de 224.0.0.0 a 239.255.255.255	*****
E	*****			de 240.0.0.0 a 255.255.255.255	*****

Fig. 4,8 Tipos de direcciones IP.

Como podemos observar en el cuadro, clases A, B y C, son las que se utilizan prácticamente en las redes, para que sean asignadas a una estación. Las direcciones D identifican sólo a un grupo de host ó se dirigen a la multidifusion de paquetes,

mientras que las de clase E están reservadas y están orientadas a fines experimentales.³⁸

La dirección de una máquina se compone de dos partes, cuya longitud puede variar dependiendo de la clase:

- **Bits de red:** son los bits que definen la red a la que pertenece el equipo.
- **Bits de host:** son los bits que distinguen a un equipo de otro dentro de una red.

Los bits de red siempre están a la izquierda y los de host a la derecha, veamos un ejemplo sencillo de una IP tipo C:

Bits de Red	Bits de Host
11000000 10101000 00000000	00010100
192.168.0.	20

Fig. 4,9 Dirección IP tipo C.

Con esta tabla podemos determinar que la dirección del host es 192.168.0.20 y la de red es 192.168.0.0, además como se trata de una IP tipo C tiene una máscara de 255.255.255.0.

La máscara de red es un número con el formato de una dirección IP que nos sirve para distinguir cuando una máquina determinada pertenece a una subred dada, con lo que podemos averiguar si dos máquinas están o no en la misma subred IP. Hagamos un ejemplo rápido de todo lo que hemos dicho.

Supongamos que tenemos dos direcciones IP de dos máquinas y tenemos que identificar si pertenecen a las misma subred. Las direcciones son: 192.168.0.40 y 192.168.0.28, con una máscara de 255.255.255.0. Aunque con sólo verlas nos damos cuenta que pertenecen a la misma red, pero demostrémoslo lógicamente.

El primer paso es convertirlas en binario, posteriormente aplicamos la operación lógica AND con el número de máscara, para obtener el número de subred.

192.168.0.40	11000000	10101000	00000000	00101000(host1)
255.255.255.0	11111111	11111111	11111111	00000000
(máscara)				
(subred)	11000000	10101000	00000000	00000000

³⁸ <http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/x-087-2-issues.ip-addresses.html>

Y

192.168.0.28	11000000	10101000	00000000	00011100(host 2)
255.255.255.0 (máscara)	11111111	11111111	11111111	00000000
(subred)	11000000	10101000	00000000	00000000

Si comparamos los resultados nos damos cuenta que son los mismos, por lo tanto, estas dos computadoras pertenecen a la misma subred, con dirección 192.168.0.0.

En las redes privadas generalmente usan la máscara 255.255.255.0, si el número no supera los 254 equipos. En una red pública las cosas cambian, debido a que cada IP tiene un costo, las redes son partidas en varias subredes, con el objeto de administrar mejor las IP's.

4.2.4.4 Direcciones IP especiales y reservadas

En el rango de 0.0.0.0 a 223.255.255.255, que de acuerdo a la figura 4,6 aparecen como utilizables, no todas son validas para asignarlas a un host, algunas de ellas tienen significados especiales. A continuación veremos algunas direcciones de este tipo, su interpretación varia dependiendo del tipo de red donde se utilicen.

Ejemplo	Significado
0.0.0.0	Hace referencia a nuestro propio host.
0.0.0.10	Hace referencia a un host dentro de la red.
192.168.1.0	Hace referencia a una red.
255.255.255.255	Hace referencia a todos los host de todas las redes. (difusión total)
192.168.0.255	Hace referencia a todos los host de una red indicada.(difusión indicada)
127.0.0.1	Realiza un eco en nuestro host.

Fig. 4,10 Direcciones especiales.

La difusión o broadcasting, se refiere al envío de un mensaje a todas las computadoras que pertenecen a la red. La dirección 127.0.0.1 se utiliza para comprobar que los protocolos TCP/IP están correctamente instalados.

Las siguientes direcciones que veremos a continuación se encuentran reservadas para uso exclusivo de las redes privadas. Con ello se garantiza que no habrá ninguna estación conectada directamente a Internet, de esta manera no ocasionaremos ningún conflicto y las estaciones podrán tener servicio de Internet.

Clases	Rango de direcciones reservadas
A	10.0.0.0
B	172.16.0.0
C	192.168.0.0

Fig. 4,11 Direcciones reservadas.

4.2.4.5 DNS (Sistema de nombre de dominio)

El direccionamiento IP le da gran flexibilidad a las redes LAN, pero en redes más grandes; como Internet, se hace difícil y pesado recordar las direcciones en la forma de secciones decimales. Las personas generalmente preferimos identificadores más comunes. Los nombres de dominio son una forma sencilla que se utilizan para encontrar un sitio en Internet, no es lo mismo recordar 132.248.10.7 que www.unam.mx

Un nombre de dominio, está formado por varios nombres que son separados por un símbolo delimitador (el punto), en el caso anterior, el dominio UNAM pertenece al dominio mx(México).

Para realizar la conversión de nombres a direcciones IP, se utiliza un servidor de dominio. Los servidores de dominio contienen una lista de posibles direcciones que el usuario puede requerir, en caso de no tenerla, manda la solicitud a otro servidor. Por lo tanto, el sistema de nombre de dominio es un conjunto de protocolos y servicios que nos permiten utilizar nombres, en vez de direcciones IP.³⁹

Si una red LAN tiene acceso a Internet, los DNS deben de estar bien definidos, ya que sin ellos tendremos problemas para encontrar algunas páginas o simplemente no podremos acceder a ningún sitio, aunque nuestra conexión esté establecida.

Es de gran importancia mencionar que los nombres de dominio no sólo se utilizan para Internet, la mayoría de la gente así relaciona el concepto. Un nombre de dominio también se puede relacionar con nuestra propia red, nosotros podemos crear nuestro propio dominio al cual se conectaran los usuarios de nuestra red como es en el caso de Windows 2003 server que cuenta con su servidor DNS y contiene los siguientes parámetros de configuración:

- Nombre del dominio
- Dirección IP del servidor de nombres
- Nombre del servidor

³⁹ http://www.geocities.com/Athens/Olympus/7428/p1_5.html

- Alias del servidor (www, ftp, mail, etc.)
- Registro de apuntadores

Nuestro nombre de dominio puede ser independiente a Internet, o ambos pueden estar relacionados dependiendo de nuestra configuración y necesidades.

4.2.4.6 Puertos y sus protocolos.

Un host puede estar conectado a distintos servicios que le provee la red, como un servidor de mails o un servidor FTP. Para distinguir las distintas conexiones que existen con una computadora, se utilizan los puertos.

Un puerto está formado por 16 bits, si calculamos el número total de puertos que existen, nos dan un total de 65536. Las aplicaciones son las encargadas de usar estos puertos para enviar y recibir mensajes. Por lo tanto, cuando una aplicación quiere mandar un mensaje, busca un puerto libre y lo utiliza

Las aplicaciones cliente, utilizan puertos que son asignados dinámicamente y no menor a 1024, la selección es aleatoria y sólo importa que esté libre. Mientras que las aplicaciones servidoras tienen bien definido el número de puerto de cada uno de los servicios que ofrecen. A continuación enlistaremos algunos de los puertos más conocidos:

Protocolo	Puerto
ftp	21/tcp
telnet	23/tcp
Smtpt	25/tcp
WWW-http	80/tcp
Name Server.	42/tcp/udp
Pop2	109/tcp
Pop3	110/tcp
nntp	119/tcp
Netbios-dgm	138/tcp/udp
Netbios-ssn	139/tcp/udp

Fig. 4,12 Principales puertos.

Describiendo a los protocolos de los puertos mencionados tenemos:

Telnet.

Telnet es un protocolo de conexión que fue la base para el protocolo FTP Y HTTP, es una herramienta de la capa de aplicación. El formato de las direcciones Telnet consta del nombre de dominio ó dirección IP y el número de puerto, como por ejemplo; pop.prodigy.net.mx 110 ó lo que es lo mismo, 148.235.52.60. 110. En Telnet se puede acceder y consultar a un dominio en específico, actualmente se sigue utilizando para consulta de bases de datos, comúnmente en consultas de cuentas de correo electrónico.

Existen otros protocolos de aplicación similares a Telnet que a su vez se ejecutan por medio de comandos, como el comando ping, una herramienta que nos sirve para verificar que un determinado dominio está respondiendo a nuestra petición, tenemos también el tracert, que nos permite realizar trazas de ruteo hacia un dominio específico ó dirección IP indicándonos los nodos por los que pasan dentro de una red.

FTP (File Transfer Protocol, Protocolo de Transferencia de archivos).

El objetivo de este protocolo es compartir archivos de forma remota entre computadoras, transfiriendo datos de una forma segura y optima.

El FTP es utilizado directamente por las aplicaciones para generar una transferencia de archivo a la hora que el usuario las requiera, sin preocuparse que en el nodo origen exista una computadora Mac o PC, las cuales son plataformas distintas. Gracias a esto no se necesita saber mucho sobre el nodo origen y se logra lo que se quiere.

Normalmente los usuarios de una red utilizan el programa cliente FTP para acceder a un servidor FTP, debido a que los programas servidores FTP no se encuentran en los ordenadores personales. Un ejemplo de un programa cliente FTP son los navegadores de Internet que conocemos, como el Internet Explorer y el Netscape.⁴⁰

HTTP (Hyper Text Transfer Protocol, Protocolo de transferencia de hipertexto).

Este protocolo se utiliza en la transferencia de hipertextos, y es usado por todos los sistemas de información que necesiten una distribución, o sea que desean mostrar o publicar información. La comunicación se realiza respetando el uso de ligas que utiliza este lenguaje.

El HTTP basa su funcionamiento en sencillas operaciones de solicitud y respuesta. Un cliente establece una conexión con un servidor y envía un mensaje con los datos de la solicitud. El servidor responde con un mensaje similar, que

⁴⁰ <http://www.uv.es/ciuv/cas/web/ftp.html#quees>

contiene el estado de la operación y su posible resultado. Todas las operaciones pueden adjuntar un objeto o recurso sobre el que operan. Los objetos son documentos en formato HTML, ficheros multimedia y aplicaciones.⁴¹

POP3. (Post Office Protocol Version 3, Protocolo de oficina Postal versión 3).

EL protocolo POP3 se encarga de hacernos llegar los correos electrónicos. Es como el cartero cuando nos trae la correspondencia. El servidor almacena los correos hasta que hay una conexión con el, los correos son almacenados en nuestra máquina después de su descarga, por lo que es más fácil de administrarlos y organizarlos. Los servicios de correo electrónico de este tipo son proporcionados por las compañías proveedoras de Internet, como Prodigy, Axtel o Terra, por referirse algunas de ellas que suministran el servicio en México.

La entrada en acción del protocolo se realiza cuando un equipo cliente quiere hacer uso del servicio, se establece una conexión TCP con el servidor, el equipo servidor inicia el servicio POP3 escuchando el puerto 110. Cuando la conexión se ha establecido, el servidor POP3 envía un saludo. El cliente y el servidor POP3 a partir de entonces intercambian órdenes y respuestas hasta que se termine la conexión.

Una sesión POP3 pasa por varios estados durante su periodo de funcionamiento. Una vez que se abre la conexión TCP tras enviar un saludo al servidor POP3, la sesión entra en la fase de AUTORIZACIÓN. En esta fase, el cliente debe identificarse ante el servidor. Una vez que el cliente es autorizado, el servidor adquiere los recursos asociados de su buzón y la sesión entra en la fase de TRANSACCIÓN. En esta fase, el cliente solicita la actuación al servidor POP3 y le son enviados los mensajes a su buzón de entrada, cuando se completa el envío, el cliente da una orden para que sus mensajes sean borrados del servidor (orden QUIT) y la sesión entra de nuevo en fase de AUTORIZACIÓN. En esta fase, el servidor POP3 libera cualquier recurso adquirido durante la fase de transacción borrando los mensajes almacenados, el servidor se despide y se cierra la conexión.⁴²

SMTP(Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo).

De manera contraria al protocolo POP, el protocolo SMTP es utilizado para el envío de correo electrónico, utilizando el puerto 25. SMTP es un protocolo independiente del sistema de transmisión utilizado, dicho sistema, sólo tiene que proporcionar un canal de transmisión que sea fiable y con entrega ordenada, haciéndose valer del protocolo TCP como transporte. Para que dos sistemas intercambien correo mediante el protocolo SMTP no es necesario que exista una

⁴¹ http://cdec.unican.es/libro/servidores_http.htm

⁴² <http://burete.forodigital.es/angel/programacion/Redes/Protocolos/Scp.html>

comunicación interactiva, ya que este protocolo usa métodos de almacenamiento y reenvío mensajes.

El servicio es proporcionado por las compañías proveedoras de Internet y busca que el envío de correo electrónico se realice de una manera confiable y eficiente. Su funcionamiento está basado en el manejo de dominios y entra en acción cuando una aplicación envía un mensaje de correo, el cual debe de estar formado por la dirección, el asunto y el contenido del mensaje. En la siguiente figura esquematizamos la entrega de correo a través de servidores SMTP:

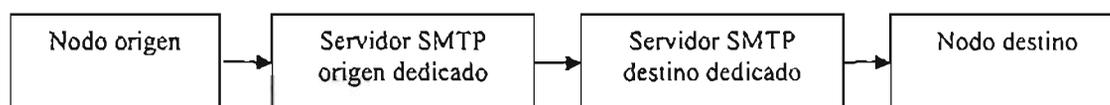


Fig. 4,13 Entrega de correo por SMTP.

Como se puede ver en la figura anterior, el envío de un mensaje se realiza por medio de servidores SMTP dedicados, el usuario origen debe de estar en el dominio para poder utilizar el servicio, es decir, si nuestra cuenta es ingenieria@prodigy.net.mx estamos registrados en el servidor smtp.prodigy.net.mx. La función de este servidor SMTP origen es comunicarse con el servidor SMTP destino para poder enviarle los mensajes que se tienen para él. La búsqueda del servidor origen se realiza mediante nombres de dominio y es necesario que la dirección destino esté registrada para proceder con la entrega de mensajes.

Los puertos poseen una memoria intermedia entre los programas y la red, de tal forma que la información sea guardada temporalmente hasta que pueda ser enviada por la red, de igual forma, en el puerto receptor la información es guardada hasta que la aplicación esté lista para recibirla.⁴³

4.3 Software

4.3.1 Sistemas operativos de red

Una vez que se han instalado los componentes físicos de una red, es necesario contar con un sistema operativo de red que administre y comparta los recursos físicos y lógicos. Como sabemos, un equipo casero no puede trabajar sin un sistema operativo, lo mismo pasa con las redes de computo. En el mercado existen diferentes sistemas operativos de red cada uno con ventajas y desventajas, la elección dependerá de las necesidades y requerimientos de cada una de las empresas u organizaciones. Actualmente los sistemas operativos de red funcionales

⁴³ <http://www.microsoft.com/latam/technet/articulos/200110/art04/default.asp>

son; Netware de Novell, sistema ya con tiempo en el mercado que sigue existiendo en las empresas aunque su tendencia es desaparecer en algunos años debido a que no ha competido a la par con Windows y Linux. De Linux como sabemos es un sistema operativo de distribución libre, eficiente en sistemas de gran robustez con la ventaja de que no pagamos licencia de uso, sin embargo no se cuenta con un soporte técnico certificado, por lo que debemos pagar por el servicio a empresas de soporte externas. Por último, tenemos Windows 2003 Server la última versión hasta el momento de Microsoft, sistema que sigue siendo el más comercial en el mundo, con el que obtenemos un soporte técnico certificado a cambio del pago de la licencia de uso, veamos más a detalle cada uno de ellos.⁴⁴

NetWare de NOVELL

El sistema operativo de red NetWare está formado por aplicaciones de servidor y cliente. La aplicación cliente se diseña para ejecutarse sobre una variedad importante de los sistemas operativos que residen en las estaciones de trabajo. Los usuarios clientes pueden acceder a la aplicación servidor a partir de ordenadores que ejecuten MS-DOS, Microsoft Windows (versiones 3.x, 9x, me, XP Windows NT 2000 y 2003), OS/2, Apple Talk o UNIX. A menudo, NetWare es la opción que se utiliza como sistema operativo en entornos de múltiples sistemas operativos mezclados.

Algunas de las versiones de este sistema operativo son; Netware 3.2, NetWare 4.x y NetWare 5.0

Veamos algunas características importantes de Netware:

- Netware opera en la mayoría de dispositivos de redes que venden los fabricantes más importantes.
- Funciona en distintas topologías lógicas.
- Está diseñado para ofrecer un soporte de servidor de archivos de red.
- Cuenta con un sistema de seguridad que garantiza confidencialidad de la información. Autorizaciones por contraseña, atributos de archivos y directorios.
- Tiene compatibilidad con Windows, por lo que un servidor Windows puede acceder a recursos de archivos e impresión de Netware. (interoperabilidad)
- Envío de mensajes por medio de comandos sencillos.

⁴⁴ <http://www.monografias.com/trabajos5/sisop/sisop.shtml>

UNIX Y LINUX

UNIX es un sistema operativo de propósito general, multiusuario y multitarea. Normalmente, un sistema UNIX está constituido por un equipo central y múltiples terminales para los usuarios. Este sistema operativo incluye las prestaciones de red, diseñado específicamente para grandes redes, pero también presenta algunas aplicaciones para equipos personales. UNIX trabaja bien sobre un equipo autónomo y, como consecuencia de sus posibilidades de multitarea, también lo hace perfectamente en un entorno de red.

El sistema operativo UNIX ha evolucionado mucho en los últimos años, es usado por sus características en la investigación científica.

UNIX es altamente adaptable al entorno cliente/servidor. Se puede transformar en un servidor de archivos instalando el correspondiente software del servidor de archivos. UNIX puede responder a peticiones realizadas en las estaciones de trabajo. El software del servidor de archivos es una aplicación más que se está ejecutando en el equipo multitarea.

Características de UNIX:

- UNIX es el sistema más usado en investigación científica, pero su aplicación en otros entornos ha tenido gran aceptación.
- La versión SVR4 (Sistema V versión 4), es la versión más actualizada del sistema UNIX de AT&T.
- En general, en las máquinas UNIX, los comandos no se ejecutarán físicamente en la computadora en la cual se está tecleando, sino en aquella a la que uno se ha conectado.
- Una computadora UNIX ofrece generalmente una serie de servicios a la red, mediante programas que se ejecutan continuamente llamados daemon.

LINUX es un clon del sistema operativo UNIX que corre en varias plataformas, especialmente en computadoras personales con procesadores Intel 386/486/586 o mejores. LINUX puede convertir cualquier computadora personal en una estación de trabajo con las mejores cualidades de UNIX. Este sistema se ha instalado tanto en negocios y universidades, como para uso personal. Lo que hace a LINUX tan diferente es que es una implementación de UNIX sin costo, además de que maneja un entorno gráfico.⁴⁵

LINUX proporciona una implementación completa del software de red TCP/IP e incluye un ambiente de programación completo que incluye todas las librerías estándar, herramientas de programación, compiladores y depuradores que

⁴⁵ <http://www.monografias.com/trabajos/soredes/soredes.shtml>

se esperarían de otros sistemas UNIX. Existe una gran variedad de software comercial disponible para LINUX. Entre otras características podemos mencionar las más importantes:

- Linux es un clon del sistema operativo UNIX
- Lo que hace a Linux diferente es que es una implementación de UNIX sin costo.
- En Linux se puede correr la mayoría del software popular para UNIX.
- Linux proporciona una implementación completa del software de red TCP/IP.
- Linux soporta consolas virtuales (VC).

WINDOWS 2003 SERVER

En nuestro caso, para la implementación del proyecto de red inalámbrica utilizaremos Windows 2003 Server, Standard Edition , sistema que cuenta con el soporte necesario para cubrir los requerimientos exigidos, con esto no queremos decir que sea el mejor sistema operativo de red existente en el mercado, como se menciono, todo dependerá de la necesidad de la empresa.⁴⁶

Entre las características más importantes que podemos mencionar de Windows 2003 Server tenemos:

- Seguridad, cuenta con una administración de los objetos de la red (Active directory) en donde podemos organizar la información en Bosques, Árboles, Dominios y Unidades organizativas, 2003 es compatible con tecnología Wifi, WEP y WPA.
- Provee confiabilidad, disponibilidad, escalabilidad y rendimiento a nivel empresarial.
- Servidor DNS y servidor DHCP integrado
- Servidor Web integrado
- Menor personal para administración de servidores.
- Simplifica la administración de los usuarios y los recursos de la red.
- Respaldo de archivos de manera automática

⁴⁶ <http://www.microsoft.com/spain/servidores/windowsserver2003/evaluation/overview/default.aspx>

- Acceso a profesionales certificados

4.3.2 Arquitecturas de los sistemas operativos más utilizadas

La arquitectura del Sistema Operativo es de suma importancia en la elección del mismo. Actualmente las arquitecturas más utilizadas son (igual a igual) y (cliente-servidor) ambas disponibles en la familia de Windows.⁴⁷

4.3.2.1 Arquitectura de igual a igual

Las redes de igual a igual surgen de la necesidad que tenían las pequeñas empresas del intercambio de información sin necesidad de invertir en grandes equipos para montar una red.

Sus principales características son:

- Todos los nodos son servidores no dedicados, se pueden compartir archivos y recursos físicos entre todas las computadoras.
- El Sistema Operativo de red se instala en cada nodo, no se requiere de un servidor dedicado.
- La Administración e instalación de la Red es muy sencilla, por lo que no se requiere de personal altamente calificado.
- Su sistema de seguridad es básico, pero puede ser suficiente para aplicaciones pequeñas.
- La principal ventaja de este tipo de redes es que son económicas, sencillas y fáciles de instalar, orientadas a cubrir el mercado de las pequeñas empresas.
- Sus desventajas podrían estibar en su poca seguridad y limitantes de comunicaciones externas.

Las Redes de igual a igual, llenan una necesidad que otras arquitecturas no cubren, que todos los nodos de la red comparten sus recursos, y no solamente servidores dedicados, hoy en día, es común que coexistan: Cliente-Servidor e igual a igual para aprovechar todas las ventajas de estas diferentes arquitecturas. En términos prácticos decimos que tenemos una red de igual a igual cuando nos unimos a un grupo de trabajo, como lo es en el caso del sistema operativo Windows.

⁴⁷ <http://www.geocities.com/SiliconValley/8195/nospp.html>

4.3.2.2 Arquitectura Cliente-Servidor

Cuando hablamos de una arquitectura Cliente-Servidor en primer lugar hablamos de que existe un servidor dedicado, se entiende que hay que aprovechar el o los procesadores del servidor para realizar las tareas más pesadas y las tareas menos pesadas dejárselas al procesador de cada una de las estaciones de trabajo.

En la actualidad la arquitectura Cliente-Servidor, principalmente se explota en servidores de bases de datos que es lo que la mayoría de las empresas necesitan para almacenar su información, algunas otras aplicaciones empleadas son, servidores de comunicaciones y servidores de impresión. Continuamente surgen aplicaciones en este modelo para todos los sistemas operativos de red, utilizándose el proceso distribuido. De igual manera que en la arquitectura de igual a igual, en el sistema operativo Windows decimos que utilizamos la arquitectura cliente-servidor cuando nos unimos a un dominio.⁴⁸

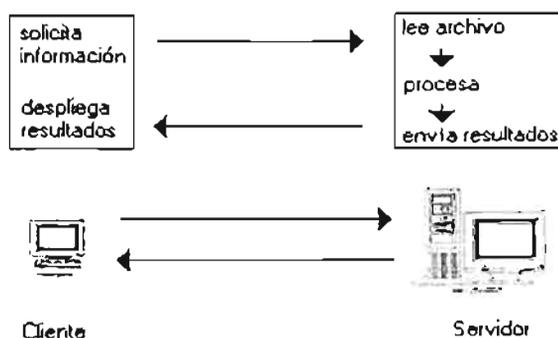


Fig. 4, 14 Arquitectura Cliente-Servidor.

4.4 Etapas para implementar un proyecto de red.

El definir las etapas que involucran a un proyecto de red, nos garantiza la obtención de una red segura y funcional, por lo que no es bueno aventurarse a realizar una red si no se realiza una planeación que contemple todas las variables que pueden surgir durante el montaje y el funcionamiento de la misma.⁴⁹ En la siguiente figura vemos todas las etapas que debemos de considerar para realizar un montaje de red:

⁴⁸ <http://www.geocities.com/SiliconValley/8195/noscs.html>

⁴⁹ <http://www.uaslp.mx>

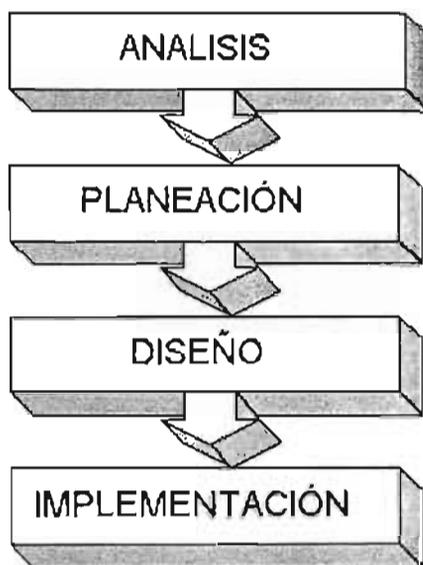


Fig. 4,15 Etapas para implementar un proyecto de red.

4.4.1 Análisis de una red

ANALISIS DE UNA RED
1. <i>Infraestructura física de la empresa.</i>
2. <i>Número, tipo de equipos y convivencia.</i>
3. <i>Ubicación física de los equipos.</i>
4. <i>Requerimientos tecnológicos y aplicaciones</i>
5. <i>Necesidades de acceso a Internet.</i>
6. <i>Presupuesto.</i>
7. <i>Opciones de crecimiento.</i>

Fig. 4,16 Puntos de análisis.

A continuación se detallan cada uno de estos elementos que debemos de tomar en cuenta, para analizar una red WLAN empresarial:

1. Infraestructura física de la empresa. Es muy importante contar con los planos arquitectónicos de la empresa en donde implementaremos la red, con el fin de determinar distancias, ubicaciones de equipos, áreas de trabajo y otros tipos de servicios; como tuberías, cable eléctrico y cable telefónico. Es muy importante tener en cuenta todos los factores que pueden intervenir, con el fin de no perjudicar o perjudicar lo menos posible las instalaciones.

Si se trata de una industria, hospital o áreas de investigación, debemos de conocer todos los factores que se manejan en ella, es decir, no debemos de exponer

cables en lugares donde las temperaturas no son aptas; como hornos, sin la protección adecuada. Debemos de tener presente que las tarjetas WLAN manejan una frecuencia abierta que comparte con algunos equipos industriales, científicos y médicos, que podrían ocasionar interferencias o pérdida de información.

Es necesario conocer el material y el grosor de las paredes o divisiones, ello nos servirá de referencia para considerar el porcentaje de atenuación, al igual que la cobertura de la tecnología utilizada, con el fin de verificar que la información fluya libremente a cada una de las estaciones de trabajo.

2. Número, tipo de equipos y convivencia. Si la empresa cuenta con equipos, debemos de conocer todos los dispositivos y recursos que formarán parte de la red. En nuestro caso, debemos de estar al tanto del número total de equipos que se montaran, con el fin de verificar que la red inalámbrica no rebase el límite de usuarios establecido por la tecnología, que los equipos cumplan con los requerimientos establecidos para poder utilizar una tarjeta wireless y exista una convivencia entre los mismos.

3. Ubicación física de equipos. Debemos de tener presente donde estarán instalados físicamente cada uno de los equipos que van a formar parte de la red y que rango de movilidad van a tener, para repartir los puntos de acceso lo más óptimo posible. Y principalmente tener muy bien contemplado el lugar donde se instalará el servidor y los dispositivos de conectividad. Este punto y los dos anteriores son esenciales en la etapa de análisis de nuestra red, debido a que tienen mucho peso sobre la ruta que tomará el proyecto.

4. Requerimientos tecnológicos y aplicaciones. Con el fin de que el proyecto sea lo más económico y funcional posible, debemos de conocer las necesidades de cada uno de los usuarios. Es necesario saber si manejan gráficos que requieran una gran cantidad de memoria o procesamiento, o sólo documentos de bajo peso que no necesiten grandes requerimientos, con el fin de optimizar al máximo las aplicaciones locales y de red, que cubran las necesidades de cada uno de los usuarios.

5. Necesidades de acceso a Internet. Otro factor importante es el acceso a Internet. Con el fin de optimizar el uso de recursos, un usuario no debe de tener acceso a Internet si no lo necesita, de lo contrario ocasionará problemas de tráfico o de virus. En caso contrario, debemos de tener bien ubicados los usuarios que podrán tener acceso a Internet. Como por ejemplo, un departamento de ventas que necesita estar bien comunicado con sus clientes por correo electrónico.

6. Presupuesto. Como todo en la vida necesitamos conocer el presupuesto con que se cuenta, para adecuar las necesidades y los requerimientos a las opciones tecnológicas.

7. Opciones de crecimiento. Debemos de tomar en cuenta si la red va a crecer a mediano o a largo plazo, con el fin de adecuar la red a las necesidades próximas.

4.4.2 Factores que intervienen en la planeación de una red

PLANEACIÓN DE UNA RED
<i>Evaluación de alternativas tecnológicas:</i> - Medio alámbrico o inalámbrico a utilizar - Servidor - Estaciones de trabajo - Equipos de conectividad a utilizar

Fig. 4, 17 Factores de planeación.

Evaluación de alternativas tecnológicas.

Una vez contemplados los puntos anteriores, debemos de considerar las alternativas tecnológicas que existen en el mercado. Como por ejemplo, el tipo de tarjetas de acceso a red que se instalarán y la velocidad de red. Veamos algunos dispositivos importantes que debemos considerar:

- Nivel y tipo de cableado.
- Marca de tarjetas de red alámbricas o inalámbricas.
- Tipo y marca de Switch o Access Point.
- Ruteadores (si es necesario)
- Marca del servidor, velocidad y capacidad de almacenamiento en disco.
- Computadoras o estaciones de trabajo.

4.4.3 Elementos que intervienen en el diseño de una red

DISEÑO
1.Arquitectura de red: - Mapa de distribución física - Mapa de distribución lógica
2.Configuración de arquitectura de red: - Protocolos - Esquema de direccionamiento - Esquema de nombramiento - Esquema de administración y monitoreo

Fig. 4, 18 Elementos de diseño.

1) Arquitectura de red

Una vez escogidos los dispositivos tecnológicos que se utilizarán, es necesario contemplar la arquitectura de red al igual que la distribución de los equipos. Para ello se necesita un mapa de distribución física de los equipos y otro de distribución lógica.

Mapa de distribución física. Este mapa debe incluir distancias, ubicación de equipos y ubicación de nodos y de puntos de acceso, considerando el rango de movilidad de los usuarios y el número de usuarios totales.

Se deben de contemplar las limitaciones físicas de la tecnología que se utilizará, como por ejemplo, verificar que la distancia del cable no rebase su límite establecido o la tarjeta inalámbrica no rebase el rango de distancia de operación.

Mapa de distribución Lógica. En este mapa se debe de mostrar el acceso a los diferentes recursos, como servidores, impresoras, aplicaciones específicas y Internet. Al realizar este diseño es necesario contemplar las limitantes lógicas que pueden surgir, como el tráfico de red y ancho de banda contemplado para las distintas áreas.

2) Configuración de arquitectura de red

Después de definir bien los puntos anteriores, el siguiente paso es contemplar la arquitectura de red con los siguientes puntos:

Protocolos que se utilizarán. Para ello es necesario revisar las diferentes tecnologías que se encuentran en el mercado que garanticen un mejor aprovechamiento de la red, de acuerdo a los requerimientos establecidos.

Esquema de direccionamiento. En base a los protocolos escogidos, debemos de realizar un esquema de direccionamiento lógico que abarque a cada uno de las máquinas de la red.

Esquema de nombramiento. Independientemente de los protocolos escogidos, debemos de establecer un esquema de nombramiento para lo diferentes recursos, como lo son las estaciones de trabajo, servidores e impresoras.

Esquema de administración y monitoreo. Para asegurar el buen funcionamiento de la red es necesario definir una estrategia de administración y monitoreo de los diferentes dispositivos que conforman la red. Como por ejemplo, definir el lugar donde el administrador realizara su trabajo. Si la empresa no cuenta con uno, es buen momento para reclutar a los candidatos o dar un curso de administración al más capaz de la compañía.

4.4.4 Implementación

Una vez que ya analizamos, planeamos y diseñamos nuestra red, lo que procede es poner en marcha la instalación, la etapa de implementación. Es claro que esta etapa es una prueba final de un correcto análisis previo de la red. La implementación nunca se debe de llevar a cabo si no se realiza una previa planeación y diseño de la misma, cosa que muchas empresas pasan por alto, sin percatarse de que pueden realizar una mala implementación, que no explote al máximo los recursos de la misma y que en un futuro no pueda existir un adecuado crecimiento a corto o mediano plazo. Si documentamos toda nuestra red desde al principio, no tendremos problema para darle un buen seguimiento al mantenimiento físico y lógico.

Ahora bien nuestro interés es implementar una red inalámbrica, por lo que en el siguiente y último capítulo detallamos la implementación de la misma.

Capítulo 5. Implementación de una red WLAN empresarial

Como sabemos el objetivo de esta tesis es implementar una red WLAN inalámbrica, en los capítulos anteriores abarcamos los conocimientos mínimos necesarios para poner en marcha una red, mismos que vamos a justificar en este capítulo.

Al igual que los investigadores utilizan el método científico para realizar un proyecto de investigación, nosotros debemos utilizar un método bien estructurado para realizar una implementación de la red, que abarque de forma general las variantes que puedan surgir a lo largo del proyecto, para garantizar su buen funcionamiento.

En la práctica nos podemos encontrar con una gran cantidad de variables: como montar una red desde cero con máquinas nuevas, montar una red con máquinas existentes, extender la red, cambiar el cableado coaxial por par trenzado, sustituir el cable viejo por nuevo, sustituir la infraestructura cableada existente para crear una red inalámbrica, entre otras. En cada una de estas opciones hay una manera de actuar diferente, por lo que debemos de estar preparados para todo.

5.1 Método para implementar una red WLAN empresarial

Hemos dividido el método de implementación de una red en 5 etapas generales mismas que nos ayudaran a realizar el proyecto lo más profesional posible. Lo primero que debemos saber es la problemática a la que nos enfrentamos, para poder planear y actuar.

5.1.1 Etapa de planteamiento del problema

La problemática consiste en montar una red de en una empresa que cambiará de instalaciones, se trata de la empresa ISATEM S.A. que realiza actividades puramente de oficina. La migración se hará a un edificio de 10 pisos, los pisos que se ocuparán son 2: se trata de la mitad del piso 10 y la mitad del piso 5. Por lo que debemos crear una red WLAN que abarque los dos pisos, utilizando la tecnología más viable y confiable que garantice un máximo rendimiento y justifique la inversión. Además se montará un servidor para la administración de la red, por lo que se cambiará de grupo de trabajo a dominio utilizando las herramientas de Windows 2003 Server. Veamos la siguiente figura:

Piso 10
Piso 9
Piso 8
Piso 7
Piso 6
Piso 5
Piso 4
Piso 3
Piso 2
Piso 1
PB

Fig. 5,1 Pisos que se conectarán.

Una vez conocido el problema debemos pensar en como resolverlo y entramos a la siguiente etapa.

5.1.2 Etapa de análisis, planeación y diseño de red

Ahora que conocemos el problema en forma general debemos realizar un estudio o análisis del proyecto para entender el problema específicamente y encontrar la solución más adecuada. En el capítulo anterior vimos los factores que debemos considerar antes de realizar el montaje, mismos que vamos aplicar.

5.1.2.1 Infraestructura de la empresa

El primer paso es realizar una visita a las instalaciones de la empresa para determinar como se elaborará el proyecto. Es necesario obtener los planos o si no se cuenta con ellos, debemos realizar un mapa del lugar.

En nuestro caso, necesitamos el mapa de las oficinas del piso 5 y piso 10. En la figura 5,2 representamos el plano del piso 10, en el cual ya están establecidos los lugares donde estarán las distintas áreas de este piso.

- 1) **Sala de recepción.** Podemos observar que hay una estación de trabajo que ocupará la recepcionista.
- 2) **Sala de juntas.** Aquí no hay ninguna computadora, pero la sala debe de estar lista para que los empleados lleven sus equipos portátiles consigo y puedan ingresar a la red.
- 3) **Comedor.** Aquí tampoco está establecida físicamente ninguna computadora, pero no habrá ningún problema si algún usuario de la red quiera comer y trabajar, o simplemente esperar algún mail urgente.

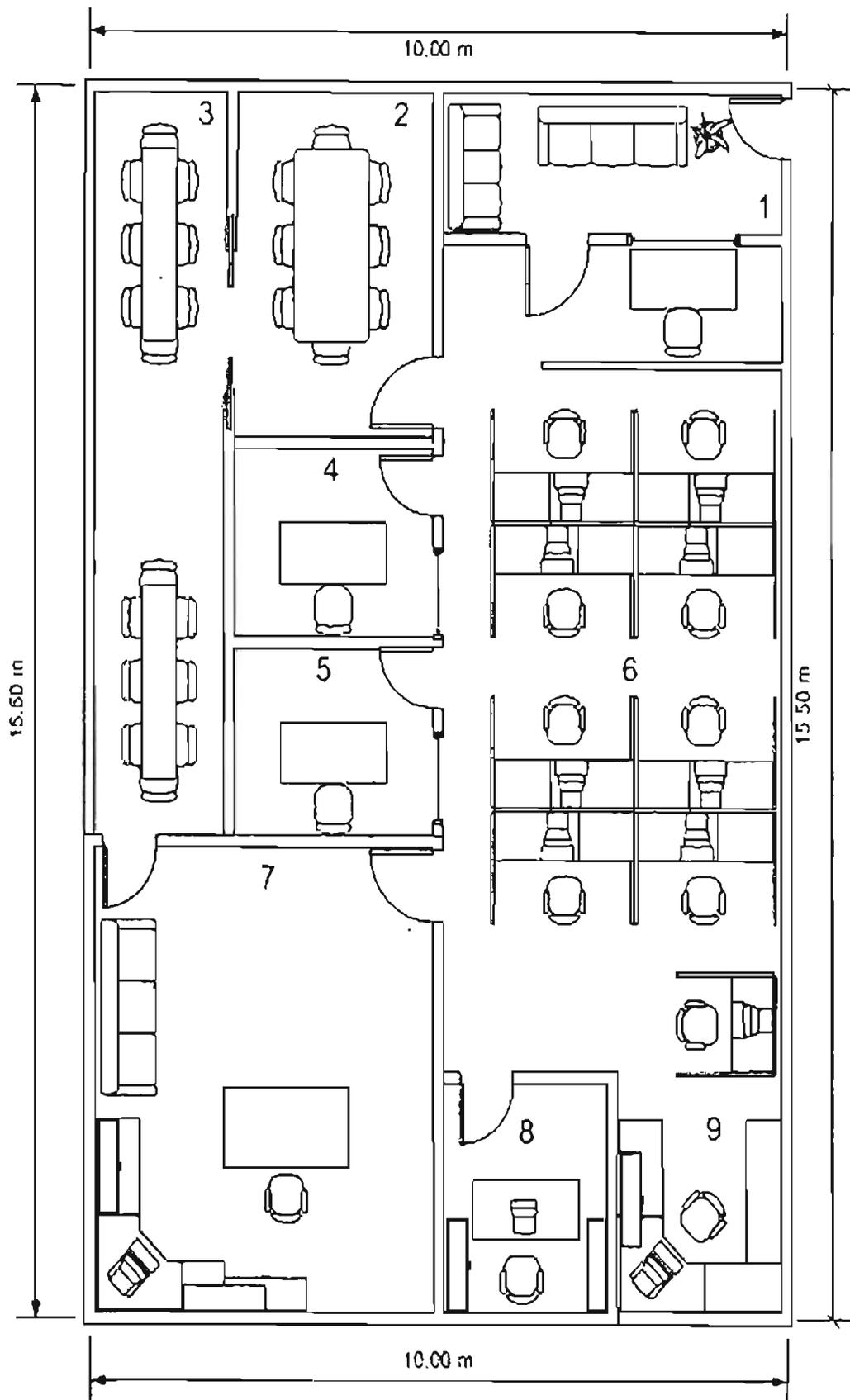


Fig. 5,2 Plano de áreas del piso 10.

- 4) **Contabilidad.** Aquí es la oficina donde estará el contador, por lo tanto se tiene contemplada una estación de trabajo.
- 5) **Administración.** Aquí es donde estará el administrador de la empresa, por lo que hay una computadora más en esta oficina.
- 6) **Área de Operación.** En esta área, se encuentran los empleados de operación, los cuales son 10 y cuentan con sus respectivas máquinas.
- 7) **Dirección.** La oficina principal, donde labora el dueño de la empresa y cuenta con su computadora.
- 8) **Gerencia.** Aquí se encuentra la oficina del gerente y su computadora.
- 9) **Site.** En esta área será el lugar donde estará el servidor y equipos de conectividad.

Si estuviéramos implementando una red cableada, este sería un buen momento para ir tomando medidas y establecer en donde van a quedar cada uno de los nodos y la longitud de cable que ocuparíamos. Pero afortunadamente no es el caso, sólo nos interesa saber el área y los obstáculos que presenta.

Analizando el plano, podemos ver que se trata de un área de 15.5 metros por 10 metros, por lo que cualquier tecnología inalámbrica que comparemos en el capítulo 3 puede cubrir esta área. Sin embargo debemos de considerar que existen divisiones de tabla roca, paredes y muros, que pueden reducir el nivel óptimo de la señal. Analicemos cada una de las áreas con las que cuenta el piso cinco:

- 10) **Oficina de almacén.** En ella estará el almacenista el cual cuenta con una computadora que se integrará a la red.
- 11) **Almacén.** En esta área no se tiene contemplada una estación de trabajo.
- 12) **Archivo general.** Tampoco aquí se tiene contemplada una estación de trabajo.
- 13) **Área de pruebas.** En este lugar no se tiene contemplada ninguna estación de trabajo.
- 14) **Servicio técnico 1.** En esta área se encontrará una de las oficinas de los dos integrantes de servicio técnico, el cual debe contar con una estación de trabajo.
- 15) **Servicio técnico 2.** Aquí estará el otro integrante de servicio técnico y su estación de trabajo.
- 16) **Sección con función no asignada.**

La figura 5,3 representa el piso 5, en el cual también están establecidas las distintas áreas de trabajo.

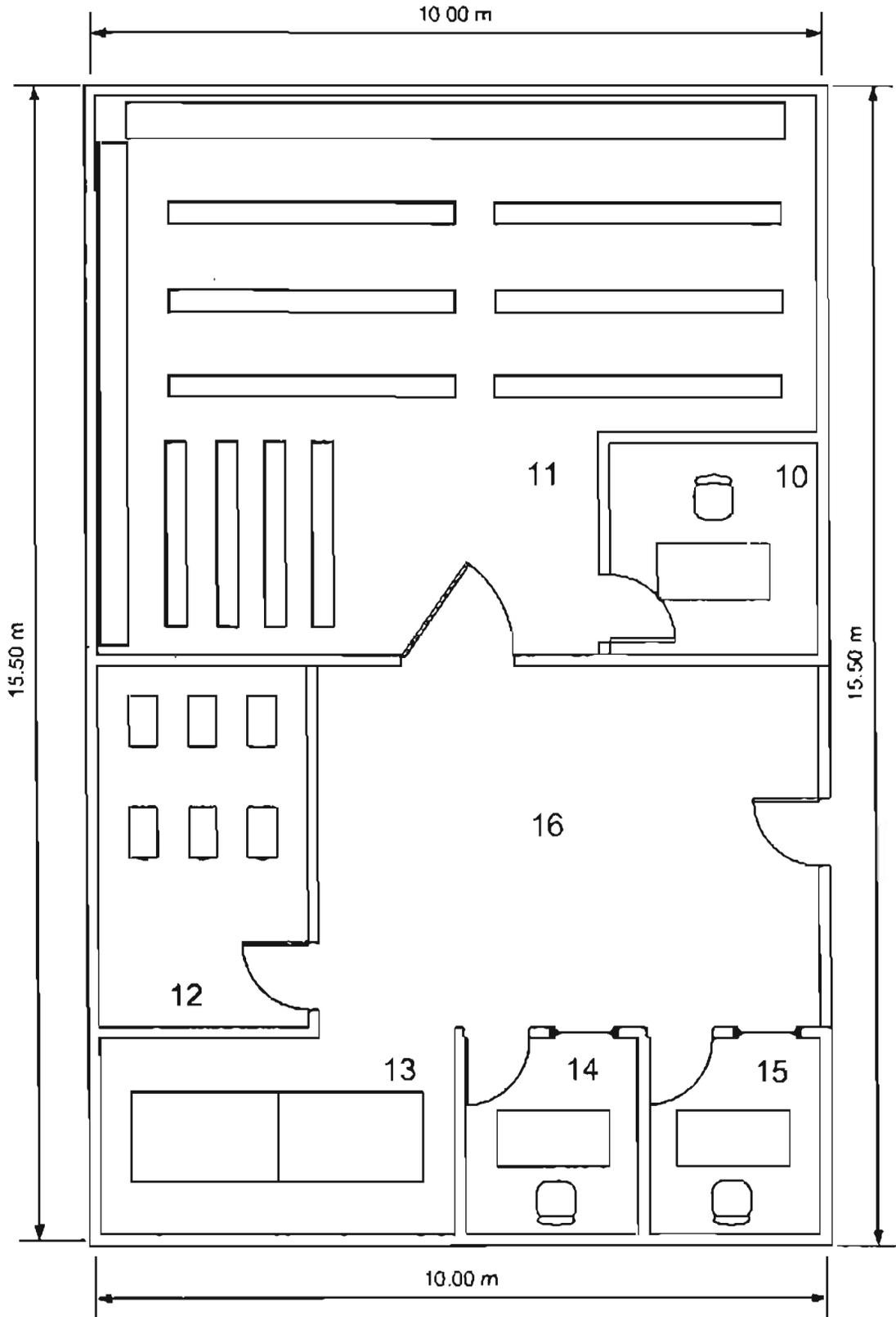


Fig. 5,3 Plano de áreas del piso 5.

Debemos dejar en claro que hay algunas áreas donde no se tiene contemplada una estación de trabajo, pero eso no quiere decir que no pueda entrar a la red mientras se está en ese sitio, sin duda es una de las ventajas de las redes inalámbricas.

Analizando de forma general las instalaciones, podemos decir que la empresa no tiene áreas de riesgo, como en algunas industrias, donde se maneja maquinaria peligrosa, por lo que esto acelera el montaje del proyecto.

Tampoco maneja aparatos o instrumentación que pueda intervenir con las ondas de radio frecuencia, como en el caso de algunos hospitales, lo que facilita las cosas.

En el aspecto de material de separación tenemos los siguientes tipos:

- Paredes de tabla roca que conforman cada una de las oficinas.
- Paneles de madera que dividen los cubículos de la zona 6.
- Paredes de tabique que delimitan el área de las oficinas.
- Ventanas de vidrio y puertas de madera.
- Planchas de concreto, que separan a cada uno de los pisos del edificio.

5.1.2.2 Características, ubicación de los equipos y requerimientos tecnológicos de los usuarios.

Ahora bien debemos hacer un cuadro donde aparezcan el número de equipos que se van a utilizar, características, el área donde se ubicarán y requerimientos tecnológicos de los usuarios.

Equipo	características	Ubicación	Requerimientos tecnológicos.
1	Dell C800 PIII 850 Mhz, 256 MB RAM y 20 GB.	Zona 1	Acceso a Internet y correo electrónico, Windows XP y Office 2003.
2	HP Compaq Business nx9030, Intel Pentium M 725 1.6 GHz, 512 MB y 40 GB en disco.	Zona 4	Acceso a Internet y correo electrónico, Windows XP y Office 2003.
3	HP Compaq Business nx9030, Intel Pentium M 725 1.6 GHz, 512 MB y 40 GB en disco.	Zona 5	Acceso a Internet y correo electrónico, Windows XP y Office 2003.
4	Fujitsu MX 400, AMD XP 1,4 Ghz. 512 MB y 40 GB en disco duro.	Zona 6	Acceso a Internet y correo electrónico, Windows XP y Office 2003.

5	Fujitsu MX 400, AMD XP 1,4 Ghz. 512 MB y 40 GB en disco duro	Zona 6	Acceso a Internet y correo electrónico, Windows XP y Office 2003.
6	Dell C800 PIII 850 Mhz, 256 MB RAM y 20 GB.	Zona 6	Acceso a Internet y correo electrónico, Windows XP y Office 2003.
7	Dell C800 PIII 850 Mhz, 256 MB RAM y 20 GB.	Zona 6	Acceso a Internet y correo electrónico, Windows XP y Office 2003.
8	Sony VAIO FX876 PIII, 800 Mhz. 128 MB RAM y 20 GB en disco duro.	Zona 6	Acceso a Internet y correo electrónico, Windows XP y Office 2003.
9	Dell C800 PIII 850 Mhz, 256 MB RAM y 20 GB.	Zona 6	Acceso a Internet y correo electrónico, Windows XP y Office 2003.
10	Dell C800 PIII 850 Mhz, 256 MB RAM y 20 GB.	Zona 6	Acceso a Internet y correo electrónico, Windows XP y Office 2003.
11	Sony VAIO FX876 PIII, 800 Mhz. 128 MB RAM y 20 GB en disco duro.	Zona 6	Acceso a Internet y correo electrónico, Windows XP y Office 2003.
12	Sony VAIO FX876 PIII, 800 Mhz. 128 MB RAM y 20 GB en disco duro.	Zona 6	Acceso a Internet y correo electrónico, Windows XP y Office 2003.
13	Sony VAIO FX876 PIII, 800 Mhz. 128 MB RAM y 20 GB en disco duro.	Zona 6	Acceso a Internet y correo electrónico, Windows XP y Office 2003.
14	TravelMate C110, Procesador Centrino 400 Mhz.. DDR-266.	Zona 7	Acceso a Internet y correo electrónico, Windows XP Tablet PC Edition y Office 2003.
15	Fujitsu MX 400, AMD XP 1,4 Ghz. 512 MB y 40 GB en disco duro.	Zona 8	Acceso a Internet y correo electrónico, Windows XP y Office 2003.
16	Fujitsu MX 400, AMD XP 1,4 Ghz. 512 MB y 40 GB en disco duro.	Zona 9	Acceso a Internet y correo electrónico, Windows XP y Office 2003.
17	PowerEdge 420SC SCI, 2,8 GHz. DDR- 1 Gb, 2 discos SCSI 36 Gb.	Zona 9	Acceso a Internet y Windows 2003 Server.
18	Dell Dimension 4700, 3 Ghz. 512 MB y 40 GB en disco duro.	Zona 10	Acceso a Internet y correo electrónico, Windows XP y Office 2003.
19	Fujitsu MX 400, AMD XP 1,4 Ghz. 512 MB y 40 GB en disco duro.	Zona 14	Acceso a Internet y correo electrónico, Windows XP, Office 2003 y Corel 10.
20	Fujitsu MX 400, AMD XP 1,4 Ghz. 512 MB y 40 GB en disco duro	Zona 15	Acceso a Internet y correo electrónico, Windows XP, Office 2003 y Corel 10.

Fig. 5,4 Tabla de equipos a instalar y sus características.

Prácticamente, el objetivo del cuadro anterior, es contemplar el número de equipos que van a hacer huéspedes de nuestra red y ubicarlos en las distintas áreas de trabajo, además de contemplar las características de cada uno de ellos para verificar que sean compatibles con la tecnología inalámbrica utilizada y evitar contratiempos de última hora.

El número de equipos que conformarán la red es de 19 contando al servidor. Las características de los equipos son suficientes para utilizar una tarjeta inalámbrica sin problemas.

Es necesario mencionar que las computadoras anteriores a 1999 pueden tener problemas de compatibilidad con el uso de Wireless, dándose el caso de que no se reconozcan las tarjetas, se bloquee el sistema o no funcione adecuadamente, estos casos son muy particulares dependiendo de la marca del equipo y de la versión del BIOS. Lo recomendable es usar equipos que tengan como mínimo un procesador Pentium II o similar con una velocidad mínima de 450 Mhz.

El sistema operativo óptimo para utilizar Wireless es Windows XP, Windows Me, Windows 2000. Windows 98 SE funciona también aunque es recomendable actualizar el sistema a una versión más reciente para obtener un máximo rendimiento. En Windows 95, 98 PE y NT 4.0 no son compatibles, ya que los productos inalámbricos actuales no habían salido al mercado en ese momento. En Linux no hay mucho de donde escoger, los productos que existen son más caros y más difíciles de conseguir.

Ahora que conocemos los puntos que debemos de tomar en cuenta para planear una red, es tiempo de empezar con el diseño de la misma.

5.1.2.3 Evaluación de alternativas tecnológicas

Ya conocemos las características técnicas de cada uno de los equipos, lo siguiente es realizar una evaluación tecnológica de los elementos de enlace. Necesitamos cubrir 2 pisos de 10 x 15.50 metros cada uno, las tecnologías más comerciales son la 802.11b que tiene una cobertura de interior de 50 metros a la redonda y la 802.11g con una cobertura interior de 30 metros a la redonda. El uso de un AP nos extiende la cobertura, al doble entre un equipo y otro, si se encuentra en medio de los dos equipos, veamos la siguiente figura:

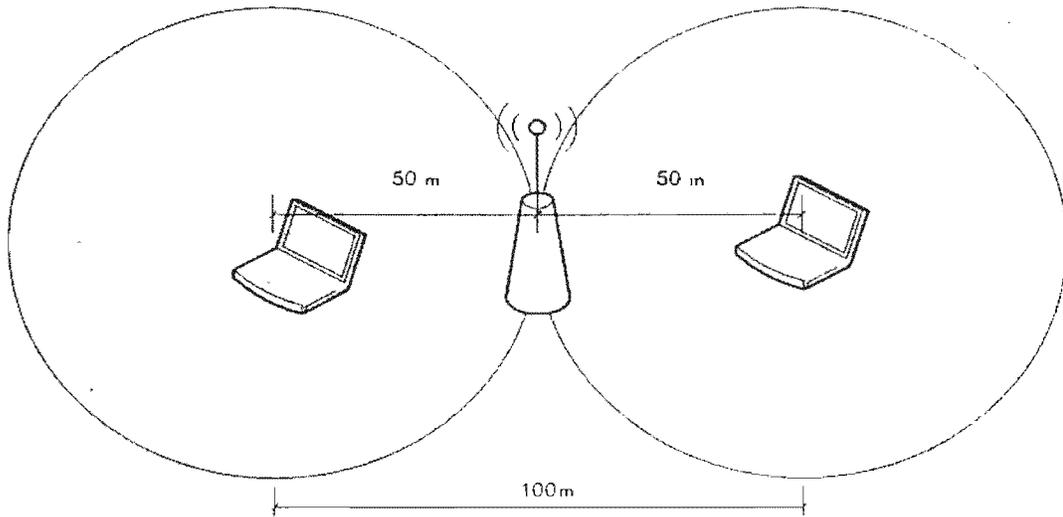


Fig. 5,5 Cobertura interior con AP.

Cualquiera de las dos tecnologías cubre perfectamente con la cobertura que necesitamos, actualmente la norma 802.11g es la tecnología con mayor velocidad de conexión que existe en el mercado mexicano, por lo tanto, es la que vamos a utilizar para realizar el enlace de red.

Ahora es necesario realizar un mapa general del proyecto de red, para determinar todos los elementos que la conformaran en los dos pisos del edificio. Observemos la siguiente figura:

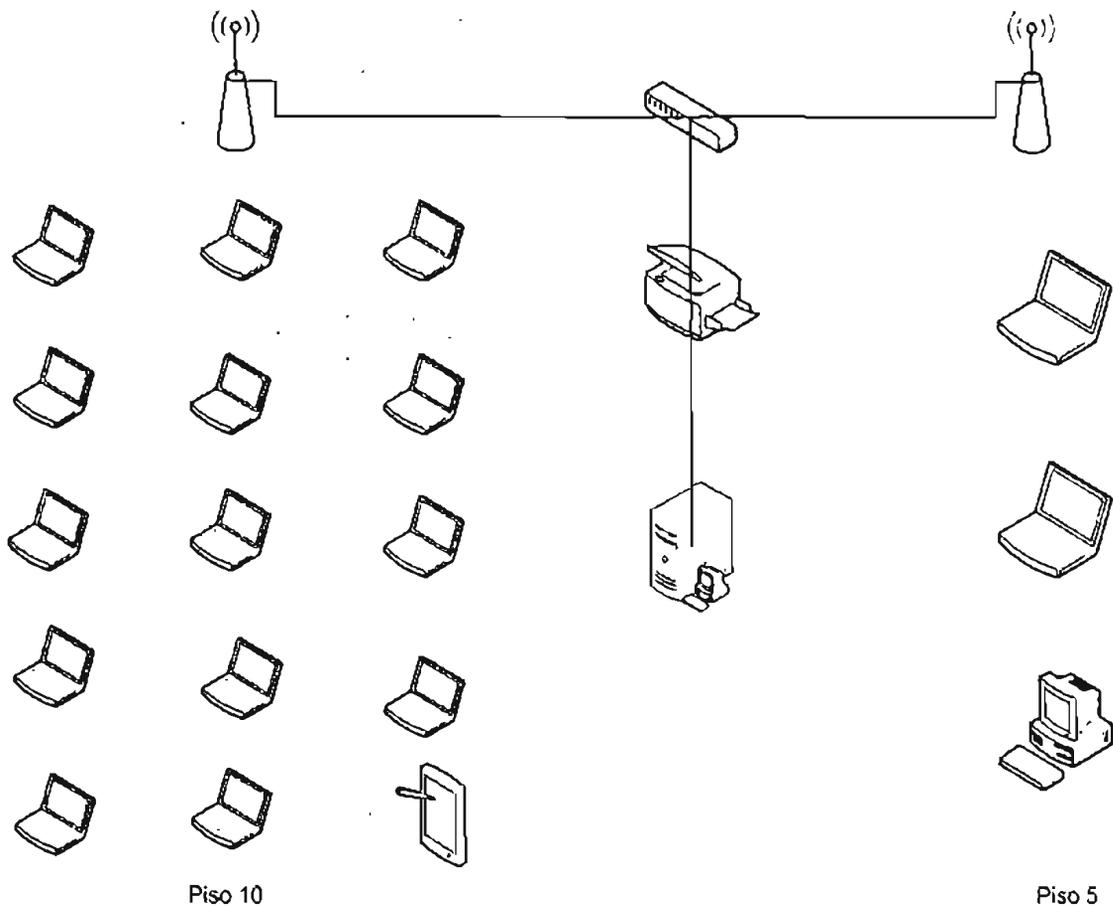


Fig. 5,6 Mapa general de equipos de red.

Como podemos observar en la figura anterior, estamos utilizando una topología en la modalidad de infraestructura, por lo que necesitamos cable para unir los puntos de acceso, la impresora general y el servidor. Aquí puede surgir una pregunta. ¿Por qué razón no ponemos al servidor y a la impresora con acceso inalámbrico? La respuesta es simple, el servidor y la impresora no tienen contemplados una movilidad, pues estarán en un sólo sitio, además de que no es conveniente reducir la velocidad de estos dos dispositivos a la mitad, es decir, tenemos más rendimiento si los dejamos trabajando a 100 Mbps que a 54 Mbps.

Hay una gran variedad de marcas que cuentan con la tecnología G, entre ellos fabricantes como U. S Robotics, Linksys, Cisco Systems, SMC Networks, 3 Com, entre otros. Por lo que ha llegado la hora de escoger un fabricante. Para tomar una decisión debemos de considerar los siguientes aspectos:

- Soporte en México
- Garantía

- Precio
- Experiencia personal en el uso de una marca.

Habrà gente que le parezca mejor una marca que otra, nosotros podemos decir que son fabricantes muy reconocidos en el mercado de redes y que garantizan un buen funcionamiento todos ellos, nos inclinaremos a utilizar Linksys para sacar adelante al proyecto, debido a su buen precio, al soporte que tiene en México y a que hemos trabajado con esta marca con buenos resultados. Veamos el modelo y el tipo que se utilizarán:

Para agregar los equipos portátiles a la red necesitaremos tarjetas PCMCIA, Linksys nos ofrece el modelo WPC540G, el cual nos permite conectarnos a una velocidad máxima de 54 Mbps, con la norma 802.11g y a 22 Mbps con la norma 802.11b, maneja una frecuencia de funcionamiento de 2.4 GHz, Observémosla en la siguiente figura:

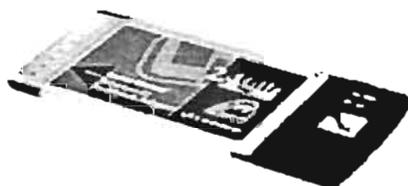


Fig. 5,7 Wireless PCMCIA modelo WPC540G para equipos portátiles.

La misma opción, pero para equipos de escritorio nos ofrece el modelo WMP54G, que vemos a continuación:

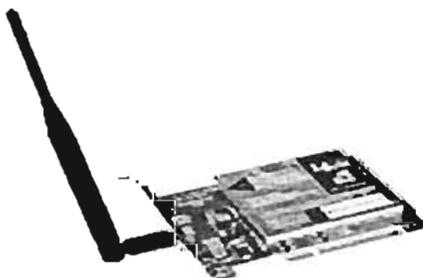


Fig. 5,8 Wireless PCI modelo WMP54G para equipos de escritorio.

Para realizar el enlace inalámbrico, utilizaremos un punto de acceso modelo WAP54G para cada uno de los pisos, es compatible con la norma 802.11g y 802.11b. En la siguiente figura lo podemos ver:



Fig. 5,9 Punto de acceso modelo WAP54G.

Para realizar el enlace cableado utilizaremos, cable UTP categoría 5, para realizar transferencias de datos a 100 Mbps y un Switch marca Linksys EGO08W, que cuenta con 8 puertos RJ-45 y maneja velocidades de 10/100/ y 1000 Mbps. Veamos la siguiente figura:



Fig. 5,7 Switch Linksys EGO08W.

Si se tratara de una red cableada este modelo no nos serviría de mucho, ya que necesitaríamos un Switch de 24 puertos por lo menos, para conectar a los 19 equipos del proyecto. Las redes inalámbricas deshacen las telarañas, por lo que no necesitaremos una panel de parcheo para organizar los cables.

5.1.2.4 Arquitectura de red

Ya que se cuenta con una lista del tipo de equipos que se van instalar y la tecnología de enlace que se va utilizar, es momento de contemplar la arquitectura de la red, para ello es necesario realizar un mapa de distribución física y otro de distribución lógica.

El fin del mapa de distribución física es hacer un diseño previo de donde estarán ubicados cada uno de los equipos, obteniendo la distancia y la movilidad de cada una de las estaciones de trabajo, también se especificarán los puertos utilizados por el Switch para cada uno de los enlaces cableados. En la siguiente tabla asignamos cada uno de los puertos RJ-45 que serán ocupados en el Switch por los recursos o dispositivos de enlace:

Número de puertos	Recursos o dispositivos de enlace
1	servidor
2	Impresora principal
3	Punto de acceso 1
4	Punto de acceso 2
5	Punto de acceso 3
6	Conexión a Internet
7	Libre
8	Libre

La figura 5,8 Tabla de asignación de puertos de Switch.

La figura 5,9 de la página siguiente, representa nuestro mapa de distribución física del piso 10.

**ESTA TESIS NO SALE
DE LA BIBLIOTECA.**

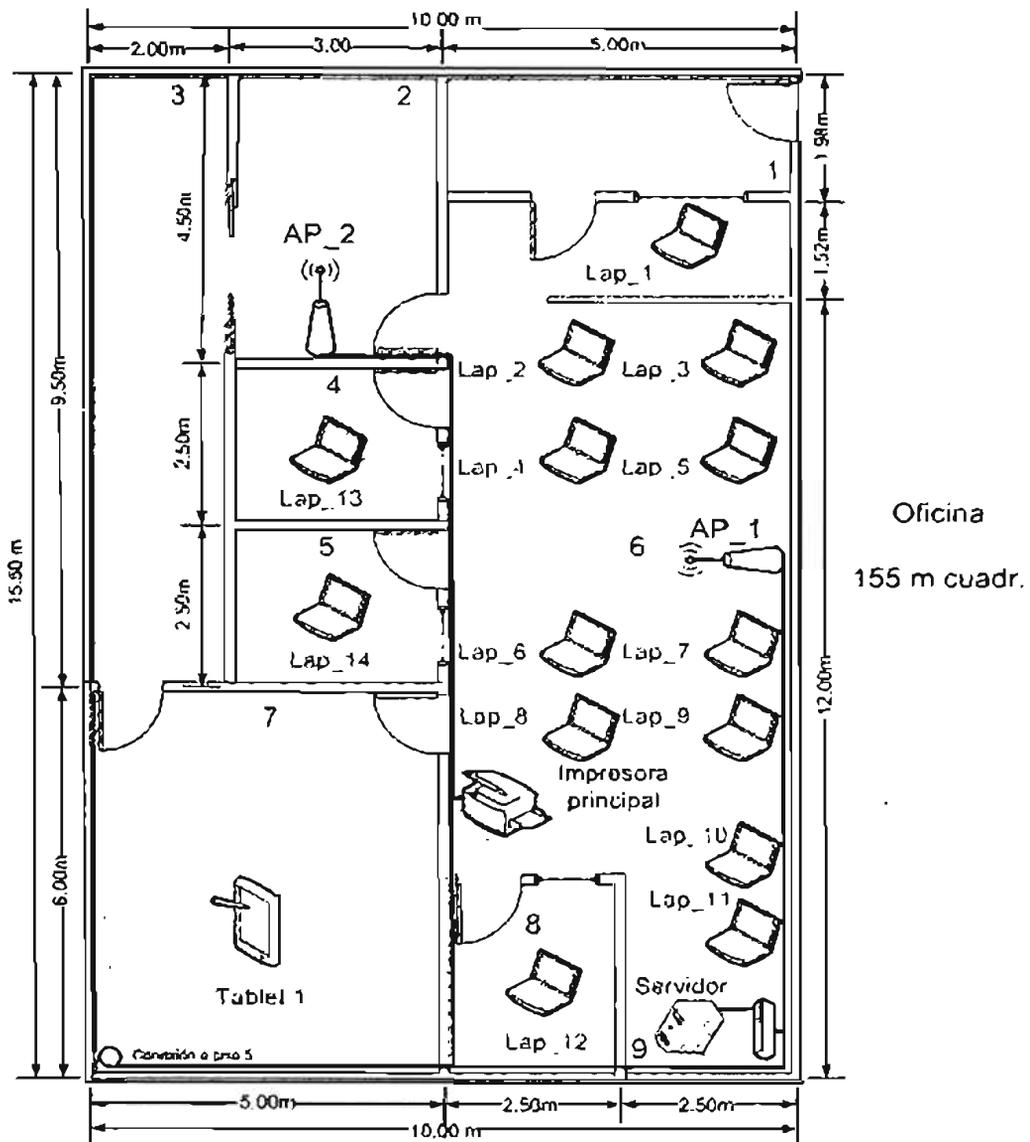


Fig. 5,9 Mapa de distribución física del piso 10.

Podemos observar en la figura anterior que el piso 10 tiene un área de 155 metros cuadrados, la cual es representada por las líneas de sombra, esta zona es cubierta perfectamente por el AP_1 que se encuentra en la zona 6, por lo que cualquier equipo que se encuentre dentro de esta área podrá acceder a la red sin problemas. Vemos también que aparece un segundo punto de acceso AP_2 que se encuentra en la zona 2, el cual no se tenía contemplado, pero tiene el objetivo de dar respaldo al AP_1 y asegurar una perfecta cobertura en la sala de juntas.

El mapa de distribución física cuenta con las medidas suficientes, para poder calcular cuanto cable nos llevaremos para realizar el enlace de recursos y puntos de acceso. Del la zona 9 donde se encuentra nuestro Switch al AP_1 tenemos una distancia recta de 7.75 m, por lo que ocuparemos un cable de 10 metros para este

enlace, mismo que será puesto dentro de una canaleta para protegerlo. Del Switch al AP_2 tenemos una distancia no lineal de 17.5 m, utilizaremos un cable de 20 metros, por último tenemos una impresora general que se encuentra a una distancia no lineal de 5 metros, utilizaremos un cable de 7 metros para el enlace. Si sumamos las distancias de cable obtenemos aproximadamente 37 metros para este piso. En la etapa de montaje definiremos mejor por donde exactamente pasarán los cables y que se debe de hacer para lograrlo. La siguiente figura representa el mapa de distribución física del piso 5:

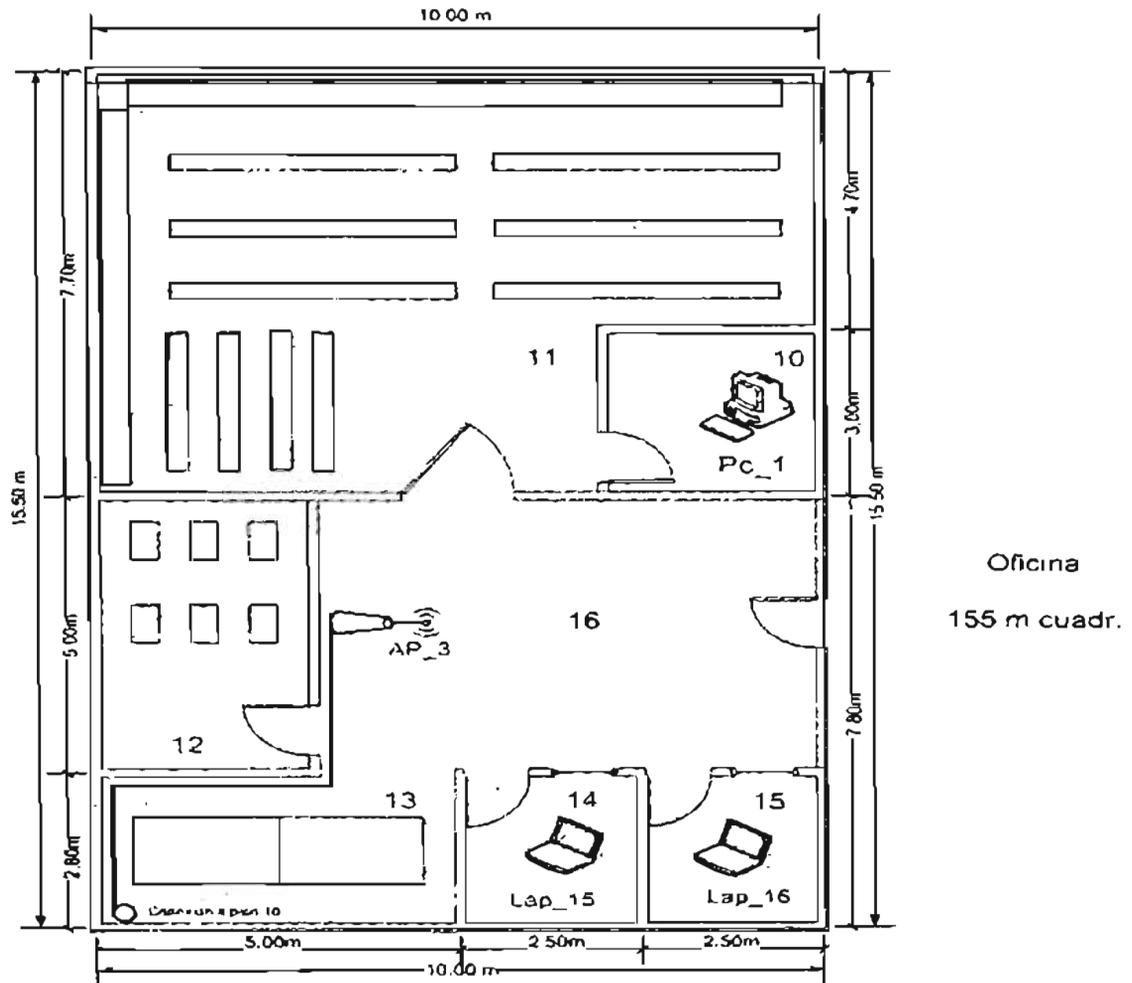


Fig. 5,10 Mapa de distribución física del piso 5.

Observamos que el área es la misma de 155 m² que en el piso 10, por lo que el punto de acceso AP_3 cubrirá sin problemas estas instalaciones. El tráfico de datos es mucho menor que la del piso 10, teniendo 3 computadoras contempladas.

El AP_3 se conectará al Switch de la zona 9, por lo que un cable bajará del piso 10 al piso 5. Desgraciadamente las planchas de concreto que separan a los diferentes pisos no permiten que la señal llegue hasta estas áreas.

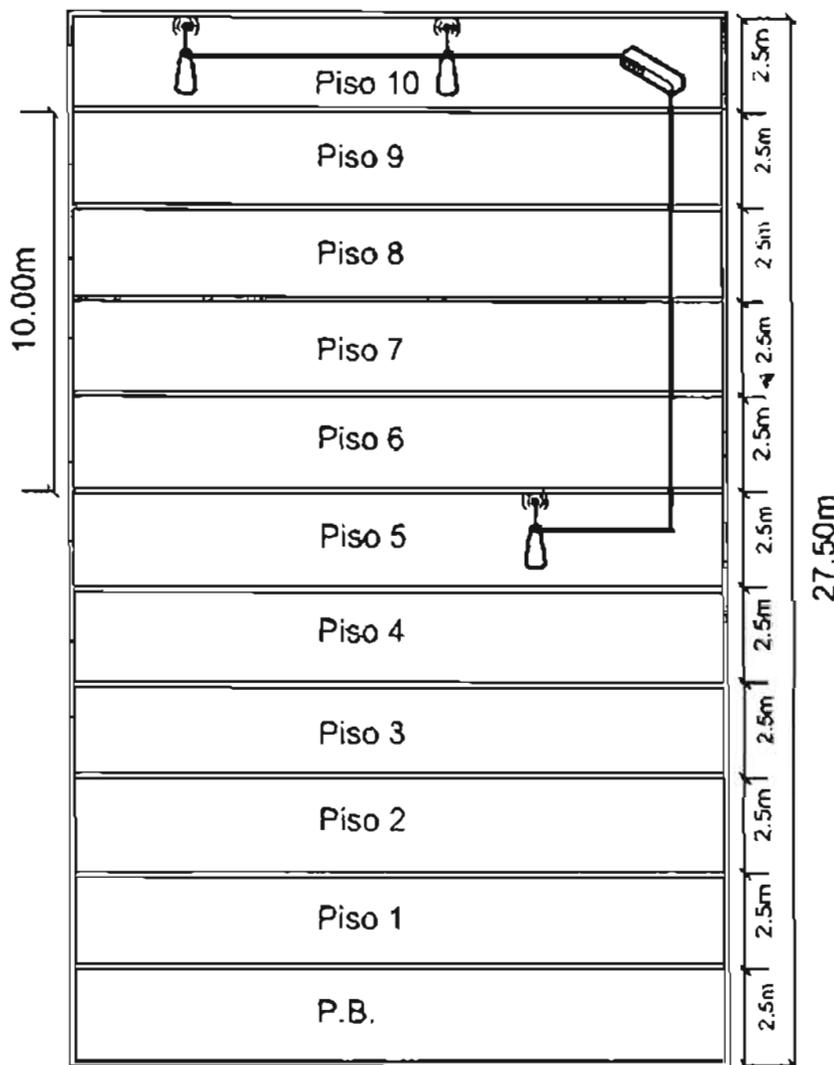


Fig. 5,11 Conexión cableada piso 5 y 10.

La longitud entre el piso 5 y el piso 10, es de 10 metros, en el piso 10 desde el punto de descenso del cable hasta el Switch, es de 12.40 metros, y por último, en el piso 5 desde el punto de ascenso del cable hasta el AP_3, la longitud es de 8.30 metros, esto nos da un total de 30.70 metros, pero utilizaremos un cable de 35 metros para realizar la conexión, dejando 4.30 metros de holgura.

Es recomendable realizar una tabla de las distintas longitudes que se utilizarán de cable, para evitar posibles imprevistos a la hora del montaje, especialmente si se trata de una red puramente cableada, en nuestro caso la haremos para contemplar las longitudes que utilizaremos para unir los dispositivos de enlace inalámbrico y recursos. También tiene el objetivo de realizar un cálculo final del cable utilizado. En la siguiente figura vemos la tabla de longitudes:

Enlace	Longitud
De Switch a AP_1	10 metros
De Switch a AP_2	20 metros
De Switch a Impresora General	7 metros
De Switch a AP_3	35 metros
De Switch a Servidor	2 metros
Total	74 metros

Fig. 5,12 Tabla de longitudes de cable entre dispositivos.

Sin duda esta tabla nos será de gran ayuda a la hora de realizar los cortes en los cables, minimizando los posibles errores, también nos ayuda a verificar que ningún cable rebase el límite establecido de 100 metros.

Lo siguiente es realizar un mapa de distribución lógica, el cual debe contener los recursos y aplicaciones que manejarán los usuarios. Con el fin de verificar que el tráfico sea fluido y sin problemas. Veamos la siguiente figura:

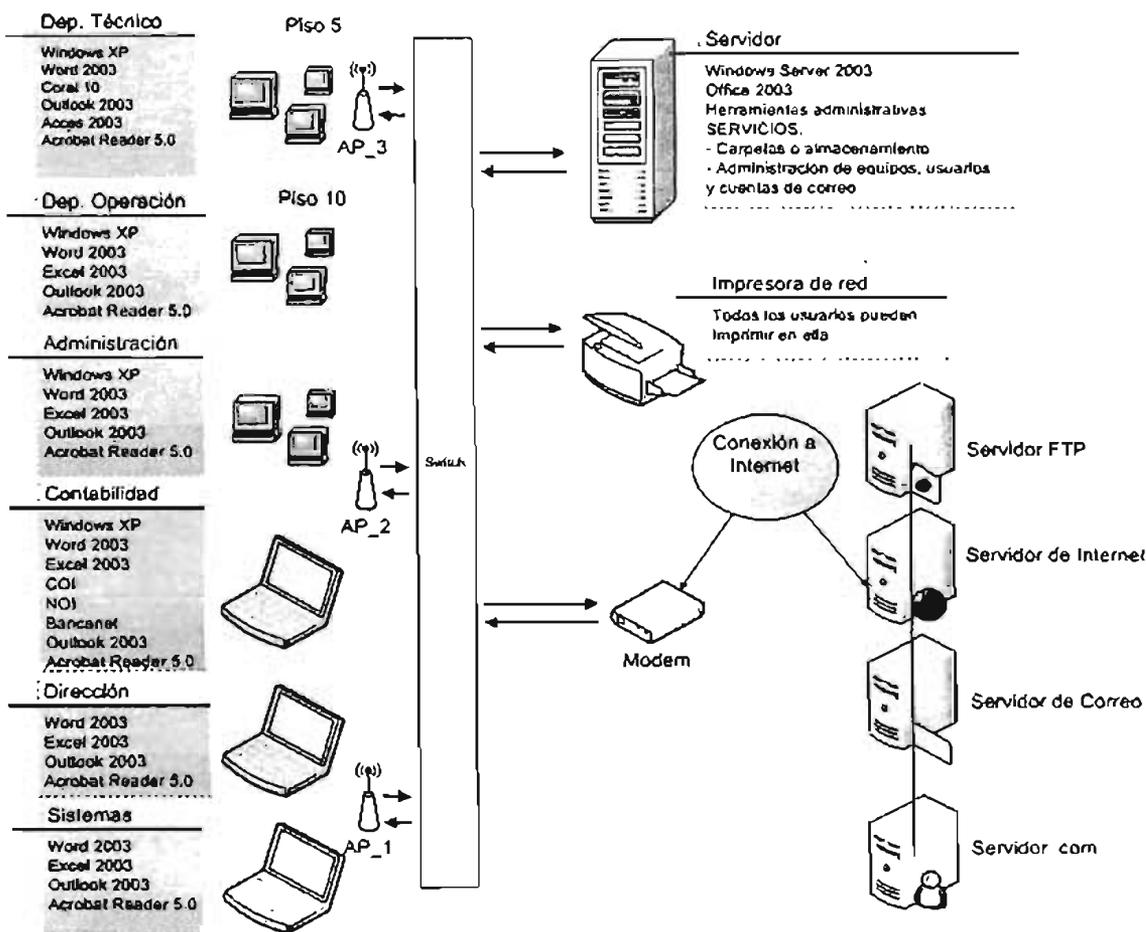


Fig. 5,13 Mapa de distribución lógica.

Observemos que el mapa de distribución lógica fue abarcado por departamentos, debido a que son las mismas aplicaciones que se utilizan en cada uno de ellos. El departamento técnico requiere de un mayor ancho de banda, debido a que se manejan imágenes en Corel. Sin embargo, la velocidad de la red inalámbrica es de 54 Mbps, lo que significa que se reduce en un 46 % de una LAN cableada de 100 Mbps, parece ser mucho pero en verdad no es así, lo importante es el tráfico al que se enfrentará, es decir, el AP_3 atiende sólo a 3 equipos, por lo que el riesgo de tráfico es mínimo, ya que la posibilidad de que los tres equipos transfieran archivos pesados al mismo tiempo es muy baja.

En el piso 10 las cosas cambian, no se tienen contemplado el uso de archivos muy pesados, sólo documentos de Word, Excel, Texto pdf y correo electrónico. Sin embargo el tráfico es mayor, pero la tecnológica nos permite tener conectados hasta 50 equipos, por lo que no debemos tener problemas con los 15 equipos inalámbricos que tenemos en este piso. A menos que todos los usuarios se pongan a bajar o a transferir música a mismo tiempo, si que la velocidad de la red bajaría considerablemente. El AP_1 puede manipular toda la información en el piso 10, sin embargo se agregó el AP_2 como medida de seguridad y como medida para evitar el posible congestionamiento del AP_1.

Referente a los recursos, podemos decir que todos los usuarios tendrán derecho de utilizar la impresora general y el acceso a Internet, la red debe de estar preparada para hacer este trabajo, ya que de lo contrario no tendría sentido utilizar esta tecnología.

5.1.2.5 Configuración de arquitectura de red

Lo siguiente es definir los protocolos que se van a utilizar para realizar la comunicación de red. La verdad no tenemos mucho de donde escoger, la globalización nos lleva a utilizar la familia de protocolos TCP/IP, ya que requerimos de los recursos que nos proporciona, como lo es la comunicación de los dispositivos de red y servicios de Internet, correo electrónico, FTP entre otros. En el anexo explicamos con más detalle la familia TCP/IP.

Como sabemos, la familia TCP/IP funciona en base a direcciones lógicas llamadas IP, por lo que ha llegado el momento de hacer un esquema de direccionamiento que abarque a cada una de las máquinas que formarán parte de la red. Ello es de vital importancia para llevar un control de direcciones y evitar posibles duplicaciones a la hora de la configuración de los equipos.

Aprovecharemos para realizar la asignación de nombres a cada uno de los recursos y estaciones de trabajo con que contará la red, ello con fines prácticos para ubicar más rápidamente a los equipos y su dirección IP.

Hay muchos estilos para nombrar a los equipos, hay gente que le gusta poner el nombre de los usuarios a los equipos, como por ejemplo: PC_lupita o Laptop_pepe, eso es muy práctico para ubicar a los usuarios y a sus computadoras, pero resulta contra productivo, cuando lupita ya no trabaje allí o pepe cambie de departamento, pueden generarse confusiones. Se debe de tener una visión a largo plazo y dar un nombre que no tengamos que cambiar frecuentemente. Por ejemplo, Lap_recepción, con ello entendemos que se trata de un equipo portátil que se encuentra en recepción y así no importa si cambian a la recepcionista, el nombre seguirá siendo el mismo.

La siguiente figura representa nuestro esquema de direccionamiento y nombramiento del piso 10:

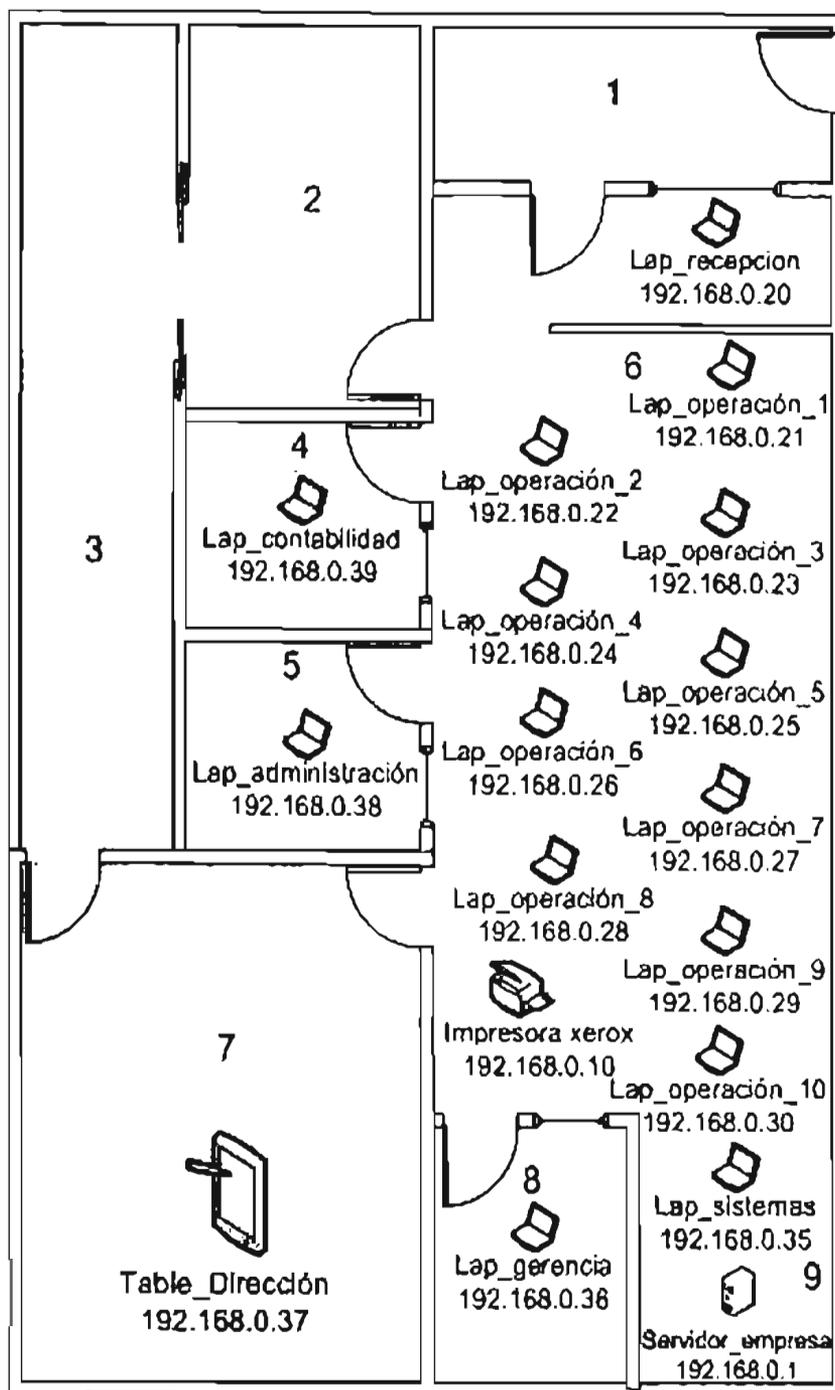


Fig. 5,13 Esquema de direccionamiento y nombramiento del piso 10.

Observemos que cada uno de los equipos tiene el nombre que aparecerá en la red y la IP que les será asignada. Haremos lo mismo con el piso 5, observemos la siguiente figura:

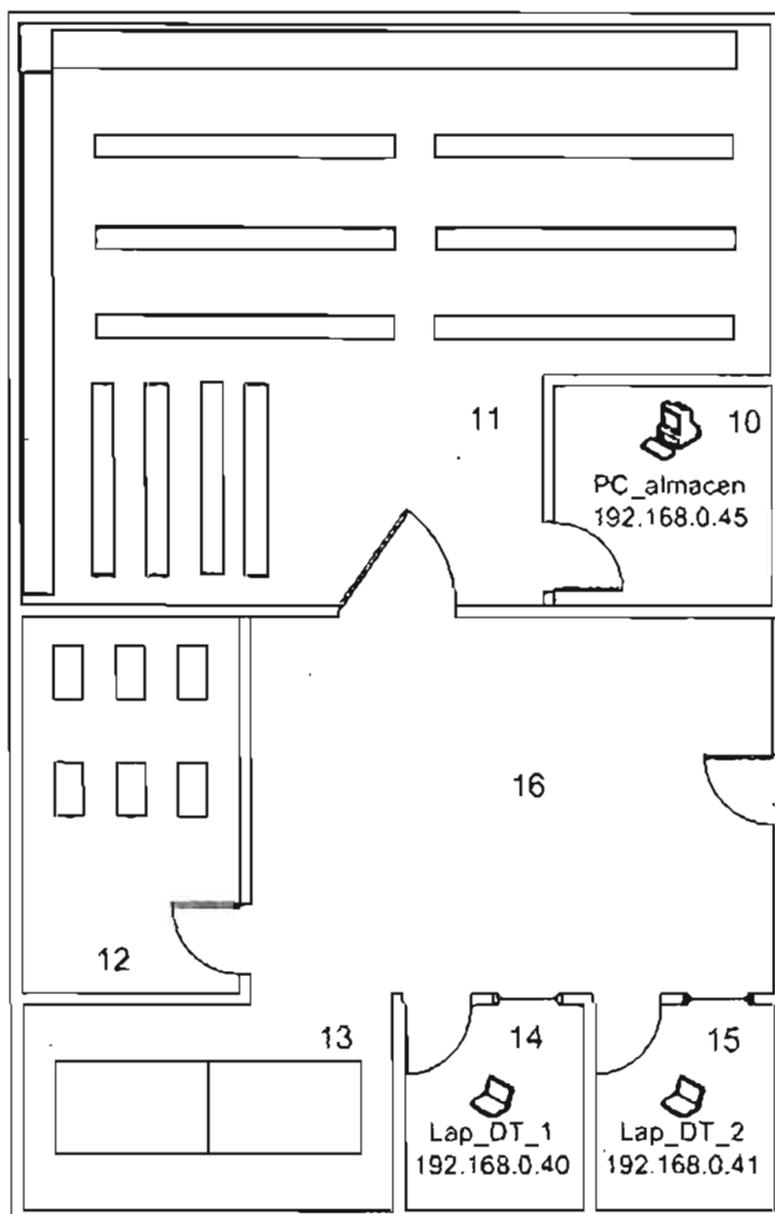


Fig. 5,14 Esquema de direccionamiento y nombramiento del piso 5.

Por último, debemos de brindarle al administrador una lista de los usuarios, la cual debe de contener el nombre del empleado, zona, usuario, clave, IP asignada y nivel de recepción de señal. Ello con el fin que el administrador tenga un informe de todos los movimientos que se realizarán y pueda realizar las operaciones que él considere necesarias, para la administración.

El administrador será la única persona que tendrá acceso total a los recursos de red, por lo que debe de ser una persona de confianza absoluta. La administración de la red será desde la zona 9, en la cual se encuentra el Site.

El modo de administrar la red corresponde al criterio del administrador, nosotros como implementadores, únicamente brindaremos una lista de configuraciones de red, para que se utilice en la administración y monitoreo, dependerá del administrador la forma en que le dará seguimiento a la administración de la red.

La siguiente tabla resume la información de configuraciones principales que se realizarán:

Nombre de usuario	Usuario	Clave	Equipo	IP	Zona	Departamento
Mayra Ramírez G.	mayra	mayra923.	Lap_recepción	192.168.0.20	1	Admon.
Miguel Sánchez R.	miguel	miguel35.	Lap_operación_1	192.168.0.21	6	Operación
Francisco García H.	francisco	fran124.	Lap_operación_2	192.168.0.22	6	Operación
Guadalupe Torrijos F.	lupe	lupe567.	Lap_operación_3	192.168.0.23	6	Operación
Elvia Aguilar T.	elvia	elvia563.	Lap_operación_4	192.168.0.24	6	Operación
Gabriela Aguilar T.	gaby	gaby185.	Lap_operación_5	192.168.0.25	6	Operación
Patricia Cisneros M.	Paty	paty745.	Lap_operación_6	192.168.0.26	6	Operación
Sandra Álvarez E.	sandra	sandra963.	Lap_operación_7	192.168.0.27	6	Operación
Deyfi Santos B	deyfy	deyfy643.	Lap_operación_8	192.168.0.28	6	Operación
Gerardo Montes S.	gerardo	gerar174.	Lap_operación_9	192.168.0.29	6	Operación
Arturo Salcido G	arturo	arturo423.	Lap_operación_10	192.168.0.30	6	Operación
Roberto Juárez G.	robert	robert912.	Lap_sistemas	192.168.0.35	9	Sistemas
Feliciano Manzano R.	feliciano	felici672.	Lap_gerencia	192.168.0.36	8	Admon.
Noel Fernandez C.	noel	noel764.	Lap_dirección	192.168.0.37	7	Dirección
Elizabeth Morales M.	eliza	eliza903.	Lap_administración	192.168.0.38	5	Admon.
Noemi Mendoza T	noemi	noemi245.	Lap_contabilidad	192.168.0.39	4	contabilidad
Javier González H.	javier	javier492.	Lap_DT_1	192.168.0.40	14	Dep. Técnico
Jesús Mercado Z.	jesus	jesus391.	Lap_DT_2	192.168.0.41	15	Dep. Técnico
Genaro Garduño A.	genaro	genaro279.	PC_almacen	192.168.0.45	10	Dep. Técnico
servidor	administrador	isatem123.	Servidorisatem	192.168.0.1	9	Sistemas
Impresora General			Impresora Xerox	193.168.0.10	6	

Fig. 5.15 Tabla de configuraciones de red.

La administración y monitoreo no es tarea fácil, para realizarla necesitamos de varias tablas que guarden información de vital importancia, como claves de usuarios, correos electrónicos y claves de acceso, estadísticas de mantenimientos lógicos y físicos, al igual que utilizar herramientas de software, como historiales de sucesos en los cuales verificamos el funcionamiento adecuado de red.

En una red WLAN tenemos que estar pendientes de que los niveles de recepción y transmisión de datos sean los adecuados, el software de las tarjetas cuenta con gráficas en tiempo real que miden el nivel de señal, ello nos ayudará a mantener un buen desempeño de la red.

5.1.2.6 *Opciones de crecimiento.*

Sabemos que toda red tiende a crecer conforme la empresa lo hace y el trabajo aumenta. Las redes inalámbricas vienen a facilitar las opciones de crecimiento, es decir, ya no nos preocuparemos por agregar un nodo cableado para conectar a un nuevo equipo de cómputo, basta con comprar una tarjeta inalámbrica e instalarla, para que pueda ser miembro de la red. Recordemos que tenemos un límite de 50 usuarios por punto de acceso, lo cual deja una gran holgura de equipos para necesidades futuras.

5.1.2.7 *Presupuesto.*

El presupuesto es uno de los puntos más importantes para montar una red, la empresa debe de contar con los recursos para poder costearla. Por lo que se debe de presentar el proyecto por escrito, con el informe de todo lo que se hará y el costo que tendrá. La empresa lo evaluará y decidirá si procede el montaje o encontró una mejor oferta en otra compañía. Si el proyecto es aprobado es muy importante establecer los días en el que se realizará el montaje, con el fin de no intervenir con las labores de la empresa.

5.1.3 *Etapa de implementación de red.*

Una vez que se tiene aprobado el proyecto, lo siguiente es seguir un plan de trabajo para el montaje de la red inalámbrica, el cual debe adaptarse al tiempo acordado para realizar la implementación. En este caso se tendrá como plazo una semana para concluir con el proyecto, por lo que debemos de tener bien claras las actividades que se realizarán en cada uno de los días. También es importante destinar de cuanto material humano o técnicos será requerido para sacar puntualmente el proyecto.

La siguiente figura representa de forma general en una gráfica de Gantt las actividades que se realizarán:

Día	Actividades	inicio	fin	duración	Sem 2 2005				
					3	4	5	6	7
1	Colocación de canaletas en el piso 5 y piso 10.	03/01/2005	03/01/2005	8h	■				
2	Instalación de parte cableada de red.	04/01/2005	04/01/2005	8h		■			
3	Instalación de switch, puntos de acceso y tarjetas inalámbricas.	05/01/2005	05/01/2005	8h			■		
4	Configuraciones de red y seguridad de la misma.	06/01/2005	06/01/2005	8h				■	
5	Configuraciones finales y prueba de red.	07/01/2005	07/01/2005	8h					■

Fig. 5,16 Tabla de actividades a realizar y gráfica Gantt.

Es momento de explicar más detalladamente lo que se realizará en cada uno de los días, para descartar posibles confusiones.

Día 1. Colocación de canaletas.

Se realiza la colocación de canaletas a 5 centímetros del techo y pegada sobre la pared, en ella viajarán los cables que conforman la parte de enlace cableado, con el fin de que estén protegidos. En algunas partes será necesario la perforación de alguna pared para que el cable pueda pasar, ello se hace en esta etapa.

La primera canaleta va del Switch (zona 9) al AP_1(zona 6), en ella sólo viajará un cable. La segunda canaleta va de la zona 9 al AP_2 (zona 2), tendrá una bajada para la impresora general. El último tramo de canaleta en este piso se unirá a la canaleta anterior (en la zona 7) hasta el punto de conexión del piso 5 (zona 8). En la figura 5,9 y 5,10 nos aclaran mejor por donde pasarán las canaletas que llevan los cables.

Las canaletas son de PVC y se fijan con un pegamento especial, la caja del jack se atornilla a la pared. En la siguiente figura se ejemplifica como debe de ir la canaleta en el caso de la impresora general.

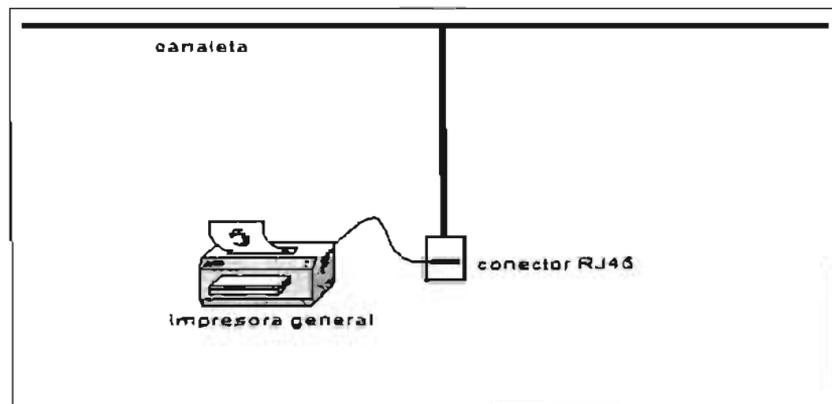


Fig. 5,17 Canaleta en la impresora general.

En el piso 5 sólo hay un tramo de canaleta que va desde el punto de conexión a piso 10 (zona 13) al AP_3 de la zona 16. Veamos la siguiente figura:

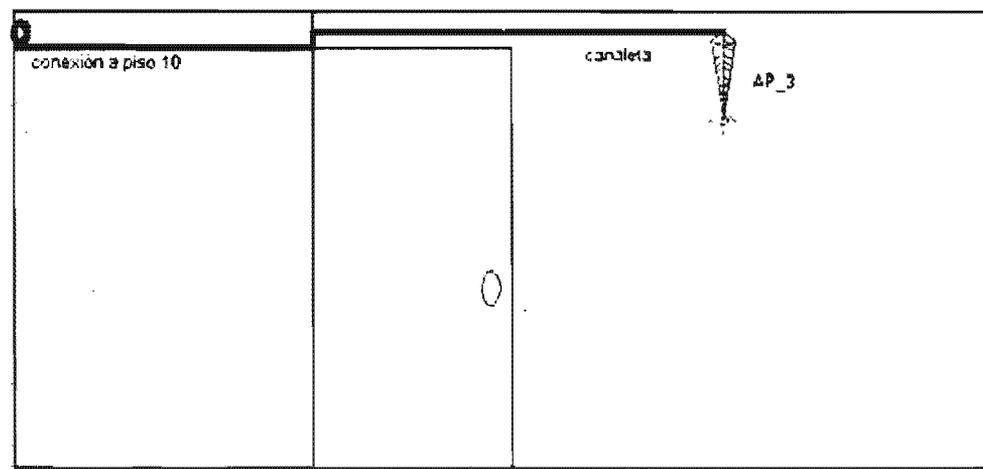


Fig. 5,18 Canaleta en el AP_3.

Una vez concluida la colocación de la estructura de canaletas, se deja que el pegamento actúe y queden bien fijadas a la pared. Aquí se da por terminado el primer día.

Día 2. Instalación de cableado.

Una vez que tenemos las canaletas bien fijadas, lo siguiente es introducir los cables dentro de ellas, para ello primeramente debemos de realizar los cortes que se tienen contemplados para cada uno de los dispositivos, debemos tener mucho cuidado en respetar las longitudes calculadas con anterioridad en la figura 5,12. En el caso, de que durante la marcha se tenga que modificar la extensión del cable, por los motivos que no se habían considerado, lo que se recomienda es medir la distancia con el cable mismo y hacer el corte cuando llegue al extremo requerido, dejando un rango de 1 a 2 metros de holgura por punta. Recordemos que más vale que sobre y no que falte.

Una vez introducido el cable, lo siguiente es realizar la ponchadura, es decir colocar los conectores RJ45 en los extremos del cable, al igual que instalar los jacks. El caso más difícil es la conexión del switch al AP_3, ya que tiene que bajar 4 pisos. El cable bajará por una sección con la que cuenta el edificio, donde se encuentran cables eléctricos y líneas telefónicas, para ello utilizaremos una guía de alambre que nos ayudara a bajar el cable, una vez que la guía llego al piso 5, se amarra el cable y se desliza hacia abajo, se introduce el cable dentro de las canaletas en los pisos correspondientes y se pone un conector RJ45 en cada una de las puntas.

Otro aspecto importante que debemos manejar con cuidado, es respetar la norma de colores en el ponchado, con ello garantizamos el buen funcionamiento del mismo y un buen mantenimiento.

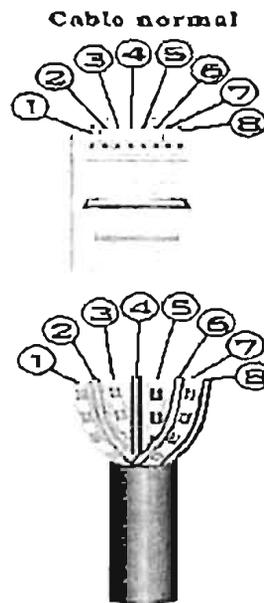


Fig. 5,19 Estándar de ponchado de UTP.

Observemos en la figura anterior la forma en que deben de ir los hilos para una conexión normal. Los pines quedan de la siguiente manera:

- Pin 1. Blanco-naranja
- Pin 2. Naranja
- Pin 3. Blanco-verde
- Pin 4. Azul
- Pin 5. Blanco-azul.
- Pin 6. Verde
- Pin 7. Blanco-café
- Pin 8. Café.

La norma de colores obedece al estándar 568-B, existe otra norma 568-A, pero trabajaremos con la primera, ya que su uso es más común.⁵⁰

En el caso del jack, debe de contar con una guía de donde van cada uno de los hilos dependiendo de la norma que trabajemos. Veamos la siguiente figura:

⁵⁰ http://www.ugr.es/~amroldan/utilidades/cableado/cables_rj45/rj45.htm#normal

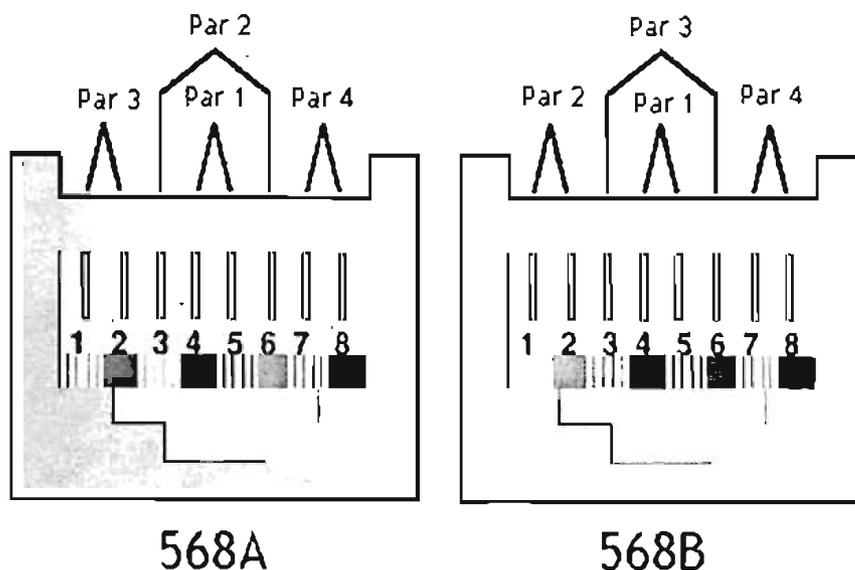


Fig. 5,20 Normas para el Jack RJ45.

Una vez colocado todo el cableado, debemos de verificar cada uno de los cables colocados, para ello necesitaremos de un probador de cables que verifique los 4 pares del UTP, si las pruebas son lo esperado, damos por concluido el día y pasamos a la siguiente etapa del montaje.

Día 3. Instalación de dispositivos de enlace.

Ahora es momento de colocar los dispositivos de enlace e instalarlos, lo primero que pondremos serán cada uno de los puntos de acceso, para ello, tenemos que fijarlos en la pared, es recomendable atornillarlos para mayor seguridad. Una vez colocados, lo siguiente es conectar el switch, también es necesario fijarlo en un lugar seguro, en este caso usaremos belcro para asegurarlo a la mesa.

Lo siguiente es realizar la conexión y la configuración de cada uno de los puntos de acceso, para ello necesitaremos conectar una computadora cualquiera al switch para empezar a realizar las configuraciones. Es recomendable realizar la instalación y prueba de cada uno de los puntos de acceso en forma independiente, es decir, una vez instalado el primer AP se continua con el siguiente. En el software, se deben de visualizar cada uno de los puntos de acceso instalados, el reconocimiento debe de ser automático, en caso de que no sea así, se puede realizar manualmente capturando un código único que posee cada AP.

El nombre que tendrá cada punto de acceso serán los que hemos venido manejando hasta el momento y se conectarán a cada uno de los puertos asignados para ello, es decir, el AP_1 al puerto 3, el AP_2 al puerto 4 y el AP_3 al puerto 5. Lo mismo será para el servidor y la impresora general, puerto 1 y puerto 2 respectivamente.

Aunque no son muchos los cables que se utilizarán, no está demás etiquetar cada uno de ellos con el nombre del dispositivo que se esté conectando.

Una vez instalados los puntos de acceso, el paso siguiente es instalar las tarjetas inalámbricas. Algunas de las computadoras personales ya cuentan con wireless instalados de fábrica, se recomienda deshabilitarlos para que no interfieran con las nuevas tarjetas. Una vez hecho esto, se instala el software y se inserta la tarjeta PCMCIA o PCI en la computadora, se reinicia el equipo y listo. Las configuraciones las dejamos automáticamente por el momento, las computadoras buscarán el punto de acceso más cercano para conectarse a la red.

Ya culminada la instalación en los 20 equipos, verificamos que puedan acceder a la red, debemos de ver en el entorno de red a cada una de las computadoras conectadas. Superada la prueba damos por terminada esta etapa. Aquí damos por terminado el montaje de red, el siguiente paso es realizar la configuraciones de red y seguridad de la misma.

5.1.4 Configuración y seguridad de red.

Es muy importante tener a una red configurada adecuadamente, con ello aseguramos un buen desempeño de la misma. El servidor nos ayuda a administrar la red y tener una mayor seguridad en la administración de usuarios, equipos y recursos.

Día 4. Configuración de red y seguridad de la misma.

Paso 1. Instalación de servidor y herramientas administrativas.

El primer paso es la instalación del servidor Dell PowerEdge 420SC y el sistema operativo junto con las herramientas administrativas. Instalaremos Windows 2003 Server como sistema operativo de red. Primeramente conectamos el servidor a la línea de energía, insertemos el disco de instalación y nos dejamos guiar por el programa de instalación, cuidando que el nombre del servidor sea "servidorisatem" tal como lo habíamos planeado anteriormente. Una vez concluida la instalación de Windows 2003 Server, agregamos las herramientas administrativas que nos ayudaran en la administración de la red, la herramienta más importante es el directorio activo (active directory) el cual nos sirve para Organizar, Administrar y Controlar recursos y lograr una administración centralizada en el servidor. En el directorio activo podemos crear de forma jerárquica; Bosques, Árboles, Dominios y Unidades organizativas.

Para agregar las herramientas administrativas, debemos dar clic en la opción "administre su servidor" y obtendremos una pantalla como la siguiente:

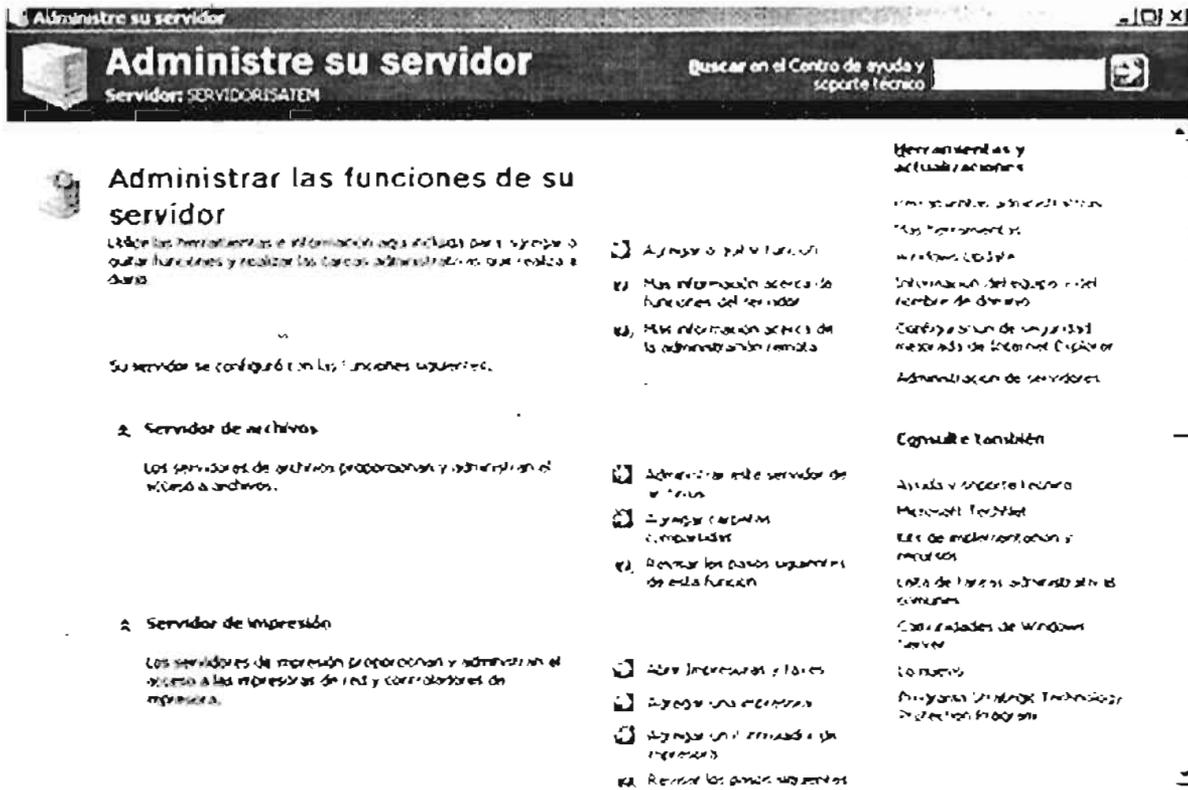


Fig. 5,21 Administrador de servidor.

Lo siguiente es dar doble clic sobre la opción “Agregar y quitar función”, para que se muestren las herramientas con que cuenta nuestro servidor y dependiendo de las necesidades, agregamos o quitamos funciones. Veamos la siguiente figura:

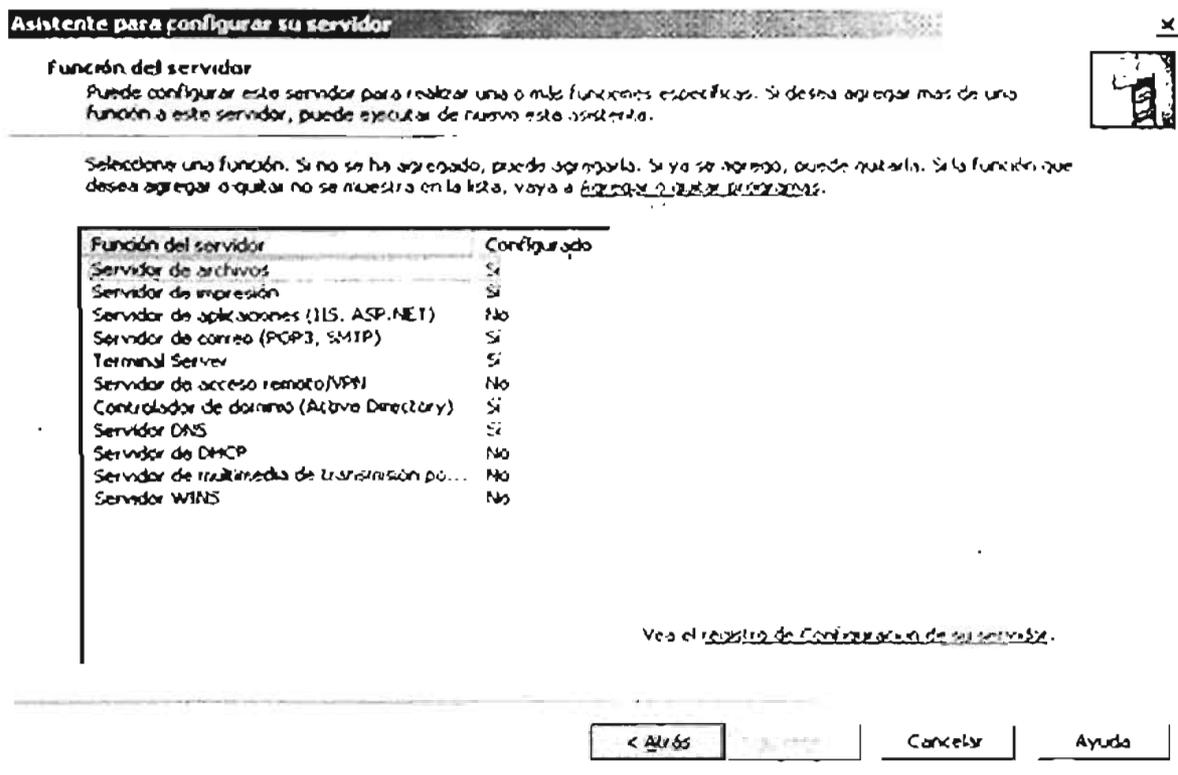


Fig. 5,22 Funciones disponibles en Windows Server 2003.

Observemos que en la pantalla de la figura anterior, tenemos deshabilitado el servidor DHCP, ya que no lo necesitamos, debido a que las direcciones IP se asignarán manualmente, contrariamente el controlador de dominio está instalado ya que nos será de gran utilidad en la administración de la red.

Paso 2. Nombramiento.

Lo siguiente es llevar a cabo el esquema de nombramiento planeado, ponerle un nombre adecuado a cada una de las máquinas. Ello es un proceso rápido, sólo cambiamos los nombres dentro de propiedades de Mi PC, reiniciamos el equipo y listo. No debemos tener mayor problema con ello.

Paso 3. Direccionamiento.

La configuración del TCP/IP la realizamos en propiedades de TCP/IP, seleccionamos “conexión de red” y seleccionamos la conexión inalámbrica,

pulsamos el botón derecho del mouse, en el menú emergente escogemos “propiedades” y damos un clic. Aparecerá una pantalla como la siguiente:

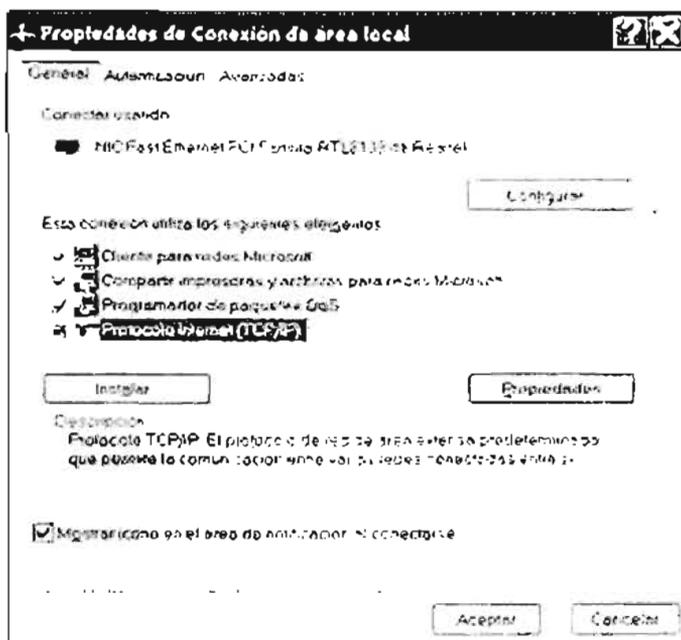


Fig. 5,23 Propiedades de conexión de área local.

Seleccionamos el protocolo TCP/IP y presionamos el botón de “propiedades”, el cual nos llevará a propiedades del protocolo, debemos habilitar la opción de “Usar la siguiente dirección IP”.

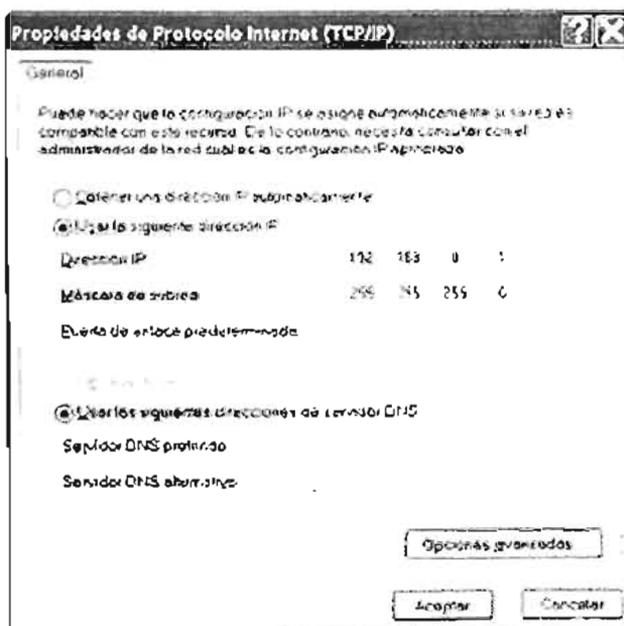


Fig. 5,24 Propiedades de TCP/IP.

Los mismo se hará con cada uno de los 20 equipos asignando la dirección IP que le corresponde de acuerdo al esquema de direccionamiento. Veamos un ejemplo de la máquina del empleado Arturo Salcido G:

Nombre de máquina: operación_10

IP: 192.168.0.30

Máscara: 255.255.255.0

Paso 4. Alta de usuarios de red.

Una vez montado el servidor y la red, lo siguiente es dar de alta a los usuarios que van utilizar los recursos de red, conforme a nuestra tabla de configuraciones de red. Para ello, tenemos que ir al directorio activo e ir agregando a cada uno de los usuarios, los campos más importantes es el de usuario y su contraseña, debemos de tener preferentemente esa información impresa para evitar errores o confusiones.

Paso 5 . Creación de un dominio.

Es recomendable cambiar de grupo de trabajo a un domino, para que el administrador tenga un mayor control sobre la red y los empleados no realicen configuraciones que puedan afectar el rendimiento de la misma, sin autorización del administrador, nosotros podemos unirnos a un dominio existente o crear nuestro propio dominio.

Un dominio es una agrupación lógica de ordenadores, que comparten un directorio centralizado, es decir, todas las cuentas y la información de seguridad. Por lo cual es más fácil que el administrador pueda realizar su trabajo con una mayor seguridad, esta base de datos se guarda dentro de los ordenadores configurados con controladores Server 2003.

El primer paso para realizar el cambio de grupo de trabajo a dominio, es crear un dominio, en este caso será "isatem.com", dicho dominio lo podemos crear en la instalación inicial del directorio activo como los vemos en la figura siguiente:

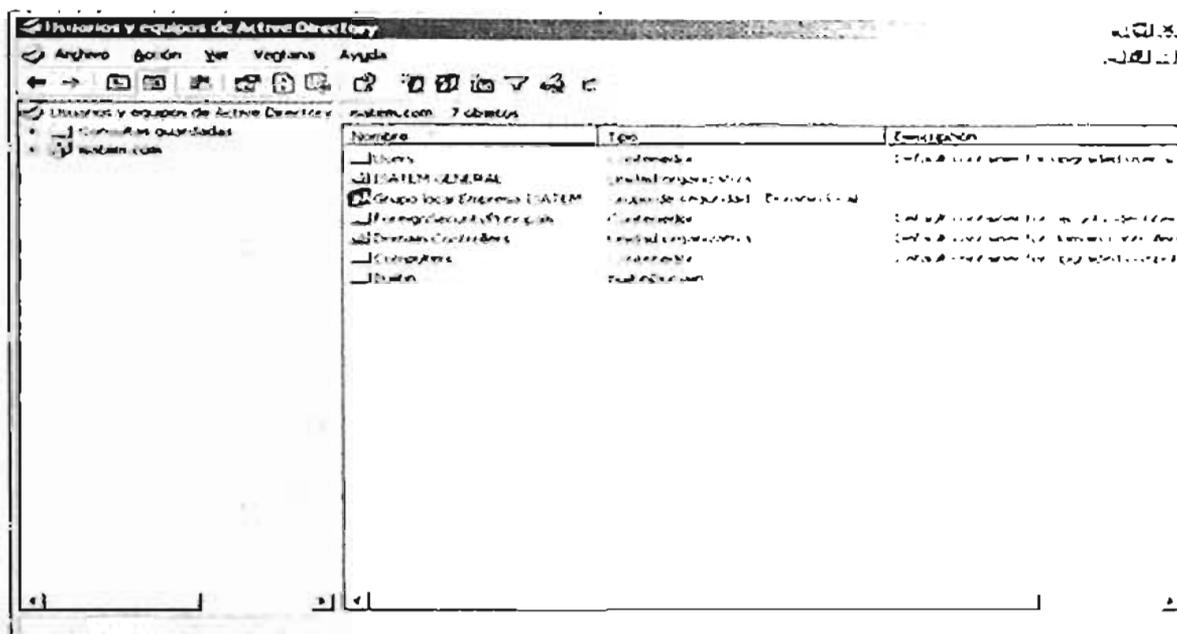


Fig. 5,25 Dominio Isatem.com.

Seguidamente se agregaran al dominio a cada una de las máquinas que conforman la red. Generalmente para ser parte del dominio necesitamos el permiso del administrador, por lo que su clave es requerida cuando realizamos cambios de configuración, es importante tenerla a la mano. En la siguiente figura vemos que la computadora “lap_gerencia” es parte del dominio “isatem.com”.

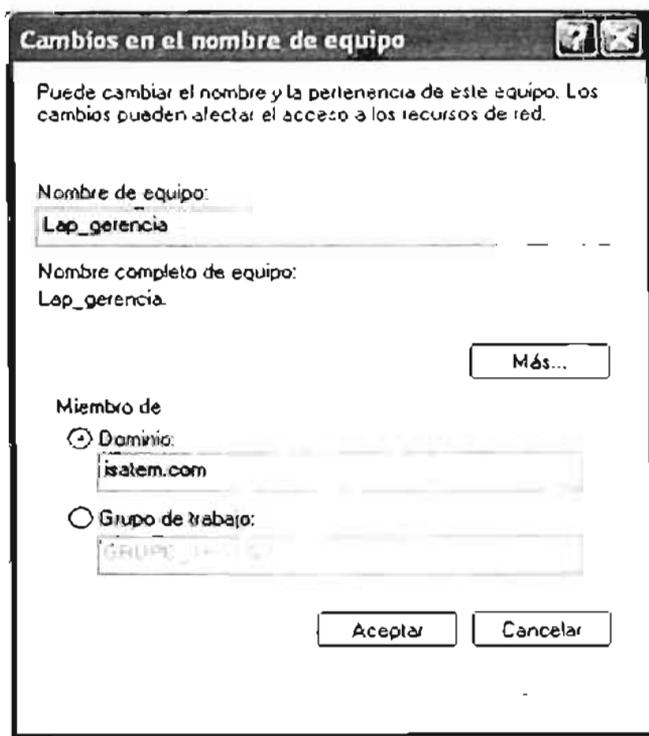


Fig. 5,26 Cambio de grupo de trabajo a dominio.

Paso 6. Unidades organizativas y permisos.

Ya que tenemos datos de alta a los usuarios, lo siguiente es la creación de carpetas y sus permisos, así mismo crear unidades organizativas asignadas al dominio. Tendremos una carpeta principal, que le llamaremos general, la cual contendrá dos carpetas, una pública y otra privada, dentro de la publica estarán cada uno de los departamentos con sus miembros, que tendrá el objetivo de compartir la información por departamento. En cambio, la privada sólo maneja carpetas personales, donde nadie podrá tener acceso mas que el dueño de la misma. Para que sea más claro observemos la siguiente figura:

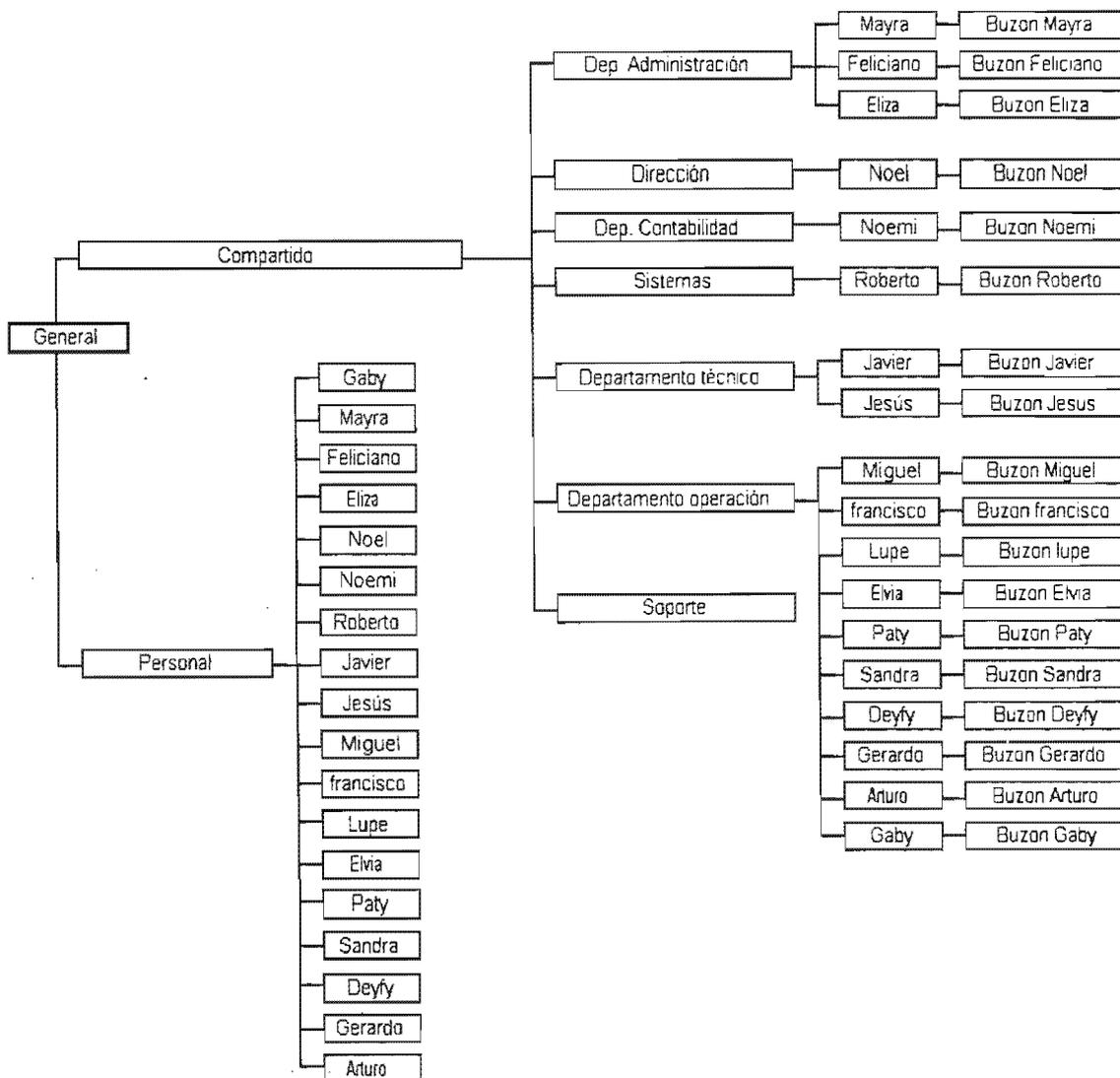


Fig. 5, 27 Organización de las carpetas de información.

La figura nos deja claro como se organizarán las carpetas dentro del disco duro del servidor, ahora aclaremos lo de los permisos. Los permisos se darán por departamentos, cualquier usuario del departamento puede ingresar libremente a las carpetas públicas de sus compañeros, pero las personas que son ajenas al departamento, no lo podrán hacer, si se desea compartir información se deberá de utilizar el buzón, para compartir la información de departamento a departamento.

En la carpeta personal sólo el dueño de la carpeta podrá tener acceso, ningún otro usuario podrá ver esa información, ya que la carpeta será invisible para sus ojos. Vemos que existe una carpeta llamada "soporte", que tiene el objetivo de guardar controladores y aplicaciones que utiliza la red, como controladores de las tarjetas inalámbricas, controladores de la impresora general o impresoras locales, etc.

Hablando de una manera técnica en nuestro caso de Windows 2003 Server tenemos: Un dominio, "isatem.com". A través del directorio activo crearemos nuestra respectiva organización jerárquica. En nuestro caso será suficiente con crear unidades organizativas, no será necesario crear Árboles o Bosques, ya que la empresa no es tan grande ni cuenta con otras sucursales con la que nos podamos enlazar.

Dentro del directorio activo crearemos unidades organizativas, con las que etiquetaremos a cada uno de los departamentos y a las carpetas principales. Una unidad organizativa llamada ISATEM GENERAL , la cual contendrá otras dos unidades organizativas llamadas; ISATEM COMPARTIDO e ISATEM PERSONAL. Veámoslo en la siguiente figura para no perdernos:

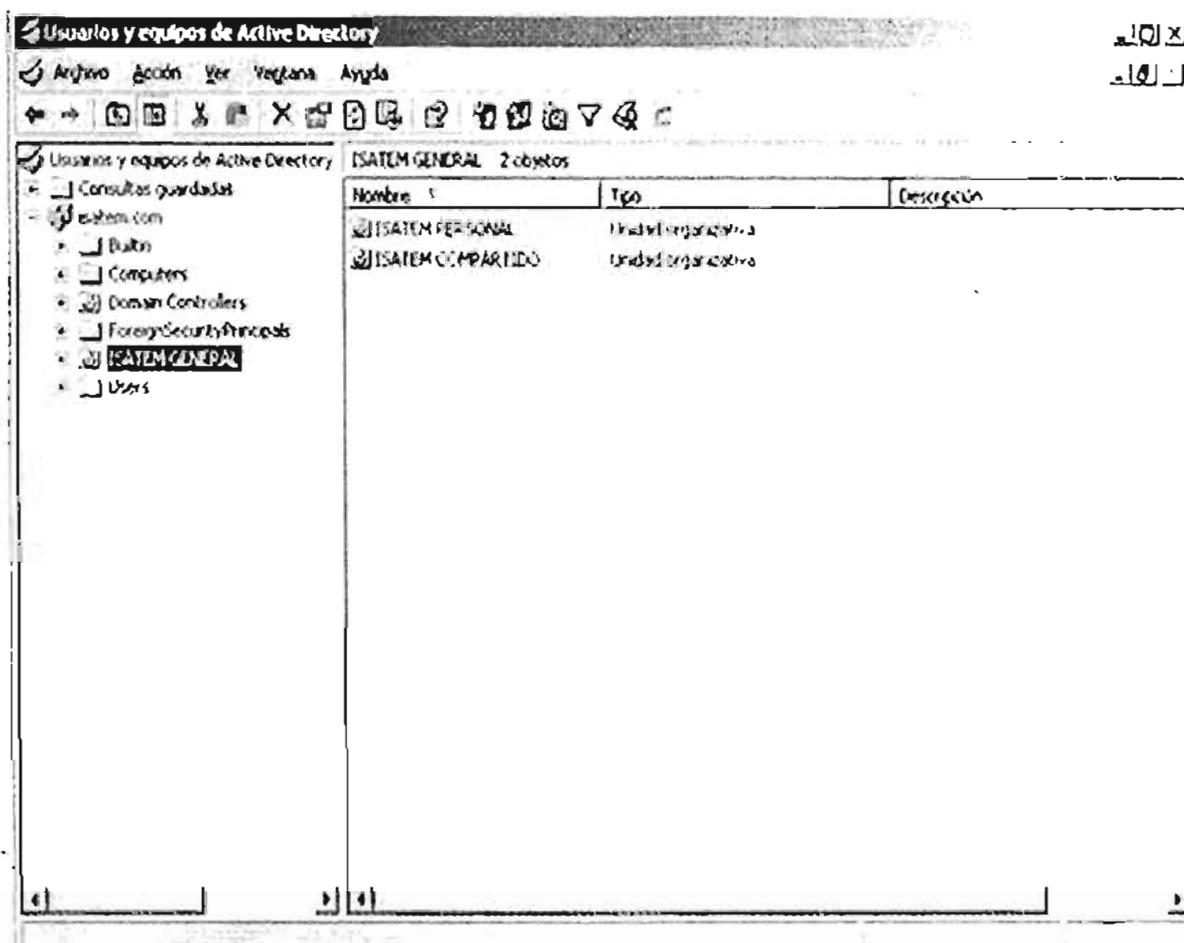


Fig. 5,27 Unidad organizativa principal llamada ISATEM GENERAL.

Dentro de la unidad ISATEM COMPARTIDA crearemos otras unidades organizativas que corresponderán a cada uno de los departamentos. Observémoslo en la siguiente figura:

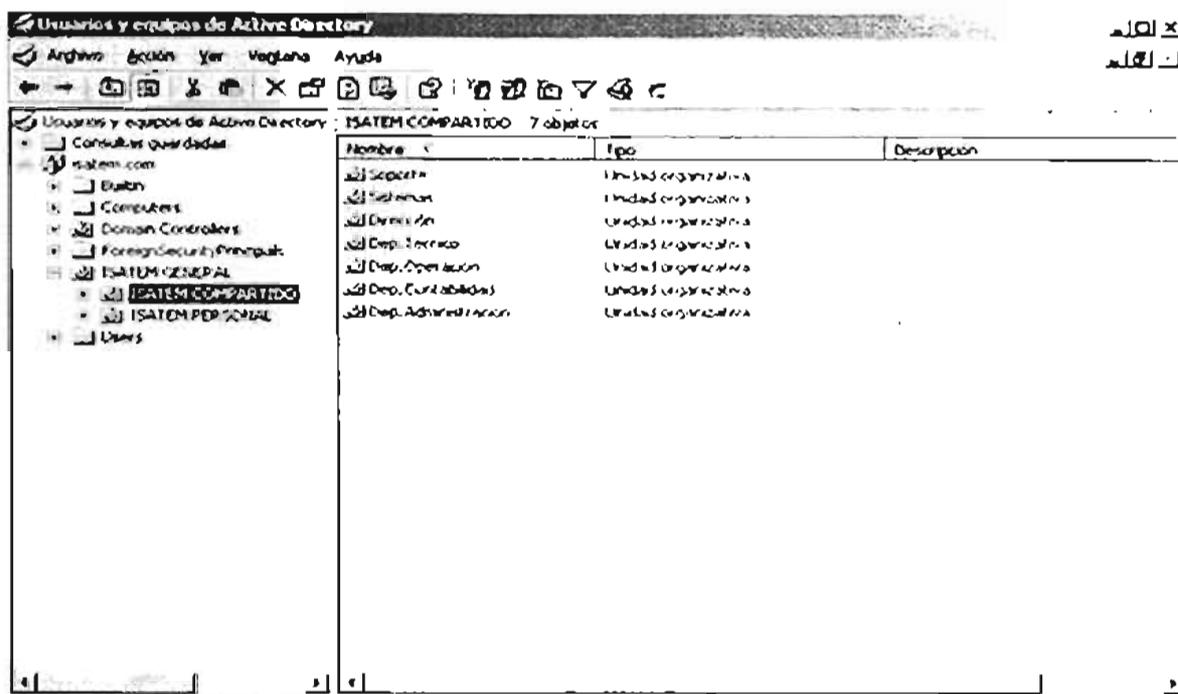


Fig. 5,29 Unidad organizativa ISATEM COMPARTIDO.

Dentro de ISATEM PERSONAL crearemos unidades organizativas personalizadas para cada uno de los usuarios de la empresa Isatem, donde solamente el dueño de la carpeta podrá ingresar. Para facilitar el trabajo, la carpeta tendrá el nombre del usuario. Veamos la figura:

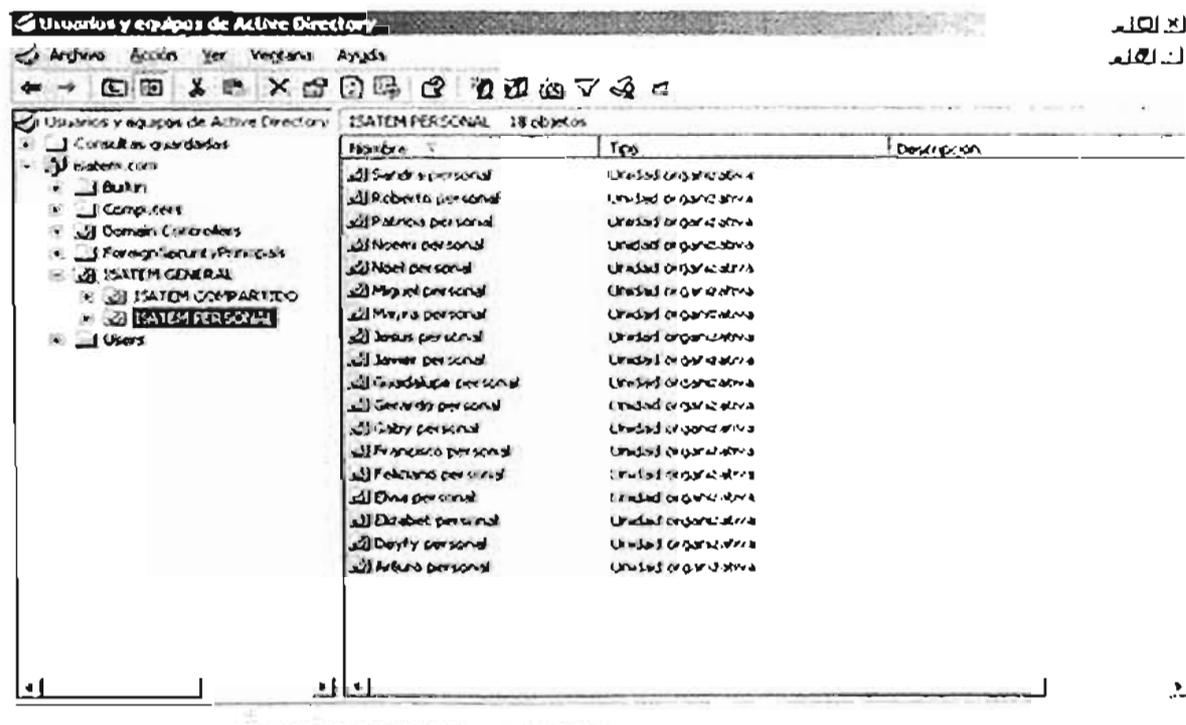


Fig. 5,20 Estructura de la unidad organizativa ISATEM PERSONAL.

Por último, observamos que el departamento de administración contiene las carpetas de cada uno de sus usuarios y que tiene como objetivo compartir información únicamente y exclusivamente entre sus miembros. Veamos la figura siguiente:

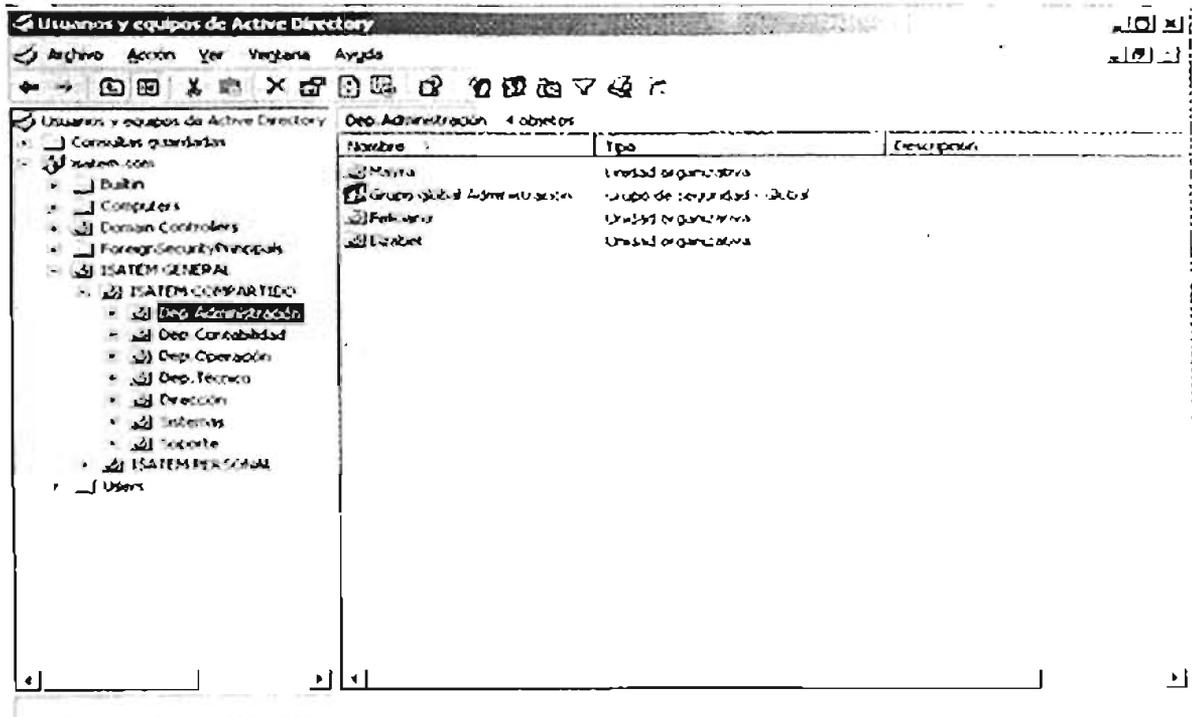


Fig. 5.31 Estructura de la unidad organizativa Dep. Administración.

En lo que respecta a la organización de los grupos globales y locales, lo explicaremos de la siguiente manera:

Tendremos un grupo local llamado “Empresa ISATEM” el cual estará compuesto por 7 grupos globales. Cada grupo global se formara con los usuarios de cada departamento. Así que tendremos 7 grupos globales uno por cada departamento. Veamos las siguientes figuras:

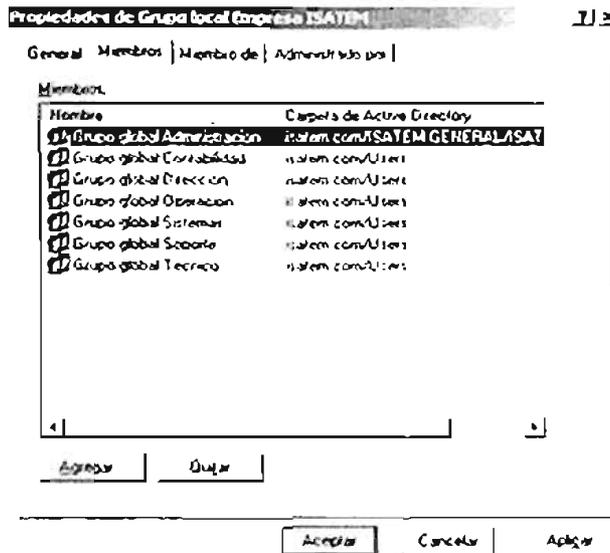


Fig. 5,31 Grupo local Empresa ISATEM.

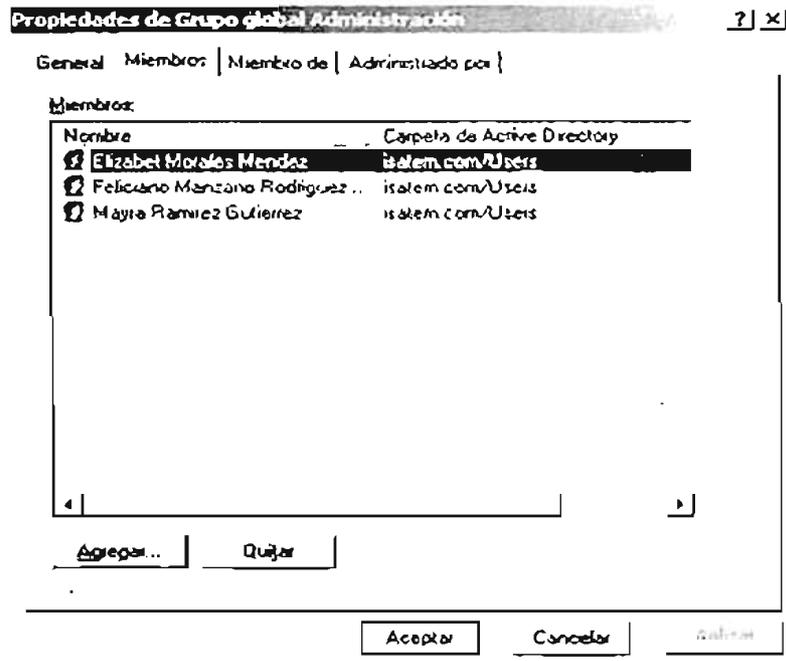


Fig. 5,32 Grupo global Administración.

El fin de crear grupos globales es para asignarle permisos a dichos grupos, organizando mejor el acceso de los usuarios para que puedan ver la información compartida entre los miembros de departamento. En la unidad organizativa ISATEM PERSONAL se le asignara el permiso correspondiente a cada usuario con su carpeta personal.

La asignación de permisos la vamos realizando carpeta por carpeta, agregando a los grupos o usuarios que tienen acceso a ellas. En la siguiente figura damos un ejemplo la asignación de permisos al Grupo global Administración en la carpeta llamada Administración:

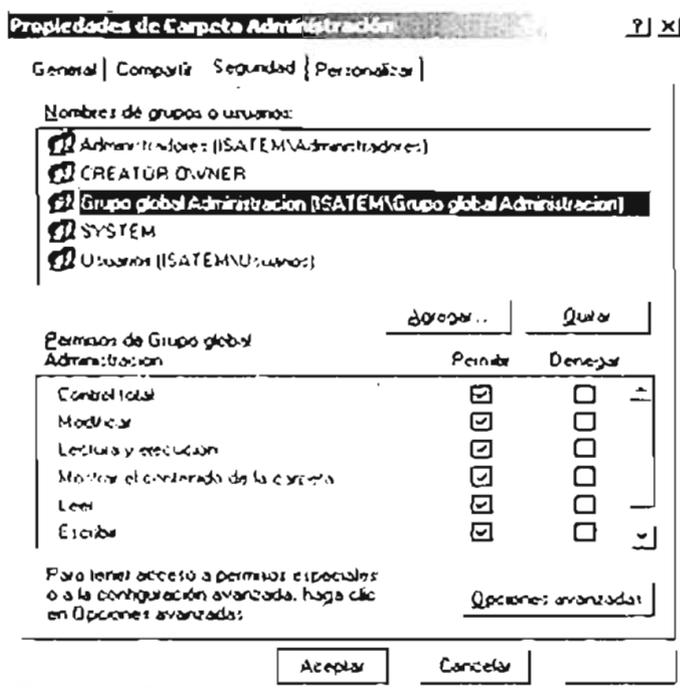


Fig. 5,33 Asignación de permisos en la carpeta administración.

Paso 7. Disco espejo.

Un aspecto muy importante que no debemos dejar pasar por alto, es la seguridad de la información dentro del disco duro, nuestro servidor tiene un segundo disco duro SCSI, que nos ayudará a mantener la información intacta en caso de posibles fallos. Es necesario tener dos discos duros para poder realizar un reflejo de la información. Es recomendable que los discos sean de la misma capacidad, aunque también podemos reflejar en dos discos de distinto tamaño.

El reflejo consiste en realizar una duplicación de información, ya que si uno de los discos llegará a fallar, el sistema se repondrá utilizando la copia de

seguridad. Para utilizar esta configuración necesitamos que los discos se encuentren en modo dinámico.

El administrador de discos nos ayuda a crear discos dinámicos, particiones primarias, extendidas y volúmenes, además de que podemos configurar un disco en espejo. Todo esto en un ambiente muy amigable, que nos permite gestionar los discos de una manera fácil y rápida.

Paso 8. Encriptación de la información.

Como ya lo hemos venido manejando, la seguridad de la información es muy importante, por lo que es necesario realizar una encriptación para evitar que la información llegue a manos ajenas a la empresa, ya que si no lo realizamos, cualquier persona que tenga una tarjeta Linsys o compatible, que se encuentre dentro de la cobertura, puede detectar nuestra red y obtener información privada.

La encriptación que utilizaremos será del tipo WEP, utilizando una llave de 128 bits o lo que es lo mismo 16 caracteres. La clave será la siguiente: "clave_isatem128b".

Por lo que debemos habilitar la clave de encriptación en el software del controlador de la tarjeta inalámbrica, poniendo la palabra clave anterior. Esto se hará tanto en el punto de acceso como en cada uno de los clientes.

Una vez configurado el WEP, debemos realizar la pruebas correspondientes y verificar que cada uno de los equipos puede leer la información encriptada, en caso de que algún equipo no tenga acceso a la red, se debe de verificar que la llave esté escrita correctamente, ya que de lo contrario no se cierra el circuito lógico, que nos permite mandar y recibir información. Por último, es recomendable cambiar la clave periódicamente, ello lo debe de realizar el administrador en plazos no mayores a 6 meses.

Día 5. Configuraciones finales y prueba de red.

Las pruebas finales son chequeos de rutina para garantizar que todo lo que se ha hecho anteriormente funcione correctamente y se alcancen las metas establecidas, en caso contrario se hacen las correcciones o las configuraciones faltantes.

Paso 1. Configuraciones finales.

Dentro de las configuraciones finales se encuentran, las que no se han realizado hasta el momento por X motivo, en este caso se encuentran, la instalación de las impresoras locales y accesorios, impresora general y conexión a Internet.

Primeramente debemos instalar las impresoras locales, para ello agregamos las impresoras, e instalamos los controladores. Una vez hecho esto, verificamos que éste funcione adecuadamente e imprimimos una hoja de prueba como garantía. Lo mismo hacemos con cada una de las máquinas que tengan asignadas una impresora local.

La instalación de la impresora general, es un poco más complicada, ya que primeramente le debemos asignar una dirección IP 192.168.0.10, ello lo realizamos en el programa de instalación que viene en el disco del fabricante. Una vez habilitada la dirección, ahora tenemos que crear un puerto IP en cada uno de los clientes, para ello Windows XP cuenta con una aplicación, ya no tenemos que usar un programa externo para realizar este tipo de configuración, únicamente debemos de cuidar que al agregar la impresora de red, tengamos la dirección correcta del puerto IP.

El paso siguiente, es agregar accesorios como escáner, fax o multifuncionales, agregamos los dispositivos e instalamos sus controladores y probamos su funcionamiento.

Lo siguiente es realizar la configuración de Internet, para ello utilizaremos un Módem inalámbrico que nos ofrece la empresa de Multivisión, bajo el nombre de e-Go Universum, un concepto puramente inalámbrico que ha sido encaminado para las pequeñas empresas. Por el momento, sólo cubre el 40 % del área metropolitana y trabaja con un espectro de radio frecuencia MMDS de 2.5 a 2.7 Ghz, que nos permite transmitir señales digitales a muy buena velocidad. Esta tecnología sólo existe en México, con una frecuencia debidamente regulada y concesionada.

Las velocidades de transmisión de datos están marcadas en 4 categorías 256 Kbps , 512 Kbps, 1 Mbps y 1.5 Mbps. Los precios son proporcionales a la velocidad.

La instalación y configuración del Módem Inalámbrico de e-Go es muy rápida, esto no lo haremos nosotros, la empresa Multivisión realiza la instalación y configuración. Solo debemos estar pendientes de que todo funcione correctamente y que el Módem se instale en el puerto número 6 del Switch, tal como se había previsto. La velocidad contratada, es de 1.5 Mbps, suficiente para nuestros 20 equipos.

Una vez que se tiene una conexión a Internet, es necesario configurar las cuentas de correo electrónico, para ello primeramente tenemos que dar de alta nuestro dominio con un carrier para poder utilizarlo públicamente. Posteriormente realizamos las configuraciones en un cliente de correo electrónico, ello lo hacemos dentro de Microsoft Outlook 2003, la configuración es muy sencilla, sólo agregamos el protocolo de entrada "pop.isatem.com" y el protocolo de salida; "smtp.isatem.com" y tener a la mano los nombres y claves de los usuarios asignados por la empresa que provee el servicio. Si el usuario cuenta con un respaldo de correos y direcciones electrónicas, se debe importar el archivo *.PST

que contiene la información. Una vez concluida la configuración se realiza un prueba de correo, para verificar que los mensajes puedan salir y llegar. Con ello se concluyen las configuraciones finales y pasamos a la prueba final.

5.1.5 Etapa de prueba de red.

La etapa de prueba viene a cerrar el proyecto, ya que si todo sale como se espera se da por concluido el trabajo. En caso contrario, se debe de regresar a alguna de las etapas anteriores para realizar la correcciones necesarias y en caso crítico, se replantea el diseño, aunque es muy difícil que suceda esto, pues estaríamos hablando de una mala planeación, que en el área de redes sería imperdonable.

Paso 2. Pruebas Finales.

Para realizar la pruebas finales es necesario reiniciar la red por completo. Apagar todos los equipos junto con el servidor para poder detectar posibles problemas y verificar que todo funcione correctamente. Una vez apagados los equipos, encendemos primeramente el servidor y consecutivamente cada una de las máquinas, verificando lo siguiente:

- 1) Que todos los equipos puedan acceder a la red de forma inalámbrica.
- 2) Que todos los usuarios puedan ingresar al dominio sin problemas.
- 3) Que todos los equipos tengan conexión a Internet.
- 4) Que los usuarios puedan hacer uso de los recursos destinados para ellos, correo electrónico, servidor de archivos y aplicaciones específicas.
- 5) Que todos los usuarios puedan imprimir en las impresoras locales y en la impresora General Xerox.
- 6) Que los equipos tengan la movilidad planeada, es decir, que funcionen tanto en la sala de juntas como en sus sitios asignados.

Una vez superadas estas pruebas finales, damos por terminada la implementación de la red, ofreciendo un mes de prueba como garantía, dejando que los usuarios realicen las pruebas finales con el trabajo mismo. Desde este momento, dejamos la red en manos del administrador, para que pueda gestionar la red a su criterio, sólo nos resta entregarle el reporte de lo realizado y esperar que no existan complicaciones posteriores.

CONCLUSIÓN

Al desarrollar el presente trabajo de tesis podemos establecer que las redes inalámbricas son toda una realidad y que han llegado para quedarse. Las redes WLAN son las primeras en adoptar esta tecnología debido a su pequeño tamaño que facilita la comunicación entre nodos. Sabemos que las redes inalámbricas no buscan desplazar al cableado, mas bien se trata de que una con otra complementen sus beneficios y puedan convivir, con ello tenemos más opciones para desarrollar una red de acuerdo a las necesidades requeridas.

Por otro lado, implementar una pequeña red inalámbrica no es complicado, pero se debe de tener mucho cuidado de que la información no se salga de los límites establecidos y rompa con la seguridad. Los cables sólo son carreteras en donde podemos canalizar la información y llevarla justo donde queremos, pero las tarjetas inalámbricas no se comportan así. El encriptar la información es sin duda un aspecto de mucha importancia. Buscar utilizar una misma marca en dispositivos de enlace es lo más adecuado, ya que nos podemos ahorrar conflictos en seguridad y en compatibilidad.

El planear y diseñar una red empresarial inalámbrica (infraestructura), no es cosa fácil, se debe de buscar, contemplar la mayoría de las variables que garanticen el correcto funcionamiento y desempeño de la misma. En la implementación que realizamos dentro del capítulo 5, abarcamos un ejemplo en la empresa ISATEM de México, sin embargo, las variables van cambiando debido a que los requerimientos empresariales no son los mismos. La planeación, el diseño y la implementación deben ser a la medida de cada compañía.

Para finalizar, debemos decir que la tecnología inalámbrica está tomando fuerza y se expande rápidamente, incluso ha saltado a las redes MAN, en la cual la tecnología Wi-Max viene sonando bastante fuerte. Esperemos que pronto esté en el mercado y que el precio no sea tan elevado.

El material que contiene la tesis ha sido escogido a nuestro criterio, buscando alcanzar el objetivo establecido en un principio. Sabemos que la información es suficiente para desarrollar habilidades que nos permitan implementar una red empresarial.

BIBLIOGRAFÍA

- Carballan falcon, José. **Cómo construir una red inalámbrica.** Ra-ma, Mexico. 2004.
- Forouzan, Behrouz A. **Tranmisión de datos y redes de comunicaciones,** 2da. Edición, McGraw Hill.
- Raya, José Luis y Raya, Laura, **Intranets y TCP/IP con Microsoft Windows Server 2003,** Ra-Ma, España 2004
- Santamaría, A y López, F.J. **Wireless LAN Systems.** Artech House, London.
- Stallings, William. **Comunicaciones y redes de computadores.** Prentice Hall, quinta edición, México 2000.
- Stallings, William, **Wireless communications and networks,** Prentice Hall, México 2003.
- Van Nee, Richard & Prasad, **Ramiee, OFDM Wireless Communication,** Artech House, Boston, 2000.
- Vallejos Soto, Antonio. **Sistemas microinformáticos y redes LAN.** Marcombo. México 1997.

MATERIAL DE APOYO EN CD ROM

- Material de **redes inalámbricas y telecomunicaciones,** ofrecido por la división de educación continua de la Facultad de ingeniería de la UNAM, coordinado por el Ing. Saul Magaña Cisneros. 2004.
- Guía interactiva y visual sobre **Redes de área local,** ofrecida por la empresa SOGRAFT creatividad digital, México 2004.

DIRECCIONES ELECTRÓNICAS

<http://cdec.unican.es/libro/apendice.htm>

(Página española publicada por la Universidad de Cantabria, con el fin de difundir información técnica educativa creación de documento HTML publicada por el ing. Luís Flores Romero)

<http://es.tldp.org/Manuales-LuCAS/GARL2/garl2/index.html>

(Página española sobre manuales de redes en linux, contiene conceptos sobre redes en general, escrita por Dlaf Krich y Ferry Dawson, publicado por ediciones Lucas)

<http://www.cnice.mecd.es>

(Sitio español dedicado a promover la educación tecnológica, cultural y literaria. Se leyó un artículo sobre el modelo OSI)

<http://noticias.nicatech.com.ni/>

(Página publicada Nic@technologies, una empresa de desarrollo de sistemas de información, redes y seguridad informática)

<http://web.frm.utn.edu.ar>

(Página publicada por la Universidad Tecnológica Nacional el cual está orientado a publicar cursos y cátedras universitarias, se consulto una manual sobre interconexión de sistemas abiertos.)

<http://www.cybercursos.net/>

(Página dedicada a la publicación de cursos vía Internet)

<http://www.comunnet.com.mx>

(Portal mexicano publicado por la empresa ComUnNet dedicada a dar accesorias técnicas y soporte técnico. Hay artículos y manuales gratis muy interesantes sobre todo en el área Inalámbrica)

<http://www.conocimientosweb.net>

(Sitio de publicación de artículos, se consultó el artículo sobre seguridad de redes WLAN, escrito por el Ing. Ángel León)

<http://www.cisco.com>

(Página de Cisco Systems, líder mundial en redes para Internet. Las soluciones de conectividad de Cisco basadas en el protocolo de Internet (IP), son la base de Internet y de las redes corporativas, educativas y de gobierno en todo el mundo)

<http://www.eveliux.com>

(Un espacio dedicado a la publicación de artículos de información tecnológica, se consulto un artículo sobre redes Inalámbricas para transmisión de datos, publicado por Evelio Martínez Martínez)

<http://es.wikipedia.org/wiki/IPv6>

(Enciclopedia virtual en Internet, con acceso a todo el público de forma gratuita, define varios conceptos tecnológicos de forma fácil de comprender)

<http://www.forest.ula.ve/>

(Espacio que brinda la Facultad de Ciencias Forestales y Ambientales para la publicación de Manuales educativos)

<http://www.geocities.com/SiliconValley/8195/index.html>

(Página publicada por Ing. Manuel Espinoza Curiel, egresado del Instituto Tecnológico de Sonora, con el fin de proporcionar información sobre redes de área local y sistemas operativos de redes)

<http://www.htmlweb.com>

(Página española que se dedica a dar asesorías, cursos y clases en línea. Ofrece también guías y manuales gratuitamente. Se consultó un tutorial de fundamentos de redes de ordenadores, escrito por Luciano Moreno)

<http://www.infinitum.d2g.com>

(Importante página dedicada a la asesoría técnica, creada para los técnicos de soporte de servicios ofrecidos por Telmex)

<http://www.laflecha.net>

(Es un diario español, que nos mantiene actualizados en todo lo relacionado a ciencia y tecnología. Obviamente las redes inalámbricas forman parte de las nuevas tecnologías y existen publicados en este sitio una gran variedad de escritos)

<http://www.microsoft.com/latam/technet>

(Guías y artículos publicados por Microsoft TechNet)

<http://www.monografias.com>

(Portal que publica artículos y trabajos escolares. Se consultó un artículo sobre redes locales inalámbricas y sistema Operativo UNIX, escrito por el Ing. en telecomunicaciones José Manuel Huidobro. Y otros temas relacionados con la tesis)

<http://www.mundofree.com/juanpablo/xarxes/gg.htm>

(Página española difundida por el Ing. Juan Pablo Sánchez, ingeniero en telecomunicaciones de la U.P. en Madrid, fundador de la TS técnicas solidarias con sede en Valencia)

<http://www.osmosislatina.com/index.htm>

(Publicado por Osmosis Latina, empresa que desarrolla software y asesora en la administración de información, se consultaron artículos relacionados con la administración de red)

<http://www.portalmundos.com>

(Un portal que aloja interesantes artículos, como “el peligro de no usar cables” escrito por Sergio de los Santos)

<http://www.redaragon.com>

(Portal español dedicado a la publicación y difusión de artículos de todo tipo, entre ellos artículos de redes)

<http://www.redestelecom.com/>

(Portal dedicado a brindar información técnica para profesionales del networking y telecomunicaciones)

<http://www.saulo.net/>

(Página publicada por el Ingeniero en Informática Saúl Barajas, muy reconocido por sus artículos sobre implementación y administración de redes)

<http://www.sorgonet.com/torderawireless/index.php>

(Sitio de publicación de artículos de transmisión de datos inalámbricos)

<http://www.telefonicapr.com/>

(Portal de una empresa telefónica Puerto Riqueña que ofrece servicios de conexión frame relay e información sobre la misma)

<http://www.usr.com>

(Página de U.S. Robotics, importante fabricante de dispositivos de comunicación)

<http://www.uaslp.mx>

(Portal de la Universidad Autónoma de San Luís Potosí, donde se publica una guía de “¿Cómo planear una red?” elaborado por el Departamento de Telecomunicaciones de la Universidad)

<http://www.ugr.es/>

(Portal de la Universidad de Granada en España, cuenta con una gran variedad de temas técnicos educativos, se consultó un artículo sobre normas de cableado UTP)

<http://www.wirelessmundi.com>

(Portal dedicado a impulsar el uso de redes inalámbricas, creado por la empresa Wireless Mundi que radica en Madrid España)

<http://www.zonablueetooth.com/documentacion.htm>

(Página española publicada por ZonaBluetooth S., una empresa joven y dinámica que cree firmemente en la especialización de contenidos y en que sólo es posible ofrecer el mejor servicio al cliente desde un conocimiento adecuado de los productos y de las posibilidades de éstos. Tiene el objetivo de dar a conocer la tecnología bluetooth y los productos que funcionan con ella)

GLOSARIO

A

Ad hoc

Se denominan redes *ad hoc*, cuando se utiliza comunicación directa de equipo a equipo. Las redes ad hoc hacen posible que los equipos "hablen" (envíen información) de manera directa de uno a otro.

AP (Access Point)

Referente al punto de acceso inalámbrico. Un transmisor y receptor o un elemento de radio que forma parte de una Red de Área Local (LAN) que actúa como punto de traspaso entre señales alámbricas a inalámbricas, y viceversa.

Ancho de banda (bandwidth)

Expresa la cantidad de datos que pueden ser transmitidos en determinado lapso. En las redes se expresa en bps.

B

Bluetooth

Un grupo de Interés especial, consiste de líderes de las industrias de telecomunicación, computación y redes; que están desarrollando un estándar para la comunicación inalámbrica a corto alcance entre aparatos. Tales como PDAs, computadores portátiles, teléfonos móviles y máquinas dispensadoras. Bluetooth utiliza la misma frecuencia de banda (2.4 GHz) que las redes inalámbricas 802.11b.

Bit

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

Byte

Unidad de información utilizada por las computadoras. Cada byte está compuesto por ocho bits. Representa un carácter en lenguaje binario.

C

Cliente

Un sistema o proceso que solicita a otro sistema o proceso que le preste un servicio. Una estación de trabajo que solicita el contenido de un archivo o servidor de archivos es un cliente de este servidor. Véase modelo Cliente-Servidor.

Congestión.

Cuando la carga existente sobrepasa la capacidad de una ruta de comunicación de datos, se dice que existe una congestión en la línea.

D

Directorio.

Espacio lógico de una estructura jerárquica en forma de árbol que contiene la información almacenada en un computador, habitualmente contenida en archivos.

Driver(Controlador).

Es un programa que controla un dispositivo. Cada dispositivo, teclado, disco duro, impresora, etc etc... necesita ser controlado por algún programa. Algunos "Drivers" vienen incorporados en el propio sistema operativo, como por ejemplo el del teclado. En otros dispositivos es necesario instalar el "driver" o controlador para que el sistema operativo pueda manejarlo. El "driver" actúa como traductor de instrucciones específicas de cada dispositivo en instrucciones genéricas que utiliza el sistema operativo.

DSSS (Direct Sequence Spread Spectrum, Espectro disperso de secuencia directa).

Es uno de los dos tipos de espectro distribuido de radio, siendo el otro Frequency-Hopping Spread Spectrum (FHSS). DSSS es una tecnología de transmisión usada en WLANs donde una señal de datos en la estación emisora se combina con una secuencia mayor de bits, que divide los datos de usuarios de acuerdo al nivel de distribución. Dicha secuencia es un patrón de bits por cada bit transmitido, el cual incrementa la resistencia de la señal a la interferencia. Si uno o más bits en el patrón se dañan durante la transmisión, los datos originales pueden recuperarse debido a la redundancia de la transmisión.

DHCP (Dynamic Host Configuration Protocol, Protocolo de configuración dinámica del host).

Un protocolo de Internet estándar en la industria definido por IETF. DHCP fue diseñado para proporcionar dinámicamente valores de configuración relacionados con comunicaciones, tales como direcciones de red para equipos clientes de red durante el inicio.

E

Encriptación (cifrado).

Es el tratamiento de los datos contenidos en un paquete a fin de impedir que nadie excepto el destinatario de los mismos, pueda leerlo. (por supuesto, éste debe conocer la clave de descifrado). Existen muchísimos tipos de cifrado.

F

Frame Relay.

Protocolo de transmisión de alta velocidad que se utiliza en las redes WAN (Wide Area Network), redes de área amplia.

FHSS (Frequency Hopping Spread Spectrum, espectro disperso con salto de frecuencia).

Es uno de los dos tipos de espectro distribuido de radio, siendo el otro Direct-Sequence Spread Spectrum (DSSS). FHSS es una tecnología de transmisión usada en WLANs donde la señal de datos se modula con un transmisor de onda corta que "horea" (salta) en secuencias al azar (aunque predecibles) de una frecuencia a otra en función del tiempo a lo largo de una amplia banda de frecuencias. La energía de la señal se distribuye en función del tiempo, en lugar de cortar cada bit en pequeños pedazos en una sola frecuencia. Esta técnica reduce la interferencia porque la señal de un sistema de onda corta sólo afectará la señal del espectro si ambos transmiten a la misma frecuencia y al mismo tiempo. Si se sincroniza apropiadamente, se mantendrá un sólo canal lógico. Las frecuencias de transmisión se determinan por el código de hopping. El receptor debe tener definido el mismo código de hopping y escuchar la señal en el momento y frecuencias correctos para recibirla bien. Las regulaciones actuales requieren a los fabricantes que usen 75 o más frecuencias por canal de transmisión con un máximo tiempo de vida (el tiempo transcurrido en una frecuencia particular durante cualquier salto) de 400 ms.

G

Gateway (pasarela).

Hoy se utiliza el término router (enrutador o direccionador) en lugar de la definición original. Actualmente una pasarela es un programa o dispositivo de comunicaciones que transfiere datos entre redes que tienen funciones similares pero operativas diferentes.

Gigabyte (GB).

Unidad de medida de memoria. 1 gigabyte = 1024 megabytes = 1.073.741.824 bytes. Algunos fabricantes de discos consideran gigabyte como 1000 megas en lugar de 1024. Aplicando esto se obtiene que un gigabyte es 1.048.576.000 bytes.

GHz.

Abreviación de GigaHerz que representa a mil millones de ciclos por segundo.

I

Infraestructura.

Se trata de un tipo de configuración para una LAN con cable o integrada inalámbrica. En este tipo de configuración, se crea una red inalámbrica mediante adaptadores inalámbricos conectados a un router inalámbrico o punto de acceso. El

router inalámbrico o punto de acceso puede conectarse a un módem de banda ancha o a una LAN existente para proporcionar conexión a Internet a la red inalámbrica.

Interfase.

Elemento de transición o conexión que facilita el intercambio de datos. El teclado, por ejemplo, es una interfase entre el usuario y la computadora.

Internet.

Aunque es una red, el término se usa habitualmente para referirse a un conjunto de redes interconectadas mediante routers.

Interoperabilidad.

Capacidad de comunicación entre diferentes programas y máquinas de diferentes fabricantes.

Intranet.

Es una red de computadores limitada a un número de usuarios determinados que generalmente están en un mismo edificio o empresa, aunque pueden estar más distanciados. Emplea tecnología Internet y Protocolos TCP/IP. Limita y restringe el acceso a cualquier persona que no esté autorizada.

IP

Es el protocolo de envío de paquetes donde el paquete tiene una dirección destino, y éste se envía sin acuse de recibo. Cuando una persona se conecta a Internet, se le asigna una dirección IP.

K

kHz.

Abreviatura de kilohertz, unidad de frecuencia equivalente a 1.000 ciclos por segundo.

Kbps.

Kilobits por segundo. Se usa para expresar la velocidad de transmisión de datos en una red. Un kilobit equivale a 1.000 bits. Con un modem de 28.8 Kbps, se transfieren 3.6K de datos por segundo.

Kerberos

Programa informático desarrollado por el MIT para proteger los intercambios en la red de una universidad o una organización.

L

LAN (Local Area Network, Red de Area Local).

Red de datos para dar servicio a un área geográfica máxima de unos pocos kilómetros cuadrados, por lo cual pueden optimizarse los protocolos de transmisión de señal de la red para llegar a velocidades de transmisión de hasta 1Gbps.

Login.

Conectarse a un computadora con identificación de usuario y contraseña. Acción de introducir el nombre a través del teclado para acceder a otro computadora.

M

Multicast.

Comunicación entre un sólo emisor y múltiples receptores en una red.

N

NIC (Network Interface Card).

Tarjeta de red. Elemento de hardware que se puede instalar en el computador para conectarse a una red.

O

Online (en línea).

En línea, conectado. Estado en que se encuentra una computadora cuando se conecta directamente con la red a través de un dispositivo, por ejemplo, un módem o una tarjeta de red.

OFDM (Ortogonal Frequency Division Multiplexing).

Es una técnica de modulación de FDM para transmitir grandes cantidades de datos digitales sobre una onda de radio. El OFDM funciona cortando la señal de radio en varias sub-señales menores que luego se transmiten simultáneamente en diferentes frecuencias al receptor.

Esta técnica reduce el crosstalk (interferencia) en las transmisiones, y por esto se utiliza en la tecnología 802.11a en WLANs. Es una alternativa al FHSS y DSSS.

OSI (Open Systems Interconnection).

Interconexión de Sistemas Abiertos. Conjunto de protocolos diseñados por comités internacionales de arquitectura de redes de computadoras.

P

Password.

Contraseña, Clave Secreta.

PCI (Peripheral Component Interconnect)

Bus local desarrollado por Intel. Existen dos variantes de este bus para PC:

- 32 Bits y 33 Mhz.

- 64 Bits y 66 Mhz.

El PCI, aunque fue desarrollado por Intel, no está ligado a ninguna plataforma y actualmente es utilizado por los computadores Macintosh modernos.

PCMCIA (Personal Computer Memory Card International Association)

Asociación Internacional de Tarjetas de Memoria para PC. Estándar de bus para tarjetas periféricas de computadoras portátiles.

Protocolo

Descripción formal de formatos de mensaje y de reglas que dos computadores deben seguir para intercambiar dichos mensajes.

Punto de acceso.

Dispositivo que transporta datos entre una red inalámbrica y una red cableada (infraestructura).

R

RAID (Redundant Array of Inexpensive o Independent Disk)

Conjunto de discos redundantes independientes, un componente importante para servidores o soluciones críticas de almacenamiento orientado a empresas o grupos de trabajo.

RF.

Radio frecuencia.

S

Server

Servidor. Cualquier computador de una red que pone los servicios de archivos, impresión o comunicaciones a disposición de otras estaciones de la red.

Subdominio

Un subdominio es un dominio que forma parte de otro dominio más general.

SSID (Service Set Identifier, identificador del conjunto de servicios)

Este es el nombre de red que se utiliza para identificar una red inalámbrica específica.

SSL (Secure Sockets Layer)

Protocolo de encriptación seguro a nivel sockets. Protocolo diseñado por la empresa Netscape para proveer comunicaciones encriptadas en Internet. Proporciona privacidad para datos y mensajes, y permite autenticar los datos enviados. Básicamente se utiliza para transmitir información personal o relacionada con tarjetas de crédito de los usuarios a través de Internet. Las direcciones de páginas Web que utilizan conexiones SSL, comienzan con *https:* en lugar del estándar *http:*.

T

TLS (Transport Layer Security).

Protocolo de encriptación seguro en la capa de transporte.

VPN (Red Privada Virtual).

Red en la que al menos alguno de sus componentes utiliza la red Internet pero que funciona como una red privada, empleando para ello técnicas de cifrado.

W

WEP (Wired Equivalent Privacy).

Técnica de seguridad implementada en las redes inalámbricas. Se trata de un estándar de cifrado que proporciona un nivel de seguridad y privacidad comparable al que se suele esperar de una LAN por cable.

WPA (Wi-Fi Protected Access. Acceso Wi-Fi protegido).

Se trata de un estándar de cifrado que supone una mejora del estándar WEP. WPA proporciona un cifrado más sofisticado y autenticación de usuario.

Wi-Fi (Wireless fidelity)

Nombre con que se le conoce al estándar 802.11b.

ANEXO A. Protocolos de comunicación.

Actualmente existen varios protocolos que se utilizan en las comunicaciones de datos. En este apartado veremos algunos de ellos, principalmente los que hacen posible que las redes funcionen, ya que son los que nos interesan.

El objetivo principal de un protocolo es definir las reglas de comunicación entre las computadoras de la red. El ejemplo más claro es la familia TCP/IP que es independientemente del sistema operativo y del fabricante del equipo, es decir, podemos comunicar equipos que tengan distinto sistema operativo como LINUX y WIDONWS, ya que cuentan con un protocolo en común que lo hace posible.

Aclaremos que existen otros protocolos que son utilizados por un sólo fabricante y que únicamente pueden ser utilizados por ellos mismos. La comunicación entre sistemas no podría darse si se manejaran distintos protocolos de comunicación, eso si sería imposible.

Definición de protocolo.

Los protocolos establecen reglas de transmisión y recepción entre los nodos que conforman una red, de modo que para que pueda haber una conexión entre dos computadoras se deben de respetar estas reglas, es decir, que hablen el mismo lenguaje.⁵¹

Familias y protocolos de comunicación

Conectar un grupo de computadoras no es una tarea sencilla, ya que hay una variedad de servicios que nosotros como usuarios podemos utilizar, por ello diferentes empresas han creado una variedad de protocolos que nos brindan una solución a nuestros requerimientos. A continuación se abarcan los protocolos y familias de protocolos más importantes y comerciales.

NetBEUI (NetBIOS Extended User Interface,, Interfaz de usuario extendida para NetBIOS)

Es un protocolo exclusivo para redes pequeñas de no más de 10 computadoras, no permite el enlace con otras redes LAN ni el acceso a Internet. Se puede decir que el NetBEUI sólo es aplicable en una pequeña red. La ventaja que tiene este protocolo es que es muy fácil de configurar; basta con instalar el protocolo y asignar un nombre a cada computadora para que comience a funcionar. Su mayor desventaja es su ineficiencia en redes de gran tamaño. Actualmente es un protocolo exclusivo de las redes Microsoft

⁵¹ <http://www.forest.uia.ve/~mana/cursos/redes/protocolos.html>

Decnet

El protocolo Decnet es el protocolo propietario de Digital Equipment Corporation. Permite tener hasta 64 redes de 1024 nodos cada una. Es uno de los protocolos más potentes ya que dentro de su configuración normal da acceso a terminales conectadas a diferentes servidores. Es un protocolo que da todas las facilidades para poder distribuir todos los recursos de nodo a nodo.

Apple Talk

Es un protocolo utilizado para interconectar computadoras Macintosh, propiedad de Apple, permite enlazar diferentes redes locales siempre y cuando estén bajo la plataforma Macintosh.

SPX/IPX

SPX (Sequential Packet Exchange, Protocolo de intercambio de paquetes secuenciales)/IPX (Internetwork Packet Exchange, Protocolo de intercambio de paquetes entre redes).

Es una familia de protocolos desarrollada por las redes Netware de Novell, creada por dicha compañía a principios de los años 80. En un principio esta familia era exclusiva de las redes Novell, aunque después se incorporó a otros sistemas operativos como Windows.

La familia SPX/IPX, permite la comunicación entre computadoras de diferentes redes por medio de los routers o encaminadores, la estructura es similar a la familia TCP/IP, su configuración es más sencilla, aunque admite menos control sobre el direccionamiento de la red. Actualmente SPX/IPX no es muy utilizado.

TCP/IP

El TCP/IP es por ahora la familia de protocolos más utilizada a nivel mundial y por su diseño permite conectar a la red más grande que se conoce hasta el momento: La Internet.⁵²

El conjunto de protocolos TCP/IP tienen las siguientes características:

- Lo conforman protocolos libres o gratuitos, su desarrollo y modificación se realiza por consenso, para que cualquier fabricante pueda desarrollar productos que cumplan con las normas establecidas.

⁵² <http://www.cybercursos.net/cursos-online/protocolos.htm#TCP/IP>

- Es independiente del Software, por lo que se pueden conectar equipos con diferente sistema operativo a redes locales y a Internet.
- Es independiente del Hardware, debido a que podemos utilizar máquinas de distintos fabricantes para integrar una red.
- El funcionamiento se basa en un esquema de direccionamiento el cual permite localizar un equipo en cualquier parte de la red.
- Los protocolos utilizados dentro de la familia son de alto nivel, por lo que ofrecen una gran variedad de servicios al usuario de manera que puede utilizarlos en el momento que prefiera.

IP versión 6

IPv6 (Internet Protocol Version 6) es la última versión del protocolo IP. Ha sido diseñado por el IETF (Internet Engineering Task Force) para reemplazar en forma gradual a la versión actual, el IPv4.

El motivo para crear un nuevo protocolo ha sido la escasez de IP's en las direcciones IPv4 (32 bits), en cambio IPv6 ofrece un espacio de 128 bits. El reducido espacio de direcciones de IPv4, junto con el hecho de faltó coordinación para su asignación durante la década de los 80, sin ningún tipo de optimización, origina que en la actualidad ya se empiece a pensar en la implementación de este protocolo. Hoy en día IPv6 funciona perfectamente en algunos enlaces remotos y en telefonía IP. Todavía no se tiene previsto sustituir totalmente a IPv4 en las redes de computadora convencionales.

Debido a la multitud de nuevas aplicaciones en las que IPv4 es utilizado, ha sido necesario agregar nuevas funcionalidades al protocolo básico, aspectos que no fueron contemplados en el análisis inicial de IPv4, lo que genera complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más de dichas funcionalidades. Entre las más conocidas se pueden mencionar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPsec) y movilidad.⁵³

Características principales de IPv6:

- Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar: más niveles de jerarquías de direccionamiento y más nodos direccionales.
- Simplificación del formato del Header. Algunos campos del header IPv4 se quitan o se hacen opcionales

⁵³ <http://es.wikipedia.org/wiki/IPv6>

- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesamiento por parte del router.
- Posibilidad de paquetes con carga útil (datos) de más de 65.355 bytes.
- Seguridad en el núcleo del protocolo (IPsec). El soporte de IPsec es un requerimiento del protocolo IPv6.
- Capacidad de etiquetas de flujo. Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo de tráfico particular, que requieren manejo especial por los routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real. Por ejemplo video conferencia.
- Auto configuración: la auto configuración de direcciones es más simple. Especialmente en direcciones Aggregatable Global Unicast, los 64 bits superiores son seteados por un mensaje desde el router (Router Advertisement) y los 64 bits más bajos son seteados con la dirección MAC (en formato EUI-64). En este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse más por la máscara de red. Además el largo del prefijo no depende en el número de los hosts por lo tanto la asignación es más simple.
- Renumeración y "multihoming": facilitando el cambio de proveedor de servicios.
- Características de movilidad, la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.
- Ruteo más eficiente en el backbone de la red, debido a la jerarquía de direccionamiento basada en aggregation.
- Calidad de servicio (QoS) y clase de servicio (CoS).

ANEXO B. Otras tecnologías de interconexión de redes.

Redes de alto desempeño

Sabemos que para montar un red LAN, necesitamos de varias tecnologías de interconexión, Ethernet, fast Ethernet o wireless, pero cuando nuestra red llega a interconectarse con otra LAN o llega a formar parte de una WAN, estamos hablando de una red de alto desempeño, en donde podemos interconectar ciudades o incluso países a través de canales privados o canales virtuales de comunicación. Para esto existen otras tecnologías de interconexión. Hoy en día las más importantes Frame relay y ATM, la primera para transmitir datos especialmente y la segunda para transmitir cualquier tipo de tráfico.

Frame Relay

Frame Relay es una tecnología de alta velocidad basada en paquetes, con asignación dinámica del ancho de banda, alto rendimiento y bajo retardo, para soportar el incremento del tráfico de información en ambientes corporativos.

Frame Relay define un formato estandarizado para los Frames, los cuales son transmitidos sobre redes LANs interconectadas o sobre una red pública de datos. Un Frame es ensamblado por el equipo Terminal del usuario y es interpretado por los procesadores nodales de Frame Relay o en su caso por ruteadores remotos.⁵⁴

Descripción del Servicio:

- El “Frame Relay” es un servicio de transmisión de voz y datos a alta velocidad que permite la interconexión de redes de área local separadas geográficamente a un costo menor.
- Es una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de marcos (“frames”) para datos, perfecto para la transmisión de grandes cantidades de datos.
- Es utilizada ampliamente en los Estados Unidos y Europa.
- Ofrece mayores velocidades y rendimiento, a la vez que provee la eficiencia de ancho de banda que viene como resultado de los múltiples circuitos virtuales que comparten un puerto de una sola línea.

⁵⁴ http://www.telefonicapr.com/prtc/portal/channel2/0,1045,2108_224293,00.html

- Los servicios de Frame Relay son confiables y de alto rendimiento. Son un método económico de enviar datos, convirtiéndolo en una alternativa a las líneas dedicadas.
- Estos servicios se basan en nuestra plataforma multifuncional ATM de avanzada tecnología que satisface las exigencias de los programas de negocios actuales.
- El Frame Relay es ideal para usuarios que necesitan una conexión de mediana o alta velocidad para mantener un tráfico de datos entre localidades múltiples y distantes.

Aplicaciones y Beneficios:

- Reducción de complejidad en la red. Conexiones virtuales múltiples son capaces de compartir la misma línea de acceso.
- Equipo a costo reducido. Se reducen las necesidades del "hardware" y el procesamiento simplificado ofrece un mayor rendimiento por su dinero.
- Mejoramiento del desempeño y del tiempo de respuesta. Conectividad directa entre localidades con pocos atrasos en la red.
- Mayor disponibilidad en la red. Las conexiones a la red pueden redirigirse automáticamente a diversos cursos cuando ocurre un error en curso principal.
- Tarifa fija los precios no son sensitivos a la distancia - lo que significa que los clientes no son penalizados por conexiones a largas distancias.
- Mayor flexibilidad. Las conexiones son definidas por los programas. Los cambios hechos a la red son más rápidos y a menor costo si se comparan con otros servicios. Frame relay envía paquetes de tamaño variable, de 4Kbs a 8Kbs, denominados tramas. Esta tecnología garantiza un uso eficiente del ancho de banda disponible y es apta para transmitir datos o imágenes estáticas. Sin embargo resulta inapropiado para datos isocrónicos debido a que el tamaño grande y variable de sus tramas no permite garantizar un retardo de entrega constante.

Frame Relay proporciona conexiones entre usuarios a través de una red pública, del mismo modo que lo haría una red privada con circuitos punto a punto. Su gran ventaja es la de reemplazar las líneas privadas por un sólo enlace a la red. El uso de conexiones implica que los nodos de la red son conmutadores, y las tramas deben de llegar ordenadas al destinatario, ya que todas siguen el mismo camino a través de la red.

Las redes Frame Relay se construyen partiendo de un equipamiento de usuario que se encarga de empaquetar todas las tramas de los protocolos existentes en una única trama Frame Relay. También incorporan los nodos que conmutan las tramas Frame Relay en función del identificador de conexión, a través de la ruta establecida para la conexión en la red.

Frame Relay puede ser implementado en software (en un router), y por tanto puede ser mucho más barato; está orientado a conexiones, como la mayoría de las WAN's y puede empaquetar tramas de datos de cualquier protocolo de longitud variable. La carga del protocolo (overhead) de Frame Relay es menor de un 5%. Como desventaja tendríamos que mencionar que Frame Relay sólo ha sido definido para velocidades de hasta 1,544/2,048 Mbps. (T1/E1), aunque esto sin duda es algo temporal, además de que no soporta aplicaciones sensibles al tiempo, al menos de forma estándar.

ATM

ATM (Modo de Transferencia Asíncrona) es una tecnología que involucra un gran ancho de banda, una conmutación de bajo retardo y una multiplexación. El principal servicio que brinda ATM es el del relevo de celda CRS (Cell Relay Service). Una celda es un bloque de información de longitud fija, en el caso de ATM, es de 53 Octetos, de los cuales 5 se utilizan en la cabecera (identificación del canal, información para la detección de errores y si la celda es o no utilizada) y los 48 restantes en la zona de carga (protocolos AAL considerados como datos del usuario).⁵⁵

ATM envía paquetes de 53 bytes, el pequeño tamaño de los paquetes garantiza un mínimo retardo aunque supone un incremento del overhead: cuanto más pequeño es el paquete, más proporción hay de cabeceras y más pérdida de ancho de banda. La ventajas obtenidas es una baja latencia que permite transportar datos isocrónicos.

ATM puede ser considerado como una tecnología de conmutación de paquetes en alta velocidad con unas características particulares:

- Los paquetes son de pequeño y constante tamaño (53 bytes).
- Es una tecnología de naturaleza conmutada y orientada a la conexión.
- Los nodos que componen la red no tienen mecanismos para el control de errores o control de flujo.
- El header de las celdas ó paquetes tiene una funcionalidad limitada.

⁵⁵ <http://www.monografias.com/trabajos/atm/atm.shtml>

Simplificando al máximo podemos ver que una red ATM está compuesta por nodos de conmutación, elementos de transmisión y equipos terminales de usuarios. Los nodos son capaces de encaminar la información empaquetada en celdas a través de caminos conocidos como Conexiones de Canal Virtual. El routing, en los nodos conmutadores de células, es un proceso de hardware mientras que el establecimiento de conexiones y el empaquetamiento / desempaquetamiento de las células son procesos del software.

Dos de los conceptos más significativos del ATM, Canales Virtuales y Rutas Virtuales, están materializados en dos identificadores en el header de cada celda (VCI y VPI) ambos determinan el routing entre nodos. Existen dos formatos de celda: la UNI (User Network Interface) utilizado en el interfaz red/usuario y la NNI (Network Interface) cuando circulan por la red.

ATM es una tecnología altamente escalable capaz de manejar desde una WAN de grandes dimensiones, hasta de controlar el mismo bus interno de un ordenador personal. Una tecnología que puede simultáneamente transportar una videoconferencia y distribuir un paquete de software a escala mundial.

ANEXO C. Especificaciones de los dispositivos de enlace utilizados en el proyecto de red.

Como ya se había mencionado anteriormente, todos los dispositivos de red que se utilizaron en el proyecto, fueron de la marca Linksys a continuación se muestran las especificaciones de los mismos tal como las menciona el fabricante:

Wireless PCMCIA WPC54G.



Package Contents

- Wireless-G Notebook Adapter
- Setup Wizard CD-ROM
- User Guide on CD-ROM
- Quick Installation
- Registration Card Minimum Requirements
- 200 Mhz or Faster Processor
- 64 MB of RAM or Better
- Available CardBus Slot
- CD-ROM Drive
- Microsoft Windows 98SE, Millennium, 2000, or XP

Features

- Operates in the 2.4Ghz frequency spectrum with throughput of up to 54 Mbps
- Complies with IEEE 802.11g standards, and backwards compatible with IEEE 802.11b products
- 32-bit CardBus Interface
- Advanced security features including WEP, TKIP and 802.1x
- Compatible with Windows 98SE, Millennium, 2000 and XP
- Free technical support—24 hours a day, 7 days a week, toll-free US calls
- 3-year limited warranty

Specifications

Model Number: WPC54G

Standards: IEEE 802.11b, 802.11g

Modulations: 802.11b: CCK (11 Mbps), DQPSK (2 Mbps), DBPSK (1 Mbps);
802.11g: OFDM
Channels: 802.11b, 11 Channels (US, Canada) 802.11g 13 Channels (Europe)
Interface: CardBus
Speed: Up to 54Mbps
LEDs: Power, Link
Security: WEP, TKIP, 802.1x
WEP Key Bits: 64 Bit and 128 Bit

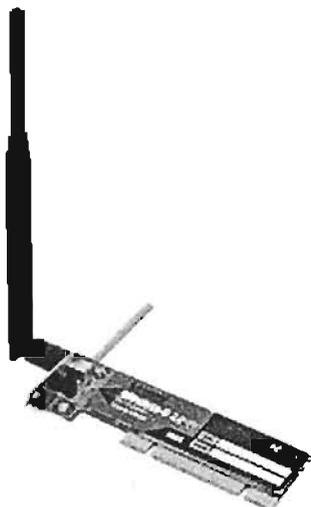
Environmental

Dimensions: 4.53" x 2.13" x 0.30" (115 mm x 54 mm x 7.5 mm) Unit Weight: 1.66 oz. (0.047 kg)
Power: 3.3V Bus powered
Certifications: FCC, IC-03, CE, WiFi (802.11b, 802.11g), WPA WHQL: 2000 and XP
Operating Temp.: 32°F to 131°F (0°C to 55°C)
Storage Temp.: -13°F to 158°F (-25°C to 70°C)
Operating Humidity: 5% to 95%, Non-Condensing
Storage Humidity: 5% to 95%, Non-Condensing

Minimum Requirements

- 500MHz or Faster Processor
- 128 MB of RAM
- Available PCI Slot
- CD-ROM Drive
- Windows 98SE, Me, 2000, or XP

Wireless PCI WMP54G.



Package Contents

- Wireless-G PCI Adapter
- External Antenna
- Setup Wizard CD-ROM with User Guide
- Quick Installation and Registration Card Minimum Requirements
- 500MHz or Faster Processor
- 128 MB of RAM
- Available PCI Slot
- CD-ROM Drive
- Windows 98SE, Me, 2000, or XP

Specifications

Model Number WMP54G

Standards IEEE 802.11g, 802.11b, PCI 2.2 and 2.3

LEDs Act: Solid when linked, flashes with traffic

Antenna 5 dBi

Transmit Power 15 dBm @ 54Mbps y 19 dBm @ 11Mbps

Sensitivity -70 dBm @ 54Mbps y -85 dBm @ 11Mbps

Security Features WEP (64-bit and 128-bit)

Modulation 802.11b: CCK (11Mbps), DQPSK (2Mbps), DBPSK (1Mbps); 802.11g:
OFDM

Network Protocols TCP/IP, IPX, NetBEUI

Environmental

Dimensions 4.80" x 8.46" x 0.91"W x H x D (122 mm x 215 mm x 23 mm)

Unit Weight 3.17 oz. (0.09 kg)

Power 3.3 V

Certifications FCC

Operating Temp. 0°C to 65°C (32°F to 150°F)

Storage Temp. -40°C to 85°C (-40°F to 185°F)

Operating Humidity 0% to 95%, Non-Condensing

Storage Humidity 0% to 95%, Non-Condensing

Warranty 3-Year Limited

Features

- Operates in the 2.4GHz frequency spectrum with data rates of up to 54Mbps
- Complies with IEEE 802.11g standard, and backwards compatible with IEEE 802.11b products
- Up to 128-bit WEP encryption
- 32-bit PCI interface
- Compatible with Windows 98SE, Millennium, 2000, and XP

Minimum Requirements

- 500MHz or Faster Processor
- 128 MB of RAM
- Available PCI Slot
- CD-ROM Drive
- Windows 98SE, Me, 2000, or XP.

Access Point WAP54G



Features

- IEEE 802.11g Supports Data Rates up to 54Mbps
- Backwards Compatible with Existing IEEE 802.11b Devices
- Setup Wizard for Easy Installation
- Supports WPA Security, 64/128-bit WEP Encryption
- Built in Web UI Configuration for easy configuration from any Web-browser
- Firmware upgradable through Web-browser
- Supports Wireless Bridging, MAC Address Filtering, and Event Logging

- Free Technical Support—24 Hours a Day, 7 Days a Week, Toll-Free US Calls
- 3-year limited warranty

Specifications

Model Number WAP54G

Standards IEEE 802.11g, IEEE 802.11b, IEEE 802.3, IEEE 802.3u

Ports One 10/100 Auto-Cross Over (MDI/MDI-X)

port, power port

Button Reset

Cabling RJ-45

LEDs Power, Activity, Link

Transmit Power 15dBm

Security Features WPA, WEP Encryption, MAC Filtering, SSID

Broadcast enable/disable

WEP Key Bits 64/128-bit

Environmental

Dimensions 7.32" x 1.89" x 6.65"

W x H x D (186 mm x 48 mm x 169 mm)

Unit Weight 16.23 oz. (0.46 kg)

Power External, 12V DC

Certifications FCC

Operating Temp. 32°F to 122°F (0°C to 40°C)

Storage Temp. -13°F to 158°F (-20°C to 70°C)

Operating Humidity 10% to 80% Non-Condensing

Storage Humidity 5% to 90% Non-Condensing

Package Contents

- Wireless-G Access Point
- Detachable Antennas
- Power Adapter
- Setup CD with User Guide
- Ethernet Network Cable
- Quick Installation
- Registration Card

Minimum Requirements

- PC with 200MHz or Faster Processor
- 64MB RAM Memory
- Internet Explorer 4.0 or Netscape Navigator 4.7 or higher for Web-based Configuration
- CD-ROM Drive
- Windows 98SE, Me, 2000, or XP
- 802.11b or 802.11g Wireless Adapter with TCP/IP Proto-col

SWITCH EGO08W



Specifications

Model Number EGO08W

Standards IEEE 802.3, 802.3u, 802.3x, 802.3ab

Ports 8 RJ-45 10/100/1000 Mbps ports

Cabling Type Category 5e Recommended

LEDs Power, Link/Act, Speed, FDX

Environmental

Dimensions 7.32" x 1.89" x 6.06"

(186 mm x 48 mm x 154 mm)

Unit Weight 1.1 lbs. (0.5 kg)

Power External Power Supply 12V DC, 2A. Input

110 V AC Consumption 18W

Certifications FCC Part 15 Class A

Operating Temp. 32°F to 122°F (-1°C to 50°C)

Storage Temp. -40°F to 158°F (-40°C to 70°C)

Operating Humidity 20% to 95%, Non-Condensing

Storage Humidity 20% to 95%, Non-Condensing

Package Contents

- One Gigabit 8-Port Workgroup Switch
- One AC Power adapter
- One registration card
- One User Guide

Minimum Requirements

- 200Mhz or Faster Processor
- 64MB RAM Recommended
- Ethernet or Gigabit Network Adapter
- Cat5e Ethernet Network Cable

Más información

E-mail: sales@linksys.com, support@linksys.com

Web: <http://www.linksys.com>