

ESCUELA POLITÉCNICA DEL EJÉRCITO
SEDE LATACUNGA

CARRERA DE INGENIERÍA
ELECTRÓNICA

Proyecto de Grado para la obtención del Título en
Ingeniería Electrónica en Instrumentación

“Estudio Diseño e Implementación de una red inalámbrica en el Instituto
Tecnológico Superior Aeronáutico”

Patricio Espín

Latacunga – Ecuador

2005

CERTIFICACIÓN

Se certifica que el presente trabajo fue desarrollado por el señor: Patricio Espín, bajo nuestra supervisión.

Ing. Eddie Galarza Zambrano
DIRECTOR DE TESIS

Ing. Nancy Guerrón Paredes
CO DIRECTOR DE TESIS

AGRADECIMIENTO

A mi familia mi esposa Gladys del Roció y a mis hijas Maria José y Geovanna Andrea que con su comprensión me han dado la tranquilidad para poder atender mis estudios

A la Escuela Politécnica del Ejercito y a sus docentes, por los conocimientos impartidos día a día durante el transcurso de mi carrera.

Al Ing. Eddie Galarza y la Ing. Nancy Guerrón, por compartir conmigo su valioso conocimiento y experiencia en el campo de la Electrónica.

A mis amigos por estar siempre a mi lado y por todos y cada uno de los momentos compartidos.

DEDICATORIA

El presente proyecto de Tesis esta dedicado de manera especial:

A Dios, por haberme concedido el don de la vida y ser mi guía en todo momento.

A mis padres, que desde el cielo me han dado la fuerza espiritual para poner todo mi empeño en la obtención de mi carrera.

A mi familia, quienes supieron darme el aliento y la fuerza necesaria para continuar y alcanzar la meta anhelada.

ÍNDICE

INTRODUCCIÓN

PAG

CAP. I GENERALIDADES DE REDES

1.1	CONCEPTO DE REDES	1
1.2	CLASES DE REDES	2
1.2.1	Lan (Local Area Network)	3
1.2.2	Wan (Wide Area network)	4
1.2.3	Man (Metropolitan Area Network)	6
1.3	REDES INALÁMBRICAS	7
1.3.1	Internet	8
1.3.2	Intranet	10
1.3.3	Extranet.....	12
1.4	COMPONENTES BÁSICOS DE UNA RED	12
1.4.1	Tarjetas de red	13
1.4.2	Tipos de tarjetas de red (Ethernet)	15
1.5	CABLEADO Y CONECTORES DE UNA RED	17
1.6	TIPOS DE CABLE	18
1.6.1	Cable par trenzado	18
1.6.2	tipos de cable par trenzado	20
1.6.3	El cable UTP	21
1.6.4	Fibra Óptica	24
1.7	CONCENTRADORES DE RED (HUBS)	26
1.7.1	Clasificación de los concentradores	28
1.8	SERVIDORES DE RED	30
1.9	ARQUITECTURA DE REDES	32
1.10	TOPOLOGÍA DE REDES	33
1.11	MÉTODO DE ACCESO	36
1.12	PROTOCOLO DE REDES	38

CAPÍTULO II REDES INALÁMBRICAS

2.1	INTRODUCCIÓN	41
-----	--------------------	----

2.2	CLASIFICACIÓN.....	42
2.3	GENERACIÓN DE RF ^{WIRELESS} INALÁMBRICAS CO ^{VI} .1N.....	48
2.4	ESTÁNDARES 802.11	49
2.5	DISPOSITIVOS WIRELESS	51
2.6	FUNCIONAMIENTO DE LOS DISPOSITIVOS	52
2.7	VELOCIDAD VS MODULACIÓN	55
2.8	TOPOLOGÍAS MODOS DE FUNCIONAMIENTO DE LOS DISPOSITIVOS	57
2.9	MESH NETWORKS	57
2.10	SEGURIDAD COMUNICACIONES WIRELESS	59
2.11	TÉCNICAS DE BÚSQUEDA REDES WIRELESS WARCHALKING	61
2.12	TÉCNICAS DE BÚSQUEDA REDES WIRELESS WARDRIVING	63
2.13	REDES DE RADIO FRECUENCIA	63

CAPÍTULO III INSTALAR UNA RED CON PUNTOS DE ACCESO

3.1	INTRODUCCIÓN	67
3.2	DONDE COLOCAR LOS PUNTOS DE ACCESO	69
3.2.1	Sobre la cobertura	70
3.2.2	Sobre la coexistencia de puntos de acceso	72
3.2.3	Sobre el ancho de banda	72
3.3	INSTALAR LA RED CON PUNTOS DE ACCESO	73
3.3.1	Análisis previo	75
3.4	CONFIGURAR LOS ORDENADORES	78
3.5	CONFIGURAR EL ADPTADOR DE RED	79

3.6	CONFIGURAR EL PROTOCOLO TCP/IP	81
3.7	CONFIGURAR EL PUNTO DE ACCESO	84
3.8	PROPIEDADES CONFIGURABLES EN EL PUNTO DE ACCESO	88
3.9	SELECCIÓN DEL CANAL	91
3.10	CONEXIÓN CON LA ^{VII} RED LOCAL E INTERNET	94
3.11	INTERCONEXIÓN DE LOS PUNTOS	95
3.12	COMPROBAR EL FUNCIONAMIENTO	95
3.13	GESTIÓN DE LA RED	98
3.14	MEDICIÓN DE LA VELOCIDAD	98
3.15	SOLUCIÓN DE PROBLEMAS	100
3.16	CONEXIONES MALAS	103

CAPÍTULO IV LA CONEXIÓN A INTERNET

4.1	INTRODUCCIÓN	104
4.2	EL ACCESO A INTERNET	105
4.3	ANCHO DE BANDA	105
4.4	EL PROVEEDOR DE ACCESO	106
4.4.1	Baja velocidad	106
4.4.2	Alta velocidad	107
4.5	EL ACCESO DE BANDA ANCHA	107
4.6	LAS VENTAJAS DE LA BANDA ANCHA	109
4.6.1	ACCESO MEDIANTE ADSL	109
4.6.2	ACCESO MEDIANTE MODEM CABLE	111
4.6.3	ACCESO POR SATÉLITE	112
4.6.4	ACCESO VIA RADIO LMDS	114
4.6.5	ACCESO MEDIANTE CIRCUITO DE DATOS	114
4.6.6	ACCESO MEDIANTE CIRCUITO PUNTO A PUNTO	115
4.7	CONEXIÓN WI-FI INTERNET	116
4.8	INSTALAR LA CONCESIÓN ENTRE WI-FI E INTERNET	117

4.9	CONFIGURAR LA CONEXIÓN EN EL PUNTO DE ACCESO	118
4.10	CONPROBACIÓN DEL ACCESO EN INTERNET	119
4.11	DIRECCIONES IP	120
4.11.1	IP internet del router	122
4.11.2	IP externa de l router	122
4.11.3	IP router remoto VIII	122

CAPÍTULO V IMPLEMENTACIÓN DE LA RED EN EL ITSA

5.1	INTRODUCCIÓN	124
5.2	ANÁLISIS DE LOS EQUIPOS EN EL MERCADO	125
5.3	ELECCIÓN DE LOS EQUIPOS A UTILIZAR	126
5.4	DETERMINAR LAS ANTENAS A UTILIZAR.....	126
5.5	EQUIPOS UTILIZADOS.....	127
5.5.1	ACCESS POINT DWL – 2000 AP +	127
5.5.2	ADAPTADOR DE RED DWL – G650 +	129
5.5.3	ADAPTADOR DE RED DWL – G520 +	131
5.5.4	DIPOLE ANTENNA DWL – 50 AT	133
5.5.5	ANTENNA OMNI ANT24 – 1500	134
5.5.6	ANTENNA PANEL DIRECTIONAL ANT24 – 1800	135
5.5.7	ANTENNA CONSTRUIDA	136
5.6	REDES CONFORMADAS	137
5.7	CONEXIÓN A INTERNET	142
5.8	IMPLEMENTACIÓN DE LA RED	148

CAPITULO VI CONCLUSIONES

6.1	CONCLUSIONES	150
6.2	RECOMENDACIONES	155

GLOSARIO
BIBLIOGRAFÍA

INTRODUCCIÓN

Una red es un conjunto de computadoras (dos como mínimo), que se unen a través de medios físicos (hardware) y lógicos (software), para compartir información y recursos, con el fin de llevar a cabo una actividad o labor de forma eficiente

Actualmente las transmisiones inalámbricas constituyen una eficaz y poderosa herramienta que permite la transferencia de voz, datos y video, sin la necesidad de utilizar cables para establecer la conexión.

Esta transferencia de información es lograda a través de la emisión de ondas de radio, permitiendo así tener dos grandes ventajas las cuales son la movilidad y flexibilidad del sistema en general.

En este trabajo realizamos la implementación de una red basada en puntos de acceso.

A las redes inalámbricas Wi – Fi con puntos de acceso se les conoce con el nombre de modo infraestructura.

La utilización de puntos de acceso es conveniente cuando se pretende crear una red permanente, aunque sea con pocos terminales, cuando se desea disponer de una amplia área de cobertura o crear una red inalámbrica con muchos usuarios. Dicho de otra forma, salvo que se vaya a realizar una comunicación esporádica entre dos o unos pocos más ordenadores se realizaría el modo ad hoc sin puntos de acceso.

Una ventaja adicional de las redes con los puntos de acceso es que se disfruta de ciertas características de gestión de red de las que carece completamente el modo ad hoc.

El propósito fundamental de la presente tesis es el de , diseñar e implementar una red inalámbrica en el edificio del Instituto Tecnológico Superior Aeronáutico (ITSA) con el fin de que los estudiantes puedan hacer uso del Internet o ingresar a la red administrativa del instituto disponiendo de una computadora portátil y una tarjeta de red inalámbrica, además

En una parte del Campus Tecnológico, en el sector donde más se concentran los estudiantes tendrán la misma facilidad.

También como parte de esta tesis se implementa un puente con el edificio comando del Ala No 12 con el fin de tener comunicación con esta dependencia ya que el ITSA es parte constitutiva del ALA No 12 y al momento no se tiene un enlace de datos e implementar un enlace de fibra óptica es muy costoso.

Para alcanzar el propósito citado anteriormente, se han desarrollado 6 capítulos.

El capítulo I comprende la información teórica de redes en general como concepto de redes, clases de redes, componentes básicos de una red, concentradores de red

En el capítulo II comprende lo que son redes inalámbricas, su clasificación, estándares 802.11, dispositivos wireless, funcionamiento, velocidad y modulación de los dispositivos, seguridad en las comunicaciones wireless

En el capítulo III se trata sobre como instalar una red inalámbrica con puntos de acceso donde se estudia como colocar estos puntos,

configurar los ordenadores, el adaptador de red, el protocolo TCP/IP, la selección de los canales

En el capítulo IV se determina como conectar la red al Internet , el ancho de banda, se analiza el proveedor de Internet, los diferentes accesos banda ancha, ADSL , MODEM, satélite, radio, se ve también la instalación y su configuración, y las distintas direcciones IP

En el capítulo V se implementa la red, realizando primeramente el análisis de los equipos existentes en el mercado, la elección del que se ajusta a las necesidades del proyecto y del Instituto, así como la elección de los equipos, las antenas, las características de lo utilizado, las redes que se conforman , como se acoplan a las redes ya existentes en el ITSA y los diferentes diagramas de conexión

Por último en el capítulo VI se determina las conclusiones y recomendaciones.

CAPÍTULO I

GENERALIDADES DE REDES

1.1 CONCEPTO DE REDES

Las redes de computadoras no son más que un conjunto de medios para proporcionar servicios de telecomunicación entre cierto número de ubicaciones. Una ubicación (fija o móvil) es conocida como punto de terminación de red o simplemente "ptr". Así pues, podríamos ver una red como algo abstracto que ofrece un determinado servicio en puntos de terminación de red (FIGURA I.1). También se puede definir "Una red es un conjunto de computadoras (dos como mínimo), que se unen a través de medios físicos (**hardware**) y lógicos (**software**), para compartir información y recursos, con el fin de llevar a cabo una actividad o labor de forma eficiente y eficaz (**FIGURA I.2**).".

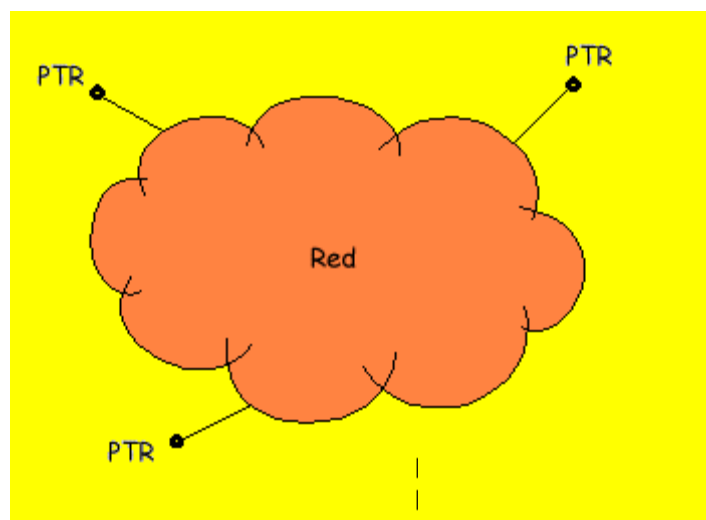


Figura 1.1. Red Abstracta

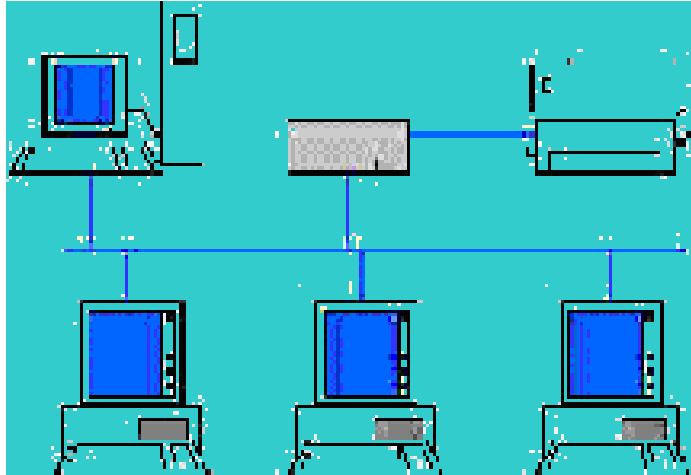


Figura 1.2. Red Real

Las redes se usan para:

- Compartir recursos, especialmente la información (los datos).
- Proveer la confiabilidad: más de una fuente para los recursos.
- La escalabilidad de los recursos computacionales: si se necesita más poder computacional, se puede comprar un cliente más, en vez de un nuevo mainframe.
- Comunicación.

1.2 CLASES DE REDES

Se puede clasificar las redes en cuanto a las dimensiones de la tecnología de transmisión y del tamaño

- **Tecnología de transmisión:**
 - **Broadcast:** Un solo canal de comunicación compartido por todas las máquinas. Un *paquete* mandado por alguna máquina es recibido por todas las otras.
 - **Point-to-point:** Muchas conexiones entre pares individuales de máquinas. (Los paquetes de A a B pueden atravesar máquinas intermedias, entonces) se necesita el ruteo (*routing*) para dirigir los paquetes de un nodo a otro.
- **Escala:**
 - Multicomputadores: 1 m
 - **LAN** (local area network): 10 m a 1 km o más
 - **MAN** (metropolitan area network): 10 km
 - **WAN** (wide area network): 100 km a 1.000 km
 - Internet: 10.000 km

1.2.1 LAN (LOCAL AREA NETWORK):

Son redes de propiedad privada que funcionan dentro de una oficina, edificio o terreno hasta unos cuantos kilómetros, generalmente son usadas para conectar computadoras personales y estaciones de trabajo en una compañía y su objetivo es compartir recursos e intercambiar información. Las redes de área local se distinguen de otro tipo de redes por su tamaño, cableado y tecnología de transmisión.

Generalmente una red LAN ([FIGURA 1.3](#)) es de tamaño restringido, limitando el tiempo de transmisión, lo cual hace factible que el diseño de la red simplifique la administración.

Las redes LAN generalmente usan una tecnología de transmisión que consiste en un cable sencillo, al cual se encuentran conectados todos los computadores, la velocidad tradicional de las redes de área local oscila entre 10 y 100 Mbps (Megabits por segundo), un Megabit son 1.000.000 de bits.).

Algunas de las características más notables de este tipo de RED son:

- Normalmente usan la tecnología de broadcast: un solo cable con todas las máquinas conectadas.
- El tamaño es restringido, así el tiempo de transmisión del peor caso es conocido.
- Velocidades típicas son de 10 a 100 Mbps

1.2.2 WAN (WIDE AREA NETWORK):

Es una red de gran alcance con un sistema de comunicaciones que interconecta redes geográficamente remotas, utilizando servicios proporcionados por las empresas de servicio público como comunicación vía telefónica o en ocasiones instalados por la misma organización. Una red se extiende por un área geográfica extensa (Ciudades, Países, Continentes) mantiene computadores con el propósito de ejecutar aplicaciones, a estos

computadores se les denomina **HOST**. Los host se encuentran conectados a subredes de comunicaciones, cuya función es conducir mensajes de un host a otro, a diferencia del sistema telefónico que conduce voz, los host conducen datos utilizando la misma vía (red telefónica).

Una red WAN también tiene la posibilidad de comunicarse mediante un sistema de satélite o radio, utilizando antenas las cuales efectúan la transmisión y la recepción.

Algunas de las características más notables de este tipo de RED son:

- Consisten en una colección de *hosts* (máquinas) o LANs de hosts conectados por una *subred*.
- La subred consiste en las líneas de transmisión y los *ruteadores*, que son computadores dedicados a cambiar de ruta.
- Se mandan los paquetes de un ruteador a otro. Se dice que la red es *packet-switched* (paquetes ruteados) o *store-and-forward* depende del tipo de router (guardar y reenviar).



Figura 1.3. Computadoras conectadas en red dentro de una oficina



Figura 1.4. Computadoras Conectadas en red en diferentes oficinas

1.2.3 MAN (METROPOLITAN AREA NETWORK):

Abarcan un área intermedia entre las LAN y las WAN. Es básicamente una versión más grande que las redes de área local (LAN), con una tecnología bastante similar. Una red de éste tipo,

puede manejar voz y datos e incluso podría estar relacionada con la red de televisión local por cable. Este estándar define un protocolo de gran velocidad, en donde los computadores conectados comparten un bus doble de fibra óptica utilizando el método de acceso llamado bus de cola distribuido.

1.3 REDES INALÁMBRICAS

Los computadores portátiles son el segmento más rápido de crecimiento en la industria de la computación. Los usuarios móviles de estos pequeños computadores quieren estar conectados en línea a su base de operaciones y necesitan obtener datos para sus aplicaciones sin estar atados a las comunicaciones terrestres. En algunos casos el obtener una conexión por cable es imposible, el ejemplo típico es un automóvil, por lo tanto se encuentra su interés en las redes inalámbricas.

Las redes inalámbricas se basan en el principio de conectar una antena a un circuito eléctrico en donde las ondas electromagnéticas se difunden para captarse en un receptor a cierta distancia.

Las redes inalámbricas son de gran importancia para los transportadores de carga pesada y pasajeros, vehículos de servicios público, personas que efectúen reparaciones en sitios de difícil acceso, y para las organizaciones militares, entre otras.

Presentan algunas desventajas como su velocidad de transmisión y recepción que puede alcanzar algunas decenas de Mbps lo cual es mucho más lento que en las redes de área local y redes de largo alcance. En algunas ocasiones las redes inalámbricas presentan interferencias de comunicaciones.

Algunas de las características más notables de este tipo de RED son:

- Una red inalámbrica usa radio, microondas, satélites, infrarrojo, u otros mecanismos para comunicarse.
- Se pueden combinar las redes inalámbricas con los computadores móviles, pero los dos conceptos son distintos:

Algunas utilidades:

Tabla 1.1 Algunas utilidades

Inalámbrico	Móvil	Aplicación
No	No	Workstations estacionarias
No	Sí	Uso de un portable en un hotel
Sí	No	LANs en un edificio sin cables
Sí	Sí	PDA (personal digital assistant)

1.3.1 INTERNET:

Es la mayor de las redes de computadoras existentes actualmente en el mundo, compuesta por millares de PCs

conectadas entre sí utilizando básicamente el medio telefónico a través del modem.

Uno de los aspectos más importantes de Internet es que utiliza una base tecnológica y protocolos de comunicación que son abiertos (no tiene un propietario exclusivo), permitiendo la comunicación integrada entre computadores de distintos fabricantes.

Sorprendentemente Internet no tiene dueño y ha surgido gracias a la colaboración entre académicos, investigadores, usuarios y empresas de todo el mundo.

Internet (FIGURA I.5) es una de la redes más flexibles del mundo de la teleinformática, dándole a las organizaciones acceso a mayor volumen de información, comunicaciones más baratas y una mayor flexibilidad que la que se puede obtener utilizando líneas privadas tradicionales.

Los beneficios generados por la tecnología Internet han contribuido al incremento del uso del entorno Internet en estos últimos años. El tráfico en la **web** ha crecido de unos cuantos centenares de miles de usuarios a millones, incrementándose el uso de gráficos, sonido, vídeo y otro tipo de datos que circulan a través de ella.

Este incremento de la riqueza informativa en Internet está dibujando un nuevo usuario. Cada vez aparecen nuevos servicios, nuevas posibilidades para el usuario: mandar o recibir presupuestos, registrarse y tener acceso a cursos de formación en línea, leer periódicos electrónicos, escuchar música, etc. Además, la explosión de las fuentes de datos ha llevado al desarrollo de navegadores que soportan una amplia gama de plataformas informáticas, incluyendo **Windows, Macintosh, IBM OS/2, Unix, etc.**

Los ínter nautas recuperan la información a través de los navegadores. Los navegadores de **Netscape y Microsoft** son las interfaces Internet más conocidas, ya que están presentes en la mayoría de las aplicaciones que residen en sistemas **Wintel (Windows/Intel)**.

- Una *Internet* es una red de redes vinculadas por **gateways**, que son computadores que pueden traducir entre formatos incompatibles.

La Internet es un ejemplo de una Internet:



Figura 1.5. Red Internet

1.3.2 INTRANET:

Es un tipo de red donde se incluye el uso de Tecnologías Internet, una red corporativa o empresarial, y la posibilidad de aislarse de la Internet global. Una Intranet es generalmente definida como el uso de tecnologías Internet dentro de una organización de un forma segura y fiable. Este entorno tiene el potencial de ser aislado y protegido pero no está definido como un entorno totalmente seguro necesariamente

La mayor diferencia entre las aplicaciones de Internet e Intranet está en los métodos de seguridad usados para dar privacidad, confidencialidad y integridad de datos. La seguridad se refiere a las políticas, acciones, y sistemas necesarios para proteger la integridad de la información de los sistemas de comunicación. Varios niveles de seguridad son necesarios para cumplir estos objetivos. Generalmente, los requisitos de seguridad de la información esta agrupados en las siguientes categorías:

- *Integridad de Información:* La garantía de que los datos no han sido alterados ni interceptados
- *Confidencialidad:* La garantía de que solo las personas a las que van dirigidas los datos acceden a estos
- *Autenticación:* La garantía de que el usuario o el grupo de trabajo que pide acceder a otro usuario, grupo de trabajo , recurso o servicio es realmente ese usuario o grupo de trabajo. Además, la garantía de que la información descrita y asociada con el autor, o administrador, de un objeto digital no sea desconocida.

- *Representación* La protección de usuarios, grupos de trabajo, recursos, y servicios de intrusiones para asegurar un determinado grado de disponibilidad, equilibrada con la importancia y sensibilidad de la información.

Establecer una intranet supone hablar de un potente sistema de comunicación, de reducción de costes, de mayor productividad y calidad, de mejorar la relación con proveedores y clientes, de obtener mayor información. Además, la instalación de una red interna dentro de la empresa supone una reconciliación con cuatro mundos dispersos: sistemas de información y bases de datos (sistemas de compra, finanzas), documentación técnica (planes, software, etc.), comunicación (correo electrónico, revistas, etc.), y el mundo exterior.

1.3.3. **EXTRANET:**

Una extranet es una red externa de colaboración que utiliza la tecnología Internet, y que interconecta a una empresa con sus proveedores, clientes u otros socios. El término ha sido acuñado para describir el software que facilita la relación entre diferentes compañías. Una extranet puede ser concebida como una parte de una intranet que es accesible para otras empresas o como una herramienta que permite la colaboración entre empresas. La información compartida podría ser accesible sólo para aquellos miembros colaboradores de la empresa que posee la intranet, y en algunos casos podría ser pública.

Una red externa de estas características tiene las siguientes aplicaciones:

- Grupos privados que cooperan con la empresa y que comparten la misma información e ideas.
- Entornos de colaboración donde algunas empresas colaboran en el desarrollo de una aplicación nueva que ellos pueden usar.
- Programas de formación u otros contenidos educativos que las empresas pueden desarrollar o compartir.
- Listas de catálogos de productos.
- Gestión de proyecto y control para empresas que forman parte de un mismo proyecto de trabajo.

1.4 COMPONENTES BÁSICOS DE UNA RED LAN

Existen elementos, desde el punto de vista del hardware, que son básicos para efectuar la conexión de redes, tales como:

1. TARJETAS DE RED (TARJETAS ETHERNET)
2. CABLEADO Y CONECTORES
3. CONCENTRADORES, HUB, ETC. (DEPENDIENDO DEL TIPO DE CABLEADO)
4. PC SERVIDOR O PCS SERVIDORES
5. IMPRESORA U OTROS RECURSOS QUE SE PUEDAN COMPARTIR
6. ESTACIONES DE TRABAJO O WORKSTATION



Figura 1.6. Componentes básicos de una red

1.4.1 TARJETAS DE RED:

Son tarjetas que se instalan en un computador con el fin de ofrecer la conexión física a una red. Cada tarjeta se encuentra diseñada para trabajar en un tipo de red específico y soporta una gran variedad de cables y tipos de bus (ISA, EISA, PCI, PCMCIA).

Las nuevas tarjetas de RED son configurables usando un programa de software que permite la configuración de los recursos asignados a la tarjeta y es mucho más fácil cuando es montada sobre los sistemas operativos que usen las librerías de auto configuración llamadas **Plug and Play**.

Las tarjetas de RED mas antiguas, utilizan un sistema de configuración a través de **Jumpers** (piezas que según su posición

y existencia permiten la configuración de un dispositivo), para la configuración de los recursos de la misma.

Los recursos utilizados por una tarjeta **ethernet**, son cuatro:

1. **Input/output Port Address** (Puerto de Dirección de entrada/salida): En el computador los puertos de entrada y salida de datos son usados por las tarjetas instaladas. Estos puertos están en un rango de dirección de 200h a 3FFh, que son para uso de comandos, respuestas de lectura y la transferencia de datos.
2. **Interrupt Request Line** (Solicitud de Interrupción): Es el canal requerido por la tarjeta para ser atendida por el procesador del computador.
3. **Direct Memory Request Line** (DMA): Es una dirección fija de la memoria RAM, para ser utilizada por la tarjeta.
4. **Buffers Memory Address**: Las tarjetas de RED utilizan espacios de memoria dejado entre la entrada y la salida de datos del puerto de direcciones y la transferencia de datos del procesador a la misma, este espacio es ocupado por el buffer de la tarjeta en la memoria RAM (C0000h) a (EFFFFh) y agiliza la entrada de la red al sistema operacional utilizado.

Las tarjetas de RED requieren un software para funcionar, el cual se denomina **Driver**, manejador o controlador. El driver es proporcionado en la mayoría de los casos por la empresa fabricante del producto o por los desarrolladores del software del sistema operacional en el cual funciona la tarjeta.

El driver posee las siguientes funciones: Inicialización de rutina, servicios de interrupción, procedimientos de enviar y recibir datos o información, procedimientos para el estado y control de la tarjeta.

1.4.2 TIPOS DE TARJETAS DE RED (ETHERNET):

Cada tarjeta de red (FIGURA I.7) tiene un conector para cada tipo de cable (coaxial, par trenzado, fibra óptica). Las tarjetas de red que funcionan para redes inalámbricas poseen una antena para comunicarse con la estación base.

La mayoría de tarjetas incluyen un zócalo para un **PROM** (Memoria programada de solo lectura, FIGURA I.7) , esta memoria realiza una inicialización remota del computador en donde se encuentra instalada, es decir, que una tarjeta con la memoria PROM puede ser instalada en computadores que no tienen instalado unidades de disco o de almacenamiento masivo, esta alternativa tiene la ventaja de rebajar costos y aumentar la seguridad de acceso a la red, ya que los usuarios no pueden efectuar copias de los archivos importantes, tampoco infectar con virus o utilizar software no autorizado. La memoria es programada para recoger la información de arranque del servidor de archivos en vez de hacerlo desde un disco local, la estación de trabajo efectúa la conexión desde la tarjeta a través de la PROM al servidor de archivos.

Las fábricas suministran las tarjetas de red y la PROM (memoria programable de solo lectura) en forma separada, información que se debe tener en cuenta al hacer el pedido.

Estos son dos ejemplos de tarjetas Ethernet existentes en el mercado de la computación y muestra de la posición del zócalo **EPROM**.



Figura 1.7. EtherLink III

En una red generalmente se usan dos clases de tarjetas; una con características especiales de configuración física para la máquina servidora o servidor de red y las tarjetas para las estaciones de trabajo o máquinas clientes. La tarjeta del servidor puede ser capaz de recibir y transmitir datos a velocidades altas, con el fin de proporcionar un excelente rendimiento al servidor, ya que maneja un tráfico exigente para los usuarios conectados a la red.

Las tarjetas de red para las estaciones de trabajo pueden no ser tan exigentes, esto depende de la carga de trabajo de la estación.

En el mercado se encuentran grandes innovaciones de tarjetas de red de varias casas fabricantes, que cambian de acuerdo a las necesidades de la red y la configuración del hardware del computador (servidor y estaciones de trabajo). Los tipos de tarjetas más comunes se basan en la tecnología del bus de la ranura en la que va a ser instalada, y al momento de adquirirla se debe verificar si posee drivers para el sistema operativo que usa el PC, DOS, WINDOWS 95, WINDOWS 98, WINDOWS MILENIUM, WINDOWS NT o 2000, WINDOWS XP, LINUX, UNIX, OS/2.

1.5 CABLEADO Y CONECTORES DE UNA RED

El cableado se refiere a los alambres que conectan los computadores individuales o grupos de computadores y terminales a una red. El cableado es utilizado en redes como un medio de transmisión bruto, el cual cumple la función de trasladar bits (datos) de un lugar a otro, existen varios tipos de cables con los cuales se puede efectuar la transmisión de datos o información, dependiendo del cable utilizado se maneja la topología de la red y sus componentes. El cable se instala normalmente en edificios por intermedio de canaletas o tubos subterráneos, los cables metálicos y coaxiales utilizan el cobre como principal material de transmisión para las redes, los cables metálicos están formados por hilos de par trenzado. El cable de fibra óptica se encuentra disponible con filamentos sencillos o múltiples, de plástico o de fibra de cristal.

Aunque el cableado parezca el elemento más simple de la RED puede ser el más costoso, comprometiendo el 50% del presupuesto total. El cableado también puede ser la mayor fuente de problemas que se presentan en la red, tanto en su instalación como en su mantenimiento, por lo tanto al hacer la instalación el cableado debe ser tomado muy en

serio, ya que la mala elección o la mala instalación puede ocasionar pérdidas en un futuro cercano o probablemente no tenga la oportunidad de volver hacer esta inversión nuevamente.

El cableado escogido para la RED debe ser capaz de transmitir cantidades masivas a grandes velocidades y a través de grandes distancias. Esta capacidad es llamada "**Alto Ancho de Banda**", que es importante para la transmisión de multimedia a través de la red.

1.6 TIPOS DE CABLE

1.6.1 CABLE PAR TRENZADO:

Por lo general, la estructura de todos los cables par trenzado no difieren significativamente, aunque es cierto que cada fabricante introduce algunas tecnologías adicionales mientras los estándares de fabricación se lo permitan. El cable está compuesto, como se puede ver en la figura 1.8, por un conductor interno que es de alambre electrolítico recocido, de tipo circular, aislado por una capa de polietileno coloreado.



Figura 1.8 Cable par trenzado

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

Un ejemplo de par trenzado es el sistema de telefonía, ya que la mayoría de aparatos se conectan a la central telefónica por medio de un par trenzado. Actualmente, se han convertido en un estándar en el ámbito de las redes LAN como medio de transmisión en las redes de acceso a usuarios (típicamente cables de 2 ó 4 pares trenzados). A pesar que las propiedades de transmisión de cables de par trenzado son inferiores, y en especial la sensibilidad ante perturbaciones extremas, a las del cable coaxial, su gran adopción se debe al costo, su flexibilidad y facilidad de instalación, así como las mejoras tecnológicas constantes introducidas en enlaces de mayor velocidad, longitud, etc.

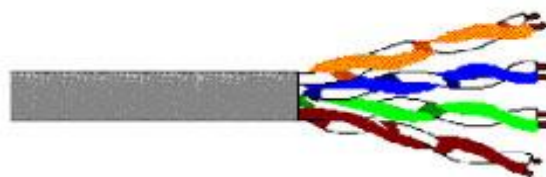


Figura 1.9 Cable par trenzado

Debajo del aislamiento coloreado existe otra capa de aislamiento también de polietileno, que contiene en su composición una sustancia antioxidante para evitar la corrosión del cable. El conducto sólo tiene un diámetro de aproximadamente medio

milímetro, y más el aislamiento el diámetro puede superar el milímetro.

Sin embargo es importante aclarar que habitualmente este tipo de cable no se maneja por unidades, sino por pares y grupos de pares, paquete conocido como cable multipar. Todos los cables del multipar están trenzados entre sí con el objeto de mejorar la resistencia de todo el grupo hacia diferentes tipos de interferencia electromagnética externa. Por esta razón surge la necesidad de poder definir colores para los mismos que permitan al final de cada grupo de cables conocer qué cable va con cual otro. Los colores del aislante están normalizados a fin de su manipulación por grandes cantidades. Para Redes Locales los colores estandarizados son:

Naranja/Blanco - Naranja

Verde/Blanco - Verde

Blanco/Azul - Azul

Blanco/Marrón - Marrón

1.6.2 TIPOS DE CABLE PAR TRENZADO:

Cable de par trenzado apantallado (STP):

En este tipo de cable, cada par va recubierto por una malla conductora que actúa de apantalla frente a interferencias y ruido eléctrico. Su impedancia es de 150 Ohm.

El nivel de protección del STP ante perturbaciones externas es mayor al ofrecido por UTP. Sin embargo es más costoso y

requiere más instalación. La pantalla del STP, para que sea más eficaz, requiere una configuración de interconexión con tierra (dotada de continuidad hasta el Terminal), con el STP se suele utilizar conectores RJ49.

Es utilizado generalmente en las instalaciones de procesos de datos por su capacidad y sus buenas características contra las radiaciones electromagnéticas, pero el inconveniente es que es un cable robusto, caro y difícil de instalar.

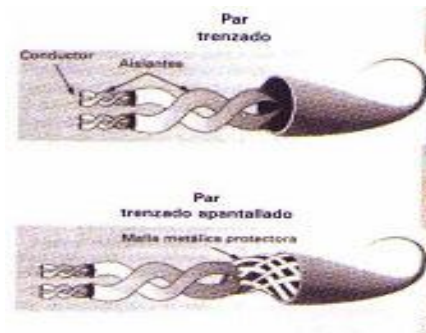


Figura 1.10. Cable Par Trenzado

1.6.3 EL CABLE UTP

El cable UTP es el más utilizado en telefonía.



Figura I.11 Cable UTP

Existe actualmente 8 categorías y cada una especifica las características eléctricas para el cable: atenuación, capacidad de la línea e impedancia.

Las categorías son las siguientes:

Categoría 1: Este tipo de cable esta especialmente diseñado para redes telefónicas, es el típico cable empleado para teléfonos por las compañías telefónicas. Alcanzan como máximo velocidades de hasta 4 Mbps.

Categoría 2: De características idénticas al cable de categoría1.

Categoría 3: Es utilizado en redes de ordenadores de hasta 16 Mbps. de velocidad y con un ancho de banda de hasta 16 Mhz.

Categoría 4: Esta definido para redes de ordenadores tipo anillo como Token Ring con un ancho de banda de hasta 20 Mhz y con una velocidad de 20 Mbps.

Categoría 5: Es un estándar dentro de las comunicaciones en redes LAN. Es capaz de soportar comunicaciones de hasta 100 Mbps. con un ancho de banda de hasta 100 Mhz. Este tipo de cable es de 8 hilos, es decir cuatro pares trenzados. La atenuación del cable de esta categoría viene dado por esta tabla referida a una distancia estándar de 100 metros:

Tabla 1.2 Distancias Estándar

Velocidad de transmisión de datos	<i>Nivel de atenuación</i>
4 Mbps	13 dB
10 Mbps	20 dB
16 Mbps	25 dB
100 Mbps	67 dB

Categoría 5e: Es una categoría 5 mejorada. Minimiza la atenuación y las interferencias. Esta categoría no tiene estandarizadas las normas aunque si está diferenciada por los diferentes organismos.

Categoría 6: No esta estandarizada aunque ya está utilizándose. Se definirán sus características para un ancho de banda de 250 Mhz.

Categoría 7: No está definida y mucho menos estandarizada. Se definirá para un ancho de banda de 600 Mhz. El gran inconveniente de esta categoría es el tipo de conector seleccionado que es un RJ-45.

En la tabla se puede ver para las diferentes categorías, teniendo en cuenta su ancho de banda, cual sería las distancia máxima recomendada sin sufrir atenuaciones que hagan variar la señal:

Tabla 1.3 Diferentes categorías

Ancho de banda	100 kHz	1 MHz	20 MHz	100 MHz
En categoría 3	2 km	500 m	100 m	No existe
En categoría 4	3 km	600 m	150 m	No existe

En categoría 5	3 km	700 m	160 m	100 m
----------------	------	-------	-------	-------

1.6.4 FIBRA ÓPTICA



Figura 1.12 Fibra Óptica

Para radiación electromagnética de muy alta frecuencia en el intervalo de la luz visible e infrarroja se utiliza un cable de fibra de vidrio que causa muy poca pérdida de energía luminosa a través de largas distancias. El diámetro de la fibra debe ser muy pequeño con el fin de minimizar la transmisión reflectora. La fibra transmisora central es de vidrio de baja pérdida y con índice de refracción relativamente alto.

Ésta se cubre con vidrio de mayor pérdida, con menor índice de refracción, para soporte y absorción de rayos

que puedan escapar de la fibra central. La fuente de luz en el transmisor puede ser un diodo emisor de luz (LED) o un láser. El detector en el otro extremo es un fotodiodo o un fototransistor.



Figura 1.13 Fibra óptica

La tecnología de la fibra óptica ha avanzado muy rápidamente. Existen en la actualidad dos métodos básicos -aunque se han desarrollado muchos más



Figura 1.14. Fibra óptica

para transmitir a través de un enlace por fibra. La transmisión óptica involucra la modulación de una señal de luz (usualmente apagando, encendiendo y variando la intensidad de la luz) sobre una fibra muy estrecha de vidrio (llamado núcleo).

La otra capa concéntrica de vidrio que rodea el núcleo se llama revestimiento. Después de introducir la luz dentro del núcleo ésta es reflejada por el revestimiento, lo cual hace que siga una trayectoria *zigzag* a través del núcleo.

Por lo tanto las dos formas de transmitir sobre una fibra son conocida como transmisión en ***modo simple*** y ***multimodo***.

1.7 CONCENTRADORES DE RED (HUBS):

Los concentradores (FIGURA 1.15) permiten la interconexión de diferentes uso a la red. Las redes locales en un principio fueron creadas llevando cable coaxial entre edificios efectuando conexiones punto a punto, cuando las estaciones se encontraban conectadas se colocaba en cada extremo de la red un terminador de red de 50 ohmios y se arrancaba la red. Con estos métodos de conexión se presentaban muchos problemas para que la red funcionara bien desde un principio, tales problemas eran básicamente: conectores mal ponchados o mal colocados, cables pisoteados o rotos, interferencias eléctricas externas y la localización de estos problemas resultaba complicada y difícil. Las topologías de las redes basadas en concentradores o hubs, fueron diseñadas para evitar algunos de estos problemas.



Figura 1.15 CONCENTRADORES DE RED (HUBS)

la primera generación de concentradores son una pieza fundamental en los sistemas de cableado estructurado, que soportan muchas tecnologías de redes de gran alcance y área local. El concentrador sirve como centro de conexión para la red de toda una planta o un edificio.

la segunda generación de concentradores (inteligentes) o concentradores multimedia, que permiten la conexión a diferentes medios físicos: 10BaseT, 10BaseF, 10Base2, 10Base5, etc. Esta segunda generación fue lanzada al mercado incluyendo funciones de administración, sistema para detección de fallas, módulos de enlace, módulos para recoger estadísticas sobre el funcionamiento de los concentradores.

la **tercera generación** son destinados a empresas; diseñados para soportar el cableado y las necesidades de interconexión de redes en una compañía, ya que son capaces de mantener sobre un mismo computador, un determinado número de redes, de tipo Ethernet, Token Ring y FDDI, con la capacidad de enrutamiento entre cada una de ellas (utilizando puentes o enrutadores), con diferentes tipos de medios físicos, y añadiendo una gestión más potente basada en protocolos estándar de gestión para su control, la arquitectura empleada entre ellos difiere pero se pueden considerar tres tipos diferentes:

- **Arquitectura multicanal:** Emplea varios canales que definen como redes diferentes tipo Ethernet, Token Ring o FDDI.
- **Arquitectura monocanal:** De alta velocidad, con comunicación sincrónica y asincrónica.
- **Arquitectura mixta:** Soporta los dos tipos de arquitecturas anteriores.

1.7.1 CLASIFICACIÓN DE LOS CONCENTRADORES:

De acuerdo como son utilizados en un sistema de cableado estructurado, se pueden definir tres categorías de concentradores:

- **Concentradores de grupo de Trabajo(Hub):** Es el que conecta un grupo de equipos de cómputo que se encuentran en una misma área de trabajo, por ejemplo los computadores que se encuentran en el mismo departamento.



Figura 1.16 Concentradores de grupo de trabajo

- **Concentrador Intermedio (switch):** Es el concentrador que se encuentra ubicado entre la central de distribución de conexiones de la red instalada y los concentradores de grupo de trabajo.



Figura 1.17 Concentrador Intermedio

- **Concentrador Principal:** Es el punto de conexión central para todos los sistemas finales conectados a los concentradores de grupos de trabajo y los concentradores intermedios.

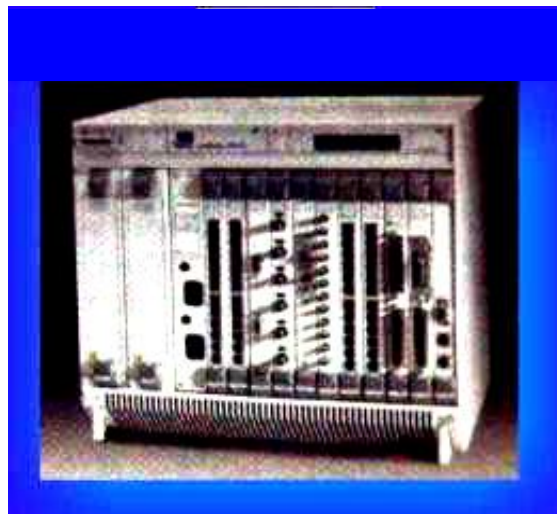


Figura 1.18 Concentrador principal

1.8 SERVIDORES DE RED:

Son unos equipos potentes que ofrecen servicios a uno o más PCs clientes, por ejemplo acceso a archivos, aplicaciones, cola de impresión, acceso remoto. En una red pueden existir varios servidores y cada uno de ellos cumplir con una función especial.

Los servidores los podemos clasificar en:

- **Servidores de Correo Electrónico:** Ofrecen los servicios de correo electrónico en el ámbito local o de toda la compañía y pueden efectuar la traducción entre diferentes tipos de correo.
- **Servidores de Fax:** Ofrece el servicio de fax para los usuarios de la red, la transmisión se realiza mediante tarjetas de fax-modem que van conectadas al servidor de fax, éste es dirigido al usuario indicado.
- **Servidor de Copias de Seguridad:** Realiza las copias de seguridad de otros servidores o computadores de usuario en la red.
- **Servidor de Impresoras:** Es el servidor que permite la rápida impresión en una o más impresoras en la red, permitiendo a cualquier usuario, según los derechos establecidos, enviar trabajos a estas impresoras compartidas; el sistema es controlado por colas de impresión, donde el administrador de impresoras es el que organizan el trabajo de acuerdo al orden recibido y las prioridades dependiendo del usuario.
- **Servidor de Base de Datos:** Es utilizado cuando hay necesidad de almacenar y procesar grandes cantidades información y brindar la información necesaria de una forma más eficaz a los usuarios.
- **Servidor de Dominio:** Es el servidor que se encarga de verificar, a través de las cuentas de usuario, el acceso de los mismos a la red y a determinados recursos compartidos.
- **Estaciones de Trabajo o Workstation:** Es un computador que trabaja como estación de usuario en la red, el cual utiliza los recursos que el servidor tiene a su disposición.



Figura 1.19 Workstation

1.9 ARQUITECTURA DE REDES

La comunicación debe ser, al menos, entre dos partes, las cuales establecen una conversación o sesión a través de las redes, requiriéndose que ambas partes estén de acuerdo en ciertas cosas básicas:

- En establecer la comunicación
- En el formato de los datos
- En la velocidad de transmisión de los datos
- En definir direcciones.
- En definir numeración de los paquetes para mantener el orden para el envío y recepción de los mismos.
- Otros mecanismos, por ejemplo, para el manejo de los errores de transmisión, desconexión, etc.

Es frecuente que estos sistemas de control se incorporen por software a cada uno de los dispositivos de la red. Bajo el concepto de Ingeniería del software, es común encontrar el software organizado en capas o layers en los cuales se agrupan "especializaciones", de la secuencia de tareas a realizar.

Al conjunto de capas y protocolos se le denomina arquitectura de red.

La estructura general de una red de telecomunicaciones, está formada por tres elementos principales:

- Nodo
- Enlace
- Protocolo

Nodo: Localización física de un proceso.

Enlace: Es el vínculo que existe entre nodos, a través del cual fluye la información.

Protocolo de redes: Definición en términos de redes, "Es el conjunto de reglas previamente establecidas que definen los procedimientos para que dos o mas procesos intercambien información. Además, se dice que estas reglas definen la sintaxis, la semántica y la sincronización del protocolo."

1.10 TOPOLOGÍAS DE REDES:

La topología en una red es las configuración adoptada por las estaciones de trabajo para conectarse entre si.

- **Topología Bus (Lineal):** Todas las estaciones se conectan directamente a un único canal físico (cable) de comunicación (bus). Según los sentidos posibles de transmisión, el bus puede ser unidireccional (principalmente buses de fibra óptica, los extremos del canal (cable) no están interconectados sino simplemente finalizados con un terminador de 50 ohmios, el terminador elimina automáticamente la señal de los extremos, es posible unir varios segmentos de buses en una configuración "multibus" siendo necesario utilizar repetidores de señal en el caso de grandes distancias.

El procedimiento de comunicación utilizando en los buses bidireccionales es el de difusión ("Broadcast") por el canal: Todas las estaciones de trabajo reciben simultáneamente el mensaje enviado, aunque solo es procesado por aquella a la que va dirigido. Al ser el bus un canal compartido existen dos problemas que deben ser resueltos a nivel de protocolo: Uno es que varios dispositivos intenten transmitir al mismo tiempo sobre el bus, produciéndose una colisión (se mezclan los mensajes y el resultado es incomprendible)

Por otro lado cuando una estación esté transmitiendo continuamente y monopolice la red. Para evitar eso, los mensajes se transmiten troceados en paquetes de datos más pequeños, haciendo una pausa entre los mismos para dar la oportunidad de transmitir a otras estaciones.

- **Topología en anillo (ring):** El medio de comunicación de una red en anillo, es que forma un bucle cerrado en el que se integran todas las estaciones de la red, mediante un pequeño repetidor que interrumpe el canal (nodo activo de regeneración de la señal), de modo que cada una de las estaciones mantienen la conexión con las otras adyacentes.

Los datos son transmitidos por el anillo de estación a estación en un solo sentido (Unidireccional), desde el origen al destino pasando por todas las estaciones intermedias que forman parte de esta topología.

En el anillo tanto el medio como cada uno de los nodos activos resultan absolutamente críticos. Existen mecanismos para reducir este riesgo, basado en la duplicación de los citados elementos críticos.

Otro riesgo de la topología en anillo, es el de la información caducada, ya que dada su estructura cerrada, al contrario de lo que sucede en el bus, la eliminación de ésta no se produce automáticamente, sino que debe existir un mecanismo específico a cargo del emisor o del destinatario de una estación especial dedicada.

- **Topología Estrella:** Es otra de las tres principales topologías. La red se une en un único punto, normalmente con control centralizado, como un concentrador de cable. Todas las estaciones se conectan al concentrador y las señales son distribuidas a todas las estaciones específicas del concentrador.
- **Topología Bus en estrella:** El fin es igual a la topología anterior. En este caso la red es un bus que se cablea físicamente como una estrella por medio de concentradores. Una red que tiene grupos de estaciones configuradas en estrella conectada con tramos largos de bus lineal.

Si todas las estaciones se encuentran en fila (como en un salón de clases o a lo largo de un pasillo en un edificio de oficinas), es una topología de Bus la cual utiliza cable coaxial ethernet. El 10BaseT de Ethernet es una topología

de estrella/bus que utiliza cable par trenzado para conectar estaciones al concentrador central, la interrupción en un cable solo afecta la estación conectada al segmento del cable. En una red de bus ethernet y una red de estrella/bus ethernet, las señales de las estaciones son difundidas a todas las estaciones del mismo segmento.

- **InterRedes:** Un nuevo concepto que ha surgido a partir de todos estos esquemas, es el concepto de InterRedes, que es el hecho de vincular redes como si se vincularán estaciones.

Este concepto, y las ideas que de este surgen, hace brotar un nuevo tipo especial de dispositivo que es un vinculador para interconectar redes entre sí (La tecnología de Internet está basada en el concepto de InterRedes), e dispositivo en cuestión se denomina "dispositivo de interconexión". Es decir, lo que se conecta, son redes locales de trabajo.

Una red de interconexión consta de LANs de diferentes departamentos o sitios que se interconectan con Bridges o routers.

Un enlace central es utilizado a menudo en los entornos locales, como un edificio. Los servicios públicos como las empresas de telefonía, proporcionan enlaces de área metropolitana o de gran alcance utilizan las tres topologías.

- **Red de enlace central:** Una red de enlace central se encuentra generalmente en los entornos de oficina o campos, en los que las redes de los pisos de un edificio se interconectan sobre cables centrales. Los Bridges y los Routers gestionan el tráfico entre segmentos de red conectados.

- **Red de malla:** Esta involucra o se efectúa a través de redes WAN, una red malla contiene múltiples caminos, si un camino falla o está congestionado el tráfico, un paquete puede utilizar un camino diferente hacia el destino. Los routers se utilizan para interconectar las redes separadas.
- **Red de estrella Jerárquica:** Esta estructuras de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada para formar una red jerárquica. Los concentradores configurados en estrellas por pisos o por departamentos están unidos por un concentrador central que maneja el tráfico de la interconexión de la red.

1.11 MÉTODOS DE ACCESO:

Una de las características más importantes de las LANs, es que son redes compartidas en las que están conectadas varias estaciones, pero solo una estación de trabajo puede efectuar transmisión en un momento determinado. El método de acceso al cable define el protocolo de comunicación que una estación de trabajo debe seguir para realizar una transmisión en un cable compartido.

Los métodos de acceso a cable primario son:

- La detección de la portadora.
- El paso de testigo.

Estos dos métodos definen básicamente las redes Ethernet y Token Ring. Estos métodos y uno nuevo se describen a continuación:

- **Acceso Múltiple por detección de portadora/detección de colisiones (CSMA/CD):** En éste sistema, las estaciones de trabajo conectadas a la red escuchan un tono de la portadora en el cable y envían la información en el momento que otras estaciones no están transmitiendo. El acceso múltiple significa que muchas estaciones comparten en mismo cable. Si dos o más estaciones detectan que la red está preparada para transmitir, pueden intentar acceder a esta de forma simultanea, provocando colisiones. Cada estación de trabajo debe entonces abandonar la operación y esperar una cierta cantidad de tiempo antes de empezar a retransmitir. El aumento del número de estaciones de la red incrementa la colisión, pero se puede dividir en segmentos, para evitar la congestión.
- **Paso de testigo:** El testigo es un paquete de datos, especial de las redes Token Ring, y la interfase de datos distribuida de fibra óptica que controla el acceso a la red.

Una estación de trabajo toma el control del paquete de datos testigo y tiene derecho de comunicar con la red. La diferencia con ethernet es que las estaciones no acceden simultáneamente a la red. Solamente transmite una estación de trabajo que obtiene el paso de testigo disponible.

- **Método de Acceso por prioridad de demandas:** Este es un sistema de acceso relativamente novedoso para ethernet de 100 Mbps. Este devuelve la operación del acceso a la red a un concentrador central , en vez de confiar en las estaciones de trabajo individuales para determinar cuando deben acceder al cable. Las estaciones de trabajo piden permiso para transmitir en la base de

datos a una prioridad y el concentrador transmite los datos de mayor jerarquía.

1.12 PROTOCOLO DE REDES:

"Es el conjunto de reglas previamente establecidas que definen los procedimientos para que dos o mas procesos intercambien información. Además, se dice que estas reglas definen la sintaxis, la semántica y la sincronización del protocolo."

- **Protocolos de bajo nivel:** El protocolo de bajo nivel es, en cierto modo, la forma en que las señales se transmiten por el cable, transportando tanto datos como información y los procedimientos de control de uso del medio por las diferentes estaciones de trabajo. Los protocolos de bajo nivel más utilizados son:
 - Ethernet.
 - Token Ring.
 - Token Bus.
 - FDDI
 - HDLC.

Los protocolos de bajo nivel, controlan el acceso al medio físico, lo que se conoce como MAC (Media Access Control), y además, parte del nivel de transmisión de datos, ya que se encargan también de las señales de temporización de la transmisión.

El protocolo de bajo nivel llamado **Ethernet**, fue diseñado originalmente por Digital, Intel y Xerox, por lo cual, la especificación original se conoce como ETHERNET DIX. Posteriormente IEEE ha definido el estándar ETHERNET 802.3. La forma de codificación difiere ligeramente en ambas definiciones.

Es el método de conexión más utilizado o extendido en la actualidad.

La velocidad de transmisión de datos es de 10 Mbps.

- **Protocolos lógicos de RED:** El protocolo lógico de red determina el modo y organización de la información (tanto datos como controles), para su transmisión por el medio físico con el protocolo de bajo nivel. Los protocolos de éste tipo mas comunes son:
 - **IPX/SPX (Internet Packet eXchange/Sequenced Packet eXchange):** Es el protocolo utilizado por el conocido Sistema Operativo de Redes Netware de Novell. SPX actúa sobre IPX para asegurar la entrega de los datos.
 - **TCP/IP:** Este no es un protocolo, sino un conjunto de protocolos, que toma su nombre de los dos más conocidos: TCP (Transmission Control Protocol, Protocolo de Control de Transmisión) e IP (Internet Protocol, Protocolo de Internet). Esta familia de protocolos es la base de la conocida y muy famosa RED INTERNET, la mayor red de ordenadores del mundo.
 - **Apple Talk:** Este protocolo está incluido en el sistema operativo del ordenador Apple Macintosh desde su aparición y permite interconectar ordenadores y periféricos con gran sencillez para el usuario, ya que no requiere ningún tipo de configuración por su parte, el sistema operativo se encarga de todo.
 - **NetBEUI: NetBIOS Extended User Interface (Intefaz de Usuario Extendido para NetBIOS).** Es la versión de Microsoft del NetBIOS (Network Basic Input/Output System, sistema básico de entrada/salida de red), que es el sistema de enlazar el software y el hardware de red en las PCs. Este protocolo es la base de la red de Microsoft Windows para Workgroup o Windows o para trabajo en

grupo. El eje fundamental de las redes basadas en sistema operativos de Microsoft, específicamente Windows.

CAPÍTULO II

REDES INALÁMBRICAS

2.1 INTRODUCCIÓN

Desde hace relativamente poco tiempo, se está viviendo lo que puede significar una revolución en el uso de las tecnologías de la información tal y como lo conocemos. Esta revolución puede llegar a tener una importancia similar a la que tuvo la adopción de Internet por el gran público.

De una forma callada, las **redes inalámbricas** o **Wireless Networks** (WN), se están introduciendo en el mercado de consumo gracias a unos precios populares y a un conjunto de entusiastas, mayoritariamente particulares, que han visto las enormes posibilidades de esta tecnología.

Las aplicaciones de las redes inalámbricas son infinitas. De momento van a crear una nueva forma de usar la información, pues ésta estará al alcance de todos a través de Internet en cualquier lugar (en el que haya cobertura).

En un futuro cercano se reunificarán todo aquellos dispositivos con los que hoy contamos para dar paso a unos nuevos que perfectamente podrían llamarse Terminales Internet en los cuales estarían reunidas las funciones de teléfono móvil, agenda, terminal de vídeo, reproductor multimedia, ordenador portátil y un largo etcétera.

Se podría dar lugar a una Internet paralela y gratuita la cual estaría basada en las redes que altruistamente cada uno de nosotros pondríamos a disposición de los demás al incorporarnos a las mismas como destino y origen de la información.

En las grandes ciudades por fin se podría llevar a cabo un control definitivo del tráfico con el fin de evitar atascos, limitando la velocidad máxima y/o indicando rutas alternativas en tiempo real.

Las tecnologías que son necesarias para llevar a cabo estos sistemas hoy existen desde ayer, su precio es mínimo o al menos muy asequible y su existencia mañana sólo depende de las estrategias comerciales de las empresas que las poseen.

Es necesario tener un cierto conocimiento sobre la tecnología que va a ser la base de estas aplicaciones, sobre las redes inalámbricas.

2.2 CLASIFICACIÓN

Lo primero que hay que hacer antes que nada, es situarse dentro del mundo inalámbrico. Para ello se hace una primera clasificación que centre ante las diferentes variantes que se encuentran:

- Redes inalámbricas personales
- Redes inalámbricas de consumo
- Redes inalámbricas 802.11

Redes inalámbricas personales

Dentro del ámbito de estas redes se puede integrar a dos principales actores:

a- En primer lugar y ya conocido por muchos usuarios están las redes que se usan actualmente mediante el intercambio de información mediante **infrarrojos**. Estas redes son muy limitadas dado su corto alcance, necesidad de "visión sin obstáculos" entre los dispositivos que se comunican y su baja velocidad (hasta 115 kbps). Se encuentran principalmente en ordenadores portátiles, PDAs (Agendas electrónicas personales), teléfonos móviles y algunas impresoras.

b- En segundo lugar el **Bluetooth**, estándar de comunicación entre pequeños dispositivos de uso personal, como pueden ser los PDAs, teléfonos móviles de nueva generación y algún que otro ordenador portátil. Su principal desventaja es que su puesta en marcha se ha ido retrasando desde hace años y la aparición del mismo ha ido plagada de diferencias e incompatibilidades entre los dispositivos de comunicación de los distintos fabricantes que ha imposibilitado su rápida adopción. Opera dentro de la banda de los 2,4 Ghz.

Redes inalámbricas de consumo

a- Redes CDMA (estándar de telefonía móvil estadounidense) y **GSM** (estándar de telefonía móvil europeo y asiático). Son los estándares que usa la telefonía móvil empleados alrededor de todo el mundo en sus diferentes variantes.

b- 802.16 son redes que pretenden complementar a las anteriores estableciendo redes inalámbricas metropolitanas (**MAN**) en la banda de entre los 2 y los 11 Ghz.

Redes inalámbricas 802.11

El estándar 802.11 fue desarrollado por el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), y define las opciones para la Capa Física de las transmisiones inalámbricas y la Capa de protocolos MAC (Control de Acceso al Medio). Representa además el primer estándar para los productos orientados a las WLAN. Además el IEEE maneja la mayoría de las normas para LAN cableada. La mayoría de los productos WLAN disponibles hoy en día en el mercado, son objeto de aplicaciones verticales que utilizan soluciones propietario, funcionando en bandas de frecuencia ISM (Bandas de Aplicaciones Industriales, Científicas y Médicas) de 900 Mhz y 2,4 Ghz. La norma IEEE 802.11 fue aprobada en junio de 1997 y especifica un subnivel de Control de Acceso al Medio (MAC) y 3 especificaciones para el nivel físico. El MAC proporciona los siguientes servicios: autenticación, deautenticación, privacidad, envío **MSDU** (servicios de estación), de asociación, distribución, integración y reasociación (servicios del sistema de distribución).

El estándar IEEE 802.11 define el protocolo para dos tipos de redes:

- Redes Ad-hoc, esta es una red simple donde se establecen comunicaciones entre las múltiples estaciones en un área de cobertura dada sin el uso de un punto de acceso o servidor. La norma especifica la etiqueta que cada estación debe observar para que todas ellas tengan un acceso justo a los medios de comunicación inalámbricos. Proporciona métodos de petición de arbitraje para utilizar el medio para asegurarse de que el rendimiento se maximiza para todos los usuarios del conjunto de servicios base. Las estaciones en este tipo de configuración se llaman **BBS** (Basic Service Set). Sin el **ESS** (Extended Service Set) las estaciones operan en un BSS independiente (**IBSS**).

- Redes Cliente/Servidor, ésta es una red que utiliza un punto de acceso que controla la asignación del tiempo de transmisión para todas las estaciones y permite que estaciones móviles deambulen por la columna vertebral de la red cliente/servidor. El punto de acceso se usa para manejar el tráfico desde la radio móvil hasta las redes cliente/servidor cableadas o inalámbricas. Esta configuración permite coordinación puntual de todas las estaciones en el área de servicios base y asegura un manejo apropiado del tráfico de datos. El punto de acceso dirige datos entre las estaciones y otras estaciones inalámbricas y/o cliente/servidor de la red. Típicamente las WLAN controladas por un punto de acceso central proporcionará un rendimiento mucho mayor. La configuración de la infraestructura es como se describe a continuación; las estaciones se comunican a puntos de acceso (Access point) que son parte del Sistema de Distribución. Un punto de acceso sirve a las estaciones en un **BSS**. El conjunto de **BSSs** se llama **ESS** (Extended Service Set). La norma sólo especifica el interface inalámbrico, es decir, entre estaciones y entre estaciones y puntos de acceso. Con un sistema de distribución, el área de cobertura se puede extender tanto como lo permitan las características del sistema.

La norma proporciona los servicios mencionados arriba con la siguiente funcionalidad: roaming dentro de un ESS, múltiples velocidades en BSSs y Administración de Energía (las estaciones pueden apagar sus transceptores para ahorrar energía).

El protocolo **MAC** es **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance).

La norma proporciona 2 especificaciones para Nivel Físico a través de radio de espectro disperso operando en la banda de 2400 - 2483.5 MHz y una para transmisión infrarroja.

Salto de frecuencia (FHSST: Tecnología de espectro ensanchado de saltos de frecuencia)

Este Sistema opera a 1 Mbps y, opcionalmente, a 2 Mbps. La versión a 1 Mbps utiliza modulación GFSK (Gaussian Frequency Shift Keying) de 2 niveles, mientras que la versión de 2 Mbps utiliza modulación GFSK de 4 niveles.

Secuencia directa (DSSST: Tecnología de espectro ensanchado de secuencia directa)

Este Sistema proporciona operación tanto a 1 como a 2 Mbps. La versión a 1 Mbps utiliza modulación DBPSK (Differential Binary Phase Shift Keying) mientras que la versión de 2 Mbps utiliza modulación DQPSK (Differential Quadrature Phase Shift Keying).

Infrarrojo

Este PHY opera a 1 Mbps y, opcionalmente, a 2 Mbps. La versión a 1 Mbps utiliza modulación por posición de pulso con 16 posiciones (16-PPM) de 2 niveles, mientras que la versión de 2 Mbps utiliza modulación 4-PPM.

Las **redes inalámbricas** o **WN** básicamente se diferencian de las redes conocidas hasta ahora por el enfoque que toman de los niveles más bajos de la pila OSI, el nivel físico y el nivel de enlace, los cuales se definen por el 802.11 del **IEEE (Organismo de estandarización internacional)**.

Como suele pasar siempre que un estándar aparece y los grandes fabricantes se interesan por él, aparecen diferentes aproximaciones al mismo lo que genera una incipiente confusión.

Nos encontramos ante tres principales variantes:

a- 802.11a:

Fue la primera aproximación a las **WN** y llega a alcanzar velocidades de hasta 54 Mbps dentro de los estándares del IEEE y hasta 72 y 108 Mbps con tecnologías de desdoblamiento de la velocidad ofrecidas por diferentes fabricantes, pero que no están (a día de hoy) estandarizadas

por el IEEE. Esta variante opera dentro del rango de los 5 Ghz. Inicialmente se soportan hasta 64 usuarios por Punto de Acceso.

Sus principales ventajas son su velocidad, la base instalada de dispositivos de este tipo, la gratuidad de la frecuencia que usa y la ausencia de interferencias en la misma.

Sus principales desventajas son su incompatibilidad con los estándares - **802.11b** y **g**, la no incorporación a la misma de **QoS** (posibilidades de asegurar de Calidad de Servicio, lo que en principio impediría ofrecer transmisión de voz y contenidos multimedia online), la no disponibilidad de esta frecuencia en Europa dado que está reservada a la **HyperLAN2** y la parcial disponibilidad de la misma en Japón.

b- 802.11b:

Es la segunda aproximación de las **WN**. Alcanza una velocidad de 11 Mbps estandarizada por el IEEE y una velocidad de 22 Mbps por el desdoblamiento de la velocidad que ofrecen algunos fabricantes pero sin la estandarización (a día de hoy) del IEEE. Opera dentro de la frecuencia de los 2'4 Ghz. Inicialmente se soportan hasta 32 usuarios por PA.

Adolece de varios de los inconvenientes que tiene el **802.11a** como son la falta de QoS, además de otros problemas como la masificación de la frecuencia en la que transmite y recibe, pues en los 2'4 Ghz funcionan teléfonos inalámbricos, teclados y ratones inalámbricos, hornos microondas, dispositivos **Bluetooth**, lo cual puede provocar interferencias.

En el lado positivo está su rápida adopción por parte de una gran comunidad de usuarios debido principalmente a unos muy bajos precios de sus dispositivos, la gratuidad de la banda que usa y su disponibilidad gratuita alrededor de todo el mundo. Está estandarizado por el IEEE.

c- 802.11g:

Es la tercera aproximación a las **WN**, y se basa en la compatibilidad con los dispositivos **802.11b** y en el ofrecer unas velocidades de hasta 54 Mbps. Funciona dentro de la frecuencia de 2,4 Ghz.

Dispone de los mismos inconvenientes que el **802.11b** además de los que pueden aparecer por la aún no estandarización del mismo por parte del IEEE (puede haber incompatibilidades con dispositivos de diferentes fabricantes).

Las ventajas de las que dispone son las mismas que las del 802.11b además de su mayor velocidad.

2.3 LA PRÓXIMA GENERACIÓN DE REDES INALÁMBRICAS CON EL 802.11n

En respuesta a la demanda del mercado creciente para redes de áreas locales inalámbricas (WLAN) de alto rendimiento, el Instituto de electrónica e ingenieros electrónicos - Asociación de estándares (IEEE-SA) ha aprobado la creación del Grupo de enfoque n (802.11 TGn) del IEEE 802.11 durante el segundo semestre de 2003. El alcance del objetivo del TGn consiste en definir modificaciones para la Capa física y la Capa de control del acceso al medio (PHY/MAC) que generen resultados de un mínimo de 100 megabits por segundo (Mbps) en el MAC SAP.

Los resultados mínimos requeridos representan un incremento 4 veces superior, aproximadamente, en el rendimiento de WLAN en comparación con las redes 802.11a/g actuales. El propósito de TGn para este próximo paso en el rendimiento de WLAN consiste en mejorar la experiencia del usuario con las aplicaciones WLAN existentes a tiempo de habilitar

aplicaciones nuevas y segmentos del mercado recientes. Al mismo tiempo, TGn espera una transición lúcida para su adopción al requerir compatibilidad retroactiva con las soluciones IEEE WLAN legadas existentes (802.11a/b/g).

Resultados de LAN inalámbrica según el Estándar de IEEE:

Tabla 2.1 Comparación de distintas velocidades de transferencia 802.11

Estándar para WLAN de IEEE	Cotizaciones Over-the-Air (OTA)	*Cotizaciones de la Capa de control del acceso al medio Servicio en punto de acceso (MAC SAP)
802.11b	11 Mbps	5 Mbps
802.11g	54 Mbps	25 Mbps (en ausencia de .11b)
802.11a	54 Mbps	25 Mbps
802.11n	200 Mbps o más	100 Mbps

2.4 ESTÁNDARES 802.11

Existen multitud de estándares definidos o en proceso de definición que es necesario conocer para una correcta interpretación de las redes **wireless**:

- **802.11a** Estándar de comunicación en la banda de los 5 Ghz, ya descrito

- **802.11b** Estándar de comunicación en la banda de los 4 Ghz, ya descrito.

- **802.11c** Estándar que define las características que necesitan los APs para actuar como puentes (bridges). Ya está aprobado y se implementa en algunos productos.

- **802.11d** Estándar que permite el uso de la comunicación mediante el protocolo

- **802.11** en países que tienen restricciones sobre el uso de las frecuencias que éste es capaz de utilizar. De esta forma se puede usar en cualquier parte del mundo.

- **802.11e** Estándar sobre la introducción del QoS en la comunicación entre PAs y TRs. Actua como árbitro de la comunicación. Esto permitirá el envío de vídeo

- **802.11f** Estándar que define una práctica recomendada de uso sobre el intercambio de información entre el AP y el TR en el momento del registro a la red y la información que intercambian los APs para permitir la interoperabilidad. La adopción de esta práctica permitirá el Roaming entre diferentes redes.

- **802.11g** Estándar que permite la comunicación en la banda de los 2,4 Ghz, ya descrito.

- **802.11h** Estándar que sobrepasa al 802.11a al permitir la asignación y de voz sobre IP.dinámica de canales para permitir la coexistencia de éste con el HyperLAN. Además define el TPC (Transmit Power Control)

según el cual la potencia de transmisión se adecua a la distancia a la que se encuentra el destinatario de la comunicación.

- **802.11i** Estándar que define la encriptación y la autenticación para complementar y mejorar el WEP. Es un estándar que mejorará la seguridad de las comunicaciones mediante el uso del Temporal Key Integrity Protocol (TKIP).

- **802.11j** Estándar que permitirá la armonización entre el IEEE, el ETSI HyperLAN2, ARIB e HISWANa.

- **802.11m** Estándar propuesto para el mantenimiento de las redes inalámbricas.

2.5 DISPOSITIVOS WIRELESS

Sea cual sea el estándar que se elija se va a disponer principalmente de dos tipos de dispositivos:

a- **Dispositivos "Tarjetas de red", o TR**, que serán los que tenga integrados en el ordenador, o bien conectados mediante un conector **PCMCIA** ó **USB** si esta en un portátil o en un slot PCI si esta en un ordenador de sobremesa. SUBSTITUYEN a las tarjetas de red Ethernet o Token Ring a las que estába acostumbrados. Recibirán y enviarán la información hacia su destino desde el ordenador en el que este trabajando. La velocidad de transmisión / recepción de los mismos es variable dependiendo del fabricante y de los estándares que cumpla.

b- **Dispositivos "Puntos de Acceso", ó PA**, los cuales serán los encargados de recibir la información de los diferentes **TR** de los que conste la red bien para su centralización bien para su encaminamiento.

COMPLEMENTAN a los Hubs, Switches o Routers, si bien los PAs pueden substituir a los últimos pues muchos de ellos ya incorporan su funcionalidad. La velocidad de transmisión / recepción de los mismos es variable, las diferentes velocidades que alcanzan varían según el fabricante y los estándares que cumpla.

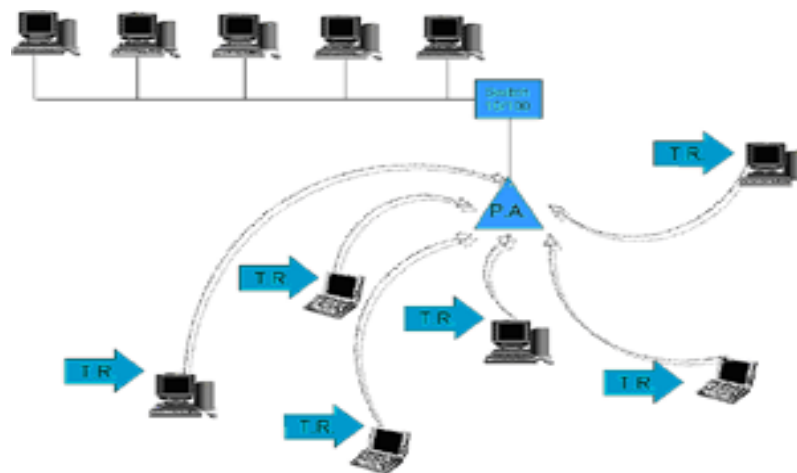


Figura 2.1 Red Inalámbrica

2.6 FUNCIONAMIENTO DE LOS DISPOSITIVOS

En este documento vamos a referirnos principalmente al **802.11g**, por ser el probable vencedor de la "guerra de estándares" abierta hoy en día, aunque lo explicado será fácilmente extrapolable a los demás teniendo en cuenta las características propias de cada uno.

Todos los estándares aseguran su funcionamiento mediante la utilización de dos factores, cuando están conectados a una red mediante un cable, sea del tipo que sea, dispone de una velocidad fija y constante. Sin embargo cuando está hablando de redes inalámbricas aparece un factor añadido que puede afectar a la velocidad de transmisión, que es la distancia entre los interlocutores.

Así pues cuando un **TR** se conecta a un **PA** se ve afectado principalmente por los siguientes parámetros:

- Velocidad máxima del **PA** (normalmente en 802.11g será de 54Mbps)
- Distancia al **PA** (a mayor distancia menor velocidad)
- Elementos intermedios entre el **TR** y el **PA** (las paredes, campos magnéticos o eléctricos u otros elementos interpuestos entre el **PA** y el **TR** modifican la velocidad de transmisión a la baja)
- Saturación del espectro e interferencias (cuantos más usuarios inalámbricos haya en las cercanías más colisiones habrá en las transmisiones por lo que la velocidad se reducirá, esto también es aplicable para las interferencias.)

Normalmente los fabricantes de **PAs** presentan un alcance teórico de los mismos que suele ser alrededor de los 300 metros. Esto obviamente es sólo alcanzable en condiciones de laboratorio, pues realmente en condiciones objetivas el rango de alcance de una conexión varía (y siempre a menos) por la infinidad de condiciones que le afectan.

Cuando pone un TR cerca de un PA dispone de la velocidad máxima teórica del PA, 54 Mbps por ejemplo, y conforme nos va alejando del PA, tanto él mismo como el TR van disminuyendo la velocidad de la transmisión/recepción para acomodarse a las condiciones puntuales del momento y la distancia.

Así pues, se podría decir que en condiciones "de laboratorio" y a modo de ejemplo teórico, la transmisión entre dispositivos 802.11 podría ser como sigue:

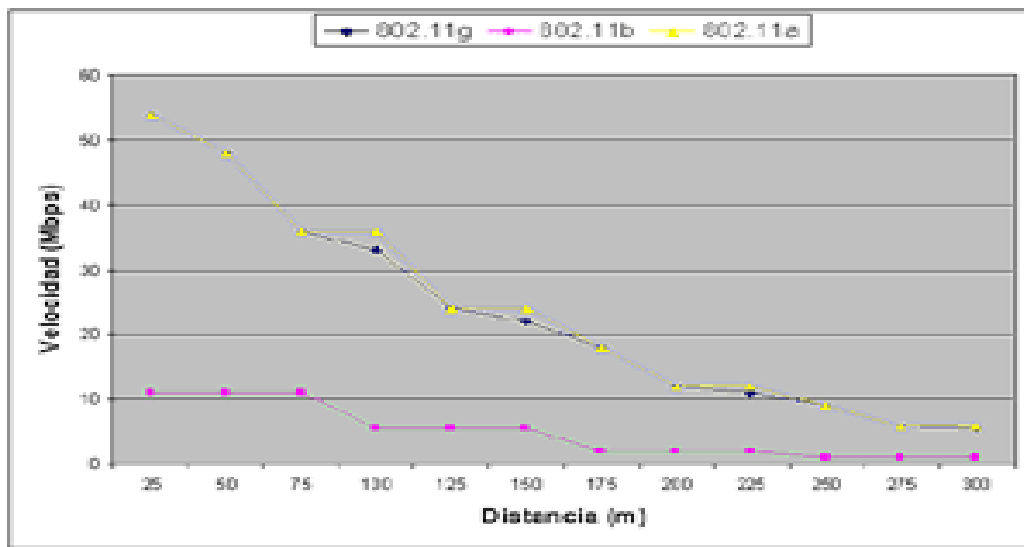


Figura 2.2. transmisión entre dispositivos 802.11

Actualmente ya hay fabricantes que ofrecen antenas que aumentan la capacidad de **TX/RX** (transmisión y recepción) de los dispositivos wireless.

Dentro de los **PAs** (actualmente ya se puede comenzar a aplicar también a los **TRs**) se puede modificar enormemente la capacidad de

TX/RX gracias al uso de antenas especiales. Estas antenas se pueden dividir en: direccionales y omnidireccionales.

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

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

2.7 VELOCIDAD VS MODULACIÓN

Cuando se transmite información entre dos dispositivos inalámbricos, la información viaja entre ellos en forma de tramas. Estas tramas son básicamente secuencias de bits. Las secuencias de bits están divididas en dos zonas diferenciadas, la primera es la cabecera y la segunda los datos que verdaderamente se quieren transmitir.

La cabecera es necesaria por razones de gestión de los datos que se envían. Dependiendo de la forma en la que se module la cabecera (o preámbulo), se puede encontrar con diferentes tipos de tramas, como son:

- **Barker.** (RTS / CTS)
- **CCK.** Complementary Code Keying
- **PBCC.** Packet Binary Convolutional Coding

- **OFDM**. Orthogonal Frequency-Division Multiplexing

Una representación gráfica de las tramas más importantes:

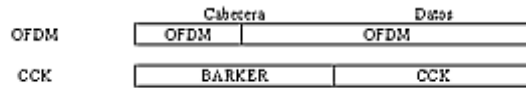


Figura 2.3 Tramas Importantes

Como se puede ver la cabecera en el caso de la codificación **OFDM** es más pequeña. A menor tamaño de cabecera menor "overhead" en la transmisión, es decir, menor tráfico de bits de gestión luego mayor "espacio" para mandar bits de datos. Lo que repercutirá positivamente en el rendimiento de la red.

Ya a primera vista se puede ver que el estándar **802.11g** es una unión de los estándares **802.11 "a"** y **"b"**. Contiene todos y cada uno de los tipos de modulación que éstos usan, con la salvedad de que "a" opera en la banda de los 5 Ghz, mientras que los otros dos operan en la del los 2,4 Ghz.

Cuando se tiene una red inalámbrica en la que todos los dispositivos son tipo "a" o todos de tipo "b" no hay problemas en las comunicaciones. Cada AP tipo "a" tendrá sólo TRs tipo "a" y los APs tipo "b" tendrán sólo TRs tipo "b". Se seleccionará la mejor modulación y se transmitirá. Si la comunicación óptima no es posible debido a una excesiva distancia entre los dispositivos o por diferentes tipos de interferencias se va disminuyendo la velocidad hasta que se encuentre la primera en la que la comunicación es posible.

En el caso de dispositivos AP 802.11g normalmente estará usando la modulación OFDM, modulación que es la óptima para este estándar.

Si por un casual un dispositivo 802.11b quisiera hablar con otro dispositivo 802.11g, este último debería aplicar una modulación compatible con el estándar "b", cosa que es capaz de hacer. Sin embargo el dispositivo "b" no puede escuchar las transmisiones de los otros dispositivos "g" que hablan con su "partner" pues éstos usan una modulación que él no es capaz de entender. Si un dispositivo "b" comenzase a hablar a la vez que un dispositivo "g" se producirían colisiones que impedirían la transmisión, no por que interfieran ya que usan diferente modulación sino porque el AP normalmente sólo será capaz de hablar con un dispositivo a la vez.

Para evitar las colisiones, los equipos "b" usan la modulación **Barker** con **TRX/CTS** (Request To Send / Clear To Send), que básicamente significa que deben pedir permiso al AP para transmitir.

2.8 TOPOLOGÍA Y MODOS DE FUNCIONAMIENTO DE LOS DISPOSITIVOS

Es conveniente el hacer una división entre la topología y el modo de funcionamiento de los dispositivos **WiFi**. Con topología se refiere a la disposición lógica (aunque la disposición física también se pueda ver influida) de los dispositivos, mientras que el modo de funcionamiento de los mismos es el modo de actuación de cada dispositivo dentro de la topología escogida.

En el mundo Wireless existen dos topologías básicas:

a- Topología Ad-Hoc. Cada dispositivo se puede comunicar con todos los demás.

b- Topología Infraestructura, en el cual existe un nodo central (Punto de Acceso WiFi) que sirve de enlace para todos los demás (Tarjetas de Red Wifi).

2.9 MESH NETWORKS

Los inicios de las redes acopladas son, militares. Inicialmente se usaron para comunicarse con aquellas unidades de militares que aún estando lejos de las zonas de cobertura de sus mandos estaban lo suficientemente cerca entre si como para formar una cadena a través de la cual se pudiese ir pasando los mensajes hasta llegar a su destino (los mandos).

Las redes **Mesh**, o redes acopladas, para definir las de una forma sencilla, son aquellas redes en las que se mezclan las dos topologías de las redes inalámbricas. Básicamente son redes con topología de infraestructura, pero que permiten unirse a la red a dispositivos que a pesar de estar fuera del rango de cobertura de los PA están dentro del rango de cobertura de algún TR que directamente o indirectamente está dentro del rango de cobertura del PA.

También permiten que los TRs se comuniquen independientemente del PA entre sí. Esto quiere decir que los dispositivos que actúan como TR pueden no mandar directamente sus paquetes al PA sino que pueden pasárselos a otros TRs para que lleguen a su destino.

Para que esto sea posible es necesario el contar con un protocolo de enrutamiento que permita transmitir la información hasta su destino con el mínimo número de saltos (**Hops** en inglés) o con un número que aún no siendo el mínimo sea suficientemente bueno.

Es tolerante a fallos, pues la caída de un solo nodo no implica la caída de toda la red.

Antiguamente no se usaba porque el cableado necesario para establecer la conexión entre todos los nodos era imposible de instalar y de mantener. Hoy en día con la aparición de las redes **wireless** este problema desaparece y permite disfrutar de sus grandes posibilidades y beneficios.

A modo de ejemplo de muestra una red acoplada formada por seis nodos. Se puede ver que cada nodo establece una comunicación con todos los demás nodos. Si este gráfico ya comienza a ser complicado, imagine si el número de nodos fuese de varios cientos.

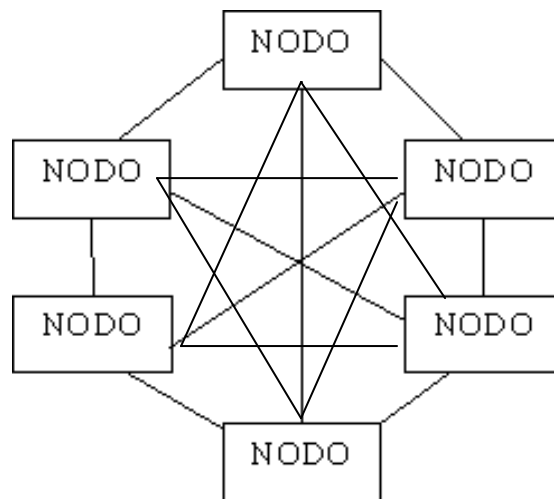


Figura 2.4 red acoplada formada por seis nodos

2.10 SEGURIDAD EN LAS COMUNICACIONES WIRELESS

La seguridad es una de los temas más importantes cuando se habla de redes inalámbricas. Desde el nacimiento de éstas, se ha intentado el disponer de protocolos que garanticen las comunicaciones, pero han sufrido de escaso éxito. Por ello es conveniente el seguir puntual y escrupulosamente una serie de pasos que permitan disponer del grado máximo de seguridad que se pueda asegurar.

a-Terminología

Para poder entender la forma de implementar mejor la seguridad en una red wireless, es necesario comprender primero ciertos elementos:

- **WEP**. Significa **Wired Equivalet Privacy**, y fue introducido para intentar asegurar la autenticación, protección de las tramas y confidencialidad en la comunicación entre los dispositivos inalámbricos. Puede ser WEP64 (40 bits reales) WEP128 (104 bits reales) y algunas marcas están introduciendo el WEP256. Es INSEGURO debido a su arquitectura, por lo que el aumentar los tamaños de las claves de encriptación sólo aumenta el tiempo necesario para romperlo.
- **OSA vs SKA**. **OSA** (Open System Authentication), cualquier interlocutor es válido para establecer una comunicación con el AP. **SKA** (Shared Key Authentication) es el método mediante el cual ambos dispositivos disponen de la misma clave de encriptación, entonces, el dispositivo TR pide al AP autenticarse. El AP le envía una trama al TR, que si éste a su vez devuelve correctamente codificada, le permite establecer comunicación.
- **ACL**. Significa Access Control List, y es el método mediante el cual sólo se permite unirse a la red a aquellas direcciones MAC que estén dadas de alta en una lista de direcciones permitidas.

- **CNAC**. Significa Closed Network Access Control. Impide que los dispositivos que quieran unirse a la red lo hagan si no conocen previamente el SSID de la misma.

- **SSID**. Significa Service Set Identifier, y es una cadena de 32 caracteres máximo que identifica a cada red inalámbrica. Los TRs deben conocer el nombre de la red para poder unirse a ella.

b- Pasos para asegurar una red inalámbrica

Se dice que una red es segura cuando casi nadie puede entrar la misma o los métodos de entrada son tan costosos que casi nadie puede llevarlos a cabo. Casi nadie puede significar que es segura en un 99'99%, por ello debe desechar la idea de que los sistemas informáticos son seguros al 100%.

Un sistema es seguro cuando tiene la protección adecuada al valor de la información que contiene o que puede llegar a contener.

Una vez situados ver los pasos que se debe seguir para introducir una seguridad razonablemente alta a red **wireless**. Debe tener en cuenta que cuando trabaja con una red convencional cableada dispone de un extra de seguridad, pues para conectarse a la misma normalmente hay que acceder al cable por el que circula la red o a los dispositivos físicos de comunicación de la misma.

c- Enumeración pasos para asegurar una red inalámbrica

A continuación se comentan los pasos necesarios para asegurar una red **Wireless**

Paso 1, activar el **WEP**.

Paso 2, debe seleccionar una clave de cifrado para el WEP lo suficientemente difícil como para que nadie sea capaz de adivinarla.

Paso 3, uso del **OSA**. Esto es debido a que en la autenticación mediante el **SKA**, se puede comprometer la clave **WEP**, que expondría a mayores amenazas.

Paso 4, desactivar el **DHCP** y activar el **ACL**. Se debe asignar las direcciones IP manualmente y sólo a las direcciones MAC conocidas.

Paso 5, Cambiar el **SSID** y modificar su intervalo de difusión.

Paso 6, hacer uso de VPNs.

Paso 7, aislar el segmento de red formado por los dispositivos inalámbricos de la red convencional.

2.11 TÉCNICAS DE BÚSQUEDA Y MARCADO DE REDES WIRELESS - WARCHALKING

Dentro del mundo **wireless**, no puede dejar de lado dos prácticas que se han extendido rápidamente entre algunas comunidades de usuarios de esta tecnología sobre todo con el ánimo de conseguir acceso gratuito a Internet. La adaptación a las nuevas tecnologías en algunos ámbitos es extremadamente rápida.

Warchalking

Es un lenguaje de símbolos normalmente escritos con tiza en las paredes que informa a los posibles interesados de la existencia de una red inalámbrica en ese punto.

La sencillez del lenguaje ha sido uno de los factores que han hecho posible su proliferación por las grandes ciudades. Además otras características como la no perdurabilidad de las marcas durante grandes periodos de tiempo hacen que sea muy dinámico y se vaya adaptando

constantemente a las características cambiantes de las redes sobre cuya existencia informa.

Los símbolos más usados son:

Retina -> SSID

)(-> *Nodo abierto*, () ?*Nodo cerrado*, (W) ?*Nodo con WEP*

1.5 -> *Ancho de Banda*

1. En primer lugar se identifica el nombre del nodo, o SSID
2. En segundo lugar se identifica el tipo de red, bien sea abierta, cerrada o con WEP.
3. En último lugar se identifica la velocidad del mismo.

2.12 TÉCNICAS DE BÚSQUEDA Y MARCADO DE REDES WIRELESS – WARDRIVING

El **WarDriving** es un método usado para la detección de redes inalámbricas.

Se realiza bien desde dentro de un vehículo o bien simplemente caminando a pie por diferentes zonas, habitualmente del centro, de una ciudad, con un dispositivo como un **PDA** o un ordenador portátil con los que se pueden detectar estas redes.

Para la identificación de las redes es necesario usar una **TR WiFi** en modo promiscuo junto con un **SW** especial, modo en el cual va a

detectar todas las redes de los alrededores que estén configuradas mediante un PA.

Una vez detectada la red, se analiza y bien se "marca" mediante el **warchalking** bien se apunta para su posterior explotación.

Adicionalmente se puede dotar al sistema de un **GPS** con el cual marcar exactamente en un mapa la posición de la red. Ya existe SW apropiado para estos casos como es el AirSnort para Linux, el BSD-AriTools para BSD y el NetStumbler para Windows.

2.13 REDES DE RADIO FRECUENCIA

Por el otro lado para las Redes Inalámbricas de Radio Frecuencia , en los Estados Unidos se permitió la operación sin licencia de dispositivos que utilizan 1 Watt de energía o menos, en tres bandas de frecuencia : 902 a 928 MHz, 2,400 a 2,483.5 MHz y 5,725 a 5,850 Mhz. Esta bandas de frecuencia, llamadas bandas ISM, estaban anteriormente limitadas a instrumentos científicos, médicos e industriales. Esta banda está abierta para cualquiera. Para minimizar la interferencia, se estipularon algunas regulaciones; ésta es una técnica de señal de transmisión llamada spread-spectrum modulation, la cual tiene potencia de transmisión máxima de 1 Watt. y deberá ser utilizada en la banda ISM. Esta técnica ha sido utilizada en aplicaciones militares. La idea es tomar una señal de banda convencional y distribuir su energía en un dominio más amplio de frecuencia. En aplicaciones militares el objetivo es reducir la densidad de energía bajo el nivel de ruido ambiental de tal manera que la señal no sea detectable. La idea en las redes es que la señal sea transmitida y recibida con un mínimo de interferencia. La tecnología de espectro de radio extendido, es una nueva banda de radio aprobada para uso por la FCC (Federal Communications Commission) en 1986 ha abierto para el mercado un gran número de productos inalámbricos. Aironet Wireless

Communications ofrece sistemas inalámbricos para bandas de radio tanto de 900 Mhz como de 2.4 Ghz. Cada una de estas bandas de radio tiene sus propias ventajas : con la de 900 Mhz ofreciendo un mejor rango y resistencia a pérdidas de señal. La banda de 2.4 Ghz por su parte, corresponde al espacio abierto amplio. Se puede obtener un gran ancho de banda sin interferencia a los 2.4 Ghz y se les permite a las compañías desarrollar productos que muevan datos a velocidades mayores. Esta banda es donde los rangos de datos de 4 Mbps llegan a ser comunes y donde un número de fabricantes tienen o tendrán dispositivos para 10 Mbps en un futuro cercano. Estos rangos mayores de datos hacen que aplicaciones de datos intensivas como videoconferencias de LAN o conexiones a Internet a altas velocidades sean posibles. Existen dos técnicas para distribuir la señal convencional en un espectro de propagación equivalente :

- La Secuencia Directa: En este método el flujo de bits de entrada se multiplica por una señal de frecuencia mayor, basada en una función de propagación determinada. El flujo de datos original puede ser entonces recobrado en el extremo receptor correlacionándolo con la función de propagación conocida. Este método requiere un procesador de señal digital para correlacionar la señal de entrada.
- El Salto de Frecuencia: Este método es una técnica en la cual los dispositivos receptores y emisores se mueven sincrónicamente en un patrón determinado de una frecuencia a otra, brincando ambos al mismo tiempo y en la misma frecuencia predeterminada. Como en el método de secuencia directa, los datos deben ser reconstruidos en base del patrón de salto de frecuencia. Este método es viable para las redes inalámbricas, pero la asignación actual de las bandas ISM no es adecuada, debido a la competencia con otros dispositivos, como por ejemplo las bandas de 2.4 y 5.8 Mhz que son utilizadas por hornos de Microondas.

Para que un sistema de radio sea eficiente y posea capacidad hay que determinar un método de acceso, modulación de radio y ancho de banda disponible adecuados; estos factores son considerados más importantes que la forma de implementarlos dentro de una zona geográfica y del espectro de ancho de banda.

El inconveniente existente en redes de radio frecuencia es que mientras la distancia de conexión aumenta, disminuye la señal de radio, ésta dado por la curvatura de la tierra y por factores físicos naturales que se transforman en obstáculos, como cerros, valles, edificios, etc.

Este diseño es muy utilizado en interferencia limitada. Existe una trayectoria normal cuando en el nivel de transferencia, de estaciones simultáneamente activas, no prevén la transferencia actual de datos. Para este tipo de diseño, los siguientes factores son importantes:

- Es necesaria una relación señal-interferencia, para una comunicación correcta.
- Se requiere de un margen expresado en estadísticas para generar esta relación, aún en niveles de señal variables.
- La posición de las antenas que realizan la transmisión, la cual puede ser limitada por las estaciones y perfectamente controlada por puntos de acceso fijos.
- La función de la distancia para el nivel de la señal. Esta dada por el valor promedio de la señal, considerando las diferencias en la altura de la antena de la terminales y los impedimentos naturales en la trayectoria.

CAPÍTULO III

INSTALACIÓN DE UNA RED CON PUNTOS DE ACCESO

3.1 INTRODUCCIÓN

A las redes inalámbricas Wi – Fi con puntos de acceso se les conoce con el nombre de modo infraestructura o modo BSS.

La utilización de puntos de acceso es conveniente cuando se pretende crear una red permanente, aunque sea con pocos terminales, cuando se desea disponer de una amplia área de cobertura o crear una red inalámbrica con muchos usuarios. Dicho de otra forma, salvo que se vaya a realizar una comunicación esporádica entre dos o algunos más ordenadores o se disponga de muy poco presupuesto (la utilización de un punto de acceso supone añadirle unos 100 dólares al presupuesto), el modo normal de configuración de las redes inalámbricas Wi – Fi es con puntos de acceso.

Una ventaja adicional de las redes con los puntos de acceso es que se disfruta de ciertas características de gestión de red de las que carece completamente el modo ad hoc sin puntos de acceso.

En el mercado ha aparecido recientemente una alternativa a los puntos de acceso que consiste en crear una red en modo ad hoc e instalar un software especial en uno de los ordenadores de la red. Este software hace las funciones de un punto de acceso software. La única ventaja que tiene esta opción es que ahorra el costo de un punto de acceso, pero a cambio condena a un ordenador a estar ocupado con esta tarea.

Un punto de acceso es un equipo que funciona en las redes inalámbricas Wi – FI como si fuera una estación base central que sirve de intermediario de todas las comunicaciones entre los ordenadores de la red. Los ordenadores que conectan vía radio a los puntos de acceso necesitan disponer de un adaptador de red. El adaptador de red es el mismo que el que se utiliza en las configuraciones ad hoc, salvo que se configura para funcionar con un punto de acceso.



Figura 3.1 Red Wi-Fi con punto de acceso

Otra de las ventajas de los puntos de acceso es que permite interconectar la red inalámbrica con una red local cableada e Internet. Para ello los puntos de acceso disponen de equipos de radio y antena para comunicarse con sus ordenadores inalámbricos y de puertos Ethernet (10/100 BaseT, RJ45) para comunicarse con la red cableada.

En las redes con los puntos de acceso no se producen comunicaciones directas entre ordenadores (aunque estén uno junto al otro), sino que todas ellas pasan por el punto de acceso. Por tanto, el punto de acceso es el equipo del que depende todas las comunicaciones y desde el que se puede gestionar toda la red.

Cada punto de acceso dispone de un área de cobertura. Un área de cobertura es la zona dentro de la cual cualquier ordenador puede comunicarse con el punto de acceso de forma inalámbrica. El mayor o menor tamaño del área de cobertura depende de distintos factores como son:

- Localización de los puntos de acceso
- Obstáculos entre el punto de acceso y el ordenador
- Interferencia radioeléctricas
- Tipos de antenas utilizadas

Si se sitúan puntos de acceso completando sus coberturas, se puede llegar a crear una red inalámbrica con áreas de servicios tan extensa como se desee.

3.2 UBICACIÓN DE LOS PUNTOS DE ACCESO

Si lo que se pretende es cubrir una pequeña área, una casa o una pequeña oficina lo más probable es que baste con colocar un solo punto de acceso en el lugar más céntrico y alto posible. A veces el lugar viene dado por el sitio donde se encuentran el acceso a Internet (ADSL, módem cable o línea telefónica). La cosa se complica cuando lo que se pretende cubrir es una gran oficina, una zona empresarial, un campus

universitario o todo un vecindario. En estos casos hay que estudiar muy bien dónde se van a colocar los puntos de acceso.

La colocación de los puntos de acceso tiene una gran base técnica, pero también tiene un gran componente artístico. Esto se debe a que cualquier cosa del entorno (muebles, estanterías, paredes, fenómenos atmosféricos, metales, árboles, etc.) puede afectar a la propagación de las ondas electromagnéticas y generalmente no es posible realizar un estudio teórico de la propagación de las ondas en nuestro entorno. Por ello teniendo presente lo que afecta a la propagación, la colocación de los puntos de acceso suele basarse en el método de prueba y error.

El método de prueba y error consiste en realizar una inspección previa, decidir los lugares de los puntos de acceso basados en esta primera inspección, hacer pruebas de cobertura con la ayuda de un ordenador portátil y recolocar los puntos de acceso hasta situarlos en su posición idónea.

En cualquier caso, antes de proceder a instalar los puntos de acceso, es necesario tener claro el área que se desea cubrir y cuántos usuarios simultáneos habrá en cada área. Un área muy congestionada puede necesitar más de un punto de acceso.

3.2.1 COBERTURA

La cobertura de un punto puede variar entre los 30 y los 300 metros dependiendo de las condiciones de visibilidad entre emisor y receptor y de las posibles interferencias que se puedan producir en la zona. En los espacios abiertos se consiguen los mayores alcances, mientras que en los lugares de interior con paredes y acceso no se pueden colocar con el único criterio del alcance teórico.

Por otro lado, la potencia de transmisión de un punto de acceso varía entre los 100 mW (límite máximo de acuerdo a la regulación europea) y 1 W (límite máximo de acuerdo con las regulaciones norteamericanas). Evidentemente, a más potencia, mayor es el alcance. No obstante, no siempre interesa que un solo punto de acceso tenga una gran cobertura. Si lo que pretende cubrir es, por ejemplo una pequeña oficina o una sala de reuniones, el disponer de una cobertura mucho mayor (llegando a la calle o a las oficinas vecinas) no tiene ningún interés y, sin embargo se aumenta el riesgo de seguridad de la red. Por otro lado, cuando se intenta cubrir un área donde se concentran muchos usuarios, a menor cobertura de cada punto de acceso, más puntos de acceso serán necesarios para cubrir la misma área y mayor será el ancho de banda total disponible (11 Mbps por cada punto de acceso en 802.11b, pero 54 Mbps en 802.11g).

Por tanto, aunque un equipo pueda tener un gran alcance, siempre hay que configurarlo para que ofrezca la justa necesaria.

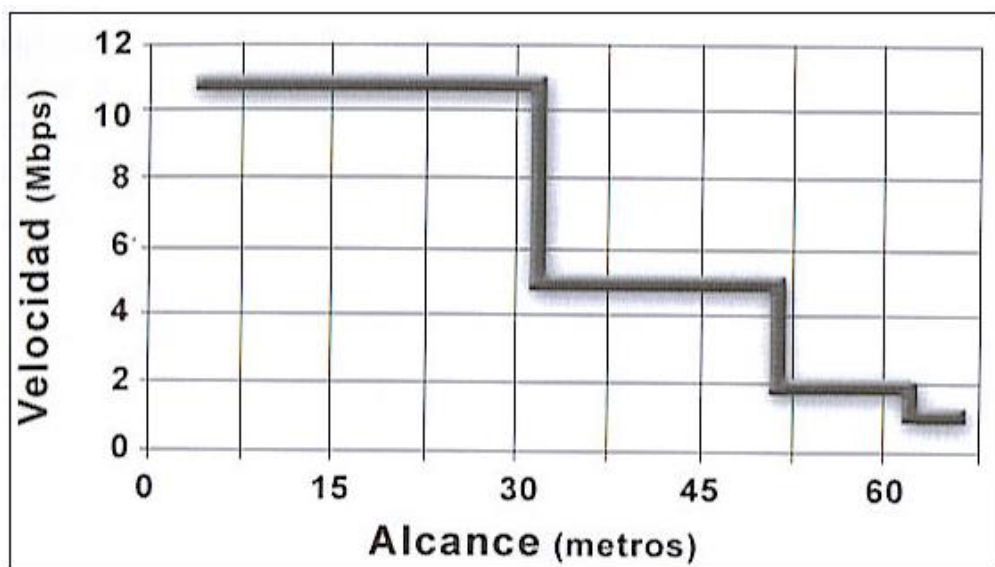


Figura 3.2 Cobertura típica en el interior de una oficina

3.2.2 COEXISTENCIA DE PUNTOS DE ACCESO

Típicamente, cada canal de protocolo DSSS de Wi – Fi necesita 22 MHz de ancho de banda (aunque esto puede variar), no obstante tiene asignado 25 MHz por canal para minimizar las interferencias entre canales. Como la banda de 2,4 GHz en la que trabaja Wi – Fi tiene un ancho de banda total de 80 MHz quiere decir que en la misma zona sólo puede coexistir tres canales (tres puntos de acceso) sin que haya interferencia entre canales.

Por otro lado, cada punto de acceso facilita un ancho de banda de 54Mbps. Al situar dos o tres puntos de acceso juntos, se consigue aumentar el ancho de banda disponible a 108 o 110 Mbps. En este caso, cada usuario podrá disponer de un máximo de 54 Mbps., pero el ancho de banda total disponible para compartir entre todos los usuarios será de 108 o 110 Mbps.

3.2.3 ANCHO DE BANDA

En el ancho de banda de que dispone cada punto de acceso Wi – Fi es de 54 Mbps. Si en un momento dado coinciden varias comunicaciones simultaneas a través del mismo punto de acceso, Los 54 Mbps se repartirán entre todas ellas. Por tanto dependiendo del número de usuarios simultáneos, el ancho de banda de cada comunicación puede ser inferior o bastante inferior a 54 Mbps.

A pesar de lo anterior, tampoco es real decir que el ancho de banda de cada ordenador es el resultado de dividir 54 Mbps. Por el número de ordenadores. La realidad es que cada ordenador no está transmitiendo y recibiendo datos de forma continua. Evidentemente, depende de la aplicación que se le dé, pero la normal es que navegar por páginas web, explorar el directorio de un disco duro remoto o utilizar una aplicación a distancia suele tener momentos de transmisión de datos entre grandes silencios de

comunicación. Esto hace que consiga un gran aprovechamiento. Con 54 Mbps. pueden trabajar decenas de usuarios en condiciones normales sin que se noten grandes retrasos, salvo en momentos puntuales.

En cualquier caso, si en la zona de cobertura de un punto de acceso se notan grandes retardos y se comprueba que no es debido a interferencias, siempre se puede añadir un nuevo punto de acceso.

3.3 INSTALACIÓN DE UNA RED DE PUNTOS DE ACCESO

Como se ha comentado anteriormente, en las redes pequeñas hay poco que analizar: se coloca el punto de acceso en el lugar más cómodo y se comprueba si cubre las expectativas. En el peor de los casos, bastará con hacer un par de intentos de colocación antes de llegar a la disposición óptima.

El tema se complica cuando se necesita cubrir una gran extensión. En estos casos si se requiere conseguir la mayor eficacia no basta con sustituir los puntos de acceso donde mejor parezca. Tampoco hay que confiar exclusivamente en el sistema de prueba y error. En estos casos es recomendable realizar un estudio más estructurado. Esto quiere decir que, antes de comenzar a poner puntos de acceso por paredes y techos, hará falta responder a algunas preguntas como las siguientes.

- Con cuántos usuarios va a contar la red

- Qué área se pretende cubrir con el servicio en la red inalámbrica

- Qué inconveniente puede presentar el entorno desde el punto de vista de la cobertura radioeléctrica.
- Qué posibles fuentes de interferencia existen en sus inmediaciones.
- Cuál será la concentración de usuarios (usos simultáneos en una misma zona)
- Perfil de movilidad de los usuarios
- Será suficiente con una velocidad de transmisión de 11Mbps.
- Qué equipamiento será necesario (adaptadores de red, puntos de acceso, etc.)
- La localización de los puntos de acceso
- Cómo se interconectan los puntos de acceso entre si.
- La selección de canales
- Qué nivel de seguridad necesitará
- Cómo se interconectará la red inalámbrica a la red cableada o Internet.
- Se necesitará expandir la red inalámbrica en un futuro. Si es así dentro del mismo edificio o fuera.
- Quién administrará la red.

Dicho de otra forma, cuanto mayor sea la red, tanto en extensión como en el número de usuarios, mayor será la necesidad de realizar un

análisis previo que permita conocer en detalle las necesidades y los recursos con los que se cuenta.

En general, el proceso de instalación de una red inalámbrica se compone de los siguientes pasos.

- Realizar un análisis previo
- Configurar los ordenadores
- Configurar e instalar los puntos de acceso
- Instalar las conexiones entre los puntos de acceso
- Configurar el acceso a Internet

3.3.1 ANÁLISIS PREVIO

El análisis previo supone simplemente definir las necesidades, analizar el terreno estudiar los posibles inconvenientes y calcular los recursos. El tener una idea clara de estos conceptos ayudará grandemente a obtener una red adecuada y eficaz.

Los pasos a dar son las siguientes:

1. Determinar las necesidades.
2. hacer un esquema de cobertura.
3. Decidir las áreas de movilidad. Habrá áreas en las que baste tener servicio mientras que en otras se necesitará garantizar

además que el servicio no se corta cuando se desplaza el usuario.

Que se debe considerar:

- Lugares con cobertura. Son aquellas zonas que tienen que estar cubiertas porque hay usuarios que necesitan conectarse a la red desde allí. Incluso puede haber zonas que necesitan estar cubiertas muy esporádicamente. En este caso, puede disponerse puntos de acceso que ocasionalmente pueden estar situadas en lugares distintos.
- Lugares por desplazarse (roaming). Son las zonas por las que se desplazan los usuarios haciendo uso de la conexión. Estas áreas deben garantizar una continuidad del servicio aunque los usuarios estén en movimiento.

4. estudiar la cobertura real. Una vez descrita las necesidades se puede hacer una comprobación práctica de la cobertura. Se instala una tarjeta WI – Fi en un ordenador portátil, se va situado el punto de acceso y el portátil en distintos sitios y se va comprobando el nivel de la señal dentro de las áreas a cubrir. Para cada localización se debe comprobar tanto el alcance, como la respuesta (velocidad máxima conseguida). Para comprobar el alcance basta con desplazarse y ver que la conexión sigue establecida. Para comprobar la calidad de respuesta, se puede realizar transferencias de archivos y ver la velocidad de transmisión de datos. En las zonas con interferencias se notará que la velocidad de transferencia puede llegar a ser realmente baja. Por cierto, la mayoría de los equipos Wi – Fi incluyen un software de utilidades que permiten verificar la claridad de la señal (fuerza de la señal, ruidos, velocidad de transmisión, ect.). este software puede resultar muy útil para estudiar la cobertura real, hay que tener en cuenta que, en general , el mejor punto para colocar un punto de

acceso será el centro de la habitación en una posición elevada. En las habitaciones repletas de obstáculos como muebles, librerías, estantes, archivadores, ect., se consigue coberturas inferiores que en las habitaciones abiertas. Hay que evitar esconder el punto de acceso dentro de los típicos cubículos separados de las oficinas, en armarios o ponerlos cerca de objetos de metal.

5. Identificar Interferencias. El entorno radioeléctrico está sujeto a la presencia de interferencias. Las interferencias puede bajar el rendimiento del sistema; por ello, es importante identificar las posibles fuentes de interferencia.

Generalmente teléfonos inalámbricos, dispositivos bluetooth, motores (de ascensores, por ejemplo) o alarmas. El impacto de esta fuentes de interferencias se puede comprobar haciendo pruebas de transferencia con los dispositivos encendidos y apagados. Se puede utilizar el software de utilidad que acompaña al equipo Wi – Fi para comprobar las interferencias. En los lugares con interferencia donde no se puede eliminar la fuente y sea necesario la cobertura, se puede colocar puntos de acceso adicionales.

6. Hacer una instalación de prueba. Ligados a este punto, se tiene una idea muy clara de las condiciones del entorno. No obstante, antes de lanzarse a instalar todos los puntos de acceso, conviene hacer una primera instalación de prueba donde solo se conecten unos cuantos usuarios. Esto puede ayudar a tener posibilidades de problemas de desplazamiento (roaming) o de congestión por interferencias.
7. Realizar la comprobación final. Una vez hechas todas las comprobaciones anteriores, se contará con todos los datos necesarios para hacer la instalación:

Localización de los puntos de acceso, identificación de zonas muertas, modelos del funcionamiento del roaming, fuentes de interferencias y número de localización de los usuarios. Basta con echarle un último vistazo a todo antes de decidir las instalaciones

3.4 CONFIGURACIÓN DE LOS ORDENADORES

Cualquier ordenador que desee conectar de forma inalámbrica a una red con puntos de acceso necesita disponer de un adaptador de red (tarjeta Wi – Fi) y configurarse adecuadamente para que el adaptador se entienda con el punto de acceso de la red deseada.

En cuanto a lo que hay que configurar desde el ordenador, hay que llevar a cabo dos tipos de configuraciones:

- Configurar el adaptador de red

- Configurar el protocolo TCP/IP

La operación de configurar el protocolo TCP/IP y el adaptador de red hay que repetirla con cada ordenador que se desee conectar al punto de acceso.

Cualquier ordenador con un adaptador Wi – Fi que tengan configurados correctamente los parámetros anteriores y que esté dentro del área de cobertura radioeléctrica de cualquier punto de acceso a la red formará parte de ella y, por tanto, podrá compartir sus recursos y tener acceso a los recursos (configurados como compartidos) del resto de ordenadores. Esto quiere decir que para añadir nuevos ordenadores a la red, simplemente hay que copiar los parámetros de cualquiera de los ordenadores ya conectados y configurárselos al nuevo ordenador.

Por cierto un mismo ordenador puede tener guardadas distintas configuraciones de red, distintos perfiles (profile en inglés). Esto es especialmente útil en casos con los que un mismo ordenador se conecta a distintas redes. En estos casos no es necesario introducir todos los parámetros cada vez que cambia de red, sino simplemente, elegir el perfil correspondiente.

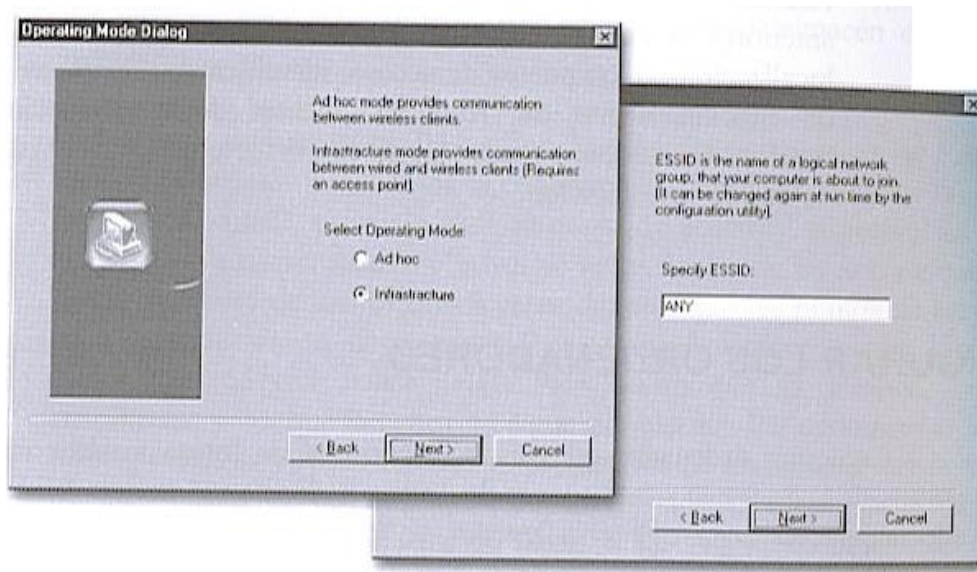


Figura 3.3. Configuración de un adaptador de red (marca Atmel)

3.5 CONFIGURACIÓN DEL ADAPTADOR DE RED

Los adaptadores de la red se configuran con una aplicación que viene en el CD incluido con el equipo. Los parámetros a configurar son los siguientes

- Tipo de red. En este caso, el tipo de red hay que configurar es el BSS, también conocido como infraestructura o con puntos de acceso.

- Nombre de red. El nombre de red debe ser el mismo que el configurado en el punto de acceso, incluidos los caracteres en mayúsculas y minúsculas. Al parámetro nombre de red también se lo conoce como Network (Nombre de red en inglés) o SSID (Service set Identifier, Identificador del Conjunto de Servicios). Muchas aplicaciones de configuración de adaptadores de red ofrecen la posibilidad de realizar una búsqueda automática de todas las redes del entorno que son recibidas por el adaptador en ese momento. En este caso, sólo habría que escoger un nombre de red de la lista.
- Canal. En este caso no es necesario configurar el canal porque el adaptador lo tomará automáticamente del punto de acceso.
- Seguridad. Es importante que los parámetros de seguridad que aquí se configuren sean los mismos configurados anteriormente en el punto de acceso. Si se tiene dudas, simplemente se dejan deshabilitados los parámetros de seguridad.

Hay que tener en cuenta que un ordenador puede tener perfil, esto es especialmente útil cuando un mismo ordenador se conecta a distintas redes. En estos casos no es necesario introducir todos los parámetros cada vez que cambia la red, sino, simplemente, elegir el perfil correspondiente.

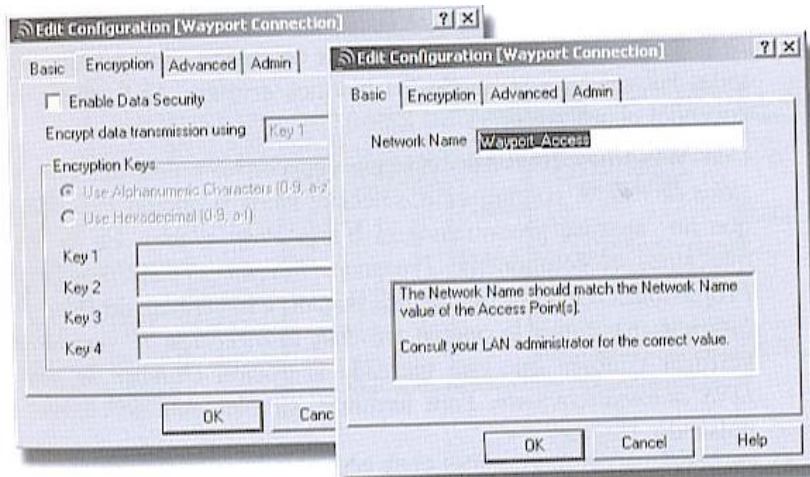


Figura 3.4 Configuración de un adaptador de red (marca Orinoco)
3.6 CONFIGURACION DEL PROTOCOLO TCP / IP

Configurar el protocolo TCP / IP en un ordenador supone configurarle una dirección IP, una máscara de subred, una puerta de enlace y un servidor DNS. No obstante en el caso de los puntos de acceso, todas estas configuraciones suelen sustituirse por configurar cada ordenador para que obtenga las direcciones IP de forma automática. El punto de acceso se encarga de pasarle a cada ordenador los datos necesarios para establecer la comunicación.

La forma de configurar el ordenador para obtener las direcciones IP de forma automática depende del sistema operativo de que se dispone.

Los pasos a dar para cada sistema operativo Windows son los siguientes:

- Con Windows 95/98 hacer clic con el botón derecho sobre el icono Entorno de red. Posteriormente, seleccionamos la opción *Propiedades*. la ventana que nos aparece nos indica los componentes de red que están instalados. Hacemos doble clic sobre el componente TCP/IP (o bien, lo marcamos y hacemos clic sobre el botón *Propiedades*). A continuación, en la ficha Dirección IP, seleccionamos Obtener una

dirección automáticamente. En la ficha Configuración Wins señalamos la opción Usar DHCP para resolución WINS. En la ficha Puerta de enlace no debe haber ninguna puerta de enlace configurada. Por último, cerramos todas las ventanas pulsando los botones Aceptar. Al finalizar habrá que apagar y encender el ordenador.

- Con Windows 2000/Me, hacer clic con el botón sobre el icono Mis sitios de red. A continuación seleccionar la opción Propiedades. En la ventana que aparece presionar Propiedades. En la lista de componentes marca el componente Protocolo Internet (TCP/IP) y presionar el botón Propiedades. Una vez que ha llegado a la ventana de Propiedades de protocolo de Internet, marca la opción Obtener la Dirección IP automáticamente. Tiene que estar marcada la opción obtener la Dirección del Servidor DNS automáticamente. Para terminar simplemente se cierran todas las ventanas pulsando Aceptar.
- Con Windows XP hay que hacer clic en Inicio, Configuración, Conexión de red. A continuación se hace clic en el botón derecho sobre Conexión de área local y se elige Propiedades. También se puede llegar aquí eligiendo Cambiar la Configuración de esta conexión en la ficha Tareas de red. Se continúa haciendo clic sobre Protocolo de Internet (TCP/IP) y luego, sobre el botón Propiedades. Se marca la opción Obtener una dirección IP del servidor DNS automáticamente. Para terminar, se cierra las ventanas pulsando Aceptar.

Aunque generalmente se configure el protocolo TCP/IP del ordenador para obtener automáticamente las direcciones IP del punto de acceso, si se desea, también podrían configurarse unos datos concretos. En este caso, los datos serían los siguientes:

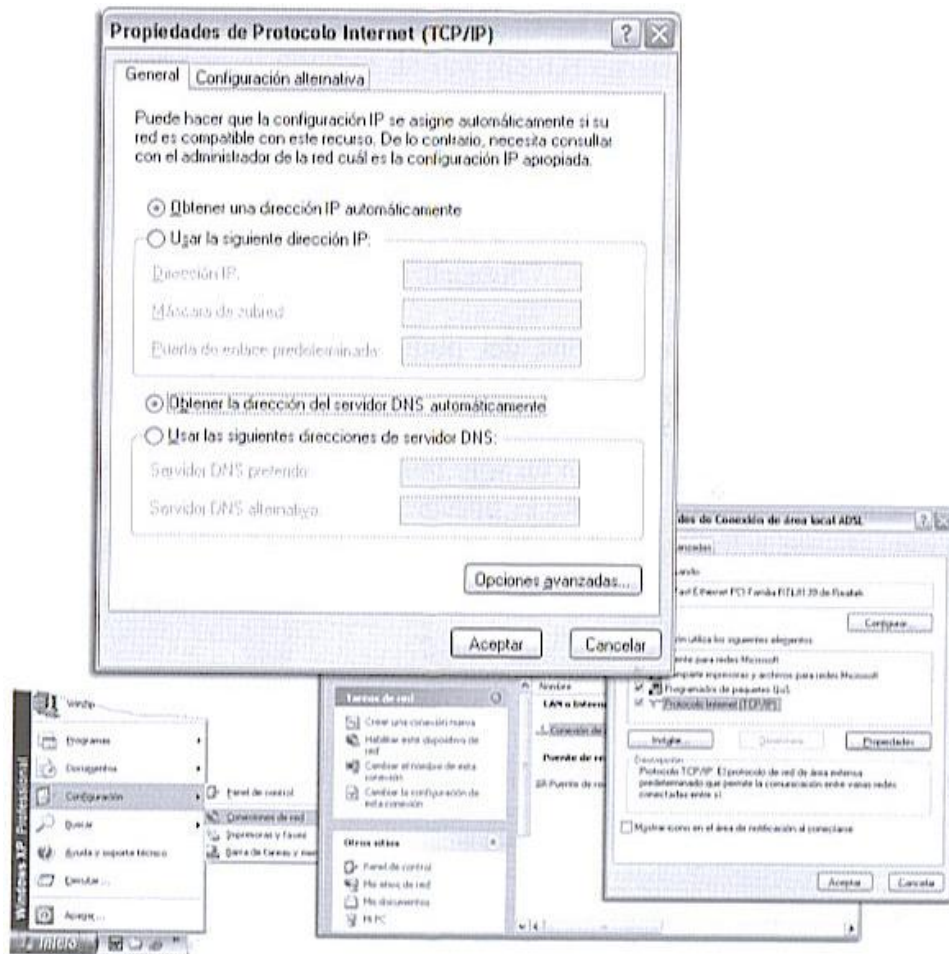


Figura 3.5 Configuración de la tarjeta Ethernet en Windows XP

Número IP del ordenador: Cualquier número siempre que esté dentro del rango de numeración de la red inalámbrica. Eso si cada ordenador debe disponer de un número IP distinto. Por ejemplo. Si el número IP del punto de acceso es el 192.168.1.1 a los ordenadores se les podría asignar los números 192.168.1.x donde x es cualquier número entre 2 y 255.

Máscara de subred. Generalmente suele utilizar como máscara de subred el número 255.255.255.0. este número es válido para redes que dispongan de menos de 255 terminales.

Puerta de enlace. Aquí habrían que indicar el número IP del punto de acceso. En el ejemplo puesto anteriormente, este número sería 192.168.1.1.

DNS: lo normal es introducir aquí la dirección IP del punto de acceso. Ya el punto de acceso sabrá asignar el DNS adecuado. No obstante si se está conectando a Internet y se conoce la dirección de los DNS, podría configurarse directamente en este campo.

3.7 CONFIGURACIÓN DEL PUNTO DE ACCESO.

Una vez que se dispone del punto de acceso antes de colocarlo en su lugar definitivo es conveniente proceder a su configuración. La mayoría de los fabricantes facilitan el punto de acceso con una configuración por defecto. Esta configuración suele ser adecuada para una red con un solo punto de acceso. En este caso, el fabricante facilita los valores (fundamentalmente el nombre de red y las características de seguridad) con los que hay que configurar los adaptadores de red de los ordenadores de los usuarios de la red, la figura 3.6 lo muestra.

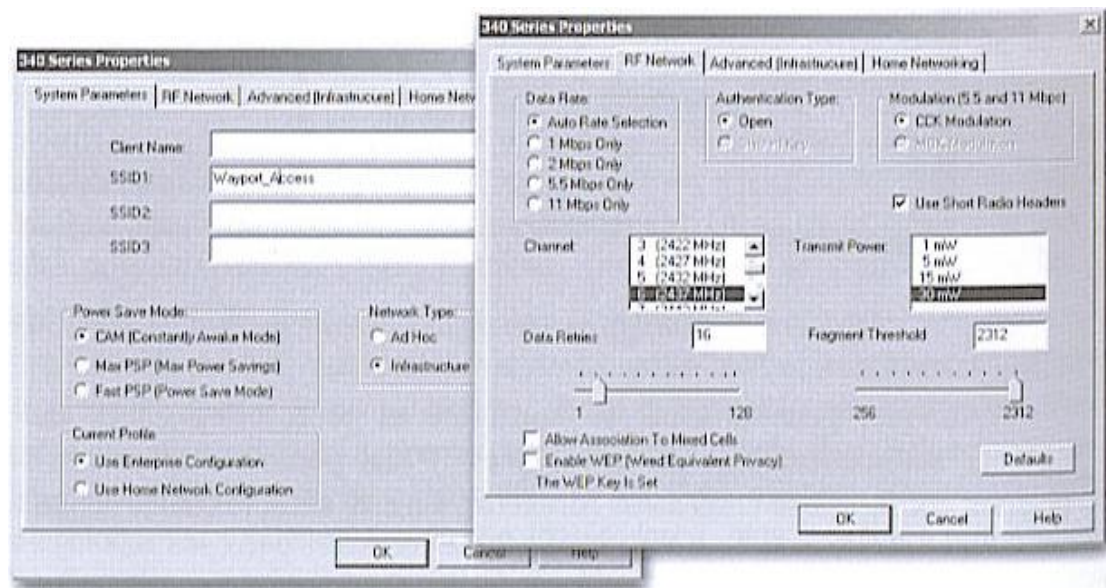


Figura 3. 6 Configuración de un punto de acceso con una aplicación particular (Cisco)

Si se desea configurar unos valores propios o se tiene la necesidad de realizar algún tipo de configuración especial, entonces será necesario modificar la configuración. La forma de configurar un punto de acceso depende del fabricante o incluso del modelo del equipo. Por ello siempre es recomendable atender a las instrucciones del manual del usuario del equipo.

En cualquier caso, los pasos a dar son los siguientes:

1. establecer una conexión entre un ordenador y el punto de acceso.

Esta conexión se puede llevar a cabo de dos formas.

- A. **Vía inalámbrica.** En este caso se debe configurar el adaptador de red del ordenador con el nombre de red (SSID) especificado en el manual de usuario del punto de acceso.
- B. **Vía cable.** En el caso de llevarse a cabo la conexión vía cable, se tiene tres posibilidades: cable Ethernet 10/100BaseT a conectar en puertos RJ45 del ordenador y del punto de acceso, cable USB o cable específico del equipo a conectar al puerto serie del ordenador.

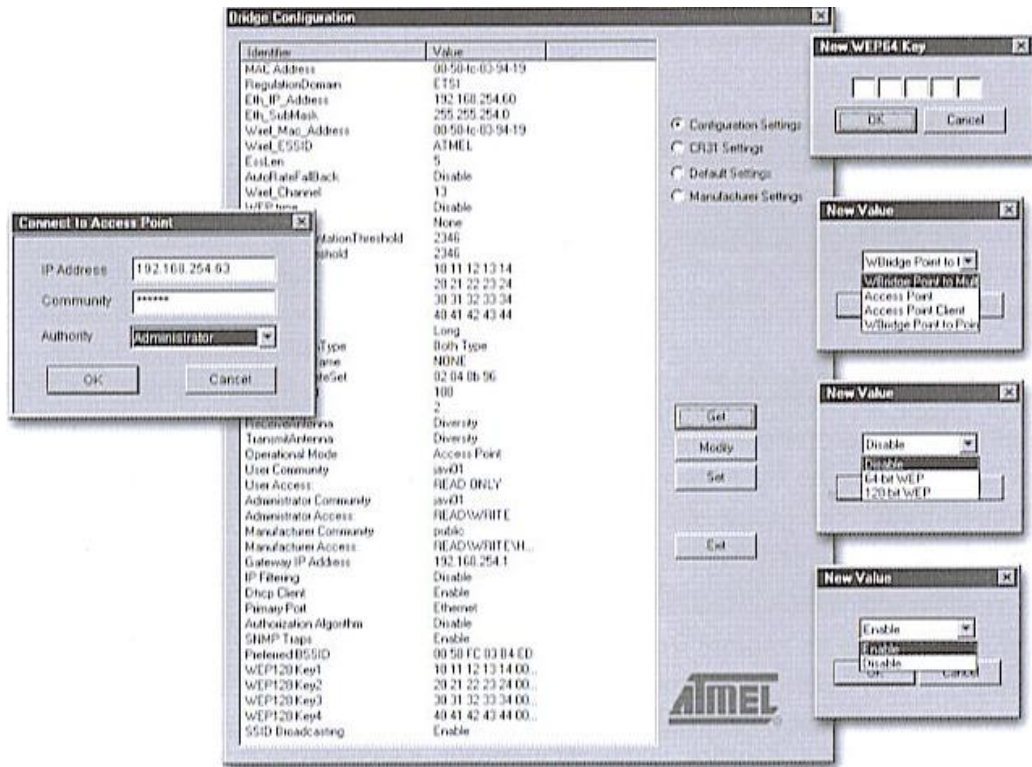


Figura 3. 7 Configuración de un punto de acceso (se muestra pantallas de configuración de distintas opciones)

2. a continuación se presenta dos alternativas dependiendo del modelo del punto de acceso.

A. Mediante una aplicación de configuración. Esto supone ejecutar una aplicación específica de configuración que viene incluida en el CD que acompaña al punto de acceso. Esta aplicación suele localizarse en el

directorio principal del CD bajo el nombre setup.

- B. **Mediante el servidor web del punto de acceso.** En este caso el punto de acceso incluye un servidor web al cual se accede desde el ordenador del usuario mediante cualquier navegador de Internet (Internet Explorer o Netscape). Previamente hay que configurar el ordenador para que obtenga la dirección IP de forma automática e introducir en el navegador de Internet la dirección (URL) que se indican en el manual del usuario del punto de acceso (una dirección IP que suele empezar por 192.168.x.x). Esto llevará a una ventana donde se solicita el nombre del usuario y clave para entrar en el menú de configuración. Estos datos pueden ser modificados por el administrador de la red, pero, por defecto el fabricante ofrece el nombre de usuarios y clave para permitirles al administrador entrar la primera vez. Estos datos por defecto suelen consistir en dejar el nombre de usuario en blanco e introducir la clave “admin”.
3. seguir las instrucciones del programa de configuración o moverse por las páginas web del punto de acceso para llevar a cabo los cambios de configuración deseados.

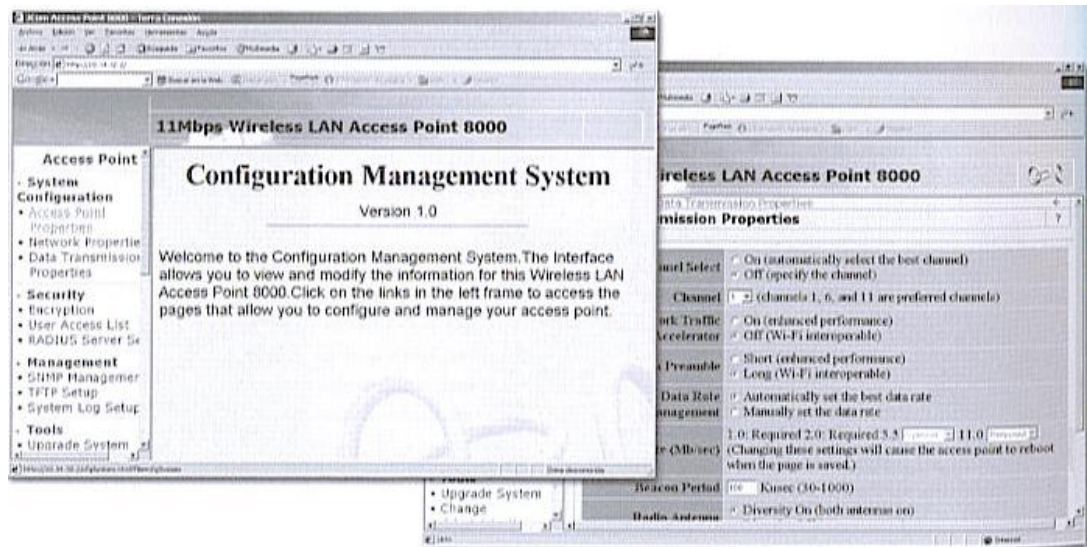


Figura 3. 8 Configuración de un punto de acceso accediendo a su servidor Web de configuración (3 COM)

Un punto importante es que, salvo que se utilice un cable específico para conectar el ordenador al punto de acceso, es necesario que el ordenador esté configurado convenientemente. Esto supone que el ordenador esté configurado para obtener la dirección IP de forma automática.

Tabla 3.1 Ejemplos de URL, usuario y clave para acceder a distintos puntos de acceso

MODELO	URL	USUARIO	CLAVE
Linksys AP router/switch	http://192.168.1.1		Admin
SpeedStream 2623	http://192.168.254.254		Admin
3Com Homeconnect	http://192.168.2.1		Admin
3Com Officeconnect	http://192.168.1.1		Admin
Adaptec Ultra Wireless	http://192.168.8.1	Admin	
Otros	http://192.168.1.250		Public

3.8 PROPIEDADES CONFIGURABLES EN EL PUNTO DE ACCESO

Existen modelos de puntos de acceso que solamente son puntos de acceso de red local inalámbrica. Sin embargo, es habitual

encontrar modelos de puntos de acceso que además incluyen en su interior un router, un switch o un módem DSL. Por este motivo las propiedades que son configurables en cada modelo de punto de acceso pueden variar dependiendo de todo lo que sea capaz de hacer. En cualquier caso, las propiedades principales propias de las funciones de punto de acceso son las siguientes:

Nombre de red (Network name). Al nombre de red se lo conoce también como SSID (Service Set Identifier, identificador del conjunto de Servicios). Los puntos de acceso suelen incluir un nombre por defecto. No obstante es recomendable sustituir este nombre por cualquier otro que se considere adecuado. Por cierto este nombre de red debe ser el que se configure en cada ordenador. Es importante recordar que en los nombres de red se diferencian las letras mayúsculas de las minúsculas.

- **Canal (Channel).** Aquí se deberá introducir el canal que se considere apropiado. Hay que tener en cuenta que aunque el sistema permita elegir cualquier canal, existen limitaciones regulatorias para el uso de los canales dependiendo del área geográfica en que se encuentre.

- **Seguridad (Security).** Los equipos Wi – Fi disponen de determinadas características de seguridad que pueden ser configuradas en el punto de acceso y en los adaptadores de cada ordenador que forme parte de la red. Es importante que los parámetros de seguridad que aquí se configuren sean los mismos que los que se configuren en cada ordenador. La primera vez que se configura un punto de acceso conviene dejar deshabilitados los parámetros WEP de seguridad. Una vez comprobado que la red funciona adecuadamente, se puede proceder a configurar las características de seguridad. Para utilizar el cifrado WEP hay que habilitar esta característica, elegir un tipo de cifrado (WEP type) e introducir una clave de cifrado

(WEP key). Sólo existen dos tipos de cifrado: 64 bits y 128 bits. El tipo de 128 bits ofrece mayor nivel de seguridad, pero también es cierto que hace bajar levemente el rendimiento. En cuanto a la clave de cifrado se trata de una palabra clave que puede incluir caracteres alfabéticos o numéricos. El sistema puede mantener hasta cuatro claves de las cuales sólo una estará activa. Periódicamente debe cambiarse la clave activa para aumentar la seguridad del sistema. Algunos sistemas incluyen una utilidad que permite generar claves de cifrado a partir de una frase (passphrase). Es más fácil recordar la frase que la clave.

Adicionalmente, los puntos de acceso ofrecen distintas características que ayudan a gestionar la red. Algunas de estas características son las siguientes:

- **Baja automática de la velocidad** (Auto rate fall back). Esta característica permite que cuando empeoren las condiciones de difusión de la señal radioeléctrica, el sistema pueda bajar la velocidad de transmisión para mantener la comunicación abierta.

- **Selección de los ordenadores autorizados** (Authorised MAC address). Algunos puntos de acceso incluyen la facilidad adicional de incluir una lista de los ordenadores autorizados (lista de direcciones MAC) a concertarse al punto de acceso. Esta característica es interesante cuando se desea incrementar la seguridad de la red pero no resulta práctica cuando se desea disponer de una red inalámbrica abierta de nuevos usuarios. En este caso tener seleccionada esta opción forzaría a cambiar la configuración del punto de acceso cada vez que se desea conectar a un nuevo equipo. Las direcciones MAC son unos números únicos que cada fabricante asignan a todos sus dispositivos inalámbricos. Este número identifica el dispositivo en forma inequívoca (incluidos los adaptadores de red de los

ordenadores). Las direcciones MAC están formadas por 12 caracteres alfanuméricos.

- **Emitir el nombre de red** (Broadcast SSID to asociate). Los puntos de acceso emiten generalmente su nombre de red (SSID) para permitirle a los posibles usuarios que pueden asociarse a la red con facilidad. No obstante si se desea aumentar la seguridad de la red, puede deshabilitarse esta opción. Esto hará que sólo puedan conectarse a la red aquellos usuarios que conozcan su nombre.
- **Clave de Acceso** (Password). El punto de acceso dispone de una clave para impedir el acceso a sus funciones de configuración. El fabricante configura a todos sus equipos con una misma clave de acceso (generalmente admin.) pero el usuario debe cambiar esta clave para aumentar la seguridad de su equipo.
- **Habilitar la red inalámbrica** (Enable Wireless Networking). Algunos equipos permiten que su función de punto de acceso pueda ser habilitada o deshabilitada. Esto es útil fundamentalmente por que el punto de acceso dispone también de las funciones de router o switch. En algún caso podría ser interesante mantener sus funciones de router y deshabilitar sus funciones de punto de acceso.

3.9 SELECCIÓN DE CANAL.

Las redes Wi – Fi dispone de 11 canales de 11 Mbps cada uno. Cada canal viene identificado por un número del 1 al 11 y por defecto, la mayoría de los puntos de acceso ya vienen configurados con un determinado canal. No obstante el número del canal que se va a utilizar cada punto de acceso es configurable. Esto es así porque, de otra

forma los puntos de acceso vecinos que vengán configurados con el mismo canal por defecto se interferirían unos a otros.

Cuando se colocan varios puntos de acceso para cubrir un área de cobertura de una misma red, debe procurarse que el área de solapamiento sea mínima y además configurar diferentes canales en cada uno de ellos.

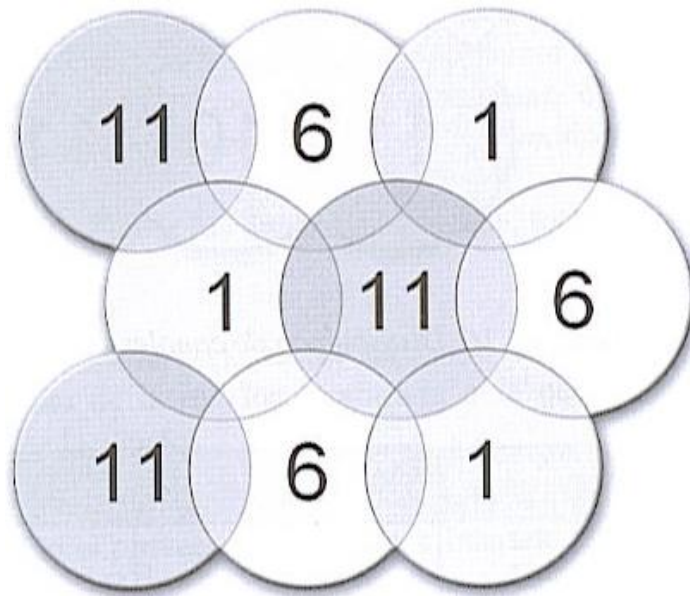


Figura 3. 9 Distribución de canales en células hexagonales

Cada número de canal $W_i - F_i$ se corresponde con una frecuencia determinada. Los números consecutivos representan también frecuencias consecutivas. Por tanto mientras más diferencias haya entre los números de canal, mayor diferencia habrá entre sus frecuencias. En una red con múltiples accesos es interesante tener en cuenta este detalle para intentar configurar a los puntos de acceso vecinos, no solamente con canales distintos (cosa imprescindible), sino que sus frecuencias estén lo más lejanas posibles.

En teoría con tan sólo tres frecuencias se podría cubrir cualquier área por grande que está fuera sin dejar zonas en sombra. Para ello, basta

con imaginarse que cada punto de acceso dispone de un área de cobertura hexagonal (lo que también se conoce como célula). Esto dejaría una distancia de cuatro canales intermedios.

En la asignación de canales a los puntos de acceso, hay que tener en cuenta que la propagación de las señales de radio se efectúan tanto horizontal como verticalmente. Esto quiere decir que si tiene plantas en un edificio cubiertas por distintos puntos de acceso habría que comprobar que no se producen interferencias entre plantas.

La teoría anterior no es del todo aplicable a países como España o Francia donde la regulación sólo permite la utilización de un número muy reducido de canales (dos en el caso de España, el 10 al 11, y cuatro en el caso de Francia del 10 al 13). En estos casos la única solución consiste en permitir zonas de sombras entre los puntos de acceso. El inconveniente es que, no sólo se impedirá el desplazamiento sin interrupción del servicio, sino que el número de usuarios que puedan coexistir en una misma área será bastante menor. Estos inconvenientes desaparecerán con la nueva tecnología de 5 GHz.

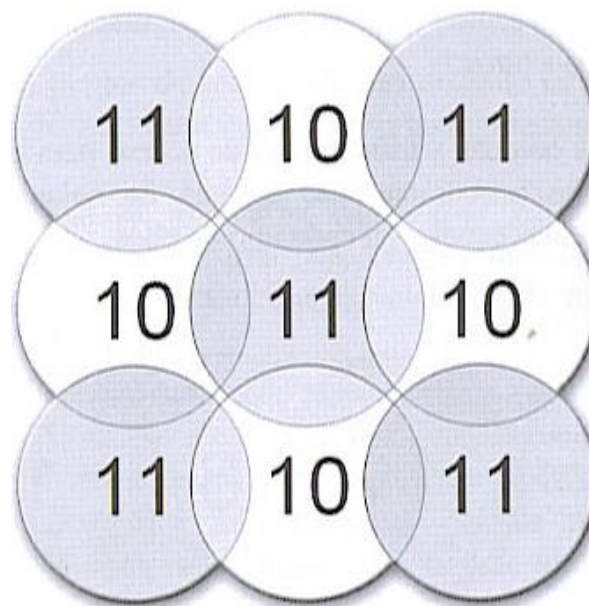


Figura 3. 10 Distribución de canales en células cuadradas

Tabla III. 2 Regulación de canales y frecuencias en distintos países

	FREC	FCC	ETSI			
CANAL	(MHz)	(USA)	(Europa)	ESPANA	FRANCIA	JAPÓN
1	2412	X				X
2	2417	X				X
3	2422	X	X			X
4	2427	X	X			X
5	2432	X	X			X
6	2437	X	X			X
7	2442	X	X			X
8	2447	X	X			X
9	2452	X	X			X
10	2457	X	X	X	X	X
11	2462	X	X	X	X	X
12	2467		X		X	X
13	2472		X		X	X
14	2484					X

3.10 CONEXIÓN CON LA RED LOCAL CABLEADA E INTERNET

Cuando se desea conectar un punto de acceso a una red local hay que configurarle a cualquier ordenador que forma parte de la red cableada. Para ello, las utilidades de configuración del punto de acceso dan la opción de configurar estos parámetros.

Una posibilidad muy común es configurar el punto de acceso para que obtenga las direcciones IP de su conexión con la red local cableada o con el proveedor de acceso a Internet (ISP) de una forma automática. Para ello, el punto de acceso ofrece la opción con el nombre Obtener una dirección IP automáticamente o similar.

Si hubiese que configurar los datos manualmente, los parámetros a configurar son los siguientes:

Dirección IP (IP Address). Es la dirección IP del punto de acceso como componente de la red local cableada o a la que el proveedor de acceso a Internet ha facilitado.

Máscara de subred (Subnet Mask). Es la máscara de la red local cableada o la que facilite el proveedor de acceso a Internet. Un número de máscara muy común es el 255.255.255.0.

Puerta de enlace (Gateway). Es el número IP del equipo al que el punto de acceso tiene que enviarle los datos con destino a Internet o red local cableada.

Servidor DNS (DNS Server). Son las direcciones IP de los DNS (servidor de nombres de dominio). Este dato lo facilita el proveedor de acceso a Internet.

3.11 INTERCONEXIÓN DE LOS PUNTOS DE ACCESO.

La interconexión entre los distintos puntos de acceso que forman una red inalámbrica suele realizarse mediante la conexión de cada uno de ellos con una red local cableada (idealmente Ethernet). Lo que sí es interesante es considerar que dicha conexión supone tener que disponer de cables que terminan de enlazar los puntos de acceso con el router, switch o hub de Ethernet.

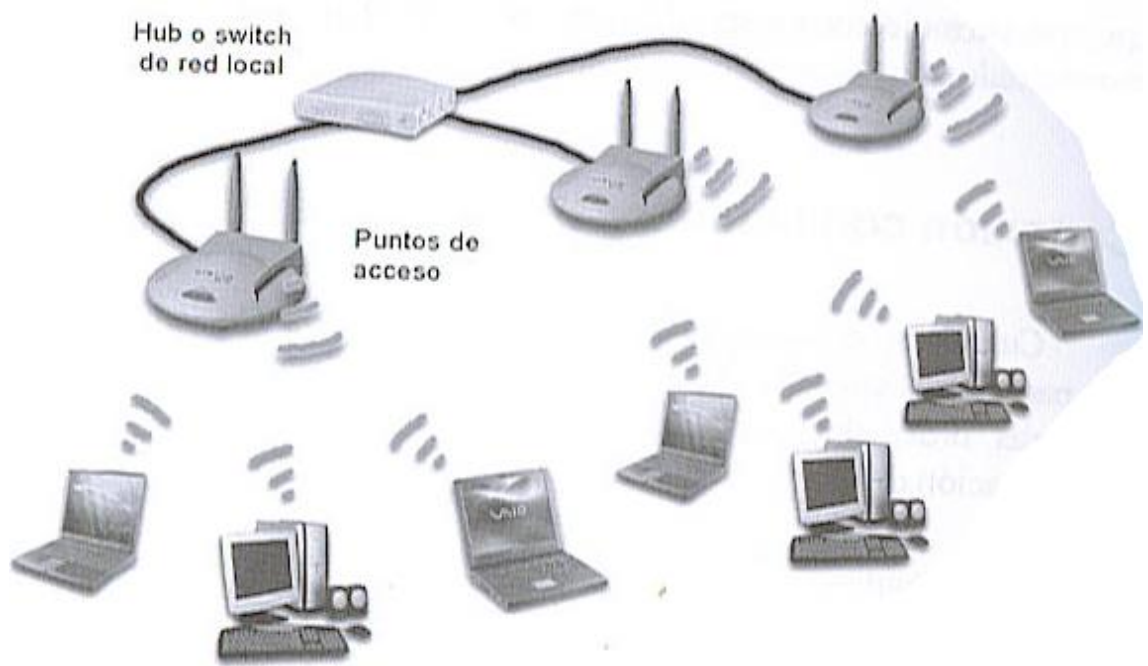


Figura 3. 11 Interconexión de los puntos de acceso

3.12 COMPROBAR EL FUNCIONAMIENTO

Una vez instalado todo lo instalable, sólo queda comprobar si funciona. Para ello se puede empezar por probar las comunicaciones entre dos de los ordenadores. Poco a poco se pueden ir conectando uno a uno el resto de usuarios hasta comprobar que todo funciona correctamente.

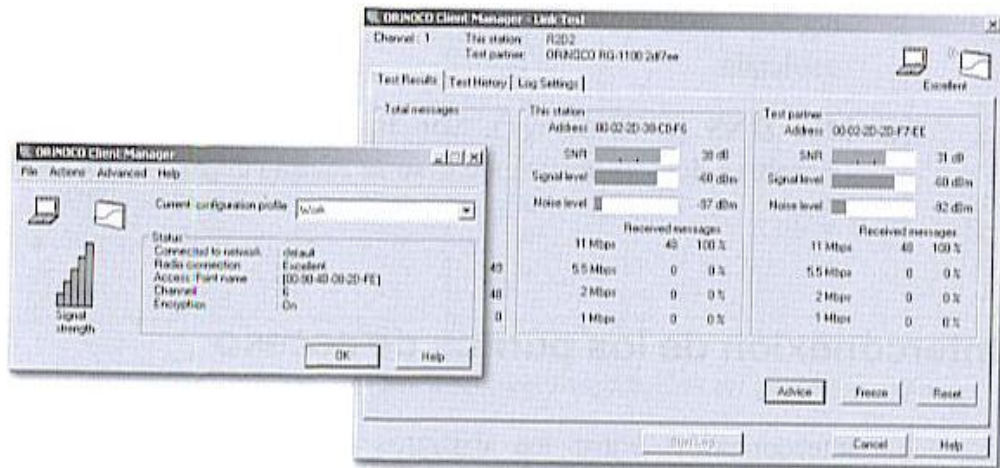


Figura 3. 12 Niveles de recepción de señal con las utilidades de Orinoco

La mayoría de los adaptadores de red incluyen en software de utilidades que permiten comprobar si el adaptador está recibiendo o no señales de otros equipos Wi – Fi (punto de acceso o adaptador), así como la calidad de dichas señales. La mejor forma de comprobar el funcionamiento de una red Wi – Fi es utilizado estas aplicaciones.

El sistema operativo Windows XP incluye aplicaciones propias tanto para la instalación de los dispositivos Wi – Fi como para su monitorización.

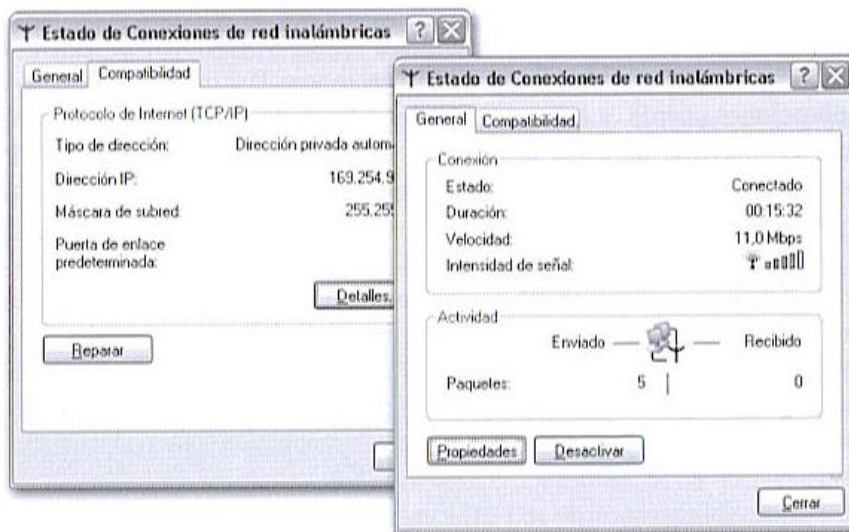


Figura 3.13. Utilidades Wi-Fi de Windows XP.

Si no se dispone de una de estas aplicaciones, se puede probar las comunicaciones abriendo el Explorador de Windows desde uno de los ordenadores y comprobar si se pueden ver los recursos que se han compartido en los otros ordenadores. Es posible que para hacer esto, tenga que hacer clic sobre la opción Entorno de red, Toda la red y sobre el grupo de trabajo que haya definido. Si el ordenador remoto tiene definido un nombre de usuario y clave de acceso para acceder a sus recursos, tendrá que introducirlos.

Para compartir recursos en un ordenador, se debe abrir el Explorador de Windows, buscar el recurso a compartir (el botón secundario). Aparecerá una lista de opciones donde podrá ver una con el nombre Compartir. Haciendo clic sobre esta opción, verá una ventana con todas las opciones de compartición.

Si se conoce el número IP del punto de acceso, se puede comprobar que un ordenador está en comunicación con el punto de acceso abriendo un navegador de Internet (Internet Explorer, por ejemplo) e introduciendo este número como dirección. Si se obtiene cualquier respuesta distinta de página no encontrada, es que funciona la conexión. Incluso, todavía sería más fiable la utilización del comando ping. Abra una ventana de DOS desde Windows y teclee ping seguido del número IP del punto de acceso (por ejemplo, ping 192.168.1.) si aparece una línea que empieza por reply from, es que la conexión funciona. Si la línea empieza por "Request timed out", es que no funciona.

3.13 GESTIÓN DE LA RED

Existen aplicaciones que permiten vigilar y gestionar el funcionamiento de la red. De hecho, existen dos tipos de aplicaciones: las que se

instalan en las estaciones, aplicaciones clientes y las que instalan el administrador para vigilar la red, aplicaciones de red. La mayoría de estos programas se basan en el protocolo SNMP (Simple Network Management Protocol, Protocolo Simple de Gestión de Red).

Las aplicaciones clientes están relacionadas con la tarjeta de red inalámbrica de que disponga. Suele ser el propio proveedor del adaptador de red el que facilita la aplicación. Estas aplicaciones facilitan información sobre la calidad de la señal, el estado de la conexión, SSID, WEP, etc. Las aplicaciones cliente permite definir distintos perfiles para que el usuario pueda utilizar la misma tarjeta en distintas redes.

Las aplicaciones de redes ofrecen herramientas tanto para el seguimiento como para la gestión de la red. La mayoría de los puntos de acceso vienen acompañados de un software de este tipo.

3.14 MEDICIÓN DE LA VELOCIDAD

La velocidad máxima a la que transmite Wi – Fi es de 54 Mbps; no obstante esta velocidad puede ser menor dependiendo de la distancia entre emisor y receptor y de las condiciones del entorno. También hay diferencia si los equipos se encuentran en el interior de un edificio o en el exterior en espacio abierto. La transmisión en el exterior suele ser de mayor calidad porque existen menos interferencias y menos equipos intentando competir por el uso del espectro radioeléctrico.

A pesar de lo anterior, la percepción de la velocidad es algo relativo. 54 Mbps. es una buena velocidad para la mayoría de las aplicaciones que de hoy en día, no obstante, se percibirá como lenta si se pretende transmitir un archivo de gran tamaño o acceder al directorio de un ordenador remoto, pero en el resto de casos es una velocidad suficiente.

Si desea comprobar la velocidad a la que está haciendo uso de la red, la mayoría de las aplicaciones cliente de las tarjetas Wi – Fi permite comprobar este dato, además de otros como la relación señal / ruido, nivel de recepción de la señal recibida, etc.

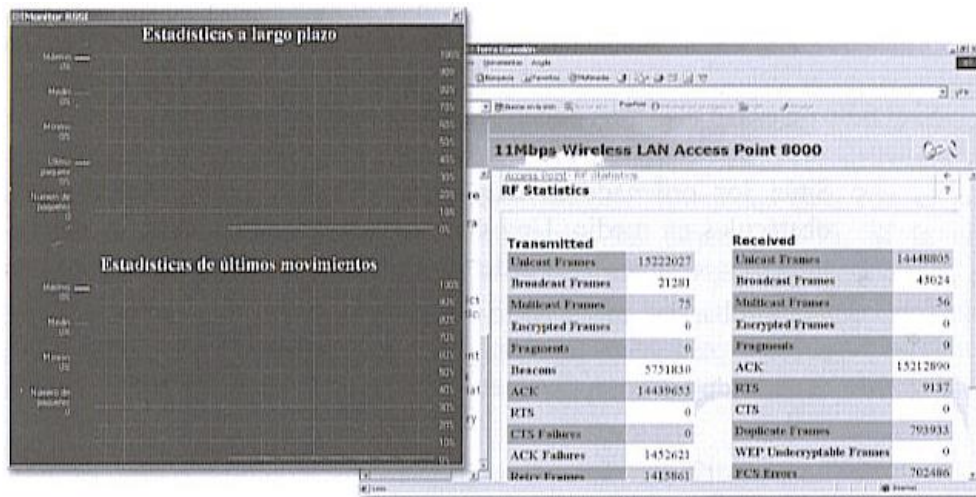


Figura 3.14 Distintas herramientas de gestión de la red

3.15 SOLUCIÓN DE PROBLEMAS

Si, después de hacer todo el trabajo de instalación y configuración en uno de los ordenadores, no es posible ver los recursos compartidos, a veces las instalaciones requieren una segunda pasada.

Lo primero que hay que hacer es comprobar lo evidente, comprobar que todos los dispositivos están encendidos, funcionando y bien conectados. Si hubiese una antena exterior, deberá comprobar que está conectada. Las tarjetas PCMCIA (PC Card) o unidades USB deben estar insertadas o conectadas al ordenador. Se puede mover estas conexiones para comprobar que están firmemente conectadas.



Figura 3.15 Dispositivo hardware detector de señal Wi-Fi (Sniffer)

Si el fallo es tan evidente, puede probar otras causas:

- Sitúe los ordenadores más cerca del punto de acceso evitando que haya obstáculos en medio. Una vez establecida la conexión en estas condiciones se podrá ir separando los ordenadores hasta situarlos en la localización deseada.
- Comprobar las luces de las unidades Wi – Fi (adaptadores de red y puntos de acceso) para comprobar si están funcionando como indican los manuales de usuarios de los equipos. Quizás esto de una pista de lo que está funcionando mal.
- La mayoría del hardware (impresoras, equipos Wi – Fi, etc) disponen de una utilidad que permite comprobar de forma local que dicho hardware está operativo. Si se dispone dicha utilidad se debe hacer la comprobación.
- Comprobar que software de utilidad que venía con la unidad Wi – Fi está instalada y funcionando correctamente.

- Desconecte y vuelva a conectar la unidad Wi – Fi. Esto hará que se reinicie la unidad. A veces es necesario este tipo de reinicio aunque la unidad haya estado funcionando bien durante mucho tiempo.

- Comprobar que los parámetros de la comunicación (Tipos de red, SSID y canal) están configurados adecuadamente en ambos equipos. Cuando en una configuración de red se va a permitir roaming (desplazamiento con servicio entre puntos de acceso), las tarjetas Wi – Fi de los ordenadores deben configurarse para que se adopten automáticamente los valores de configuración de SSID y canal de punto de acceso. Si fuese este el caso, comprobar que está configurado correctamente.

- Comprobar que los parámetros de seguridad están configurados en los mismo valores en ambos equipos.

- Comprobar que el nombre de un ordenador es distinto al nombre del otro y que no coinciden con el nombre del grupo de trabajo.

- Comprobar que las direcciones TCP/IP son distintas en todos los ordenadores o bien, que los ordenadores están configurados para obtener las direcciones IP de forma automática

- Comprobar que los adaptadores de red están instalados correctamente en el ordenador. Se puede comprobar esto haciendo clic con el botón derecho sobre el Mi Pc, luego sobre Propiedades y Gestor de dispositivos y comprobar que la unidad Wi – Fi se encuentran en la lista de hardware conectado en el ordenador y que no tiene ningún signo de exclamación sobre él. El signo de exclamación indicaría que existe algún conflicto con este hardware. Si fuese este el caso, desinstale la unidad (a través de Añadir / Quitar hardware del Panel de Control) e instálelo de nuevo.

- Si ninguna de las comprobaciones anteriores ha sacado de dudas aunque sea poco probable, lo mismo está ante un fallo hardware. El fallo puede estar en el ordenador, el punto de acceso en la tarjeta Wi – Fi (El adaptador de red). Por ejemplo, si otros ordenadores consiguen funcionar bien con el punto de acceso, se puede probar en intercambiar las tarjetas Wi – Fi. Si la conexión funciona con esta nueva tarjeta Wi – Fi, es posible que la tarjeta Wi – Fi anterior esté estropeada. Si la tarjeta Wi – Fi funciona bien con el nuevo ordenador es posible que el ordenador anterior tenga algún problema. Si lo que no funciona es el punto de acceso, se puede intercambiar este equipo por otro y hacer una comprobación similar a lo anterior.

- A veces, lo que está estropeado son los circuitos electrónicos de un dispositivo, si no los conectores o los cables. Esto se puede comprobar intercambiando los cables o los dispositivos, aunque Wi – Fi sea inalámbrico, existen dispositivos que se conectan a los ordenadores o equipos de red (Switch hubs, routers, etc.) utilizando cables.

- Si ha llegado hasta aquí sin resolver el problema, le queda todavía las siguientes opciones. Lea la sección problemas (Problems) o la sección preguntas frecuentes (FAQ) del manual de usuario de la unidad Wi – Fi . También puede acceder a la web del fabricante y leer estas mismas secciones por si hubiese algo nuevo, no incluido en el manual.

3.16 CONEXIONES MALAS

Si se puede establecer una conexión, pero esta conexión tiene muy mala calidad, puede hacer las siguientes comprobaciones:

- Intentar enviar o recibir un archivo si se puede acceder a dicho archivo, pero la comunicación va extremadamente lenta (nunca se termina de completar la transmisión), comprobar las posibles fuentes de interferencias o si existe un número muy elevado de usuarios conectados en sólo punto de acceso.
- Si a veces funcionan bien las comunicaciones y otras veces no, comprobar si los fallos coinciden con las circunstancias de haber muchos usuarios conectados a la red. Es posible que en esas circunstancias se tengan sobrecargados los puntos de acceso. En estos casos se puede instalar puntos de acceso adicionales a lado del anterior o comprobar reposicionando el punto de acceso, se consigue mejorar la respuesta.

CAPÍTULO IV

LA CONEXIÓN A INTERNET

4.1 INTRODUCCIÓN

Dicen los expertos que en un futuro próximo la mayor parte de nuestra información estará en internet. Esto nos permitirá disponer la información independientemente de donde nos encontramos: en casa, en la oficina, de visita profesional o personal o de vacaciones. Siempre podremos acceder a nuestras bases de datos, catálogos de fotos, documentos, libros o aplicaciones.

Pues bien, las redes inalámbricas permiten que todos los dispositivos conectados a la red puedan compartir una única conexión a Internet. Evidentemente esto no significa que todos los usuarios tengan que ver las mismas páginas web. Cada usuario puede navegar por sus propias páginas, leer su correo o hacer cualquier otro uso de Internet. Lo que sí es cierto es que el ancho de banda de la conexión es compartido entre los usuarios. Por tanto, es posible que en algunos momentos la conexión vaya algo más lenta de lo habitual, pero, en general, la navegación será bastante buena. Si no lo fuera siempre se pueda contratar una velocidad mayor de acceso a Internet o contratar más de una línea de acceso.

La inmensa mayoría de los modelos de punto de acceso ya tienen integrada la posibilidad de compartir una conexión a Internet o cualquier otra red. Esto es posible por que el punto de acceso tiene integrada la función de router. El router es un equipo que hace de intermedio entre

el Internet y cada uno de los ordenadores de la red privada en este caso inalámbrica.

Evidentemente, para compartir un acceso que permite acceso a Internet, lo primero es disponer del acceso. Las empresas que facilitan los servicios de acceso a Internet se conocen con el nombre de proveedores de acceso o por el acrónimo en inglés, ISP, Internet Service Provider.

Aunque existen puntos de acceso que permiten compartir el acceso a Internet de baja velocidad (56 Kbps) lo más recomendable es disponer de un acceso de banda ancha: ADSL, módem cable, satélite, etc.

4.2 EL ACCESO A INTERNET

La red de Internet es una red global interconectada con prácticamente todos los tipos de redes públicas de telecomunicaciones existentes en la actualidad. Esto quiere decir que cualquier persona que tenga acceso a una red de comunicaciones (red telefónica, red de móviles, RDSI, satélites, etc.) podrá tener acceso a través de ésta a la red de Internet.

La red pública más extendida es la red telefónica básica. Esto hace que la mayoría de los usuarios de Internet utilicen esta red como su acceso habitual. No obstante, existen otros caminos de acceso a Internet que son utilizados fundamentalmente por aquellos usuarios que necesiten un acceso a más alta velocidad (banda ancha) o que están situados en unos emplazamientos sin cobertura telefónica.

4.3 ANCHO DE BANDA

Un término que se utiliza frecuentemente cuando se habla del acceso a Internet es el de banda ancha o banda estrecha. Cuando se hable de comunicación digital, la palabra ancho de banda hace referencia a la velocidad con la que se transmiten los datos entre dos puntos (los bits por segundo). El ancho de banda de acceso a Internet es la velocidad con la que se está conectando con esta red. El estar conectado a Internet con banda estrecha significa estar conectado a baja velocidad y el hacerlo con banda ancha significa disponer de alta velocidad.

Realmente, la frontera entre la banda ancha y estrecha no está claramente definida. No obstante, se entiende que la velocidad que se puede alcanzar utilizando un canal telefónico o RDSI es la banda estrecha y las velocidades superiores son banda ancha. En este sentido la frontera entre ambas bandas se encuentra en 64 Kbps. Igual o menor es banda estrecha, superior es banda ancha. En la práctica, la banda empieza en 128 Kbps ya que no existe comercializada ninguna conexión superior a 64 y menor a 128 Kbps.

4.4 EL PROVEEDOR DE ACCESO

Un proveedor de acceso, también conocido como ISP (Internet Service Provider, Proveedor del Servicio de Internet), es un intermediario que facilita el acceso a Internet a las personas o empresas interesadas. Los proveedores de acceso suelen ofrecer a sus clientes la posibilidad de acceder a Internet por cualquiera de los sistemas siguientes:

4.4.1 BAJA VELOCIDAD

(banda estrecha), mediante un módem de red telefónica básica o de RDSI. Para ello, le facilitan al cliente un nombre de usuario y clave y una lista de números telefónicos de acceso para que el

cliente elija el número que le venga mejor dependiendo de dónde se encuentre.

4.4.2 ALTA VELOCIDAD

(banda ancha), mediante circuito dedicado. En este caso, dependiendo del tipo de proveedor de acceso de que se trate, puede ofrecer un tipo de solución tecnológica u otra. ADSL, módem cable, LMDS, circuito Frame Relay, solución por satélite, etc. En cada caso, el proveedor de acceso suele facilitarle al usuario el equipamiento necesario.

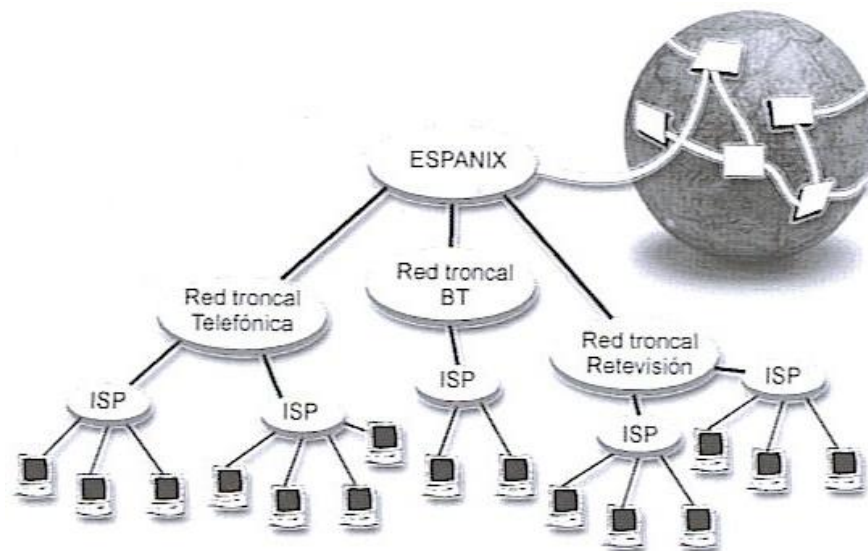


Figura 4.1 visión simplificada de una red de acceso a Internet

Por otro lado, como toda conexión a Internet requiere una configuración en el ordenador del usuario, el proveedor de acceso siempre tiene que proporcionar al usuario todos los parámetros necesarios para realizar esta configuración.

4.5 EL ACCESO DE BANDA ANCHA

El estar conectado a Internet con banda ancha quiere decir que se dispone de un gran ancho de banda o, lo que es lo mismo, que se está conectando a Internet a alta velocidad. En la práctica, esto significa de una conexión igual o superior a 128 Kbps.

El acceso a Internet mediante banda ancha y a bajo coste es un servicio relativamente reciente. De hecho, aunque las redes de televisión por cable ofrecían esta posibilidad desde hace tiempo, la introducción masiva de este tipo de acceso ha venido de la mano del servicio ADSL.

Los servicios de acceso a Internet en banda ancha más comunes son los siguientes:

- Acceso mediante ADSL
- Acceso mediante módem cable
- Acceso vía satélite
- Acceso vía radio LMDS
- Acceso vía circuito dedicado de datos

Por cierto cuando se accede a Internet por línea telefónica o RDSI, es necesario disponer de la línea y luego contactar con un proveedor de acceso a Internet. Sin embargo, cuando se accede a Internet con banda ancha, el propio proveedor de servicios de banda ancha facilita el acceso a Internet, cuentas de correo e incluso, espacio para la creación de páginas web. Esto quiere decir que estos casos no hace falta contratar con ningún otro proveedor de acceso a Internet.

Tabla 4.1 Comparación de las distintas formas de acceso a Internet

CARACTERÍSTICAS	TIPO DE ACCESO				
	LINEA TELEFON	LINEA RDSI	ADSL	CABLE MODEM	LMDS
Velocidad máxima	56K	64/128K	2M	2M	2M
Tipos Tarificación	X Tiempo	X Tiempo	Fijo x Mes	Fijo x Mes	Fijo x Mes
Red Soporte	RTB	RDSI	RTB/RDSI	TV Cable	Radio
Tipos de Medios	Compartido	Compartido	Dedicado	Compartido	Compartido
Tipo de MODEM	56K	RDSI	ADSL	Cable	Lmds
Equipo Especial			Filtro	Filtro	E. radio
Seguridad	Baja	Baja	Alta	Media	Media

Eficiencia	Baja	Baja	Alta	Media	Media
Web Hosting	SI	SI	Si	No	No
Usuario/clave acceso	SI	SI	No	No	No
Siempre conectado	No	No	Si	Si	Si
Banda Ancha	No	No	Si	Si	Si
NOTAS: - Equipamiento especial suele ser facilitado por el proveedor del servicio de acceso - RTB significa línea telefónica básica o línea telefónica normal					

4.6 VENTAJAS DE LA BANDA ANCHA

La posibilidad de acceder a Internet con banda ancha está haciendo que surjan servicios que se aprovechen de alta velocidad. Por ejemplo, la posibilidad de incorporar vídeo está dando paso a popularizar aplicaciones como tele vigilancia, tele formación o videoconferencias. Ver una imagen del negocio, una panorámica de la habitación donde están los niños (en la guardería o en casa) o celebrar una reunión familiar sin moverse de casa siempre no ha sido posible, pero ahora está al alcance por muy pocos dólares.

Las ventajas principales de los servicios de acceso a Internet con banda ancha son las siguientes:

ALTA VELOCIDAD. Ofrece una velocidad de acceso a Internet de hasta 2 Mbps.

SIEMPRE CONECTADO. No hace falta perder tiempo establecido la conexión. La conexión de banda ancha está siempre activa y funcionando.

VOZ Y DATOS SIMULTÁNEAMENTE. Función de forma completamente las 24 horas al día por un bajo precio fijo mensual.

4.6.1 ACCESO MEDIANTE ADSL

ADSL son las siglas de una nueva tecnología pensada para poder transmitir datos a alta velocidad (banda ancha) a través de los bucles de abonado de las líneas telefónicas. El bucle de abonado es el par de hilos de cobre que va desde la casa del usuario hasta la central telefónica y que suele utilizar para disponer del servicio telefónico o de fax.

Aunque la tecnología ADSL permite velocidad de hasta 8 Mbps, la velocidad real que puede conseguir el usuario depende de la distancia del domicilio del usuario a la central telefónica del proveedor del servicio ADSL.

El significado de las siglas ADSL es **Asymmetric Digital Subscriber Line o Línea de Abonado Digital Asimétrica**. La letra A de asimétrico significa que no emplea el mismo ancho de banda para subir (transmisión usuario – red) que para bajar información (transmisión red – usuario). En la práctica, esto quiere decir que la mayoría de los recursos de la conexión se emplea en la bajada de información, como suele ser habitual en el uso de Internet.

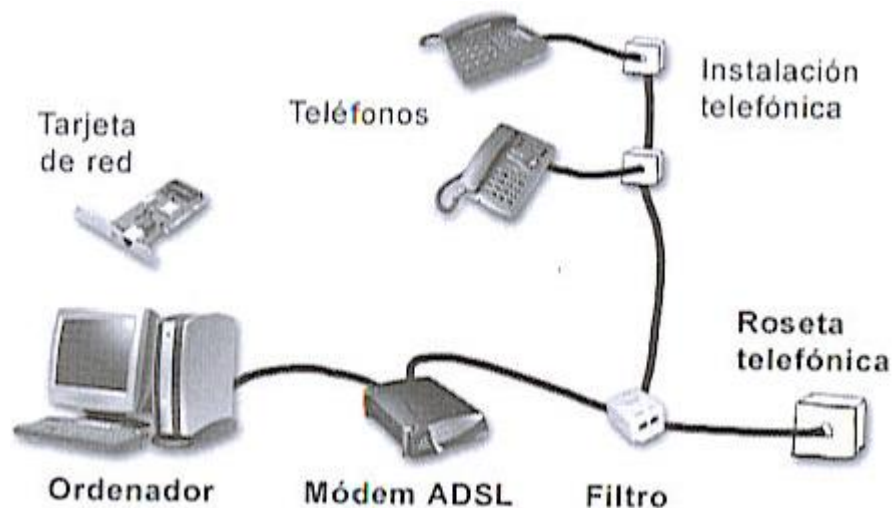


Figura 4.2 Instalación de un acceso ADSL

Para instalar el servicio ADSL, se necesita disponer de un filtro (splitter o microfiltros) y un módem ADSL (ATU – R, ADSL Terminal Unit – Remote). Este módem ADSL ofrece una salida de la red Ethernet. Esto quiere decir que cualquier ordenador (que disponga de una tarjeta de Ethernet) o punto de acceso Wi – Fi puede conectarse directamente al módem ADSL.

Tabla 4. 2 Tipos de Acceso a Internet desde el hogar.

CARACTERÍSTICA	VALORACIÓN
Linea Telefónica Básica	48.4%
ADSL	32.1%
MODEM Cable	14.7%
Linea RDSI	3.5%
Punto a Punto	0.3%
Otros sistemas (redes de datos, etc)	0.8%

4.6.2 ACCESO MEDIANTE MODEM CABLE

El módem cable es un dispositivo, un módem, que permite el acceso a Internet a alta velocidad a través de las redes de televisión por cable. El sistema permite velocidades de hasta 40 Mbps, aunque, por razones técnicas y comerciales los proveedores suelen limitar este acceso a velocidades por debajo de 2 Mbps. Evidentemente, este servicio es propio de las empresas de televisión por cable y como se puede suponer, la recepción de los canales de televisión no se ve afectada por la existencia del módem cable.

Es importante destacar que algunos operadores de cable no cuenta con un sistema de cable bidireccional, por lo que, en estos

casos, el usuario necesita disponer además de una línea telefónica. La información usuario – Internet sube por la línea telefónica, mientras que la información Internet – usuario baja por la red de cable de alta velocidad. En este caso, al sistema se lo conoce como TRI (Telephony Return Interface, Interfaz de Retorno Telefónico). Las redes de televisión digital por satélite o por radio suelen utilizar este sistema.

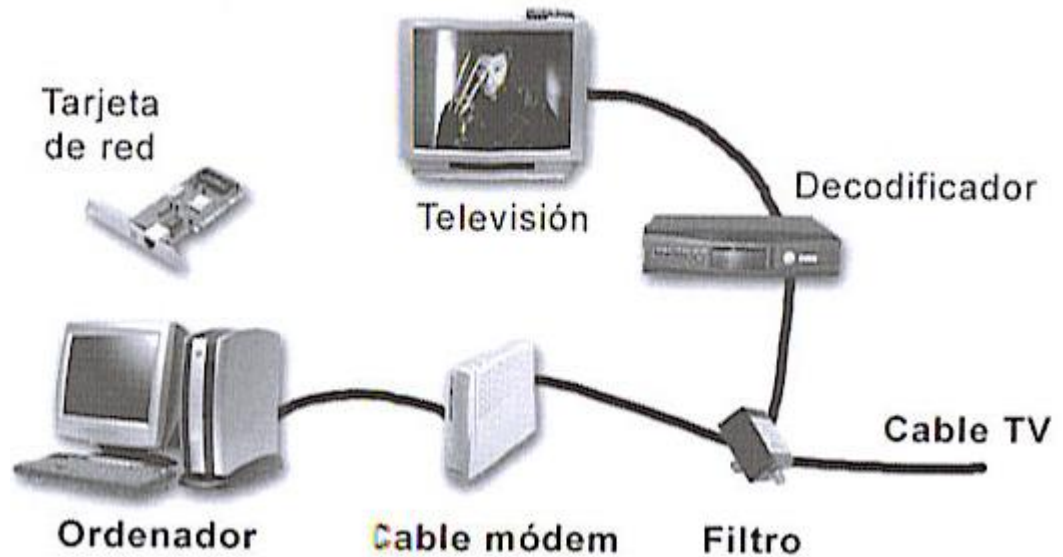


Figura 4.3 Instalación de un acceso por cable MODEM

Tabla 3.3 Tamaño de las informaciones

TIPO DE INFORMACIÓN	TAMANO TÍPICO
Mensaje de correo electrónico	2.2KB
Documento de 20 paginas	44KB
Imagen gráfica	330KB
Un minuto de audio	475KB
Un minuto de video	2.400KB

4.6.3 ACCESO POR SATÉLITE

Si se vive en un lugar remoto donde no se tiene acceso a la mayor parte de las nuevas tecnologías, pero se necesita de una conexión a Internet de alta velocidad, la solución apropiada es la conexión por satélite. La conexión por satélite sólo necesita tener una vista despejada hacia el cielo del sur (o del norte, si se encuentra en el hemisferio sur)

El satélite puede ofrecer velocidades de hasta 400 Kbps sin necesidad de disponer de línea telefónica o velocidades incluso mayores para aquellos sistemas que se apoyan en el uso de la línea telefónica para la transmisión usuario – Internet.

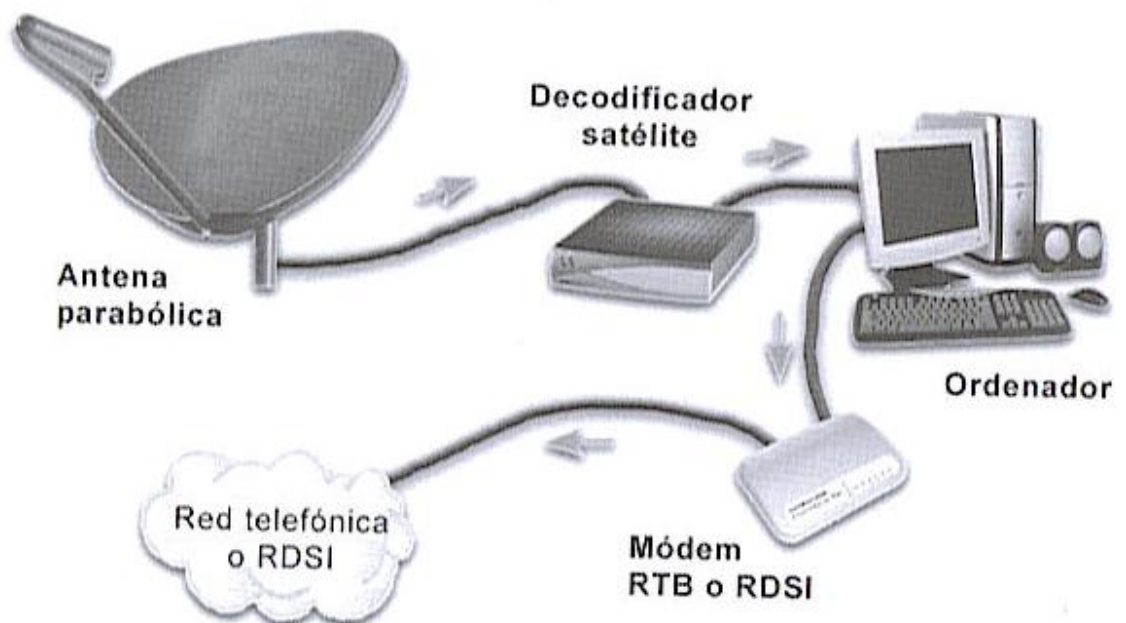


Figura 4. 4 Instalación de un acceso por satélite

El usuario necesita disponer de una antena parabólica, un módem especial (decodificador) para este tipo de conexiones y el

software correspondiente. Todo este equipamiento suele ser proporcionado por el proveedor del servicio.

Existen tres proveedores típicos de este tipo de servicios: las operadoras de telecomunicaciones, las empresas de televisión por satélite (Vía Digital o Canal Satélite Digital) y las empresas especializadas en este tipo de conexión para Internet.

Tabla 4. 4 Comparación de tiempos y tecnología

MODO DE ACCESO	VELOCIDAD DE TRANSMISIÓN	TIEMPO NECESARIO
Modem sobre GSM	9.600 Kbps	1 h 56' 30 "
Red telefónica básica	56 Kbps	2' 26 "
Acceso básico RDSI	64 Kbps	2' 8 "
Dos canales RDSI	128 Kbps	1' 4 "
ADSL 256 Kbps	256 Kbps	32 "
ADSL 512 Kbps	512 Kbps	16 "
UMTS 1 Mbps	1 Mbps	8 "
ADSL 2 Mbps	2 Mbps	4 "
ADSL máximo	8 Mbps	1 "
VDSL 55 Mbps	55 Mbps	0,1 "
Circuito Dedicado	155 Mbps	0,05 "

4.6.4 ACCESO VIA RADIO LMDS

La tecnología LMDS (Local Multipoint Distribution Service o Servicio Local Distribución Multipunto) permite un acceso a Internet de banda ancha hasta 8 Mbps mediante el establecimiento de un enlace de radio bidireccional. Por el mismo enlace pueden facilitarse servicio de telefonía, datos y vídeo.

La particularidad de LMDS es que el enlace de radio tiene que tener una visibilidad directa entre la antena parabólica a instalar en el domicilio del usuario y la estación base del operador del servicio. La estación base puede tener un alcance de hasta siete

kilómetros para un servicio sin restricciones o hasta veinte kilómetros con un menor ancho de banda. Una única estación base puede gestionar las comunicaciones de más de cuatro mil usuarios.

4.6.5 ACCESO MEDIANTE CIRCUITOS DE DATOS

Otras de las posibilidades de acceder a Internet es mediante circuitos de datos. En este caso se ha llamado circuito de datos a las líneas punto a punto y los circuitos de redes públicas de transmisión de datos. Esta solución suele ser adecuada para organizaciones que desean ofrecer información a la red o para aquellas empresas que desean conectar una red de área local (o Intranet) a Internet.

4.6.6 ACCESO MEDIANTE CIRCUITOS PUNTO A PUNTO.

A este tipo de circuitos se les conoce como circuitos dedicados o circuitos alquilados. Un circuito punto a punto es una línea dedicada exclusivamente a mantener una conexión entre dos ordenadores. Estos circuitos se alquilan generalmente a las compañías telefónicas, encargándose éstas de utilizar el medio más adecuado en cada caso para su constitución (por ejemplo, fibra óptica, par de hilos telefónicos, microondas, etc). Una conexión de este tipo suele tener una velocidad de transmisión de entre 64 Kbps y 2 Mbps, aunque también son normales velocidades superiores, pudiéndose llegar a los 622 Mbps.

Los circuitos punto a punto no tiene tiempo de establecimiento de conexión, no tienen una limitación de velocidad y no comparten el acceso con otros usuarios, por lo que resulta ser el medio más

rápido y eficaz de conectarse a Internet pero también es el más caro, por lo que en ocasiones puede convertirse en un lujo innecesario. En general este tipo de conexiones es propio de grandes organizaciones de pequeñas empresas relacionadas con Internet.

4.7 LA CONEXIÓN DE WI – FI INTERNET

La conexión de una red inalámbrica Wi – Fi con Internet se lleva a cabo a través del punto de acceso. En el mercado existen distintos modelos de puntos de acceso con distintas características. No obstante, las facilidades que puede presentar un punto de acceso para su conexión a Internet son las siguientes:

- Disponer de un puerto 10/100 Base – T (RJ – 45 o Ethernet, también conocido como uplink port) por donde conectarse al módem ADSL, al módem cable o al hub o switch de la red local cableada que ya está conectada a Internet.
- Disponer internamente de la funcionalidad hub. Esto facilitaría de dos a cuatro puertos exteriores 10/100 Base – T (RJ – 45 o Ethernet) por donde poder conectarse a la red local cableada con conexión a Internet o al módem ADSL / cable. Adicionalmente esta funcionalidad de hub permitirá crear una pequeña red local cableada de dos a cuatro ordenadores. Si se necesitare de más de cuatro puertos, siempre se puede utilizar otro hub o switch y conectarlo al punto de acceso para extender la red cableada.
- Un puerto serie RS – 232 a donde se le puede conectar un módem tradicional de red telefónica (V90 a 56 Kbps). Esta conexión a Internet a baja velocidad podría ser utilizada como acceso principal a

Internet o como acceso secundario de seguridad en el caso de que falle la conexión principal de banda ancha (ADSL o módem cable)

- Disponer internamente de un módem V90 (56 Kbsp) de línea telefónica. En este caso, el punto de acceso muestra al exterior un conector RJ11 (el conector telefónico al que se enchufan los teléfonos normales) que hay que conectar a la línea telefónica. Igual que en el caso anterior, esta conexión a Internet de baja velocidad podría ser utilizada como acceso secundario a Internet.

Esto quiere decir que la conexión de una red Wi – Fi a Internet pasa, generalmente, por conectar el punto de acceso a una red cableada que ya dispone de acceso a Internet o por conectarlo a un módem ADSL o módem cable.

Aparte de llevar a cabo esta conexión, y configurarla adecuadamente, existen puntos de acceso que incluyen la funcionalidad de router. Esto quiere decir que el punto de acceso podría ser configurado, por ejemplo con unas mejores medidas de seguridad (configuración de filtros), para compartir más de una dirección IP pública entre sus problemas de acceso a determinadas aplicaciones de Internet, etc.

4.8 INSTALACIÓN CONEXIÓN ENTRE WI – FI E INTERNET

Las interconexiones entre un punto de acceso Wi – Fi y un módem ADSL / cable pueden diferir levemente de unos fabricantes a otros; no obstante los conceptos básicos son los mismos.

La interconexión de la red Wi – Fi con el módem ADSL / cable consiste en interconectar ambos equipos mediante un cable 10 / 100 Base – T (RJ45). Para ello, primeramente hay que comprobar que tanto la red Wi – Fi como la conexión ADSL / cable están instaladas y funcionando correctamente de forma independiente.

Si la conexión ADSL / cable está funcionando conectada directamente a un ordenador, el trabajo consiste en sustituir el ordenador por el punto de acceso. Esto supone configurar el punto de acceso con los mismos parámetros con los que está configurando el ordenador y cambiar la conexión del cable del ordenador al punto de acceso.

Hay que tener presente que estas desconexiones y conexiones son muchos más seguras si se hacen habiendo apagado previamente los equipos a los que hay que desconectar o conectar los cables.

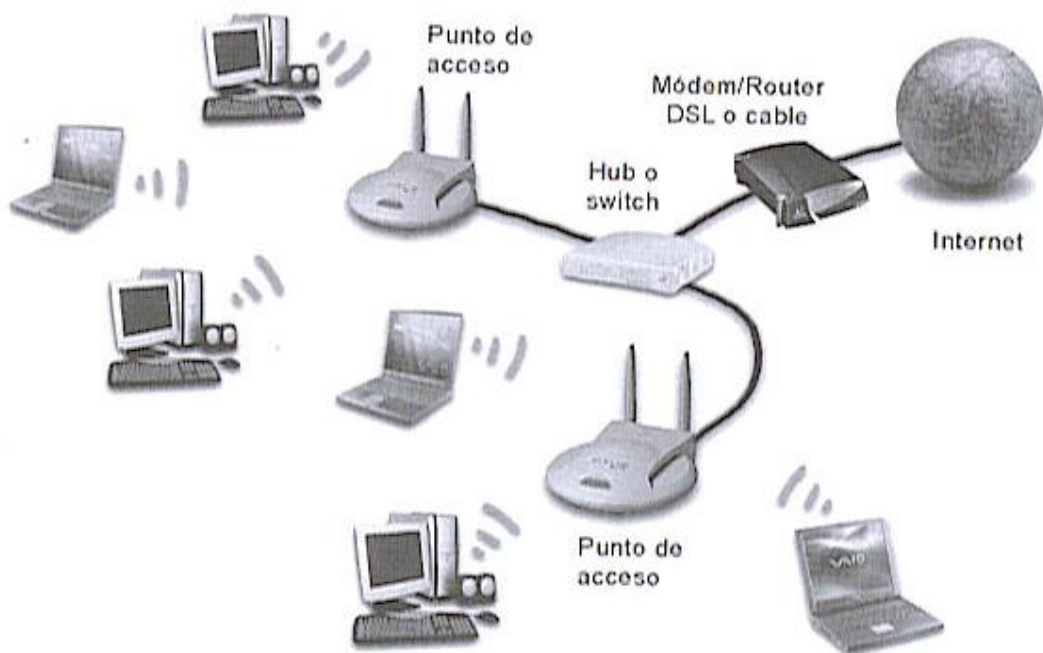


Figura 4.5 Conexión a Internet con Banda Ancha

4.9 CONFIGURACIÓN LA CONECCIÓN EN EL PUNTO DE ACCESO

Para configurar el punto de acceso, se debe ejecutar el software de utilidad que acompaña a los equipos Wi – Fi (suele venir en un CD). Este software permite verificar las conexiones, modificar las configuraciones y en general, gestionar las comunicaciones de la unidad Wi – Fi. Cada fabricante llama a este software de una manera. Por ejemplo, Sony lo llama Gíreles Palette (Paleta inalámbrica) y Orinoco lo llama Client Manager (Gestor de Cliente)

Por cierto, es siempre una buena idea acceder al web del fabricante de los dispositivos Wi – Fi para comprobar si existe una versión más moderna de los controladores, firmware y software de utilidad de estos dispositivos Wi – Fi. Si así fuera, es recomendable instalar las versiones más antiguas del CD.

Cuando se pone en marcha el software de configuración del punto de acceso y una vez introducida la identificación del punto de acceso y su clave, habrá que buscar la opción de configuración del puerto Ethernet. Generalmente se muestra un menú donde simplemente hay que elegir la opción general utilizada (ADSL, módem cable, red de área local o conexión local) o bien se muestran las opciones a configurar (números IP, etc). Para terminar se sale del programa de configuración aceptando los cambios. Esto hará que la nueva configuración se transmita al punto de acceso y todo quede listo para utilizar el acceso a Internet.

4.10 COMPROBACIÓN DEL ACCESO EN INTERNET

Para comprobar si el acceso a Internet está funcionando correctamente simplemente hay que abrir un navegador (Internet Explorer) y ver si se puede acceder a cualquier página web. Si las páginas web se pueden ver sin problemas, esto funciona. Si, por lo contrario se tiene como respuesta el famoso mensaje de que la página no se puede mostrar, entonces tenemos un problema.

Antes de darlo todo por perdido, conviene intentar acceder a distintas páginas. Es posible equivocándose a la hora de introducir el nombre de la página. Si aun así se tiene problemas, se debe comprobar la conexión a Internet desde ese ordenador conectándolo directamente al módem ADSL / cable. Si no funciona debe configurar dicha conexión en el ordenador siguiendo las instrucciones de la guía de usuario del módem DSL / cable.

Si el ordenador puede acceder a Internet desde el módem DSL / cable pero no desde la conexión inalámbrica y por otro lado la conexión inalámbrica de este ordenador funciona adecuadamente, sólo quedan dos puntos por comprobar: o el cable de conexión entre el punto de acceso y el módem no es el correcto o no está bien conectado, o el punto de acceso no está bien configurado.

En cuanto al cable, existen dos tipos de cables Ethernet categoría 5 (RJ54): cruzado y no cruzado. Los cables de tipo no cruzado no suelen tener ningún tipo de marca mientras que los de tipo cruzado suelen tener una marca especial, por ejemplo una marca negra donde se puede leer Crossover, Xover o similar se debe asegurar que se está utilizando un cable Ethernet categoría 5 (RJ45) no cruzado para conectar el módem ADSL / cable con el punto de acceso.

Se utiliza un router que es un equipo que sirve de intermedio entre los ordenadores de una red local (inalámbrica o cableada) y una red exterior (típicamente Internet). Esto es precisamente lo que hacen los puntos de acceso, por lo que es habitual que estos equipos ofrezcan determinadas funcionalidades de los routers.

4.11 DIRECCIONES IP

Todos los ordenadores o equipos que forman parte de una red local tienen que disponer de una dirección IP. Esta dirección IP es la que identifica al ordenador para todas sus comunicaciones. A las direcciones IP que utilizan los equipos de una red local se las conoce como dirección IP privada.

Las direcciones IP privadas tienen la misma apariencia que las direcciones IP de Internet. A estas últimas se las conoce como direcciones IP públicas. En ambos casos, las direcciones IP están formadas por una cadena de cuatro cifras separadas por un punto. Cada una de esas cifras puede tomar un valor entre 0 y 255. Por ejemplo 10.13.163.1 es una dirección IP. Sin embargo aunque ambos tipos de direcciones tengan las mismas apariencias, arbitrariamente son asignadas por el administrador o usuario de la red local, mientras que las direcciones IP públicas son asignadas por las autoridades de Internet

Las direcciones IP privadas están reguladas por el documento RFC 1918. En este documento se define que, para que una dirección IP privada sea compatible con Internet, debe estar dentro de los siguientes rangos:

Clase A. 10.0.0.0 a 10.255.255.255

Clase B. 172.16.0.0 a 172.31.255.255

Clase C. 192.168.0.0. a 192.168.255.255

Estas direcciones no son reconocidas por la red Internet. Esto quiere decir que ningún paquete de datos que tenga una de estas direcciones como identificación origen o destino puede progresar dentro de Internet. Esta particularidad impide que las direcciones IP privadas sean visibles directamente desde Internet. Por tanto el administrador de una red de área local es libre de utilizar cualquiera de estas direcciones dentro de su red.

Cuando una red local está conectada a Internet, su router es el que se encarga de traducir las direcciones IP privadas a públicas y viceversa, para que se pueda llevar a cabo la comunicación. El sistema que hace esto se conoce como NAT (Network Address Translation o Traducción de Dirección de Red). Por tanto un router debe tener una dirección IP privada (IPLAN) que lo identifique dentro de la red local y una dirección IP pública (IPWAN) que lo identifique en Internet.

Por último, el router tiene que saber que dirección de Internet tienen que enviar toda la información que salga de la red local. Esta dirección coincide con la dirección IP del router del proveedor de acceso (IP router remoto).

Direcciones configurables en un router son:

4.11.1 IP INTERNA DEL ROUTER

también conocida como dirección privada del router o IP LAN. Es la dirección IP que identifica al router dentro de la red local. Desde el punto de vista de los ordenadores de la red, la dirección IP interna del router es su puerta de enlace con Internet. Generalmente, la dirección interna del router suele ser la primera dirección IP del rango de direcciones privadas. Por ejemplo 172.26.0.1 o 192.168.0.1

4.11.2 IP EXTERNA DEL ROUTER

también conocida como dirección IP pública del router o dirección IP WAN. Es la dirección IP con la que se puede acceder al router desde Internet. No obstante, suele ser normal que el router esté

configurado con unos filtros para que, aun conociendo esta dirección, nadie ajeno pueda acceder a este equipo por el proveedor de acceso.

4.11.3 IP ROUTER REMOTO

es la dirección IP del router de la red del proveedor de acceso a Internet (ISP). Este valor puede generarse automáticamente.

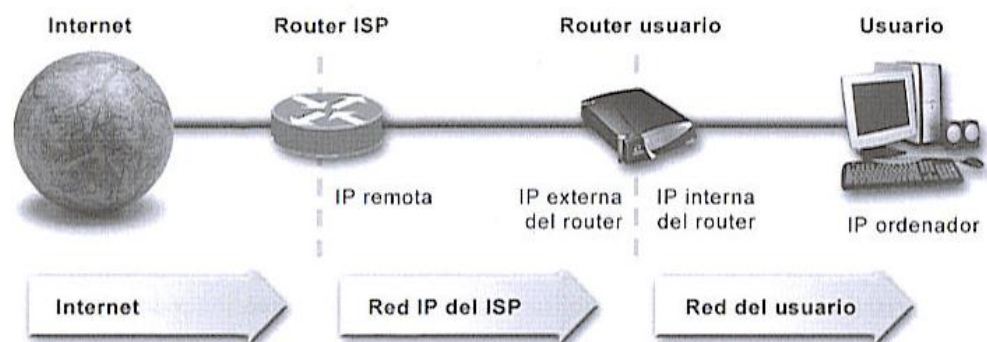


Figura 4.6 Las distintas direcciones de una IP de una conexión DSL

Tabla 4. 5 Configuraciones de direcciones IP

Ordenador	Router (LAN)	Router (Wan)	Router remoto
IP privada del ordenador p.e. 192.168.0.2 3,4.....	IP privada p.e. 192.168.0.1	IP pública	(IP pública AND máscara)+2

CAPÍTULO V

IMPLEMENTACIÓN DE LA RED EN EL ITSA

5.1 INTRODUCCIÓN

Las redes inalámbricas pueden tener mucho auge en nuestro país debido a la necesidad de movimiento que se requiere en la industria, esta tecnología puede ser utilizada junto con los lectores ópticos en el área de la industria en nuestra localidad, para controlar la producción, para determinar exactamente en donde ha habido retrasos y de esa manera poder atacarlos inmediatamente y no detener la producción. Pero también se le puede utilizar en la educación como la implementación de la RED en el ITSA para junto con una laptop pueda ser utilizado principalmente en el edificio y en parte del CAMPUS TECNOLÓGICO para ingresar a la red del ITSA o para disponer del INTERNET.

Como ya se dijo es totalmente factible el crear una red híbrida, porque seguirá teniendo las ventajas de la velocidad que brinda la parte cableada y expandirá las posibilidades con la parte inalámbrica, en este trabajo se observó la implementación de una red híbrida Ethernet, que se puede considerar una de las redes de más uso en el mundo.

Para poder realizar una implementación, se debe dejar lo que ya existe, para poderlo hacer compatible, y crear componentes nuevos o agregarles características a los que ya existen. Para el caso de Ethernet se puede considerar mejor el modo cuasi-difuso con la reflexión activa (por satélites), debido a que el satélite se coloca en la parte alta de la oficina y puede cubrirla toda, así cualquier computadora móvil siempre

tendrá señal de comunicación a la red, siempre que no se salga de la habitación.

5.2 ANÁLISIS DE LOS EQUIPOS EN EL MERCADO.

Luego de un análisis costo beneficio, tomando en consideración las marcas existentes en el mercado de dispositivos inalámbricos como:

3-COM

D-LINK

LINK-SYS

CISCO

US ROBOTICS

Determine que con unos muy buenos resultados de funcionamiento a un costo que permite hacer la inversión de una red inalámbrica en el Instituto Tecnológico Superior Aeronáutico, la mejor opción es la implementación utilizando la marca D-link.

Dentro de el Standard 802.11 se elige el 802.11g como el mejor para nuestros propósitos, principalmente por estar en la banda de 2.4 GHZ, lo que incrementa el alcance, que será la prioridad en el momento de lograr el propósito de enlazar todos los equipos desde todas y cada una de las aulas del edificio del ITSA utilizando uno o máximo dos “access point” por piso ubicados estratégicamente. En cuanto al resto de parámetros, los estándares existentes 802.11 a, 802.11b, 802.11g no existe mayor diferencia, otro de los parámetros que permite tomar la decisión de utilizar 802.11g, es que en esta banda de frecuencia no se necesita tener autorización de ninguna entidad para utilizarla, y por la

velocidad de 54 Mbps, por que la velocidad del 802.11 b esta limitada a 11 Mbps.

5.3 ELECCIÓN DE LOS EQUIPOS A UTILIZAR

En primera instancia se realizan pruebas de cobertura dentro del edificio utilizando un access point y una tarjeta de red inalámbrica PCMCIA en una computadora portátil LAPTOP, con el propósito de tener movilidad tanto con el access point, como con el punto de red y verificar los alcances de los equipos en cada uno de los pisos del edificio,

Se debe mencionar que el access point elegido es de última generación de 54 Mbps de velocidad, que puede incrementar su velocidad a 108 Mbps. Pude comprobar que estos alcances eran muy limitados y la señal existía en los corredores del edificio, pero al ingresar con la portátil en las aulas, la señal se perdía, con lo cual no se lograba el objetivo.

5.4 DETERMINACIÓN DE LAS ANTENAS A UTILIZAR

Debido a los problemas presentados se decidió cambiar de antenas con el fin de incrementar la ganancia, es así que adquirí en primera instancia antenas de 5 db de ganancia y no de 3db, que es con las que originalmente vienen los access point. Se realizaron las mismas pruebas y se tenía una señal mejor sin ser óptima, es decir que al ingresar con el punto de red a las aulas se tenía una intensidad, con la puerta abierta del aula y al cerrar la misma se obtenía una señal, en el rango del access point que tiene los siguientes rangos de captación de señal que son:

Excelente

Muy Bueno

Bueno

Bajo

Muy Bajo

Sin señal

Con el fin de no incrementar los costos y lograr el objetivo decidí construir antenas caseras con muy buenos resultados y a muy bajos costos, las mismas que probé una vez terminada su construcción en los access point ,reemplazando las de 5 db que fueron utilizadas en principio y dieron un alcance de un 30% mayor. Sin embargo estas antenas son direccionales y omnidireccionales que son las que requiere, por lo que se utilizó en estas aplicaciones, y se las dejo para utilizarlas mas adelante.

5.5 EQUIPOS UTILIZADOS

Finalmente se determina que los equipos necesarios son los siguientes:

5.5.1 ACCESS POINT DWL-2000AP+

D-Link AirPlus G+ 2.4GHz Wireless Access Point, 54Mbps (802.11g). (8 x)



Figura 5.1 D-Link AirPlus G+ 2.4GHz

General:

El DWL-2000AP+ es un Access Point Inalámbrico potenciado, perteneciente a la nueva línea AirPlus XtremeG+ de D-Link, que responde al estándar 802.11g, operando a 54Mbps de velocidad y gracias al nuevo Chip de Texas Instruments(tm), puede alcanzar en throuput comparable a los 100Mbps en una red FastEthernet.

El modo de operación 8x-exclusivo de D-Link- le permite alcanzar una velocidad de operación ocho veces más rápida que una red Wireless tradicional de 11Mbps, con un throuput real de 36Mbps aproximadamente.

El DWL-2000AP+ interopera en forma transparente con cualquier producto D-Link Air y D-Link AirPlus, o con cualquier producto de otros vendedores, bajo el estándar 802.11b y por supuesto con el estándar 802.11g. En conjunto con las altas tasas de transferencia, un muy buen nivel de seguridad y cuatro modos de operación, hacen del DWL-2000AP+ la solución ideal para la nueva tecnología, además de proteger las inversiones wireless ya hechas (de haberlas)

El Access Point AirPlusXtremeG DWL-2000AP+ incorpora mecanismos adicionales de seguridad, tales como Wi-Fi(tm) Protected Access (WPA) y 802.1x, que en conjunto con un servidor Radius proporcionan un mayor nivel de Seguridad.

Las principales características y facilidades son las siguientes:

- Velocidad de Transmisión de hasta 88Mbps en modalidad 8 x, en 2.4GHz
- Velocidad de Transmisión de hasta 54Mbps, en 2.4GHz
- Compatible con productos que operen bajo el estándar 802.11b y 802.11g, y la serie b+ de D-Link,
- Cuatro modos de operación. Access Point, Bridge PtP, Bridge PtMP y AP Cliente,
- Seguridad Avanzada, WPA y 802.1x,
- Antena desmontable con conector RSMA,
- Fácil Instalación,
- Alto Rendimiento, y
- Fácil integración en red.

5.5.2 ADAPTADOR DE RED DWL-G650+

[Adaptador de red PCMCIA Inalámbrico Wi-Fi](#)

Conectividad inalámbrica Plus G para notebooks que tiene las características:

- Estándar IEEE.802.11g totalmente compatible con 802.11b.
- Hasta 54Mbps.
- Rendimiento 8x (88Mbps)



Figura 5.2 Adaptador de red PCMCIA Inalámbrico Wi-Fi

Descripción

La tarjeta D-Link AirPlus XtremeG+ DWL-G650+ es un adaptador Wireless PCMCIA de alto rendimiento, perteneciente a la nueva línea AirPlus XtremeG+ de D-Link, que responde al estándar 802.11g, operando a 54Mbps de velocidad y gracias al nuevo Chip de Texas Instruments, puede alcanzar un throughput comparable a los 100Mbps de una red FastEthernet.

El modo de operación 8x-exclusivo de D-Link- le permite alcanzar una velocidad de operación ocho veces más rápida que una red Wireless tradicional de 11Mbps, con un throughput real de 36Mbps aproximadamente.

La DWL-G650+ interopera en forma transparente con cualquier producto D-Link Air y D-Link AirPlus, o con cualquier producto de otros vendedores, bajo los estándares 802.11b y por supuesto con el 802.11g. En conjunto con las altas tasas de transferencia, un muy buen nivel de seguridad hacen de la DWL-G650+ la opción ideal para la nueva tecnología, además de proteger las inversiones wireless ya hechas.

El Adaptador Wireless AirPlusXtremeG DWL-G650+ incorpora mecanismos adicionales de seguridad, tales como Wi-Fi(tm) Protected Access (WPA) y 802.1x, que en conjunto con un servidor Radius proporcionan un mayor nivel de Seguridad.

Las principales características y facilidades son las siguientes:

- Velocidad de Transmisión de hasta 88Mbps en modalidad 8 x, en 2.4GHz
- Velocidad de Transmisión de hasta 54Mbps, en 2.4GHz
- Compatible con productos que operen bajo el estándar 802.11b y 802.11g, y la serie b+ de D-Link,
- Seguridad Avanzada, WPA y 802.1x,
- Antena desmontable con conector RSMA, fácil Instalación,
- Alto Rendimiento, y
- Fácil integración en red.

5.5.3 ADAPTADOR DE RED DWL-G520+

El adaptador D-Link AirPlus G+ 2.4GHz Wireless PCI Adapter, es de 54Mbps para la norma (802.11g). (8 x)



Figura 5. 3 D-Link AirPlus G+ 2.4GHz Wireless

Descripción

La tarjeta D-Link AirPlusXtremeG+ DWL-G520+ es un adaptador Wireless PCI de alto rendimiento, perteneciente a la nueva línea AirPlus XtremeG+ de D-Link, que responde al estándar 802.11g, operando a 54Mbps de velocidad y gracias al nuevo Chip de Texas Instrument, puede alcanzar en throughput comparable a los 100Mbps de una red FastEthernet.

El modo de operación 8x-exclusivo de D-Link, le permite alcanzar una velocidad de operación ocho veces más rápida que una red Wireless tradicional de 11Mbps, con un throughput real de 36Mbps aproximadamente.

La DWL-G520+ interopera en forma transparente con cualquier producto D-Link Air y D-Link AirPlus, o con cualquier producto de otros fabricantes, bajo los estándares 802.11b y por supuesto con el 802.11g. En conjunto con las altas tasas de transferencia, un muy buen nivel de seguridad hacen de la DWL-G520+ la opción ideal para la nueva tecnología, además de proteger las inversiones wireless ya hechas.

El Adaptador Wireless AirPlusXtremeG DWL-G520+ incorpora mecanismos adicionales de seguridad, tales como Wi-Fi(tm) Protected Access (WPA) y 802.1x, que en conjunto con un servidor Radius proporcionan un mayor nivel de Seguridad.

Las principales características y facilidades son las siguientes:

- Velocidad de Transmisión de hasta 88Mbps en modalidad 8 x, en 2.4GHz
- Velocidad de Transmisión de hasta 54Mbps, en 2.4GHz
- Compatible con productos que operen bajo el estándar 802.11b y 802.11g, y la serie b+ de D-Link,

- Seguridad Avanzada, WPA y 802.1x,
- Antena desmontable con conector RSMA, fácil Instalación,
- Alto Rendimiento, y
- Fácil integración en red.

5.5.4 ANTENA DIPOLO DWL-50AT



Figura 5.4 antenna dipole

La antena DWL-50AT es una antena Dipolo de 5 dBi de ganancia con conector SMA reverso. Puede ayudar a mejorar la tasa de transmisión y extender el área de cobertura de los Wireless Access Points o Gateways Residenciales.

Los actuales productos en los que puede ser instalada esta antena es en Internet Server y Gateway para Cable Módem/XDSL módem DI-714.

5.5.5 ANTENA OMNI ANT24-1500

Es una antena externa de 15dBi Omni Antenna compuesta de supresor de transitorios



Figura V.5 Antenna omni

Tabla 5.1 Características técnicas

Tipo de Antena	Omni – Direccional
Tipo de Polarización	Vertical
Rango de Frecuencia	2.4 ~ 2.5 GHz
Ganancia	15dBi
HPBW /horizontal	360°
HPBW /vertical	5°
Impedancia	50 Ohms, +/- 5 ohm
Tipo de conector de la antena	Tipo N (Female)

Tabla 5.2 Características físicas

Dimensión Antena	1600 mm
Peso	750 grs.

5.5.6 ANTENA PANEL DIRECCIONAL ANT24-1800

Directional Panel Ant./18dBi/15deg with surge arrestor



Figura V.6 directional panel antenna

Tabla 5.3 Características técnicas

Tipo de Antena	Pannel - Direccional
Tipo de Polarización	Linear Vertical
Rango de Frecuencia	2.4 ~ 2.5000 GHz
Ganancia	18dBi
HPBW /horizontal	15°
HPBW /vertical	15°
Front to Back ratio	26Db
Downtilt	0°
Impedancia	50 Ohms
Tipo de conector de la antena	Tipo N (Female)
Lightning protection	DC ground

Tabla 5.4 Características físicas

Velocidad de Viento Soportada	180Km/Hr
Temperatura de Operación	-40 a 80°C

Humedad de Oprc.	100% No condensada a 25°C
Dimensión Antena	360 x 360 x16 mm
Peso	3,250Grs.

5.5.7 ANTENA CONSTRUIDA



Figura 5.7 antena construida

5.6 REDES CONFORMADAS

Diagrama de Conexión de la red dentro del edificio

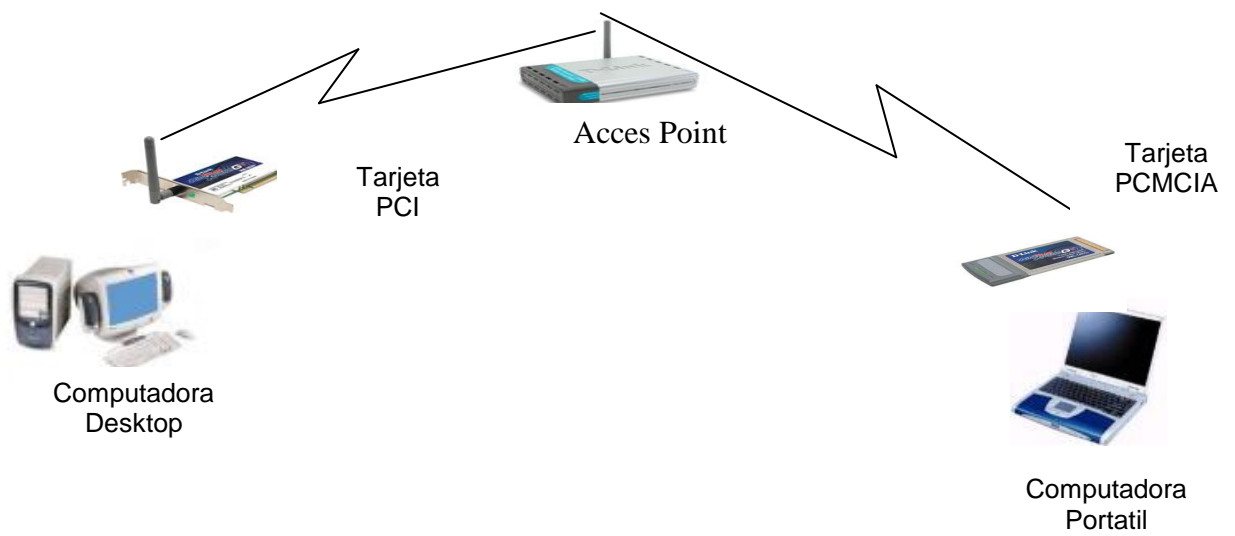


Figura 5.8 Conexión de la red dentro del edificio

Diagrama de conexión de la red

Para unir la red del edificio con otra sección en el ITSA o fuera de él, a donde se quiera extender la RED

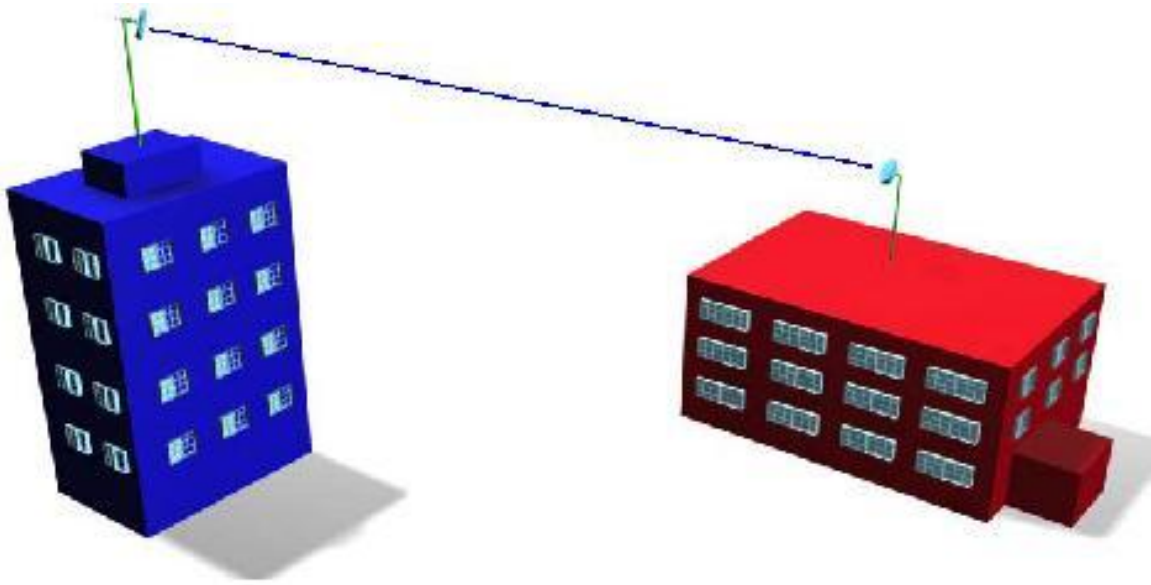


Figura 5.9 Diagrama de conexión entre el ITSA y el Comando del Ala N. 12

Dispositivos que conforman la conexión de la red

Para unir la red del edificio con otra sección en el ITSA o fuera de él, a donde se quiera extender la RED

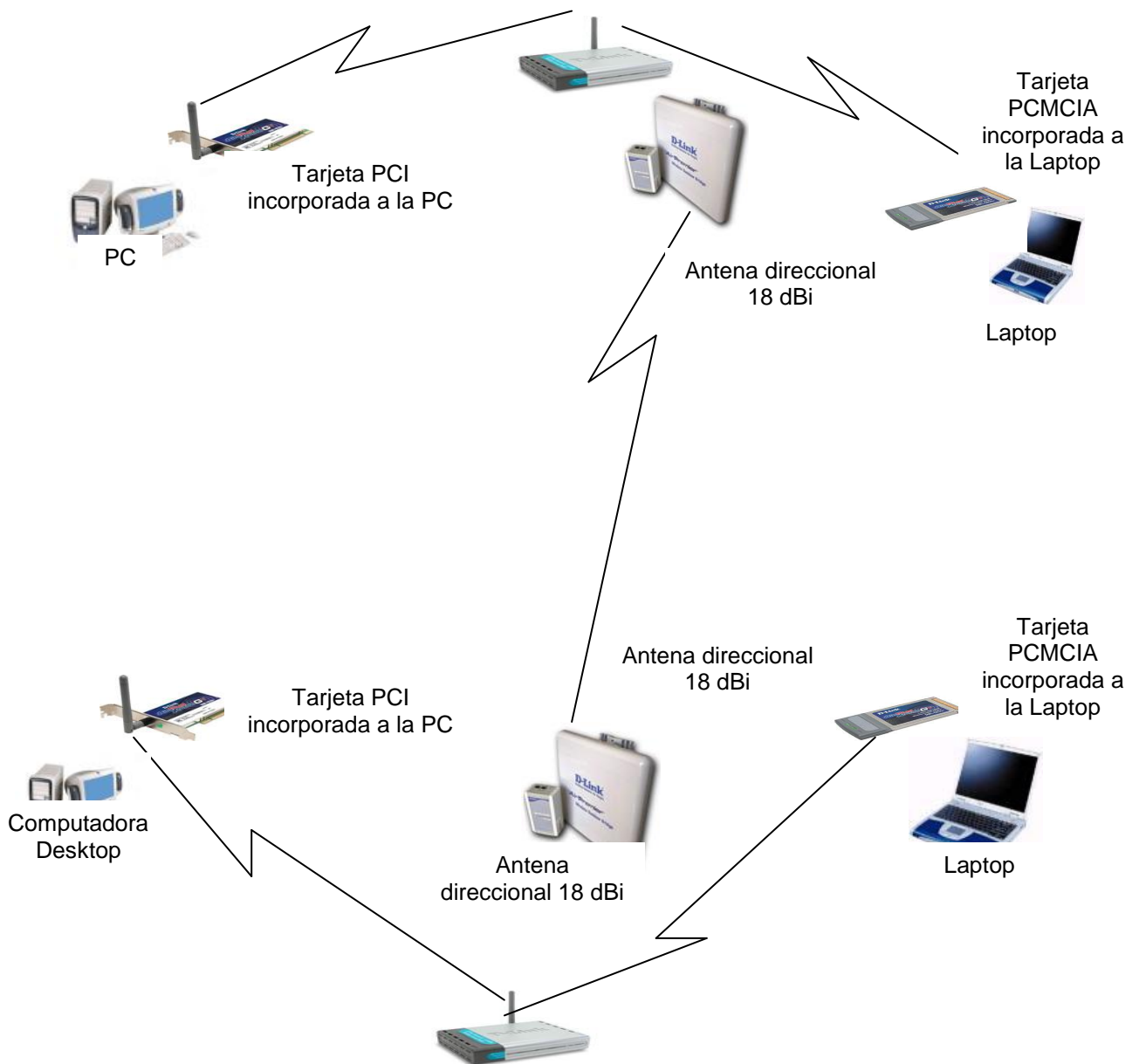


Figura 5.10 Diagrama de conexión entre el ITSA y el Ala N. 12

Diagrama de conexión de la red

Fuera del edificio del ITSA con una antena omnidireccional de 15 dBi para cubrir una área, alrededor del edificio principal

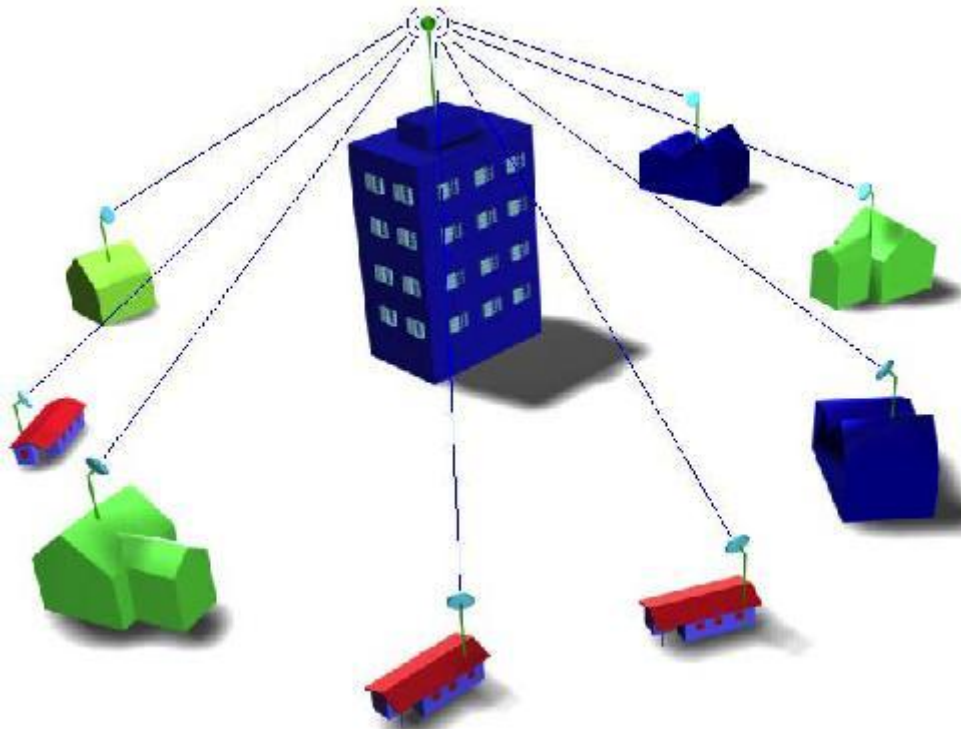


Figura 5.11 Conexión de la red para cubrir una área del Campus tecnológico fuera del edificio principal

Dispositivos que conforman la conexión de la red

Fuera del edificio del ITSA con una antena omnidireccional de 15 dBi para cubrir un área, alrededor del edificio principal

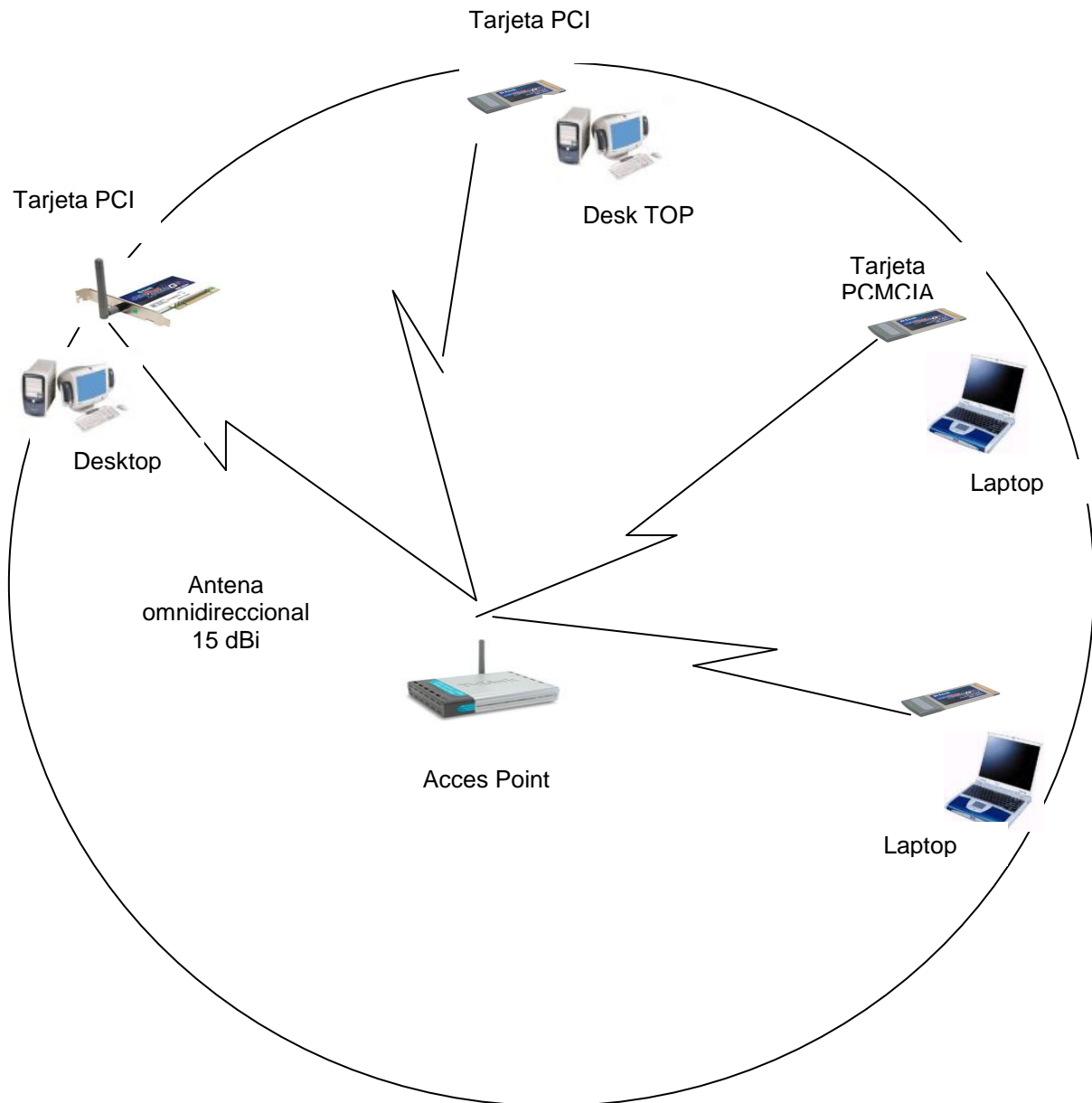


Figura V.12 Conexión de la red para cubrir una área del Campus tecnológico fuera del edificio principal

5.7 CONEXIÓN A INTERNET

Para el caso de TCP/IP el uso de computadoras móviles es interesante pues, por ejemplo, una de las características y requisitos en Internet es que debe tener una dirección de red fija y ésta es almacenada en la tablas de ruteo, para poder encontrar la dirección de una estación cuando se requiere. La computación móvil rompería con este esquema básico de Internet, por eso el estudio del modelo presentado resulta interesante, pues es una propuesta para solucionar el problema ya descrito.

Este modelo en realidad es bastante sencillo y se adapta al modelo Internet existente, se presuponen 3 nuevas entidades para soportar el modelo. Lo interesante es que se debe de generar una nueva red lógica y un Ruteador móvil el cual es el punto más importante del modelo, pues este es el que siempre sabe en donde se encuentra la Estación Móvil, y se encarga de determinar por donde viajará el paquete y determinará que hacer en caso de que la Computadora Móvil no se encuentre en ninguna célula de la red.

Para lograr que este modelo funcione en Internet, se realiza un doble encapsulamiento, el primero es el encapsulamiento normal de Internet en el cual se tiene la dirección de la computadora destino, el segundo encapsulamiento lo realiza el Ruteador Móvil y se tiene como dirección de destino la Estación Base correspondiente a donde se encuentre la Computadora Móvil.

Se integró al trabajo una comparación de características de equipo existente en el mercado, con la finalidad de determinar si este equipo satisface las necesidades de implementación de una red híbrida y se comprobó que sí existen adaptadores y punto de acceso para la instalación de la red.

Se asegura que soporta equipos móviles y el software de Windows reconoce a la computadora móvil y se encarga de sincronizar archivos en transmisiones.

Realizando una profunda comparación de la gama de redes inalámbricas con las LANs cableadas, se llega a la conclusión que ambos sistemas de telecomunicación no son en absoluto excluyentes sino complementarios, ya que es el sistema inalámbrico el que funciona con el usuario final, pero este sistema se basa en los sistemas alámbricos.

Con las redes inalámbricas se ofrece como gran prestación el ahorro del costoso cableado del edificio. Como punto negativo se tiene que comentar el inconveniente de transmitir por un medio que cuenta con interferencias y otros factores no propicios, lo que dificulta poder alcanzar velocidades comparables con las de las redes alámbricas.

En el trabajo realizado se realiza la integración de las dos tecnologías, es decir la tecnología alámbrica y la inalámbrica, de manera que se aplique la que mejor resultado tenga en cada uno de los casos que se presenten.

El sector de las redes inalámbricas necesita de un acuerdo entre las principales empresas de telecomunicaciones para que se unifique un estándar que fructifique en un mercado necesitado de estándares en la materia. Aunque se haya definido el estándar de redes inalámbricas 802.11.

Las redes inalámbricas tomarán buena parte del mercado en un futuro próximo, ya que proporcionan unas ventajas de movilidad y flexibilidad tales, que los usuarios las aceptarán cuando llegue la tecnología estandarizada al mercado, teniendo en cuenta los precios, porque el usuario siempre cuida sus intereses económicos.

CONEXIÓN DE LA RED INALÁMBRICA A LA RED ALÁMBRICA DEL EDIFICIO PARA ACCEDER AL INTERNET

DE: ITSA - LATACUNGA
PARA: ING. JENNY RAZO

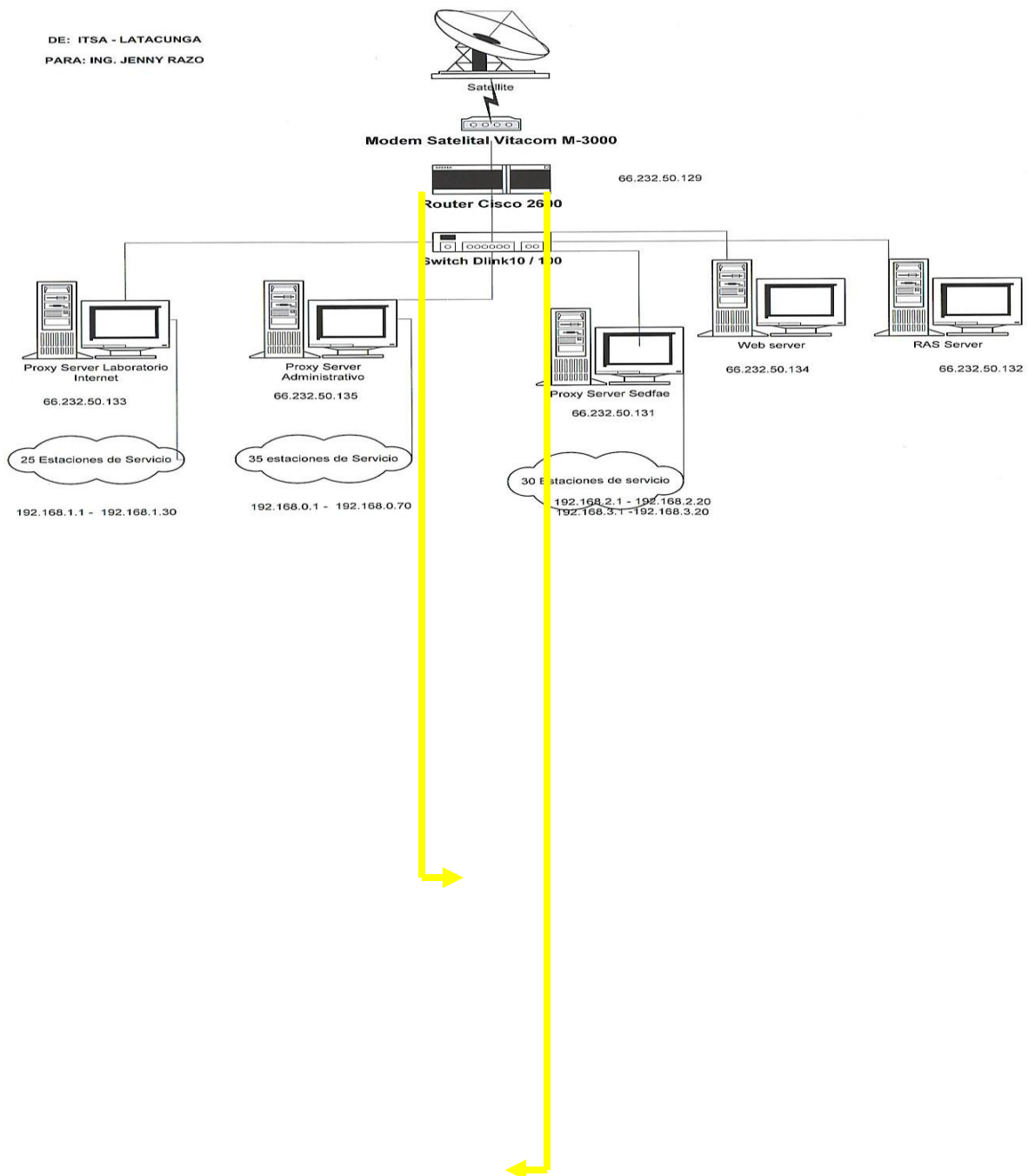




Figura 5.13 conexión de la red inalámbrica a la red del edificio para acceder al Internet

**CONEXIÓN DE LA RED INALÁMBRICA A LA RED ALÁMBRICA
PARA ACCEDER AL INTERNET**

Red Primer Piso

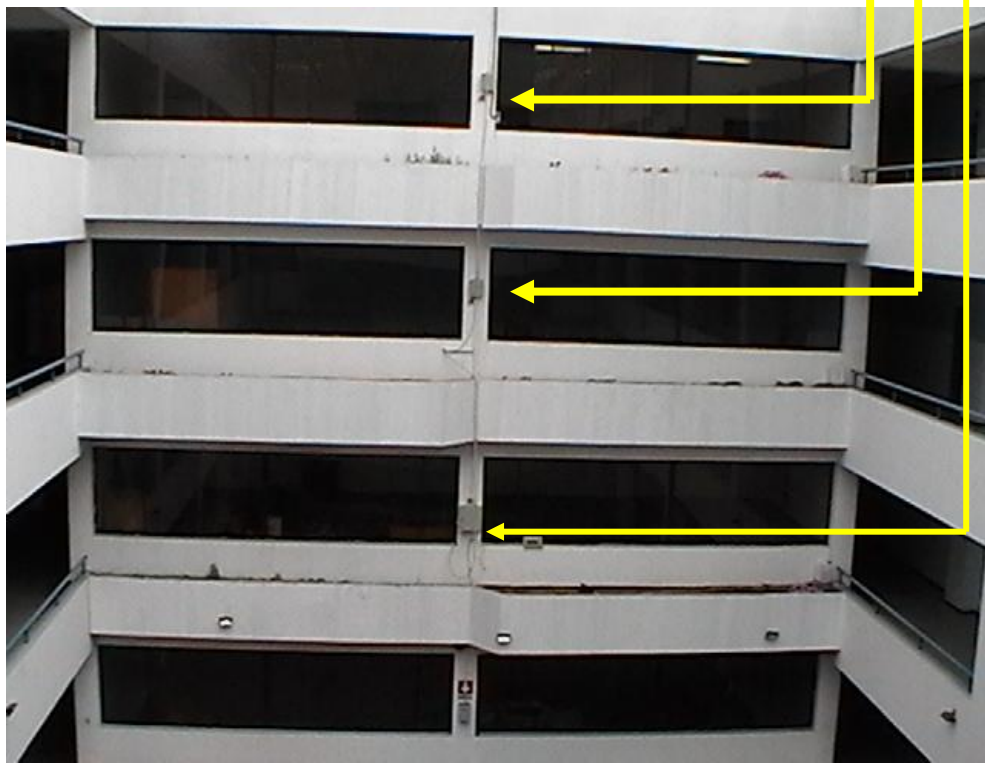
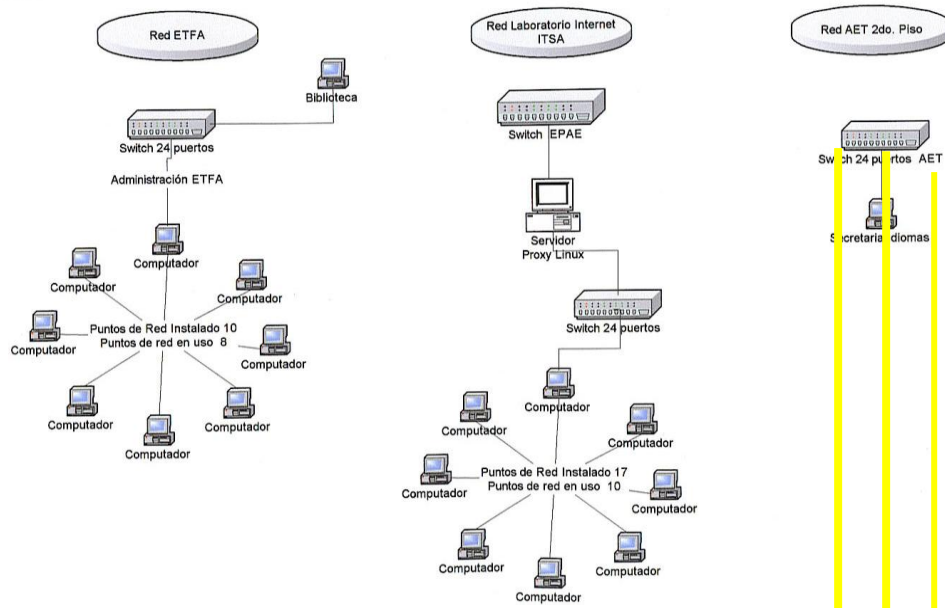


Figura 5.14 conexión de la red inalámbrica a la red alámbrica para acceder al Internet

Red Segundo Piso

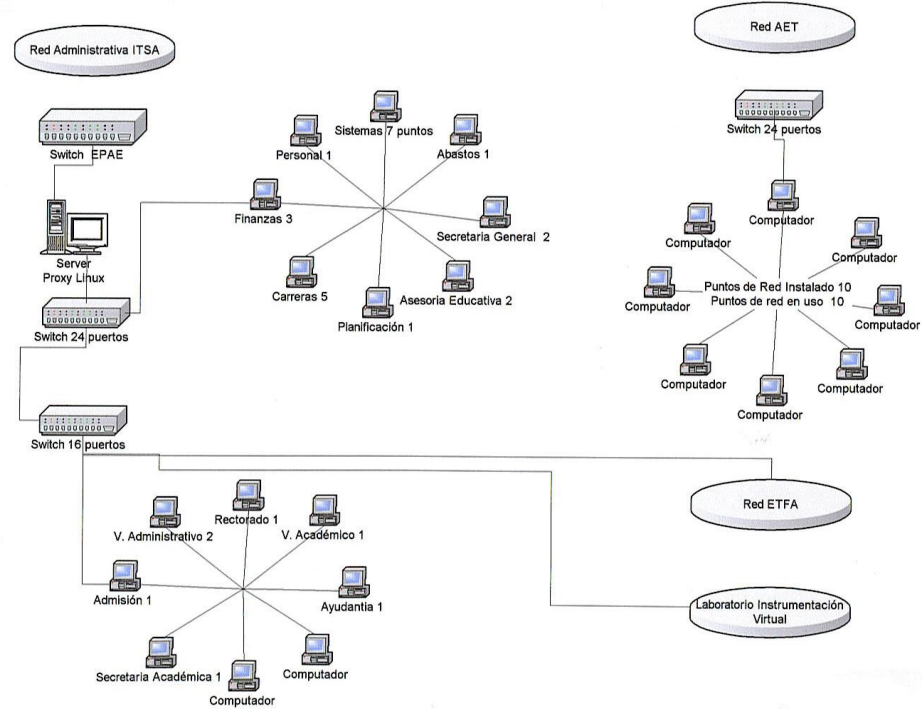


Figura 5.15 Red instalada en el segundo piso del ITSA

Red Tercer Piso

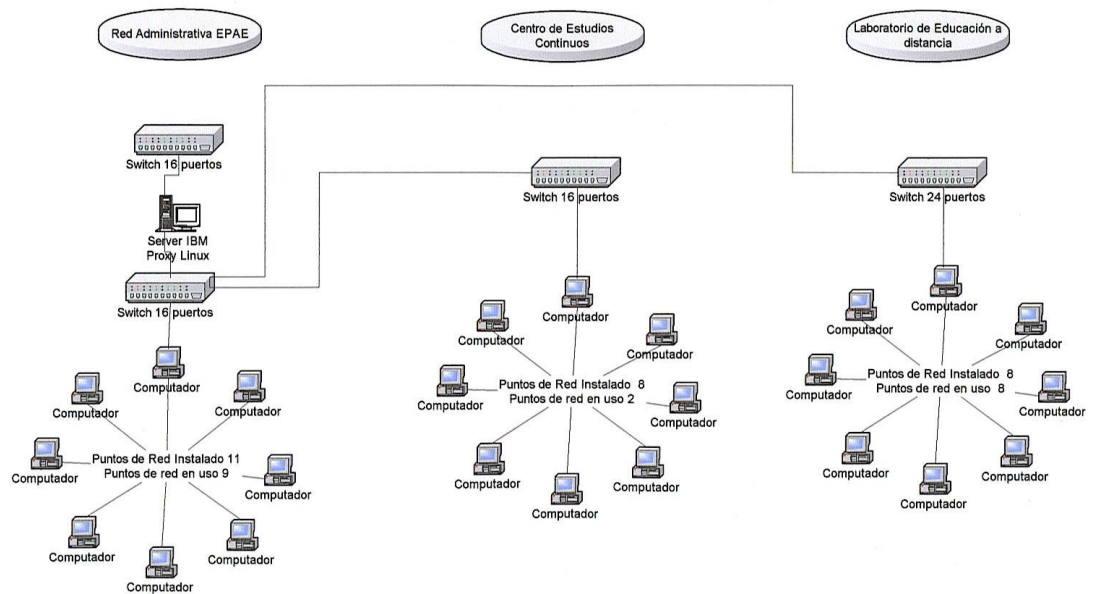


Figura 5.16 Red instalada en el tercer piso del ITSA

Red Laboratorios

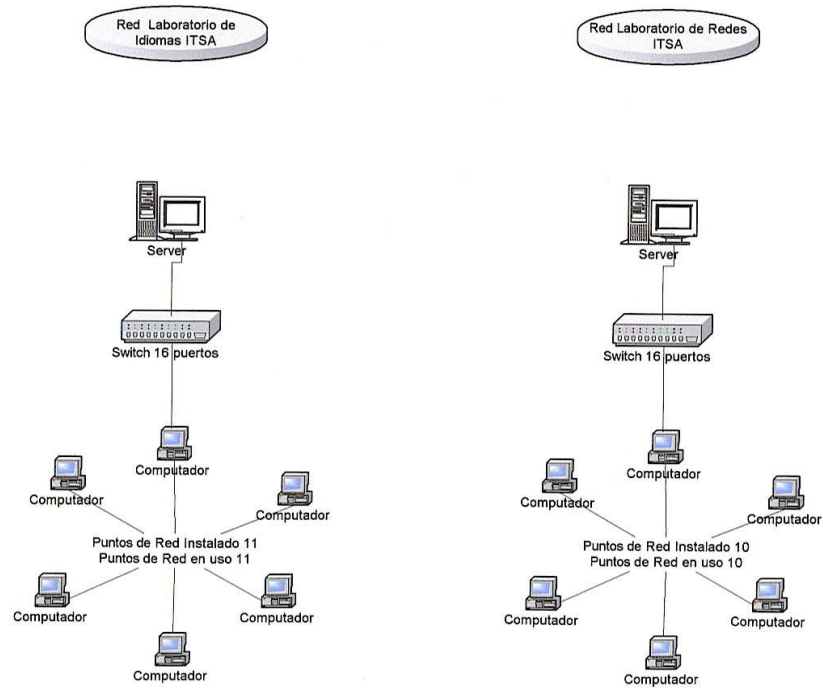


Figura 5.17 Red instalada en los laboratorios del ITSA

Red Planta Baja

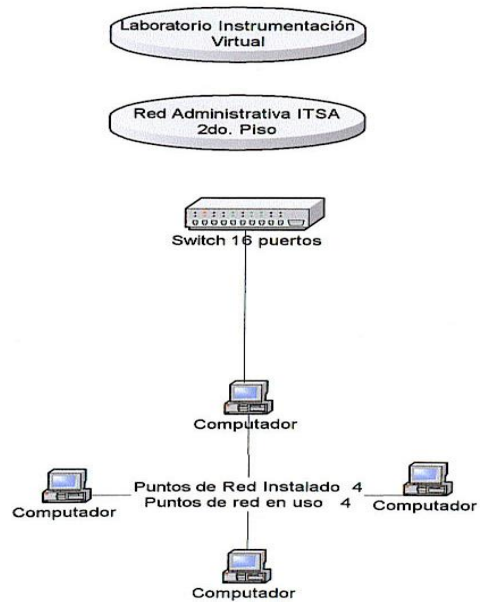


Figura 5.18 Red instalada en la planta baja del ITSA

5.8 IMPLEMENTACIÓN DE LA RED (INSTALACIONES)

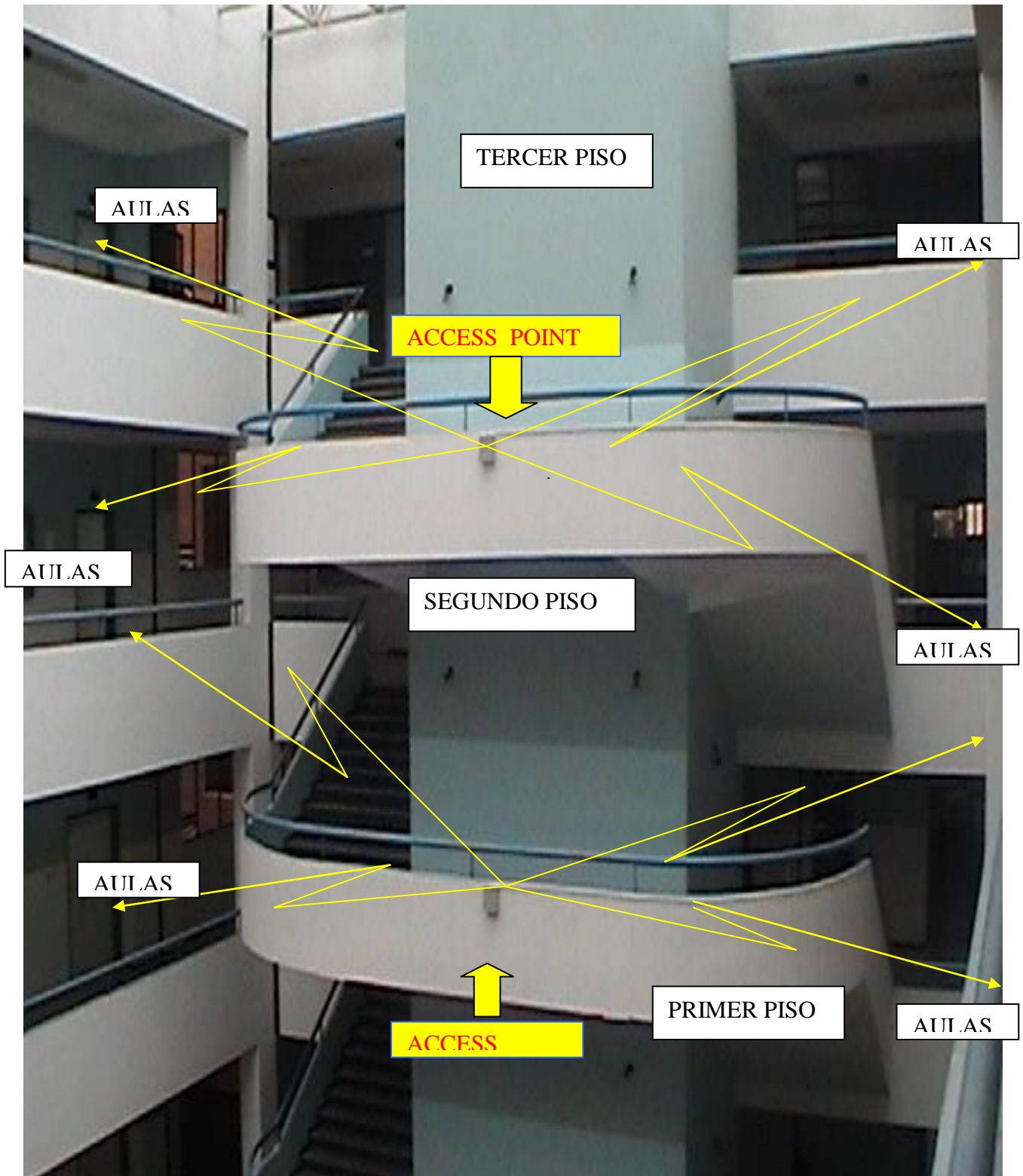


Figura 5.19 implementación de la red en el ITSA (instalaciones)

COBERTURA DE LA RED DENTRO DEL EDIFICIO

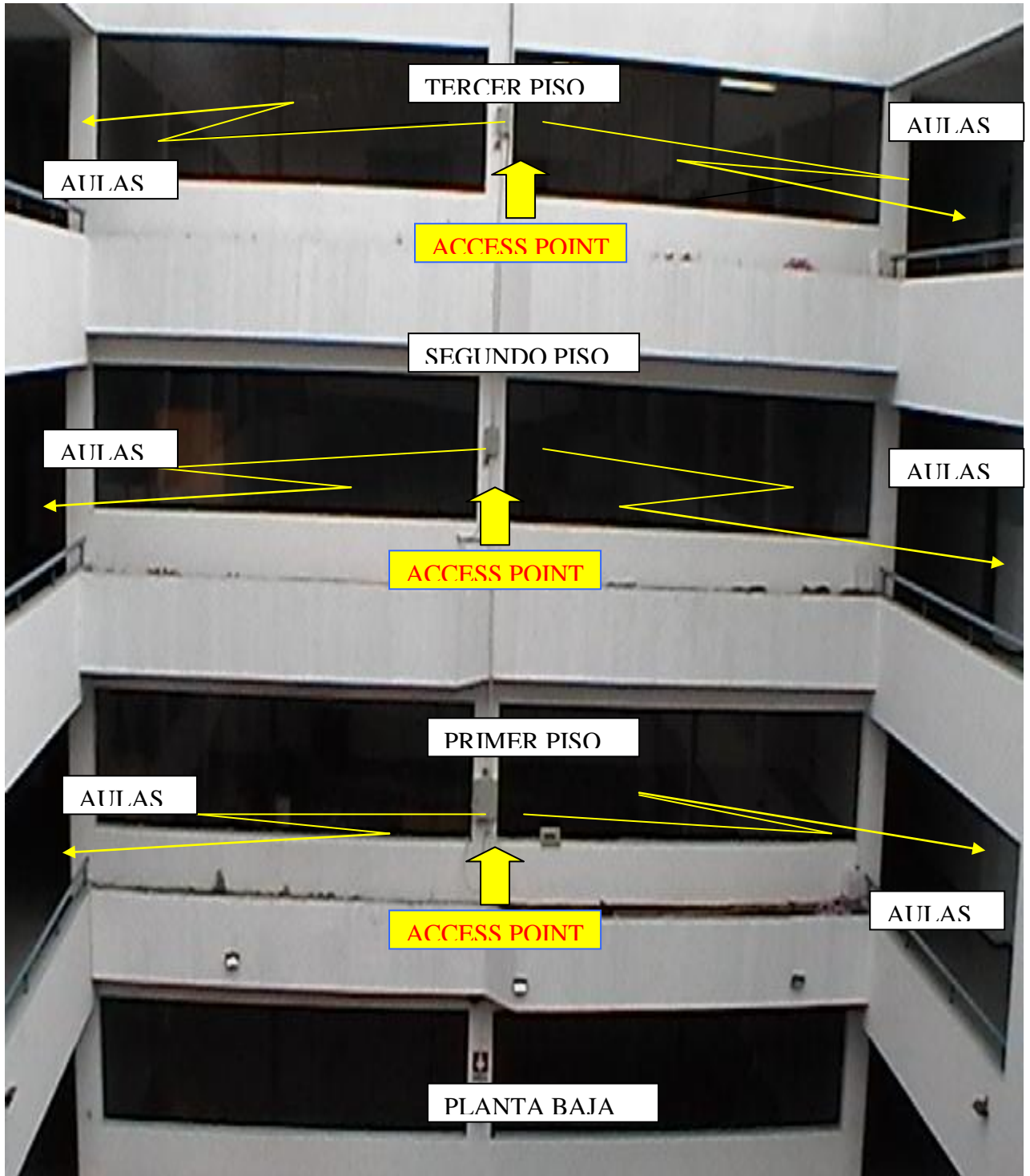


Figura 5.20 cobertura de la red dentro del edificio

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- Se cumplió con el objetivo de este proyecto de tesis.
- la mayoría de comunicaciones telefónicas o informáticas de un futuro próximo se realizarán en algún punto de forma inalámbrica.
- El estándar IEEE 802.11 se basa en el mismo marco de estándares que Ethernet. Esto garantiza un excelente nivel de interoperatividad y asegura una implantación sencilla de las funciones y dispositivos de interconexión Ethernet/WLAN.
- A menudo, las infraestructuras de comunicación basadas en esquemas de cableado tradicionales no son factibles debido a motivos técnicos o económicos. En estos casos, los productos inalámbricos se erigen como alternativas flexibles a las redes cableadas.
- La tecnología inalámbrica también ofrece excelentes soluciones cuando se necesitan instalaciones de red temporales.

- El estándar 802.11 define varios métodos y tecnologías de transmisión para implantaciones de LAN inalámbricas. Este estándar no sólo engloba la tecnología de radiofrecuencia sino también la de infrarrojos. Asimismo, incluye varias técnicas de transmisión como:
 - Modulación por saltos de frecuencia (FHSS)
 - Espectro de extensión de secuencia directa (DSSS)
 - Multiplexación por división en frecuencias octogonales (OFDM)
- Todos los productos electrónicos del mercado deben cumplir con unas normativas rigurosas sobre radiación electromagnética. Los organismos de estandarización nacionales, europeos e internacionales establecen las normativas con detalle para asegurar que las tecnologías inalámbricas no tengan consecuencias negativas sobre los diversos sistemas que utilizan tecnología de radiofrecuencia (RF). Los productos WLAN cumplen con estos estándares de seguridad y con las normativas de compatibilidad electromagnética (EMC).
- Los productos de red inalámbrica son seguros no sólo respecto a otros productos electrónicos y de red, sino, lo que es más importante, respecto a las personas. Los productos de redes inalámbricas, estandarizados como IEEE 802.11, se han diseñado para usarse en oficinas y otros lugares de trabajo. Por lo tanto, emiten un grado reducido de energía, lo cual es inofensivo.
- Las funciones de la capa MAC IEEE 802.11 no sólo gestionan y coordinan el acceso al canal de transmisión, sino que hasta cierto punto se encargan de la autenticación y otras tareas de administración y seguridad.
- Para implantar redes o infraestructuras LAN inalámbricas es imprescindible realizar un trabajo de planificación y diseño previo. Hay que plantearse una serie de preguntas y tomar las decisiones en función de las respuestas dadas:

1. ¿Qué tipo de topología de red debe implantarse (red ad-hoc o estructural)?

2. ¿Cuál es la ubicación ideal de los puntos de acceso ?

3. ¿Qué frecuencias deben utilizar ?

4. ¿Cómo puede garantizarse un nivel de seguridad adecuado en las LAN inalámbricas?

- El estándar IEEE 802.11 describe los protocolos y las técnicas de transmisión correspondientes a los dos modos principales de construir y utilizar una LAN inalámbrica RF.
- Los puntos de acceso son componentes de red que controlan y gestionan toda la comunicación que se produce dentro de una célula LAN inalámbrica, entre células LAN inalámbricas y, finalmente, entre células LAN inalámbricas y otras tecnologías LAN, Los puntos de acceso garantizan un empleo óptimo del tiempo de transmisión disponible en la red inalámbrica.
- Si se ha configurado la encriptación WEP, el sistema móvil debe utilizar la misma clave que los puntos de acceso
- Con la repetición, un punto de acceso puede reemitir la señal inalámbrica de un PA a otro.
- Según las distancias que la conexión inalámbrica tenga que enlazar mediante bridge y las condiciones ambientales concretas, será necesario uno u otro tipo de antena. Las antenas especiales de alta ganancia, universales, de punto a punto y de punto a multipunto constituyen la solución idónea para las aplicaciones que deben cubrir grandes distancias o penetrar estructuras.
- Los productos WLAN utilizan una técnica de transmisión denominada DSSS (Modulación por saltos de frecuencia). DSSS se diseñó especialmente para garantizar las transmisiones, que con esta técnica son seguras, sólidas y menos propensas a las interferencias.
- La tecnología inalámbrica basada en transmisiones por RF puede considerarse segura y no es particularmente vulnerable a las

“escuchas” (datos importantes espiados por personas no autorizadas) si se han implantado y configurado correctamente las funciones de seguridad disponibles.

- IEEE 802.11 también describe el uso de otros mecanismos para mejorar la seguridad mediante métodos de autorización y encriptación. La WEP (Wired Equivalent Privacy), por ejemplo, es una técnica de encriptación adicional basada en el algoritmo RC4. Estándares nuevos, como el IEEE 802.11i (antes WEP2), pueden proporcionar niveles de seguridad todavía más altos. La implantación de éstos y de otros métodos de autorización y encriptación garantizan que la seguridad en las redes WLAN sea igual o incluso superior a la de las tecnologías LAN convencionales.
- Si los clientes desean niveles de seguridad todavía más altos, se pueden añadir mecanismos y soluciones suplementarias. Algunas de estas soluciones pueden ser programas de autorización, redes VPN o grandes sistemas de firewall.
- La identificación SSID (Service Set ID) podría considerarse el nombre de la red inalámbrica.
- Para disponer de un buen grado de seguridad es aconsejable elegir SSID difíciles de adivinar,
- Los productos IEEE 802.11g poseen un alto grado de compatibilidad con versiones anteriores (con productos ajustados a IEEE 802.11 e IEEE 802.11b) y todavía utilizan la banda de frecuencia ISM (2,4 GHz). Eso significa también que las distancias de transmisión de los productos 802.11b y 802.11g son más o menos las mismas.
- Asimismo, deben hacerse algunas transacciones en cuanto a compatibilidad y alcance. Como los estándares 802.11a y 802.11b operan en bandas de frecuencia distintas, los productos no son compatibles.
- La frecuencia de funcionamiento más alta del estándar 802.11a tiene como consecuencia un alcance relativamente más corto. Se necesitarán más puntos de acceso 802.11a para cubrir la misma zona. Pero incluso con estos inconvenientes, las pruebas iniciales

demuestran que los productos 802.11a ofrecen un rendimiento casi tres veces superior al de los 802.11b en cuanto a alcances en interiores.

- El estándar IEEE 802.11g alcanza velocidades más altas y es compatible con los equipos 802.11b ya existentes. El 802.11g opera en la misma banda de frecuencia de 2,4 GHz y con los mismos tipos de modulación DSSS que el 802.11b a velocidades de hasta 11 Mbps, mientras que a velocidades superiores utiliza tipos de modulación OFDM más eficientes.
- La compatibilidad con versiones anteriores protege la inversión de los clientes en varios aspectos. Una tarjeta de interfaz de red IEEE 802.11g, por ejemplo, puede funcionar con un punto de acceso 802.11b y viceversa, a velocidades de hasta 11 Mbps.
- El principal mecanismo para compartir canales en el sistema 802.11 es CSMA/CA. Para que este método funcione, cada radio debe ser capaz de detectar a todas las demás radios asociadas al mismo punto de acceso (incluido, obviamente, el propio PA).
- Todos los clientes y puntos de acceso 802.11g deben ser capaces de retroceder y operar exactamente como un dispositivo 802.11b heredado. De esta forma, la migración a la tecnología 802.11g es fácil y dinámica.
- Aunque OFDM sea una tecnología excelente para las aplicaciones WLAN de interior, las leyes de la física indican que el alcance de la comunicación es proporcional a la longitud de onda. En otras palabras, los objetos dispersan y atenúan la energía de radiofrecuencia de un modo más eficaz cuanto más alta sea la frecuencia utilizada.
- En un espacio abierto, las diferencias de propagación no deberían suponer ningún problema. Sin embargo, la mayoría de sistemas WLAN funcionan en interiores, donde los espacios abiertos son limitados y casi todas las señales de radio tiene que atravesar paredes, mobiliario y otros obstáculos.

- Los equipos IEEE 802.11a alcanzan velocidades de datos más altas en alcances cortos o, como en el ejemplo, en un vestíbulo donde es posible la propagación por un espacio abierto. No obstante, la velocidad de los datos disminuye rápidamente cuando la señal debe atravesar paredes y otros obstáculos.

6.2 RECOMENDACIONES

- Cuando se utilice las computadoras portátiles en el interior del edificio es preferible hacerlo manteniendo en lo posible línea de vista con los access points.
- Cuando se utilice las computadoras dentro de las aulas es más conveniente hacerlo con la puerta del aula abierta para garantizar un mejor enlace.
- El enlace entre el Instituto Tecnológico Superior Aeronáutico y el Ala No 12 se debe utilizar con el fin de disponer de LOTUS NOTES en el ITSA e ingresar a la red de la Fuerza Aérea.
- Considerar las debidas seguridades en la red.
- Se debe contratar un servicio de Internet solo para la red inalámbrica para dar mayor agilidad en el uso, ya que se puede congestionar la red del ITSA.
- Si la demanda de la red inalámbrica se incrementa, se debería ampliar, implementando más access points hacia el sitio de mayor demanda.

- Se debe cobrar un valor módico a los usuarios de la red que permita realizar el mantenimiento permanente de la red.
- Las tarjetas de red que fueron adquiridas por el instituto como parte de este proyecto se debe entregar en base a un estudio de las prioridades de requerimiento a quienes dispongan computadoras portátiles y las tarjetas de PC se las entregue al departamento de informática para que se implemente la red de acuerdo a las necesidades.
- Que se entregue este proyecto al departamento de informática para que se administre la red.

GLOSARIO

ASCII

El protocolo ASCII es un protocolo de 7 [bits](#) que consiste en 128 caracteres que hacen el alfabeto (en minúsculas y mayúsculas), números, caracteres que están en el teclado estándar y ciertos caracteres especiales de control.

ARIB e HISWANa:

BAUDIOS

Es el número de cambios de frecuencia ocurridos en un segundo.

Barker con TRS/CTS: (Request To Send / Clear To Send)

Broadcast: Un solo canal de comunicación compartido por todas las máquinas

BITS DE DATOS

Los sistemas de comunicación utilizan 7 u 8 bits para representar un paquete de datos (La cual es mensaje o grupo de datos de longitud fija).

BITS DE PARO

Cada paquete de datos utiliza un solo bit como carácter de comienzo en un paquete y entre uno y dos bits para marcar el fin de un paquete.

BITS POR SEGUNDO

Es la cantidad de bits que puede transmitir un dispositivo durante un segundo (Esta unidad de medida es más adecuada para medir la velocidad de un modem que [baudios](#)).

Buffers Memory Address: espacios de memoria dejado entre la entrada y la salida de datos del puerto

BS estación base. (base station.)

CONTROL DE FLUJO

Es el proceso de decirle a cada computadora que deje de enviar datos y comience a transmitir otra vez. En la facultad de ingeniería se utiliza el [XON/XOFF](#) como control de flujo y [ASCII](#) como protocolo.

COMPRESIÓN DE DATOS

La compresión de datos consiste en hacer que los archivos de datos ocupen menos espacio de almacenamiento con técnicas de reescritura de bits sin que éstos pierdan su contenido cualitativo.

CSMA/CD sensor de medio de acceso múltiple/con detección de colisión. (carrier sense multiple access /collision detect.)

CP señal de presencia de colisión. (collision presence.)

CSMA/CA: (Carrier Sense Multiple Access with Collision Avoidance).

DOS sistema operativo de disco. (disk operating system.)

DLL capa de enlace de datos. (data link layer.)

Direct Memory Request Line: (DMA): Es una dirección fija de la memoria RAM

DNS (Domain Name Server)

El servicio del Servidor de Nombres se encarga de convertir direcciones [IP](#) a una máquina con dominio de red (por ejemplo si usted le hace un telnet a mozart.ing.ula.ve en realidad se está comunicando con la máquina 150.185.146.1). El DNS es muy útil ya que le permite entre otras cosas utilizar "nombres de máquinas" en vez de direcciones IP.

DSSST: Tecnología de espectro ensanchado de secuencia directa

DBPSK: (Differential Binary Phase Shift Keying)

Driver: manejador o controlador

DIRECCIÓN IP

Es un conjunto de cuatro grupos de 8 bits cada uno (para un total de 32 bits) asignados de manera tal que cada máquina tiene una identificación única dentro de la red Internet.

Ethernet : Los recursos utilizados por una tarjeta

FTP (Protocolo de transferencia de archivos)

El ftp (file transfer protocol) es un servicio que le permite intercambiar archivos entre máquinas que están conectadas a Internet, utilizando el protocolo tcp/ip; sin embargo debido a que los servidores ftp son muy numerosos, encontrar el archivo entre miles de estos puede ser una ardua tarea. para realizar una búsqueda de cuales servidores tienen un determinado archivo puede utilizar un servidor [Archie](#) o [World Wide Web](#), los cuales le dirán en que lugar está (después solo deberá conectarse a dicho servidor para traerse el archivo).

FHSST: Tecnología de espectro ensanchado de saltos de frecuencia

Gateways: son computadores que pueden traducir entre formatos incompatibles.

Hardware: medios físicos

HANDSHAKE (Apretón de manos)

Es la manera en como dos modems se envían datos para intercambiar información.

HOST: se encuentran conectados a subredes de comunicaciones

IEEE instituto de ingenieros eléctricos y electrónicos. (Institute of Electrical and Electronics Engineers.)

ISM bandas de aplicaciones industriales, científicas y médicas. (bands industrial, scientific and medical.)

(ISA, EISA, PCI, PCMCIA): tipos de bus

Input/output Port Address: Puerto de Dirección de entrada/salida

Interrupt Request Line: Solicitud de Interrupción

IRQ

IRQ son las iniciales de *Interrupt Request* (Petición de interrupción). Este método lo utilizan los dispositivos cuando necesitan la atención del CPU (Unidad Central de Procesos, el corazón de la máquina).

JAM señal de presencia de colisión.

Jumpers: piezas que según su posición y existencia permiten la configuración de un dispositivo

KBPS kilo bits por segundo.

LAN local area network: 10 m a 1 km o más

LLC control de enlace lógico. (logic link control.)

MAN metropolitan area network: 10 km

Mainframe. grandes computadores

Megabits: un megabit es 1.000.000 bits

MODEM

Es un puente entre señales digitales y señales analógicas. El convierte los *altos y bajos* de una señal digital en una señal analógica al variar, o modular, la frecuencia de una onda eléctrica, un proceso similar al utilizado por las estaciones FM de radio.

Netscape y Microsoft: son las interfaces Internet

OSI interconexión de sistemas abiertos. (open system interconnection.)

OFDM: modulación que es la óptima para este estándar

packet-switched: paquetes ruteados

PARIDAD

Como una forma de corrección de error, los dos sistemas conectados pueden convenir en usar paridad par, paridad impar o sin paridad. Si se ponen de acuerdo en usar algún tipo de paridad entonces los sistemas suman los [bits](#) contenidos en el carácter y entonces le suman otro bit llamado el bit de paridad. Este puede contener un 1 o un 0, dependiendo de los que se necesite, para hacer un número total ya sea par o impar, dependiendo de lo que los sistemas hayan acordado.

Point-to-point: Muchas conexiones entre pares individuales de máquinas

ptr: punto de terminación de red

Plug and Play : librerías de auto configuración

PROM: Memoria programada de solo lectura

PMA conexión al medio físico. (physical medium attachment.)

PUERTO SERIAL COM

Puerta de entrada y salida que permite la transmisión y recepción de datos en serie.

PPP (Protocolo de Punto a Punto)

El significado de estas siglas es Point to Point Protocol. es el estándar oficial de Internet para la transmisión de paquetes por una línea síncrona o asíncrona. Este protocolo está diseñado para enlaces simples que transportan paquetes entre dos máquinas. PPP incluye una serie de características como :disca bajo demanda, redisca si esta ocupado,

uso de más de un protocolo de capa de red, negociación de opciones, etc.

RAM memoria de acceso aleatorio. (random access memory.)

software: medios lógicos

store-and-forward: guardar y reenviar

S.C.T. secretaria de comunicaciones y transporte.

SCRIPTS

Scripts son programas miniaturas dentro de un programa, los cuales pueden automatizar sus sesiones en línea y otras tareas. Un script propiamente programado puede llamar a un Boletín electrónico o BBS, entrar en él, buscar todo su correo y salirse.

TCP/IP protocolo de control de transmisión/protocolo internet. (transmission control protocol/internet protocolo.)

UDP protocolo de datagrama de usuario. (user datagrama protocolo.)

WAN: wide area network: 100 km a 1.000 km

web: unos cuantos centenares de miles de usuarios

Windows, Macintosh, IBM OS/2, Unix: plataformas informáticas

Wintel (Windows/Intel): aplicaciones que residen en sistemas

WWW: las empresas vienen usando y adaptando la tecnología Internet

XON/XONFF

Es un control de flujo de software que implica el envío de códigos especiales de control como parte de los datos. Es usualmente necesario para las transferencias [ASCII](#).

BIBLIOGRAFÍA:

- COMUNICACIONES INALÁMBRICAS David Roldan Martínez
- COMUNICACIONES Y REDES DE COMPUTADORES William Stallings
- DOCUMENTO IEEE "Redes Híbridas" pag 21-26
1992 Universidad de Aveiro, Portugal
Rui T. Valadas, Adriano C. Moreira, A.M. de Oliveira Duarte.
- DOCUMENTO IEEE "Ruteando con TCP/IP" pag 7-12
1992 IBM T.J. Watson Reserach Center Charles E. Perkins.
- DOCUMENTO IEEE "Características de una Radio LAN" pag 14-19
1992 LACE Inc. Chandos A. Rypinski.
- HACKING WIRELESS SEGURIDAD DE REDES INALÁMBRICAS
Andrew A. Vladimirov
- INTRODUCCIÓN A LAS REDES INALÁMBRICAS Adam Engst
Glenn Fleishman
- MANUAL DE REDES INALÁMBRICAS Bruce Alexander
- WIRELESS LOS MEJORES TRUCOS Rob Flickenger
- WI-FI Cómo construir una red inalámbrica José A. Carballar

Paginas web:

- www.monografias.com/trabajos/redesinalam/redesinalam.shtml - 101k - 25 Jul 2005 –
- www.monografias.com/trabajos12/reina/reina.shtml - 101k - 25 Jul 2005
- www.microsoft.com/latam/windowsxp/pro/biblioteca/planning/wirelesslan/intro.asp - 37k
- www.microsoft.com/latam/technet/articulos/windowsxp/2008/default.asp - 45k
- www.mercadolibre.com.ar/jm/search?as_categ_id=1709 - 97k –
- www.mailxmail.com/curso/informatica/wifi - 15k - 25 Jul 2005
- www.maestrosdelweb.com/editorial/redeswlan/ - 35k
- www.20minutos.es/noticia/10373/0/inalambrico/internet/cables/ - 35k
- www.ltn.net/T/Idioma/Español/Computadoras/Redes/ - 15k –
- www.itlp.edu.mx/publica/tutoriales/redes/ - 1k
- www.monografias.com/Computacion/Redes/ - 28k - 25 Jul 2005
- www.monografias.com/trabajos18/redes-computadoras/redes-computadoras.shtml - 93k
- www.redes.upv.es/ - 7k - 25 Jul 2005

Latacunga, agosto del 2005

.....
Patricio Espín
CI. 1706487756

.....
Ing. Nancy Guerrón Paredes

DIRECTORA DE CARRERA DE ELECTRONICA

.....
Ab. Eduardo Vasquez

SECRETARIO ACADEMICO