UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

CONEXIÓN INALAMBRICA A ZONAS DE DIFÍCIL ACCESO

T E S I S

Para Obtener el Título de:

INGENIERO EN COMPUTACIÓN

Presentan:

Martínez Herrera Rodrigo
Mendoza Yáñez Moises

Director de Tesis: M.C. María Jaquelina López Barrientos

AGRADECIMIENTOS

Moises Mendoza Yáñez

A mis Padres (Dámaso y Mary): Gracias padres por elegirme para estar en este mundo a su lado, por su comprensión, amor y lección de vida, por ayudarme a ser lo que soy y mostrarme cómo se llega al triunfo, esta meta que logro y las demás se las dedicare a mis padres, gracias nuevamente padres mi amor infinito para ustedes.

A mis hermanos (Luisa, Rosa, Toña, Silvia, Carmen, Toño, Pedro, Cocoy, Mario, Abraham y Monse): A todos y cada uno les agradezco permitirme ser parte de ustedes, gracias por sus múltiples consejos y enseñanzas, gracias por su apoyo incondicional, gracias por su tiempo, gracias por estar conmigo en las buenas y en las malas, pero sobre todas las cosas gracias por ser mis hermanos, los admiro y amo.

A mis sobrinos (Carlos, Pamela, Diana, Toñin, Sofi, Jaque, Rodrigo, Fany, Luís, Karen, Mary Fer, Xadani, Emmanuel, Emilio y Federico): Gracias a mis niños por que fueron parte de mi inspiración para lograr esta meta ya que su alegría me dio ánimos para seguir adelante a lo largo de mi carrera, a ustedes mis ñiños los amo.

A mis amigos (Rodrigo, Carlos, Alfredo, Jesús, Nallely, Porras y Lalo): Por estar a mi lado y apoyarme incondicionalmente, por dejarme entrar en sus vidas y compartirlas conmigo, a ustedes amigos gracias.

A la señora Silvia mamá de Rodrigo y a toda su familia por aceptarme como uno más de ustedes gracias, los quiero.

A mi directora y asesora de tesis Jaquelina por apoyarnos en nuestro trabajo, guiarnos y llevarnos hasta el final de la mano gracias.

Rodrigo Martínez Herrera

A mi Abuela (Rosario) y a mi Madre (Silvia): Gracias por enseñarme a vivir cada día, por inculcarme los principios y valores que han hecho de mí una persona independiente y autónoma, por su amor y comprensión y la paciencia que me han dedicado, nada de esto hubiera sido posible sin ustedes. Todo mi amor para ustedes.

A mis hermanos (Norma y Juan Carlos): Les agradezco toda su disposición para poder hacer de nuestra familia una fortaleza impenetrable, los amo.

A mi sobrina (Hanna): Gracias a mi pequeñita que me mostró cuan simple puede ser la vida para sentir alegría en los momentos más difíciles, te adoro pequeña.

A mis tíos y primos (Antonio, Ángel, Ismael, Rubén, Eloisa, Zeferino, Edith, Arturo, Ismael, Oscar, Daniel, Ismael, Gerardo, Osvaldo, Iván, Cesar, David, Sol y Chayo), gracias por ser esa gran familia apoyadora.

A mis amigos (Moy, Porras, Lalo, Jesús, Ana, Lourdes, Marcos, Luís, Gustavo, Josué, Loyda, Mele, Fabián, Anabel, Claudia, Israel, Toño y Luís): Por hacerme sentir que la vida no se compone de un solo momento, por compartir cada momento vivido a su lado, gracias amigos.

A nuestra directora y asesora de tesis Jaquelina por enseñarnos que vale la pena el esfuerzo y la paciencia para conseguir las metas deseadas.

ÍNDICE

Páginas

PRÓLOGO

En estos tiempos donde las comunicaciones juegan un papel de suma importancia en el desarrollo de un país y de las personas que lo habitan, he aquí el esbozo de una tesis que primordialmente está enfocada a la computación y las comunicaciones, donde podemos ver uno de tantos problemas cotidianos a los que los ingenieros en computación se pueden enfrentar como es la incomunicación de ciertas áreas geográficas.

Tenemos un lugar sin servicio de Internet de banda ancha, debido a la lejanía de las centrales Telmex (Teléfonos de México) que podrían dotar de servicio a dicho lugar. El radio aproximado de cobertura de una central es de 3km, y se tienen 3 centrales triangulando el sitio que necesita el servicio, dos de ellas ubicadas hacia el sur oeste y sur este con una distancia entre 4 y 3.5km respectivamente, y la tercera ubicada al norte a 3km de distancia que da un servicio muy breve y de mala calidad, debido al recorrido de las líneas telefónicas que deben hacer a lo largo de las calles perpendiculares a la Avenida Aztecas, provocando que la señal sufra de ruido y de una atenuación muy significativa en la transmisión y recepción de datos, no afectando en gran magnitud a la señal de voz.

El problema de algunos servicios en este caso Internet se ve limitado en ciertas zonas de nuestra ciudad (México DF) al darnos cuenta nosotros los realizadores de esta tesis que teníamos un problema con este servicio y que el problema se podía resolver ingeniando algún tipo de enlace. ¿Este tipo de enlace cómo sería? si tenemos en cuenta que estas grandes empresas llámese TELMEX y CABLE no tenían cubierta esta zona y por lo tanto no tenían el servicio de Internet y para solicitarlo se gastaría mucho, así que, pensamos en otras alternativas. En la búsqueda de estas alternativas nos encontramos con algo muy interesante y que podríamos hasta comentarlo como una “innovación” llamada wifi o tecnología wireless, esta tecnología vino a resolver muchas de las dudas

que teníamos acerca del enlace entre dos puntos remotos para poder compartir Internet sin necesidad de un cableado de punto a punto, lo mencionamos como interesante ya que nos metimos al área de telecomunicaciones esto es, construir antenas y por medio de éstas antenas y otros dispositivos lograr dicho enlace.

En la puesta de dispositivos y leyendo manuales así como documentos de Internet y libros, nos dimos cuenta que no solo eran dispositivos y antenas si no que también el sistema operativo que nos permitiera en primer lugar accesibilidad esto es, que los sistemas operativos existentes para nosotros tiene varias limitantes, además del precio, pues la curva de aprendizaje y es el pagar por ellos cantidades fuera de nuestro presupuesto como estudiantes, así que también nos dimos a la tarea de investigar que tipos de sistemas operativos nos permitían el acceso sin pagar licencia y nos encontramos con GNU Linux siendo éste el que utilizamos en nuestro trabajo de tesis.

Como las antenas son específicas para cierto espectro de frecuencia depende de lo que queramos hacer, al investigar esto nos dimos cuenta que no en todos los países existen los mismos materiales ya que nos basamos para la construcción de estas antenas en algunos manuales hechos en España, Argentina y Alemania principalmente la construcción de estas antenas fue en si un reto para nosotros lograrlo y hacer que funcionaran. Las antenas fueron probadas para ver si los dispositivos empleados no sufrían pérdidas, estas primeras pruebas fueron a corta distancia claro ya con el sistema funcionando correctamente que esta parte del sistema la verán en los capítulos que componen esta tesis, no fue nada fácil pero sí interesante, teniendo estas primeras pruebas y el sistema ya funcionando pasamos a la etapa de montar las antenas. Esta etapa fue de las mas complicadas ya que como se mencionara en este trabajo los obstáculos son factor importante para realizar el enlace, esto es entre los dos puntos del enlace había árboles y edificios que no se habían tomado en cuenta pero como buenos ingenieros logramos montarlas con ayuda de algunos binoculares unos radios de comunicación y procedimos a tomar el método a

prueba y error, cabe aclarar que esta forma no es la mas idónea pero es una manera barata de hacerlo y así lo hicimos por falta de apoyos y recursos.

Siguiendo en esta misma línea montamos las antenas en tubos galvanizados y con los binoculares, veíamos donde se colocaba la antena y con ayuda de los espejos también verificamos la ubicación de las mismas entonces por medio de los radios nos comunicábamos para saber y encontrar el enlace entre las dos antenas esto los hacíamos por medio de un ping y cuando este ping respondieran ese momento las dejábamos estáticas para probar el enlace y posteriormente compartir Internet. Cabe aclarar que las distancias que se muestran en las tablas del capítulo 6 son o fueron hechas sin montar las antenas en línea recta y tratando que las condiciones fueran las mostradas en la tabla para hacer el comparativo de los obstáculos, qué tanto interfieren y cómo se puede mejorar o modificar y tomar una alternativa para darnos una idea de cómo hacer un mejor enlace.

I. INTRODUCCIÓN

I.1 Panorama General

La necesidad de contar con la disponibilidad de información en un grupo de personas o en una sociedad de una manera rápida y simple, hace abrir nuevas alternativas para buscar y poder encontrar su satisfacción. Esta necesidad puede ser solventada a través de una herramienta moderna como es la computadora, la cual permite almacenar y recuperar dicha información, teniendo además de su disponibilidad la posible apertura hacia otras nuevas aplicaciones o soluciones; básicamente por la velocidad en la realización de tareas, el tamaño reducido para lograr almacenar enormes cantidades de datos, y la posible presentación de éstos en forma escrita o visualizada a través de un monitor de computadora.

Considerando la disponibilidad de la información de una forma rápida y simple, además de llegar a los distintos puntos donde se encuentra cada persona con acceso a una computadora (usuario), o grupo de personas; es necesario entonces conectar varias computadoras entre sí, para de esta manera tener un canal de transmisión de información entre ellas y proporcionar así a cada usuario de la información requerida. A dicha conexión se le denomina red de computadoras, que en nuestro caso particular crea un canal de comunicación entre cada persona y la información que algún otro equipo de cómputo le pueda brindar.

Para poder tener un equipo de cómputo que sirva como fuente de información para las demás computadoras interconectadas, es necesario que una de éstas, denominada como servidor, deba tener una conexión a Internet abastecida de un proveedor en el mercado, o estar conectado por algún medio físico a otro equipo de cómputo muy similar a él, pero que tenga la posibilidad de compartirle el servicio de Internet, y así, éste a su vez permita conectar a Internet a todas las demás computadoras para las que actúa como servidor.

La conexión a Internet la otorga un proveedor dedicado a ello, con este servicio se puede compartir información mutuamente entre una enorme cantidad de usuarios, principalmente como consulta de numerosas fuentes de información, su difusión y transferencia, o como comunicación personal. Tenemos entonces la posibilidad de hacer de una red de computadoras una conexión hacia una red mucho mayor a nivel mundial, llamada Internet.

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 la 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 precios populares y a un conjunto de entusiastas, mayoritariamente particulares, que han visto las enormes posibilidades de esta tecnología.

Es evidente que la tecnología inalámbrica está suscitando no sólo el interés teórico del mercado por las novedades tecnológicas que aporta, sino también interés práctico, ya que se le suponen crecimientos y cifras de negocio a los que la Industria de Tecnologías de la Información ya no está acostumbrada.

I.2 Problemática

Tenemos un lugar sin servicio de Internet de banda ancha, debido a la lejanía de las centrales Telmex (Teléfonos de México) que podrían dotar de servicio a dicho lugar. El radio aproximado de cobertura de una central es de 3km, y se tienen 3 centrales triangulando el sitio que necesita el servicio, dos de ellas ubicadas hacia el sur oeste y sur este con una distancia entre 4 y 3.5km respectivamente, y la tercera ubicada al norte a 3km de distancia que da un servicio muy breve y de mala calidad, debido al recorrido de las líneas telefónicas que deben hacer a lo largo de las calles perpendiculares a la Avenida Aztecas, provocando que la señal sufra de ruido y de una atenuación muy significativa en la transmisión y recepción de datos, no afectando en gran magnitud a la señal de voz.
En el siguiente mapa (fig. I.1) mostramos como están ubicadas las centrales de Telmex así como sus distancias al punto ciego de cobertura.

I.3 Objetivos

Objetivo general:

Dotar de servicio de Internet a una red de computadoras tipo LAN.

Objetivos particulares:

Realizar la conexión punto a punto de 2 computadoras.

Dotar de servicio a la zona de difícil acceso.

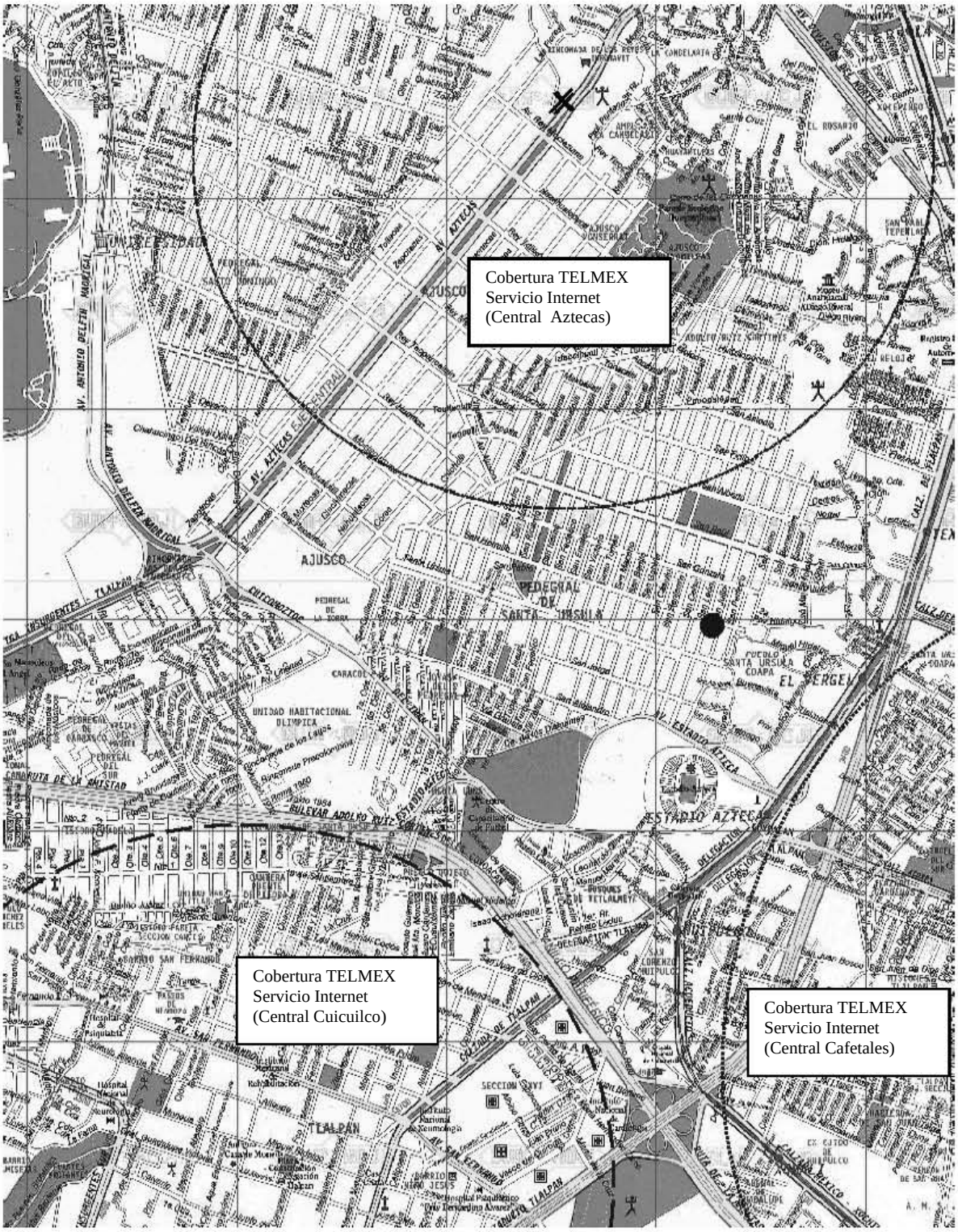


Fig. I.1 Ubicación de las regiones de Servicio

● Lugar sin Servicio de Internet

II. ANTECEDENTES

II.1 Clasificación de las redes de datos

Según su área de cobertura, las redes de datos se clasifican:

Como de ámbito personal (PAN, Personal Area Net Works, con alcances de pocas decenas de metros), locales (LAN, Local Area Net Works, cientos de metros), metropolitanas (MAN, kilómetros) y de larga distancia (WAN, World Area Net Works).

Según la naturaleza del medio de soporte físico para el transporte de la información, las dividiríamos en fijas (por cableado estructurado o fibra, fundamentalmente) e inalámbricas (emisiones de radio u ópticas por medio aéreo).

Redes de Área Local (LAN)

Son redes de propiedad privada, de hasta unos cuantos kilómetros de extensión. Por ejemplo una oficina o un centro educativo.

Se usan para conectar computadoras personales o estaciones de trabajo, con objeto de compartir recursos e intercambiar información.

Están restringidas en tamaño, lo cual significa que el tiempo de transmisión, en el peor de los casos, se conoce, lo que permite cierto tipo de diseños (deterministas) que de otro modo podrían resultar ineficientes. Además, simplifica la administración de la red.

Suelen emplear tecnología de difusión mediante un cable sencillo al que están conectadas todas las máquinas.

Operan a velocidades entre 10, 100 y 1000 Mbps.

Tienen bajo retardo y experimentan pocos errores.

Redes de Área Metropolitana (MAN)

Son una versión mayor de la LAN y utilizan una tecnología muy similar. Actualmente esta clasificación ha caído en desuso, normalmente sólo distinguiremos entre redes LAN y WAN.

Redes de Área Amplia (WAN)

Son redes que se extienden sobre un área geográfica extensa. Contiene una cierta cantidad de máquinas dedicadas a ejecutar los programas de usuarios (hosts). Estos están conectados por la red que lleva los mensajes de un host a otro.

Estas LAN de host acceden a la subred de la WAN por un router. Suelen ser por tanto redes punto a punto.

La subred tiene varios elementos:

- Líneas de comunicación: Mueven bits de una máquina a otra.
- Elementos de conmutación: Máquinas especializadas que conectan dos o más líneas de transmisión. Llamados encaminadores o routers.

Cada host está después conectado a una LAN en la cual está el encaminador que se encarga de enviar la información por la subred.

Una WAN contiene numerosos cables conectados a un par de encaminadores. Si dos encaminadores que no comparten cable desean comunicarse, han de hacerlo a través de encaminadores intermedios. El paquete se recibe completo en cada uno de los intermedios y se almacena allí hasta que la línea de salida requerida esté libre.

Se pueden establecer WAN en sistemas de satélite o de radio en tierra en los que cada encaminador tiene una antena con la cual poder enviar y recibir la información.

II.1.2 Tipología de las redes de área local

Hay muchos parámetros que conforman la arquitectura de una red de área local, en seguida veremos algunos de ellos.

*Según la técnica de transmisión***:** redes de difusión y redes punto a punto.

*Según método de acceso al medio***:** CSMA y Token.

*Por su topología o disposición en el espacio***:** estrella, bus, anillo y mixtas.

II.1.3 Técnicas de transmisión

Redes de difusión

Tienen un solo canal de comunicación compartido por todas las máquinas, en principio todas las máquinas podrían "ver" toda la información, pero hay un "código" que especifica a quien va dirigida.

Redes punto a punto

Método de acceso al medio

En las redes de difusión es necesario definir una estrategia para saber cuando una máquina puede empezar a transmitir para evitar que dos o más estaciones comiencen a transmitir a la vez (colisiones).

CSMA

Se basa en que cada estación monitoriza o "escucha" el medio para determinar si éste se encuentra disponible para que la estación puede enviar su mensaje, o por el contrario, hay algún otro nodo utilizándolo, en cuyo caso espera a que quede libre.

Token

El método del testigo (token) asegura que todos los nodos van a poder emplear el medio para transmitir en algún momento. Ese momento será cuando el nodo en cuestión reciba un paquete de datos especial denominado testigo. Aquel nodo que se encuentre en posesión del testigo podrá transmitir y recibir información, y una vez haya terminado, volverá a dejar libre el testigo y lo enviará a la próxima estación.

II.1.4 Topología de las redes

Se entiende por topología de una red local la distribución física en la que se encuentran dispuestos los ordenadores que la componen. De este modo, existen tres tipos, que podíamos llamar "puros". Son los siguientes:

- Estrella.
- Bus
- Anillo

Topología en Estrella.

Esta topología se caracteriza por existir en ella un punto central, o más propiamente nodo central, al cual se conectan todos los equipos, de un modo muy similar a los radios de una rueda (Ver figura II.1).

De esta disposición se deduce el inconveniente de esta topología, y es que la máxima vulnerabilidad se encuentra precisamente en el nodo central, ya que si este falla, toda la red fallaría. Este posible fallo en el nodo central, aunque posible, es bastante improbable, debido a la gran seguridad que suele poseer dicho nodo.

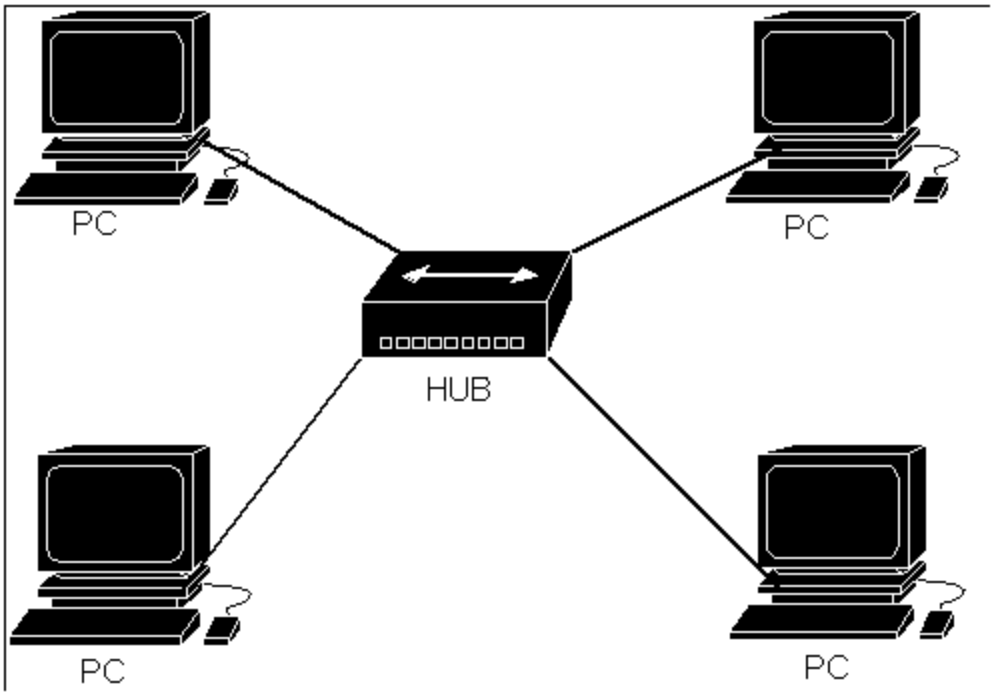


Fig. II.1 Topología tipo estrella.

Sin embargo presenta como principal ventaja una gran modularidad, lo que permite aislar una estación defectuosa con bastante sencillez y sin perjudicar al resto de la red.
Para aumentar el número de estaciones, o nodos, de la red en estrella no es necesario interrumpir, ni siquiera parcialmente la actividad de la red, realizándose la operación casi inmediatamente.
La topología en estrella es empleada en redes Ethernet y ArcNet.

Topología en Bus

En la topología en bus, al contrario que en la topología de Estrella, no existe un nodo central, si no que todos los nodos que componen la red quedan unidos entre sí linealmente, uno a continuación del otro (Ver figura II.2).

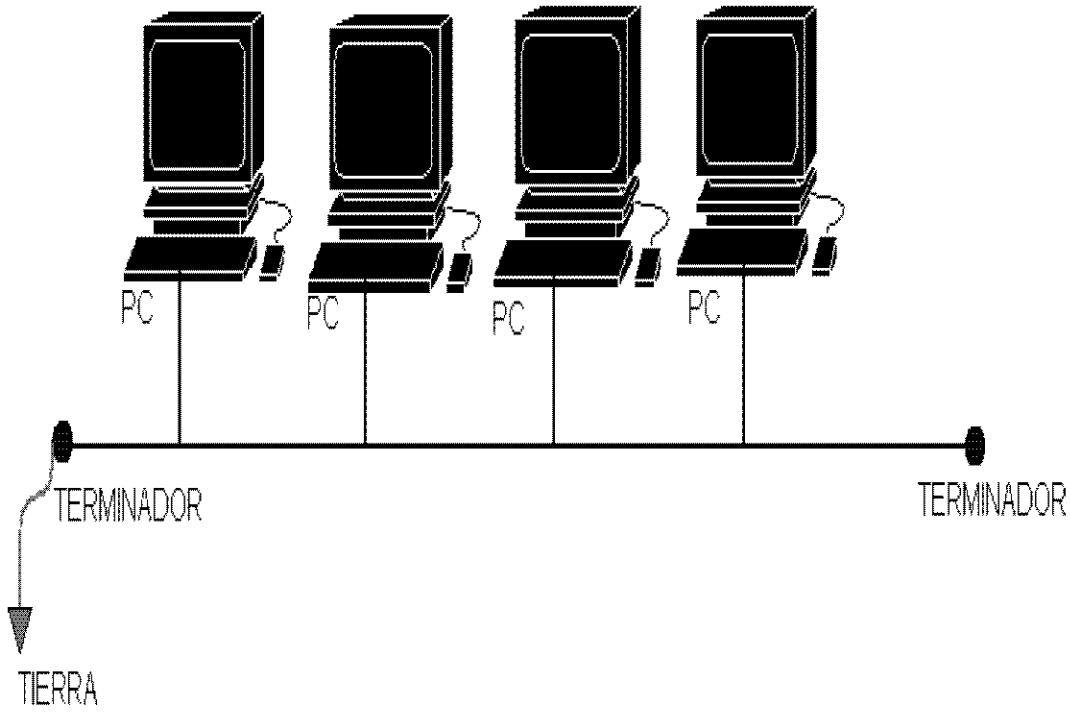


Fig. II.2 Topología tipo bus

El cableado en bus presenta menos problemas logísticos, puesto que no se acumulan montones de cables en torno al nodo central, como ocurriría en la topología tipo estrella. Pero, por el contrario, tiene la desventaja de que un fallo en una parte del cableado detendría el sistema, total o parcialmente, en función del lugar en que se produzca. Es además muy difícil encontrar y diagnosticar las averías que se producen en esta topología.

Debido a que en el bus la información recorre todo el bus bidireccionalmente ósea en las dos direcciones, hasta hallar su destino, la posibilidad de interceptar la información por usuarios no autorizados es superior a la existente en una Red en estrella debido a la modularidad que ésta posee. La red en bus posee un retardo en la propagación de la información mínimo, debido a que los nodos de la red no deben amplificar la señal, siendo su función pasiva respecto al tráfico de la red. Esta pasividad de los

nodos es debida al método de acceso empleado que a la propia disposición geográfica de los mismos en red.
La Red en Bus necesita incluir en ambos extremos del bus, unos dispositivos llamados terminadores, los cuales evitan los posibles rebotes de la señal, introduciendo una impedancia característica (50 Ohms.)
Añadir un nuevo nodo a una red en bus, supone detener al menos por tramos, la actividad de la red. Sin embargo es un proceso rápido y sencillo. Esta topología es tradicionalmente usada en redes Ethernet.

Topología en Anillo

El anillo, como su propio nombre indica, consiste en conectar linealmente entre sí todos los ordenadores, en un bucle cerrado. La información se transfiere en un solo sentido a través del anillo, mediante un paquete especial de datos, llamado testigo, que se transmite de un nodo a otro, hasta alcanzar el nodo destino (Ver figura II.3).

El cableado de la red en anillo es el más complejo de los tres enumerados, debido por una parte al mayor coste del cable, así como a la necesidad de emplear unos dispositivos denominados Unidades de Acceso Multiestación (MAU) para implementar físicamente el anillo.

A la hora de tratar con fallos y averías, la red en anillo presenta la ventaja de poder derivar partes de la red mediante los MAU's, aislando dichas partes defectuosas del resto de la red mientras se determina el problema. Un fallo, pues, en una parte del cableado de una red en anillo, no debe detener toda la red. La adición de nuevas estaciones no supone una complicación excesiva, puesto que una vez más los MAU's aíslan las partes a añadir hasta que se hallan listas, no siendo necesario detener toda la red para añadir nuevas estaciones.
Dos buenos ejemplos de red en anillo serían Token-Ring y FDDI (fibra óptica).

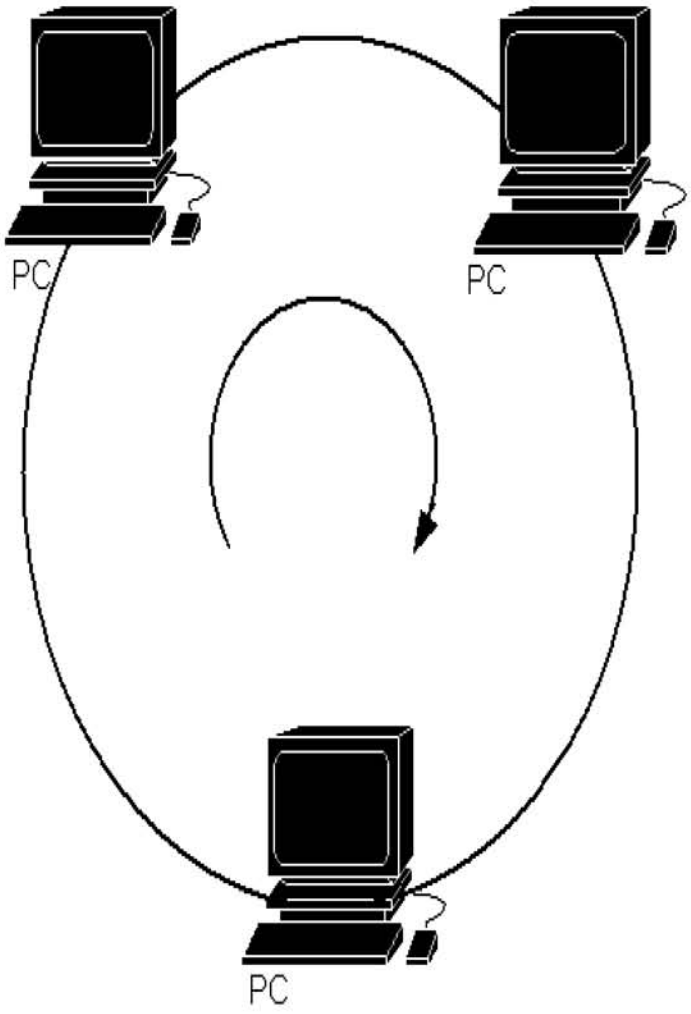


Fig. II.3 Topología tipo anillo

II.1.5 Arquitectura de redes

Las redes están compuestas por muchos dispositivos diferentes que deben trabajar juntos para crear una red funcional. Los dispositivos que comprenden las partes de hardware de la red incluyen tarjetas adaptadoras de red, cables, conectores, concentradores y hasta la computadora misma. Los dispositivos de red los fabrican, por lo general, varias compañías. Por lo tanto, es necesario que haya entendimiento y comunicación entre los fabricantes, en relación con la manera en que cada

componente trabaja e interactúa con los demás componentes de la red.

Afortunadamente, se han creado estándares que definen la forma de conectar componentes de hardware en las redes y el protocolo (o reglas) de uso cuando se establecen comunicaciones por red. Los tres estándares o arquitecturas más populares son: ARCnet, Ethernet y Token Ring. Ethernet y Token Ring son estándares respaldados por el organismo IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), mientras que ARCnet es un estándar de la industria que ha llegado a ser recientemente uno de los estándares del ANSI (Instituto Nacional de Estándares Americanos).

Redes ARCnet

Producida en los años setenta por Datapoint Corporation, la red de cómputo de recursos conectados (ARCnet) es un estándar aceptado por la industria, aunque no lleva un número estándar de IEEE. ANSI reconoció a ARCnet como estándar formal, lo que la hizo parte de su estándar de LAN ANSI 878.1. Como soporta una velocidad de transferencia de datos de 2.5 Mbps, ARCnet usa una topología lógica de bus y una ligera variación de la topología física de estrella. Cada nodo de la red está conectado a un concentrador pasivo o a uno activo. La NIC en cada computadora está conectada a un cable que a su vez está conectado a un concentrador activo o pasivo. ARCnet se basa en un esquema de paso de señal (token passing) para administrar el flujo de datos entre los nodos de la red. Cuando un nodo está en posesión del token (señal), puede transmitir datos por la red. Todos los nodos, a excepción del receptor pretendido, pasan por alto los datos. Conforme se pasa el token a cada nodo, el nodo puede enviar datos.

Ya que cada nodo sólo puede enviar datos cuando tiene el token, en ARCnet no suceden las colisiones que suelen darse en un esquema como el de CSMA/CD. Por lo tanto, ARCnet es menos susceptible a la saturación de la red que Ethernet. Durante algún tiempo ARCnet fue el estándar para LAN más popular; pero por causa en parte a su relativa baja velocidad (2.5

Mbps comparados con los 10 Mbps de Ethernet), casi no se usa para instalaciones nuevas.

Redes Ethernet

Ethernet, al que también se conoce como IEEE 802.3, es el estándar más popular para las LAN que se usa actualmente. El estándar 802.3 emplea una topología lógica de bus y una topología física de estrella o de bus. Ethernet permite datos a través de la red a una velocidad de 10 Mbps. Ethernet usa un método de transmisión de datos conocido como Acceso Múltiple con Detección de Portadora y Detección de Colisiones (CSMA/CD). Antes de que un nodo envíe algún dato a través de una red Ethernet, primero escucha y se da cuenta si algún otro nodo está transfiriendo información. De no ser así, el nodo transferirá la información a través de la red. Todos los otros nodos escucharán y el nodo seleccionado recibirá la información. En caso de que dos nodos traten de enviar datos por la red al mismo tiempo, cada nodo se dará cuenta de la colisión y esperará una cantidad de tiempo aleatoria antes de volver a hacer el envío. La topología lógica de bus de Ethernet permite que cada nodo tome su turno en la transmisión de información a través de la red. Así, la falla de un solo nodo no hace que falle la red completa. Aunque CSMA/CD es una forma rápida y eficiente para transmitir datos, una red muy cargada podría llegar al punto de saturación. Sin embargo, con una red diseñada adecuadamente, la saturación rara vez es preocupante. Existen tres estándares de Ethernet, 10BASE5, 10BASE2, y 10BASE-T, que definen el tipo de cable de red, las especificaciones de longitud y la topología física que debe utilizarse para conectar nodos en la red.

Redes Token Ring

Token Ring, también llamado IEEE 802.5, fue ideado por IBM y algunos otros fabricantes. Con operación a una velocidad de 4 Mbps o 16 Mbps, Token Ring emplea una topología lógica de anillo y una topología física de estrella. La NIC de cada

computadora se conecta a un cable que, a su vez, se enchufa a un hub central llamado unidad de acceso a multiestaciones (MAU). Token Ring se basa en un esquema de paso de señales (token passing), es decir que pasa un token (o señal) a todas las computadoras de la red. La computadora que esté en posesión del token tiene autorización para transmitir su información a otra computadora de la red. Cuando termina, el token pasa a la siguiente computadora del anillo. Si la siguiente computadora tiene que enviar información, acepta el token y procede a enviarla. En caso contrario, el token pasa a la siguiente computadora del anillo y el proceso continúa. La MAU se salta automáticamente un nodo de red que no esté encendido. Sin embargo, dado que cada nodo de una red Token Ring examina y luego retransmite cada token (señal), un nodo con mal funcionamiento puede hacer que deje de trabajar toda la red. Token Ring tiende a ser menos eficiente que CSMA/CD (de Ethernet) en redes con poca actividad, pues requiere una sobrecarga adicional. Sin embargo, conforme aumenta la actividad de la red, Token Ring llega a ser más eficiente que CSMA/CD.

Nuevas tecnologías

Existen varias tecnologías nuevas que satisfacen las necesidades de las redes actuales, incluyendo a Fast Ethernet, FDDI, Frame Relay y ATM.

Fast Ethernet, llamado también 100BASEX, es una extensión del estándar Ethernet que opera a velocidades de 100 Mbps, un incremento 10 veces mayor que el Ethernet estándar de 10 Mbps.

La interfaz de distribución de datos por fibra óptica (FDDI) es un estándar para la transferencia de datos por cable de fibra óptica. El estándar ANSI X3T9.5 para FDDI especifica una velocidad de 100 Mbps.

Nota: En todo el apartado de arquitectura de redes, tomamos ideas de http://www.geocities.com/SiliconValley/8195/redes.html#tres

Dado que el cable de fibra óptica no es susceptible a la interferencia eléctrica o tan susceptible a la degradación de la señal de red como sucede con los cables de red estándar, FDDI permite el empleo de cables mucho más largos que otros estándares de red.

El Frame Relay (retransmisión de tramas) es un servicio orientado a la conexión, para mover datos de un nodo a otro a una velocidad razonable y bajo costo. El frame relay puede verse como una línea virtual rentada. El usuario renta un circuito virtual permanente entre dos puntos y entonces puede enviar tramas o frames (es decir, paquetes) de hasta 1600 bytes entre ellos. Además de competir con las líneas rentadas, el frame relay compite con los circuitos virtuales permanentes de X.25.
ATM, que significa modo de transferencia asíncrona, es un conjunto de estándares internacionales para la transferencia de datos, voz y video por medio de una red a muy altas velocidades. Puesto que opera a velocidades que van desde 1.5 Mbps hasta 1.5 Gbps, ATM incorpora parte de los estándares Ethernet, Token Ring y FDDI para la transferencia de datos.

II.1.6 Descripción del modelo OSI

El modelo de referencia OSI es la arquitectura de red actual más prominente. El objetivo de éste es el de desarrollar estándares para la interconexión de sistemas abiertos (Open System Interconnection, OSI). El término OSI es el nombre dado a un conjunto de estándares para las comunicaciones entre computadoras, terminales y redes. OSI es un modelo de 7 capas, donde cada capa define los procedimientos y las reglas (protocolos normalizados) que los subsistemas de comunicaciones deben seguir, para poder comunicarse con sus procesos correspondientes de los otros sistemas. Esto permite que un proceso que se ejecuta en una computadora, pueda comunicarse con un proceso similar en otra computadora, si tienen implementados los mismos protocolos de comunicaciones de capas OSI. Algunas de las funciones de cada capa o nivel se describen a continuación:

Nivel	Nombre	Función	Dispositivos y protocolo
1	Físico	Se ocupa de la transmisión del flujo de bits a través del medio.	Cables, tarjetas y repetidores (hub). RS-232, X.21.
2	Enlace	Divide el flujo de bits en unidades con formato (tramas) intercambiando estas unidades mediante el empleo de protocolos.	Puentes (bridges). HDLC y LLC.
3	Red	Establece las comunicaciones y determina el camino que tomarán los datos en la red.	Encaminador (router). IP, IPX.
4	Transporte	La función de este nivel es asegurar que el receptor reciba exactamente la misma información que ha querido enviar el emisor, y a veces asegura al emisor que el receptor ha recibido la información que le ha sido enviada. Envía de nuevo lo que no haya llegado correctamente.	Pasarela (gateway). UDP, TCP, SPX.
5	Sesión	Establece la comunicación entre las aplicaciones, la mantiene y la finaliza en el momento adecuado. Proporciona los pasos necesarios para entrar en un sistema utilizando otro. Permite a un mismo usuario, realizar y mantener diferentes conexiones a la vez (sesiones).	Pasarela.
6	Presentación	Conversión entre distintas representaciones de datos y entre terminales y organizaciones de sistemas de ficheros con características diferentes.	Pasarela. Compresión, encriptado, VT100.
7	Aplicación	Este nivel proporciona unos servicios estandarizados para poder realizar unas funciones especificas en la red. Las personas que utilizan las aplicaciones hacen una petición de un servicio (por ejemplo un envío de un archivo). Esta aplicación utiliza un servicio que le ofrece el nivel de aplicación para poder realizar el trabajo que se le ha encomendado (enviar el archivo).	X.400

II.2 Redes inalámbricas

Las genéricamente denominadas “redes inalámbricas Ethernet (Wireless Ethernet)” son redes inalámbricas basadas en emisiones de radio, con unos fundamentos tecnológicos análogos a las redes Ethernet cableadas y, principalmente, orientadas a cubrir el segmento de redes LAN y, ocasionalmente, también PAN.

II.2.1 Historia

Las primeras experiencias con redes inalámbricas datan de 1979 cuando científicos de IBM en Suiza despliegan la primera red de importancia con tecnología infrarroja. No es hasta 1985 cuando se comienzan los desarrollos comerciales de redes con esta filosofía, momento en el que el órgano regulador del espectro radioeléctrico americano, la FCC, asigna un conjunto de estrechas bandas de frecuencia para libre uso en las bandas de los 2,4 y los 5 GHz. Inmediatamente, la asociación de ingenieros electrónicos, IEEE, designa una comisión de trabajo para desarrollar una tecnología de red en dichas bandas: la 802.11. A partir de ese momento se liberan una serie de estándares, el más reciente de los cuales es el IEEE 802.11h.

II.2.2 Clasificación de redes inalámbricas

Lo primero es situarnos dentro del mundo inalámbrico. Para ello vamos a hacer una primera clasificación que nos centre ante las diferentes variantes que podemos encontrarnos:

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

Redes inalámbricas personales

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

a- En primer lugar 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. Estas redes no entran dentro del ámbito del presente documento.

Redes inalámbricas 802.11

Las redes inalámbricas(WN ó wireless Networks) 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 confusión.

Nos encontramos ante tres principales variantes:

1- 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 (al 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 aseguro 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 esta frecuencia está reservada a la HyperLAN2 y la parcial disponibilidad de la misma en Japón.

El hecho de no estar disponible en Europa prácticamente la descarta de nuestras posibilidades de elección para instalaciones en este continente.

2- 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 (al 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, etc. 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 que también es gratuita alrededor de todo el mundo. Está estandarizado por el IEEE.

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

Nota: Mas información sobre los estándares respectivos 802.11a, b y g se pueden consultar en el apéndice II.1 y en la página oficial de la IEEE (www.iee.org.com).

II.2.3 Dispositivos wireless

Sea cual sea el estándar que elijamos vamos a disponer principalmente de dos tipos de dispositivos:

a- Dispositivos “Tarjetas de red” ó TR, que serán los que tengamos integrados en nuestra computadora, o bien conectados mediante un conector PCMCIA ó USB si estamos en un portátil o en un slot PCI si estamos en un ordenador de escritorio. Substituyen a las tarjetas de red Ethernet o Token Ring a las que estábamos acostumbrados. Recibirán y enviarán la información hacia su destino desde el ordenador en el que estemos 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 PA’s pueden sustituir 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.

Estos dos tipos de dispositivos podemos observarlos en la figura II.4 que se muestra a continuación.

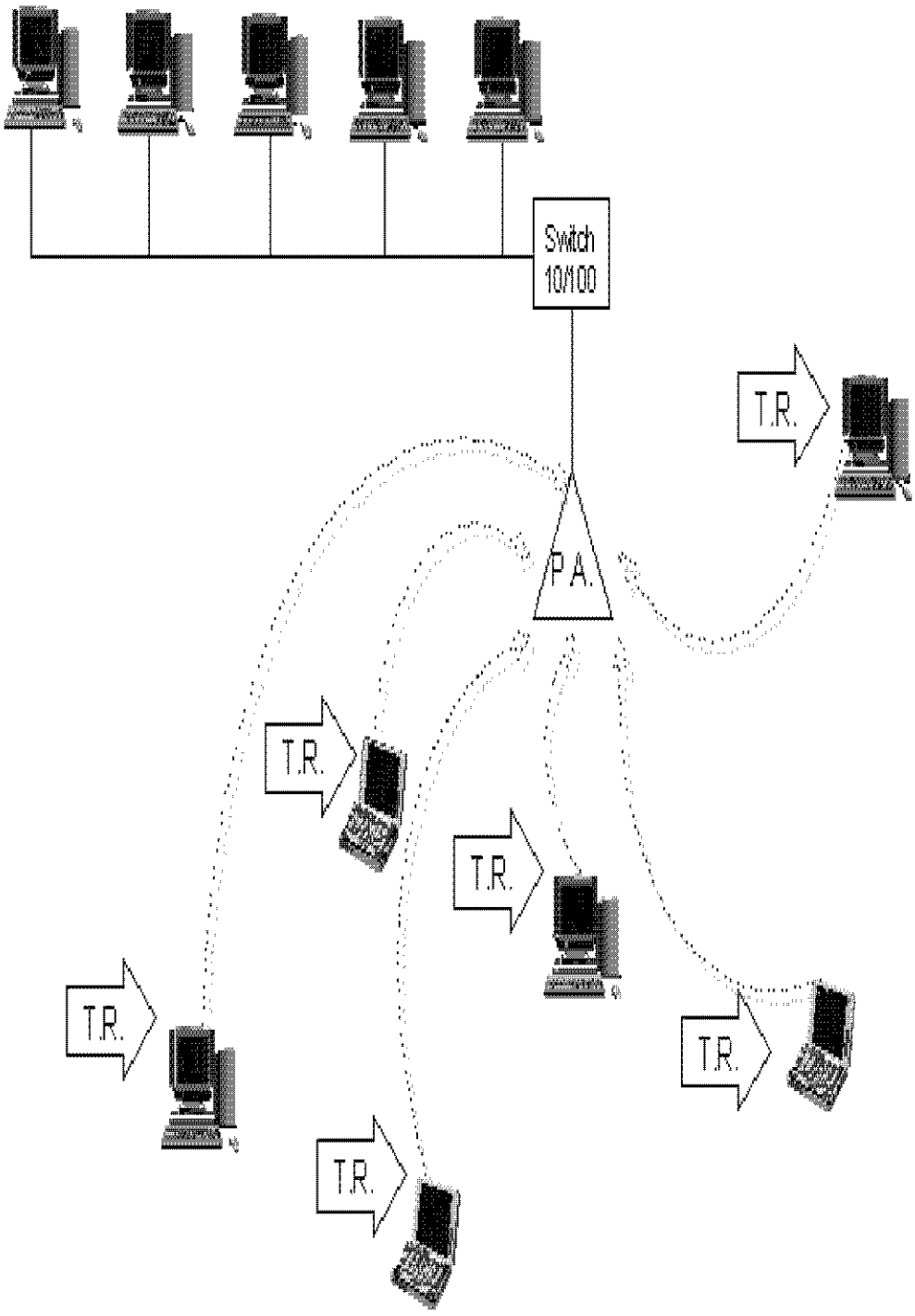


Fig. II.4 Representación gráfica de una red inalámbrica equivalente a una red cableada.

Funcionamiento de los dispositivos

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

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)
- 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 PA's presentan un alcance teórico de los mismos que suele andar 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 ponemos una TR cerca de un PA disponemos de la velocidad máxima teórica del PA, 54 Mbps por ejemplo, y conforme nos vamos 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.

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

Dentro de los PA's (actualmente ya se puede comenzar a aplicar también a los TR's) se puede modificar enormemente la capacidad de TX/RX gracias al uso de antenas especiales. Estas antenas se pueden dividir en:

- Direccionales
- Omnidireccionales

A) Las antenas Direccionales "envían" la información a una cierta zona de cobertura, a un ángulo de apertura 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. Esto es una antena direccional al darle un cierto ángulo y cierta potencia podremos comunicarnos con otra antena a cierta distancia y con cierto ángulo de apertura, en la figura II.5 se muestra como trabaja una antena direccional.

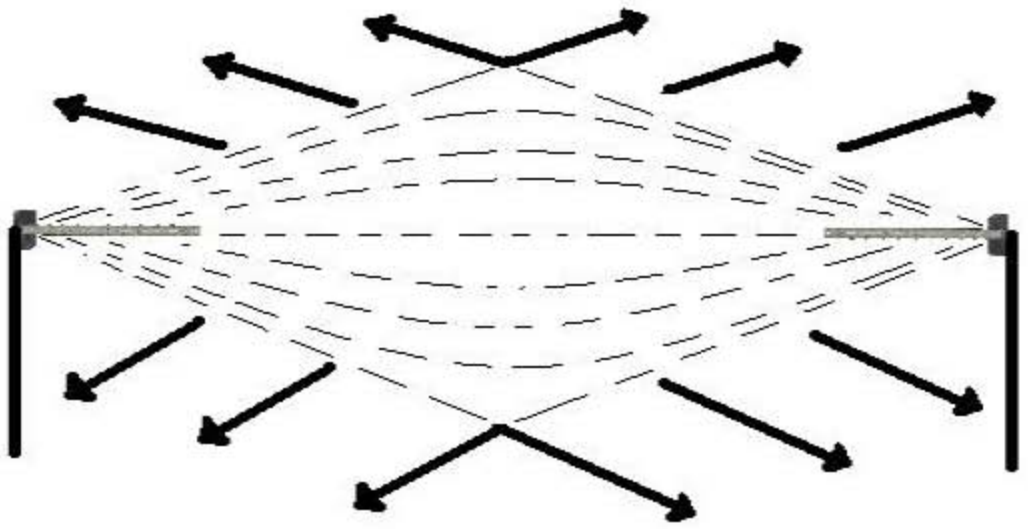


Figura II.5 Transmisión de antenas direccionales.

B) 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. La transmisión de este tipo de antenas se muestra en la figura II.6.

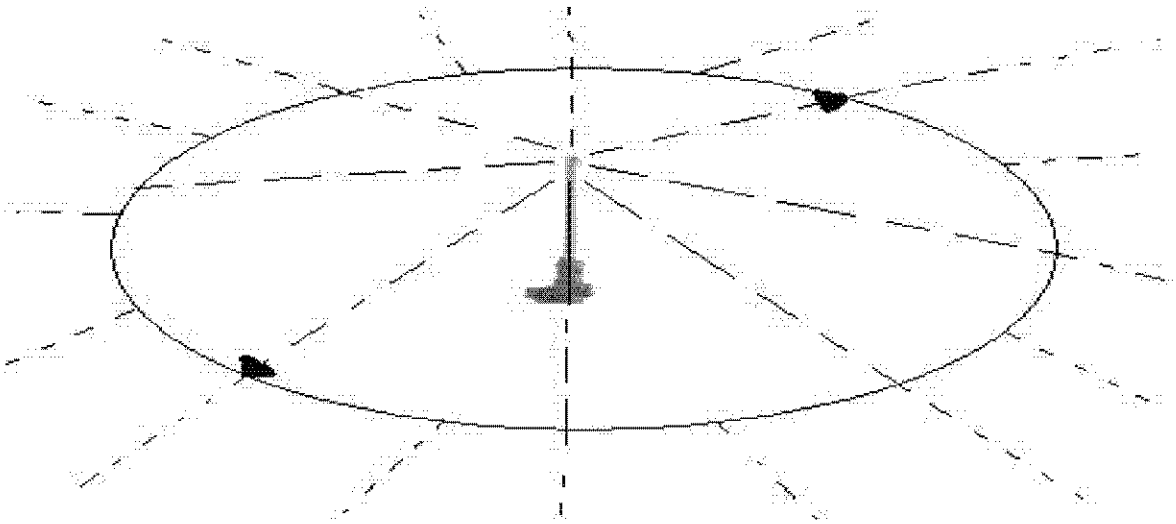


Figura II.6 Transmisión de antena omnidireccional

II.2.4 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 nos referimos 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 tres topologías básicas:

a) Topología Ad-Hoc. Cada dispositivo se puede comunicar con todos los demás. Cada nodo forma parte de una red Peer to Peer o de igual a igual, para lo cual sólo vamos a necesitar el disponer de un SSID igual para todos los nodos y no sobrepasar un número razonable de dispositivos que hagan bajar el rendimiento. A más dispersión geográfica de cada nodo más dispositivos pueden formar parte de la red, aunque algunos no lleguen a verse entre si.

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). Este nodo sirve para encaminar las tramas hacia una red convencional o hacia otras redes distintas. Para poder establecerse la comunicación, todos los nodos deben estar dentro de la zona de cobertura del AP[1].

Todos los dispositivos, independientemente de que sean TRs o PAs tienen dos modos de funcionamiento. Tomemos el modo Infraestructura como ejemplo:

Modo Managed, es el modo en el que la TR se conecta al AP para que éste último le sirva de “concentrador”. La TR sólo se comunica con el AP.

Modo Master. Este modo es el modo en el que trabaja el PA, pero en el que también pueden entrar los TRs si se dispone del firmware apropiado o de un ordenador que sea capaz de realizar la funcionalidad requerida.

Estos modos de funcionamiento nos sugieren que básicamente los dispositivos WiFi son todos iguales, siendo los que funcionan como APs realmente TRs a los que se les ha añadido cierta funcionalidad extra, vía firmware o vía SW. Para realizar este papel se pueden emplear máquinas antiguas 80486 sin disco duro y bajo una distribución especial de linux llamada LINUXAP – OPENAP.

[1] http://www.el202.net/hitech202/redes_wifi_para_todos_as.htm

III. SISTEMA OPERATIVO PARA EL ENLACE INALÁMBRICO.

III.1 Análisis de Sistema Operativo

El sistema operativo juega un papel importante en el presente desarrollo debido a que la tecnología que utilizamos requiere de este para poder ser mas eficiente y/o eficaz esto es que su estructura y portabilidad nos de mejoras en el proyecto, podemos agregar también el costo de el sistema ya que la tecnología wireless no es accesible a todo el público, además es importante considerar que en el mercado podemos encontrar software libre y comercial, esto debido a que hay varios tipos de usuarios que requieren de diferentes sistemas según las necesidades de cada cual.

El software libre es aquel en el que su código fuente es liberado y esta a la mano de quien quiera mejorarlo o modificarlo según se necesite. El software comercial esta dirigido principalmente a un usuario común que tiene que pagar por usar todo tipo de programas y el código fuente por el que paga no esta a disposición de modificarlo para su mejora.

La selección del sistema operativo fue en función a una comparación entre sistemas operativos conocidos, que hemos usado (windows, linux y mac) y con los cuales contábamos. Los sistemas como Windows 98 requieren:

- Procesador 486DX / 66 MHz ó superior.
- 16 MB de memoria; a más memoria mayor rendimiento.
- Una instalación típica requiere aproximadamente 195 Mb de espacio libre en el disco duro, pero puede variar entre 120 y 295 Mb, dependiendo de la configuración del ordenador y de las opciones que desee instalar.
- CD-ROM o DVD-ROM (también existen discos de 3.5" disponibles).
- Monitor VGA o superior.
- Ratón Microsoft o compatible

y Mac Matrox RTMac requiere la siguiente configuración mínima de sistema:

- Placa base Power Mac G4 mono o multi procesador con AGP
- Procesador PowerPC G4 a 400 MHz
- 320 MB de RAM (mínimo)
- Una ranura PCI libre
- Mac OS versión 9.2.2
- Final Cut Pro 3.0.4
- QuickTime 5

para que funcionen, se tiene que pagar una licencia que tiene un costo medio por arriba de los mil pesos mexicanos dependiendo la versión, no solo esto, también nos percatamos que no cualquier dispositivo en el caso de Mac era compatible.
En cuanto a Windows es amigable con más dispositivos así que probamos y de verdad tuvimos problemas para poder añadir el controlador pcmcia para una tarjeta wireless orinoco silver, que se necesitaba. Estas experiencias, el costo de licencia, así como algunas deficiencias como que el sistema se hacia lento, salía la famosa pantalla de error que Windows tiene programada cuando se desborda la memoria u ocurre algún otro error del sistema ya que Windows a diferencia de Linux no maneja los multiprocesos que estos a su vez nos permiten que si una aplicación llegara en dado caso a bloquearse nos permitirá desbloquearlo sin que nos salga una pantalla azul de error y además no tendremos la necesidad de reiniciar nuestro sistema solo la aplicación que se trabo, entre otros, nos orillaron a probar con otro sistema, un sistema con muchas bondades, como es multiplataforma, además de que tiene código abierto, este sistema no tiene costo alguno y se llama Unix/linux.

Para la selección de una distribución de linux, instalamos varias de ellas que aparecen en seguida:

- Mandrake 9, 10 y 10.1
- Debian GNU/Linux 3.0 Woody

- Gentoo
- SUSE linux 7
- Red Hat 7

Estas distribuciones las probamos y dentro de los problemas más frecuentes tuvimos; la dificultad de instalación, así como poder levantar algunos dispositivos necesarios tales como; las tarjetas wifi. Otro contratiempo fue el parchar ó actualizar el kernel. El kernel ó núcleo actúa como intermediario entre sus programas y la computadora. En primer lugar, gestiona la memoria de todos los programas o procesos, y se asegura de que se reparten los ciclos del procesador. Además, proporciona una interfaz amigable para que los programas hablen fácilmente con su hardware.

Realmente, el núcleo hace más cosas, pero las anteriores son las más importantes.

Es importante parchar el kernel ya que los núcleos nuevos normalmente ofrecen la posibilidad de entenderse con más accesorios hardware, o sea, incluyen más manejadores (drivers), se ejecutan más rápidamente, son más estables o corrigen errores de otras versiones.

Así entonces parchar ó actualizar el kernel nos permitirá configurar los módulos necesarios para nuestro proyecto, algunas distribuciones requieren de una instalación rápida y literalmente fácil pero otras son un poco complicadas ya que debemos tener ciertos conocimientos para no afectar algún dispositivo de las maquinas utilizadas.

Finalmente después de varias pruebas de funcionalidad de las distribuciones arriba mencionadas instalamos la distribución Red Hat 7.2 que resolvió muchas dificultades, ya que, su instalación fue relativamente rápida y fácil, además de que es muy ligera y/o el espacio que se necesita en disco duro para poder instalarlo es relativamente poco sus características mas notables son:

- Administrador de ficheros Nautilus para la administración de ficheros gráficos

- Particionamiento automático y perfiles kickstart automáticos en el programa de instalación actualizado
- Herramienta de configuración de red para conectarse a Internet fácilmente
- La nueva herramienta de administración para el usuario acelera la administración del sistema para el usuario
- La nueva herramienta de visualización del hardware permite una rápida inspección del sistema

Mejoras del kernel 2.4

- Sistema de ficheros Journaling ext3
- Aumento del soporte para dispositivos

Los módulos para implementar wireless los levantamos de una manera increíble ya que sólo tuvimos que parchar y/o actualizar el módulo de linux Red Hat 7.2, así como agregar otros módulos.

Dada la estructura y portabilidad del sistema operativo creemos poderlo implementar en cualquier equipo genérico (PC).

A continuación se presentan Ventajas correspondientes

La instalación:

- En Linux a pesar de todos los esfuerzos la instalación no resulta sencilla siempre, pero te permite personalizar totalmente los paquetes que quieras instalar.
- En Windows la instalación es mínimamente configurable aunque es muy sencilla.

La compatibilidad:

- Aunque Linux no está detrás de ninguna casa comercial gracias a su elevada popularidad ofrece una alta compatibilidad ofreciendo, además, actualizaciones frecuentes.

- Windows al ser parte de Microsoft intenta ofrecer una gran cantidad de drivers ya que su gran poder económico hace que las empresas mismas de hardware creen sus propios drivers.

Software:

- Linux al tener menos software en algunos campos sufre una menor aceptación por parte de las empresas, aunque gracias a los apoyos de empresas como Sun Microsystems o IBM se han logrado muchos avances.
- Windows al ser el mas fácil de usar en las empresas, posee una gran cantidad de software.

Robustez:

- Linux se ha caracterizado siempre por la robustez de su sistema ya que pueden pasar meses e incluso años sin la necesidad de apagar o reiniciar el equipo, también si una aplicación falla simplemente no bloquea totalmente al equipo.
- En Windows siempre hay que reiniciar cuando se cambia la configuración del sistema, se bloquea fácilmente cuando ejecuta operaciones aparentemente simples por lo que hay que reiniciar el equipo.

Espacio:

- Linux requiere de un menor espacio en disco duro debido a su estructura portátil y una interfase ligera.
- Windows maneja una interfase que ocupa mayor espacio en disco duro así como el formato de archivos que maneja Windows necesitan de un mayor espacio en disco duro.

Nota: Toda esta información fue recopilada de varias páginas en Internet y revistas de Linux como son: http://www.todo-linux.com ,http://www.linuxwiki.de, http://wiki.colinux.org , http://linux.editme.com.

III.2-Levantamiento del módulo pcmcia y el kernel

La mayoría de las tarjetas que se venden actualmente son del tipo Orinoco (Lucent), Symbol HR y Prism 2, nosotros utilizamos del tipo orinoco. Todas ellas están soportadas por el driver orinoco_cs incluído en el kernel 2.4.x, pero sólo para trabajar en modo managed o ad-hoc, porque no soportan el modo master.

Cuando configuramos el kernel, al usar una tarjeta ethernet PCMCIA, activamos el soporte para red, y desactivamos los controladores normales de tarjetas de red de Linux, incluyendo "pocket and portable adapters". Todos los controladores para tarjetas de red PCMCIA están compilados como módulos cargables. Cualquiera de los controladores compilados dentro de su kernel solamente desperdiciará espacio.

A continuación una sinopsis del proceso de instalación:

- Se descomprime pcmcia-cs-3.0.x.tar.gz en /usr/src
- Ejecutamos "make config" en el nuevo directorio pcmcia-cs-3.0.x
- Ejecutamos "make all", y luego "make install".
- Configuramos el script de inicio y los archivos de opciones en /etc/pcmcia para su sitio.

Cuando ejecutamos "make config", se nos preguntaron algunas opciones de configuración y el sistema se encarga de verificar que se satisfagan todos los prerrequisitos para instalar soporte PCMCIA.

Red Hat 7.2

Red Hat usa una filosofía diferente (al menos en la versión 7.2), en vez de configurar la red dentro de los directorios en /etc/pcmcia, lo hace en los mismos directorios donde se configuran las interfaces de red, en **/etc/sysconfig/network-**

scripts/ifcfg-ethX. Por lo tanto los parámetros de red hay que configurarlos en dichos directorios, por ejemplo:

```
DEVICE=eth1
MODE=managed
ESSID="Nombre_de_red"
BROADCAST=192.168.0.100
NETMASK=255.255.255.0
NETWORK=192.168.0.0
```

DEVICE=Dispositivo se refiere a un ente físico o lógico, en Linux cada ente físico tiene su propio dispositivo, como ejemplo el mouse tiene el ente lógico /dev/mouse que es un archivo del filesystem principal. También puede haber dispositivos sin ente físico como es el caso de /dev/null que es el basurero. En nuestro caso el dispositivo hace referencia a una tarjeta de red.

eth1=Dispositivo de ethernet o parámetro de red.

MODE=En modo podemos utilizar alguno de los tres que se nombran en el capítulo 2, en nuestro caso utilizaremos el modo ad-hoc.

Managed=Uno de los tres modos que se pueden utilizar en las redes inalámbricas.

ESSID= Es un grupo de trabajo en una red.

BROADCAST=Apunta hacia el gateway 192.168.1.1

NETMASK=Máscara de subred.255.255.255.0

NETWORK= Red de computadoras- Dirección IP de la red 192.168.X.X

NOTA: En los apéndices III.1 y III.2 se explica más a fondo el levantamiento y/o configuración del módulo pcmcia, así como la instalación de RED HAT 7.2.

IV. Integración de hardware

IV.1-Análisis de antenas

Concepto de Antena

Una antena es un dispositivo capaz de emitir y recibir energía en forma de radiofrecuencia (ondas electromagnéticas), que adapta la salida del emisor y la entrada del receptor al medio de transmisión (el aire).

Funcionamiento de una antena

La antena es un conductor eléctrico que recibe o emite ondas de radiofrecuencia al circular por él una corriente alterna. Un campo ya sea magnético o eléctrico, crea una tensión de energía en el espacio que rodea al conductor. Dependiendo de las variaciones de valor y polaridad de esta tensión, el campo eléctrico aparecerá y desaparecerá instantánea y periódicamente. Una parte mínima ocurrirá con el campo magnético, que seguirá las variaciones de la corriente que circula por la antena. Es decir, la antena toma y devuelve energía al generador periódicamente, y parte de dicha energía en forma de campo electromagnético que no es devuelta, es radiada ó emitida a través del aire la cual representa la información que llegará al receptor.

Sistema Radiante

Es una composición básicamente de 3 elementos:

1. Receptor-transmisor.- El emisor ó transmisor se encarga de convertir la información analógica ó digital en ondas electromagnéticas. El receptor va a realizar esta misma actividad pero de manera contraria, esto es, de ondas electromagnéticas a señales analógicas ó digitales.

2. Línea de transmisión.- A través de la cual la energía viaja desde el transmisor a la antena sin radiar energía, comportándose simplemente como un medio de transporte, que no forma parte de la antena.

3. Antena.- Encargada de enviar y recibir las ondas electromagnéticas, hace las veces de emisor y receptor (ver figura 4.1).

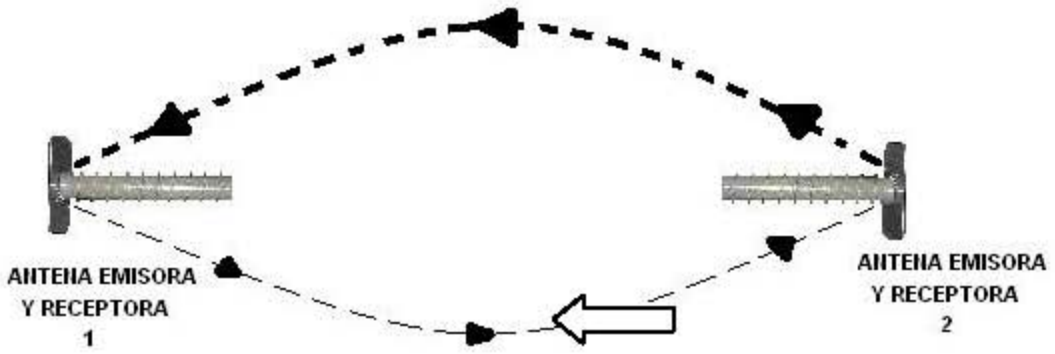


Fig. 4.1 Antena Emisora-Receptora

Frecuencia

Es el número de ciclos que tiene una onda por unidad de tiempo (en un segundo). Su medida es el Hertz, pudiéndose llamarse ondas hertzianas.

Longitud de onda

Es la longitud medida en metros correspondiente a un ciclo de la onda considerada, sabiendo que las ondas hertzianas viajan en el espacio con la velocidad de la luz (300,000 Km/s). En otras palabras, si tenemos una onda electromagnética con una frecuencia de 1 Hertz ó 1 ciclo en un segundo, su longitud de onda sería de 300,000 Km.

Tipos de antenas

Las características principales que se tienen en una antena son: Directividad, Impedancia, ganancia, polarización y ancho de banda.

Dentro de la enorme gama de antenas conocidas, cada uno de sus tipos va a depender de las características que las definen, las cuales además de cumplir con sus requisitos específicos, determinan también su calidad. Algunas características destacan más entre sí, con el fin de lograr mejorías en cuanto a conveniencias del enlace, normas federales, obstáculos físicos o cualquier otro existente.

1. De acuerdo a su posición y forma, una antena emite la energía entregada por el transmisor en una disposición específica. A esta forma se le conoce como patrón de radiación o directividad.
Dependiendo de las necesidades de cobertura o directividad del enlace, los tipos posibles son:
Unidireccionales: el haz de rayos se emite en una sola dirección, por lo que se aplica a los sistemas de comunicación punto a punto.
Omnidireccionales: el haz de rayos se emite en todas direcciones.
Sectoriales: el haz de rayos se emite en un ángulo determinado.

2. De acuerdo a su frecuencia, una antena va a depender elementalmente de la frecuencia de las ondas que serán transmitidas, esta frecuencia tiene una longitud de onda determinada, que va a definir el tamaño de la antena y también influirá en la potencia necesaria para transmitir diferentes frecuencias ya que tienen distintas longitudes de onda.
La longitud o tamaño de las antenas está directamente relacionado con la frecuencia de la señal que se va a transmitir. Mientras más alta la frecuencia, menor es la longitud de onda, y más pequeña debe ser la antena.

3. De acuerdo a su impedancia, el valor de la impedancia de una antena es la resistencia que ésta presenta en su punto de conexión a la señal de corriente alterna que le llega del transmisor por la línea de transmisión.
Ésta es medida en ohmios y existe un valor adoptado universalmente para las antenas de los equipos de radio, que es igual a 50 ohmios. Cuando la impedancia de la antena es de un valor diferente se emplean bobinas, transformadores o metales con el fin de acoplar esas impedancias.

4. De acuerdo a su ganancia, la ganancia de una antena se mide por comparación de la potencia que sería necesaria aplicar a una antena patrón para producir, en la misma dirección y a igual distancia, un campo electromagnético de la misma intensidad.
Si consideramos el patrón de radiación, se dice que una antena concentra la señal hacia una sola dirección, esto hace parecer como si la señal fuera emitida con una potencia mayor.
La ganancia de las antenas se mide en decibeles, que es la unidad de medida. A mayor cantidad de decibeles, mejor calidad en el enlace.

5. De acuerdo a su polarización, la polarización de una antena se refiere a la dirección del campo eléctrico dentro de la onda electromagnética emitida por ésta. Las antenas verticales emiten un campo eléctrico vertical por lo tanto su polarización es vertical. Las antenas horizontales tienen, por lo tanto, polarización horizontal. La polarización vertical es aquella en la que el sentido del campo eléctrico es de arriba hacia abajo y la horizontal el sentido del campo eléctrico es de izquierda a derecha.

Para que haya una buena comunicación entre dos antenas, éstas deben tener el mismo tipo de polarización. En el caso de las ciudades, se utilizan preferiblemente las antenas verticales tanto para las antenas fijas, como para las antenas móviles. La parte más importante en una antena, es la llamada “elemento”, puesto que es la fuente de radiación más simple.

A continuación se tienen los tipos generales de antenas, y sus respectivas características que las hacen muy particulares:

La antena tipo Hertz, que consiste en una antena horizontal aislada de la tierra con un tamaño de media longitud de onda de la frecuencia que se desea transmitir. Esta antena está formada por dos alambres aislados en los extremos de cualquier superficie conductora, y separados en el centro por otro aislador, se le llama comúnmente como antena dipolo. Genera campos electromagnéticos polarizados horizontalmente, radia en dirección perpendicular al conductor y su ángulo de salida depende mucho de su altura respecto al suelo.

La antena tipo Marconi, que utiliza como uno de sus polos la tierra, mide un cuarto de la longitud de la onda para transmitir. Esta antena se monta verticalmente y radia uniformemente alrededor del horizonte, produce campos polarizados verticalmente.

La antena vertical conectada a tierra y la antena vertical con plano de tierra. Esta deben tener una longitud aproximada de media onda y la antena con plano de tierra se puede construir con una longitud de un cuarto de onda, pero además posee en su parte inferior un plano de tierra formado por alambres gruesos o por tubos de aluminio delgados que se distribuyen en forma radial. Este plano de tierra metálico simula o reemplaza el efecto de la superficie de la tierra en el proceso de creación de las ondas electromagnéticas en la antena.

La antena coaxial se usa principalmente para instalaciones fijas de base, y en algunos casos para operación móvil. Su construcción es más compleja y casi no se ha popularizado su uso.

La antena de plano de tierra es omnidireccional y no tiene ganancia. Es posible modificarla e introducirle ganancia para hacerla semidireccional. Es económica y con un buen rendimiento para enlaces locales. Estas antenas se utilizan especialmente en las estaciones fijas o bases.

La antena vertical está formada por varios elementos en forma de parrilla o arreglo de varillas paralelas. Su forma es parecida a las antenas receptoras de televisión; esta antena recibe el

nombre de "YAGI", debido a que fue ideada por los japoneses Yagi y Uda. En las antenas direccionales tipo YAGI la señal se concentra en una sola dirección tanto de transmisión como de recepción. Se construyen con dos o más elementos dependiendo de la ganancia deseada.

Las antenas pueden ser construidas multibanda a través del uso de circuitos resonantes (bobinas y condensadores intercalados) colocados en puntos específicos de la antena. Por ejemplo en las antenas verticales y en las Yagi.

La antena direccional cuádrica o cúbica está formada por cuadros de alambre sostenidos por elementos aislantes en forma de cruz. Cada cuadro tiene una longitud de un cuarto de onda por cada lado. En la configuración más común se tienen dos cuadros; uno se utiliza como elemento principal o excitador y el otro como reflector.

La antena de Reflector o Parabólica es un reflector metálico, de forma parabólica, esférica o de bocina, que limita las radiaciones a un cierto espacio, concentrando la potencia de las ondas; se utiliza especialmente para la transmisión y recepción vía satélite.
Tipos de antenas para enlaces inalámbricos: los diferentes tipos de antenas mencionados se muestran en la fig. IV.2

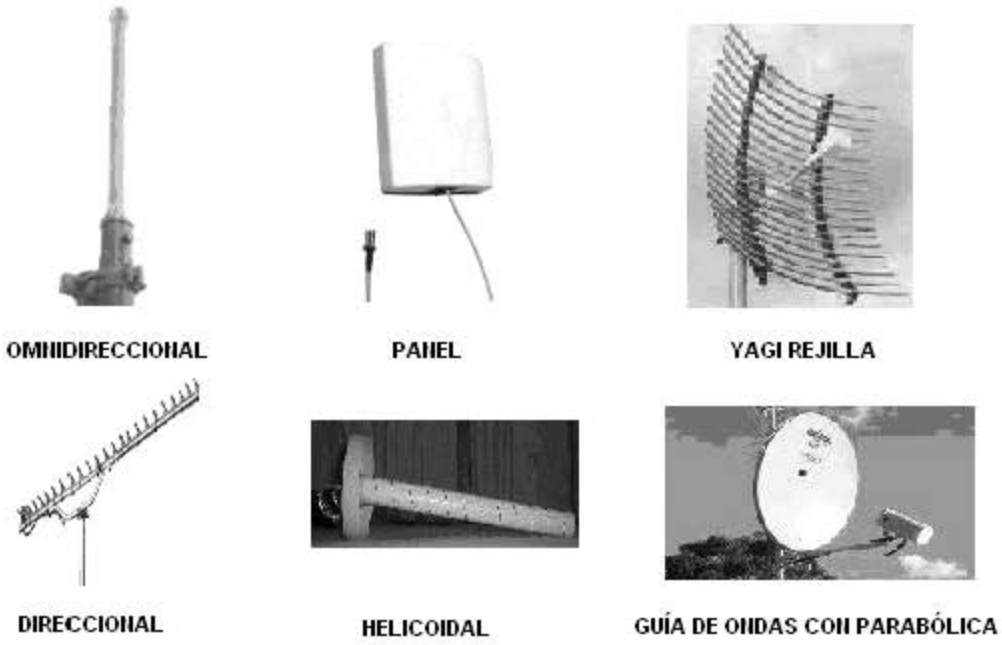


Figura IV.2 Diferentes tipos de antenas

IV.2-Selección y construcción

De acuerdo a nuestras necesidades de conexión, el enlace debe hacerse entre dos sitios en específico, por lo que primeramente se define un enlace tipo punto a punto, el cual corresponde al tipo de antenas direccionales.

Posteriormente la frecuencia de las señales a utilizar, para esto es necesario considerar los dispositivos que se tienen en el mercado para hacer un enlace inalámbrico entre dos computadoras, en nuestro caso para realizar un enlace de tipo inalámbrico.

Una antena de tipo parabólica sería una buena alternativa, pero se tendría un enlace con cobertura mayor a la requerida para nuestros fines, además del soporte demasiado robusto para lograr la altura necesaria (9-10m) y así tener punto de vista entre ambas antenas, incluyendo así un mayor costo y complicaciones de normas por colocación del equipo.

Entre las antenas que se tienen, es necesario elegir una resistente y con el menor peso posible, pero sin olvidar que necesitamos que envíe ondas de 2.4GHz debido a que este espectro de frecuencias es de uso común o en otras palabras es gratis y para no caer en aspectos legales, con una ganancia mínima de 12db esto debido a que la COFETEL nos marca un limite en cuanto a potencia que es de máximo 23db y con una ángulo de apertura lo más reducido posible ya que esto evitara posibles intromisiones de algunos otros nodos que estén en la misma frecuencia.

Para establecer un enlace con esta frecuencia consideramos los requisitos siguientes:

- Dos PC’s O Lap Top
- Dos tarjetas wireless 802.11b con conector de antena externa
- Dos “pigtails” o cable conversor de tipo de conectores
- Cable coaxial y conectores
- Dos antenas
- Los factores que van a condicionar y determinar el funcionamiento y el rendimiento del enlace son los siguientes:
- Potencia de transmisión de las tarjetas
- Calidad de los conectores
- Longitud y calidad del pigtail ó cable conversor
- Longitud y calidad del cable coaxial
- Ganancias y tipos de antenas
- Distancia entre antenas
- Zona de Fresnel
- Condiciones del terreno y meteorológicas

4.3-Análisis para la adquisición de tarjetas

En principio, la opción más “barata” casi siempre es una tarjeta o adaptador wireless, sea tipo PCMCIA, PCI o USB. Las tarjetas son más “baratas” pero presentan el inconveniente de que tienen que estar unidas físicamente a un PC. Los adaptadores USB también han de estar unidos a un PC a través de un cable USB el cual también tiene una longitud máxima determinada.

Los AP ó Access Point, sin embargo, son aparatos independientes capaces de actuar por sí solos si están debidamente configurados. Los AP suelen tener una salida Ethernet la cual enlazaremos con nuestra red de cable o con nuestro equipo directamente, con lo cual no dependen de un PC para funcionar.

Si la distancia entre el PC y la antena es de menos de 100 metros, merece la pena adquirir una tarjeta. Sin embargo, si la distancia entre el PC y la antena es de más de cien metros, el cable coaxial debe de ser de no más de 15 metros y de gran calidad, lo que eleva su costo. Para cubrir esas largas distancias disponemos de la posibilidad de conectar un AP situado en un lugar cercano a la antena, aunque sea en el exterior o a la intemperie (existen modelos diseñados específicamente para ello) y conectar el AP al PC a través de cable UTP, el cual es eficiente y más económico.

Si tomamos esta opción, también se nos plantea la problemática de la alimentación del AP. Para no tener que realizar una instalación eléctrica adicional para el AP, existe la opción de utilizar PoE (Power over Ethernet) lo que consiste en aprovechar el cable UTP tanto para datos como para tensión eléctrica. Existen modelos de AP provistos de esta capacidad.
En nuestro caso intentaremos utilizar tarjetas en ambos puntos del enlace, aunque en uno de ellos la distancia puede llegar a ser algo larga.

Potencia necesaria

Cuanto mayor sea la potencia, mejor será el enlace ya que entre mas potencia en la señal mas distancia puede abarcar el enlace. Aunque la diferencia en mW (miliwatts) es grande entre los dos tipos de tarjeta más comunes (30mW vs. 100mW, lo cual es casi el triple), la diferencia equivalente en dBm no es tan grande (15dBm vs. 20dBm). Por ello será necesario calcular si es suficiente con tarjetas de 30mW.

Potencia de transmisión de las tarjetas
Según la potencia de transmisión de las tarjetas, podemos clasificarlas en dos tipos generales:
30 mW de potencia de transmisión (aprox. 15 dB)
100 mW de potencia de transmisión (aprox. 20 dB)
Cuanto mayor sea la potencia de transmisión, mayor será el alcance del enlace, siempre teniendo en cuenta los demás factores condicionantes como lo son:

- Los obstáculos como árboles, postes y edificios principalmente.
- El clima si es día lluvioso o con mucho aire.

IV.4-Análisis para la adquisición de los conectores utilizados

Calidad de los conectores

Se debe tener cuidado con la realización de las conexiones, adaptaciones y soldaduras de los conectores. Es preferible emplear conectores y herramientas de calidad y ganar en estabilidad del enlace y evitar pérdidas de señal. Para este tipo de cableado se suele utilizar conectores de tipo N.

Longitud y calidad del pigtail

El pigtail es un tramo de cable que en un extremo tiene un tipo de conector que va conectado a la tarjeta (el tipo de conector depende del modelo de la tarjeta) y en el otro extremo tiene un conector al cual conectaremos el cable coaxial. Este conector suele ser de tipo N.

Cuanto más corto y de más calidad sea el pigtail, menor será la pérdida de señal. El pigtail podemos comprarlo hecho o bien hacer uno a la medida de nuestras necesidades. Se aconseja que en ningún caso el pigtail supere los 2 metros de longitud, si bien unos 20cm pueden ser suficientes.

Conectores

Existen multitud de tipos de conectores para cable coaxial, pero quizá el que más nos conviene y el más usado habitualmente sea el de tipo N. Se van a usar los conectores N para las antenas, tanto en macho como hembra ver figura IV.3. Son conectores relativamente fáciles de localizar, y de ellos depende la calidad de un buen enlace. Una mala soldadura, un conector de baja calidad, puede introducir una cantidad importante de pérdidas que hagan imposible establecer un enlace. Hay que recordar que los conectores también tienen pérdidas, no por el conector en sí, sino por el enlace entre el cable y el conector: el estaño, mala sujeción o mala calidad de ambos.

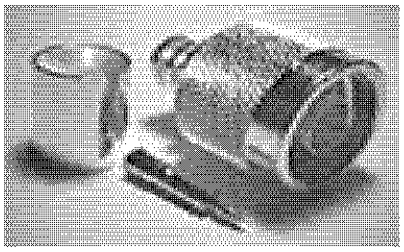


Figura IV.3 Conector tipo N macho.

El conector más importante y también, más caro, es el famoso conector MC, de las AVAYA y ORINOCO ver figura IV.4. Este conector tiene un diámetro de 2 milímetros y 1 centímetro de largo.

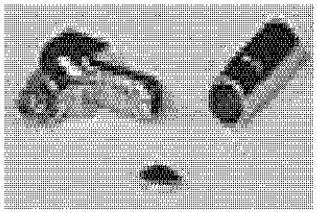


Figura IV.4 Conector tipo MC

IV.5-Cableado

Longitud y calidad del cable coaxial

El cable coaxial es un factor importante para efectuar el tipo de montaje. El coaxial deberá recorrer desde la antena (colocada habitualmente en el exterior del edificio y en el punto más alto de éste) hasta la ubicación del PC (normalmente dentro del edificio). Debemos tener en cuenta:
Cuanto más largo sea el cable coaxial, mayor será la pérdida de señal.

La calidad del cable afecta a la pérdida de señal / metro. Podríamos decir que:
Cable de menor pérdida = cable más grueso y rígido = cable más caro

No existe longitud máxima para el cable coaxial, pero a mayor longitud, mayor pérdida.

A continuación, en la siguiente tabla (Tabla IV.1) se muestra la relación entre modelos de cable LMR y pérdida de señal / metro longitudinal a una frecuencia de 2.4GHz:

Cable	Pérdida en dB/100m
LMR-200	54.2
LMR-240	41.5
LMR-400	21.7
LMR-600	14.2
LMR-900	9.58
LMR-1200	7.27
LMR-1700	5.51

Tabla IV.1 Modelos de cable y perdida de señal

IV.6-Pruebas de conectividad.

Distancia entre antenas

La distancia entre ambas antenas puede calcularse en caso de conocer el resto de factores determinantes. En nuestro caso, conocemos la distancia que queremos cubrir, adaptando entonces el resto de materiales a la distancia.
Cuanto mayor sea la distancia entre antenas, obviamente mayor será la pérdida de señal. La distancia máxima puede variar desde varios metros hasta decenas o cientos de kilómetros. Es altamente recomendado que haya una línea de visión directa entre las antenas.
Podemos calcular la pérdida de señal por propagación entre antenas con la siguiente fórmula:

$P_p = 40 + 20 \cdot \text{Log}(d)$

P_p = Pérdida por propagación en dB

d = distancia en metros entre las antenas

Zona de Fresnel

La llamada zona de Fresnel es una zona de despeje adicional que hay que tener en consideración además de haber una visibilidad directa entre las dos antenas ver figura 4.5. Este factor deriva de la teoría de ondas electromagnéticas respecto de la expansión de las mismas al viajar en el espacio libre. Esta expansión resulta en reflexiones y cambios de fase al pasar sobre un obstáculo. El resultado es un aumento o disminución en el nivel de señal recibido.

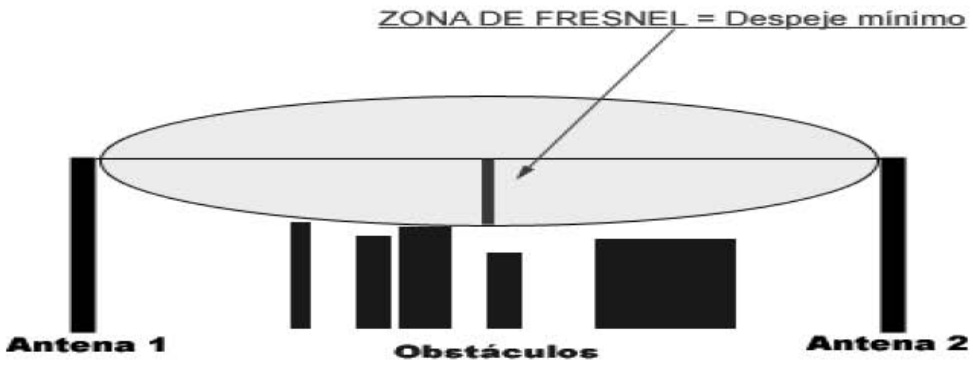


Figura 4.5 Zona de fresnel

Toda la zona de fresnel debe permanecer despejada de obstáculos ya que corresponde a la línea de vista entre las dos antenas.

La tabla IV.2 es de gran ayuda para calcular la zona de Fresnel:

Distancia entre antenas (en Km)	Zona de Fresnel (en metros)
1	3.9
2	5.6
3	7.1
4	8.4
5	9.7
6	11.0
7	12.3
8	13.6
9	15.0
10	16.4
11	17.9
12	19.4
13	21.0
14	22.7
15	24.4
16	26.2
17	28.0
18	29.9
19	31.9
20	34.0
25	45.4
30	58.7

Tabla IV.2 Cálculo de zona de fresnel

Nota: la zona de Fresnel expresada en la tabla IV.2 (la que usaremos en la práctica) es calculada según el 70% de la 1ª zona de Fresnel a una frecuencia de 2.4GHz + la curvatura terrestre para cada distancia.

Condiciones del terreno y meteorológicas

Los árboles, los edificios, tendidos eléctricos, etc. influyen en la recepción de la señal. La señal se reflecta en los objetos y llega con retardo de fase a la antena receptora, pudiendo provocar pérdidas de señal. Podemos corregir este efecto desplazando 6cm longitudinalmente hacia delante o hacia atrás la antena receptora (6cm es la mitad de la longitud de onda, es decir, desde un pico hasta un valle de la senoide).
El hielo y la nieve influyen negativamente en las antenas cuando están en contacto directo con éstas. La lluvia en sí tiene poco impacto sobre la pérdida por propagación, pero en el caso de las antenas “flat-pannel”, puede disminuir su rendimiento si se crea una película de agua en el panel de la antena.

Teniendo en cuenta todos estos factores condicionantes para una buena comunicación procedimos a hacer todo tipo de pruebas de conectividad.

En condiciones meteorológicas como en lluvia, en calor y clima templado así como con presencia de aire y sin éste, todas estas pruebas las colocamos en una tabla de resultados que podremos ver en el capítulo 6 de pruebas y resultados.

NOTA: Para la construcción de una antena casera como la utilizada en este proyecto, en el apéndice IV-1 viene una guía completa de cómo construir este tipo de antena, cabe destacar que este manual de construcción de antenas está basado en el libro ARRL Antenna Handbook que se puede ver dentro de la bibliografía utilizada.

V. Software para comunicaciones

V.1- IPV4, IPTABLES Y TCPDUMP

La tecnología inalámbrica nos puede ayudar a conectar computadoras a distancia. Funciona con tarjetas inalámbricas con un TX/RX interno a 2.4 GHz mientras que la interfaz de software es del tipo Ethernet, con una dirección física diferente para cada tarjeta en el mundo. Normalmente la potencia de transmisión es de 10-20 mW hasta 100mW (ver estándar IEEE 802.11 y licencias FCC/CEPT).

El aspecto más importante en la comunicación inalámbrica es una línea visual clara: se debe ver (a simple vista o con binoculares) una antena desde el otro extremo pudiendo existir entre ambos un pequeño árbol como máximo.

La distancia depende de la antena (y eventualmente de un amplificador) utilizada: de 2 a 300 metros con una antena omnidireccional; 1 Km. con una direccional; de 2 a 3 Km. con una omnidireccional amplificada (200mW); algunos kms. con una antena parabólica. 50 a 60 kms con una antena parabólica o direccional amplificada.

Otro aspecto que debemos tener en cuenta es que no siempre el uso de tarjetas inalámbricas amplificadas es legal en algunos países, pero en nuestro caso (México) nos referimos a las leyes actuales dictaminadas por la COFETEL.

Existen una serie de requisitos para configurar una red inalámbrica;

Requerimientos software:

1. Conceptos generales como dirección IP, máscara de red, enrutamiento, incluidos en el Linux NET3-4-HOWTO
2. Conceptos específicos de red como proxy arp, bridging, proc fs, contenidos en Proxy-ARP-Subnet, Bridge Mini-Howto y en las fuentes del kernel LiNUX (2.2.x o 2.4.x) en Documentation/networking/ ip-sysctl.txt)

3. Conocimientos de red inalámbrica como modo de acceso (ADHOC, INFRAESTRUCTURA y PUNTO DE ACCESO), concepto de canal, definiciones de exterior e interior y algunos más que se pueden encontrar en algunos documentos que tratan sobre redes inalámbricas: estándar IEEE 802.11, CEPT, etc.

Requerimientos no-software:

1. Experiencia mínima en antenas, montaje y orientación
2. Instalación de hardware de PC con especial cuidado en no producir interferencias entre diferentes tarjetas inalámbricas (si es necesario).

5.1.1 Protocolo IP

El protocolo IP es el software que implementa el mecanismo de entrega de paquetes sin conexión y no confiable (técnica del mejor esfuerzo). Se utilizó dicho protocolo por las siguientes características:

1. Define la unidad básica para la transferencia de datos en una interred, especificando el formato exacto de un data grama IP.

2. Realiza las funciones de enrutamiento.

3. Define las reglas para que los Host y Routers procesen paquetes, los descarten o generen mensajes de error.

Además, el protocolo IP se puede utilizar independientemente del sistema operativo que tengamos instalado en los equipos que vamos a comunicar.

5.1.2 IPTABLES

IPtables es un sistema de firewall vinculado al kernel de Linux que se ha extendido enormemente a partir del kernel 2.4 de este sistema operativo. Al igual que el anterior sistema ipchains, un firewall de iptables no es como un servidor que lo iniciamos o detenemos, iptables está integrado con el kernel, es parte del sistema operativo.
Las reglas de firewall están a nivel de kernel, y al kernel lo que le llega es un paquete (digamos, un marrón) y tiene que decidir que hacer con él. El kernel lo que hace es, dependiendo si el paquete es para la propia máquina o para otra máquina, consultar las reglas de firewall y decidir que hacer con el paquete según mande el firewall. Este es el camino que seguiría un paquete en el kernel:

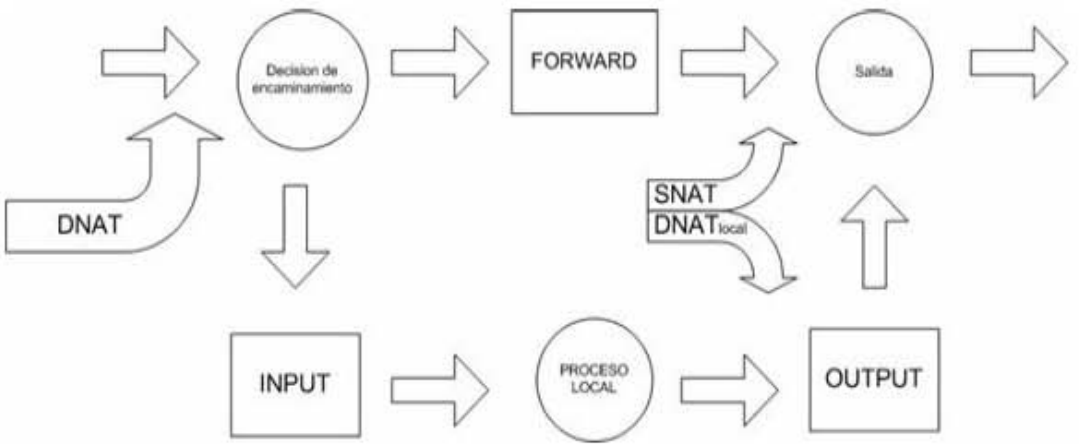


Figura V.1: cuando un paquete u otra comunicación llega al kernel con iptables se sigue este camino.

Como se ve en la figura V.1, básicamente se verifica si el paquete esta destinado a la propia máquina o si va a otra. Para los paquetes (o datagramas, según el protocolo) que van a la propia máquina se aplican las reglas INPUT y OUTPUT, y para filtrar paquetes que van a otras redes o maquinas se aplican simplemente reglas FORWARD.

INPUT, OUTPUT y FORWARD son los tres tipos de reglas de filtrado. Pero antes de aplicar esas reglas es posible aplicar reglas de NAT: estas se usan para hacer redirecciones de puertos o cambios en las direcciones IP de origen y destino.

5.1.3 Tcpdump

Tcpdump (en versión Windows, Windump) son programas cuya utilidad principal es analizar el tráfico que circula por la red. Se apoya en la librería de captura pcap, la cual presenta una interfaz uniforme y que esconde las peculiaridades de cada sistema operativo a la hora de capturar tramas de red.

Lo primero que debemos averiguar cuando estamos usando el tcpdump, son las interfaces que queremos escuchar. Por defecto cuando se ejecuta sin parámetros, en los Linux se pone a escuchar en la eth0, mientras que en Windows hay que especificar la interfaz donde quiere escuchar.

V.2 Comunicación entre las tarjetas inalámbricas

Transmisión inalámbrica

Espectro electromagnético

Cuando los electrones se mueven crean ondas electromagnéticas que se pueden propagar en el espacio libre, aun en el vacío.

La cantidad de oscilaciones por segundo de una onda electromagnética es su frecuencia, f, y se mide en Hz. La distancia entre dos máximos o mínimos consecutivos se llama longitud de onda y se designa con la letra griega λ.
Al conectarse una antena apropiada a un circuito eléctrico, las ondas electromagnéticas se pueden difundir de manera eficiente y captarse por un receptor a cierta distancia. Toda la comunicación inalámbrica se basa en este principio.
En el vació todas las ondas electromagnéticas viajan a la misma velocidad, sin importar su frecuencia. Esta velocidad, usualmente

llamada velocidad de la luz, c, es aproximadamente $3x10^8$ m/seg. Las porciones de radio, microondas, infrarrojo y luz visible del espectro pueden servir para transmitir información modulando la amplitud, la frecuencia o la fase de las ondas.

Radio Transmisión

Las ondas de radio son fáciles de generar, pueden viajar distancias largas y penetrar edificios sin problemas, de modo que se utilizan mucho en la comunicación, tanto de interiores como de exteriores. Las ondas de radio también son omnidireccionales, o sea viajan en todas las direcciones desde la fuente, por lo cual el transmisor y el receptor no tienen que alinearse.

Las propiedades de las ondas de radio dependen de la frecuencia. A bajas frecuencias, las ondas de radio cruzan bien los obstáculos, pero la potencia se reduce drásticamente con la distancia a la fuente. A frecuencias altas, las ondas de radio tienden a viajar en línea recta y a rebotar en los obstáculos. También son absorbidas por la lluvia. Todas las ondas de radio están sujetas a interferencia por los motores y equipos eléctricos. Debido a la capacidad de viajar distancias largas y la interferencia entre usuarios, los gobiernos legislan el uso de radiotransmisores.

Transmisión Por Microondas

Por encima de los 100MHZ las ondas viajan en línea recta y, por tanto se pueden enfocar en un haz estrecho. Concentrar toda la energía en haz pequeño con una antena parabólica produce una señal mucho más alta en relación con el ruido, pero las antenas transmisora y receptora se deben alinear entre sí.

Ondas Infrarrojas

Las ondas infrarrojas se usan mucho para la comunicación de corto alcance. Por ejemplo los controles remotos de los equipos utilizan comunicación infrarroja. Estos controles son direccionales, tienen el inconveniente de no atravesar los objetos sólidos. El hecho de que las ondas infrarrojas no atraviesen los sólidos es una ventaja. Por lo que un sistema infrarrojo no interferirá un sistema similar en un lado adyacente. Además la seguridad de estos sistemas contra espionaje es mejor que la de los sistemas de radio.

Este sistema no necesita de licencia del gobierno para operar en contraste con los sistemas de radio. Esta propiedad ha hecho del infrarrojo un candidato interesante para las LAN inalámbricas en interiores.

Transmisión Por Ondas De Luz

Este tipo de transmisión se ha usado durante siglos. Una aplicación es conectar las LAN de dos edificios por medio de láser montados en la parte más alta de los edificios, esta señalización óptica es unidireccional por lo que cada edificio necesita su propio láser y su propio foto detector. Este esquema ofrece un ancho de banda muy alto y un costo muy bajo. Fácil de instalar y no requiere de licencia. Por ser un haz muy estrecho tiene ventajas pero también es una debilidad. La desventaja es que los rayos láser no pueden penetrar la lluvia ni la niebla densa, funcionan bien en días soleados.

V.3 CONFIGURACIÓN DE LAS TARJETAS INALÁMBRICAS

Las formas de trabajo de las tarjetas wireless tienen básicamente tres opciones: ad-hoc, managed y master.

Ad-hoc: estas redes se construyen normalmente con computadoras con las tarjetas "normales" y se configuran de modo que todas las computadoras de la red trabajan "par a par", todas reciben los paquetes de todas y envían sus propios paquetes a todas las computadoras de la red.

Para esto no se necesita nada especial, sólo definir una red con un nombre (ESSID), preferiblemente encriptar a 128 bits (con WEP) y no tener demasiadas computadoras en la misma red.

Managed: en este caso existe un servidor independiente, Access Point (o Base Station en terminología comercial de Apple) al cual se conectan todas las computadoras. El access point entonces envía las tramas 802.11 a los destinatarios finales. Normalmente los access points soportan roaming, es decir los clientes pueden estar en movimiento e ir cambiando de punto de acceso de acuerdo a la potencia de la señal. La diferencia fundamental entre una tarjeta que soporte ser access point (o modo master) es que hay que hacer bridging de paquetes IP y además manipulan los bits de 802.11 a bajo nivel, normalmente en la propia tarjeta. También los access points suelen ofrecer servicios de enrutado IP, servidor DHCP y bridging sobre una Ethernet. Cuando una computadora o tarjeta está conectado a la red a través de un punto de acceso se dice que está en modo managed.

Master: es el modo en que trabaja el access point descrito en el punto anterior. Como veremos al final, es posible también fabricar un access point con Linux.

Configuración de las tarjetas con: iwconfig

Una vez cargados los módulos del kernel que sean necesarios, la configuración de las tarjetas se hace de forma similar a las Ethernet con el comando ifconfig pero esta vez ayudado con un

nuevo comando, el **iwconfig**, que permite cambiar los parámetros específicos de las redes inalámbricas. Por ejemplo:

- Identificador de red (**essid**)
- Frecuencia o canal (**freq**/**channel**)
- Modo (**mode**: master|managed|ad-hoc)
- Velocidad (**rate**)
- Clave de encriptación (**key**/**enc**)
- Potencia de transmisión (**txpower**)
- etc.

En pocas palabras, con **iwconfig** configuramos los parámetros especiales de wireless y con el **ifconfig** configuramos los parámetros normales de la red IP.

Encriptación

Si especificamos una clave (key) en el iwconfig, las transmisiones estarán encriptadas con el protocolo WEP. En Linux hay dos formas de especificarlas:

1. Con passphrase: iwconfig interface key "s: mi_clave". La clave debe ser de 5 caracteres para encriptación de 40 bits y de 13 para 128 bits (en realidad de clave de 104 bits).
2. Con clave en hexadecimal: iwconfig interface key "mi_clave_en_hexa". En este caso se introduce la clave directamente con 5 o 13 caracteres especificados en hexadecimal.

Para mayor seguridad se recomienda que los caracteres que forman la clave sean aleatorios.

V.4 Configuración de los equipos wireless

El método de acceso al medio de 802.11, a diferencia con 802.3, es MACAW [15]. MACAW es un método de acceso al medio desarrollado a partir del método MACA [16] (Medium Access Collision Avoidance). Consiste en retransmitir tramas antes de hacer la retransmisión real, pidiendo permiso al nodo receptor para hacerla. El emisor emite un mensaje ``Request To Send'', que tiene que ser contestado por el receptor con un mensaje

``Clear To Send'' para poder hacer la retransmisión. Cuando el emisor recibe el mensaje ``Clear To Send'', ya puede hacer la retransmisión real con los datos. Los vecinos que también quieran retransmitir datos, al ver los mensajes ``Request To Send'' y ``Clear To Send'' saben que el canal está ocupado. Cuando una trama de datos acaba de ser retransmitida, el receptor envía un mensaje de acuse de recibo ``ACK'' al emisor, de esta forma los vecinos ya saben que pueden volver a intentar su transmisión. En MACAW también se introduce CSMA/CA a la hora de mandar los mensajes ``Request To Send'':

Una estación que quiera retransmitir, primero escucha el canal para determinar si otra estación está retransmitiendo. Si el canal no está ocupado, la estación retransmitirá el mensaje.

Un problema esencial es que las estaciones no son capaces de detectar la colisión entre dos retransmisiones, por eso se opta por un método de prevención de colisiones. Esta prevención se logra esperando un tiempo aleatorio antes de retransmitir el mensaje cuando se encuentra que el canal no está ocupado. Entre las transmisiones de una estación se deben dejar espacios de tiempo predeterminados. Una vez que ha pasado este espacio, se espera un tiempo aleatorio para volver a escuchar el canal esperando que se libere. Si el canal está ocupado, se vuelve a esperar un espacio de tiempo, pero más reducido al anterior, y así sucesivamente. De esta forma se garantiza una cantidad mínima de colisiones.

Existen varios tipos de dispositivos 802.11, y la más popular es la conocida como 802.11b (*Para conocer mas a fondo el estándar podemos consultar el apéndice II.1*), que alcanza velocidades de transmisión de 11 Mbps. Las redes de este tipo se están extendiendo a un paso muy acelerado, ya que usadas en dispositivos como computadoras portátiles y computadoras de mano les dota al usuario de una gran movilidad y un ancho de banda alto.

Cada tarjeta de comunicaciones de tipo Ethernet posee una dirección de acceso al medio (MAC), que es unívoca. El mecanismo de localización de la ubicación actual del portátil (segundo paso básico del proyecto) se basa exclusivamente en

este hecho: estas direcciones son asignadas por el fabricante de las tarjetas y no pueden ser modificadas a través de software.

Esta localización consiste en el espionaje del tráfico de la red de área local en la que se encuentra la computadora portátil para capturar las direcciones MAC de las máquinas que están conectadas en la red. A partir de estas direcciones, y habiendo configurado correctamente el sistema, este debería ser capaz de determinar donde se encuentra y poder configurar correctamente

la interfaz de red. Las direcciones MAC que se especifiquen en el archivo de configuración deberían ser de máquinas que suelan estar normalmente encendidas y generando tráfico en la red, como servidores de aplicaciones, servidores de Web y servidores de DNS.

Introducción al ``sniffing'': la biblioteca libpcap

El término ``sniffing'' se refiere al espionaje del tráfico de una red por parte de una máquina que captura la información aunque ésta vaya dirigida a otras máquinas, filtrando ésta información para conseguir unos datos en concreto. Para ello, tan solo debe tener acceso al medio físico por el que se transmite la información. Para este propósito se ha estudiado la biblioteca libpcap, que proporciona servicios para el espionaje del tráfico de una red de área local. Ésta biblioteca está escrita para el lenguaje de programación C, y ha sido desarrollada por los mismos autores del conocido programa de espionaje de red llamado Tcpdump [17]. La planificación básica de una aplicación que utilice la biblioteca lipcap es la siguiente:

- Determinar la interfaz por la que se desea realizar el espionaje.
- Inicializar la librería pcap especificándole esta interfaz.
- Determinar qué tipo de información es la que nos interesa ver mediante un filtro, por ejemplo, tan solo los paquetes TCP o los datagramas IP.
- Iniciar el bucle principal de pcap, en el cual se capturan los paquetes. Cada vez que se captura un paquete que se

ajusta a las especificaciones del apartado anterior, se realiza una llamada a una función que se le ha pasado como parámetro en la inicialización. En esta función el programador manejara la información como desee.

- Cerrar la sesión cuando se haya adquirido la información deseada.

El espionaje se puede realizar gracias a que se configura la tarjeta de comunicaciones 802.3 o 802.11 en modo promiscuo, esto es, de modo que pueda recibir las tramas Ethernet aunque no vayan dirigidas a su dirección MAC. De esta forma, la tarjeta de comunicaciones captura todas las tramas Ethernet que se transmitan por el medio físico al que esta tiene acceso (el tramo de red en el caso de 802.3 y el área de cobertura de la red en el caso de 802.11).

15, 16. - The Internet Engineering Task Force. http://www.ietf.org
17.- *Tcpdump Public Repository.* http://www.tcpdump.org

VI. PRUEBAS Y RESULTADOS

En las tablas VI.1 y Vl.2 podemos ver las distancias y los tiempos que tardaron los dos nodos en comunicarse ya sea con un ping, o compartiendo la comunicación a la WLAN.

Estas medidas se tomaron con el fin de darnos una idea de cómo trabaja la tecnología wireless y los dispositivos implementados para la comunicación de estos dos nodos.

La importancia de estas medidas es que la tecnología y los dispositivos que se utilizaron no se habían aplicado para una distancia tan grande por ello, es que tomamos varias medidas para saber su comportamiento y su factibilidad de uso para la solución del problema, las condiciones meteorológicas y ambientales se tomaron en cuenta ya que esta tecnología tiene algunas variaciones por manejar microondas ya que su medio de transmisión es el aire, esto también para saber como ajustar las antenas ya que el aire las mueve y se pierde señal si no tenemos línea de vista, las medidas se tomaron en el día, la tarde y la noche para saber o darnos una idea cercana de a que hora hay mas perturbación.

Observamos que en la tabla hay ciertas medidas que se disparan esto nos llevó a darnos cuenta que el tipo de medición es muy relativo y depende de factores como la distancia, las condiciones meteorológicas, los obstáculos y el tipo de máquinas y dispositivos WiFi que se utilicen, tomando esto en cuenta, para realizar las mediciones tomamos una muestra y utilizamos la estadística, esto es, que para cada medida mostrada, hicimos la medición 10 veces a la misma distancia y esas 10 veces las sumamos y dividimos entre diez y esa medida fue la que plasmamos en las tablas ya que en las mediciones que tomábamos, una o dos salían disparadas así que utilizamos una media para dar este valor.

Entonces los valores tomados en la tabla VI.1 fueron solo para saber que los dos nodos se podían ver o comunicar, y cuando hicimos el enlace, tomamos valores, luego entonces dimos el segundo paso, que era compartir la conexión a Internet generando la tabla VI.2.

Los resultados obtenidos son los que se muestran en las tablas VI.1 y Vl.2, el único medio con el que contamos para comunicarnos a Internet fue un MODEM de 56 kbps, y con variaciones fuertes debido al tipo de conexión vía telefónica, de manera que al lograr la comunicación, nos dio gusto saber que la tecnología que utilizamos dio resultados positivos, esto lo mencionamos, por que esta tecnología relativamente nueva en el país que solo se utiliza para lugares cerrados la pudimos utilizar para conectar dos equipos de cómputo a una distancia de 930 metros con antenas bidireccionales, recursos limitados y con una conexión mas eficiente que un MODEM casero conectado vía telefónica.

Todos los valores que muestran las tablas VI.1 y Vl.2, nos hablan del tiempo que se emplea para que estos dos nodos se comuniquen y compartan conexión a determinadas distancias y con condiciones climatológicas diferentes así pues estas dos tablas son parte del final de un proyecto que iniciamos para compartir conexión a zonas de difícil acceso apoyándonos en la tecnología wireless y los diferentes dispositivos utilizados para lograr el objetivo; en las conclusiones damos nuestro punto de vista acerca de lo logrado y lo que falta por hacer ó mejorar.

Con las medidas mostradas en las tablas VI.1 y Vl.2 podemos observar con claridad que a menor distancia la comunicación entre los dos nodos es mas rápida con respecto al tiempo y a mayor distancia aumenta el tiempo de respuesta de los dos equipos.

Distancia (*metros*)	Sin obstáculos (*milisegundos*)			Con obstáculos (*milisegundos*)								
				Lluvia			**Viento**			**Otros**		
	Día	Tarde	Noche	Día	Tarde	Noche	Día	Tarde	Noche	Día	Tarde	Noche
10	1.96	1.96	1.96	2.00	2.01	2.01	2.10	2.11	2.10	3.00	2.99	2.99
50	1.96	1.96	1.97	2.01	2.01	2.01	2.11	2.11	2.11	3.01	3.01	3.00
100	1.99	1.99	1.98	2.04	2.03	2.03	2.14	2.15	2.15	3.10	3.11	3.11
200	2.00	2.00	2.01	2.10	2.11	2.11	2.20	2.20	2.20	3.20	3.21	3.20
450	2.02	2.03	2.03	2.13	2.15	2.15	2.30	2.30	2.30	3.31	3.33	3.40
620	2.08	2.10	2.10	2.20	2.21	2.21	2.36	2.37	2.37	3.40	3.42	3.42
810	2.15	2.15	2.14	2.28	2.28	2.27	2.41	2.41	2.42	3.50	3.51	3.50
930	2.18	2.19	2.19	2.32	2.31	2.31	2.45	2.45	2.46	3.52	3.54	3.54

Tabla VI.1-Medidas tomadas a diferentes distancias con y sin obstáculos realizando un ping.

Distancia *(metros)*	Sin obstáculos *(segundos)*			Con obstáculos *(segundos)*								
				Lluvia			**Viento**			**Otros**		
	Día	Tarde	Noche	Día	Tarde	Noche	Día	Tarde	Noche	Día	Tarde	Noche
10	5.60	5.63	5.61	7.51	7.51	7.50	8.00	8.01	7.60	9.00	9.00	9.00
50	5.61	5.62	5.62	7.52	7.55	7.53	8.02	8.05	8.02	9.03	9.03	9.05
80	5.66	5.65	5.66	7.56	7.58	7.56	8.08	8.07	8.09	9.08	9.10	9.10
100	5.70	5.70	5.70	7.63	7.62	7.60	8.09	8.10	8.15	9.20	9.15	9.16
200	5.80	5.83	5.80	7.66	7.66	7.67	8.15	8.14	8.17	9.22	9.22	9.24
450	5.86	5.88	5.86	7.71	7.70	7.71	8.20	8.22	8.20	9.25	9.26	9.25
620	5.90	5.92	5.90	7.76	7.76	7.78	8.26	8.27	8.25	9.30	9.35	9.35
810	6.00	6.03	6.00	7.90	7.91	7.91	8.40	8.38	8.36	9.50	9.51	9.48
930	6.20	6.25	6.19	8.00	8.10	8.01	8.48	8.49	8.48	9.70	9.80	9.72

Tabla VI.2-Medidas tomadas a diferentes distancias descargando una trama de 409600kb de Internet con y sin obstáculos

Si tomamos la primera medida que es la de 10 metros y la ultima que fue la de 930 metros que en nuestro caso es con obstáculos (ver tabla Vl.2) tendremos una diferencia en segundos de:

Por ejemplo con lluvia 0.49 segundos por el día, por la tarde seria de 0,59 segundos y por la noche es de 0.51 segundos, esto es medio segundo mas lo que tarda en comunicarse de la ultima medida con respecto a la primera y si observamos las demás medidas van por la misma medida de medio segundo.

Si observamos una vez más las tablas VI.1 y Vl.2 podremos apreciar que sin obstáculos tarda menos tiempo en comunicarse a diferencia que cuando hay obstáculos, ahora si hablamos de que tenemos obstáculos la prueba que tardo menos tiempo en comunicarse fue la de lluvia.

Para nuestro caso tomamos la de otros obstáculos como árboles que interfirieron en el enlace aunque no de manera total ya que solo son ramas las que interfieren y no el tronco esto es si el tronco estuviera en plena interferencia con la línea de vista las ondas de radio chocarían y seria difícil comunicar las computadoras y en el caso de que se pudieran comunicar seria muy tardado el tiempo de respuesta.

Ahora para tener un enlace ideal o lo mejor posible seria que las antenas estuvieran en línea de vista esto es sin obstáculos y por el día según los cálculos que se tomaron y se plasmaron en las tablas VI.1 y Vl.2

CONCLUSIONES

La necesidad de poder compartir información entre dos computadoras que se encontraban en distintos lugares geográficos, nos llevó a buscar alguna alternativa para que pudiéramos llevar a cabo dicha conexión, los equipos que necesitábamos conectar se encontraban a una distancia aproximada de 930 metros uno del otro; por consiguiente una conexión por cable utp no era viable por la distancia, una conexión vpn (Red Privada Virtual) salía de nuestro presupuesto, una conexión por módem es demasiado lenta, además de requerir una línea telefónica, ya que en la zona geográfica en donde nos encontrábamos con los equipos, los proveedores de servicios de Internet de banda ancha no tiene cobertura, esto es: ni Telmex, ni cablemoden, ni siquiera la conexión inalámbrica de mvs nos podían dar el servicio.

Esto nos motivó a investigar el desarrollo de las redes inalámbricas, dado que contábamos con dos equipos portátiles, el primer paso fue documentarnos en el sistema operativo a usar en este proyecto, analizando los posibles candidatos, evaluamos entre sistemas propietario y sistemas de código abierto.

Nuestra primera opción fue utilizar Microsost Windows XP, la principal ventaja es que tiene muy buen soporte en drivers para el hardware que utilizamos, además incluye por default herramientas para la detección de redes inalámbricas, la configuración del dispositivo es relativamente sencilla, y cuenta también con la posibilidad de implementar seguridad para redes inalámbricas utilizando WEP, (protocolo de encriptación para redes inalámbricas).

La principal desventaja es que al ser software de propietario, se tiene que pagar por la licencia de uso, el monto de la

licencia para los fines de nuestro proyecto rebasaba por mucho a nuestro presupuesto, además no es posible implementar los servicios de red que necesitábamos como hacer proxy, firewall y nat de forma nativa con el sistema, esto significa el usar software de terceros, que a su vez también son propietarios. Además existe la posibilidad de que para el hardware que estábamos usando no hubiera controladores actualizados para la versión del Sistema Operativo que queríamos utilizar.

La segunda opción que se analizó fue el sistema operativo MacOS, esa opción fue descartada de inmediato, ya que las plataformas de hardware con las que contábamos eran pc, entonces la incompatibilidad entre el hardware y el software era muy marcada, aunque vimos alternativas como la de correr virtualmente el sistema MacOs en una plataforma PC, la desventaja de hacerlo de esta forma, era que necesitábamos mayor capacidad en el hardware con que contamos, tanto en memoria RAM para que la emulación del SOP corriera con los requerimientos mínimos, por lo que la idea de invertir en mas hardware no era coherente con nuestro presupuesto.

La tercera y última opción analizada fue gnulinux, que es un sistema de código abierto y que se basa en la licencia GPL que marca los lineamientos para poder usarlo, una de las principales desventajas era que no teníamos un conocimiento tan profundo como en los otros sistemas analizados, no sabíamos como instalar el sistema ni como configurar dispositivos y nuestro contacto con linux era muy escaso y se había limitado a haber navegado en Internet con algún explorador.

Pero lo que se nos hizo atractivo fue que no teníamos que pagar alguna licencia por su uso, podíamos tener el sistema y copiarlo y distribuirlo sin caer en la ilegalidad, además encontramos vasta información acerca del sistema y de como

en algunos otros países (principalmente España) las redes inalámbricas montadas en linux habían resuelto problemas similares al que teníamos. Por tanto ya contábamos con algunas nociones para atacar nuestro problema.

En el capitulo III realizamos una comparativa esquematizando los puntos principales que nos llevaron a seleccionar el sistema operativo que utilizamos en nuestro proyecto, las observaciones están basadas en lo equipos con los que contamos (vistos en el capitulo III).

Haciendo la comparativa entre los sistemas operativos propuestos, nos inclinamos hacia linux en primera parte por el costo, aunque tuvimos que invertir más tiempo en el aprendizaje, sin embargo hay demasiada información en la red acerca de linux y de como crear enlaces inalámbricos utilizando cierto tipo de tarjetas.

Por lo tanto invertimos más tiempo en investigación acerca del sistema operativo, desde la instalación, uso y adecuación para nuestro hardware en particular, pero la ventaja es que para los fines que perseguimos, se cumplen las expectativas en cuanto a investigación, aplicación y adaptabilidad de los recursos con los que contamos.

Basándonos en primera instancia en los objetivos particulares, podemos concluir que la tecnología inalámbrica es funcional para lograr una conexión entre dos equipos de cómputo, teniendo en cuenta los dispositivos a utilizar en el enlace entre estos dos puntos, así mismo el software que se utilizó para la implementación de dichos dispositivos.

Sabiéndonos triunfantes debido al enlace con éxito que obtuvimos podemos decir que esta travesía al realizar el trabajo de tesis aquí mostrado podemos expresar una gran satisfacción, ya que para este problema que se nos presentó en esta realidad lo supimos resolver y dar una solución.

Visto lo expuesto en este trabajo de tesis, nos dimos cuenta que una conexión de este tipo, tiene varias ventajas sobre una conexión alámbrica por modem a 56 kbps máximo, por ejemplo las velocidades alcanzadas y registradas en el capítulo 6 de resultados nos pueden dar una idea de la comparativa en cuanto al desempeño en velocidad de conexión entre el enlace alámbrico por modem y el inalámbrico con la tarjeta pcmcia; además es una alternativa para lograr compartir puntos en los que no se tiene acceso a la red de forma "convencional" esto es: ya sea por conexión (modem) o conexión adsl, además que las compañías proveedoras de servicios no tienen la cobertura total del servicio.

Se dota finalmente del servicio de Internet, utilizando la ingeniería respaldada por la tecnología wireless con gran éxito, podemos concluir que dicha tecnología se puede utilizar en varios casos con problemática parecida.

Para mejorar la conexión realizada, se pueden utilizar otro tipo de dispositivos, llámese antenas de mejor calidad, mas potencia y baja pérdida, ya que como se expuso las antenas utilizadas aunque son funcionales son de fabricación casera. No así las últimas mejoras en cuanto a tecnología wireless y una mejor ubicación en cuanto al levantamiento de antenas para que su línea de vista sea lo mejor posible.

Introducción:

La norma 802 fue desarrollada por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) norteamericanos, y versa sobre la arquitectura de redes de datos LAN (Local Area Network). Esta norma establece un estándar de tecnología en el mercado mundial, garantizando que los productos compatibles con dicha norma sean compatibles entre sí.
La norma posee muchos apartados que describen y especifican las distintas funciones que se implementan en una comunicación de datos por una red electrónica de enlaces, por ejemplo:

802 std: Provee las directivas de la norma

802.1b: Define una arquitectura OSI compatible, servicios y protocolos para ser usados en un ambiente LAN/WAN.

802.1d: Especifica una arquitectura y protocolos para la interconexión entre la 802.1b y los puentes MAC (Media Access Control)

802.2: Control de enlaces lógicos

802.3: Métodos de Acceso CSMA/CD y sustratos físicos

802.4: Métodos de accesos a buses "token passing" y sustratos físicos

802.5: Métodos de accesos a "token ring" y sustratos físicos

802.6: Métodos de accesos a buses duales en colas distribuidas

802.9: Integridad de servicios en interfaces LAN con MAC

802.10: Seguridad en LAN/WAN

802.11: Control de accesos a redes inalámbricas ("Wireless") locales (LAN) y sustratos físicos etc. Nosotros nos concentraremos en describir el apartado 802.11 que describe y especifica una interfase inalámbrica para comunicaciones de

datos compatibles con la norma 802. Dentro del apartado 802.11 se establece una subdivisión en las interfases inalámbricas a saber:

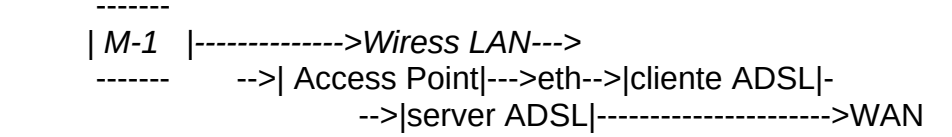
802.11a: Describe interfases inalámbricas en la banda de 5.8 GHz con velocidades de transmisión de datos a 54 Mbps.

802.11b: ídem a la anterior pero ahora en la banda de 2.4 GHz con velocidades de transmisión de de datos a 11 Mbps.

Existe otra subdivisión dentro de esta norma en lo referente a la modulación de datos. Esta describe los métodos DSSS (Direct Sequence Spread Spectrum), FHSS (Frecuency Hoping Sread Spectrum). El mundialmente más usado es el DSSS. Cabe destacar que la banda de 2.4 GHz utilizada en la tecnología 802.11b no está regulada por la CNC y su uso es libre.
La tecnología para la 802.11a está todavía en pañales y se presupone que en el futuro ofrecerá soluciones para el mercado de datos inalámbricos no argentinos, pues está sí está regulada la banda de 5.8 GHz por la CNC.

Aplicaciones Internas:

Se definen así a aplicaciones internas a edificios, oficinas, etc. cuyo radio de acción se limita a distancias menores a los 200 metros. Esto permite ofrecer soluciones de fácil instalación sin tendido de cables y permitiendo la movilidad de las PC. Esto permite el uso de "laptops" en la red LAN para trabajos en inventarios, recolección de datos, etc.
Contratando un servicio Internet ADSL se puede distribuir conectividad a la red WAN por medio de un dispositivo llamado "access point"



Aplicaciones Externas:

Se definen a aplicaciones de largo alcance pudiendo alcanzar radios de acción de varios kilómetros. Entre estas aplicaciones se puede mencionar los enlaces punto a punto de datos a 11 Mbps y servicios de Internet inalámbrica. Esto permite dar servicio de Internet a localidades sin mediar conexión telefónica. Pero siempre existe en estos casos los fenómenos atmosféricos que atenúan en nivel de las señales. Por lo que un diagrama de una topología de servicio es crítica.

Componentes de un sistema 802.11b:

AP (Access Point): Es un punto de acceso a la LAN cableada.

CPE (Customer Premise Equipment): Es un dispositivo que se instala del lado abonado o subscriptor (no AP) para entablar un diálogo con el AP.

Se puede mencionar la existencia de una red cableada tradicional del lado del AP y su conexión Internet. Del lado del CPE se puede mencionar la existencia de una tarjeta inalámbrica su antena. Típicamente un sistema 802.11 se compone de 1 AP y tantos CPE como máquinas deseamos conectar a la red LAN tal que la velocidad de transferencia no decaiga de manera crítica, sino se deberá usar otro AP más.

En aplicaciones externas se recomienda que la trayectoria entre el AP y el CPE esté libre de obstáculos. Esto se lo conoce como "enlace visual" pues uno debe poder ver la antena del otro. Los rangos de coberturas sin repetidores se recomienda que no exceda los 5 Km. Pero esto está supeditado a la infraestructura del sistema. Lo que se recomienda es:

Longitud y tipo de cable instalado entre el CPE y su antena externa, no debe superar los 5 m y cable 9913.

Ganancia de la antena del CPE, debe estar entre los 7 dbi a los 24 dbi.

Ganancia de la antena del nodo donde está ubicado el AP debe ser entre los 6 dbi a los 13 dbi. La antena puede ser cónica omnidirecional horizontal o sectorizada.

El uso de amplificadores bidireccionales en el nodo AP incrementa la cobertura del sistema.

Seguridad en las comunicaciones:

Como la banda de 2.4 GHz no está regulada por la CNC, cualquier usuario/empresa puede instalar un sistema 802.11b. Por ende se debe contar con herramientas de seguridad para evitar no solo interferencias sino intromisiones no deseadas. En general las placas ofrecen varias herramientas nativas como:

Contar con 14 canales de frecuencias seleccionadas dentro de la banda, permitiendo escoger un canal libre de interferencias.

Poseer códigos de encriptación (WEP) entre las comunicaciones con el uso de claves que van desde 40 a 128 bits.

Cada placa posee un número único MAC inmodificable. Asociado con el AP o con el CPE. Luego a nivel de aplicación se puede restringir el acceso a máquinas amigas a la LAN.

Calidad de Servicio:

Cualquier usuario evalúa la calidad del servicio de transferencia de datos en función de cuan veloz (bps) es un enlace. Haciendo referencia a la norma 802.11b la transferencia máxima de datos es de 11 Mbps. Cabe destacar algunas observaciones. En todo protocolo de red los datos se encapsulan en las distintas capas del modelo OSI agregando a los paquetes de datos ciertos contenidos propios conocidos como "overhead". Estos "overhead" cumplen funciones de seguridad, direccionamiento, administración de tráfico, etc. pero no forman parte de los datos a transmitir/recibir. Para fines de la velocidad esto implica una

reducción de la velocidad de transferencia. En la tecnología 802.11b se estima un decaimiento de hasta el 60% de la velocidad de datos procesados por estos "overhead". Por ende el ancho de banda real puede llegar a ser de 4 a 5 Mbps en los peores casos. Puntos a tener en cuenta:

1) En una misma red LAN inalámbrica se recomienda no exceder el uso de más de 3 canales DSSS ó su equivalente a 33 Mbps de tráfico incluyendo los "overhead".

2) Un fenómeno común en esta tecnología es la captura del ancho de banda por ciertos usuarios dejando al resto en la pobreza de recursos. Es decir la norma no establece reglas para el uso inteligente del ancho de banda y gana siempre el primero que toma más.

3) Las tarjetas inalámbricas adaptan la velocidad de transferencia de datos acorde a la relación señal/ruido (en db) recibida. El equipo puede variar la velocidad entre 1, 2, 5.5, y 11 Mbps. Esto debe tenerse en cuenta ya que en casos de mucho ruido y poca visibilidad con el nodo puede ser mucho menores a las deseadas.

802.11g

La nominación de redes inalámbricas "a," "b," y "g" no es indicativa del nivel de resultados que podemos esperar. La primera fue la "b," "a" es la más rápida y "g" marca la diferencia. 802.11g mueve los datos a 54 Mbps, lo que es mucho más rápido que 802.11b. Tanto 802.11g como 802.11b se ejecutan en la frecuencia 2.4 GHz.

Las mejoras en velocidad y la compatibilidad entre "b" y "g" ponen sobre la mesa un extremo muy interesante. En la mayoría de las redes 802.11, los datos se trasladan a través de un dispositivo de hardware llamado punto de acceso (aunque también se denomina, concentradores, router, o estación base).

Hay varios tipos de puntos de acceso. Si en su red utiliza los dos equipos 802.11b y 802.11g, el punto de acceso tiene que ser 802.11g para que la red utilice toda la velocidad que permite 802.11g. El punto de acceso es el lugar de transmisión entre los equipos así que asegúrese de que es tan rápido como el equipo más rápido de toda la red si quiere disfrutar de velocidad. Así que no se gaste el dinero en actualizar uno de los equipo si no actualiza también el punto de acceso.

Tecnología	Velocidad	Inalámbrico	Costo
Ethernet 10/100	100 Mbps	No	Bajo
Gigabit Ethernet	1,000 Mbps	No	Muy alto
802.11b	11 Mbps	Si	Medio
802.11a	54 Mbps	Si	Alto
802.11g	54 Mbps	Si	Medio

Instalando Red Hat Linux 7.2

Instalar paso a paso Red Hat Linux 7.2 desde cero.

Si deseamos instalar Linux en una PC que ya tiene Windows es recomendable tener instalado el programa Boot LILO y utilizar CFDISK para preparar las particiones del disco duro para la instalación de Linux.

Linux necesita al menos 2 particiones creadas en el disco rigido, una partición tipo Linux-Swap que tenga el doble del tamaño de la memoria ram de la PC, y una partición Ext2 o Ext3 con al menos 2 Gb. de tamaño, aunque seria conveniente que fuera mas grande.

Para la elaboración de este documento se tomo nota paso a paso durante el proceso de instalación en una PC con Windows 98 instalado en una Computadora con disco duro de 15 Gb. particionado de la siguiente manera:

partición primaria: FAT32 2 Gb. disco C
partición Linux Swap: 128 Mb.
partición Linux Ext3: 2 Gb.

Configuración del Setup

Entrar al Setup de la PC y seleccionar booteo de CD-ROM, salir del Setup grabando los cambios, insertar el CD Nº 1 de Red Hat 7.2 y Bootear la PC, aparecerá una pantalla con el mensaje "Welcome to Red Hat Linux 7.2", y presionamos Enter.

Selección del Idioma de Instalación

Aparece la primer pantalla en modo gráfico y en idioma inglés, seleccionamos "Spanish" y presionamos "Next”.

Teclado

Ya en español, seleccionamos el modelo y tipo de teclado, por ejemplo 101 teclas Spanish. Hay un renglón donde podemos probar la configuración seleccionada antes de continuar. Para continuar presionamos "Siguiente".

Mouse

Seleccionamos el tipo de mouse conectado a la PC, generalmente el sugerido esta OK. Presionamos "Siguiente".

Bienvenida

Bienvenida en Modo Gráfico, presionamos "Siguiente".

Tipo de Instalación

Seleccionamos "Personalizada" y luego "Siguiente".

Particionamiento del disco duro

Seleccionamos "partición manual con Cfdisk (solo expertos)".

Puntos de Montaje

Aparece el detalle de las particiones del disco duro, hacemos doble click en la partición "Ext2" o "Ext3" que creamos con CFDSIK; En punto de montaje ponemos "/" sin las comillas, y marcamos la opción "Formatear la partición como Ext3", presionamos OK y luego "Añadir de todas maneras" si se nos pregunta.

También podemos hacer click en una partición de Windows a la que queramos acceder desde linux (las particiones de Windows están identificadas con el tipo "VFAT") y en punto de montaje escribimos por ejemplo "/Windows_d", y dejamos la opción "No cambiar (conservar los datos)" para no perder la información que tengamos en la partición de Windows; Presionamos OK y finalmente "Siguiente". Aparecerá un cartel de Advertencia indicando que se borraran los datos en las 2 particiones de Linux, Swap y Ext3, en este caso presionamos "Si" para continuar.

Instalación del Gestor de Arranque

Marcamos las opciones "Utilizar Grub como gestor de arranque", instalar gestor de arranque en: "Primer sector de partición de Inicio", luego presionamos "Siguiente" para continuar.

Contraseña del Gestor Grub

Marcamos la opción "Desea utilizar la contraseña para grub" y colocamos la contraseña deseada, finalmente presionamos "Siguiente".

Configuración de la Red

En caso de que nuestra PC disponga de placa de red aparecerá esta pantalla; se recomienda utilizar IP’s fijas para cada PC, por eso quitamos la marca "configurar utilizando DHCP" y completamos los campos con los siguientes datos:

Dirección IP: 192.168.1.5
Mascara de Red: 255.255.255.0
Red: 192.168.1.0
Broadcast: 192.168.0.255
Nombre del Host: sicanet
Puerta de enlace: 192.168.1.1 (o la IP de la PC que comparte Internet)
DNS primario: 192.168.1.1 (o la IP de PC que comparte Internet, o IP del proveedor de Internet)

Para finalizar presionamos "Siguiente".

Configuración del Firewall

Escogemos el nivel de seguridad "Intermedio", también la opción "Personalizar", marcamos como dispositivo fiable la placa de red de nuestra intranet "eth0" y marcamos las opciones del servidor que deseamos permitir entrada, por ejemplo "www", "smtp", "ftp",

etc. y presionamos "Siguiente" para continuar.

Selección del soporte de Idioma

Para nuestro caso seleccionamos "Spanish (México)" en la lista de idiomas, pero también dejo "Spanish (Spain)" por las dudas. Además selecciono "Spanish (México)" presionando en la flecha hacia abajo en el menú desplegable. Para continuar presionamos "Siguiente".

Selección del uso horario

Se busca en la lista la opción "América/México" o en tu caso la que corresponda a tu ubicación geográfica, y luego presionamos "Siguiente" para continuar.

Configuración de las cuentas

Debemos ingresar la contraseña que deseamos utilizar como administradores "root", y debajo ingresar nuevamente la contraseña para confirmar.
Si lo deseamos podemos agregar algunas cuentas adicionales con el botón "añadir", por ejemplo:
Nombre de usuario: moyete
Nombre Completo: Moyses
Contraseña: la que deseemos
Confirmar Contraseña:
y presionamos "Aceptar". Para finalizar presionamos "Siguiente".

Configuración de la Autenticación

Para nuestro caso dejamos las opciones como están y presionamos "Siguiente" para continuar.

Selección de grupos de paquetes

Marcamos todas las opciones a excepción de: "Servidor News", "Todo". Lo que si marcaremos es "Selección individual de los paquetes". Para continuar presionamos "Siguiente".

Selección individual de paquetes

Hacemos 2 clicks en "Aplicaciones" y luego 1 click en "Base de Datos", marcamos las opciones "mysql", “mysql-devel", y "mysqlclient9".
Volviendo a la visión de carpetas de la izquierda hacemos 2 clicks en "Desarrollo" y luego 1 click en "Lenguajes", buscamos en la lista de la derecha y marcamos las opciones "perl-dbd-mysql", "php-mysql", y "php-odbc", las demás opciones quedan como están, y finalmente presionamos "Siguiente" para continuar.

Configuración de la tarjeta de Video

En este punto seleccionamos la tarjeta de video de nuestra PC, que generalmente es detectada automáticamente por lo que solo debemos presionar "Siguiente" para aceptar lo sugerido y continuar.

Confirmación de Comienzo de Instalación

Al presionar "Siguiente" comenzará la parte automatizada de la instalación de Red Hat Linux 7.2 en nuestra PC; Luego de unos minutos se nos solicitara que insertemos el CD Nº 2, mientras tanto podemos tomarnos un café y relajarnos.

Creación del diskette de arranque

Insertamos un diskette en la unidad A: y presionamos "Siguiente".

Selección del Monitor

En la mayoría de los casos se detectara automáticamente el monitor que tengamos en nuestra PC y sólo deberemos presionar "Siguiente" para continuar.

Personalizar la configuración de X

Si lo deseamos podemos presionar el botón "Comprobar la configuración" para asegurarnos que tenemos el video y monitor bien configurados; Si vemos bien la pantalla de prueba respondemos "Si" a la pregunta. Luego Marcamos la Opción "KDE" y "Modo Gráfico", Para finalizar presionamos "Siguiente".

Reiniciando la PC

Retiramos el Cd de RH 7.2, el diskette de unidad A: y presionamos el botón "Salir" para finalizar con la instalación. El CD se expulsara solo luego de presionar "Salir".

Primer Booteo con Linux

Tendremos la opción de arrancar con Windows o Linux, elegimos esta última opción. Luego del proceso de arranque normal de Linux nos aparece una pantalla en modo gráfico solicitando usuario y contraseña, alli ingresamos usuario (login) "root" y la contraseña (password) que elegimos con anterioridad y presionamos "GO".

Primer ingreso al entorno de escritorio KDE

Aparecerá la ventana de un programa "Asistente de configuración" o "Desktop Settings Wizard", presionamos el botón "Next" en las 5 pantallas que van apareciendo, y finalmente el botón "Finish".

Consejos útiles de Kandalf

Como el nombre lo indica es una ventana que muestra consejos para utilizar el entorno de escritorio KDE. Cerramos la ventana con el botón "Cerrar", y si lo deseamos le sacamos la opción de ejecutar al inicio de sesión.

Finalizar la Sesión y salir de Linux

Para finalizar la sesión, reiniciar o apagar el equipo seleccionamos con el mouse el primer icono abajo a la izquierda, sobre la barra de tareas (el que tiene un engranaje con la letra K) y luego la opción "Terminar" del menú desplegado. Respondemos "Terminar" a la pregunta "Terminar la sesión KDE?".
Nota: para apagar el equipo seleccionamos en la pantalla que nos pide usuario y contraseña, la opción "Shutdown" y luego "OK". Y para Reiniciar seleccionamos "Shutdown", luego "Reboot" y finalmente "OK".

Cómo montar una red wireless con Linux

Redes Wireless con Linux

Las redes Wireless 802.11b, de 11 Mbps están convirtiéndose en una opción muy válida y popular en los últimos meses. Además que los precios han bajado notablemente, dan una enorme comodidad si tenemos varios ordenadores en casa y el soporte que hay en Linux es muy potente y variado. En éste artículo explicamos las diferentes opciones y como instalarlo y configurarlo en Linux. Aunque sin duda la estrella es, al menos para nosotros, **como montar un *access point wireless* en Linux con una tarjeta PCMCIA normal, corriente y barata.**

.

Introducción

Como veremos en este artículo, con Linux se pueden hacer muchas cosas que son imposibles en sistemas operativos propietarios, como por ejemplo construir un *Access Point* basado en Linux a partir de una tarjeta Conceptronic (Chipset PRISM2) bastante barata y que no está, en principio, preparada para hacer de *Master (o access point)* de una red.

Las forma de trabajo de las tarjetas wireless tienen básicamente tres formas: *ad-hoc* y *managed* y *master*.

Ad-hoc: estas redes se construyen normalmente con ordenadores con las tarjetas "normales" y se configuran de modo que todos los ordenadores de la red trabajan "par a par", todos reciben los paquetes de todos y envían sus propios paquetes a todos los ordenadores de la red. Para esto no se necesita nada especial, sólo definir una red con un nombre (ESSID), preferiblemente encriptar a 128 bits (con WEP) y no tener demasiados ordenadores en la misma red.

Managed: en este caso existe un servidor independiente, *Access Point* (o *Base Station* en terminología comercial de Apple) al cual se conectan todos los ordenadores. El *access point* entonces envía las tramas 802.11 a los destinatarios finales. Normalmente los *access points* soportan *roaming*, es decir los clientes pueden estar en movimiento a ir cambiando de punto de acceso de acuerdo a la potencia de la señal. La diferencia fundamental entre una tarjeta que soporte ser *access point* (o *modo master*) es que hay que hacer bridging de paquetes IP y además manipulan los bits de 802.11 a bajo nivel, normalmente en la propia tarjeta. También los *access points* suelen ofrecer servicios de enrutado IP, servidor DHCP y bridging sobre una Ethernet. Cuando un ordenador o tarjeta está conectado a la red a través de un punto de acceso se dice que está en modo *managed*.
Master: es el modo en que trabaja el access point descrito en el punto anterior. Como veremos al final, es posible también fabricar un *access point* con Linux.

Módulos del kernel

La mayoría de las tarjetas que se venden actualmente son del tipo Orinoco (Lucent), Symbol HR y Prism 2. Todas ellas están soportadas por el driver **orinoco_cs** incluido en el kernel 2.4.x, pero **sólo para trabajar en modo managed o ad-hoc**, no soportan el modo *master*.
Además tienen un pequeño problema, los drivers no están del todo actualizados con la última versión y cuando la tarjeta comparte interrupciones con otros dispositivos genera un montón de líneas de logs por "eventos vacíos". Este problema ya está solucionado en las últimas versiones que se pueden bajar de **http://ozlabs.org/people/dgibson/dldwd/** y compilarlos. Es bastante sencillo y el README lo explica claramente.
Pero como veremos más adelante, existen otras opciones, los nuevos **linux-wlan-ng** o el fantástico **driver para Prism2** (i.e. los usados por Conceptronic) que nos permitirán hacer que nuestro Linux se convierta en un *access point* de muy bajo costo si tenemos una tarjeta Prism2 de Intersil.

Configuración de las tarjetas: iwconfig

Una vez cargados los módulos del kernel que sean necesarios, la configuración de las tarjetas se hace de forma similar a las Ethernet con el comando ifconfig pero esta vez ayudado con un nuevo comando, el **iwconfig**, que permite cambiar los parámetros específicos de las redes inalámbricas. Por ejemplo:
Identificador de red (**essid**)
Frecuencia o canal (**freq**/**channel**)
Modo (**mode**: *master*|*managed*|*ad-hoc*)
Velocidad (**rate**)
Clave de encriptación (**key**/**enc**)
Potencia de transmisión (**txpower**)
etc.
En pocas palabras, con **iwconfig** configuramos los parámetros especiales de wireless y con el **ifconfig** configuramos los parámetros normales de la red IP.

NOTA sobre encriptación

Si especificamos una clave (key) en el iwconfig, las transmisiones estarán encriptadas con el protocolo WEP. En Linux has dos formas de especificarlas:
Con passphrase: iwconfig interface key "s:mi_clave". La clave debe ser de 5 caracteres para encriptación de 40 bits y de 13 para 128 bits (en realidad de clave de 104 bits).
Con la clave en hexadecimal: iwconfig interface "mi_clave_en_hexa". En este caso se introduce la clave directamente con 5 o 13 caracteres especificados en hexadecimal.

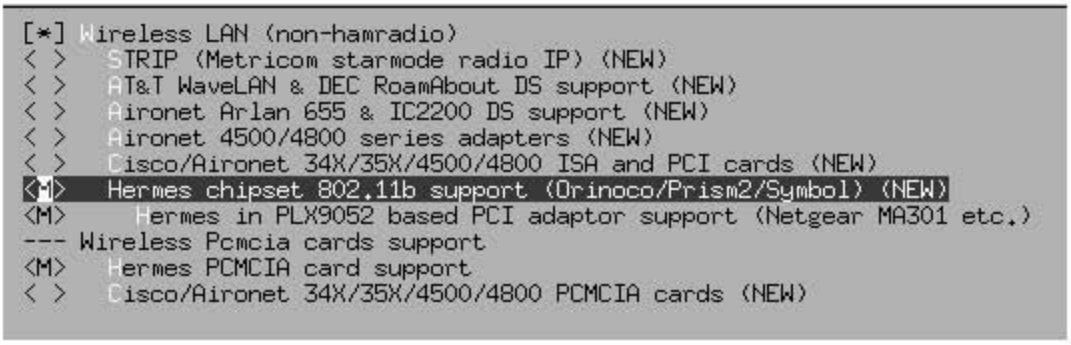
Para mayor seguridad se recomienda que los caracteres que forman la clave sean aleatorios.

Usuarios de Mac OS X

Para introducir la clave en el gestor del Airport del Mac OS X, hay que hacerlo con los caracteres en hexadecimal poniendo un **$** al principio.

Configuración de un cliente Linux (*Managed* o *infraestructure*)

Vayamos primero a lo más simple: **ya tienes un *access point*** y quieres hacer funcionar tu tarjeta PCMCIA en tu Linux, en este caso se llama modo "infraestructura".
Quizás hayas comprado la tarjeta con un adaptador PCI, en ambos casos tienes que habilitar el soporte Cardbus en el kernel. Para ello tienes que ir a "**General Setup:PCMCIA CardBus Support**" y seleccionar "**Cardbus Support**".
Ahora tienes que seleccionar los drivers orinoco_cs, para ello vas a "**Networking Device Support:Wireless LAN (non-hamradio)**" y seleccionar las opciones y subopciones del "**Hermes Chipset 802.11 support (Orinoco/Prism/Symbol)**".



Ahora deberías compilar el kernel y asegurarte que tienes instalado los paquetes para soporte PCMCIA, deberías tener un directorio /etc/pcmcia/ con varios archivos ahí dentro. Si tienes eso y el kernel compilado e instalado, sólo hace falta configurar la red. Yo trabajo normalmente en Debian, pero también explicaré las diferencias en la configuración para RedHat.

Debian (PCMCIA)

La configuración de la red en Debian puede hacerse directamente en los archivos .opts de /etc/pcmcia.

Primero hay que hacer que reconozca automáticamente la tarjeta Conceptronic, para ello hay que editar el archivo

/etc/pcmcia/config.opts y agregar lo siguiente para que reconozca la tarjeta y cargue el módulo orinoco:

```
card "Conceptronic Wireless"
 version "802.11", "11Mbps Wireless LAN Card"
 bind "orinoco_cs"
```

Ahora hay que editar el archivo /etc/pcmcia/wireless.opts y poner las siguientes líneas:

```
*,*,*,*)
 INFO="Nombre..."
 ESSID="Nombre_de_red"
 MODE="Managed"
 RATE="auto"
# La clave se pone si es encriptada
 KEY="s:mi_clave"
 ;;
```

Ahora en el /etc/pcmcia/networks.opts hay que poner los datos de la red IP:

```
case "$ADDRESS" in
*,*,*,*)
 INFO="Nombre...."
 # Transceiver selection, for some cards -- see 'man ifport'
 IF_PORT=""
 # Use BOOTP (via /sbin/bootpc, or /sbin/pump)? [y/n]
 BOOTP="n"
 # Use DHCP (via /sbin/dhcpcd, /sbin/dhclient, or /sbin/pump)? [y/n]
 # Solo si tenemos DHCP
 DHCP="y"
 ...
 # Host's IP address, netmask, network address, broadcast address
 # Solo si no tenemos DHCP
 #IPADDR="192.168.0.130"
 #NETMASK="255.255.255.128"
 #NETWORK="192.168.0.128"
 #BROADCAST="192.168.0.255"
 # Gateway address for static routing
 #GATEWAY="192.168.0.1"
 # Things to add to /etc/resolv.conf for this interface
...
```

Debian (PCI y Airport)

En caso que la tarjeta no sea una PCMCIA, es decir tengamos un Apple con tarjeta Airport o una con adaptador PCI, la configuración en Debian se hace directamente en el /etc/network/interfaces. Por ejemplo:

```
auto eth1
# ejemplo con dhcp
iface eth1 inet dhcp
 #address 192.168.0.140
 #netmask 255.255.255.0
 #network 192.168.0.0
 #gateway 192.168.0.1
 wireless_essid Nombre_de_red
 wireless_mode Managed
 wireless_key s:mi_clave
 wireless_rate auto
 wireless_nick sofi
```

Red Hat

Red Hat usa una filosofía diferente (al menos en la versión 7.2), en vez de configurar la red dentro de los archivos en /etc/pcmcia, lo hace en los mismos archivos donde se configuran las interfaces de red, en /etc/syconfig/network-scripts/ifcfg-ethX. Por lo tanto los parámetros de red hay que configurarlos en dichos archivos, por ejemplo:

```
DEVICE=eth1
MODE=managed
ESSID="Nombre_de_red"
RATE=auto
TXPOWER=auto
KEY="s:mi_clave" # Solo si va encriptado
BOOTPROTO=static
IPADDR=192.168.0.3
BROADCAST=192.168.0.255
NETMASK=255.255.255.0
NETWORK=192.168.0.0
ONBOOT=yes
```

Configuración de Redes *ad-hoc*

La configuración de un red ad-hoc permite montar una red entre pocos ordenadores sin necesidad de contar con un access point. El modo de funcionamiento es peer-to-peer, todos los ordenadores reciben los paquetes enviados por algunos de ellos. Por eso una red de tipo ad-hoc funciona bien cuando hay pocos ordenadores.

La única diferencia en cuanto a configuración es que hay que poner modo ad-hoc en vez de managed. Por ejemplo:

```
iface eth1 inet dhcp
 #address 192.168.0.140
 #netmask 255.255.255.0
 #network 192.168.0.0
 #gateway 192.168.0.1
 wireless_essid Nombre_de_red
 wireless_mode ad-hoc
 wireless_key s:mi_clave
 wireless_rate auto
 wireless_nick sofi
```

Conectividad entre la wireless y la Ethernet

¿Quieres que haya interconectividad entre los ordenadores con wireless y los conectados a la Ethernet? Ésta es una de las importantes tareas realizadas por los access-points.

Si piensas hacer algo de lo que se explica a continuación, es necesario conocer los fundamentos de funcionamiento de redes IP y Ethernet (para eso están los cursos de redes en la Universidad, FP o academias de informática :-). Si no tienes idea no intentes entender lo que viene a continuación, llama a un amigo que sí sepa de redes y/o ponte a estudiar de cursos o tutoriales disponibles en Internet.

En caso que montes una red ad-hoc, necesitas que uno de los ordenadores con una interfaz inalámbrica y otra Ethernet se encargue de ese trabajo de enrutado. Por suerte, el protocolo IP está basado totalmente en software y el Linux es capaz de hacer dichas tareas de enrutado IP. En este caso te recomiendo que aprendas enrutamiento IP y configures dos redes IP distintas,

una será la Ethernet y la otra la wireless. Uno de los Linux deberá hacer el enrutado IP.

Pero además hay otras opciones que trabajan a niveles más bajos y que permiten tener una sola red IP a partir de dos redes físicas distintas:

- Proxy arp: Para que dos ordenadores en una LAN Ethernet con TCP/IP puedan comunicarse necesitan conocer la dirección MAC (Ethernet) del otro ordenador. De estar tarea se encarga el protocolo ARP, que mediante paquetes broadcast averiguan y crean un tabla que relaciona direcciones IP con direcciones MAC (probar el comando arp -a). El Linux soporta proxy arp por defecto, sólo hay que configurarlo mediante las variables disponibles en /proc.
- Bridging: El bridging es una opción más avanzada que el proxy arp, y se necesita opciones especiales del kernel además del paquete bridge-utils. Si deseas esta opción, mira como se configura el bridge en la sección que viene a continuación (Configuración de Linux como un Access Point).

Configuración de Linux como un Access Point

NOTA: Montar un access point, con todos sus requerimientos, no es algo trivial (para los usuarios de Windows: no piensen que en Windows sería más fácil, ahora mismo es imposible hacer en Windows lo que explico aquí, no os queda más opción que comprar un Access Point), sino que hay que saber de redes y configurar y compilar el kernel como así también sentirse cómodos usando las utilidades y configurando PCMCIA. Si no es así, quizás no entiendas lo que se explica a continuación, es mejor que empieces con algo más sencillo, como lo explicado en los pasos anteriores, o que te ayude "en vivo" algún amigo que ya lo haya hecho.

Mi filosofía es que cuando no se conoce algo y hay que aprender, hay que hacerlo paso a paso, desde lo más fácil a lo más complejo. Aunque en mis primeras pruebas con wireless en Linux pasaron por todas las etapas explicadas anteriormente, mi objetivo desde el principio era poder tener un access point corriendo en Linux.

Debo decir que he tenido mucha suerte, ya que las tarjetas que compré, la Conceptronic PCI C11iDT:

y la Conceptronic PCMCIA Airbridge 11CC:

ambas (como creo que todas las Conceptronic, por cierto, el Web que tienen es realmente lamentable para el tipo de empresa que son), usan el chipset Prism2.5 de Intersil. Digo que he tenido mucha suerte porque he encontrado que un grupo de pirados liderados por Jouni Malinen están desarrollando un excelente módulo de Linux para las Prism2 (Host AP) que permite trabajar en modo Master, aunque el fabricante diga que no se puede.

```
[gallir@ponti gallir]$ /sbin/iwconfig wlan0
wlan0 IEEE 802.11-DS ESSID:"Antoli" Nickname:"ponti"
 Mode:Master Frequency:2.422GHz Access Point: 00:50:C2:01:96:14
 Bit Rate:2Mb/s Tx-Power=20 dBm Sensitivity=1/3
 Retry min limit:8 RTS thr:off Fragment thr:off
 Power Management:off
 Link Quality:0 Signal level:0 Noise level:0
 Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
 Tx excessive retries:3167 Invalid misc:2038 Missed beacon:0
```

Así que al final he logrado lo que quería, la tarjeta PCI que había instalado en mi Linux de mesa funcionó en modo Master y pude interconectar ordenadores con Linux en PC e iBook, Mac OS X y del innombrable, con encriptación WEP de 128 bits.

Como la tarjeta PCI es sólo una PCMCIA con un adaptador, la saqué del adaptador y terminé instalándola en un portátil muy antiguo (P133, 32 MB RAM) para que me hiciese de servidor de acceso para toda la red de casa, con bridging, servidor DHCP y control de direcciones MAC:

```
[gallir@ponti gallir]$ ps ax
 PID TTY    STAT TIME COMMAND
 1   ?      S   0:03 init [3]
 2   ?      SW  0:00 [keventd]
 3   ?      SW  0:00 [kapmd]
 4   ?      RWN 0:00 [ksoftirqd_CPU0]
 5   ?      SW  0:06 [kswapd]
 6   ?      SW  0:00 [bdflush]
 7   ?      SW  0:00 [kupdated]
 8   ?      SW  0:01 [kjournald]
 228 ?      S   0:02 /sbin/cardmgr
 694 ?      S   0:05 syslogd -m 0
 699 ?      S   0:03 klogd -2
 831 ?      S   0:00 /usr/sbin/apmd -p 10 -w 5 -W -P...
 851 ?      SL  0:00 ntpd -U ntp
 933 ?      S   0:33 /usr/sbin/sshd
```

```
 984  ?      S   0:00 gpm -t ps/2 -m /dev/mouse
 1002 ?      S   0:00 crond
 1038 ?      S   0:00 /usr/sbin/atd
 1045 tty1   S   0:00 login -- root
 1046 tty2   S   0:00 login -- root
 1047 tty3   S   0:00 /sbin/mingetty tty3
 5636 ?      S   0:04 /usr/sbin/dhcpd
 5835 tty1   S   0:00 -bash
 6734 tty2   S   0:00 -bash
 7691 ?      S   0:03 /usr/sbin/sshd
 7692 pts/0  S   0:00 -bash
 7905 pts/0  R   0:00 ps ax
[gallir@ponti gallir]$ /sbin/lsmod
Module        Size Used by
hostap_cs    82496 1
3c574_cs      8400 1
ds            6384 2 [hostap_cs 3c574_cs]
yenta_socket  8368 2
pcmcia_core  38016 0 [hostap_cs 3c574_cs ds yenta_socket]
```

También he probado el mismo portátil con la otras tarjetas Conceptronic que compré (la PCMCIA de la segunda foto) y funciona perfectamente, aunque su alcance es levemente inferior debido a la antena pequeña incluida, pero aún así la red funciona

a 11 mbps en todo el piso a pesar de que la portátil está en una mala ubicación.

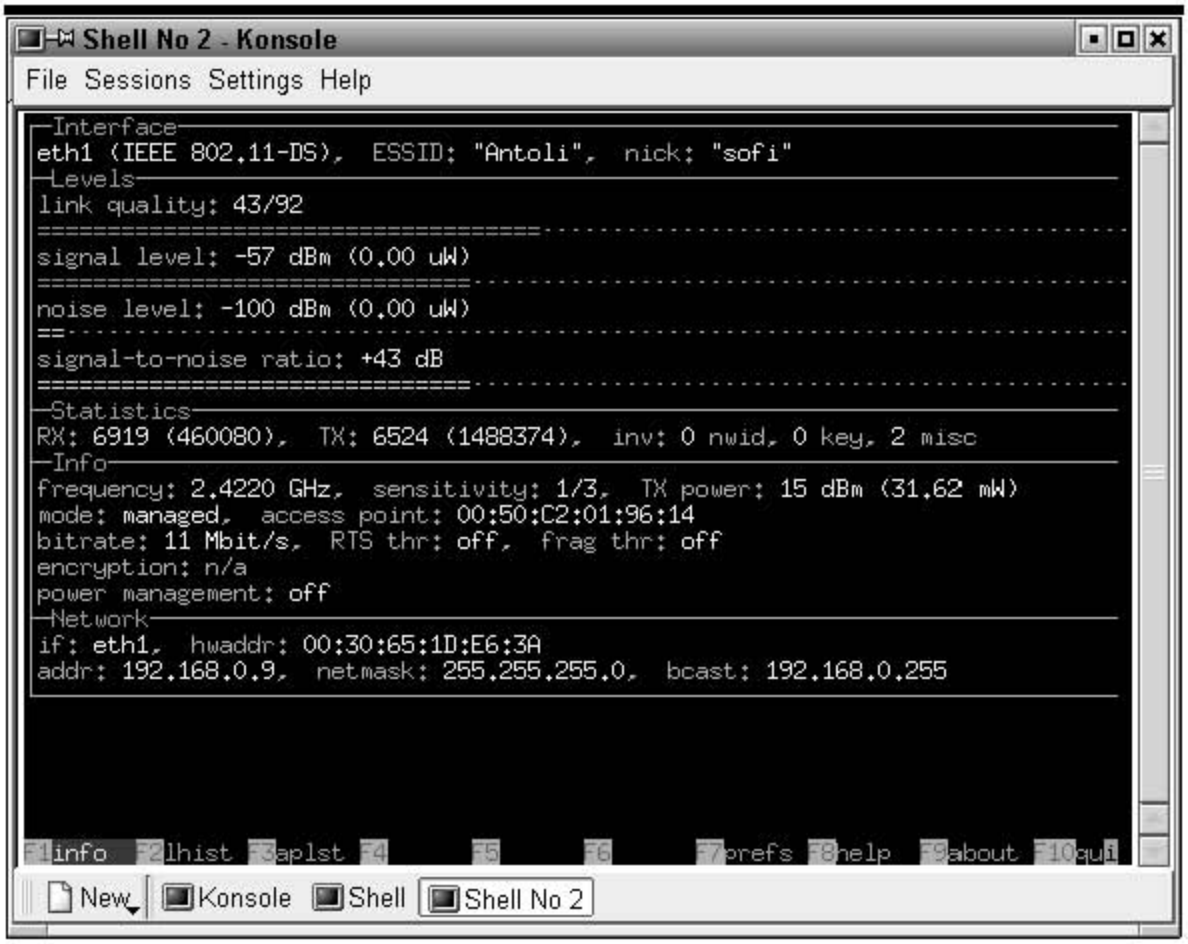
Instalación del módulo Host AP

En la página web del Host AP y en el README del software (un tgz) está bien explicado como instalar el módulo hostap en sus distintas variantes, especialmente PCMCIA y PCI. Básicamente hace falta los fuentes del kernel que se está usando (se pone el path en el Makefile), luego sólo hay que compilarlo y hacer un make install para que instale los módulos en el directorio correspondiente (/lib/modules/2.4.18/pcmcia/ en mi caso) y el archivo de configuración de la PCMCIA (hostap_cs.conf) en el directorio /etc/pcmcia .

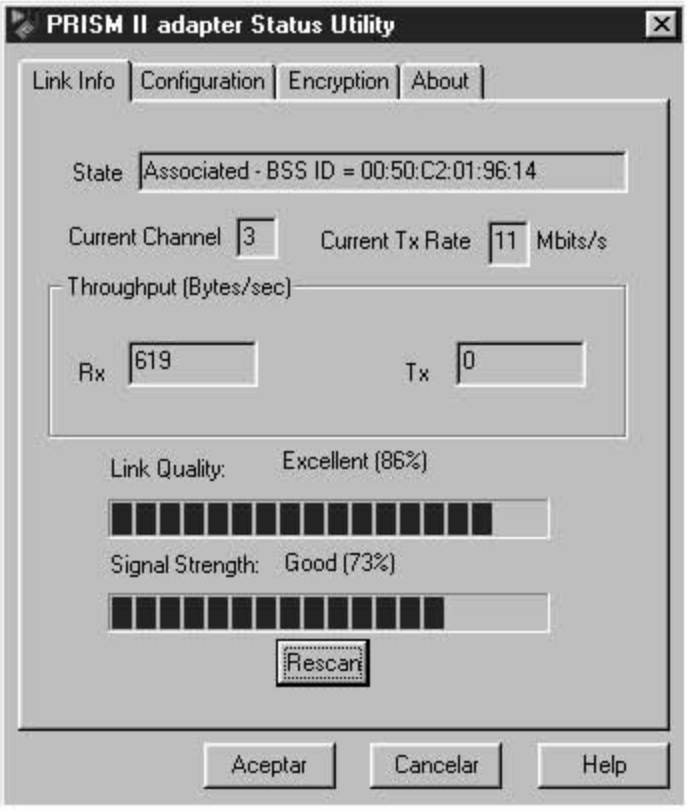
Una vez instalado, si usamos la opción PCMCIA (seguramente sí, aunque tengamos el adaptador PCI) debemos indicar a los módulos del PCMCIA que cuando detecte esa tarjeta cargue el módulo hostap_cs.

Para ello editamos el archivo /etc/pcmcia/config.opts y ponemos las siguientes líneas:

```
card "Conceptronic Wireless"
 version "802.11", "11Mbps Wireless LAN Card"
 bind "hostap_cs"
```



wavemon sobre un Linux en el Apple iBook con Airport conectado el Access Point



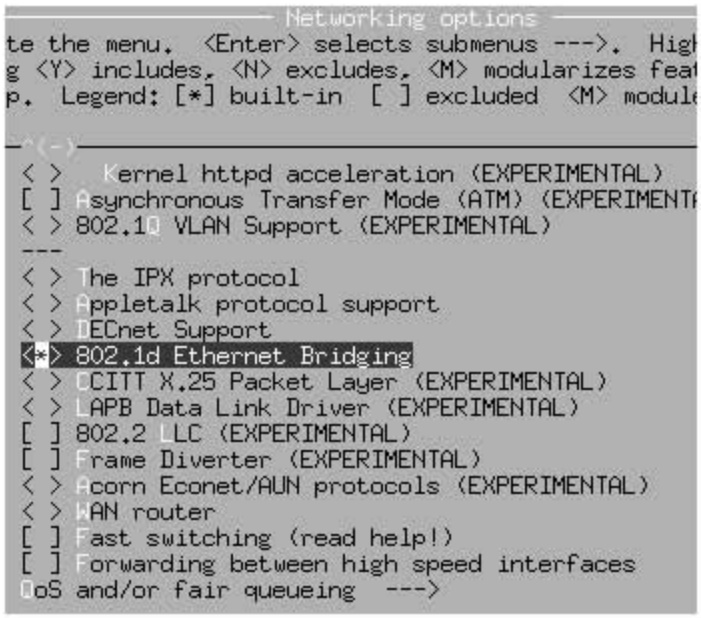
Este es el Windows de mi hija, en su habitación, también con una tarjeta Conceptronic conectado a la red wireless a través del Linux AP

Con eso ya tenemos casi todo lo referente a drivers, ahora hay que configurar la red.

Bridging

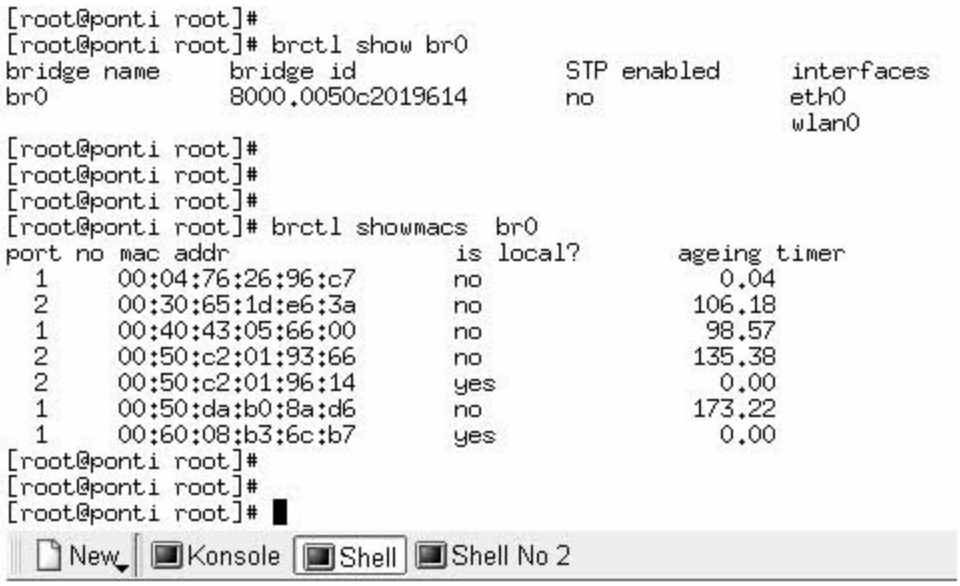
Como comenté anteriormente, no basta con poner la tarjeta en modo Master para tener un access point, sino que hay además interconectar la red Ethernet y la inalámbrica. Yo opté por hacer bridging entre ambas redes, así trato toda la red de mi casa como si fuese una sola, sin preocuparme en dar direcciones IP de distintas redes si estoy conectado por Ethernet o Wireless.

Para hacer bridging en Linux hay que habilitar dicha opción en el kernel:



Luego hay que instalar el paquete bridge-utils que está disponible en Debian (en Red Hat hay que buscarlo en rpmfind.net, cuando yo lo hice sólo estaba disponible en la versión RawHide pero me funcionó perfectamente sobre una RedHat 7.2).

El programa principal de dicho paquete, brctl, permite crear y configurar interfaces virtuales que incluyen las interfaces sobre las que se aplicará el bridging.



En la imagen de arriba se puede observar primero la configuración del bridge definido (br0), que incluye a las interfaces eth0 y wlan0 (en el módulo hostap las interfaces wireless se denominan wlanX). Veréis que he deshabilitado el spanning tree protocol ya que en mi red estoy seguro que no hay bucles (es muy simple), pero si tú no lo estás, déjalo habilitado.

A continuación se puede observar (con el argumento showmacs) los ordenadores conectados a cada red, la 1 es la Ethernet y la 2 es la wlan0. Las marcadas como local son las interfaces del servidor, las demás son las remotas.

ATENCIÓN: las interfaces que forman parte de un bridge no deben tener ninguna dirección asignada, en los archivos de configuración de la tarjeta hay que ponerle una IP 0.0.0.0 en vez de una IP real, ya que deben trabajar en modo promiscuo.

Definición del br0 en Debian

En Debian es muy fácil configurarlo, ya que el /etc/network/interfaces es muy flexible y potente, en mi caso sólo tuve que poner

```
auto br0
iface br0 inet static
 address 192.168.0.10
 netmask 255.255.255.0
 network 192.168.0.0
 gateway 192.168.0.1
 bridge_ports eth0 wlan0
 bridge_stp off
 bridge_maxwait 5
```

Les recomiendo leer además lo de RedHat para entender mejor el procedimiento completo.

Definición del br0 en Red Hat

En Red Hat es un poco más complicado por dos razones, no hay un archivos interfaces como en Debian y además las tarjetas de red PCMCIA se configuran siempre desde el /etc/sysconfig/network-scripts/ifcfg-xxx. Pero yo le hice un truco bastante sucio, tengo un ifcfg-eth0, ifcfg-wlan0 y ifcfg-zbr0 (el z lo pongo para que se llame después de llamar a los de las interfaces). El contenido de cada archivo es:

/etc/sysconfig/network-scripts/ifcfg-eth0

```
DEVICE=eth0
IPADDR=0.0.0.0
BOOTPROTO=static
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-wlan0

```
DEVICE=wlan0
MODE=Master
ESSID=Antoli
RATE=auto
TXPOWER=auto
KEY="s:mi_clave"
BOOTPROTO=static
ONBOOT=yes
/usr/bin/prism2_param wlan0 host_decrypt 1
```

NOTA: Con la ejecución de "/usr/bin/prism2_param wlan0 host_decrypt 1" estoy obligando a hacer el desencriptado WEP de las tramas en el propio driver, por software, en vez de hacerlo en la tarjeta. La conveniencia o no de usarlo depende de la tarjeta que uséis y la versión del driver. O sea, probadlo, quizás vuestra tarjeta no funcione con encriptación de 128/104 bits sin esa opción. El comando prism2_param es un script incluido en el paquete hostap y sirve para simplificar las llamadas al iwpriv para cambiar parámetros de la tarjeta.

/etc/sysconfig/network-scripts/ifcfg-zbr0

```
/usr/sbin/brctl delif br0 eth0
/usr/sbin/brctl delif br0 wlan0
/usr/sbin/brctl delbr br0
/usr/sbin/brctl addbr br0
/usr/sbin/brctl addif br0 eth0
/usr/sbin/brctl addif br0 wlan0
/usr/sbin/brctl stp br0 off
DEVICE=br0
BOOTPROTO=static
BROADCAST=192.168.0.255
IPADDR=192.168.0.3
NETMASK=255.255.255.0
NETWORK=192.168.0.0
ONBOOT=yes
```

Creo que he comentado al menos lo más importante, si algo se me hubiese pasado, disculpas, son muchas cosas en un sólo artículo... pero quería que tuvieras al menos una guía para demostrar la potencia de Linux en el área de wireless.

El datagrama IP

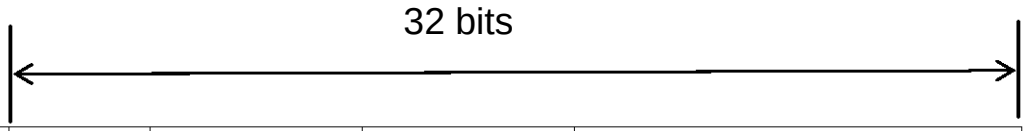
El esquema de envío de IP es similar al que se emplea en la capa Acceso a red. En esta última se envían Tramas formadas por un Encabezado y los Datos. En el Encabezado se incluye la dirección física del origen y del destino.

En el caso de IP se envían datagramas, estos también incluyen un Encabezado y Datos, pero las direcciones empleadas son Direcciones IP.

Encabezado	Datos

Formato del datagrama IP

Los datagramas IP están formados por Palabras de 32 bits. Cada datagrama tiene un mínimo (y tamaño más frecuente) de cinco palabras y un máximo de quince.



1	Ver	Hlen	TOS	Longitud Total
2	Identificación		Flags	Desp. De Fragmento
3	TTL		Protocolo	Checksum
4	Dirección IP de la Fuente			
5	Dirección IP del Destino			
	Opciones IP (Opcional)			Relleno
	DATOS			

* Ver: versión de IP que se emplea para construir el datagrama. Se requiere para que quien lo reciba lo interprete correctamente. La actual versión IP es la 4.

* Hlen: tamaño de la cabecera en palabras.

* TOS: tipo de servicio, la gran mayoría de los Host y Routers ignoran este campo, su estructura es:

Prioridad	D	T	R	Sin Uso

La prioridad (0 = Normal, 7 = Control de red) permite implementar algoritmos de control de congestión más eficientes; los tipos D, T y R solicitan un tipo de transporte dado: D = Procesamiento con retardos cortos, T = Alto Desempeño y R = Alta confiabilidad. Nótese que estos bits son solo "sugerencias", no es obligatorio para la red cumplirlo.

* Longitud Total: mide en bytes la longitud de dato el Datagrama permite calcular el tamaño del campo de datos: Datos = Longitud Total \x{2013} 4 * Hlen.

Antes de continuar con la segunda palabra del Datagrama IP, hace falta introducir conceptos relacionados con la fragmentación.

Fragmentación

En primer lugar, ¿de qué tamaño es un datagrama? el tamaño para un datagrama debe ser tal que permita el encapsulamiento, esto es, enviar un datagrama completo en una trama física; el problema está en que el datagrama debe transitar por diferentes redes físicas, con diferentes tecnologías y diferentes capacidades de transferencia; a la capacidad máxima de transferencia de datos de una red física se le llama MTU (el MTU de Ethernet es de 1500 bytes por trama, la de FDDI es de 4497 bytes por trama), cuando un datagrama pasa de una red a otra con un MTU menor a su tamaño es necesaria la fragmentación. A las diferentes partes de un datagrama se les llama fragmento. Al proceso de reconstrucción del datagrama a partir de sus fragmentos se le llama reensamblado de fragmentos.

El control de la fragmentación de un datagrama IP se realiza con los campos de la segunda palabra de su cabecera:

* Identificación: número de 16 bits que identifica al datagrama, que permite implementar números de secuencias y que permite reconocer los diferentes fragmentos de un mismo datagrama, pues todos ellos comparten este número.

* Banderas: ún campo de tres bits donde el primero está reservado. El segundo, llamado bit de no - fragmentación significa: 0 = Puede fragmentarse el datagrama o 1 = No puede fragmentarse el datagrama; el tercer bit es llamado más \x{2013} fragmentos y significa: 0 = único fragmento ó ultimo fragmento, 1 = aun hay más fragmentos; cuando hay un 0 en más \x{2013} fragmentos, debe evaluarse el campo desp. de Fragmento: si este es cero, el datagrama no esta fragmentado, si es diferente de cero, el datagrama es un último fragmento.

* Desp. de fragmento: a un trozo de datos se le llama Bloque de Fragmento, éste campo indica el tamaño del desplazamiento en bloques de fragmento con respecto al datagrama original, empezando por el cero.

Para finalizar con el tema de fragmentación, hay que mencionar el Plazo de Reensamblado, que es un time out que el Host destino establece como máximo para esperar por todos los fragmentos de un datagrama. Si se vence y aun no llegan TODOS, entonces se descartan los que ya han llegado y se solicita el reenvío del datagrama completo.

* TTL: tiempo de Vida del datagrama, especifica el número de segundos que se permite al datagrama circular por la red antes de ser descartado.

* Protocolo: especifica que protocolo de alto nivel se empleo para construir el mensaje transportado en el campo datos de datagrama IP algunos valores posibles son: 1 = ICMP, 6 = TCP, 17 = UDP, 88 = IGRP (protocolo de enrutamiento de gateway interior de CISCO).

* Checksum: es un campo de 16 bits que se calcula haciendo el complemento a uno de cada palabra de 16 bits del encabezado, sumándolas y haciendo su complemento a uno.

Esta suma hay que recalcularla en cada nodo intermedio debido a cambios en el TTL o por fragmentación.

* Dirección IP de la Fuente:

* Dirección IP del Destino:

* Opciones IP: existen hasta 40 bytes extra en la cabecera del Datagrama IP que pueden llevar una o más opciones, su uso es bastante raro.

  - o Uso de ruta estricta (camino obligatorio)
  - o Ruta de origen desconectada (nodos obligatorios)
  - o Crear registro de ruta
  - o Marcas de tiempo
  - o Seguridad básica del Departamento de Defensa
  - o Seguridad extendida del Departamento de Defensa

Enrutamiento IP

Enrutar es el proceso de selección de un camino para el envío de paquetes. La computadora que hace esto es llamada Router.

En general se puede dividir el enrutamiento en entrega directa y entrega indirecta: la entrega directa es la transmisión de un datagrama de una máquina a otra dentro de la misma red física; la entrega indirecta ocurre cuando el destino no está en la red local, lo que obliga al Host a enviar el datagrama a algún Router intermedio. Es necesario el uso de mascaras de subred para saber si el Host destino de un datagrama está o no dentro de la misma red física.

Encaminamiento con Salto al Siguiente

La forma más común de enrutamiento requiere el uso de una Tabla de Enrutamiento IP, presente tanto en los Host como en los Routers, estas tablas no pueden tener información sobre cada posible destino, de hecho, esto no es deseable; en vez de ello se aprovecha el esquema de direccionamiento IP para ocultar detalles acerca de los Host individuales; además, las tablas no contienen rutas completas, sino solo la dirección del siguiente paso en esa ruta.

En general una tabla de encaminamiento IP tiene pares (Destino, Router), donde destino es la dirección IP de un destino particular y Router la dirección del siguiente Router en el camino hacia destino. Nótese que Router debe ser accesible directamente desde la máquina actual.

Este tipo de encaminamiento trae varias consecuencias, consecuencia directa de su naturaleza estática:

1. Todo tráfico hacia una red particular toma el mismo camino, desaprovechando caminos alternativos y el tipo de tráfico.

2. Solo el Router con conexión directa al destino sabe si este existe o esta activo.

3. Es necesario que los Routers cooperen para hacer posible la comunicación bidireccional.

Algoritmo de Enrutamiento IP

Ruta Datagrama

(Datagrama) {
Extrae de la Cabecera de Datagrama la dirección de destino D;
extrae de D el prefijo de Red N;
si N corresponde a cualquier dirección directamente conectada entonces

envía el Datagrama a D sobre la Red N;
si no
si en la tabla hay una ruta especifica para D entonces
envía Datagrama al salto siguiente especificado;
si no
si en la tabla hay una ruta para la red N entonces
envía Datagrama al salto siguiente especificado;
si no
si en la tabla hay una ruta por defecto entonces
envía el Datagrama a la dirección por defecto;
si no
declarar Fallo de Enrutamiento;
Fsi
Fsi
Fsi
Fsi
}

Manejo de datagramas entrantes

Cuando un datagrama llega a un Host, el software de red lo entrega a IP. IP verifica la dirección de destino y si esta concuerda con la de la máquina local, entonces acepta el datagrama y lo entrega a las capas superiores; de no coincidir la dirección de destino, el datagrama es descartado.

Por otra parte, un Router que reciba un datagrama compara la dirección de destino con la suya propia, si coinciden, el datagrama pasa a las capas superiores, sino, se le aplica el algoritmo de encaminamiento y se reenvía el datagrama.

Direccionamiento sin Clase

Mediante el empleo de máscaras de subred, se logra convertir una única red (generalmente una Clase B) en múltiples redes lógicas interconectadas y administradas por la organización propietaria. El problema se presenta cuando el crecimiento explosivo de las redes locales produce el fenómeno ROADS (Running Out of Address Space), que consiste simplemente en el

agotamiento del espacio útil de direcciones, causado por la gran demanda de las direcciones Clase B, de las cuales solo hay 16.384, mientras que las Clases C permanecían sin asignar (pués aunque hay 2.097.152 de ellas, nadie las quiere por ser muy pequeñas).

Para enfrentar este problema se desarrollo el esquema de Direcciones sin Clase, que consiste en asignar a una misma organización un bloque contínuo de direcciones de Clase C; de esta manera, una organización que requiera conectar a Internet un número moderado de Hosts (digamos 3.800) puede recibir un bloque de 16 redes contínuas de Clase C (por ejemplo, de la red Clase C 199.40.72.0 a la 199.40.87.0), con lo cual dispone de 4.096 direcciones IP validas para administrar.

CIDR Enrutamiento Inter \x{2013} Dominio Sin Clases (Classless Inter \x{2013} Domain Routing)

El esquema de direcciones sin clase genera el problema de aumentar la información que debe incluirse en las tablas de enrutamiento. En el caso del ejemplo, se tendría que incluir 16 nuevas entradas en cada tabla de enrutamiento de cada Host y Router. CIDR resuelve el problema al incluir en las tablas información acerca del tamaño de los bloques y el número de bloques, así, en las tablas de enrutamiento IP se tienen pares (Destino, Router), donde destino no es una dirección de Host o Red tradicional, sino que incluye información acerca del número de redes que incluye el bloque (en nuestro ejemplo, 16) y el tamaño de cada una de esas redes (en el ejemplo, son Clases C, 256 direcciones cada una).

El Direccionamiento sin clase modifica la estructura de una dirección IP, de esta manera:

Prefijo de Red	Identificador de Host

Así, CIDR debe incluir en las tablas de enrutamiento cuál es la primera red que compone el bloque, cuántos bits se emplean como Prefijo de Red y la máscara de subred que se emplea. En

nuestro ejemplo, las tablas de enrutamiento IP contendrían esta información:

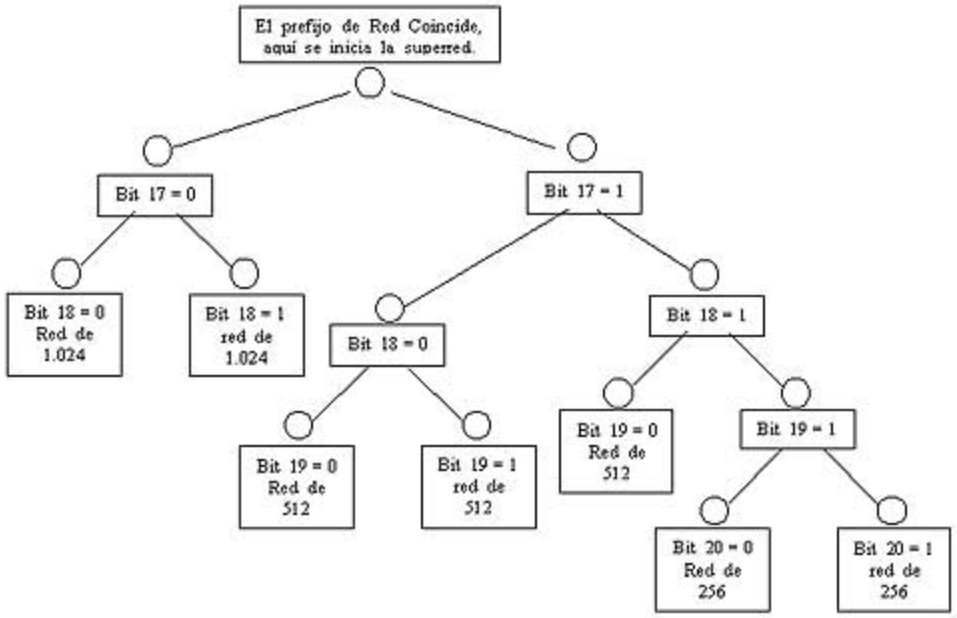
199.40.72.0/20 255.255.240.0

Refiriéndose a un bloque que se inicia con la red 199.40.72.0 y que tiene 20 bits en el prefijo de red. La máscara 255.255.240.0 (11111111.11111111.11110000.00000000) nos indica que se están usando 4 bits extra (los que se han resaltado) para identificar a las redes que componen al bloque. Nótese que cuatro bits permiten agrupar precisamente 16 redes Clase C.

Un aspecto importante que hay que subrayar es que en ningún momento cambia el algoritmo básico de enrutamiento IP, lo que cambia es el contenido de las tablas; además, las nuevas tablas contienen información resumida, por lo que buscar una dirección destino en la tabla se hace de otra manera, pero el algoritmo permanece inalterado.

El problema de buscar direcciones de destino en una tabla, consiste en que cualquier dirección cuya máscara de destino tenga menos bits, incluye a la que tiene mas bits. Con esto quiero decir que una máscara de subred como 255.255.0.0 (11111111.11111111.00000000.00000000, es decir, 16 bits de prefijo de red) incluye dentro de sí a la máscaras de subred 255.255.128.0 (11111111.11111111.10000000.00000000, 17 bits de prefijo de red) y ésta a su vez incluye a la máscara 255.255.192.0 (11111111.11111111.11000000.00000000) y en general, entre menos bits tiene el prefijo de red, más direcciones Host abarca; por esta razón, cuando se explora la tabla de enrutamiento IP en busca de una dirección de destino, se hace una búsqueda que inicia con las máscaras de más bits y termina en la de menos bits; es decir, se inicia con máscaras como 255.255.255.255 (todo en uno) y se continúa con la 255.255.255.254 (31 unos y un cero) y así sucesivamente. Esto quiere decir que tendrían que hacerse 32 recorridos secuenciales a la tabla, lo cual es muy ineficiente en cuanto a tiempo, pues además de ser un procedimiento demorado, se sabe ya que direcciones normales de Clase B (255.255.0.0) requieren 16 barridos a la tabla; además, hacen falta 32 barridos para notar que no hay una entrada en la tabla para esa dirección.

Por esta razón se emplean otros métodos para hacer estas búsquedas en las tablas de enrutamiento IP. Un esquema muy popular emplea un Arbol Binario, en el cual cada bit representa una nueva rama en el árbol. Así, en nuestro ejemplo, podrían dividirse las direcciones asignadas a la organización (4.096) en subredes de esta forma: dos subredes de 1.024 direcciones cada una, tres de 512 y dos de 256 direcciones. De esta forma, el árbol resultante tendría esta forma:



ICMP: Protocolo de Mensajes de Control de Interred (Internet Control Message Protocol)

Si un Router no puede enrutar o entregar un Datagrama, o si detecta una situación anómala que afecta su capacidad de hacerlo (por ejemplo, la congestión), debe informar a la fuente original para que evite o solucione el problema.

ICMP es un mecanismo para realizar esta operación, es considerado como una parte obligatoria de IP y debe ser incluido en todas sus implementaciones. ICMP comunica la capa de Interred de una máquina con la misma capa en otra máquina. ICMP es un protocolo de reporte de errores (no los corrige), además, ICMP sólo puede informar del error a la fuente del

Datagrama, es esta máquina la que debe implementar mecanismos para enfrentar el problema.

Los mensajes de ICMP requieren doble encapsulamiento: los mensajes ICMP viajan empaquetados en Datagramas IP aún así, no se considera a ICMP un protocolo de nivel superior a IP.

Formato del Mensaje ICMP

Aunque cada tipo de mensaje tiene su propio formato, todos ellos comparten los primeros tres campos: TIPO (8 bits), CODIGO (8 bits) y CHECKSUM (16 bits).

El campo TIPO identifica al tipo de mensaje ICMP y determina su formato. Puede tener alguno de estos valores:

* 0 : Respuesta de Eco (Echo Replay)
* 3 : Destino Inaccesible (Host Unreachable)
* 4 : Acallamiento de Origen (Source Quench)
* 5 : Redireccionar (Redirect)
* 8 : Solicitud de Eco (Echo Request)
* 11 : Tiempo Excedido
* 12 : Problema de Parámetros
* 13 : Solicitud de Timestamp
* 14 : Respuesta de Timestamp
* 17 : Solicitud de mascara de subred
* 18 : Respuesta de mascara de subred

Mensajes Solicitud de Eco y Respuesta al Eco

Este es el tipo de mensaje que envía la máquina cuando se emplea el comando ping. Solicitud de Eco pide a la máquina destino que responda con una Respuesta de Eco con un número de secuencia apropiado.

TIPO (8 o 0)
CODIGO (0)
CHECKSUM
Identificador
Número de Secuencia

Datos Opcionales
Mensaje Destino Inaccesible.

Es el mensaje empleado para reportar que no es posible entregar un Datagrama. El campo CODIGO describe mejor el problema:

* 0 : Red Inaccesible
* 1 : Host Inaccesible
* 2 : Protocolo Inaccesible
* 3 : Puerto Inaccesible
* 4 : Necesita Fragmentación
* 5 : Falla en la Ruta de Origen
* 6 : Red de Destino Desconocida
* 7 : Host Destino Desconocido
* 8 : Host de Origen Aislado
* 9 : Comunicación con Red Destino Administrativamente Prohibida
* 10 : Comunicación con Host Destino Administrativamente Prohibida
* 11 : Red Inaccesible por el tipo de servicio
* 12 : Host Inaccesible por el tipo de servicio

TIPO (3)
CODIGO (0...12)
CHECKSUM
NO \x{2013} USADO (debe ser cero)
Encabezado IP + Primeros 8 bytes de Datos IP

Los errores de red inaccesible por lo general implican fallas de enrutamiento. Debido a que el mensaje ICMP contiene la cabecera del Datagrama que lo produjo (en el campo de datos), el origen sabrá cual destino es inaccesible.

Mensaje de Acallamiento de Origen

Debido a que IP funciona sin conexión un Router no puede reservar memoria o recursos de comunicación antes de recibir

los Datagramas, en consecuencia los Routers pueden verse repentinamente saturados por el trafico, a esta situación se le llama congestión.

El congestionamiento se da porque un Host de alta velocidad genera Datagramas mas rápido de lo que el Router puede manejar o porque muchos Host envían Datagrama a la misma dirección al mismo tiempo.

Cuando los Datagramas llegan mas rápido de lo que un Router puede manejarlos, este los coloca en un buffer, si los Datagramas son parte de una ráfaga pequeña, esto soluciona el problema, pero si continúan llegando Datagramas se saturan los buffers y el Router debe descartar los nuevos Datagramas, es entonces cuando el Router genera un mensaje ICMP de Acallamiento de Origen solicitando a este reducir la tasa de envío de Datagramas; no existe un mensaje ICMP para revertir esta solicitud, en general poco después de bajar la tasa de envío, los Hosts la aumentan progresivamente hasta recibir otro mensaje de Acallamiento de Origen.

TIPO (4)
CODIGO (0)
CHECKSUM
NO - UTILIZADO (debe ser cero)
Encabezado IP + 8 primeros bytes de Datos IP

El objetivo de este mensaje era aliviar el problema de la congestión, pero no tuvo éxito. Se dejó al implementador decidir sobre cuando enviar estos mensajes, por lo que cada fabricante emplea su política favorita sin que ninguna solucione el problema del todo. Por otra parte, ICMP informa al Host de origen que su Datagrama ha sido descartado, pero puede que este Host no sea el causante de la congestión; además, cómo responder al mensaje ICMP?. Documentos como Requisitos para los Routers (RFC 1812) estipulan que NO se deben enviar mensajes de Acallamiento de Origen, se está trabajando en mecanismos más eficientes.

Mensaje Redireccionar

Se asume que los Routers conocen rutas correctas. Los Host comienzan con información mínima de enrutamiento y aprenden nuevas rutas de los Routers. En caso de que un Host utilice una ruta no óptima, el Router que lo detecta envía un mensaje ICMP Redireccionar solicitándole que actualice su tabla de enrutamiento IP.

TIPO (5)
CODIGO (0...3)
CHECKSUM
Dirección IP del Router
Encabezado de IP + 8 primeros bytes de Datos IP

Mensaje Tiempo Excedido

Debido a que los Routers sólo deciden sobre el próximo "Salto" usando tablas locales, errores en esas tablas pueden generar "ciclos de enrutamiento" para algún destino, esto provoca que los Datagramas sean descartados por vencimiento de su TTL; siempre que un Router descarte un Datagrama ya sea por vencimiento de TTL o por vencimiento del Tiempo de Reensamblado, envía un mensaje de Tiempo Excedido a la fuente.

TIPO (11)
CODIGO (0 o 1)
CHECKSUM
NO \x{2013} UTILIZADO (debe ser cero)
Encabezado de IP + 8 primeros bytes de Datos IP
CODIGO = 0: Descartado por vencimiento de TTL
CODIGO = 1: Descartado por vencimiento de Tiempo de Reensamblado.

Mensaje Problema de Parámetros

Cuando un Router o un Host encuentra un problema que no ha sido cubierto con los mensajes ICMP anteriores, envía este mensaje.

TIPO (12)
CODIGO (0 o 1)
CHECKSUM
Indicador
NO \x{2013} Utilizado (debe ser cero)
Encabezado de IP + 8 primeros bytes de Datos IP

El campo indicador apunta al campo dentro del encabezado IP que generó el problema.

Mensaje Solicitud de Timestamp y Respuesta de Timestamp

Una técnica sencilla provista por TCP/IP para sincronizar relojes emplea ICMP para obtener la hora de la otra máquina. Una máquina envía a otra una solicitud de Timestamp, solicitándole que informe su valor actual para la hora del día, la otra maquina envía una respuesta de Timestamp con esa información.

TIPO (13 o 14)
CODIGO (0)
CHECKSUM
Identificador
Numero de Secuencia
Timestamp Origen
Timestamp al Recibir
Timestamp al Transmitir

Mensaje Solicitud de Máscara de Subred y Respuesta de Máscara de Subred

Para aprender la máscara de subred utilizada por la red local, una máquina puede enviar un mensaje ICMP Solicitud de Mascara de Subred a un Router y esperar su Respuesta, si la

máquina no conoce la dirección del Router, puede enviar este mensaje por difusión.

TIPO (17 o 18)
CODIGO (0)
CHECKSUM
Identificador
Numero de Secuencia
Mascara de Subred

IPTABLES

¿Cómo se pone en marcha? Realmente lo que se hace es aplicar reglas, para ello se ejecuta el comando iptables, con el que añadimos, borramos, o creamos reglas, por ello un firewall de iptables no es sino un simple script de shell en el que se van ejecutando las reglas de firewall.
Notas: bueno, para los más conocedores. Se puede implementar un script de inicio en /etc/rc.d/INIT.d (o /etc/INIT.d) con el que hagamos que iptables se "inicie o pare" como un servidor más; lo podemos hacer nosotros o es probable que venga en la distribución (como en redhat por ejemplo). También se pueden salvar las reglas aplicadas con el comando iptables-save en un fichero y gestionar ese fichero con una aplicación o front-end desde la X o desde webmin.

Iptables es una aplicación en línea de comandos que gestiona el filtrado de paquetes en sistemas Linux (kernels 2.4.x), en base a las reglas que hayamos definido. Iptables es mucho más potente que su antecesor Ipchains (kernels 2.2.x).

La estructura de Iptables es básicamente una cola: cuando un paquete llega, este es validado contra cada una de las reglas del firewall, en el momento que alguna regla casa (match), se ejecuta la acción que haya sido definida en la regla (descartar el paquete, acceptarlo, enrutarlo, etc).

La estructura de un comando iptables es la siguiente:

iptables -t [tabla] -[AIRDLFZNXP] [regla] [criterio] -j [acción]

Vamos a ver que es cada cosa:

-t [tabla]	Esta parte del comando especifica cuál es la tabla en la que queremos añadir la regla. Existen 3 tipos de tablas válidas: nat, filter y mangle, siendo filter la tabla por defecto si se omite esta parte del comando. **Nat** se refiere a las conexiones que serán modificadas por el firewall, como por ejemplo, enmascarar conexiones, realizar redirecciones de puertos, etc. **Filter** es la tabla donde se añaden las relacionadas con el filtrado. **Mangle** también modifica paquetes pero, a diferencia de Nat, es mucho más potente, con Mangle podemos modificar cualquier aspecto del paquete (flags, TTL, etc).
-[AIRDLFZNXP] [regla]	Hay 4 opciones básicas con las que se puede jugar en este apartado del comando. Estas opciones básicas son las siguientes : • **A** es para añadir (Append) una regla. Reglas válidas son INPUT, FORWARD y OUTPUT. • **L** es para listar las reglas. • **F** es para borrar todas las reglas o en el caso de INPUT, FORWARD o OUTPUT seán dados como argumento se borraran las reglas asociadas solo a esa clase. • **P** establece la política por defecto del firewall. Por defecto es aceptar todas las conexiones.
[criterio]	Aquí es donde se especificarán las características del tipo de paquete que casará con esta regla. Para establecer reglas sencillas (reglas stateless), podemos operar con las siguientes opciones: -s (ip/red fuente), -d (ip/red destino), --sport (puerto fuente), --dport (puerto destino), y -p (protocolo). Un ejemplo de comando de la sintaxis de un comando iptables sencillo podría ser este (la parte en que se define el criterio de la regla está en negrita) iptables -A FORWARD **-p [protocolo] -s [ip/red fuente] --sport [puerto fuente] -d [ip/red destino] --dport [puerto destino]** -j DROP
-j [action]	Aquí establecemos que es lo que hay que hacer con el paquete. Las posibles opciones son: ACCEPT, REJECT, DROP, REDIRECT, LOG (existen más, pero estas son las básicas). **ACCEPT** aceptará el paquete **REJECT o DROP** lo desecharán, la diferencia entre ellos reside en que DROP descartará el paquete silenciosamente y REJECT emitirá un paquete ICMP Port Unreachable, indicando que está cerrado. **REDIRECT** redirigirá el paquete a donde se indique en el criterio del comando y por último... **LOG** lo logeará para su posterior análisis.

Comando	iptables -A INPUT -p tcp -i eth0 --dport 80 -j DROP
Descripción	Cerrar conexiones entrantes desde eth0 y hacia el puerto (local) 80 (HTTP)

Iptables es muy flexible y puede hacer cualquier cosa que se les ocurra a los paquetes que pasan por la red, man iptables y www.netfilter.org nos informarán de todo lo que hay que saber.

Para finalizar el tutorial relámpago, vamos a ver unos ejemplos y lo que hacen, que muchas veces aclaran más las cosas que la pura documentación.

Comando	iptables -t nat -A POSTROUTING -o eth0 -s 10.0.0.0/255.255.255.0 -j MASQUERADE
Descripción	Enmascarar por las conexiones procedentes de la red 10.0.0.0 como si lo hicieran desde la ip configurada en la interfaz eth0. (Típica regla en un router linux compartiendo la conexión eth0 con la red local conectada a eth1).Una regla equivalente a esta puede ser esta (si atacamos por SNAT en lugar de MASQUERADE): iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to ip-de-eth0 NOTA: Para que esta regla funcione correctamente, así como todas las reglas FORWARD, PREROUTING, etc, es necesario activar el forwardeo entre interfaces en el kernel : #echo 1 > /proc/sys/net/ipv4/ip_forward

Comando	iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 3128
Descripción	Redireccionar al puerto 3128 (proxy) todos los paquetes que entran por eth1 y con destino puerto 80 (HTTP), de esta manera conseguimos un proxy transparente.

Comandos	iptables -A INPUT -p tcp -i eth0 -m state --state NEW,ESTABLISHED,RELATED --dport 22 -j ACCEPT iptables -A INPUT -p all -i eth0 -m state --state NEW,INVALID -j DROP

Descripción	Detener todas las conexiones entrantes desde la interfaz eth0 menos la conexiones al servicio ssh. La primera regla deja pasar los paquetes al 22 y la segunda cierra todo lo demás. Sin embargo todas las conexiones que se realicen desde la máquina (como navegar, consultar correo, etc) estarán permitidas por que no son conexiones iniciadas desde "fuera". Con ipchains este tipo de reglas (reglas de inspección de estado, statefull) no existían.

Comandos	iptables -A INPUT -i eth0 -p icmp --icmp-type 8 -j DROP iptables -A FORWARD -i eth0 -p icmp --icmp-type 8 -j DROP
Descripción	Deshabilitar los paquetes ICMP entrantes de tipo echo (8) para el firewall (regla INPUT) y la red protegida (regla FORWARD).

Comandos	iptables -A INPUT -i eth0 -f -m length --length 0:40 -j DROP iptables -A FORWARD -i eth0 -f -m length 0:40 -j DROP
Descripción	Denegar paquetes fragmentados por debajo de 40 bytes. Tanto para conexiones que dirigidas al firewall (regla INPUT) como las que pasan a través de él (regla FORWARD). Esta regla evita ataques del tipo "Tiny Fragment Attack"

TCPDUMP

Para averiguar la interfaces en cualquier Unix recurrimos al comando ifconfig -a el cual nos da una lista de las interfaces que tenemos, así como sus parámetros de configuración.

```
[terron@ux02 ~]$ /sbin/ifconfig –a

eth0      Link encap:Ethernet  HWaddr addr
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:646760 errors:0 dropped:0 overruns:0 frame:0
          TX packets:449673 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          Interrupt:5 Base address:0x2c20

eth1      Link encap:Ethernet  HWaddr addr
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1321583 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1778135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
```

```
          Interrupt:9 Base address:0x3000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:39747 errors:0 dropped:0 overruns:0 frame:0
          TX packets:39747 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0

[terron@ux02 ~]$
```

Usando los datos del ejemplo anterior, en el Linux si queremos escuchar en la interfaz eth0, usaremos tcpdump -i eth0, mientras que en el caso de Windows si queremos escuchar en la ethernet usaremos windump -i \Device\Packet_{8435447C-6020-481F-A720-44D940909166}.

Cuando estamos leyendo la red, puede que no nos interese que el tcpdump intente resolver los nombres de las máquinas (pueden que no estén dadas de alta en el DNS, por motivos de seguridad, etc), para ello disponemos de la opción **-n**.

Para establecer la longitud de los datos que captura tcpdump usamos **-s len**, donde len es la longitud que nos interesa. Por defecto el tcpdump sólo captura los primeros 68 bytes, lo cual es útil si lo único que se quiere son las cabeceras IP, TCP o UDP, pero que en caso de estar esnifando protocolos como el NFS truncan los datos. En ese caso podemos ajustar la longitud de la captura a la MTU del medio que estamos usando con esta opción. Por ejemplo para capturar toda la trama Ethernet podemos usar -s 1500.

En función de la cantidad de información que queramos a la hora de que el tcpdump nos interprete, podemos usar -v,-vv,-vvv, aumentando el grado de información con cada una de las opciones.

Si queremos imprimir el contenido del paquete, podemos usar la opción -x. Si además queremos que nos imprima en ASCII el contenido de los paquetes podemos usar **–X**, la longitud que imprime viene determinada por la opción **-s** o los 68 bytes que usa captura por defecto.

Podemos trabajar offline con el tcpdump. Si queremos grabar nuestra captura para posteriormente leerla y analizarla usamos la opción **-w file** donde file es el nombre del fichero donde queremos grabar la captura de datos. Posteriormente podemos leer y analizar offline con **-r file**. Además este tipo de ficheros de captura lo pueden leer otros analizadores como por ejemplo Ethereal.

Interpretando la salida

Lo primero que hay que decir es que la salida depende del protocolo que estemos analizando. Para empezar comentar que todas las capturas del tcpdump tienen como primer campo una marca de tiempo, que indica cuando ha sido capturado el paquete.

Peticiones ARP/RARP

El protocolo ARP (address reslotion protocol), sobre Ethernet está documentado en la RFC 826. RARP puede encontrarse en la RFC 1293. Las peticiones arp aparecen de la siguiente manera:

```
18:33:49.908612 arp who-has 192.168.1.2 tell 192.168.1.1
18:33:49.908691 arp reply 192.168.1.2 is-at 0:2:a5:ee:ec:10
```

En este caso, la máquina 192.168.1.1 pregunta por la dirección Ethernet 192.168.1.2 (suponemos ambas máquinas en la misma subred). Como vemos la 192.168.1.2 responde; en este caso, vemos los valores numéricos puesto que he usado la opción -n, las mayúsculas indican la máquina por la cual se está preguntando, y la minúscula la máquina que hace la pregunta.

```
18:33:49.908612 arp who-has MAQUINA tell otra
18:33:49.908691 arp reply MAQUINA is-at 0:2:a5:ee:ec:10
```

TCP

La línea general de un paquete TCP es como sigue:

src > dst: flags [dataseq ack window urgent options]

El protocolo TCP se define en la RFC 793 en principio **src**, **dst** y **flags** están siempre presentes, los otros dependiendo del tipo de conexión TCP que se trate, el significado de dichos parámetros es:

- **src**: Dirección y puerto origen. En caso de no especificar el parámetro -n se intenta resolver el nombre vía DNS y el se busca el nombre del puerto vía (normalmente en los Unix en /etc/services).
- **dst**: Dirección y puerto destino, exactamente igual que el caso anterior.
- **flags**: Indica los flags de la cabecera TCP. Puede ser un ., cuyo significado es que no hay flags, o bien una combinación de S (SYN), F (FIN), P (PUSH), W (reducción de la ventana de congestión), E (ECN eco).
- **dataseq**: El número de secuencia del primer byte de datos en este segmento TCP. El formato es primero:ultimo(n), que significa que desde a primero a último (sin incluir último) hay un total de n bytes de datos. Ojo cuando hay segmentos con SYN, que también ocupa un número del espacio de secuencia.
- **ack**: El número de asentimiento indica el número siguiente de secuencia que se espera recibir. Ojo los SYN también se asienten.
- **win**: Tamaño de la ventana de recepción.
- **urgent**: Existen datos urgentes.
- **options**: Indica la existencia de opciones. En caso de que haya van entre < y >.

En el siguiente ejemplo, (viene en la página de manual del tcpdump), podemos ver:

1. rtsg.1023 > csam.login: S 768512:768512(0) win 4096 <mss 1024>
2. csam.login > rtsg.1023: S 947648:947648(0) ack 768513 win 4096 <mss 1024>

3. rtsg.1023 > csam.login: . ack 1 win 4096
4. rtsg.1023 > csam.login: P 1:2(1) ack 1 win 4096
5. csam.login > rtsg.1023: . ack 2 win 4096
6. rtsg.1023 > csam.login: P 2:21(19) ack 1 win 4096
7. csam.login > rtsg.1023: P 1:2(1) ack 21 win 4077
8. csam.login > rtsg.1023: P 2:3(1) ack 21 win 4077 urg 1
9. csam.login > rtsg.1023: P 3:4(1) ack 21 win 4077 urg 1

Esto simula una conexión originada por la máquina rtsg con destino a csam, con el servicio rlogin.
El significado de las líneas anteriores es:

1. Inicio de conexión de *rtsg* -> *csam* SYN ISN 768512 ventana de 4096
2. SYN de *csam* -> *rtsg* ISN 947648 ventana de 4096 ACK del SYN anterior.
3. ACK del SYN mandado por *csam*. No hay flags
4. 1 byte de datos de *rtsg* -> *csam*. Flag *PUSH* activado., (los números de secuencia son relativos al ISN a menos que especifiquemos la opción -*S*, en cuyo caso pone los números de secuencia se imprimen de manera absoluta).
5. ACK del byte de datos anterior por parte de *csam*.
6. 19 bytes de datos de *rtsg* a *csam*.
7. *csam* manda 1 byte de datos a *rtsg*, y manda el ACK de los 19 bytes enviados por *rtsg*. La ventana de recepción ha bajado en 19 bytes. Flag *PUSH*
8. *csam* envía un byte de datos urgente. Flag *PUSH*.
9. Idem anterior.

UDP

Un paquete UDP se imprime de la siguiente manera:

origen.srcport > destino.dsrpot: udp len

- **origen**: Nombre o dirección origen.
- **srcport**: Puerto origen.
- **destino**: Nombre o dirección destino.
- **dstport**: Puerto destino
- **len**: Longitud de los datos de usuario.

Ejemplo:

12:35:21.457350 10.10.109.10.1025 > 192.168.1.2.1345: udp 121 [ttl 1]

En algunos casos, puede interpretar protocolos que vayan encapsulados en los paquetes UDP, como NFS o DNS, el grado de detalle en la interpretación de estos protocolos dependerá del grado de detalle (controlado con la opción -v) que queramos darle.

Fragmentos de datagramas IP

Los datagramas fragmentados se indican con una expresión al lado de los mismos entre paréntesis:

(frag id:size@offset+) (frag id:size@offset)

id es el identificador de fragmento.
size tamaño del fragmento.
offset posició del fragmento en el datagrama original.

Si existe el **+** al final de **offset** significa que aún quedan más fragmentos. En caso de ausencia, que es el último.

Los datos del protocolo del nivel superior, sólo se imprimen en el primer fragmento.

Filtros

Es lo más importante que nos permite hacer el tcpdump, el uso de filtros. Un filtro es una expresión que va detrás de las opciones y que nos permite seleccionar los paquetes que estamos buscando. En ausencia de ésta, el tcpdump volcará todo el tráfico que vea el adaptador de red seleccionado.
La expresión que se usa para definir el filtro tiene una serie de primitivas y tres posibles modificadores a las mismas. Esta expresión será verdadera o falsa y hará que se imprima o no el paquete de datos.

Los 3 modificadores posibles son:

- tipo. Puede ser **host**, **net** o **port**. indican respectivamente una maquina, por ejemplo **host 192.168.1.1** una red completa, por ejemplo **net 192.168**, o un puerto concreto, por ejemplo **port 22**. Por defecto se asume el tipo **host**.
- dir. Especifica desde o hacia donde se va a mirar el flujo de datos. Tenemos **src** o **dst** y podemos combinarlos con **or** y

and. Para el caso de de protocolos punto a punto podemos sustituir por **inbound** o **outbound**.Por ejemplo si queremos la dirección de destino 10.10.10.2 y la de origen 192.168.1.2, el filtro serma **dst 10.10.10.2 and src 192.168.1.2** si se quiere que sea la dirección destino 192.168.1.1 o la dirección origen 192.168.1.2, serma **dst 192.168.1.1 or src 192.168.1.2**. Pueden seguirse combinando con la ayuda de paréntesis o las palabras **or** y **and**. Si no existe se supone **src or dst**. Por supuesto, esto se puede combinar con los modificadores de tipo anteriores.

- proto. En este caso es el protocolo que queremos capturar. puede ser **tcp**,**udp**,**ip**,**ether** (en este caso captura tramas a nivel de enlace,**arp** (peticiones arp), **rarp** (peticiones reverse-arp),**fddi**(para redes FDDI, pero realmente el encapsulado es igual al ether). Hay otros niveles de enlace para redes Decnet y lat, pero dado su escaso uso, me remito a la página de manual del programa.

Siempre podemos combinar expresiones con ayuda de paréntesis. Ojo con el tema de los paréntesis en los shell de Unix, porque son metacaracteres interpretan.

A continuación se dan las primitivas que pueden usarse. Lo que aparece entre [y] es opcional, y el | significa "o". El resto se tiene que poner si queremos poner el filtro con el comportamiento.

- **[dst|src] host máquina**. Cierto si la dirección destino u origen del paquete es **maquina** lo cual puede ser una dirección IPv4 (o IPv6 si se ha compilado soporte para el mismo), o un nombre del DNS. Si queremos restringir a dirección destino podemos restringir con **dst**. Para dirección origen **src**.

Ejemplos:

- Capturar el tráfico cuya IP origen sea 192.168.1.1
- **tcpdump src host 192.168.1.1**
- **windump src host 192.168.1.1**

- Capturar todo el tráfico cuya dirección origen o destino sea 192.168.1.2

- **tcpdump host 192.168.1.2**

- **windump host 192.168.1.2**

- **ether src|dst|host edir**. Este filtro es cierto sm la dirección origen (**src**), la destino (**dst**) o el cualquiera de las dos(**host**) coincide con **edir**. Hacer notar que **src**,**dst** o **host** es obligatorio especificarlo*.*

  Ejemplos:

  - Capturar el tráfico con destino a la dirección Ethernet 0:2:a5:ee:ec:10.

    tcpdump ether dst 0:2:a5:ee:ec:10
    windump ether dst 0:2:a5:ee:ec:10

  - Capturar el tráfico que vaya a la máquina cuya dirección MAC es 0:2:a5:ee:ec:10.

    tcpdump ether host 0:2:a5:ee:ec:10
    windump ethert host 0:2:a5:ee:ec:10

- **gateway máquina**. Cierto en caso de que el paquete use **máquina** como router. **máquina** debe estar definida en **/etc/ethers** y **/etc/hosts**, realmente los paquetes que cumplen con esa condición son aquellos que tienen como dirección ethernet destino **máquina**, pero ni la dirección IP destino u origen es **máquina**.
- **[dst|src] net red**. Cierto en caso de que la red de la dirección destino, origen o ambas sea **red**. El parámetro **red** puede ser una dirección numérica (por ejemplo 192.168.1.0) o bien un nombre que se resuelve a dirección, en los Unix, con ayuda del **/etc/networks**. Decir que también se admite el clásico direccionamiento CIDR. Podemos especificar una máscara poniendo **red** como **net red mad mascara** o bien usar **/**, **net red/bits**. Hacer notar que el uso de **net ... mask** no es compatible con direcciones IPv6, si queremos hacer referencia a la red destino usamos **dst** como prefijo. Para la red origen usamos **dst**.

Ejemplos:

- Capturar todo el tráfico cuya red destino sea 192.168.1.0.

  tcpdump dst net 192.168.1.0
  windump dst net 192.168.1.0

- Capturar todo el tráfico cuya red origen sea 192.168.1.0/28

  tcpdump src net 192.168.1.0 mask 255.255.255.240
  tcpdump src net 192.168.1.0/28

- Capturar todo el tráfico con origen o destino en la 10.0.0.0/24

  tcpdump net 10.0.0.0/24
  tcpdump net 10.0.0.0 mask 255.255.255.0

- **[dst|src] port puerto**. Cierto en caso de que el puerto (ya sea udp o tcp) coincida con **puerto**. Si no se especifica **dst** o **src**, será cierto tanto puerto origen como destino. Si queremos restringir a destino usamos **dst** y a origen usamos **src**. El puerto es un valor numérico entre 0-65535 o bien un nombre que en Unix se resuelve a través del /etc/services.

Ejemplos:

- Capturar todo el tráfico con destino al puerto 23

  tcpdump dst port 23

- Capturar todo el tráfico con destino o origen puerto 80

  tcpdump port 23

- **less longitud**. Cierto en caso de que el tamaño del paquete sea menor o igual **longitud**.
- **greater longitud**. Cierto en caso de que el tamaño del paquete sea mayor o igual que **logitud**.
- **ip proto protocolo**. En este caso escucha el **protocolo** que se le indique, el protocolo puede ser **icmp**, **icmp6**, **igmp** (internet group managent protocol), **igrp** (interior gateway routing protocol), **pim** (protocol independent multicast), **ah** (IP

Authentication header), **esp** (encapsulating security payload), **udp** o **tcp**. En caso de usar **icmp**, **udp** o **tcp** hay que escapar el protocolo, poniendo un ****, es decir, ip proto \icmp. Ojo con ese caracter que también hay que escaparlo en los shells de Unix.

Por comodidad se disponen los alias **tcp**, **udp** e **icmp** que equivalen a **ip proto tcp or ip6 proto tcp**, etc*.*

Ejemplos:

- Capturar el todo los paquetes icmp

tcpdump ip proto \\ip

(en Unix hay que escapar el \).

- Capturar todo el tráfico udp

tcpdump ip proto \\udp
tcpdump udp

(el alias es más cómodo)

- **ip6 proto protocolo**. Cierto si es un paquete de IPv6 con el protocolo **protocolo**.
- **ip6 protochain protocolo**. Es un número que en los Unix puede leerse en **/etc/protocols**. En este caso lo que se busca es que dentro de los diferentes cabeceras que puede tener un paquete IPv6 una de ellas sea el **protocolo** especificado.
- **ip protochain protocolo**. Igual que el caso anterior pero para IPv4.
- **ether broadcast**. Cierto si la trama capturada va dirigida hacia la dirección de difusión Ethernet. La palabra ether es opcional.
- **ip broadcast**. Cierto si el paquete va dirigido a la dirección de difusión de IP. Esta dirección se comprueba si es todo 0 o 1, o bien se comprueba la dirección local de la subred.
- **ether multicast**. Cierto si la trama va dirigida a una dirección multicast Ethernet.
- **ip multicast**. Cierto si el paquete va dirigido a una dirección multicast IP.
- **ip6 multicast**. Cierto si el paquete va dirigido a una dirección multicast IPv6.
- **ether proto protocolo**. Cierto si el protocolo que contiene la

trama es de tipo **protocolo** Los protocolos son **ip**, **ip6**, **arp**, **rarp**, **atalk**, **aarp**, **decnet**, **sca**, **lat**, **mopdl moprc** e **iso**.

Además estos nombres son identificadores que deben de ser escapados con ****.

Sin embargo hay una serie de alias que hacen más cómodo la expresión en los filtros. Dichas expresiones son **ip**,**ip6** ,**arp**,**rarp**,**aarp**, **decnet** e **iso**, siendo equivalentes a **ether proto ip**, **ether proto ip6**, etc.

Ejemplos:

- Capturar todo tráfico arp

tcpdump -n ether proto \\arp
tcpdump -n arp

(el alias es más cómodo)

- Capturar todo tráfico ip

tcpdump -n ether proto \\ip
tcpdump -n ipi

- **vlan [vlanid]**. Cierto si la trama capturada es un paquete 802.1Q VLAN, hacer notar de que esto cambia el resto de la interpretación del paquete capturado, en especial los desplazamientos a partir de los cuales empiezan a decodificar los protocolos, ya que se asume que estamos capturando paquetes que viajan en tramas VLAN, por último si está presente el parámetro vlanid, sólo se mostraran aquellos paquetes que vayan a la VLAN **vlanid**.

Combinando los filtros

Se pueden combinar las expresiones anteriores con los ayuda de los operadores **not**, **and** y **or** (corresponden a la negación, el y lógico y el o lógico, dando lugar a filtros más complejos. Podemos usar también los equivalentes del lenguaje C: **!**, **&&** o **||**.

Ejemplos:

- Capturar todo el tráfico Web (TCP port 80)

tcpdump tcp and port 80

- Capturar el todas las peticiones DNS

tcpdump udp and dst port 53

- Capturar el tráfico al puerto telnet o ssh

tcpdump tcp and \(port 22 or port 23\)

(los "\" son para escapar en el shell de Unix)

- Capturar todo el tráfico excepto el web

tcpdump tcp and not port 80

Filtros Avanzados

Para los realmente muy cafeteros, el tcpdump permite hacer filtros a mano, indicando que bytes de la trama queremos atrapar y como los queremos interpretar, cuando queremos definir filtros de esta manera la expresión general es:

expr relop expr

Donde **relop** puede ser cualquiera de las operaciones de relación de C: **>**,**<**, **>= <=**, **=** y **!=**. **expr** es una expresión aritmética compuesta por una serie de números enteros, los operadores binarios de C, (**+**, **-**, *****, ***/***, **&** y **|**), un operador de longitud, **len**, y una serie de palabras reservadas que nos permiten el acceso a los diferentes paquetes de datos (**ether**, **fddi**, **tr**, **ip**, **arp**, **rarp**, **tcp**, **udp**, **icmp** e **ip6**).
Para acceder a los datos dentro de un paquete, usamos los modificadores anteriores y una expresión entera. Opcionalmente podemos especificar el tamaño de los datos que accedemos.

proto [expr : tam]

Asm por ejemplo, el primer byte de la trama Ethernet será ether[0], la primera palabra será ether[0:2]. El parámetro **tam** puede ser 1 (por defecto y no hace falta especificarlo), 2 o 4.

Fabricación de una antena helicoidal 2.425GHz para dispositivos inalámbricos en la banda ISM Traducción de la página http://users.bigpond.net.au/jhecker/

Traducción original: Inco
Revisión: Paul Salazar Mora
Revisión: Daniel Martínez Ponce (DMescal)

(Nota: Se han omitido referencias a algunos lugares y tiendas de Camberra, Australia).

(Nota: Creo que las plantillas a las que se hace referencia no son correctas y es mejor hacer unas nuevas con el programa HelixCalc, que sí que las hace muy bien).

Introducción:

Como algunos lectores ya sabrán, el Grupo de Usuarios de Linux de Camberra se ha embarcado en un proyecto de creación de una red inalámbrica a lo largo de Camberra. Parte de la existencia de este experimento se debe a la compra, a precio de saldo, de un gran número de tarjetas "Lucent WaveLAN", que fueron reemplazadas por las tarjetas del standard 802.11. Las tarjetas resultaron baratas, pero las antenas "tile" que venían con ellas no eran buenas para conexiones de larga distancia, no llegando más allá de unos cientos de metros. Además, las antenas comerciales que sí podían utilizarse para realizar el trabajo eran caras, más bien grandes, y antiestéticas, especialmente las que tienen forma de cono.

Así las cosas, no hay ninguna razón por la que esta antena helicoidal que describimos no pueda ser utilizada con cualquier otro equipo de la banda de los 2.4 GHz, tales como las nuevas tarjetas inalámbricas del tipo 802.11, o como los emisores de vídeo. Por favor, si alguien utiliza la antena con estos equipos que me lo haga saber.
La idea de partida es que cualquiera pudiera hacerse su propia antena para uniones punto a punto, y que lo pudiera hacer de forma barata. Los criterios principales eran que fuera fácil de construir, duradera y de bajo coste. La durabilidad es importante, ya que no se quería que el viento, las palomas o cualquier otro pajarraco arruinase tu sesión de Quake III o de Unreal Tournament. Los pájaros que se posan sobre las antenas provocan una importante disminución de la señal.

La antena se deriva de la información del libro de antenas Helicoidales "ARRL Antenna Book".

Piezas necesarias:
Para construir una antena necesitarás:
1 pza de 0.60 metros de tubo de PVC de 40 mm del que se utiliza en desagües (N.T. en el original se habla de que tenga 40mm de diámetro en el interior y unos 42- 43 mm en el exterior y yo sólo he encontrado el que normalmente se utiliza en fontanería que es de 40mm exteriores).

No te preocupes demasiado con este tema, según sea el tubo que compres tienes que diseñar las plantillas para ese tubo.
1 tapa de 40mm de PVC. (tapón para el tubo de PVC que compres).
1 tapa de 150 mm de PVC (o una pieza de plástico grueso o madera de similares dimensiones). Los tapones de tuberías de PVC grandes os sirven.
2 Abrazaderas en U de 25 o 35 mm (también llamado pernos en U, el tamaño de los mismos no importa demasiado, estos sirven para sujetar la antena a un mástil, no tienes que ponerlos obligatoriamente)
8 tuercas y 8 arandelas más para las abrazaderas anteriores.
0.7 mm de grosor de tamaño suficiente como para cortar un círculo de 130 mm de diámetro o una pieza apropiada de

aluminio o similar de una lata de membrillo (N.T.: o de una caja de galletas de esas holandesas con mucha mantequilla). Las hojas de aluminio planas comunes no sirven ya que son demasiado finas y se estropean cuando las taladras o cortas.
1 hoja de metal de 0.4.(aunque no sea del mismo grosor puedes utilizar un retal de la tapa o del culo de la caja de galletas holandesas que emplearas para hacer el circulo anterior).
Varios metros de cable de cobre esmaltado de 1 mm de diámetro (puede ser mayor diámetro pero no menor).
Un conector tipo N de montaje en panel (resulta apropiado el que tiene una base cuadrada con cuatro agujeros para sujetarlo con tornillos).
3 tornillos, tuercas y arandelas para sujetar el conector tipo N.
1 tornillo, 1 tuerca y arandelas, para unir el tapón grande la chapa circular y el tapón pequeño. (El tamaño del tornillo no importa, pero como consejo emplea un tornillo de cabeza redonda, porque si pones los pernos en U, el tornillo no te molesta al sujetar la antena a un mástil).
Araldit de secado lento (pegamento de dos componentes). También sirve pegamento de PVC normal, pero a la hora de pegar el tubo al tapón pequeño tienes muy poco tiempo para cuadrar todo porque este pegamento en cuestión de 1-2 min seca.
Loctite 424 o similar (superglue o una pistola de pegamento termofusible también puede valer).
Sellador de silicona.
Cinta adhesiva.
Herramientas que necesitarás:
Sierra para metales
Lija del numero 5 para madera (también sirve una lima pero tienes que ser un poco hábil con ella, en cambio con la lija la dejas sobre la mesa y rozas el tubo sobre ella ;)
Una escuadra de carpintero para medir ángulos rectos (te puede servir cualquier otro utensilio que tenga 90º , esto lo vas a utilizar para dejar lo mas nivelado posible el corte del tubo.
Cortador de cables fuerte.
Llaves apropiadas para las tuercas utilizadas.
Un destornillador Philips para los tornillos del conector tipo N.
Un taladro
Un juego de brocas para hacer agujeros desde pequeños a realmente grandes.

Tijeras (pero no unas buenas tijeras, ya que las destrozarás y a tu madre no le gustará).
Cutter.
Los tapones para PVC de 40 milímetros tienen que tener la base completamente plana (los hay de base plana y otros con base abombada). Hay también algún tipo de estos tapones que en el centro, por la parte interior, tienen partes de plástico que pueden molestar a la hora de poner una tuerca.

Construcción:

Imprime y recorta las plantillas que hay en el de plantillas circle.pdf y rhspiral.pdf o lhspiral.pdf. Deberás utilizar la plantilla de rhspiral para antenas con espiral hacia la derecha y lhspiral para antenas con espiral hacia la izquierda. Necesitarás la plantilla circular para hacer el plano de tierra (reflector), a no ser que puedas trazar un buen círculo de 130 mm de diámetro con una regla o un compás.
Actualización: descarga HelixCalc de la sección de teoría para poder diseñar tus propias plantillas
También te las puedes hacer a mano:

Para la plantilla del tubo, imprimes una, mides el perímetro del tubo y en un simple folio haces un rectángulo el lado mas corto del rectángulo es la medida del perímetro del tubo y el lado mas grande el tamaño del lateral grande el folio.(para que entren todas las espiras posibles en cada folio).

Recortas la plantilla impresa, la plantas encima del rectángulo que has dibujado en el folio y la primera diagonal de la plantilla impresa la continuas hasta el lateral del rectángulo. Ahora solo falta utilizar escuadra y cartabón trazas una línea paralela al lateral mas pequeño del rectángulo, que tiene que cortar justo donde corta la diagonal y el lateral grande del rectángulo. La distancia que hay entre el corte de la diagonal con el lateral mas corto superior es la distancia que tienes que emplear entre espira y espira, ahora traza paralelas a lo largo del rectángulo con esa distancia, y luego une con diagonales una paralela con otra, si esto no lo entiendes fíjate en la plantilla que has impreso y te

tiene que quedar mas grande o mas pequeña (yo solo te estoy explicando como sacar la escala sin tener que hacer cálculos ;)

Como esta plantilla tendrás que utilizar 2 o 3 plantillas.

Para la plantilla del círculo sacas la escala así 150(diámetro del tapón grande)/130 (diámetro del círculo de la plantilla) =diámetro de tu tapón/x es decir:

150/130=d/x d= diámetro de tu tampón

Despejas x y te sale el diámetro del círculo a dibujar.

Divides entre 2 el resultado y te dibujas un círculo con un compás con radio.

Corta el tubo de 40mm de PVC con una longitud de 550mm (55cm). Para sacar tu medida justa del tubo:

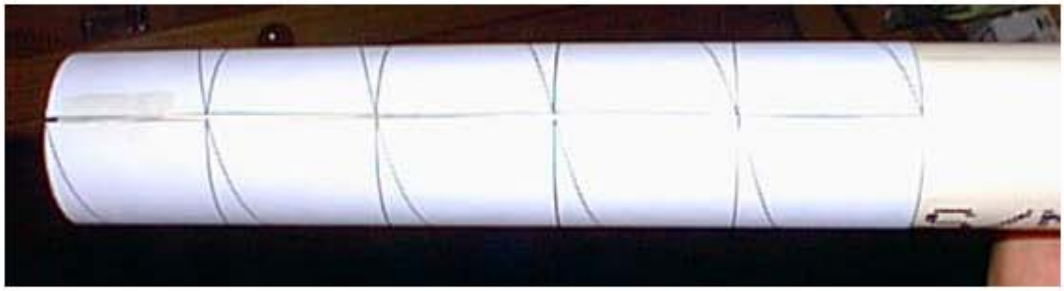
Numero de espiras que quieres que tenga * la distancia entre espira y espira (la has sacado antes al dibujar las paralelas, distancia entre paralela y paralela) + la altura del tapón sin contar el grosor del culo del tampón. (la altura del tapón la puedes hallar cogiendo el tubo lo introduces en el tapón y marcas en el tubo con un lápiz hasta donde llega el tapón sacas el tapón y mides desde la marca hasta el lateral del tubo, pues esa es la medida que tienes que sumar)

Ejemplo: 11(espiras) * 5cm (distancia) + 3,7cm (altura tapón)=58,7cm

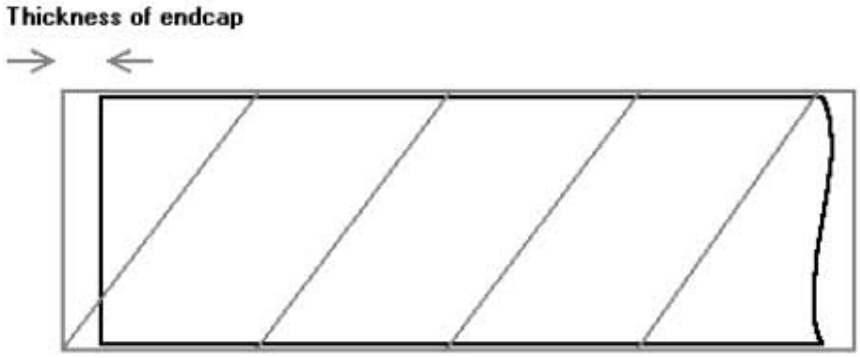
Pues 58,7 cm es el tamaño al que tiene que tener el tubo (un consejo deja un milímetro o dos más porque como me imagino que no serás un maestro con la sierra tu corte no será recto) ahora con la escuadra compruebas de donde te tienes que rebajar un poco, hasta dejarlo los mas nivelado posible, para rebajarlo coge la lija y dejalo nivelado y con la medida justa del tamaño del tubo.

Envuelve las plantillas de bobinado alrededor del tubo de PVC haciendo que coincidan los trazos de los bordes y los de las

espirales. No es demasiado importante si no coincide a la perfección. Da igual si utilizas la plantilla de espiral a izquierdas o la de espiral a derechas, pero lo que sí es importante es que la antena con la que se va a comunicar sea del mismo tipo. *Si combinas una antena de espiral a derechas con una de espiral a izquierdas entonces las señales no serán utilizables en absoluto*.



El extremo en el que empieces con la plantilla será el que conectarás a la base. Fíjate que el comienzo de la plantilla debe estar desplazado con respecto al tubo una medida igual a la altura del tapón de PVC que has hallado antes (en el ejemplo son los 3,7cm que tiene que quedar sin cubrir por la plantilla). Véase el diagrama. Esto compensará el grosor del tapón.



Utilizando un pico afilado (N.T. yo utilicé la punta caliente de un soldador de estaño tipo lápiz JBC) perfora la plantilla a lo largo de la línea espiral a unos intervalos regulares, digamos 5 o 6 por vuelta. Esto dejará unas marcas en el PVC que después seguiremos para enrollar el cable alrededor. Desplaza la plantilla y repite el paso anterior hasta que tengas una espiral completa alrededor de toda la longitud del tubo. Haz otra marca en el

punto final de la espiral de la plantilla. Ahora te deberían quedar libres unos cuantos milímetros de tubo. Esto es correcto.

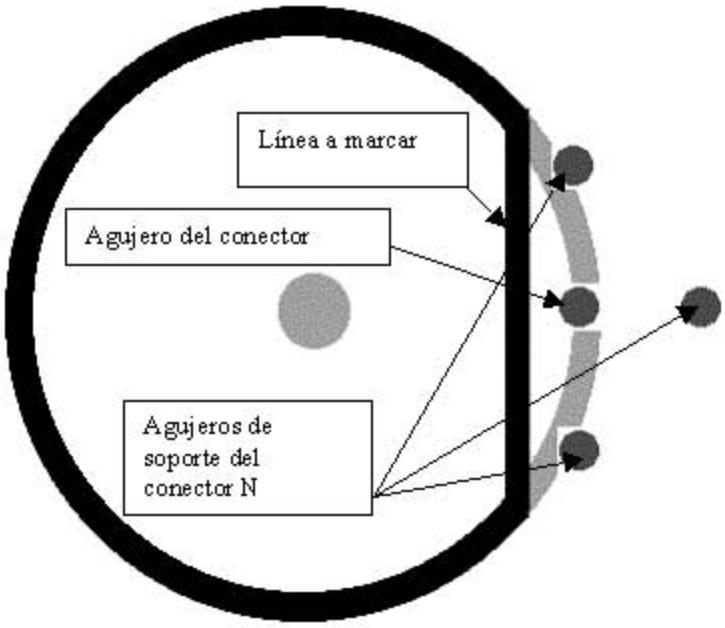
Un consejo es que marques los puntos donde corta un extremo del papel con otro en línea recta hacia abajo para así poder ver el principio y el final del hilo en la misma perpendicular)

Coge el alambre de 1mm y, utilizando algo como superglue o Loctite 424, sujeta el final del cable en donde la espiral acaba en el tubo (el punto final descrito en el apartado anterior). Enrolla lentamente el alambre alrededor del tubo, siguiendo las marcas de la espiral. Dos o tres veces en cada vuelta deberás poner más pegamento para sujetar el alambre en su lugar.
Cuándo te acerques a la base no pegues nada en la última vuelta y corta el alambre dejando que sobren unos 10 o 15 cm mas de lo necesarios. Descansa mientras el pegamento seca.
Recorta de la lamina de metal el círculo de que te has creado antes, con unas tijeras de recortables de papeleria lo haces perfectamente es como cortar una cartulina.
Haz agujeros con el taladro en la tapa de 150 mm de PVC y en el círculo de 130mm de chapa. Debes hacer un agujero para el tornillo central y otros para el conector (el del centro del conector y tres más pequeños para sujetarlo).

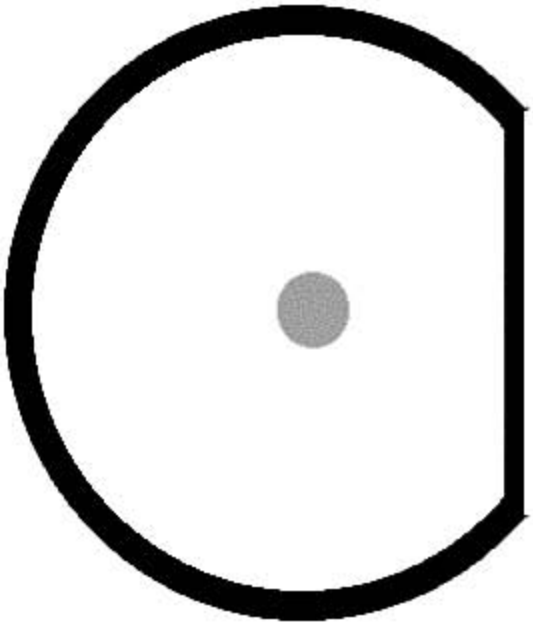
Normalmente los tapones llevan marcado el centro, por lo cual solo tienes hacer el agujero con la broca apropiada que tiene que ser del tamaño del tornillo a emplear.
Yo hice primero el agujero al tapón grande, luego por la parte de abajo coloqué la chapa circular mas o menos centrada y por el propio agujero del tapón grande hice el agujero a la chapa con esto conseguí centrar lo máximo posible la chapa ;)

Después hice el agujero al tapón pequeño por el centro que viene marcado de fábrica (todo esto siempre con la misma broca). *Nota, si por lo que sea no vienen marcados los centros de fábrica como sabes los diámetros de los tapones con un compás te haces los círculos de los tampones en un folio y después marcas los centros de los tapones con estas plantillas.*
Para hacer los agujeros del conector N al tapón grande me hice una plantilla en papel del tapón pequeño, la recorte y cogí el conector N sobre la plantilla y marqué estas posiciones de los

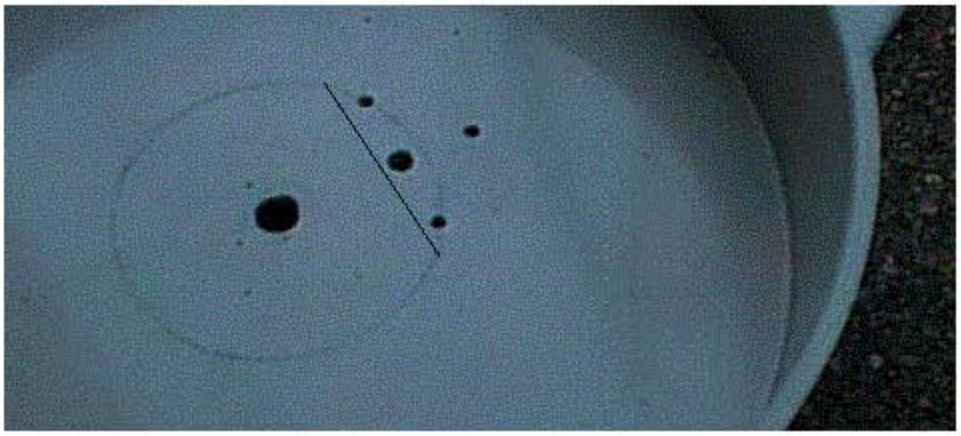
agujeros,(calcule dejar sitio para poder colocar las tuercas de los tornillos para sujetarlo) marque una línea en la plantilla para ver por donde tenía que cortar el tapón pequeño para dejar espacio para los agujeros en el conector grande. Mirar en la foto.



Después corte el tapón por la línea pintada en la plantilla. El tapón queda así:

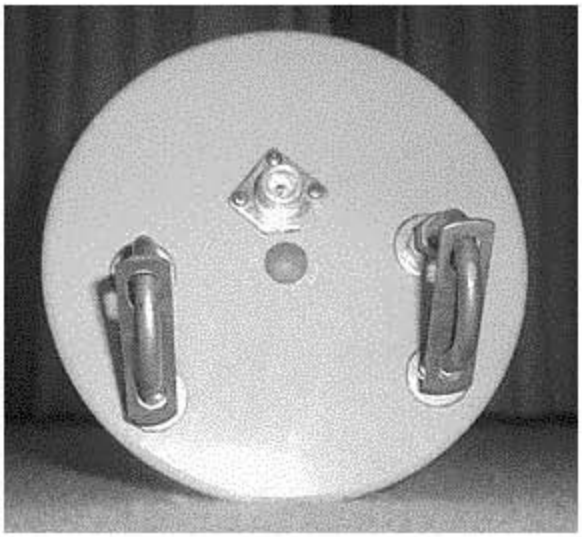


La plantilla del tapón pequeño con la marca de los agujeros la pintas en el interior del tapón grande y le haces los agujeros en el tapón grande. Al pasar la plantilla te tiene que quedar así:



Ahora haz los agujeros para el conector tipo N (te aconsejo que verifiques con el conector que estan en su sitio todos los agujeros antes de hacerlo ;).
Cuando atornilles las dos piezas juntas debería parecerse a esto... (falta colocar el circulo de chapa del reflector y el conector tipo N).

A continuación deberás hacer los taladros para poner las dos abrazaderas tipo U, dependiendo del tamaño que utilices. Tendrás que tener cuidado de que la posición de las abrazaderas sea correcta, de manera que el mástil que ha de sujetarse a ellas no moleste posteriormente a la hora de conectar el cable al conector tipo N.
Mira la foto siguiente para ver como tienen que quedar las abrazaderas.



Una vez hecho todos los agujeros en el tapón grande coloca la chapa redonda por la parte exterior del tapón haciendo que coincidan los agujeros centrales y con el taladro haz los agujeros en la chapa a través de los que tienes en el tapón grande, después quita la chapa y al agujero central del conector N hazle un agujero mas grande la razón es para que no llegue a tocar en ningún momento la chapa con la parte del conector este contacto lo tiene que hacer con los agujeros de soporte del conector (es la masa del conector).
Coloca la hoja circular de metal en la tapa grande de y atornilla el tapón de 40 mm, asegurándote que todos los agujeros de la hoja de aluminio y del tapón coincidan perfectamente. (como vamos a dejar fija ya la hoja circular primero haz la prueba de que coinciden los agujeros, luego échale unas gotas de superglue a la hoja circular y déjala ya fija sobre el tapón grande pegándola en la parte interior del tapón.
Acopla el conector tipo N.

Para que se igualen las impedancias (desde la nominal de 150 ohmios de la antena a la de 50 ohmios del conector y los cables) necesitas un chapa que va soldada al conector de tipo N, pasa entre el tubo y el tapón hasta llegar al final del hilo que ahí de nuevo va soldado. (esta chapa la puedes sacar de un retal de la caja de galletas que hemos usado para hacer la hoja circular es perfectamente valida para soldar, el aluminio no se puede soldar a si que no te molestes en utilizarlo, ya que no te servirá. El cobre o latón si servirán.

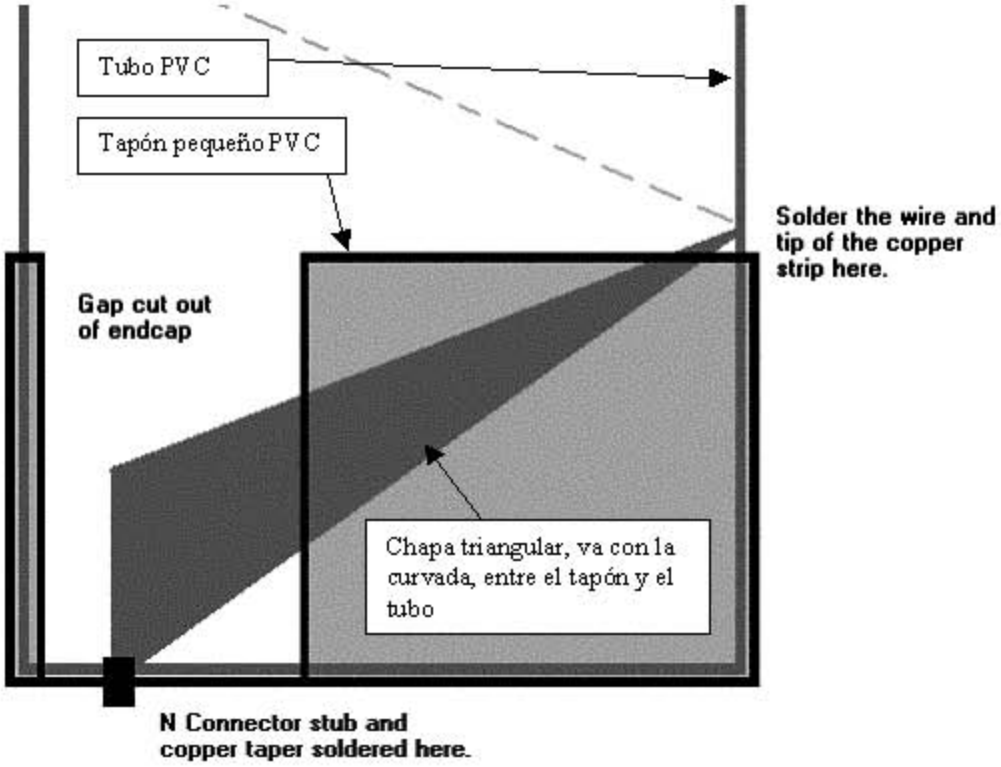
Necesitas que sea de una longitud tal que te permita seguir el trazo espiral alrededor del tubo hasta el final.

Para la chapa hazte una plantilla necesitas solo un compás y una regla y tienes que hacer un triángulo con estas medidas en los lados 17mm, 71mm y una hipotenusa de 73mm. Esta plantilla ponla encima del retal de la tapa de galletas y con las tijeras corta el triángulo.

Introduce el tubo en el tapón de 40mm y *haz una marca en donde la espiral se encuentra con la parte final del tapón*. Corta el cable en este punto dejando unos milímetros de más. Con el cutter rasca el esmalte del final del cable para dejarlo brillante y preparado para soldar con facilidad.

Con cuidado, suelda el final del pico estrecho de la tira de cobre al cable, de modo que la otra esquina de la a la chapa se pueda soldar elegantemente sobre el terminal del conector tipo N. (La chapa va entre el tubo y el tapón) Así que haz los ajustes correspondientes para que desde la soldadura del cable hasta el conector N(al que soldaras la chapa luego) quede la chapa perfectamente con el tubo puesto en el tapón , cuando veas que está, pega la chapa en el tubo con superglue, para que no se te mueva al pegar el tubo con el pegamento de PVC al tapón

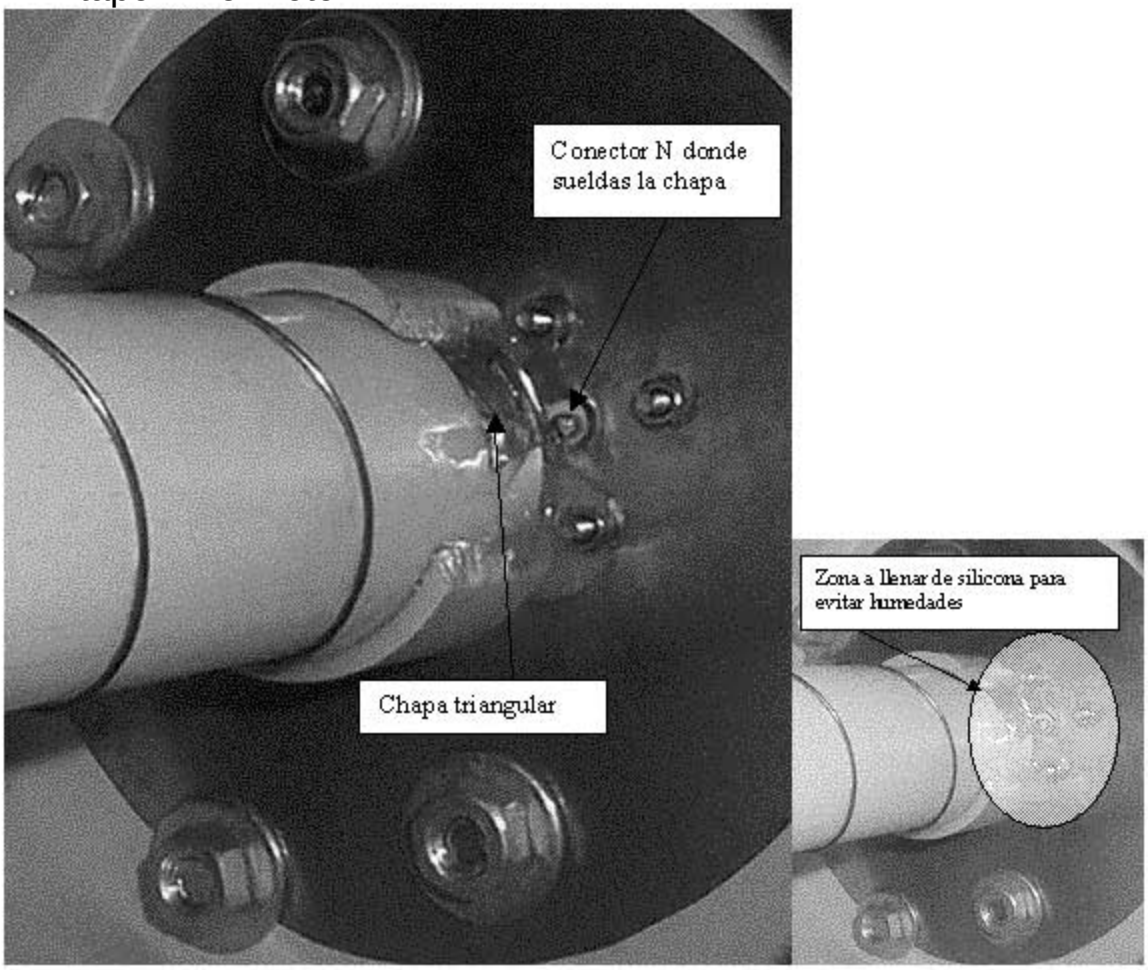
Esta chapa en triángulo, actúa como transformador de impedancias. No sé realmente cómo funciona, pero lo he hecho cuatro veces con pequeñas diferencias de longitud, y según el analizador de dos puertos funciona correctamente.



Saca el tubo y raya la parte interior del tapón de 40mm y las zonas correspondientes del tubo de 40mm de manera que el pegamento sujete mejor. Antes de pegar limpia completamente todas las superficies.

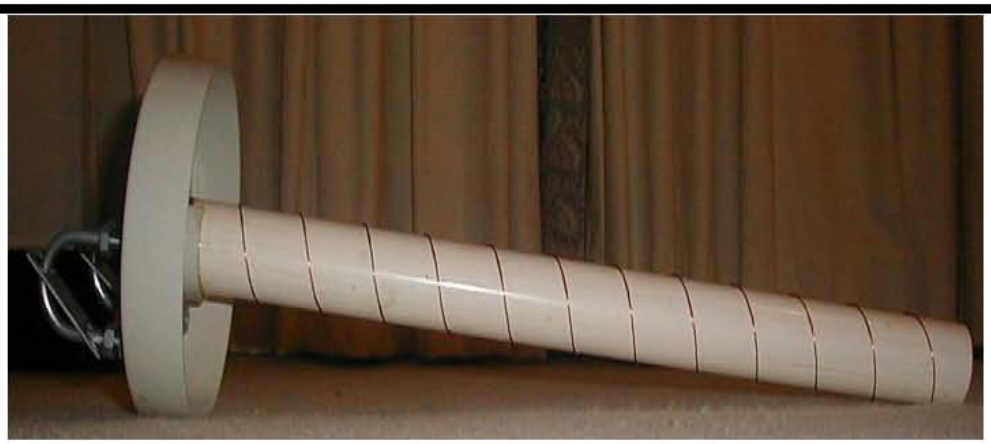
Haz una mezcla de un poco de Araldite de secado lento (no el de 5 minutos). Aplica el Araldite al tubo y al interior del tapón. Vuelve a introducir el tapón en su sitio, alineando la esquina de la tira de cobre con el terminal del conector. (Si haces esto con el pegamento de PVC de secado rápido tendrás 1-2 min para conseguir ajustar todo perfectamente). Un montón del pegamento rebosará. Suelda la esquina de la tira al pin central del conector N. Luego con silicona inunda todo el contenido de la

chapa los tornillos el conector N y las ranuras entre la chapa y le tapón. Ver Foto:



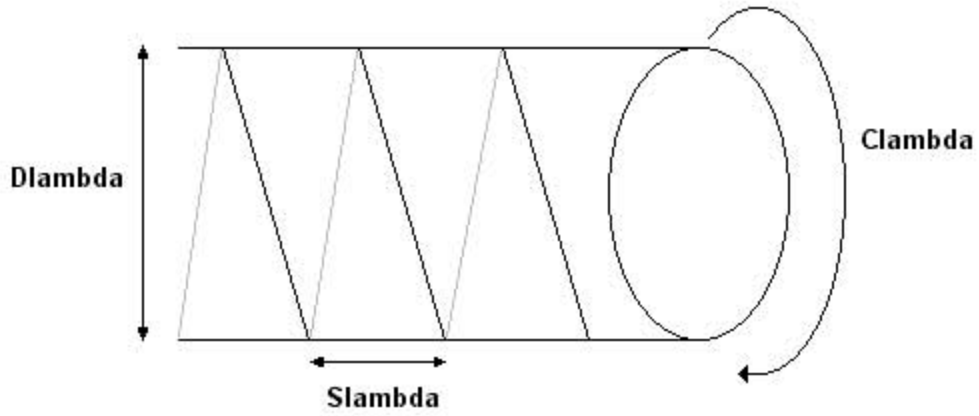
Deja que seque el pegamento (un día más o menos). Coloca las abrazaderas en U y... ya tienes tu propia antena helicoidal. Cuando tengas la chapa en su lugar y todo junto pegado y atornillado deberías tener algo parecido a la siguiente imagen.

La razón de que el tapón grande sea de 150mm es que se pueda colocar, desplazándolo sobre el montaje, un trozo de tubo PVC de 150mm de diámetro, que encaje en el primer tapón, y colocar otro tapón en el otro extremo, de manera que todo el conjunto queda perfectamente protegido de las inclemencias del tiempo y de la acción de los pájaros. Si colocas tu antena en el exterior, asegúrate de poner una buena cantidad de silicona alrededor del conector, y asegúrate de que el agua no puede hacer que contacten eléctricamente el terminal central de conector y el plano de tierra (hoja metálica). La experiencia demuestra un funcionamiento deficiente cuando llueve o hay niebla debido a que la condensación hace una especie de cortocircuito entre la tierra y el terminal de señal. También tengo noticias de que la protección de cinc del galvanizado de las abrazaderas puede provocar reacciones de tipo galvánico con la chapa de tierra, de modo que puede ser necesario colocar arandelas de plástico, teflón o goma para prevenir el deterioro de la lámina.
Aquí tienes una imagen del producto terminado.



Detalles importantes:
El tubo de PVC que yo he utilizado no se calienta si se introduce en un microondas funcionando durante unos pocos minutos, de modo que no absorbe ninguna de las ondas. Comprueba que esto sea así en el tubo o material que vayas a utilizar metiendo una parte en el microondas (con un pequeño vaso de agua) y asegúrate de que no se calienta o quema. Si fuera así no sería un buen material para hacer la antena.
El ajuste de impedancias que he descrito con la tira de cobre/latón me funcionó de varias maneras, todas las cuáles me las inventé sobre la marcha. La verdad, me quedé impresionado cuando el analizador de puertos me indicó lo bien que el circuito de ajuste estaba funcionando.
Hasta que no haga más pruebas, no diré que con esta antena se pueden conseguir 10Kms de cobertura (aunque es bastante posible y esa es la distancia que se pretende). Deberían funcionar bien a unos 3-4Km con buena visibilidad (sin demasiadas obstrucciones como árboles o tejados)
Hay multitud de variaciones sobre este mismo diseño. Utiliza la imaginación para inventar posibles variaciones que funcionen. Usar obleas de circuitos PCB de una sola cara es una opción, ya que la fibra de vidrio es muy resistente, y el cobre que ya está acoplado puede hacer de reflector.
Teoría
El diseño de esta antena se deduce del estupendo libro ARRL Antenna Handbook. En el capítulo 19 hay una serie de diseños de antenas helicoidales y cálculos matemáticos que detallan como calcular y calibrar un diseño de una antena.

He perdido las notas originales de mi diseño y por los tanto he deducido estas de los archivos PDF y tomando medidas de las antenas que tengo hechas.
Las siguientes fórmulas son de las páginas 19-23 del libro citado. Las copio aquí ya que no todo el mundo tiene acceso al libro.



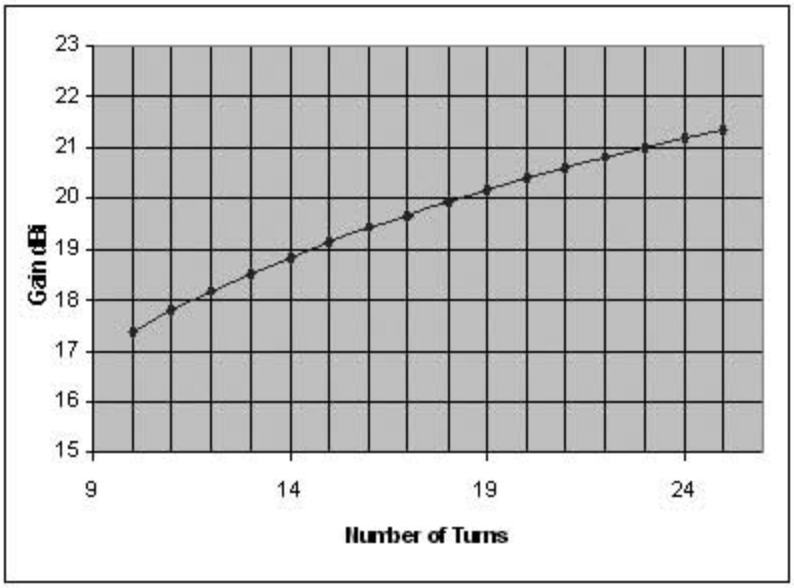
Cl tiene que estar entre 0.75L-1.133L y es el perímetro del arrollamiento Sl tiene que estar entre 0.2126Cl y 0.2867Cl y es la longitud axial de una vuelta G tiene que estar entre 0.8L y 1.1L y es el diámetro del plano de tierra o reflector Cl = pi * D es el perímetro de arrollamiento, y viene fijado por el tubo de PVC que pensemos utilizar como base para la antena. (Longitud = Diámetro * pi).

La frecuencia central (2.425GHz) tiene una longitud de onda **L** = 0.123711 metros.

Cl = pi * 0.040m = 0.12566 m (12.56 cm) = 1.0576 veces **L**
Sl = 0.2126 * 0.12566 = 0.02671 (o sea 26.7 milímetros, 2.67 cm)

La ganancia de la antena dada en dBi viene definida como ...
Ganancia = 11.8 + 10log10(Cl * Cl * n * Sl) donde n es el número de espiras.
Ganancia = 11.8 + 10log10(1.0576 * 1.0576 * 22 * 0.2126) = 18.9 dBi

La tabla siguiente muestra la relación entre número de espiras y ganancia. Como puede verse, para ganar 3 dbs más, es necesario doblar casi el número de espiras y por lo tanto la longitud de la antena.

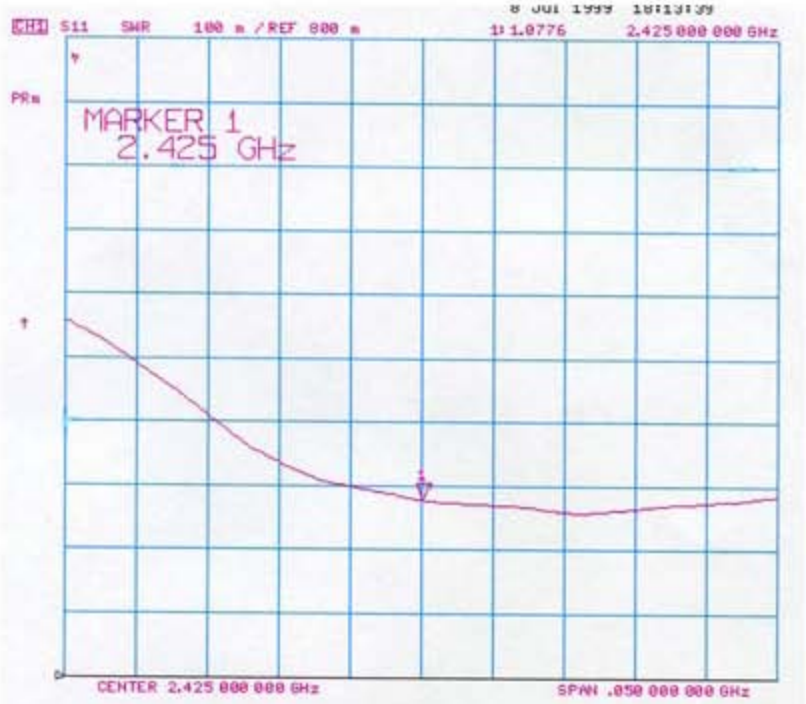


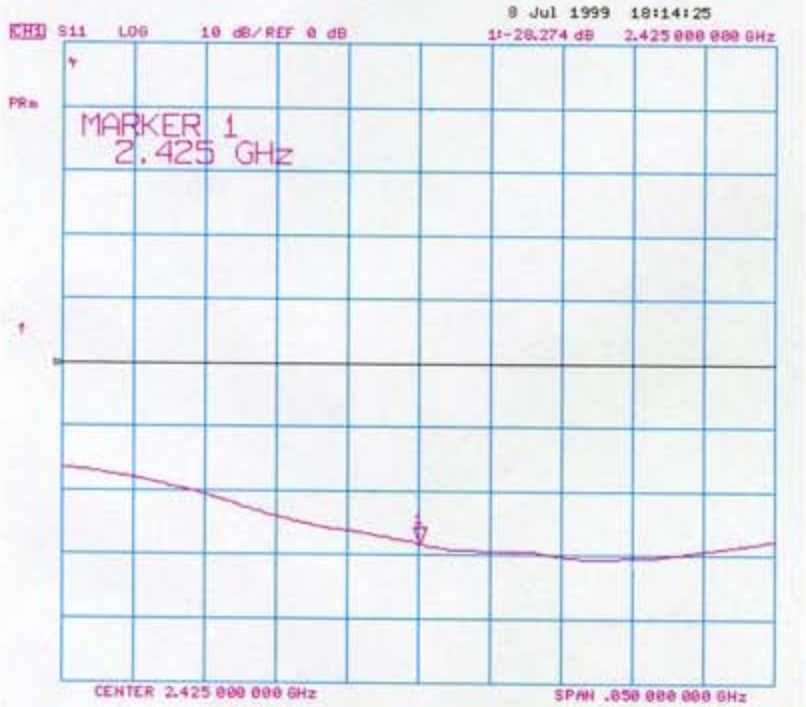
Algunas de las nuevas tarjetas 802.11 te permiten seleccionar la frecuencia central (canal) en la que emitirán. Es posible que basándote en esto quizás quieras calcular la antena nuevamente para que se acomode lo más posible a tu instalación.
HelixCalc.
He escrito una pequeña utilidad para diseñar e imprimir las plantillas que necesites, de modo que no estarás obligado a utilizar las que yo generé. Puedes cambiar varios de los parámetros (como se describe arriba), y después imprimir una plantilla para el cableado y otra para el plano de tierra. Puedes trabajar tanto en pulgadas como en centímetros. Desgraciadamente existe un pequeño error: la longitud total de la antena genera un resultado equivocado. Puedes calcular la longitud total de la antena manualmente multiplicando el numero de espiras por la longitud de una sola espira Slamda, que se muestra en una caja en el programa. He perdido el fuente del programa y quizás algún día lo vuelva a codificar. Sin embargo, la plantilla de bobinado que se imprime sí es correcta. HelixCalc
Rendimiento

He medido la eficiencia de estas antenas midiendo los parámetros S11. A continuación están las medidas de las dos antenas construí. El diagrama de arriba es la medida SWR (Standing Wave Ratio, Cociente de Onda Estacionaria) y el de abajo es la medida “Log return". Ambas antenas están muy bien, y cumplen las reglamentaciones del espectro radioeléctrico (SWR de 1:1.15 o mejor). Parece ser que el apaño de la tira de cobre/latón para ajustar las impedancias funciona extemadamente bien. Todavía no he probado el funcionamiento a más distancia.

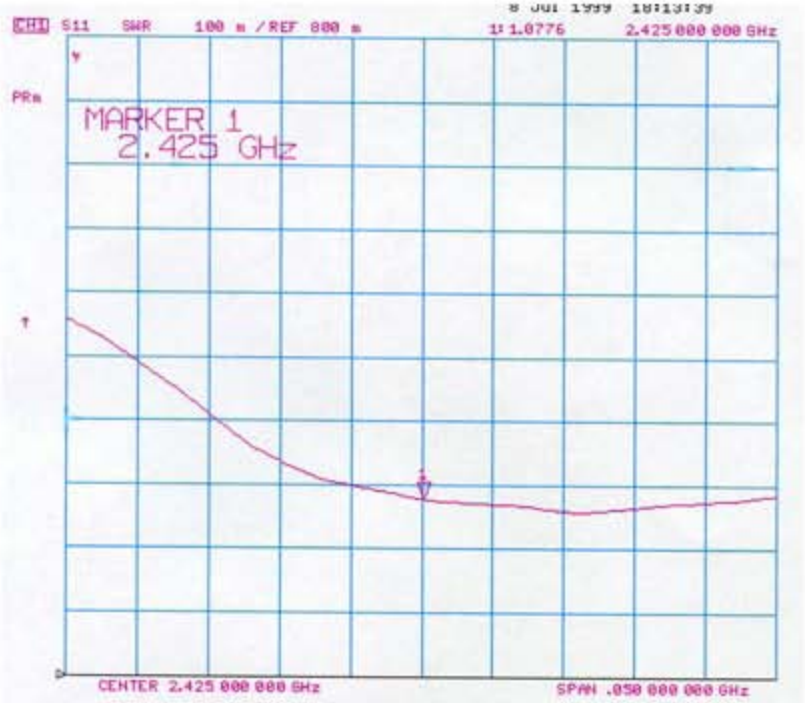
Hecha un vistazo aquí para ver algunas fotografías de antenas que hemos realizado otras personas y yo. Si montas una antena basada en este diseño, te agradecería que me enviases algunas fotos y una descripción , de manera que pueda añadirlas a esta sección.

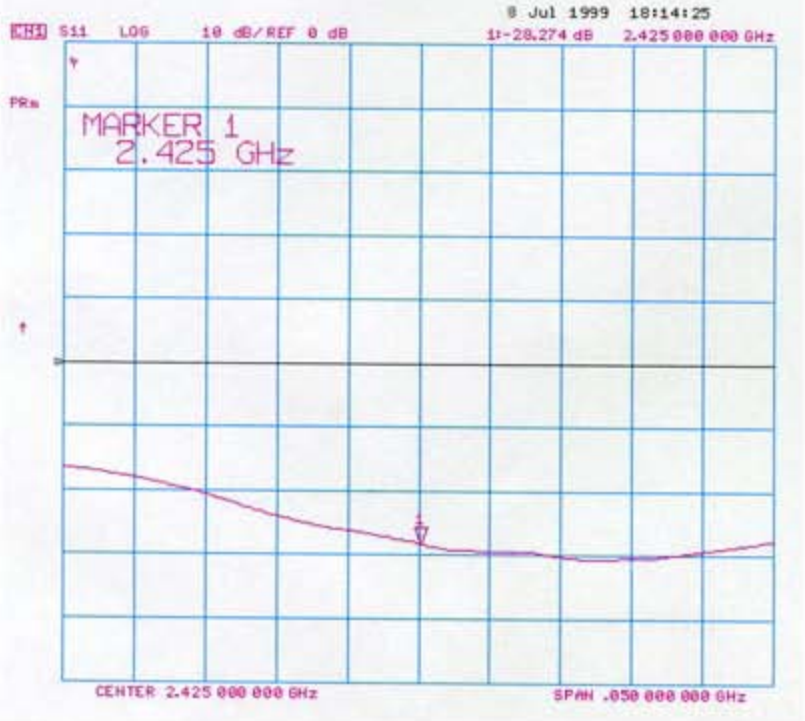
Antena #1


CH1 S11 SWR 100 m /REF 000 m
1: 1.0776
2.425 000 000 GHz
PRm
MARKER 1
2.425 GHz
CENTER 2.425 000 000 GHz
SPAN .050 000 000 GHz


8 Jul 1999 18:14:25
CH1 S11 LOG 10 dB/REF 0 dB
1: -28.274 dB
2.425 000 000 GHz
PRm
MARKER 1
2.425 GHz
CENTER 2.425 000 000 GHz
SPAN .050 000 000 GHz

Antena #2

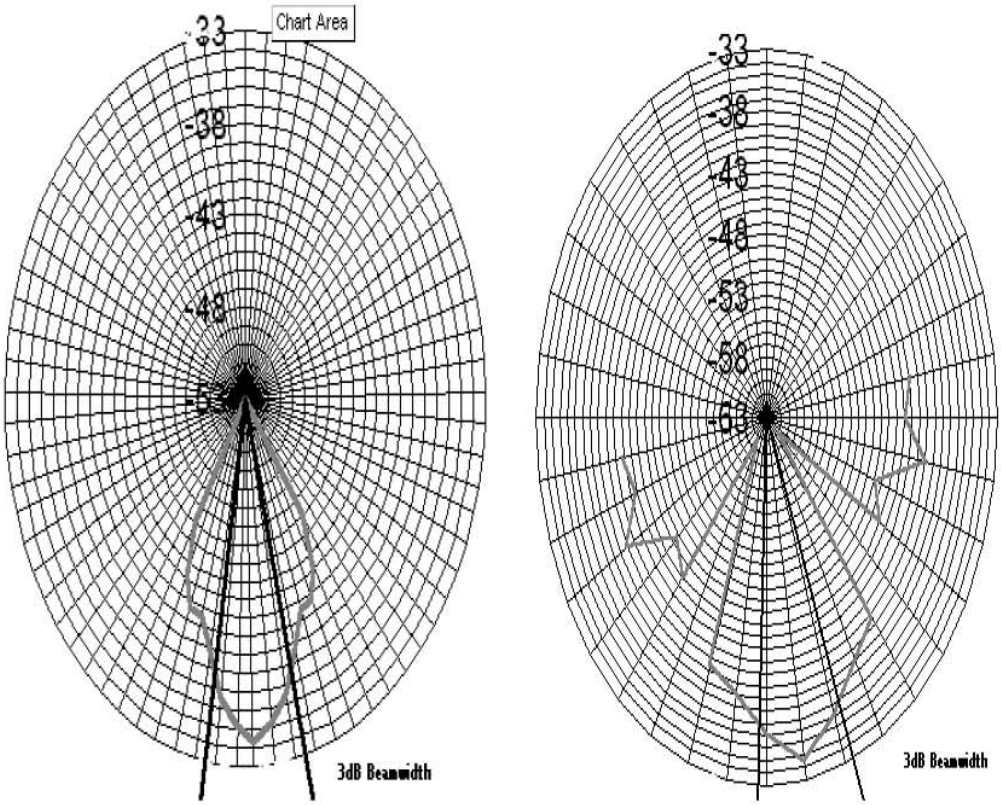

CH1 S11 SWR 100 m / REF 800 m
1: 1.0776
2.425 000 000 GHz
PRm
MARKER 1
2.425 GHz
CENTER 2.425 000 000 GHz
SPAN .050 000 000 GHz


8 Jul 1999 18:14:25
CH1 S11 LOG 10 dB/ REF 0 dB
1: -28.274 dB
2.425 000 000 GHz
PRm
MARKER 1
2.425 GHz
CENTER 2.425 000 000 GHz
SPAN .050 000 000 GHz

Patrones de radiación

A continuación tienes las medidas de algunos patrones de radiación. Desafortunadamente, debido a mi instalación, sólo pude hacer medidas a 180 grados en la parte delantera. El primer patrón se hizo tomando medidas con intervalos de 5 hasta 40 grados, y después dibujando la gráfica reflejada para tener el patrón completo. Los puntos de -3Db se marcaron de acuerdo con la teoría de que el lóbulo tiene aproximadamente 40 grados de ancho. Los segundos patrones se hicieron utilizando intervalos de 10 hasta 90 grados. En ellos se muestra claramente el primer nulo a unos 40 grados del eje de la antena. La relación delante-detrás se midió en 20 dB.

Half Power Beam Width = 52 / (C? * sqrt(n * S?)) degrees
= 52 / (1.066 * sqrt(13 * 0.31830))
= 23.98 degrees



Updated: 24 March 2001

GLOSARIO DE TÉRMINOS

BLUETOOHT

Es una tecnología de transferencia inalámbrica que permite conexiones, sin cables, a corta distancia, entre computadoras de escritorio y portátiles, asistentes digitales personales (PDA), teléfonos móviles, impresoras, escáner, cámaras digitales e incluso electrodomésticos. El fundamente de Bluetooth (un chipset) es transferir información y voz a la frecuencia de la banda ISM. Todos los dispositivos con tecnología Bluetooth vienen con una dirección estándar para conectar uno-a-uno o uno-a-siete (para formar una pico-red), con un alcance de hasta 10 metros (100 metros más adelante9, utilizando una transmisión de baja potencia. Bluetooth no solamente posee una elevada velocidad de transferencia de 1MB/s, también podría ser encriptado con un código pin. Con una velocidad de salto de 1600 saltos por segundo, su interceptación es difícil y la interferencia por ondas electromagnéticas es pequeña.

BOOT

(En inglés pateo) Inicio de una computadora.

BUS

Conjunto de dispositivos de conexión utilizados por los distintos componentes de unacomputadora para intercambiar datos e información. Se caracterizan por su capacidad y los elementos que unen, clasificándose en bus de direcciones, bus de datos, bus de entrada/salida, etcétera.

BYTE

Ocho bits que representan un carácter. Unidad básica de información con la que operan las computadoras.

CD ROM (COMPACT DISC-READ ONLY MEMORY)

La aplicación de la tecnología digital y láser a la informática supuso la transferencia de los compact disc utilizados de manera genérica para la comercialización de grabaciones musicales al campo de las computadoras. Los CDROM cuentan con importantes ventajas: su bajo precio de producción, su fiabilidad, su capacidad (hasta 600 MB) y su facilidad de uso y manejo. Un único pero importante inconveniente está frenando su expansión como soporte de almacenamiento alternativo al tradicional disquete de tecnología magnética: no puede ser regrabado. Una vez grabado el CD-ROM, sólo puede realizarse un acceso de lectura a éste. Aunque existen dispositivos de grabación de CD-ROMs, su precio queda fuera del rango en el que se mueven los usuarios domésticos.
Muchos expertos se empeñan en asegurar que el CD-ROM es el soporte de la información del futuro y, de hecho, estamos asistiendo a una increíble proliferación de títulos de todo tipo y de literatura asociada al fenómeno del CD-ROM. Esta una unidad óptica que funciona a base de láser que lee las impurezas del disco, la cual son transformadas en cadenas de bits (1 y 0).

CFDISK

Comando en Linux que nos ayuda a crear particiones en nuestro disco duro.

CUSTOM

Personalizar.

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL).

Protocolo de configuración dinámica de host. Protocolo que usan las computadoras para obtener información de configuración. El DHCP permite asignar una dirección IP a una computadora sin

requerir que un administrador configure la información sobre la computadora en la base de datos de un servidor.

DRUID

Programa que sirve para realizar particiones en Linux.

DSSS

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

DRIVE-BY HACKING

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

ESID

Identificador del punto de acceso, es un nombre del tipo mi red sin hilos, utilizado por los clientes para conectarse a el.

ETHERNET

Tipo de red muy estandarizada cuyo desarrollo inicial corresponde a Xerox. Su topología es en bus (no confundir con el concepto Bus como "canales" internos a la computadora). Puede alcanzar velocidades entre 1 y 20 Mbps (megas por segundo), aunque es normal los 10 Mbps utilizando banda base. Se monta sobre cable coaxial.

FIRMWARE

Son programas, generalmente responsables de un dispositivo, que tienen como característica común que están almacenados en memoria ROM (Memoria de sólo lectura).

FRAME

En gráficos por computadora, contenido de una pantalla de datos o su espacio de almacenamiento equivalente.

1. En comunicaciones, bloque fijo de datos transmitidos como una sola entidad. También llamado packet (paquete).
2. En autoedición, caja movible y de tamaño flexible, que contiene una imagen gráfica.
3. En inteligencia artificial, estructura de datos que contiene una descripción general de un objeto, que se deriva de conceptos básicos y de la experiencia

FRAME RELAY

Sistema de transmisión basado en la conmutación.

GRUB

Gestor de arranque.

HW

Abreviación de Hardware todo lo físico que se puede tocar en una computadora.

HERTZ

Frecuencia de vibraciones eléctricas (ciclos) por segundo. Abreviado "Hz"; un Hz es igual a un ciclo por segundo. En 1983, Heinrich Hertz detectó las ondas electromagnéticas.

HOST

Utilizado a veces como sinónimo de mainframe, en realidad identifica a la computadora central en un sistema informático complejo. Computador central o principal en un entorno de procesamiento distribuido. Por lo general se refiere a una gran computadora de tiempo compartido o una computadora central que controla una red.

HOTSPOT

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

HUB

Dispositivo que integra distintas clases de cables y arquitecturas o tipos de redes de área local. Existe una palabra castellana para identificar un Hub, Concentrador. La puntualización es que el Concentrador está a nivel 3 de OSI. Núcleo, centro. Dispositivo de conexión central en una red que une líneas de comunicaciones en una configuración en estrella. Los núcleos pasivos son unidades de conexión que no agregan nada a los datos que pasan a través de ellos. Los núcleos activos, algunas veces también llamados repetidores de multipuertos, regeneran los bits de datos con el fin de mantener una señal fuerte, y los núcleos inteligentes proporcionan funcionalidad incrementada.

IEEE (INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS)

Asociación de profesionales norteamericanos que aporta criterios de estandarización de dispositivos eléctricos y electrónicos.

IP

Dirección IP. Matrícula que identifica a un ordenador de la red. A los ordenadores personales se les asigna una IP adress para que naveguen por la red, que cambia en cada sesión de acceso a Internet.

LAN (Red de Área Local)

Generalmente se considera que son las redes cuyo ámbito está restringido a un edificio o a unidades físicas similares.

LAP TOP

Computadora portátil, construida con una pantalla líquida, teclado integrado con mouse anexo. Estas computadoras tienen gran uso para las personas de negocios que deben de estar fuera de la compañía y gracias a un módem pueden estar conectados a la misma. Las laptops son muy sofisticadas y a la vez muy costosas.

LILO

Gestor de arranque encargado de arrancar el so.

LINUX

Es, en un sentido muy amplio, un sistema operativo. Sin embargo, más purista y específicamente, Linux es un kernel. El kernel de un sistema operativo, se refiere a su núcleo. El kernel de un sistema operativo se encarga de gestionar los recursos de la memoria, habilitar el acceso a los sistemas de archivos, administrar recursos de red, y muchas cosas más.

MAC

Macintosh. Serie de computadores personales de Apple. El Mac original con su gabinete vertical se introdujo en 1984. El sistema operativo del Mac con su interfaz gráfica de usuario ha proporcionado una medida de consistencia y facilidad de uso que es sin igual. La familia Macintosh es la serie de computadores personales más grande, en uso, y no compatible con IBM.<p>Hasta 1994, los Mac recibían potencia exclusivamente de la familia de CPU 680x0 de Motorola. En 1994, Apple introdujo los Power Macintosh (PowerMac), que usan la PowerPC CPU y proporcionan un desempeño mejorado. Los PowerMac utilizan una versión PowerPC del Mac OS, que ejecuta aplicaciones PowerMac nativas y emula aplicaciones Mac 680x0. También ejecuta aplicaciones DOS y Windows a través de emulación de Insignia Solutions.

(Medium Access Control) En redes, es una subcapa de la capa de enlace que aparece en las Redes de Area Local y se encarga de controlar el acceso al medio. Es diferente para cada tipo de red, de acuerdo con la técnica que se emplee.

MAN

Es un tipo de red que se expande por pueblos o ciudades y se interconecta mediante diversas instalaciones públicas o privadas, como el sistema telefónico o los suplidores de sistemas de comunicación por microondas o medios ópticos.

MBPS

Medida para la velocidad de transmisión hecha en mega bits por segundo.

MS-DOS (MICROSOFT DÍSK OPERATING SYSTEM)

Sistema operativo de disco monousuario (para un solo usuario) y compatible (que puede ejecutarse en cualquier computadora personal compatible con la IBM-PC), diseñado por la compañía Microsoft para la PC de IBM, introducida en 1981. Se ejecuta automáticamente cuando se arranca la PC. La forma de dictarle órdenes a DOS es a través de instrucciones tipeadas en líneas de comandos a partir de un signo inicial. Esta interfaz presupone la memorización de una serie de sintaxis de signos (barras de directorios, letras, signos de puntuación, etc.) y palabras para cumplir con distintas tareas y recorridos dentro del sistema. Luego de conocer todas sus variantes, los usuarios de DOS pueden lograr un grado de control satisfactorio con el fin de crear directorios, realizar backups, copiar archivos y subir o bajar por las ramas de los directorios, entre otras actividades.

PAN

Tipo de red donde permite interconectar dispositivos electrónicos dentro de un rango de pocos metros, para comunicar y sincronizar información.

PCI (PERIPHERAL COMPONENT INTERFACE)

Término ingles que significa Conexión de Componentes Periféricos.
Se trata de un tipo de ranura de conexión para tarjetas de aplicación que se encuentran en la placa base de la computadora.

PCMCIA (PERSONAL COMPUTER MEMORY CARD INTERNATIONAL ASSOCIATION)

Asociación Internacional de tarjetas de Memoria para Computadoras Personales. Tarjeta estandarizada de expansión para computadoras personales. Tecnología que permite conectar fácilmente gran variedad de dispositivos a una computadora, normalmente un portátil o un PDA. Para conectar este dispositivo es necesario que el ordenador disponga del mismo tipo de ranura.

PDA (PERSONAL DIGITAL ASSITANT)

Asistentes digitales personales. Es una pequeña computadora que cabe en el bolsillo. Se utilizan como agenda y como bloc de notas.

PUNTO DE ACCESO O “ACCESS POINT”

El dispositivo físico, similar a un hub, permite al usuario acceder a una red inalámbrica.

RED

La intercomunicación entre ordenadores permite no sólo el intercambio de datos, sino también compartir recursos de todo tipo, optimizando así elevadas inversiones. Las redes son el soporte para estas conexiones y (aparte la diferenciación más genérica entre redes públicas y privadas), según el objeto de definición, la terminología es variada.

RED AD HOC

Conexión punto a punto entre dos computadoras mediante tarjetas inalámbricas, no es necesario disponer de un punto de acceso.

ROUTER

Originalmente, se identificaba con el término gateway, sobre todo en referencia a la red Internet. En general, debe considerarse como el elemento responsable de discernir cuál es el camino más adecuado para la transmisión de mensajes en una red compleja que está soportando un tráfico intenso de datos.

ROOT

Directorio raíz en un sistema de directorios o en Linux súper usuario.

RX

Abreviación de receptor.

SET UP

Programa de preparación, de montaje y de ajuste que se utiliza para configurar un sistema o aplicación para un entorno computacional determinado. En las PC se aplica para informar al sistema operativo sobre un cambio importante en un dispositivo, por ejemplo, en una nueva unidad de disco o en un monitor. Generalmente, la instalación de los programas en inglés se realiza desde un archivo con este nombre.

SLOT

Ranura, en español. Se trata de cada uno de los alojamientos que tiene la placa madre en los que se insertan las tarjetas de expansión. Todas estas ranuras están conectadas entre sí y una computadora personal tiene generalmente ocho, aunque puede llegar a doce.

SOURCE

Fuente.

SW

Abreviación de software todo lo intangible dentro de una computadora.

SWAP

Memoria de intercambio.

SWITCH

Dispositivo de red que filtra, envía e inunda de frames en base a la dirección de destino de cada frame. El switch opera en la capa de enlace de datos del modelo OSI. 2.) Término general que se aplica a un dispositivo electrónico o mecánico que permite establecer una conexión cuando resulte necesario y terminarla cuando ya no hay sesión alguna que soportar.

TARJET

Destino.

TOPOLOGÍA

Forma física de integrar y distribuir un red de computadoras. La topología a usar esta directamente relacionada con el tamaño de la red (n de pc's), tamaño de la empresa o laboratorio.

TX

Abreviación de transmisor.

USB (UNIVERSAL SERIAL BUS)

Bus serie universal. La característica principal de este bus reside en que los periféricos pueden conectarse y desconectarse con el equipo en marcha, configurándose de forma automática. Conector externo que llega a transferencias de 12 millones de bits por segundo. Totalmente PnP, sustituirá al puerto serie y paralelo, gracias a la posibilidad de conectar 127 dispositivos.

WAN (RED DE ÁREA AMPLIA)

Cualquier red pública es de este tipo. Su característica definitoria es que no tiene límites en cuanto a su amplitud. Existen redes privadas de gran cobertura soportadas en estructuras físicas que son propiedad de operadores nacionales o internacionales.

WARCHALKING

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

WEP

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

WIFI

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

WINDOWS

Entorno gráfico diseñado por Microsoft para realizar todas las funciones efectuadas por DOS de manera más simple y amigable. Windows ha cumplido con dos objetivos: la posibilidad de realizar varias tareas en forma simultánea (multitarea) y el intercambio de información entre distintos programas. Windows adhiere a la tendencia GUI (interfaz gráfica de usuario) Plantea la recreación de un escritorio real de trabajo, presentándolo gráficamente en el monitor. Para ello, exhibe íconos, pequeñas representaciones gráficas que evocan a los objetos de la vida real y que pueden ser activados mediante la presión de un botón del mouse.

WIRELESS

Tecnología relativamente estandarizada para redes inalámbricas que utilizan ondas de radio.

WISP

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

WLAN

Acrónimo de "Wireless Local Area Network", red sin hilos de ámbito local, no confundir con LAN o WAN.

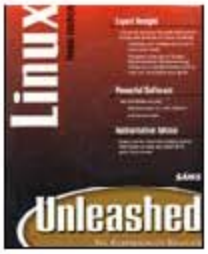
BIBLIOGRAFÍA

Title: Linux Complete Command Reference
Author(s): Red Hat
Imprint: Sams
Publisher: Macmillan Computer Publishing
ISBN:0672311046

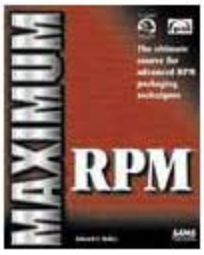
Title: Linux Configuration and Installation
Author(s): Patrick Volkerding
Imprint:M&T Books
Publisher:IDG Books Worldwide, Inc.
ISBN:1558285660

Title: Linux in Plain English
Author(s): Patrick Volkerding, Kevin Reichard, Eric Foster-Johnson
Imprint:M&T Books
Publisher:IDG Books Worldwide, Inc.
ISBN:1558285423

Title:LINUX System Administrator's Survival Guide
Author(s):TIM PARKER
Imprint: Sams
Publisher: Macmillan Computer Publishing
ISBN:0672308509



Title: Linux Unleashed, Third Edition
Author(s): Tim Parker
Imprint: Sams
Publisher: Macmillan Computer Publishing
ISBN:0672313723



Title: Maximum RPM (RPM)
Author(s): Edward Bailey
Imprint: Sams
Publisher: Macmillan Computer Publishing
ISBN:0672311054

Title: Red Hat Linux Unleashed, Second Edition
Author(s): David Pitts, et al.
Imprint: Sams
Publisher: Macmillan Computer Publishing
ISBN:0672311739

Title: Using Linux
Author(s): William Ball
Imprint: Que
Publisher: Macmillan Computer Publishing
ISBN:0789716232

Title:Routing TCP/IP
Author(s): Jeff Doyle
Publisher: Macmillan Computer Publishing

MESOGRAFÍA

http://redwireless.rastreador.com/
http://www.todo-linux.com/modules.php?name=News&file=article&sid=2482
http://linuv.uv.es/article35.html
http://www.gpltarragona.org/node/view/203
http://www.linuxwiki.de/
http://wiki.colinux.org/cgi-bin
http://linux.editme.com/
http://bulma.net/body.phtml?nIdNoticia=1309
http://www.wl0.org/~sjmudd/wireless/network-structure/html/index.html#AEN55
http://www.atinachile.cl/node/2132
http://www.mailxmail.com/WEB%20CAPITULO%202/ANTENAS%20DIR%20Y%20OMNI.htm
http://www.techpage.com/topologia%20de%20redes.htm
http://www.adventonetworks.com
http://www.lug-wireless.com/Antena%20helicoidal.html
http://www.lug-wireless.com/WL200%20recontra-mini-howto.html
http://www.almontewireless.com
http://ozlabs.org/people/dgibson/dldwd/
http://www.linux-wlan.org/
http://hostap.epitest.fi/
http://bulma.net/body.phtml?nIdNoticia=1891
http://mnm.uib.es/~gallir/
http://bulma.net/body.phtml?nIdNoticia=1309
http://www.sjdjweis.com/linux/proxyarp/
http://www.camaradediputados.org.mx/CAPITULO%20II%20Del%20espectro%20radioel%E9ctrico.htmL
http://www.wa1mba.org/rfconn.htm,
http://minyos.its.rmit.edu.au/~rmmca/pl259tst.html,
http://www.gohts.com/techwire/coax.html
http://www.tm.agilent.com/
http://www.vandenhul.com/other/c-connec.htm
http://www.connectronicsinc.com/,
http://www.mackie.com/TechSupport/Glossary/M-Z.asp
http://www.deltarf.com/
http://www.maurymw.com/
http://www.tldp.org/HOWTO/Adv-Routing-HOWTO-16.html#ss16.2
http://www.conceptronic.net/products.asp?p=C11iDT&Aktie=5&mt=C11iDT&mp=11
http://www.conceptronic.net/products.asp?p=CON11C&Aktie=5&mt=CON11C&mp=1 http://www.polakilandia.org/gwlan/
http://rpmfind.net/
http://www.commonmicrowave.com
http://www.netscum.com/~clapp/wireless.html

http://frenopatico.net
http://www.cis.ohio-state.edu/~jain/cis788-97/wireless_lans/index.htm|
http://www.amazon.com/
http://computers.cnet.com/hardware
http://www.jdjstore.com/inprow20.html
http://www.softelecom.com/modelo_osi/
http://www.palowireless.com/i802_11/
www.sss-mag.com/pdf/802_11tut.pdf
http://www.networkcomputing.com/1115/1115ws2.html
http://www.intelligraphics.com/articles/80211_article.html
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifisoho.mspx
http://debaser.ath.cx/atroz/docs/aps/hostapmode.html