Redes Inalámbricas en los Países en Desarrollo

Una guía práctica para planificar y construir infraestructuras de telecomunicaciones de bajo costo

Redes Inalámbricas en los Países en Desarrollo

Por más información acerca de este proyecto, visítenos en *http://wndw.net/*

Primera edición, enero de 2006
Segunda edición, junio de 2007

ISBN: 978-0-9778093-5-6

Tabla de Contenido

Sobre este Libro

¿Dónde Comenzar?

Una Introducción Práctica a la Física de Radio

Diseño de Redes

Antenas y Líneas de Transmisión

Equipamiento para Redes

Seguridad

Construyendo un Nodo en Exteriores

Resolución de Problemas

Voz sobre IP

Estudios de Casos

Sobre este Libro

Este libro es parte de un conjunto de materiales sobre el mismo tema: Redes Inalámbricas en los Países en Desarrollo. Aunque no todos los materiales están disponibles en el momento de esta edición, los mismos van a incluir:

- Libros impresos
- Una versión electrónica gratuita en formato PDF (Portable Digital Format) del texto que puede ser distribuida libremente
- Una lista de correo electrónico para la discusión de conceptos y técnicas descritas en el libro
- Casos de estudio adicionales, materiales de entrenamiento e información relacionada

Para consultar estos y otros materiales, visite nuestro sitio web en: *http://wndw.net/*

Las copias impresas pueden ser ordenadas desde el servicio de impresión a demanda Lulu.com. Para conocer los detalles sobre cómo ordenar una copia impresa puede consultar el sitio web (*http://wndw.net/*). El PDF va a ser actualizado periódicamente y solicitándolo desde el servicio de impresión a demanda se asegura que usted va a recibir siempre la última revisión.

El sitio web va a incluir más casos de estudio, referencias a páginas externas, así como actualizaciones del equipamiento. Aquellos voluntarios que quieran aportar ideas son bienvenidos. Por favor suscríbase a la lista de correo electrónico y envíe sus comentarios.

Los materiales de entrenamiento fueron escritos para cursos dados por la Association for Progressive Communications (APC Asociación para el Progreso de las Comunicaciones) y el Abdus Salam International Centre for Theoretical Physics (ICTP, Centro Internacional de Física Teórica). Para más detalles acerca de esos cursos y sus materiales de trabajo vea la página web *http://www.apc.org/wireless/* y *http://wireless.ictp.it/*. Información adicional fue suministrada por la International Network for the Availability of Scientific Publications (INASP, Red internacional para la Disponibilidad de Publicaciones Científicas), *http://www.inasp.info/*. Algunos de esos materiales han sido incorporados directamente en este libro.

Créditos

Este libro se inició como el proyecto BookSprint en la versión 2005 del WSFII, en Londres, Inglaterra (*http://www.wsfii.org/*). Un equipo central de siete personas construyó los lineamientos iniciales durante el transcurso del evento, presentó los resultados en la conferencia y escribió el libro en el curso de unos pocos meses. Rob Flickenger actuó como autor principal y editor. A lo largo del proyecto el grupo central solicitó activamente la contribución y la retroalimentación de la comunidad de redes inalámbricas.

Grupo Central

- **Corinna "Elektra" Aichele**. Los intereses principales de Elektra incluyen: sistemas autónomos de energía y sistemas de comunicación inalámbrica (antenas, redes inalámbricas de largo alcance y redes mesh). Realizó una pequeña distribución de Linux basada en Slackware orientada a redes mesh. Esta información es por supuesto redundante si uno lee el libro… *http://www.scii.nl/~elektra*

- **Rob Flickenger** fue el autor principal, editor e ilustrador de este libro. Ha estado escribiendo profesionalmente desde el 2002. Escribió y editó varios libros incluyendo, Building Wireless Community Networks y Wireless Hacks, de los cuales existen las versiones en español, Construyendo Redes Inalámbricas Comunitarias y Trucos Inalámbricos, publicados por O'Reilly Media. Co-fundó Metrix Communication LLC (*http://metrix.net/*), una compañía de equipamiento inalámbrico dedicada a las redes inalámbricas ubicuas y al desarrollo de software y estándares libres. Antes de convertirse en miembro activo de SeattleWireless (*http://seattlewireless.net*), fue uno de los fundadores principales del proyecto NoCat (*http://nocat.net/*).

  El objetivo último de Rob es la realización de Infinite Bandwidth Everywhere for Free (Ancho de banda infinito y gratuito en todas partes). Algunas de las aventuras vividas a lo largo del camino para la realización este objetivo están publicadas en *http://constructiveinterference.net/*

- **Carlo Fonda** es miembro de la Radio Communications Unit (Unidad de Radiocomunicaciones) del Abdus Salam International Centre for Theoretical Physics (ICTP, Centro Internacional de Física Teórica) en Trieste, Italia.
- **Jim Forster** ha dedicado su carrera al desarrollo de software, trabajando mayormente en redes y sistemas operativos en compañías de productos. Tiene experiencia en la puesta en marcha de varias compañías fallidas en Silicon Valley, así como de una exitosa, Cisco Systems. Luego de trabajar mucho en el desarrollo de productos, sus actividades más recientes se centran en proyectos y políticas para mejorar el acceso a Internet en los países en vías de desarrollo. Puede ser contactado en *jrforster@mac.com*.
- **Ian Howard**. Luego de viajar alrededor del mundo como paracaidista del ejército canadiense, Ian Howard decidió cambiar su arma por una computadora.

  Después de graduarse en ciencias del medio ambiente en la Universidad de Waterloo, escribió en una propuesta, “La tecnología inalámbrica tiene la oportunidad de eliminar la brecha digital. Las naciones pobres, que no tienen la infraestructura para la interconectividad como nosotros, ahora van a ser capaces de crear una infraestructura inalámbrica." Como recompensa, Geekcorps lo envió a Mali como el Gerente de Programas de Geekcorps Mali, donde lideró un grupo que dotó estaciones de radio con interconexiones inalámbricas y diseñó sistemas para compartir contenidos.

  Actualmente es consultor en varios programas de Geekcorps.
- **Tomas Krag** dedica sus días al trabajo en wire.less.dk, una organización sin fines de lucro, con base en Copenhaguen, que fundó con su amigo y colega Sebastian Büttrich a principios del 2002. wire.less.dk se especializa en soluciones con redes inalámbricas y tiene su foco principal en redes inalámbricas de bajo costo para los países en desarrollo.

  Tomas también está asociado al Tactical Technology Collective http://tacticaltech.org/, una organización sin fines de lucro con base en Ámsterdam “para fortalecer los movimientos de redes y tecnología social en países en transición y en vías de desarrollo, así como promover el uso efectivo, consciente y creativo de las nuevas tecnologías por parte de la sociedad civil.” Actualmente sus energías están avocadas al Wireless Roadshow (*http://www.thewirelessroadshow.org/*), un proyecto que ayuda a socios de la sociedad civil en los países en desarrollo a planificar, construir y mantener soluciones de conectividad basadas en frecuencias libres y tecnologías abiertas.
- **Marco Zennaro**, también conocido como marcusgennaroz, es un ingeniero electrónico que trabaja en el ICTP en Trieste, Italia. Un radioaficionado que ha estado utilizando BBSes desde que era un

adolescente, es feliz de conjugar ambas actividades trabajando en el campo de las redes inalámbricas. Aún lleva consigo su Apple Newton.

Además del grupo central, otras personas han contribuido en la escritura, sugerencias y la edición del libro, brindando sus habilidades para hacer de este proyecto lo que es.

Colaboradores

- **Sebastián Büttrich** (*wire.less.dk*) posee conocimientos generales en tecnología con formación en programación científica y física. Originario de Berlín, Alemania, trabajó con IconMedialab en Copenhaguen desde 1997 a 2002. Posee un Ph.D. en física cuántica de la Universidad Técnica de Berlín. Su conocimiento en física incluye campos tales como radio frecuencia y espectroscopía de microondas, sistemas fotovoltaicos y matemáticas avanzada. También es músico profesional.
- **Kyle Johnston**, *http://www.schoolnet.na/*
- **Adam Messer**. Habiéndose capacitado originalmente como científico de insectos, Adam Messer se metamorfoseó en un profesional de las telecomunicaciones luego de que una conversación inesperada en 1995 lo llevó a fundar uno de los primeros ISPs (Proveedores de Servicios de Internet) de África. Siendo pionero en proveer servicios inalámbricos en Tanzania, Messer trabajó once años en África del este y del sur en comunicaciones de voz y datos tanto para nuevas empresas como para multinacionales de celulares. En la actualidad reside en Amán, Jordania.
- **Ermanno Pietrosemoli** ha estado involucrado en la planificación y construcción de redes de computadoras durante los últimos veinte años. Como presidente de la Fundación Escuela Latinoamericana de Redes “EsLaRed”, www.eslared.org.ve, ha estado enseñando comunicaciones de datos en varios países, manteniendo su base en Mérida, Venezuela.
- **Dana Spiegel** es consultor independiente de software y fundador de sociableDESIGN (*www.sociabeDESIGN.com*), una firma consultora que se especializa en software social y tecnologías inalámbricas. Se desempeña como director ejecutivo y como miembro de la junta directiva de NYCwireless (*www.nycwireless.net*), una organización sin fines de lucro de la ciudad de Nueva York que se dedica al desarrollo de redes inalámbricas públicas gratuitas. También escribe el blog Wireless Community (*www.wirelesscommunity.info*).
- **Alberto Escudero-Pascual** y **Louise Berthilson** son los fundadores de IT+46 *http://www.it46.se*, una compañia sueca que se creo inicialmente para localizar aplicaciones informáticas libres a la lengua Suajili. La empresa trabaja con el objetivo de transfeir conocimientos a los beneficiarios para el cambio social. Desde el año 2004 han capacitado a más 300 personas en

12 países y liberado más de 500 páginas de documentación en las áreas de comunicaciones inalámbricas, VoIP, seguridad y TICs para el desarrollo.

Brindaron su Apoyo

- **Lisa Chan** (*http://www www.cowinanorange.com/*) fue la editora principal.
- **Richard Lotz** (*http://greenbits.net/~rlotz/*) realizó revisiones técnicas y sugerencias. Trabaja en proyectos de SeattleWireless y prefiere dejar su nodo (y su casa) desconectados.
- **Casey Halverson** (*http://seattlewireless.net/~casey/*) realizó revisiones técnicas y sugerencias.
- **Catherine Sharp** (*http://odessablue.com/*) colaboró en la edición.
- **Matt Westervelt** (*http://seattlewireless.net/~mattw/*) realizó revisiones técnicas y colaboró en la edición. Es el fundador de SeattleWireless (*http://seattlewireless.net*), y un difusor de FreeNetworks por todo el mundo.

La Traducción al Castellano

El equipo del Booksprint quiere agradecer la enorme contribución realizada por colegas y amigos alrededor del mundo quienes hicieron posible que el libro "Redes Inalámbricas en los Países en Desarrollo" esté disponible en varios idiomas.

La traducción al castellano de la primera edición fue realizada por Alexandra Dans, y revisada por Guido Iribarren, Bernabé García, Magdalena Bergamino, Javier Vito Spezzi, Miguel Angel Argañaraz, Bruce Schulte, Lourdes Pietrosemoli y Sylvia Cadena. El libro fue editado por Ermanno Pietrosemoli, quien se encargó de garantizar que los conceptos técnicos fueran preservados y expresados correctamente. La coordinación de las contribuciones y revisiones previas se realizó con el apoyo de WiLAC <*www.wilac.net*>.

El Equipo de trabajo quiere agradecer a nuestras organizaciones y familias que nos han permitido dedicar tiempo y energía para hacer esto posible:

- Fundación EsLaRed <*www.eslared.org.ve*>
- WiLAC <*www.wilac.net*>
- Instituto para la Conectividad en las Américas - ICA <*www.icamericas.net*>

El equipo quiere agradecer a los organizadores de WSFII por proveer el espacio, apoyo y el ancho de banda ocasional que sirvió como incubadora para este proyecto. Queremos agradecer especialmente a los gestores de

las redes comunitarias en cualquier lugar, quienes dedican mucho de su tiempo y energía para alcanzar la promesa de una Internet global. Sin ustedes las redes comunitarias no podrían existir.

Sobre la segunda edición

Para esta segunda edición, se incorporó como un nuevo capítulo, la guía sobre VoIP desarrollada por Alberto Escudero-Pascual y Louise Berthilson de IT+46 en Suecia, así como cuatro estudios de caso sobre despliegue de redes inalámbricas en América Latina: 1) la experiencia del Sistema de Información Agraria de Huaral, en Perú; 2) la experiencia para el despliegue de la red del estado de Mérida, en Venezuela; 3) la experiencia de ChileSinCables, en Chile; y 4) EHAS - Enlace Hispanoamericano de Salud.

1
¿Dónde Comenzar?

Este libro fue realizado por un equipo de personas quienes, cada una en su campo, son participantes activas en la inacabable tarea de expandir la cobertura de Internet más allá de lo que nunca ha llegado. La masiva popularidad de las redes inalámbricas ha llevado a una disminución continua del costo del equipamiento, mientras que la capacidad del mismo continúa incrementándose. Creemos que aprovechando este contexto, las personas van a comenzar a formar parte en la construcción de su propia infraestructura de comunicaciones. Esperamos no sólo convencer al lector de que esto es posible, sino también, mostrarle cómo hemos logrado que esas redes funcionen ofreciendo la información y herramientas necesarias para emprender una red en su comunidad.

La infraestructura inalámbrica puede ser construida a muy bajo costo en comparación con las alternativas tradicionales de cableado. Pero construir redes inalámbricas se refiere sólo en parte al ahorro de dinero. Proveyendo a su comunidad con un acceso a la información más sencillo y económico, la misma se va a beneficiar directamente con lo que Internet tiene para ofrecer. El tiempo y el esfuerzo ahorrado gracias a tener acceso a la red global de información, se traduce en bienestar a escala local, porque se puede hacer más trabajo en menos tiempo y con menos esfuerzo.

Así mismo, la red se transforma el algo más valioso cuanta más gente esté conectada a ella. Las comunidades que se conectan a Internet a una alta velocidad participan en el mercado global, donde las transacciones suceden alrededor del mundo a la velocidad de la luz. Las personas de todo el mundo se están encontrando con que el acceso a Internet les brinda una voz para discutir sus problemas, políticas, y cualquier cosa que sea importante en sus vidas, de una forma con la cual el teléfono y la televisión simplemente no pueden competir. Lo que hasta hace poco sonaba a ciencia ficción se está

transformando en realidad, y esta realidad se está construyendo sobre redes inalámbricas.

Pero aún sin acceso a Internet, las redes inalámbricas comunitarias tienen un gran valor. Les permiten a las personas colaborar en proyectos a largas distancias. Comunicaciones de voz, el correo electrónico y otros datos pueden ser intercambiados a un bajo costo. Involucrando a las personas de la comunidad en la construcción de la red, el conocimiento y la confianza se extienden a toda la comunidad y la gente comienza a comprender la importancia de tomar parte en su infraestructura de comunicaciones. En última instancia, la gente se hace consciente de que las redes de comunicaciones se hacen para permitirles conectarse unos con otros.

En este libro nos enfocaremos en las tecnologías inalámbricas de redes de datos que operan en la familia de estándares 802.11. Aunque dicha red puede transmitir datos, voz y video (tal como el tráfico tradicional de Internet), las redes descritas en este libro son redes de datos. No cubrimos GSM, CDMA u otras tecnologías inalámbricas de voz, ya que el costo de utilizar esas tecnologías va mucho más allá del alcance de la mayoría de los proyectos de las comunidades.

Propósito de este libro

El objetivo general de este libro es ayudarlo a usted a construir tecnologías de comunicación accesibles para su comunidad por medio del buen uso de todos los recursos disponibles. Utilizando equipamiento económico disponible, se pueden construir redes de alta velocidad de transmisión que conecten áreas remotas, proveer acceso de banda ancha donde ni siquiera existe la conexión por discado y conectarlo a usted y a sus vecinos a Internet. Utilizando materiales locales y fabricando partes usted mismo se pueden armar enlaces de red confiables con muy poco presupuesto. Más aún, trabajando con su comunidad usted puede construir una infraestructura de telecomunicaciones que beneficie a todos los que participen en ella.

Este libro no es una guía para configurar una tarjeta de radio en su laptop o seleccionar los productos adecuados a la red de su hogar. El énfasis está puesto en el armado de infraestructuras de enlace con la intención de ser utilizadas como el eje de redes inalámbricas de amplio alcance. Con este objetivo en mente, la información es presentada desde varios puntos de vista, incluyendo factores técnicos, sociales y económicos. Los estudios de casos presentados muestran los intentos de instalación de esas redes, los recursos utilizados, y los resultados obtenidos en dichos intentos.

Desde los primeros experimentos con transmisión de chispas con bobinas interrumpidas al final del siglo antepasado, la tecnología inalámbrica ha sido

un área que ha evolucionado rápidamente. Si bien en este libro proporcio-namos ejemplos específicos de cómo construir enlaces de datos de alta velocidad, las técnicas descritas en el mismo no intentan remplazar las infraestructuras de cableado existentes (tales como el sistema telefónico y la fibra óptica). Por el contrario, estas técnicas permiten incrementar la capacidad de esos sistemas, y proveer conectividad en áreas donde la fibra u otro tipo de cable son una solución poco práctica.

Esperamos que este texto le sea útil para solucionar sus necesidades específicas de comunicación.

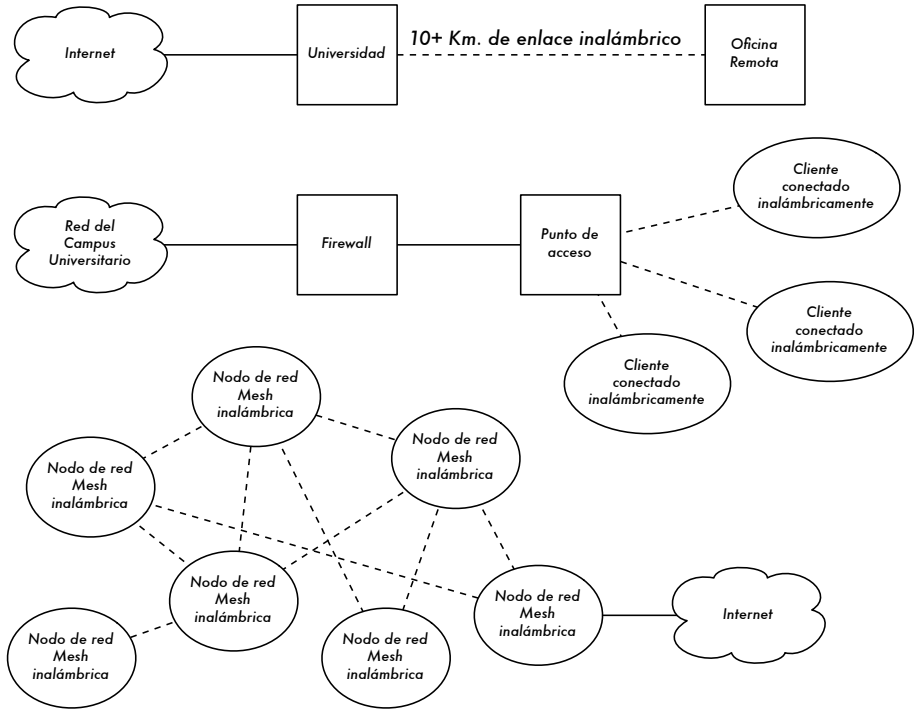


Figura 1.1: Algunos ejemplos de redes inalámbricas.

Incorporar una red inalámbrica a una red preexistente

Si usted es el administrador de una red, puede preguntarse cómo puede incorporar una red inalámbrica a su infraestructura de red actual. La tecnología inalámbrica puede ayudar de muchas formas, desde ser una simple extensión (como una red cableada Ethernet de varios kilómetros) hasta ser un concentrador (*hub*) inalámbrico que le permite conectar un gran

número de computadoras. Aquí le brindamos algunos ejemplos de cómo puede beneficiarse su red de la tecnología inalámbrica.

Protocolos de redes inalámbricas

La tecnología principal utilizada actualmente para la construcción de redes inalámbricas de bajo costo es la familia de protocolos 802.11, también conocida en muchos círculos como Wi-Fi. La familia de protocolos de radio 802.11 (802.11a, 802.11b, and 802.11g) han adquirido una gran popularidad en Estados Unidos y Europa. Mediante la implementación de un set común de protocolos, los fabricantes de todo el mundo han producido equipamiento altamente interoperable. Esta decisión ha resultado ser de gran ayuda para la industria y los consumidores. Los compradores pueden utilizar equipamiento que implementa el estándar 802.11 sin miedo a "quedar atrapado con el vendedor". Como resultado, pueden comprar equipamiento económico en un volumen que ha beneficiado a los fabricantes. Si por el contrario estos últimos hubieran elegido implementar sus propios protocolos, es poco probable que las redes inalámbricas fueran económicamente accesibles y ubicuas como lo son hoy en día.

Si bien nuevos protocolos como el 802.16 (también conocido como WiMax) van a ser capaces de solucionar algunas limitaciones observadas en el protocolo 802.11, les queda un largo camino para alcanzar la popularidad y el precio de ese equipamiento. Como los productos que soportan WiMax apenas están entrando al mercado en el momento que se escribe este libro, nos vamos a enfocar fundamentalmente en la familia 802.11.

Existen muchos protocolos en la familia 802.11 y no todos están relacionados específicamente con el protocolo de radio. Los tres estándares implementados actualmente en la mayoría de los equipos disponibles son:

- **802.11b**. Ratificado por IEEE el 16 de setiembre de 1999, el protocolo de redes inalámbricas 802.11b es probablemente el más asequible hoy en día. Millones de dispositivos que lo utilizan han sido vendidos desde 1999. Utiliza una modulación llamada Espectro Expandido por Secuencia Directa –***Direct Sequence Spread Spectrum*** (***DSSS***)– en una porción de la banda ISM desde 2400 a 2484 MHz. Tiene una tasa de transmisión máxima de 11Mbps, con una velocidad real de datos utilizable mayor a 5Mbps.
- **802.11g**. Como no estuvo finalizada sino hasta junio de 2003, el protocolo 802.11g llegó relativamente tarde al mercado inalámbrico. A pesar de esto, el protocolo 802.11g es hoy por hoy el estándar de facto en la redes inalámbricas utilizado como una característica estándar en virtualmente todas las laptops y muchos de los dispositivos handheld. Utiliza el mismo rango ISM que 802.11b, pero con el esquema de modulación denominado

Orthogonal Frequency Division Multiplexing (***OFDM***) –Multiplexaje por División de Frecuencias Ortogonales. Tiene una tasa de transmisión máxima de 54Mbps (con un rendimiento real de hasta 25Mbps), y mantiene compatibilidad con el altamente popular 802.11b gracias al soporte de las velocidades inferiores.

- **802.11a**. También ratificado por la IEEE el 16 de septiembre de 1999 el protocolo 802.11a utiliza OFDM. Tiene una tasa de transmisión máxima de 54Mbps (con un rendimiento real de hasta 27Mbps). El 802.11a opera en la banda ISM entre 5725 y 5850MHz, y en una porción de la banda UNII entre 5.15 y 5.35GHz. Esto lo hace incompatible con el 802.11b o el 802.11g, y su alta frecuencia implica un rango más bajo comparado con el 802.11b/g al mismo nivel de potencia. Si bien esta porción del espectro es relativamente inutilizada comparada con la de 2.4GHz, desafortunadamente su uso es legal sólo en unos pocos lugares del mundo. Realice una consulta a sus autoridades locales antes de utilizar equipamiento 802.11a, particularmente en aplicaciones externas. Esto mejorará en el futuro, pues hay una disposición de la unión Internacional de comunicaciones (UIT) instando a todas las administraciones a abrir el uso de esta banda. El equipo es bastante barato, pero no tanto como el 802.11b/g.

Además de los estándares mencionados anteriormente, hay fabricantes que ofrecen extensiones que permiten velocidades de hasta 108Mbps, mejor encriptación, y mayor rango. Desafortunadamente esas extensiones no funcionan entre productos de diferentes fabricantes, y adquirirlos lo va a atar a un vendedor específico. Nuevos productos y estándares (tales como 802.11n, 802.16, MIMO, y WiMAX) prometen incrementos significantes en velocidad y alcance, pero recién se están comenzando a comercializar y la disponibilidad e interoperabilidad entre marcas no está clara.

Dada la ubicuidad del equipo, un mejor rango, y la naturaleza libre de licencias de la banda ISM 2.4GHz, este libro se va a concentrar en el armado de redes utilizando los protocolos 802.11b y 802.11g.

Preguntas y Respuestas

Si usted es nuevo en el armado de redes inalámbricas seguramente tenga varias preguntas acerca de lo que la tecnología puede hacer, así como cuánto cuesta. Aquí listamos algunas preguntas frecuentes con la referencia a las páginas que contienen las respuestas y sugerencias.

Energía

- ¿Cómo puedo suministrar energía a mi equipo de radio si no hay electricidad disponible? **Capítulo 7**.

- ¿Debo colocar un cable eléctrico hasta la punta de la torre? **Capítulo 7**.
- ¿Cómo puedo utilizar paneles solares para dar energía a mi nodo inalámbrico manteniéndolo activo durante la noche? **Capítulo 7**.
- ¿Por cuánto tiempo va a funcionar mi punto de acceso con una batería? **Capítulo 7**.

Administración

- ¿Cómo puedo monitorear y gestionar puntos de acceso remotos desde mi oficina? **Capítulo 6**.
- ¿Qué debo hacer cuando la red falla? **Capítulos 6 y 8**.
- ¿Cuáles son los problemas más comunes encontrados en las redes inalámbricas y cómo puedo solucionarlos? **Capítulo 8**.

Distancia

- ¿Cuál es el rango de mi punto de acceso? **Capítulo 3**.
- ¿Existe alguna fórmula que me permita saber cuán lejos puedo llegar con un punto acceso dado? **Capítulo 3**.
- ¿Cómo puedo saber si un lugar alejado puede ser conectado a Internet utilizando un enlace inalámbrico? **Capítulo 3**.
- El fabricante dice que mi punto de acceso tiene un rango de alcance de 300 metros. ¿Eso es cierto? **Capítulo 3**.
- ¿Cómo puedo proveer de conectividad inalámbrica a muchos clientes remotos esparcidos alrededor de la ciudad? **Capítulo 3**.
- ¿Es verdad que puedo llegar a mucha más distancia utilizando una lata o una lámina de aluminio como antena? **Capítulo 4**.
- ¿Puedo utilizar una red inalámbrica para conectarme a un sitio remoto y compartir una conexión central única a Internet? **Capítulo 3**.
- Parece que mis enlaces inalámbricos son demasiado largos. ¿Puedo colocar un repetidor en el medio para mejorarlos? **Capítulo 3**.
- ¿Debo utilizar un amplificador? Capítulos **3 y 4**.

Instalación

- ¿Cómo puedo instalar mi AP para uso interior junto a la antena en mi techo? **Capítulo7**.

- ¿Realmente es útil agregar un "protector de rayos" y una puesta a tierra al mástil de mi antena, o no es tan necesario? **Capítulos 5 y 7**.
- ¿Puedo construir el mástil por mi mismo? ¿Cómo puedo hacerlo? **Capítulo 7**.
- ¿Por qué mi antena funciona mucho mejor cuando la coloco en otra orientación? **Capítulo 4**.
- ¿Qué canal debo utilizar? **Capítulo 2**.
- ¿Las ondas de radio atraviesan edificios y árboles? ¿Qué pasa con las personas? **Capítulo 2**.
- ¿Las ondas de radio atraviesan una colina que esté en el camino? **Capítulo 2**.
- ¿Cómo construyo una red mesh? **Capítulo 3**.
- ¿Qué tipo de antena es la mejor para mi red? **Capítulo 4**.
- ¿Puedo construir un punto de acceso utilizando un PC reciclado? **Capítulo 5**.
- ¿Cómo puedo instalar Linux en mi AP? ¿Por qué debo hacerlo? **Capítulo 5**.

Dinero

- ¿Cómo puedo saber si un enlace inalámbrico es adquirible con una cantidad limitada de dinero? **Capítulo 5**.
- ¿Cuál es la mejor AP por el menor precio? **Capítulo 5**.
- ¿Cómo puedo localizar y cobrar a los clientes por el uso de mi red inalámbrica? Páginas **Capítulo 6**.

Socios y Clientes

- ¿Si soy un proveedor de conexión, aún necesito el servicio de un ISP? ¿Por qué? **Capítulo 3**.
- ¿Con cuántos clientes puedo cubrir mis costos? **Capítulo 10**.
- ¿Cuántos clientes va a soportar mi red inalámbrica? **Capítulo 3**.
- ¿Qué debo hacer para que mi red inalámbrica funcione más rápido? **Capítulo 3**.
- ¿Mi conexión a Internet es tan rápida como puede serlo? **Capítulo 3**.

Seguridad

- ¿Cómo puedo proteger mi red inalámbrica del acceso no autorizado? **Capítulo 6**.
- ¿Es cierto que una red inalámbrica siempre es insegura y está abierta al ataque de piratas informáticos (hackers)? **Capítulo 6**.
- ¿Es cierto que el uso de software libre hace que mi red sea menos segura? **Capítulo 6**.
- ¿Cómo puedo ver qué está sucediendo en mi red? **Capítulo 5**.

2
Una Introducción Práctica a la Física de Radio

Las comunicaciones inalámbricas hacen uso de las ondas electromagnéticas para enviar señales a través de largas distancias. Desde la perspectiva del usuario, las conexiones inalámbricas no son particularmente diferentes de cualquier otra conexión: el navegador web, el correo electrónico y otras aplicaciones funcionan como se esperaba. Pero las ondas de radio tienen algunas propiedades inesperadas en comparación con una red cableada Ethernet. Por ejemplo, es muy sencillo ver el camino que esta última toma: localice el conector de su computadora, siga el cable hacia el otro extremo, ¡y lo habrá encontrado! También se puede confiar en que desplegar muchos cables Ethernet unos al lado de otro no va a causar problemas, ya que los cables confinan efectivamente las señales dentro de sí.

Pero ¿Cómo saber por dónde están circulando las ondas emanadas de su tarjeta inalámbrica? ¿Qué sucede cuando esas ondas rebotan en los objetos del lugar o, en el caso de un enlace externo, en los edificios? ¿Cómo pueden utilizarse varias tarjetas inalámbricas en la misma área sin interferir unas con otras?

Para construir enlaces inalámbricos de alta velocidad, es importante comprender cómo se comportan las ondas de radio en el mundo real.

¿Qué es una onda de radio?

En general estamos familiarizados con las vibraciones u oscilaciones de varias formas: Un péndulo, un árbol meciéndose con el viento, las cuerdas de una guitarra –son todos ejemplos de oscilaciones.

Lo que tienen en común es que algo, como un medio o un objeto, está vibrando de forma periódica, con cierto número de ciclos por unidad de tiempo. Este tipo de onda a veces es denominada onda mecánica, puesto que son definidas por el movimiento de un objeto o de su medio de propagación.

Cuando esas oscilaciones viajan (esto es, cuando las vibraciones no están limitadas a un lugar) hablamos de ondas propagándose en el espacio. Por ejemplo, un cantante crea oscilaciones periódicas de sus cuerdas vocales al cantar. Estas oscilaciones comprimen y descomprimen el aire periódicamente, y ese cambio periódico de la presión del aire sale de la boca del cantante y viaja a la velocidad del sonido. Una piedra arrojada a un lago causa una alteración que viaja a través del mismo como una ***onda***.

Una onda tiene cierta ***velocidad***, ***frecuencia*** y ***longitud de onda***. Las mismas están conectadas por una simple relación:

```
Velocidad = Frecuencia * Longitud de Onda
```

La longitud de onda (algunas veces denotada como **lambda**, **λ**) es la distancia medida desde un punto en una onda hasta la parte equivalente de la siguiente, por ejemplo desde la cima de un pico hasta el siguiente. La frecuencia es el número de ondas enteras que pasan por un punto fijo en un segundo. La velocidad se mide en metros/segundo, la frecuencia en ciclos por segundo (o Hertz, abreviado ***Hz***), y la longitud de onda, en metros.

Por ejemplo, si una onda en el agua viaja a un metro por segundo y oscila cinco veces por segundo, entonces cada onda tendrá veinte centímetros de largo:

```
1 metro/segundo = 5 ciclos/segundos * λ
λ = 1 / 5 metros
λ = 0,2 metros = 20 cm
```

Las ondas también tienen una propiedad denominada ***amplitud***. Esta es la distancia desde el centro de la onda hasta el extremo de uno de sus picos, y puede ser asimilada a la “altura” de una onda de agua. La relación entre frecuencia, longitud de onda y amplitud se muestra en la Figura 2.1.

Las ondas en el agua son fáciles de visualizar. Simplemente tire una piedra en un lago y verá las ondas y su movimiento a través del agua por un tiempo. En el caso de las ondas electromagnéticas, la parte que puede ser más difícil de comprender es: ¿Qué es lo que está oscilando?

Para entenderlo, necesitamos comprender las fuerzas electromagnéticas.

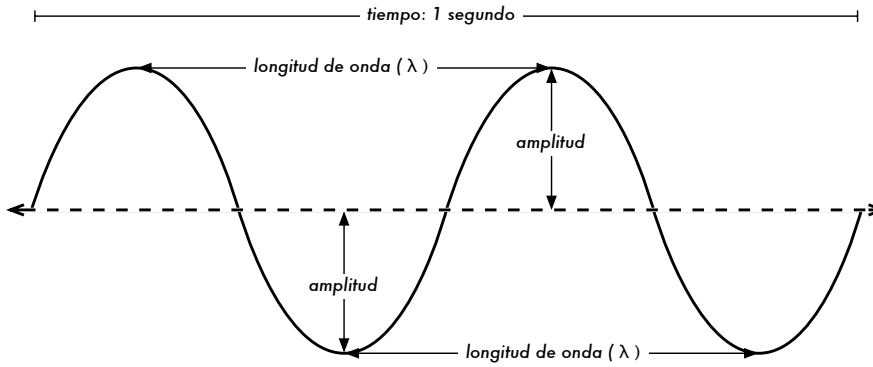


Figura 2.1: Longitud de onda, amplitud, y frecuencia. En este caso la frecuencia es 2 ciclos por segundo, o 2 Hz.

Fuerzas electromagnéticas

Las fuerzas electromagnéticas son fuerzas entre cargas y corrientes eléctricas. Nos percatamos de ellas cuando tocamos la manija de una puerta después de haber caminado en una alfombra sintética, o cuando rozamos una cerca eléctrica. Un ejemplo más fuerte de las fuerzas electromagnéticas son los relámpagos que vemos durante las tormentas eléctricas. La ***fuerza eléctrica*** es la fuerza entre cargas eléctricas. La ***fuerza magnética*** es la fuerza entre corrientes eléctricas.

Los electrones son partículas que tienen carga eléctrica negativa. También hay otras partículas, pero los electrones son responsables de la mayor parte de las cosas que necesitamos conocer para saber como funciona un radio.

Veamos qué sucede en un trozo de alambre recto en el cual empujamos los electrones de un extremo a otro periódicamente. En cierto momento, el extremo superior del alambre está cargado negativamente –todos los electrones están acumulados allí. Esto genera un campo eléctrico que va de positivo a negativo a lo largo del alambre. Al momento siguiente, los electrones se han acumulado al otro lado y el campo eléctrico apunta en el otro sentido. Si esto sucede una y otra vez, los vectores de campo eléctrico, por así decirlo, (flechas de positivo a negativo) abandonan el alambre y son radiados en el espacio que lo rodea.

Lo que hemos descrito se conoce como dipolo (debido a los dos polos, positivo y negativo), o más comúnmente ***antena dipolo***. Esta es la forma más simple de la antena omnidireccional. El movimiento del campo electromagnético es denominado comúnmente ***onda electromagnética***.

Volvamos a la relación:

```
Velocidad = Frecuencia * Longitud de Onda
```

En el caso de las ondas electromagnéticas, c es la velocidad de la luz.

```
c = 300.000 km/s = 300.000.000 m/s = 3*10^8 m/s
c = f * λ
```

Las ondas electromagnéticas difieren de las mecánicas en que no necesitan de un medio para propagarse. Las mismas se propagan incluso en el vacío del espacio.

Potencias de diez

En física, matemáticas e ingeniería, a menudo expresamos los números como potencias de diez. Encontramos esos términos por ejemplo en giga-hertz (GHz), centi-metros (cm), micro-segundos (μs), y otros.

Potencias de diez			
Nano-	10^{-9}	1/1000000000	n
Micro-	10^{-6}	1/1000000	μ
Milli-	10^{-3}	1/1000	m
Centi-	10^{-2}	1/100	c
Kilo-	10^{3}	1 000	k
Mega-	10^{6}	1 000 000	M
Giga-	10^{9}	1 000 000 000	G

Conociendo la velocidad de la luz, podemos calcular la longitud de onda para una frecuencia dada. Tomemos el ejemplo de la frecuencia para redes inalámbricas del protocolo 802.11b, la cual es:

```
f = 2,4 GHz
  = 2.400.000.000 ciclos / segundo

Longitud de onda landa (λ) = c / f
                           = 3*10^8 / 2,4*10^9
                           = 1,25*10^-1 m
                           = 12,5 cm
```

La frecuencia y la longitud de onda determinan la mayor parte del comportamiento de una onda electromagnética, desde las antenas que construimos hasta los objetos que están en el camino de las redes que intentamos hacer funcionar. Son responsables por muchas de las diferencias entre los estándares que podamos escoger. Por lo tanto, comprender las ideas básicas de frecuencia y longitud de onda ayuda mucho en el trabajo práctico con redes inalámbricas.

Polarización

Otra cualidad importante de las ondas electromagnéticas es la ***polarización***. La polarización describe la dirección del vector del campo eléctrico.

En una antena bipolar alineada verticalmente (el trozo de alambre recto), los electrones sólo se mueven de arriba a abajo, no hacia los lados (porque no hay lugar hacia donde moverse) y por consiguiente los campos eléctricos sólo apuntan hacia arriba o hacia abajo verticalmente. El campo que abandona el alambre y viaja como una onda tiene una polarización estrictamente lineal (y en este caso vertical). Si acostamos la antena en el suelo (horizontal) tendremos una polarización lineal horizontal.

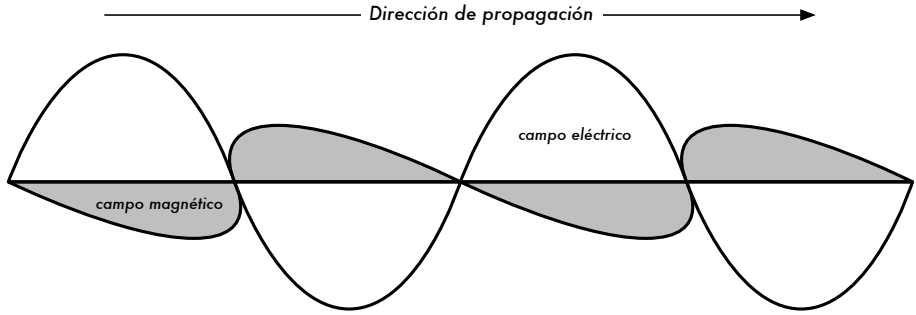


Figura 2.2: El campo eléctrico y el campo magnético complementario de una onda electromagnética. La polarización describe la orientación del campo eléctrico.

La polarización lineal es solo un caso especial, y nunca es perfecta: en general siempre tenemos algunos componentes del campo también en otras direcciones. El caso más general es la polarización elíptica, cuyos extremos son la polarización lineal (una sola dirección) y la polarización circular (ambas direcciones con igual intensidad).

Como se puede imaginar, la polarización es importante cuando alineamos las antenas. Si ignoramos la polarización, podemos tener muy poca señal aún teniendo las mejores antenas. A esto se le denomina desadaptación de polarización.

El espectro electromagnético

Las ondas electromagnéticas abarcan un amplio rango de frecuencias (y correspondientemente, de longitudes de onda). Este rango de frecuencias y longitudes de onda es denominado espectro electromagnético. La parte del espectro más familiar a los seres humanos es probablemente la luz, la porción visible del espectro electromagnético. La luz se ubica aproximadamente entre las frecuencias de $7{,}5*10^{14}$ Hz and $3{,}8*10^{14}$ Hz, correspondientes a longitudes de onda desde cerca de 400 nm (violeta/azul) a 800 nm (rojo).

Normalmente también estamos expuestos a otras regiones del espectro electromagnético, incluyendo los campos de la red de distribución eléctrica ***CA*** (***Corriente Alterna***), a 50/60 Hz, Rayos-X / Radiación Roentgen, Ultravioleta (en las frecuencias más altas de la luz visible), Infrarrojo (en las frecuencias más bajas de la luz visible) y muchas otras. ***Radio*** es el término utilizado para la porción del espectro electromagnético en la cual las ondas pueden ser transmitidas aplicando corriente alterna a una antena. Esto abarca el rango de 3 Hz a 300 GHz, pero normalmente el término se reserva para las frecuencias inferiores a 1 GHz.

Cuando hablamos de radio, la mayoría de la gente piensa en la radio FM, que usa una frecuencia de alrededor de 100 MHz. Entre la radio y el infrarrojo encontramos la región de las microondas –con frecuencias de 1 GHz a 300 GHz, y longitudes de onda de 30 cm a 1 mm.

El uso más popular de las microondas puede ser el horno de microondas, que de hecho trabaja exactamente en la misma región que los estándares inalámbricos de los que estamos tratando. Estas regiones caen dentro de las bandas que se están manteniendo abiertas para el uso general, sin requerir licencia. Esta región es llamada ***banda ISM*** (*ISM Band*), que significa Industrial, Científica y Médica, por su sigla en inglés. La mayoría de las otras regiones del espectro electromagnético están altamente controladas por la legislación mediante licencias, siendo los valores de las licencias un factor económico muy significativo. Esto atañe específicamente a aquellas partes del espectro que son útiles para la difusión masiva (como lo son la televisión y la radio), así como también para comunicaciones de voz y datos. En la mayoría de los países, las bandas ISM han sido reservadas para el uso libre.

Las frecuencias más interesantes para nosotros son 2400 – 2484 MHz, que son utilizadas por los estándares de radio 802.11b y 802.11g (correspondientes a longitudes de onda de alrededor de 12,5 cm). Otro equipamiento disponible comúnmente utiliza el estándar 802.11a, que opera a 5150 – 5850MHz (correspondiente a longitudes de onda de alrededor de 5 a 6 cm).

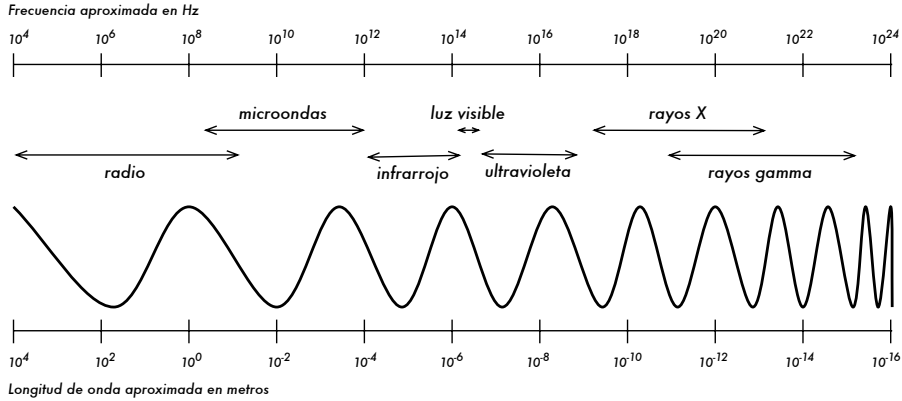


Figura 2.3: El espectro electromagnético.

Ancho de Banda

Un término que vamos a encontrar a menudo en la física de radio es ***ancho de banda***. El ancho de banda es simplemente una medida de rango de frecuencia. Si un rango de 2400 MHz a 2480 MHz es usado por un dispositivo, entonces el ancho de banda sería 0,08 GHz (o más comúnmente 80MHz).

Se puede ver fácilmente que el ancho de banda que definimos aquí está muy relacionado con la cantidad de datos que puedes trasmitir dentro de él – a más lugar en el espacio de frecuencia, más datos caben en un momento dado. El término ancho de banda es a menudo utilizado por algo que deberíamos denominar tasa de transmisión de datos, como en "mi conexión a Internet tiene 1 Mbps de ancho de banda", que significa que ésta puede trasmitir datos a 1 megabit por segundo.

Frecuencias y canales

Miremos un poco más de cerca como se utiliza la banda 2,4 GHz en el estándar 802.11b. El espectro está dividido en partes iguales distribuidas sobre la banda en ***canales*** individuales. Note que los canales son de un ancho de 22MHz, pero están separados sólo por 5MHz. Esto significa que los canales adyacentes se superponen, y pueden interferir unos con otros. Esto se representa visualmente en la Figura 2.4.

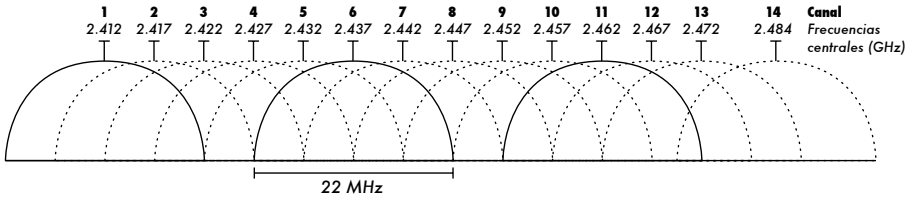


Figura 2.4: Canales y frecuencias centrales para 802.11b. Note que los canales 1, 6, y 11 no se superponen.

Para una lista completa de canales y sus frecuencias centrales para 802.11b/g y 802.11a, vea el Apéndice A.

Comportamiento de las ondas de radio

Hay algunas reglas simples que pueden ser de mucha ayuda cuando realizamos los primeros planes para una red inalámbrica:

- Cuanto más larga la longitud de onda, más lejos llega
- Cuanto más larga la longitud de onda, mejor viaja a través y alrededor de obstáculos
- Cuanto más corta la longitud de onda, puede transportar más datos

Todas estas reglas, simplificadas al máximo, son más fáciles de comprender con un ejemplo.

Las ondas más largas viajan más lejos

Suponiendo niveles iguales de potencia, las ondas con longitudes de onda más larga tienden a viajar más lejos que las que tienen longitudes de onda más cortas. Este efecto es visto a menudo en la radio FM, cuando comparamos el rango de un transmisor de radio FM a 88MHz con el rango a 108MHz. Los transmisores de frecuencia más baja tienden a alcanzar distancias mucho más grandes a la misma potencia.

Las ondas más largas rodean los obstáculos

Una onda en el agua que tiene 5 metros de largo no va a ser detenida por un trozo de madera de 5 mm que esté sobresaliendo de la superficie. Sin embargo, si la pieza de madera fuera de 50 metros (por ej. un barco), se interpondría en el camino de la onda. La distancia que una onda puede viajar depende de la relación entre la longitud de onda de la misma y el tamaño de los obstáculos en su camino de propagación.

Es difícil visualizar las ondas "atravesando" objetos sólidos, pero ese es el caso con las ondas electromagnéticas. Cuanto más larga la longitud de onda (y por lo tanto una frecuencia más baja) las ondas tienden a penetrar objetos mejor que las que tienen longitudes de onda más corta (y por consiguiente una frecuencia más alta). Por ejemplo, la radio FM (88-108MHz) puede atravesar edificios y otros obstáculos fácilmente, mientras que las ondas más cortas (cómo los teléfonos GSM operando a 900MHz o 1800MHz) tienen más dificultades en penetrar edificios. Este efecto es debido en parte a los diferentes niveles de potencia utilizados por la radio FM y el GSM, pero también debido a las longitudes de onda más cortas de las señales GSM.

Las ondas más cortas pueden transmitir más datos

Cuanto más rápida sea la oscilación o ciclo de la onda, mayor cantidad de información puede transportar –cada oscilación o ciclo- puede ser utilizado por ejemplo para transmitir un bit digital, un '0' o un '1', un 'sí' o un 'no'.

Existe otro principio que puede ser aplicado a todos los tipos de ondas y que es extremadamente útil para comprender la propagación de ondas de radio. Este principio es conocido como el ***Principio de Huygens***, nombrado en honor de Christiaan Huygens, matemático, físico y astrónomo holandés, que vivió entre 1629 y 1695.

Imagínese que toma una vara y la introduce verticalmente en un lago en calma, haciendo que el agua ondee y baile. Las ondas se alejarán de la vara –el lugar donde la introdujo en el agua– formando círculos. Ahora, donde las partículas de agua están oscilando y bailando, harán que las partículas vecinas hagan lo mismo: desde cada punto de perturbación, se origina una nueva onda circular. Esto es, de una forma simple, el principio de Huygens. Según *wikipedia.org*:

> *"El principio de Huygens es un método de análisis aplicado a los problemas de la propagación de ondas en el límite de campo lejano. Establece que cada punto de un frente de onda que avanza es, de hecho, el centro de una nueva perturbación y la fuente de un nuevo tren de ondas; y que esa onda avanzando como un todo puede ser concebida como la suma de todas las ondas secundarias surgiendo de puntos en el medio ya atravesado. Esta visión de la propagación de ondas ayuda a comprender mejor la variedad de fenómenos de las ondas, tales como la difracción."*

Este principio se aplica tanto para las ondas de radio como para las ondas en el agua, para el sonido y para la luz –sólo que la longitud de onda de la luz es muy corta como para que los seres humanos podamos ver sus efectos directamente.

Este principio va a ayudarnos a comprender tanto la difracción como las zonas Fresnel, la necesidad de línea visual, y el hecho de que algunas veces las ondas voltean las esquinas, más allá de la línea visual.

Veamos entonces qué sucede con las ondas electromagnéticas cuando viajan.

Absorción

Cuando las ondas electromagnéticas atraviesan algún material, generalmente se debilitan o atenúan. La cantidad de potencia perdida va a depender de su frecuencia y, por supuesto, del material. El vidrio de una ventana obviamente es transparente para la luz, mientras que el vidrio utilizado en los lentes de sol filtra una porción de la intensidad de la luz y bloquea la radiación ultravioleta.

A menudo se utiliza el coeficiente de absorción para describir el impacto de un material en la radiación. Para las microondas, los dos materiales más absorbentes son:

- **Metal**. Los electrones pueden moverse libremente en los metales, y son capaces de oscilar y por lo tanto absorber la energía de una onda que los atraviesa.
- **Agua**. Las microondas provocan que las moléculas de agua se agiten, capturando algo de la energía de las ondas[1].

En la práctica de redes inalámbricas, vamos a considerar el metal y el agua como absorbentes perfectos: no vamos a poder atravesarlos (aunque capas finas de agua podrían permitir que una parte de la potencia pase). Son a las microondas lo que una pared de ladrillo es a la luz. Cuando hablamos del agua, tenemos que recordar que se encuentra en diferentes formas: lluvia, niebla, vapor y nubes bajas, y todas van a estar en el camino de los radioenlaces. Tienen una gran influencia y en muchas circunstancias un cambio en el clima puede hacer caer un radioenlace.

Existen otros materiales que tienen un efecto más complejo en la absorción de radiación.

---

1. Un mito común es que el agua “resuena” a 2,4GHz, que es la frecuencia utilizada por los hornos de microondas. En realidad, el agua aparentemente no tiene ninguna frecuencia “resonante”. El agua gira y se agita en presencia de radiaciones y se calienta en la presencia de ondas de radio de alta potencia a cualquier frecuencia. La frecuencia ISM de 2,4GHz no requiere licencia y por lo tanto es una buena elección para utilizarla en hornos de microondas.

Para los **árboles** y la **madera**, la cantidad de absorción depende de cuánta cantidad de agua contienen. La madera vieja y seca es más o menos transparente, la madera fresca y húmeda va a absorber muchísimo.

Los plásticos y materiales similares generalmente no absorben mucha energía de radio pero esto varía dependiendo de la frecuencia y el tipo de material. Antes de construir un componente de plástico (por ejemplo, una protección climática para los dispositivos de radio y sus antenas), es siempre una buena idea verificar que el material no absorba la energía de radio alrededor de 2,4GHz Un método simple de medir la absorción del plástico a 2,4GHz es poner una muestra en un horno microondas por un par de minutos. Si el plástico se calienta, entonces absorbe la energía de radio y no debe ser utilizado.

Finalmente, hablemos de nosotros mismos: los humanos (como otros animales) estamos compuestos mayormente de agua. En lo que a redes inalámbricas se refiere, podemos ser descritos como grandes bolsas llenas de agua, con la misma fuerte absorción. Orientar un punto de acceso en una oficina de forma que su señal deba pasar a través de mucha gente es un error clave cuando instalamos redes en oficinas. Lo mismo sucede en clubes nocturnos, cafés, bibliotecas e instalaciones externas.

Reflexión

Al igual que la luz visible, las ondas de radio son reflejadas cuando entran en contacto con materiales que son apropiados para eso: para las ondas de radio, las principales fuentes de reflexión son el metal y las superficies de agua. Las reglas para la reflexión son bastante simples: el ángulo en el cual una onda incide en una superficie es el mismo ángulo en el cual es desviada. A la luz de las ondas de radio, una reja densa de metal actúa de igual forma que una superficie sólida, siempre que la distancia entre las barras sea pequeña en comparación con la longitud de onda. A 2,4GHz, una rejilla metálica con separación de un centímetro (1cm) entre sus elementos va a actuar igual que una placa de metal.

A pesar de que las reglas de reflexión son bastante simples, las cosas pueden complicarse mucho cuando imaginamos el interior de una oficina con varios objetos pequeños de metal de formas variadas y complicadas. Lo mismo sucede en las situaciones urbanas: mire alrededor en su ciudad e intente ubicar todos los objetos de metal. Esto explica el por qué el ***efecto multitrayectoria*** (***multipath***), (es decir el que las señales lleguen al receptor a través de diferentes caminos, y por consiguiente en tiempos diferentes), juega un rol tan importante en las redes inalámbricas. La superficie del agua, con olas y encrespaduras que cambian su orientación todo el tiempo, hace que sea prácticamente imposible calcular precisamente la reflexión.

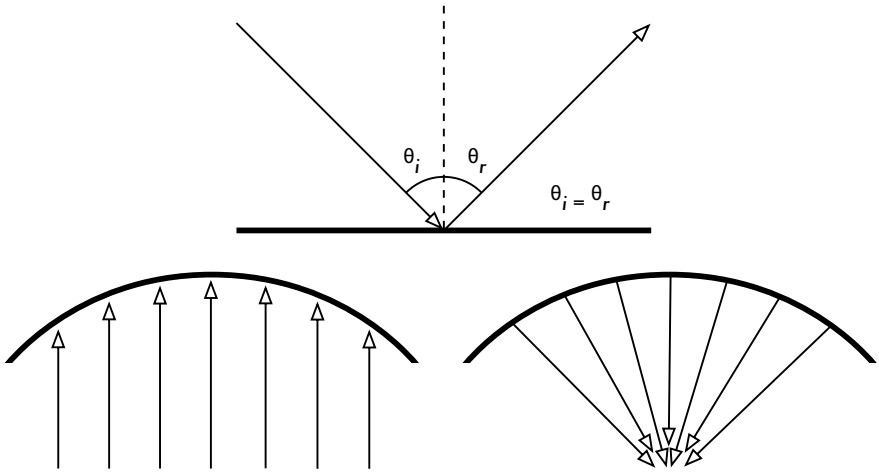


Figura 2.5: Reflexión de ondas de radio. El ángulo de incidencia es siempre igual al ángulo de reflexión. Una antena parabólica utiliza este efecto para concentrar las ondas de radio que caen sobre su superficie en una dirección común.

Debemos agregar que la polarización tiene un impacto: las ondas de di-ferente polarización en general van a ser reflejadas de forma diferente.

Utilizamos la reflexión en ventaja nuestra en la construcción de las antenas: por ej. poniendo grandes parábolas detrás de nuestro transmisor/receptor para recoger las ondas de radio y concentrarlas en un punto.

Difracción

Difracción es el comportamiento de las ondas cuando al incidir en un objeto dan la impresión de doblarse. Es el efecto de “ondas doblando las esquinas”.

Imagine una onda en el agua viajando en un frente de onda plano, tal como una ola llegándose a una playa oceánica. Ahora ponemos en su camino una barrera sólida, como una cerca de madera, para bloquearla. Luego practicamos una estrecha rendija en esa pared, como una pequeña puerta. Desde esta abertura va a comenzar una onda circular, y por supuesto va a alcanzar puntos que están en una línea directa detrás de esa abertura, pero también a ambos lados de ella. Si miramos este frente de onda –y pudiera ser también una onda electromagnética– como un haz de luz, sería difícil explicar cómo logra alcanzar puntos que están ocultos por una barrera. Cuando lo modelamos como un frente de onda, el fenómeno tiene sentido.

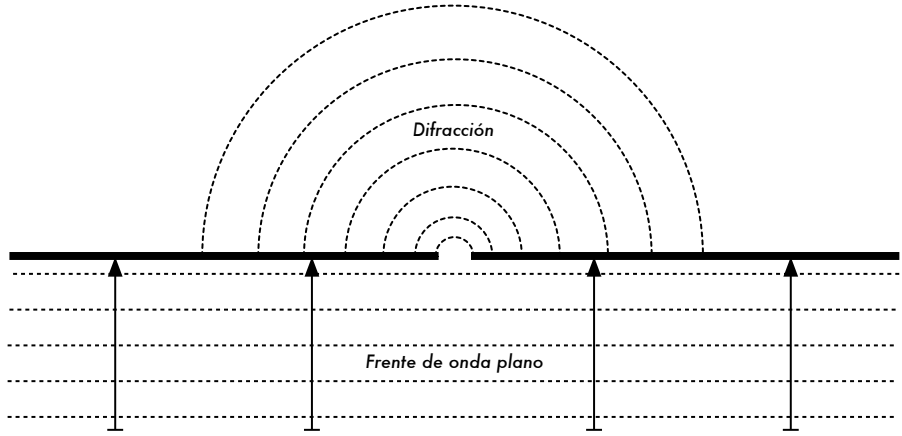


Figura 2.6: Difracción a través de una ranura pequeña.

El Principio de Huygens provee un modelo para comprender este comportamiento. Imagine que en un momento determinado, cada punto del frente de onda puede ser considerado como el punto de inicio de otra onda esférica (*wavelet*). Esta idea fue desarrollada más adelante por Fresnel, y si describe adecuadamente el fenómeno todavía es tema de debate. Pero para nuestros propósitos el modelo de Huygens describe el efecto bastante bien.

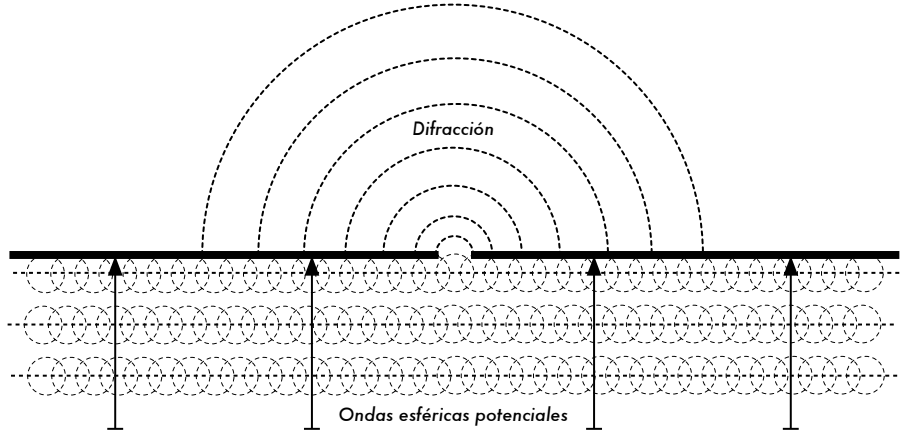


Figura 2.7: El Principio de Huygens.

Es por medio del efecto de difracción que las ondas van a “doblar” las esquinas, o van a atravesar una abertura en una barrera. La longitud de onda de la luz visible es muy pequeña como para que los humanos puedan observar este efecto directamente. Las microondas, con una longitud de onda de varios centímetros, muestran los efectos de la difracción cuando chocan contra paredes, picos de montañas y otros obstáculos. La

obstrucción provoca que la onda cambie su dirección y doble en las esquinas.

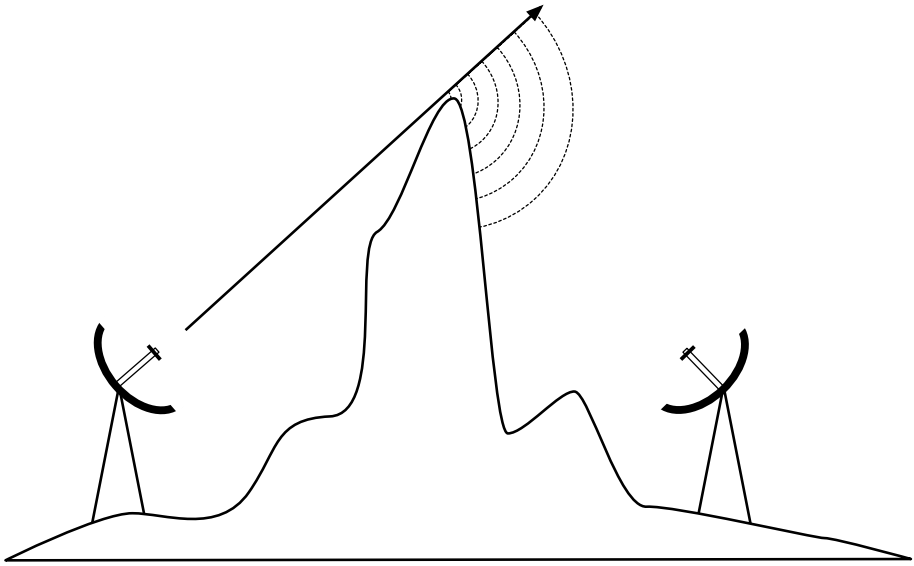


Figura 2.8: Difracción en la cima de una montaña.

Tenga en cuenta que en la difracción se genera una pérdida de potencia: la potencia de la onda difractada es significativamente menor que el frente de onda que la provoca. Pero en algunas aplicaciones muy específicas, se puede aprovechar el efecto de difracción para rodear obstáculos.

Interferencia

Cuando trabajamos con ondas, uno más uno no es necesariamente igual a dos. Incluso puede resultar cero.

Esto es sencillo de entender cuando dibujamos dos ondas senoidales y sumamos las amplitudes. Cuando un pico coincide con el otro pico, tenemos un resultado máximo (1 + 1 = 2). Esto es denominado i***nterferencia constructiva***. Cuando un pico coincide con un valle, tenemos una completa aniquilación ((1 + (-)1 = 0), se denomina ***interferencia destructiva***.

Puede probar esto creando dos olas circulares en el agua mediante dos varitas: verá que cuando dos olas se cruzan, hay áreas con picos de onda más grandes y otras que permanecen casi planas y en calma.

Para que trenes de ondas se sumen o cancelen perfectamente, tienen que tener exactamente la misma longitud de onda y una relación de fase fija, esto significa posiciones fijas desde el pico de una onda hasta las otras.

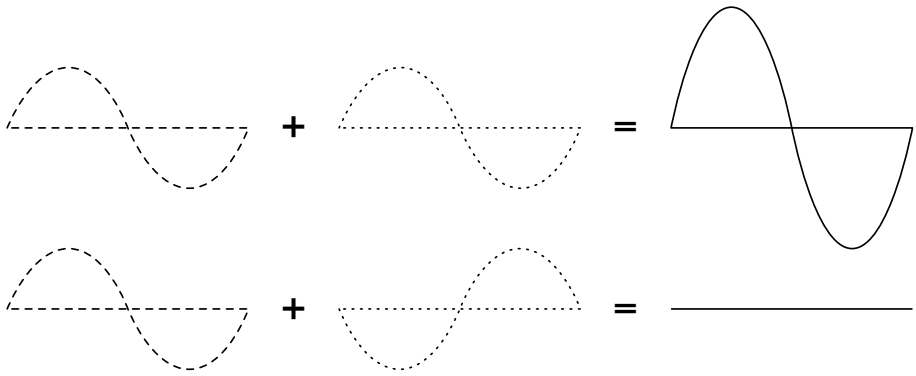


Figura 2.9: Interferencia constructiva y destructiva.

En la tecnología inalámbrica, la palabra Interferencia es usada típicamente en un sentido amplio, para disturbios desde otras fuentes RF (radio frecuencia), por ejemplo canales adyacentes. Entonces, cuando los constructores de redes inalámbricas hablan de interferencia, generalmente se refieren a todos los tipos de alteraciones generadas por otras redes y otras fuentes de microondas. La interferencia es una de las fuentes de dificultades principales en el despliegue de enlaces inalámbricos, especialmente en ambientes urbanos o en espacios cerrados (como en un local para conferencias) donde muchas redes pueden competir por el uso del espectro.

Siempre que las ondas de igual amplitud y fases opuestas se crucen en el camino, son eliminadas y no se pueden recibir señales. El caso más común es que las ondas se combinen y generen una nueva forma de onda que no puede ser utilizada efectivamente para la comunicación. Las técnicas de modulación y el uso de canales múltiples ayuda a manejar el problema de la interferencia, pero no lo elimina completamente.

Línea visual

El término ***línea visual***, a menudo abreviada como ***LOS*** (por su sigla en inglés, *Line of Sight*), es fácil de comprender cuando hablamos acerca de la luz visible: si podemos ver un punto B desde un punto A donde estamos, tenemos línea visual. Dibuje simplemente una línea desde A a B, y si no hay nada en el camino, tenemos línea visual.

Las cosas se ponen un poco más complicadas cuando estamos tratando con microondas. Recuerden que la mayoría de las características de propagación de las ondas electromagnéticas son proporcionales a la longitud de onda. Este es el caso del ensanchamiento de las ondas a medida que avanzan. La luz tiene una longitud de onda de aproximadamente 0,5 micrómetros, las

microondas usadas en las redes inalámbricas tienen una longitud de onda de unos pocos centímetros. Por consiguiente, los haces de microondas son más anchos –necesitan más espacio.

Note que los haces de luz visibles también se ensanchan, y si los dejamos viajar lo suficiente, podemos ver los resultados a pesar de su pequeña longitud de onda. Cuando apuntamos un láser bien enfocado a la luna, el haz se extenderá abarcando más de 100 metros de radio cuando alcance su superficie. Puede observar este efecto por usted mismo utilizando un apuntador láser económico y un par de binoculares en una noche clara. En lugar de apuntar a la luna, hágalo sobre una montaña distante o una estructura desocupada (como una torre de agua). El radio de su haz va a incrementarse con la distancia.

La línea visual que necesitamos para tener una conexión inalámbrica óptima desde A hasta B es más que simplemente una línea delgada –su forma es más bien la de un cigarro, un elipsoide. Su ancho puede ser descrito por medio del concepto de zonas de Fresnel.

La zona de Fresnel

La teoría exacta de las zonas de Fresnel es algo complicada. Sin embargo el concepto es fácilmente entendible: sabemos por el principio de Huygens que por cada punto de un frente de onda comienzan nuevas ondas circulares. Sabemos que los haces de microondas se ensanchan. También sabemos que las ondas de una frecuencia pueden interferir unas con otras. La teoría de zona de Fresnel simplemente examina a la línea desde A hasta B y luego al espacio alrededor de esa línea que contribuye a lo que está llegando al punto B. Algunas ondas viajan directamente desde A hasta B, mientras que otras lo hacen en trayectorias indirectas. Consecuentemente, su camino es más largo, introduciendo un desplazamiento de fase entre los rayos directos e indirectos. Siempre que el desplazamiento de fase es de una longitud de onda completa, se obtiene una interferencia constructiva: las señales se suman óptimamente. Tomando este enfoque, y haciendo los cálculos, nos encontramos con que hay zonas anulares alrededor de la línea directa de A a B que contribuyen a que la señal llegue al punto B.

Tenga en cuenta que existen muchas zonas de Fresnel, pero a nosotros nos interesa principalmente la zona 1. Si ésta fuera bloqueada por un obstáculo, por ej. un árbol o un edificio, la señal que llegue al destino lejano será atenuada. Entonces, cuando planeamos enlaces inalámbricos, debemos asegurarnos de que esta zona va a estar libre de obstáculos. En la práctica en redes inalámbricas nos conformamos con que al menos el 60% de la primera zona de Fresnel esté libre.

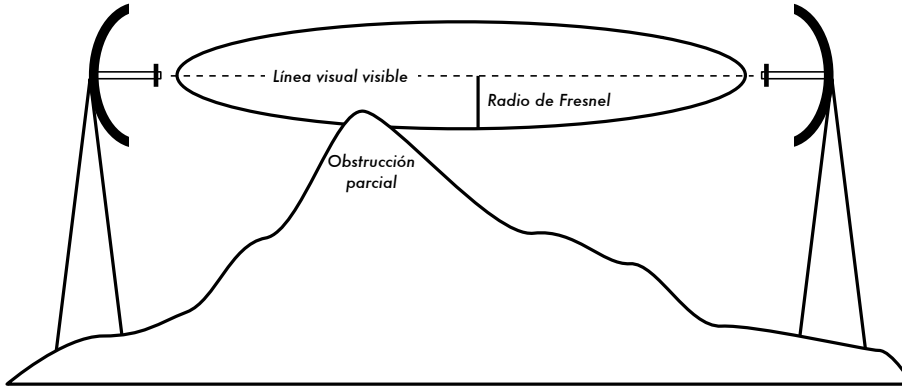


Figura 2.10: La zona de Fresnel es bloqueada parcialmente en este enlace, aunque la línea visual no está obstruida.

Aquí hay una formula para calcular la primera zona de Fresnel:

```
r = 17,31 * sqrt((d1*d2)/(f*d))
```

...donde **r** es el radio de la primera zona en metros, **d1** y **d2** son las distancias desde el obstáculo a los extremos del enlace en metros, **d** es la distancia total del enlace en metros, y **f** es la frecuencia en MHz. Note que esta fórmula calcula el radio de la zona. Para calcular la altura sobre el terreno, debe sustraerse este resultado de una línea trazada directamente entre la cima de las dos torres.

Por ejemplo, calculemos el tamaño de la primera zona de Fresnel en el medio de un enlace de 2km, transmitiendo a 2437MHz (802.11b canal 6):

```
r = 17,31 sqrt(1 * (1000 * 1000) / (2437 * 2000))
r = 17,31 sqrt(1000000 / 4874000)
r = 7,84 metros
```

Suponiendo que ambas torres tienen 10 metros de altura, la primera zona de Fresnel va a pasar justo a 2,16 metros sobre el nivel del suelo en el medio del enlace. Pero, ¿cuán alta puede ser una estructura en este punto para despejar el 60% de la primera zona?

```
r = 0,6 *17,31 sqrt( (1000 * 1000) / (2437 * 2000))
r = 4,70 metros
```

Restando el resultado de los 10 metros, podemos ver que una estructura de 5,30 metros de alto en el centro del enlace aún permite despejar el 60% de la primera zona de Fresnel. Esto es normalmente aceptable, pero en el caso de que hubiera una estructura más alta habría que levantar más nuestras antenas, o cambiar la dirección del enlace para evitar el obstáculo.

Energía

Cualquier onda electromagnética contiene energía, o potencia –lo podemos sentir cuando disfrutamos (o sufrimos) del calor del sol. La potencia **P** es de una importancia clave para lograr que los enlaces inalámbricos funcionen: se necesita cierto mínimo de potencia para que el receptor le dé sentido a la señal.

Vamos a volver con más detalles sobre la potencia de transmisión, pérdidas, ganancia y sensibilidad del radio en el capítulo tres. Ahora vamos a discutir brevemente cómo se define y calcula la potencia **P**.

El campo eléctrico se mide en V/m (diferencia de potencial por metro), la potencia contenida en él es proporcional al campo eléctrico al cuadrado

$$P \sim E^2$$

En la práctica, medimos la potencia por medio de algún tipo de receptor, por ej. una antena y un voltímetro, un medidor de potencia, un osciloscopio, o inclusive una tarjeta inalámbrica y una computadora portátil. La potencia es proporcional al cuadrado del voltaje de la señal.

Calcular en dBs

La técnica sin duda más importante para calcular la potencia es por ***decibeles*** (***dB***). No hay física nueva en esto –es solamente un método conveniente que hace que los cálculos sean muy simples.

El decibel es una unidad sin dimensión[2], esto es, define la relación entre dos medidas de potencia. Se define como:

```
dB = 10 * Log (P1 / P0)
```

…donde **P1** y **P0** pueden ser de los dos valores cualquiera que queremos comparar. Típicamente, en nuestro caso, se tratará de potencia.

¿Por qué es tan práctico el uso de decibeles? Muchos fenómenos de la naturaleza se comportan de una manera que nosotros llamamos exponencial. Por ejemplo, el oído humano escucha un sonido dos veces más fuerte que otro si el primero tiene diez veces su intensidad física.

---

2. Otro ejemplo de unidad sin dimensión es el porcentaje (%) el cual también puede utilizarse en todo tipo de cantidades o números. Mientras que otras medidas tales como pies y gramos son absolutas, las unidades sin dimensión representan una relación.

Otro ejemplo, muy relacionado con nuestro campo de interés, es el de la absorción. Imaginemos una pared en el camino de nuestro enlace inalámbrico, y cada metro de esa pared absorbe la mitad de la señal disponible. El resultado va a ser:

```
0 metros=   1 (señal completa)
1 metro     =     1/2
2 metros    =     1/4
3 metros    =     1/8
4 metros    =     1/16
n metros    =     1/2^n  = 2^-n
```

Este es el comportamiento exponencial.

Pero una vez que hemos aprendido cómo aplicar el logaritmo (log), las cosas son mucho más sencillas: en lugar de elevar un valor a la potencia n-ésima, vamos a multiplicarlo por **n**. En lugar de multiplicar valores, los vamos a sumar.

Aquí hay algunos valores utilizados comúnmente que es importante recordar:

```
 +3 dB  = doble potencia
 -3 dB  = potencia media
+10 dB = orden de magnitud (10 veces la potencia)
-10 dB  = un décimo de potencia
```

Además de los dBs adimensionales, hay cierto número de definiciones relacionadas que están basadas en una referencia P0 fija. Los más relevantes para nosotros son:

```
dBm   relativo a P0 = 1 mW
dBi   relativo a una antena isotrópica ideal
```

Una ***antena isotrópica*** es una antena hipotética que distribuye uniformemente la potencia en todas direcciones. La antena que más se aproxima a este concepto es el dipolo, pero una antena isotrópica perfecta no puede ser construida en la realidad. El modelo isotrópico es útil para describir la ganancia de potencia relativa de una antena real.

Otra forma común (aunque menos conveniente) de expresar la potencia es en milivatios (***miliwatts***). Aquí hay algunas equivalencias de niveles de potencia expresadas en miliwatts y dBm:

```
  1 mW      = 0 dBm
  2 mW      = 3 dBm
100 mW      = 20 dBm
  1 W       = 30 dBm
```

La física en el mundo real

No se preocupe si los conceptos de este capítulo parecen desafiantes. Entender cómo las ondas de radio se propagan e interactúan con el medio ambiente es un campo de estudio complejo en sí mismo. La mayoría de la gente encuentra difícil la comprensión de fenómenos que no puede ver con sus propios ojos. En este punto, esperamos que el lector pueda comprender que las ondas de radio no viajan por un camino recto predecible. Para construir redes de comunicación confiables, se debe ser capaz de calcular cuánta potencia se necesita para cruzar una distancia dada, y predecir cómo van a viajar las ondas a lo largo del camino.

Hay mucho más que aprender acerca de la física de radio de lo que nosotros podemos explicar aquí. Para encontrar más información acerca de esta área de conocimiento en constante desarrollo, consulte los recursos listados en el Apéndice A. Ahora que tiene una idea de cómo predecir la forma en que las ondas de radio van a interactuar en el mundo real, usted está preparado para comenzar a utilizarlas para las comunicaciones.

3
Diseño de Redes

Antes de adquirir equipamiento o decidirse por una plataforma de soporte físico, se debe tener una clara idea de la naturaleza de sus problemas de comunicación. En realidad, si usted está leyendo este libro es porque necesita conectar sus redes de computadoras para compartir recursos y en última instancia acceder a Internet. El diseño de red que elija para implementarlo debe concordar con los problemas de comunicaciones que está tratando de resolver. ¿Necesita conectar un lugar remoto a una conexión de Internet en el centro de su campus? ¿Es probable que su red crezca para incluir varios lugares alejados? ¿La mayoría de los componentes de su red van a estar instalados en locaciones fijas, o se va a expandir para incluir cientos de computadoras portátiles itinerantes y otros dispositivos?

Cuando resolvemos un problema complejo, a menudo es útil hacer un dibujo de sus recursos y problemas. En este capítulo, veremos cómo otras personas han construido redes inalámbricas para resolver sus problemas de comunicación, incluyendo diagramas de la estructura esencial de la red. Vamos a cubrir los conceptos que definen TCP/IP, el principal lenguaje de programación hablado actualmente en Internet. Mostraremos varios métodos sencillos para hacer que la información fluya eficientemente por su red y por la del resto del mundo.

Diseñando la red física

Puede parecer raro que hablemos de la red “física” cuando construimos redes inalámbricas. Después de todo ¿dónde está la parte física de la red? En estas redes, el medio físico que utilizamos para la comunicación es obviamente la energía electromagnética. Pero en el contexto de este capítulo, la red física se refiere al tema mundano de dónde poner las cosas. ¿Cómo va a organizar el equipamiento de forma que pueda alcanzar a sus

clientes inalámbricos? Sea que deba llegar hasta una oficina en un edificio o exten-derse a lo largo de muchas millas, las redes inalámbricas son organizadas en estas tres configuraciones lógicas:

- Enlaces punto a punto
- Enlaces punto a multipunto
- Nubes multipunto a multipunto

El diseño de la red física que elija va a depender de la naturaleza del problema que esté tratando de resolver. Si bien diferentes partes de su red pueden aprovechar las tres configuraciones, los enlaces individuales van a estar dentro de una de esas topologías. La aplicación de estas topologías se describe mejor mediante un ejemplo.

Punto a punto

Los enlaces ***punto a punto*** generalmente se usan para conectarse a Internet donde dicho acceso no está disponible de otra forma. Uno de los lados del enlace punto a punto estará conectado a Internet, mientras que el otro utiliza el enlace para acceder al mismo. Por ejemplo, una Universidad puede tener una conexión *Frame Relay* o una conexión VSAT dentro del campus, pero difícilmente podrá justificar otra conexión de la misma índole a un edificio muy importante fuera del campus. Si el edificio principal tiene una visión libre de obstáculos hacia el lugar remoto, una conexión punto a punto puede ser utilizada para unirlos. Ésta puede complementar o incluso remplazar enlaces discados existentes.

Con antenas apropiadas y existiendo línea visual, se pueden hacer enlaces punto a punto seguros de más de treinta kilómetros.

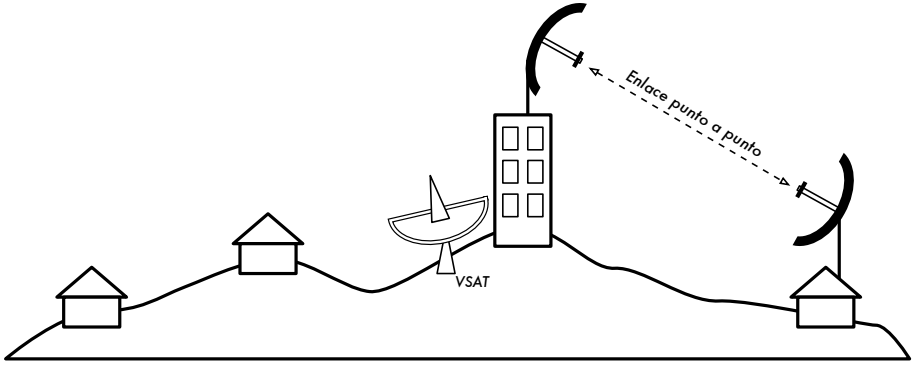


Figura 3.1: Un enlace punto a punto le permite a un lugar remoto compartir una conexión central a Internet.

Por supuesto, una vez hecha una conexión punto a punto, se pueden añadir otras para extender la red aún más. Si en nuestro ejemplo, un edificio alejado se encuentra en la cima de una gran colina, puede ser posible ver otras locaciones importantes que no pueden ser vistas directamente desde el campus central. Mediante la instalación de otro enlace punto a punto hacia el lugar remoto, se puede unir a la red otro nodo y hacer uso de la conexión central a Internet.

Los enlaces punto a punto no necesariamente tienen que estar relacionados con el acceso a Internet. Supongamos que debe desplazarse hasta una estación de monitoreo meteorológico alejada, –ubicada en lo alto de una colina–, para recolectar los datos que ella toma. Podría conectar el lugar con un enlace punto a punto, logrando la recolección y el monitoreo de datos en tiempo real, sin tener que ir hasta el lugar. Las redes inalámbricas pueden proveer suficiente ancho de banda como para transmitir grandes cantidades de datos (incluyendo audio y video) entre dos puntos, aún en ausencia de conexión a Internet.

Punto a multipunto

La siguiente red más comúnmente encontrada es la ***punto a multipunto*** donde varios nodos[1] están hablando con un punto de acceso central, esta es una aplicación punto a multipunto. El ejemplo típico de esta disposición es el uso de un punto de acceso inalámbrico que provee conexión a varias computadoras portátiles. Las computadoras portátiles no se comunican directamente unas con otras, pero deben estar en el rango del punto de acceso para poder utilizar la red.

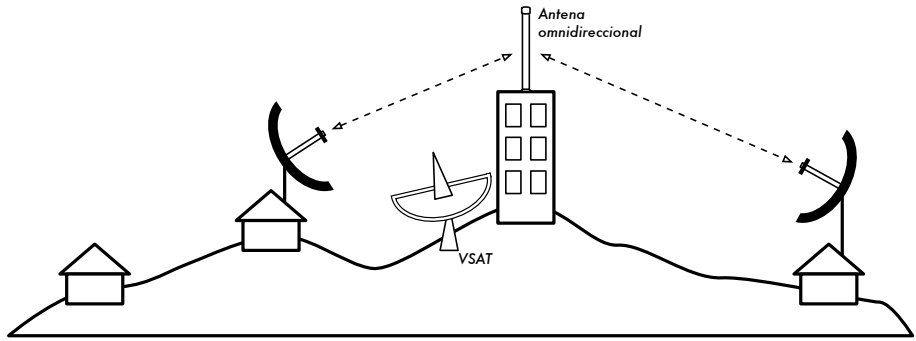


Figura 3.2: La conexión VSAT central es compartida por múltiples sitios remotos. Estos tres lugares también pueden comunicarse directamente a velocidades mucho más rápidas que las ofrecidas por VSAT.

1. Un ***nodo*** es todo dispositivo capaz de enviar y recibir datos en una red. Los puntos de acceso, enrutadores, computadoras y laptops son todos ejemplos de nodos.

La red punto a multipunto también puede ser aplicada a nuestro ejemplo anterior en la universidad. Supongamos que el edificio alejado en la cima de una colina está conectado con el campus central con un enlace punto a punto. En lugar de colocar varios enlaces punto a punto para conexión a Internet, se puede utilizar una antena que sea visible desde varios edificios alejados. Este es un ejemplo clásico de conexión de área extendida ***punto*** (sitio alejado en la colina) a ***multipunto*** (muchos edificios abajo en el valle).

Existen algunas limitaciones con el uso de punto a multipunto en distancias muy grandes, que van a ser tratadas más adelante en este capítulo. Estos enlaces son útiles y posibles en muchas circunstancias, pero no cometamos el clásico error de instalar una torre de radio de gran potencia en el medio de un pueblo esperando ser capaces de servir a miles de clientes, como podría hacerlo con una estación de radio FM. Como veremos, las redes de datos se comportan de forma muy diferente a las emisoras de radiodifusión.

Multipunto a multipunto

El tercer tipo de diseño de red es el ***multipunto a multipunto***, el cual también es denominado red ***ad hoc*** o en malla (***mesh***). En una red multipunto a multipunto, no hay una autoridad central. Cada nodo de la red transporta el tráfico de tantos otros como sea necesario, y todos los nodos se comunican directamente entre sí.

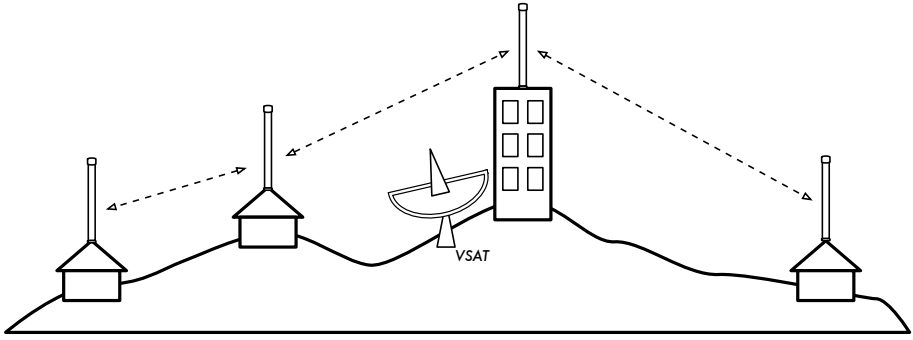


Figura 3.3: Una red en malla (mesh) multipunto a multipunto. Cada punto puede acceder a otro a gran velocidad, o utilizar la conexión central VSAT para acceder a Internet.

El beneficio de este diseño de red es que aún si ninguno de los nodos es alcanzable desde el punto de acceso central, igual pueden comunicarse entre sí. Las buenas implementaciones de redes *mesh* son auto-reparables, detectan automáticamente problemas de enrutamiento y los corrigen. Extender una red *mesh* es tan sencillo como agregar más nodos. Si uno de los nodos en la "nube" tiene acceso a Internet, esa conexión puede ser compartida por todos los clientes.

Dos grandes desventajas de esta topología son el aumento de la complejidad y la disminución del rendimiento. La seguridad de esta red también es un tema importante, ya que todos los participantes pueden potencialmente transportar el tráfico de los demás. La resolución de los problemas de las redes multipunto a multipunto tiende a ser complicada, debido al gran número de variables que cambian al moverse los nodos. Las nubes multipunto a multipunto generalmente no tienen la misma capacidad que las redes punto a punto o las redes punto a multipunto, debido a la sobrecarga adicional de administrar el enrutamiento de la red, y al uso más intensivo del espectro de radio.

Sin embargo, las redes *mesh* son útiles en muchas circunstancias. Al final de este capítulo, vamos a ver algunos ejemplos de cómo construir una red *mesh* multipunto a multipunto utilizando un protocolo de enrutamiento denominado OLSR.

Use la tecnología adecuada

Todos estos diseños de redes pueden ser usados para complementarse unos con otros en una gran red y, obviamente, también se pueden suplementar con técnicas tradicionales de cableado de redes. Es una práctica común, por ejemplo, usar un enlace inalámbrico de larga distancia para proveer acceso a Internet a una ubicación remota, y luego armar un punto de acceso en ese lugar para proveer acceso local. Uno de los clientes de este punto puede también actuar como nodo *mesh*, permitiendo que la red se disperse orgánicamente entre usuarios de computadoras portátiles quienes compartirán el enlace original de acceso a Internet punto a punto.

Ahora que tenemos una idea más clara de la configuración de las redes inalámbricas, podemos comenzar a entender como se realiza la comunicación en dichas redes.

La red lógica

La comunicación es posible sólo cuando los participantes hablan un lenguaje común. Pero una vez que la comunicación se torna más compleja que una simple radiodifusión, los ***protocolos*** se vuelven tan importantes como el lenguaje. Todas las personas en un auditorio pueden hablar inglés, pero sin un conjunto de reglas que establezca quién tiene el derecho a usar el micrófono, la comunicación de las ideas individuales a todo el auditorio es casi imposible. Ahora imagine un auditorio tan grande como el mundo, lleno de todas las computadoras que existen. Sin un conjunto común de protocolos de comunicación que regulen cuándo y cómo cada computador puede hablar, Internet sería una cacofonía, con cada máquina intentando hablar al mismo tiempo.

TCP/IP comprende el conjunto de protocolos que permiten que sucedan las conversaciones en Internet. Entendiendo TCP/IP, usted puede construir redes que virtualmente pueden crecer a cualquier tamaño, y en última instancia formar parte de la Internet global.

El Modelo TCP/IP

Las redes de datos se describen a menudo como construidas en muchas capas. Cada capa depende de la operación de todas las capas subyacentes antes de que la comunicación pueda ocurrir, pero sólo necesita intercambiar datos con la capa superior o la inferior. El modelo de redes TCP/IP[2] comprende 5 capas, como se muestra en este diagrama:

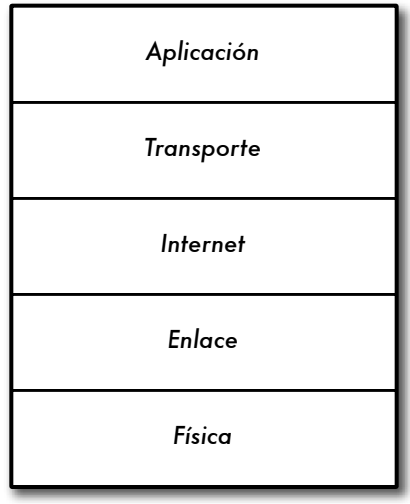


Figura 3.4: El modelo de redes TCP/IP.

En la sección anterior sobre el diseño de redes se describió la capa uno: la ***capa física***. Este es el medio físico donde ocurre la comunicación. Puede ser un cable de cobre CAT5, un cable de fibra óptica, ondas de radio, o cualquier otro medio.

La siguiente capa se denomina ***capa de enlace***. Cuando dos o más nodos comparten el mismo medio físico (por ejemplo, varias computadoras conectadas a un concentrador (*hub*), o un cuarto lleno de computadoras portátiles usando el mismo canal de radio) la capa de enlace establece quién tiene el turno para transmitir en el medio. Ejemplos comunes de protocolos de enlace son Ethernet, Token Ring, ATM, y los protocolos de redes

---

2. El modelo TCP/IP no es un estándar internacional, y su definición varia. Aquí es incluido como un modelo pragmático utilizado para comprender y solucionar problemas en las redes Internet.

inalámbricas (802.11 a/b/g). La comunicación sobre esta capa se llama de ***enlace local***, ya que todos los nodos pueden comunicarse unos con otros directamente. En redes tipo Ethernet, cada nodo tiene su propia ***dirección MAC*** (***Media Access Control***), que es un número único de 48 bits asignado a cada dispositivo de red cuando es fabricado.

Justo sobre la capa enlace está la ***capa Internet***. Para TCP/IP, está constituido por el Protocolo Internet (**IP**). En la capa Internet, los paquetes pueden salir del enlace local de red y ser retransmitidos a otras redes. Los *enrutadores* realizan esta función teniendo por lo menos dos interfaces de red, una en cada una de las redes a ser interconectadas. Los nodos en Internet son especificados por su única ***dirección IP*** global.

Una vez establecido el enrutamiento en Internet, se necesita un método para alcanzar un servicio particular en una dirección IP dada. Esta función es realizada por la próxima capa, la ***capa de transporte***. TCP y UDP son ejemplos comunes de protocolos de la capa de transporte. Algunos protocolos de la capa de transporte (como el TCP) aseguran que todos los datos han llegado a su destino, y son reensamblados y entregados a la próxima capa en el orden correcto.

Finalmente, en la cima tenemos la ***capa de aplicación***. Esta es la capa con la que la mayoría de los usuarios tienen contacto, y es el nivel en el que ocurre la comunicación humana. HTTP, FTP, y SMTP son todos protocolos de la capa de aplicación. Las personas están por encima de todas estas capas, y necesitan poco o ningún conocimiento de las capas subyacentes para usar efectivamente la red.

Una manera de mirar al modelo TCP/IP es pensar en una persona que entrega una carta en un edificio de oficinas. Va a tener que interactuar primero con la calle (capa física), poner atención al tráfico de la misma (capa de enlace), doblar en los lugares correctos para conectarse con otras calles y llegar a la dirección correcta (capa Internet), ir al piso y oficina correcta (capa transporte), y finalmente encontrar el destinatario o recepcionista que puede recibir la carta (capa de aplicación). Las cinco capas pueden ser recordadas fácilmente usando la frase **F**avor **E**ntrar, **I**nmediatamente **T**omar el **A**scensor, para la secuencia de capas Física, Enlace de Datos, Internet, Transporte, y Aplicación, o en inglés “**P**lease **D**on't **L**ook **I**n **T**he **A**ttic,” que se usa por “**P**hysical / **D**ata **L**ink / **I**nternet / **T**ransport / **A**pplication”

Redes inalámbricas 802.11

Antes de que los paquetes puedan ser reenviados y enrutados en Internet, la capa uno (física) y dos (enlace) necesitan estar conectadas. Sin conectividad de enlace local, los nodos no pueden hablarse y enrutar paquetes.

Para proveer conectividad física, los dispositivos de redes inalámbricas deben operar en la misma porción del espectro de radio. Como pudimos ver en el capítulo dos, esto significa que los radios 802.11a se comunican con otro radio 802.11a en frecuencias de 5GHz, y que los radios 802.11b/g hablan con otros 802.11b/g en 2,4GHz, pero un dispositivo 802.11a no puede interoperar con uno 802.11b/g, puesto que usan porciones completamente diferentes del espectro electromagnético.

Más específicamente, las tarjetas inalámbricas deben concordar en un canal común. Si a una tarjeta de radio 802.11b se le asigna el canal 2 mientras que otra el canal 11, no podrán comunicarse.

Cuando dos tarjetas inalámbricas son configuradas para usar el mismo protocolo en el mismo canal de radio, están prontas para negociar conectividad al nivel de la capa de enlace. Cada dispositivo 802.11a/b/g puede operar en uno de los cuatro modos posibles:

1. El ***Modo maestro*** (también llamado ***AP*** o ***modo de infraestructura***) se utiliza para crear un servicio que parece un punto de acceso tradicional. La tarjeta de red crea una red con un canal y un nombre específico (llamado **SSID**), para ofrecer sus servicios. En el modo maestro, las tarjetas inalámbricas administran todas las comunicaciones de la red (autentificación de clientes inalámbricos, control de acceso al canal, repetición de paquetes, etc.). Las tarjetas inalámbricas en modo maestro sólo pueden comunicarse con tarjetas asociadas a ella en modo administrado.
2. El ***Modo administrado*** es denominado algunas veces ***modo cliente***. Las tarjetas inalámbricas en modo administrado sólo pueden unirse a una red creada por una tarjeta en modo maestro, y automáticamente cambiarán su canal para que corresponda con el de ésta. Luego ellas presentan las credenciales necesarias al maestro, y si estas credenciales son aceptadas, se dice que están asociadas con la tarjeta en modo maestro. Las tarjetas en modo administrado no se comunican unas con otras directamente, y sólo se van a comunicar con una tarjeta asociada en modo maestro.
3. El ***Modo ad hoc*** crea una red multipunto a multipunto donde no hay un único nodo maestro o AP. En el modo *ad hoc*, cada tarjeta inalámbrica se comunica directamente con sus vecinas. Cada nodo debe estar dentro del alcance de los otros para comunicarse, y deben concordar en un nombre y un canal de red.
4. El ***Modo Monitor*** es utilizado por algunas herramientas (tales como Kismet, descrito en el capítulo seis) para escuchar pasivamente todo el tráfico de radio en un canal dado. En el modo monitor, las tarjetas inalámbricas no trasmiten datos. Se utiliza para analizar problemas en

un enlace inalámbrico o para observar el uso del espectro en el área local. El modo monitor no es usado para las comunicaciones normales.

Cuando implementamos un enlace punto a punto, o punto a multipunto, un radio opera en modo maestro, mientras que los otros operan en modo administrado. En una red *mesh* multipunto a multipunto, todos los radios operan en modo *ad hoc* de manera que puedan comunicarse directamente.

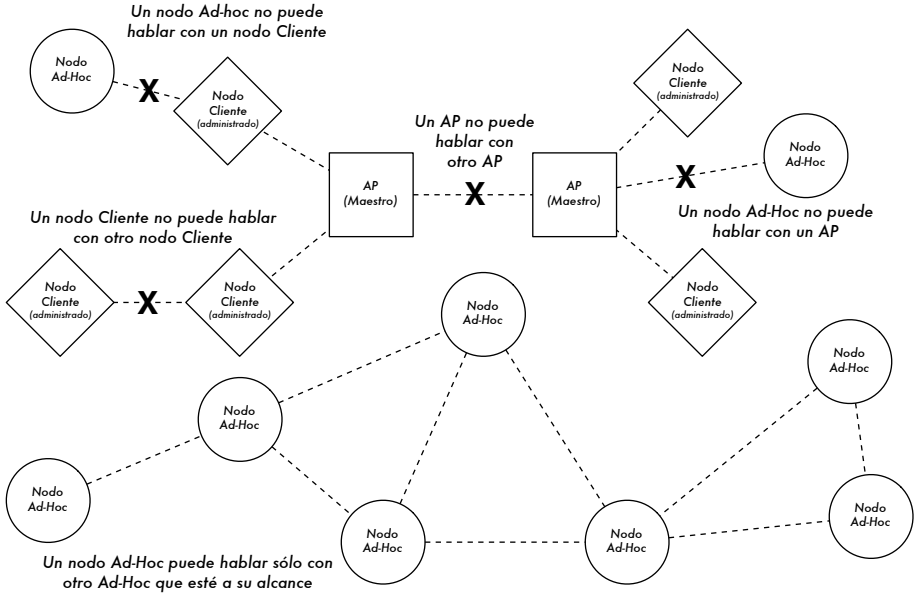


Figura 3.5: AP, clientes, y nodos ad hoc.

Es importante mantener estos modos en mente cuando realiza su diseño de red. Recuerde que los clientes en modo administrado no pueden comunicarse unos con otros directamente, por lo que es posible que quiera instalar un repetidor en modo maestro o *ad hoc*. Como veremos más adelante, el modo *ad hoc* es más flexible pero posee algunos problemas de prestaciones comparado con la utilización de los modos maestro o administrado.

Ahora que sus tarjetas inalámbricas proveen conectividad física y de enlace, están listas para comenzar a pasar paquetes a la capa 3: la capa Internet.

Redes Internet

Direcciones IP, direccionamiento de redes, enrutamiento y reenvío son conceptos relacionados e importantes en redes Internet. Una ***dirección IP*** es un identificador para un nodo de red como un PC, un servidor, un

enrutador o un puente. El ***direccionamiento de redes*** es un sistema usado para asignar estos identificadores en grupos convenientes. El ***enrutamiento*** mantiene un registro del lugar en la red donde están ubicados esos grupos. Los resultados del proceso de enrutamiento se guardan en una lista llamada ***tabla de enrutamiento***. El ***reenvío*** es la acción de usar la tabla de enrutamiento para mandar un paquete al destino final o al "próximo salto" en la dirección a ese destino.

Direcciones IP

En una red IP[3], la dirección es un número de 32 bits, usualmente escrito como 4 números de 8 bits expresados en forma decimal, separados por puntos. Algunos ejemplos de direcciones IP son 10.0.17.1, 192.168.1.1 ó 172.16.5.23.

Direccionamiento de redes

Las redes interconectadas deben ponerse de acuerdo sobre un plan de direccionamiento IP. En Internet, hay comités de personas que asignan las direcciones IP con un método consistente y coherente para garantizar que no se dupliquen las direcciones, y establecen nombres que representan a grupos de direcciones. Esos grupos de direcciones son denominados sub-redes, o subnets. Grandes subnets pueden ser subdivididas en subnets más pequeñas. Algunas veces un grupo de direcciones relacionadas se denomina espacio de direcciones.

En Internet, ninguna persona u organización posee realmente estos grupos de direcciones porque las direcciones sólo tienen significado si el resto de la comunidad de Internet se pone de acuerdo sobre su uso. Mediante acuerdos, las direcciones son asignadas a organizaciones en relación con sus necesidades y tamaño. Una organización a la cual se le ha asignado un rango de direcciones, puede asignar una porción de ese rango a otra organización como parte de un contrato de servicio. Las direcciones que han sido asignadas de esta manera, comenzando con comités reconocidos internacionalmente, y luego repartidas jerárquicamente por comités nacionales o regionales, son denominadas ***direcciones IP enrutadas globalmente***.

Algunas veces es inconveniente o imposible obtener más de una dirección IP enrutada globalmente para un individuo u organización. En este caso, se puede usar una técnica conocida como Traducción de Direcciones de Red o ***NAT*** (*Network Address Translation*). Un dispositivo NAT es un enrutador con

---

3. En este libro vamos a tratar primariamente con IPv4, la versión de este protocolo de mayor uso hoy en día. Aunque IPv6 va a remplazar a IPv4 en algún momento futuro, discutir IPv6 está fuera del alcance de este libro.

dos puertos de red. El puerto externo utiliza una dirección IP enrutada globalmente, mientras que el puerto interno utiliza una dirección IP de un rango especial conocido como ***direcciones privadas***[4]. El enrutador NAT permite que una única dirección global sea compartida por todos los usuarios internos, los cuales usan direcciones privadas. A medida que los paquetes pasan por él los convierte de una forma de direccionamiento a otra. Al usuario le parece que está conectado directamente a Internet y que no requieren software o controladores especiales para compartir una única dirección IP enrutada globalmente.

Enrutamiento

Internet está cambiando y creciendo constantemente. Continuamente se agregan nuevas redes, se añaden y remueven enlaces entre redes, que fallan y vuelven a funcionar. El trabajo del ***enrutamiento*** es determinar la mejor ruta al destino, y crear una tabla de enrutamiento que liste el mejor camino para todos los diferentes destinos.

Enrutamiento estático es el término utilizado cuando la tabla de enrutamiento es creada por configuración manual. Algunas veces esto es conveniente para redes pequeñas, pero puede transformarse rápidamente en algo muy dificultoso y propenso al error en redes grandes. Peor aún, si la mejor ruta para una red se torna inutilizable por una falla en el equipo u otras razones, el enrutamiento estático no podrá hacer uso de otro camino.

Enrutamiento dinámico es un método en el cual los elementos de la red, en particular los enrutadores, intercambian información acerca de su estado y el estado de sus vecinos en la red, y luego utilizan esta información para automáticamente tomar la mejor ruta y crear la tabla de enrutamiento. Si algo cambia, como un enrutador que falla, o uno nuevo que se pone en servicio, los protocolos de enrutamiento dinámico realizan los ajustes a la tabla de enrutamiento. El sistema de intercambio de paquetes y toma de decisiones es conocido como protocolo de enrutamiento. Hay muchos protocolos de enrutamiento usados en Internet hoy en día, incluyendo OSPF, BGP, RIP, y EIGRP.

Las redes inalámbricas asemejan a las redes cableadas, en el sentido de que necesitan protocolos de enrutamiento dinámicos, pero tienen suficientes diferencias para requerir protocolos de enrutamiento orientados a sus necesidades específicas. En particular, las conexiones de las redes cableadas generalmente funcionan bien o no funcionan (por ejemplo, un cable Ethernet está enchufado o no). Las cosas no son tan claras cuando se trabaja con redes inalámbricas. La comunicación inalámbrica puede ser afectada por objetos en movimiento en el camino de la señal, o por señales

---

4. El término direcciones privadas es definido en RFC 1918, http://www.ietf.org/rfc/rfc1918

que interfieren. Consecuentemente, los enlaces pueden no funcionar bien, o funcionar pobremente, o variar entre los dos extremos. Ya que los protocolos de red existentes no toman en cuenta la calidad de un enlace cuando realizan decisiones de enrutamiento, el comité IEEE 802.11 y el IETF están trabajando en estandarizar protocolos para redes inalámbricas. En la actualidad está poco claro cuándo va a surgir un estándar único que tome en cuenta los enlaces de calidad variable.

Mientras tanto, hay muchos intentos de programación *ad hoc* que quieren solucionar el problema. Algunos ejemplos incluyen ***Hazy Sighted Link State*** (***HSLS***) 'Visión Borrosa del Estado del Enlace', ***Ad-hoc On-demand Distance Vector*** (***AODV***) 'Vector de Distancia bajo Demanda *ad hoc*', y ***Optimized Link State Routing*** (***OLSR***) 'Enrutamiento Optimizado según el Estado de la Red'. Otro es el ***SrcR***, una combinación de DSR y ETX implementada por el proyecto Roofnet del MIT. Más adelante en este capítulo vamos a ver ejemplos de cómo implementar una red utilizando OLSR para realizar decisiones de enrutamiento.

Reenvío

El ***reenvío*** es mucho más sencillo que el direccionamiento y el enrutamiento. Cada vez que un enrutador recibe un paquete, consulta su tabla de enrutamiento interna. Comenzando con el bit más significativo (de mayor orden), escudriña la tabla de enrutamiento hasta encontrar la entrada que tenga el mayor número de bits coincidentes con la dirección destinataria. A esto se le llama ***prefijo*** de la dirección. Si en la tabla se encuentra una entrada que coincide con el prefijo, el campo ***hop count*** (***cuenta de salto***) o ***TTL*** (***tiempo de vida***) se decrementa. Si el resultado es cero, el paquete se descarta y se envía una notificación de error al emisor del mismo. De lo contrario, el paquete se envía al nodo o interfaz especificado en la tabla de enrutamiento. Por ejemplo, si la tabla de enrutamiento contiene estas entradas:

```
Destination     Gateway         Genmask         Flags Metric  Iface
10.15.6.0       0.0.0.0         255.255.255.0   U     0       eth1
10.15.6.108     10.15.6.7       255.255.255.255 UG    1       eth1
216.231.38.0    0.0.0.0         255.255.255.0   U     0       eth0
0.0.0.0         216.231.38.1    0.0.0.0         UG    0       eth0
```

... y el paquete llega con la dirección de destino 10.15.6.23, el enrutador sería enviado por la interfaz eth1. Si el paquete tiene un destino de 10.15.6.108, sería reenviado al gateway (pasarela) 10.15.6.7 (ya que es más específica y hay más coincidencia de bits de alto orden que la ruta a la red 10.15.6.0.).

El destino 0.0.0.0 es una convención especial denominada ***gateway por omisión***. Si ningún prefijo corresponde a la dirección de destino, el paquete es

enviado al gateway por omisión. Por ejemplo, si un destino fuera 72.1.140.203, el enrutador reenviaría el paquete a 216.231.38.1 (que presumiblemente acercaría el paquete a su último destino, y así sucesivamente).

Si un paquete llega y no se encuentra una entrada apropiada (por ej. no se ha definido un gateway por omisión y ningún prefijo corresponde a una ruta conocida), se descarta el paquete y se regresa un paquete de error al emisor inicial.

El campo TTL se utiliza para detectar bucles de enrutamiento. En su ausencia, un paquete podría circular indefinidamente entre dos enrutadores que se listan mutuamente como el mejor próximo salto. Esta clase de bucles puede causar mucho tráfico innecesario en la red y constituye una amenaza a su estabilidad. Usar el campo TTL no soluciona los bucles de enrutamiento, pero ayuda a prevenir la destrucción de una red debido a una mala configuración.

Unificando todo

Una vez que todos los nodos de la red tienen una dirección IP, pueden enviar paquetes de datos a cualquier otro nodo. Mediante el enrutamiento y el reenvío, esos paquetes pueden llegar a nodos en redes que no están conectadas físicamente con el nodo original. Este proceso describe mucho de lo que "sucede" en Internet. Esto es ilustrado en la siguiente figura:

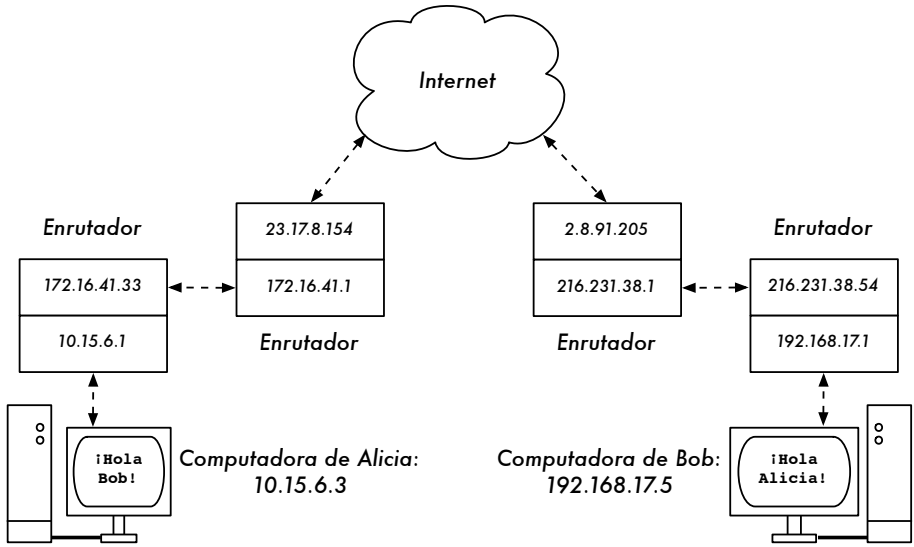


Figura 3.6: Redes Internet. Cada segmento de la red tiene un enrutador con dos direcciones IP, realizando un "enlace local" a dos redes diferentes. Los paquetes son reenviados entre enrutadores hasta que encuentran su destino.

En este ejemplo se puede ver el camino que toman los paquetes cuando Alicia habla con Bob utilizando un servicio de mensajería instantánea. Cada línea punteada representa un cable Ethernet, un enlace inalámbrico, o cualquier otro tipo de red física. El símbolo de la nube es usado comúnmente para "La Internet", y representa cualquier número de redes IP involucradas. Ni Alicia ni Bob necesitan preocuparse de cómo operan esas redes, siempre que los enrutadores reenvíen el tráfico IP hasta el destino final. Si no fuera por los protocolos de Internet y la cooperación de todos en la red, este tipo de comunicación sería imposible.

Ahora que hemos visto cómo fluyen los paquetes en las redes IP, vamos a ver un tipo de red IP muy especializada: una red mallada (*mesh*) OLSR.

Redes mesh con OLSR

La mayoría de las redes WiFi operan en el modo infraestructura: consisten en un punto de acceso en algún lugar (con un radio operando en el modo maestro), conectado a una línea DSL u otra red cableada de larga distancia. En un "hot spot" el punto de acceso generalmente actúa como una estación master que distribuye el acceso a Internet a sus clientes, que operan en el modo administrado. Esta topología es similar al servicio GSM de teléfonos móviles. Los teléfonos móviles se conectan a una estación base sin la cual no se pueden comunicar entre sí. Si hace una llamada en broma a un amigo que está del otro lado de la mesa, su teléfono envía los datos a la estación base de su proveedor que puede estar a una milla de distancia. Luego la estación base reenvía los datos al teléfono de su amigo.

Las tarjetas WiFi en el modo administrado tampoco pueden comunicarse directamente. Los clientes –por ejemplo, dos computadoras portátiles en la misma mesa– tienen que usar un punto de acceso como intermediario. Todo el tráfico entre dos clientes conectados a un punto de acceso debe ser enviado dos veces. Si los clientes A y C se comunican, el cliente A envía datos al punto de acceso B, y luego el punto de acceso va a retransmitir los datos al cliente C. Una transmisión puede tener una velocidad de 600 kbyte/seg (que es prácticamente la máxima velocidad que podemos obtener con 802.11b). En nuestro ejemplo, puesto que los datos deben ser repetidos por el punto de acceso antes de que lleguen a su objetivo, la velocidad real entre ambos clientes va a ser de sólo 300 kbyte/seg.

En el modo *ad hoc* no hay una relación jerárquica entre maestro-cliente. Los nodos pueden comunicarse directamente si están dentro del rango de su interfaz inalámbrica. Por lo tanto, en nuestro ejemplo ambas computadoras podrían conectarse a la velocidad máxima cuando operan en *ad hoc* bajo circunstancias ideales.

La desventaja del modo *ad hoc* es que los clientes no repiten el tráfico destinado a otros clientes. En el ejemplo del punto de acceso, si dos clientes A y C no pueden "verse" directamente con su interfaz inalámbrica, todavía se pueden comunicar si el AP está dentro del rango inalámbrico de ambos clientes.

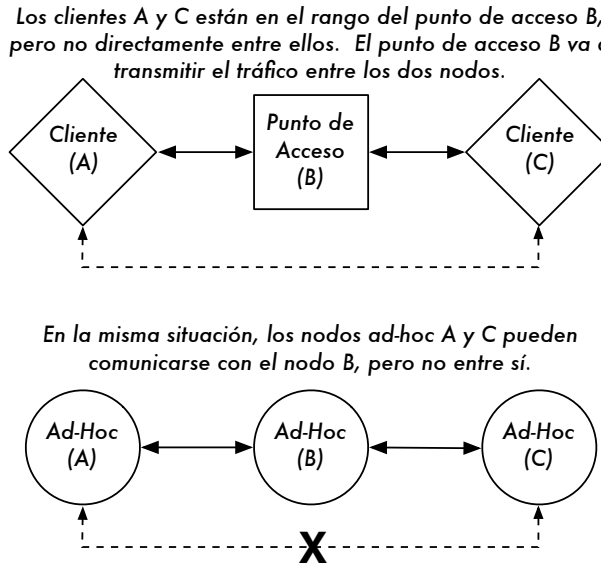


Figura 3.7: El punto de acceso B va a transmitir el tráfico entre los clientes A y C. En el modo ad hoc, el nodo B no va a transmitir el tráfico entre A y C por omisión.

Los nodos *ad hoc* no repiten datos por omisión, pero pueden hacerlo si se aplica el ***enrutamiento***. Las redes malladas (*mesh*) están basadas en la estrategia de que cada nodo actúa como un relevo para extender la cobertura de la red inalámbrica. Cuantos más nodos, mejor será la cobertura de radio y rango de la nube mallada.

Hay un tema álgido que debe ser mencionado en este punto. Si el dispositivo utiliza solamente una interfaz de radio, el ancho de banda disponible se ve reducido significativamente cada vez que el tráfico es repetido por los nodos intermedios en el camino desde A hasta B. Además, va a haber interferencia en la transmisión de esos nodos compartiendo el mismo canal. Por lo tanto, las económicas redes *malladas ad hoc* pueden suministrar muy buena cobertura de radio a una red inalámbrica comunitaria a expensas de la velocidad –especialmente si la densidad de los nodos y la potencia de transmisión son elevadas. Si una red *ad hoc* consiste sólo en unos pocos nodos que están funcionando simultáneamente, si no se mueven y siempre tienen radioenlaces estables –y una larga lista de otras condicionantes– es posible escribir a mano una tabla de enrutamiento individual para todos los nodos.

Desafortunadamente, esas condiciones raramente se encuentran en el mundo real. Los nodos pueden fallar, los dispositivos WiFi pueden cambiar de lugar, y la interferencia puede hacer que los radioenlaces estén inutilizados en cualquier momento. Además nadie quiere actualizar varias tablas de enrutamiento a mano si se adiciona un nodo a la red. Mediante la utilización de protocolos que mantienen automáticamente las tablas de enrutamiento individuales de cada nodo involucrado, podemos olvidarnos de esos temas. Los protocolos de enrutamiento más comunes en el mundo cableado (como el OSPF) no funcionan bien en este ambiente porque no están diseñados para tratar con enlaces perdidos o con topologías que cambian rápidamente.

Enrutamiento mallado con olsrd

El Optimized Link State Routing Daemon –olsrd– (Demonio de Enrutamiento de Estado de Enlace) de *olsr.org* es una aplicación desarrollada para el enrutamiento de redes inalámbricas. Nos vamos a concentrar en este software de enrutamiento por varias razones. Es un proyecto fuente abierta que soporta Mac OS X, Windows 98, 2000, XP, Linux, FreeBSD, OpenBSD y NetBSD. Olsrd está disponible para puntos de acceso que corren Linux como Linksys WRT54G, Asus WI500g, AccessCube o Pocket PCs que corren Linux Familiar, y viene incluido en los equipos Metrix que corren Metrix Pebble. Olsrd puede manejar interfaces múltiples y puede extenderse con diferentes *plug-ins*. Soporta IPv6 y está siendo desarrollado y utilizado activamente en redes comunitarias alrededor del mundo.

Existen varias implementaciones para OLSR, que comenzaron como un borrador IETF escrito en el INRIA en Francia. La implementación de *olsr.org* comenzó como la tesis de máster de Andreas Toennesen en la Universidad UniK. El demonio de enrutamiento se modificó con base en la experiencia práctica de las redes comunitarias gratuitas. El olsrd actual difiere significativamente del borrador original porque incluye un mecanismo denominado Link Quality Extension (Extensión de la Calidad del Enlace) que mide la cantidad de paquetes perdidos entre nodos y calcula las rutas de acuerdo con esta información. Esta extensión rompe la compatibilidad con los demonios de enrutamiento que adhieren al borrador del INRIA. El olsrd disponible en *olsr.org* puede ser configurado para comportarse de acuerdo al borrador del IETF que carece de esta característica –pero no hay una razón para deshabilitar el Link Quality Extension (Extensión de la Calidad del Enlace), a menos que se requiera la compatibilidad con otras implementaciones.

Teoría

Después de haber corrido olsrd por un rato, cada nodo adquiere conocimiento acerca de la existencia de los otros nodos en la nube *mallada*, y sabe cuáles

nodos pueden ser utilizados para enrutar el tráfico hacia ellos. Cada nodo mantiene una tabla de enrutamiento que cubre la totalidad de la nube *mesh*. Este enfoque de enrutamiento mallado es denominado ***enrutamiento proactivo***. En contraste, los algoritmos de ***enrutamiento reactivo*** buscan rutas sólo cuando es necesario enviar datos a un nodo específico.

Hay argumentos en favor y en contra del enrutamiento proactivo, y hay muchas otras ideas acerca de cómo hacer el enrutamiento mallado que vale la pena mencionar. La ventaja más grande del enrutamiento proactivo es que sabemos quién está dentro o fuera de la red y no debemos esperar hasta que se encuentre una ruta. El alto tráfico de protocolo y la mayor cantidad de carga de CPU son algunas de las desventajas. En Berlín, la comunidad de Freifunk está operando una nube mallada donde olsrd tiene que administrar más de 100 interfaces. El promedio de carga del CPU causada por olsrd en un Linksys WRT54G corriendo a 200 MHz es aproximadamente del 30% en la *mesh* de Berlín. Hay un límite al grado hasta el cual la extensión de un protocolo proactivo puede escalar –dependiendo de cuántas interfaces estén involucradas y cuán a menudo se actualizan las tablas de enrutamiento.

Mantener rutas en una nube mallada con nodos estáticos toma menos esfuerzo que hacerlo en una *mesh* compuesta de nodos que están en constante movimiento, ya que la tabla de enrutamiento no necesita ser actualizada tan a menudo.

Mecanismo

Un nodo que corre olsrd envía constantemente mensajes de "*Hello*" con un intervalo dado para que sus vecinos puedan detectar su presencia. Cada nodo computa una estadística de cuántos "Hellos" ha recibido y perdido desde cada vecino –de esta forma obtiene información sobre la topología y la calidad de enlace de los nodos en el vecindario. La información de topología obtenida es difundida como mensajes de control de topología (TC messages) y reenviada por los vecinos que olsrd ha elegido para ser relevadores "multipunto".

El concepto de relevadores multipunto es una nueva idea en el enrutamiento proactivo que viene desde el borrador de OLSR. Si cada nodo retransmite la información de topología que ha recibido, se puede generar una sobrecarga innecesaria. Dichas transmisiones son redundantes si un nodo tiene muchos vecinos. Por esta razón, un nodo olsrd decide cuáles vecinos serán designados "relevadores multipunto favorables", encargados de reenviar los mensajes de control de topología. Nótese que los relevadores multipunto son elegidos exclusivamente con el propósito de reenviar mensajes de CT, la carga útil (payload) se enruta utilizando todos los nodos disponibles.

Existen otros dos tipos de mensajes en OLSR que informan cuándo un nodo ofrece una pasarela (*gateway*) a otras redes (mensajes HNA) o tiene múltiples interfaces (mensajes MID). No hay mucho más que decir acerca de estos mensajes más allá del hecho de que existen. Los mensajes HNA hacen al olsrd muy conveniente para conectarse a Internet con un dispositivo móvil. Cuando un nodo *mesh* se mueve detectará pasarelas a otras redes y siempre elegirá la pasarela a la que tenga la mejor ruta. No obstante, olsrd no es a prueba de balas. Si un nodo anuncia que es una pasarela a Internet –cuando en realidad no lo es, porque nunca tuvo acceso o lo perdió– los otros nodos van a creer esta información de todas formas. La seudo-pasarela es un agujero negro. Para solucionar este problema se desarrolló una aplicación de pasarela dinámica. La aplicación detecta automáticamente si la pasarela está verdaderamente conectada y si el enlace está activo. Si no es así, olsrd interrumpe el envío de mensajes HNA falsos. Es muy recomendable construir y utilizar esta aplicación en lugar de depender de los mensajes HNA estáticos.

Práctica

Olsrd implementa enrutamiento IP en una aplicación interna de los usuarios –la instalación es bastante sencilla. Los paquetes de instalación están disponibles para OpenWRT, AccessCube, Mac OSX, Debian GNU/Linux y Windows. OLSR es una parte estándar de Metrix Pebble. Si usted debe compilar desde la fuente, por favor lea la documentación que viene con el paquete. Si todo está configurado correctamente, lo único que tiene que hacer es iniciar el programa OLSR.

En primer lugar debe asegurarse de que cada una de las interfaces del nodo de la *mesh* tiene asignada una dirección IP estática. No se recomienda (ni es práctico) utilizar DHCP en una red IP mallada. Una solicitud DHCP no va a ser contestada por un servidor DHCP si el nodo que la solicita necesita un enlace de múltiples saltos para alcanzarlo, y aplicar relevo de DHCP (DHCP relay) en toda una malla es poco práctico. El problema podría ser resuelto utilizando IPv6, puesto que se dispone de suficientes direcciones para generar una IP a partir de la dirección MAC para cada tarjeta involucrada (como se sugiere en "IPv6 Stateless Address Autoconfiguration in large mobile *ad hoc* networks" por K. Weniger y M. Zitterbart, 2002).

Una página-wiki donde todas las personas interesadas pueden elegir una dirección IPv4 para cada interfaz que esté corriendo OLSR daemon puede ayudar al propósito bastante bien. No existe una manera sencilla de automatizar el proceso cuando se utiliza IPv4.

En general, la dirección de difusión en las interfaces *mesh* debe ser 255.255.255.255, por convención. No hay una razón para ingresar explícitamente la dirección de difusión, ya que olsrd puede ser configurado

para reemplazar cualquier dirección de difusión con su valor por convención. Sólo debemos asegurarnos de que las configuraciones son las mismas en todos lados. Olsrd puede hacer esto por sí mismo. Cuando se establece un archivo de configuración olsrd por omisión, esta característica debe ser habilitada para eliminar confusiones del tipo “¿por qué los otros nodos no pueden ver mi máquina?"

Configuremos ahora la interfaz inalámbrica. Aquí hay un comando que ejemplifica como configurar una tarjeta WiFi con el nombre wlan0 utilizando Linux:

```
iwconfig wlan0 essid olsr.org mode ad-hoc channel 10 rts 250 frag 256
```

Verifique que la parte inalámbrica de la tarjeta WiFi ha sido configurada de manera que tenga una conexión *ad hoc* con otros nodos *mesh* dentro del rango directo (salto único). Asegúrese de que la interfaz usa el mismo canal inalámbrico, el mismo nombre de red inalámbrica ESSID (Extended Service Set IDentifier) y tiene la misma Cell-ID (Identificación de la Célula) que todas las otras tarjetas WiFi que conforman la malla. Muchas tarjetas WiFi o sus respectivos drivers no actúan de acuerdo con el estándar 802.11 para redes *ad hoc* y por lo tanto no pueden conectarse a una célula. Por otro lado pueden ser incapaces de conectarse con otros dispositivos en la misma tabla, aún si están configurados con el canal y el nombre de la red inalámbrica correctos. Incluso pueden confundir otras tarjetas que se comportan de acuerdo con el estándar creando su propio Cell-ID en el mismo canal y con el mismo nombre de red inalámbrica. Las tarjetas WiFi hechas por Intel que son distribuidas en Notebooks Centrino tienen esta falla.

Para comprobar esto puede utilizar el comando **`iwconfig`** cuando utiliza Linux GNU. Aquí están lo resultados de mi computadora:

```
wlan0   IEEE 802.11b  ESSID:"olsr.org"
        Mode:Ad-Hoc  Frequency:2.457 GHz  Cell: 02:00:81:1E:48:10
        Bit Rate:2 Mb/s   Sensitivity=1/3
        Retry min limit:8   RTS thr=250 B   Fragment thr=256 B
        Encryption key:off
        Power Management:off
        Link Quality=1/70  Signal level=-92 dBm  Noise level=-100 dBm
        Rx invalid nwid:0  Rx invalid crypt:28  Rx invalid frag:0
        Tx excessive retries:98024 Invalid misc:117503 Missed beacon:0
```

Es importante configurar el valor umbral “RTS” '*Request To Send*' para una malla, con el fin de mitigar el efecto de las colisiones entre las transmisiones de los nodos del mismo canal. RTS/CTS establece un procedimiento antes de la transmisión de cada paquete para estar seguro de que el canal está libre. Esto implica una sobrecarga, pero incrementa la prestación en el caso de nodos ocultos –¡y éstos son inherentes a una *mesh*! Este parámetro establece el tamaño del paquete más pequeño (en bytes) para el cual el

nodo envía RTS. El valor umbral de RTS debe ser menor que IP-Packet Size" –Tamaño del paquete IP– y que el "Fragmentation Threshold" –Umbral de Fragmentación–; en caso contrario estaría deshabilitado. En nuestro ejemplo este valor es de 256 bytes. TCP es muy sensible a las colisiones, por lo tanto es importante habilitar RTS.

La fragmentación permite dividir un paquete IP en una ráfaga de paquetes más pequeños para su transmisión. Si bien implica una sobrecarga, en un medio ambiente ruidoso esto reduce la penalización por los errores y le permite a los paquetes atravesar ráfagas de interferencia. Las redes *mesh* son muy ruidosas porque los nodos utilizan el mismo canal y por lo tanto las transmisiones están predispuestas a interferir unas con otras. Este parámetro configura el tamaño máximo antes de que un paquete de datos sea dividido y enviado en una ráfaga –un valor igual al tamaño máximo del paquete IP deshabilita el mecanismo, por lo tanto el umbral de fragmentación debe ser menor que el tamaño del paquete IP. Se recomienda utilizar el umbral de fragmentación.

Una vez que se asigna una dirección IP válida y una *máscara de red*, y que la interfaz inalámbrica está funcionando, el archivo de configuración de olsrd debe ser cambiado para que éste encuentre y utilice las interfaces sobre las cuales debe trabajar.

Para Mac OS-X y Windows se dispone de una buena guía para la configuración y el monitoreo del demonio. Desafortunadamente, esto lleva a que los usuarios que tienen poco conocimiento previo hagan mal las cosas –como permitir agujeros negros. En BSD y Linux el archivo de configuración **`/etc/olsrd.conf`** tiene que ser editado con el editor de texto.

Una configuración olsrd simple

No vamos a mostrar un archivo de configuración completo. Aquí hay algunas de las cosas esenciales que deben ser chequedas.

```
UseHysteresis           no
TcRedundancy            2
MprCoverage             3
LinkQualityLevel        2
LinkQualityWinSize      20

LoadPlugin "olsrd_dyn_gw.so.0.3"
{
        PlParam     "Interval"   "60"
        PlParam     "Ping"       "151.1.1.1"
        PlParam     "Ping"       "194.25.2.129"
}

Interface "ath0" "wlan0" {
        Ip4Broadcast 255.255.255.255
}
```

Hay muchas más opciones disponibles en el archivo **`olsrd.conf`**, pero estas opciones básicas le van a permitir comenzar. Después de realizar estos pasos, olsrd puede ser iniciado con un simple comando en el terminal:

```
olsrd -d 2
```

Personalmente, cuando usamos una estación de trabajo recomiendo correrlo con la opción de depuración –d 2, especialmente la primera vez. Podemos ver qué es lo que hace olsrd y monitorear cómo están funcionando los enlaces a sus vecinos. En dispositivos integrados el nivel de depuración debe ser 0 (apagado), porque genera mucha carga en la CPU.

El resultado debe ser algo parecido a esto:

```
--- 19:27:45.51 ------------------------------------------- DIJKSTRA

192.168.120.1:1.00 (one-hop)
192.168.120.3:1.00 (one-hop)

--- 19:27:45.51 ------------------------------------------------ LINKS

IP address       hyst   LQ     lost   total  NLQ    ETX
192.168.120.1    0.000  1.000  0      20     1.000  1.00
192.168.120.3    0.000  1.000  0      20     1.000  1.00

--- 19:27:45.51 ---------------------------------------- NEIGHBORS

IP address       LQ     NLQ    SYM   MPR   MPRS  will
192.168.120.1    1.000  1.000  YES   NO    YES   3
192.168.120.3    1.000  1.000  YES   NO    YES   6

--- 19:27:45.51 ---------------------------------------- TOPOLOGY

Source IP addr   Dest IP addr     LQ     ILQ    ETX
192.168.120.1    192.168.120.17   1.000  1.000  1.00
192.168.120.3    192.168.120.17   1.000  1.000  1.00
```

Utilizar OLSR en Ethernet y en interfaces múltiples

No es necesario tener una interfaz inalámbrica para probar o utilizar olsrd, aunque fue diseñado para éstas. También puede ser utilizado en cualquier NIC. Las interfaces WiFi no tienen que operar siempre en el modo *ad hoc* para formar una malla cuando los nodos *mesh* tienen más de una interfaz. Para los enlaces dedicados puede ser una buena opción que corran en el modo de infraestructura. Muchas tarjetas y manejadores (drivers) WiFi tienen problemas en el modo *ad hoc*, pero el modo de infraestructura trabaja bien –porque todos esperamos que al menos esta característica funcione. El modo *ad hoc* no ha tenido muchos usuarios hasta ahora, por lo que la implementación del mismo ha sido descuidada por muchos fabricantes.

Actualmente, debido al aumento de la popularidad de las redes *mesh*, se está mejorando esta situación.

Muchas personas utilizan olsrd en interfaces cableadas así como inalámbricas porque no piensan en la arquitectura de red. Simplemente conectan antenas a sus tarjetas WiFi, cables a sus tarjetas Ethernet, habilitan olsrd para que corra en todas las computadoras e interfaces y arrancan. Esto es abusar de un protocolo que fue diseñado para hacer redes inalámbricas en enlaces con pérdidas; pero, ¿por qué no?

Se espera que olsrd sea un superprotocolo. Evidentemente no es necesario enviar mensajes de "Hello" cada dos segundos en una interfaz cableada – pero funciona. Esto no debe ser tomado como una recomendación – simplemente es sorprendente lo que la gente hace con este protocolo y todavía les funciona. De hecho la idea de tener un protocolo que hace todo es muy atractiva para los novatos que quieren tener una LAN enrutada de tamaño pequeño a mediano.

Aplicaciones (*plug-ins*)

Existen varias aplicaciones para olsrd. Para obtener una lista completa, puede chequear el sitio web *olsr.org*. Aquí hay unas instrucciones resumidas para la aplicación de visualización de la topología de la red **`olsrd_dot_draw`**.

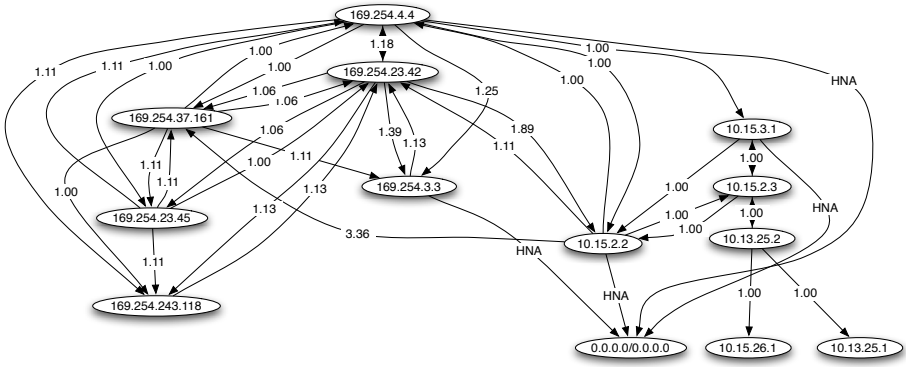


Figura 3.8: Una topología de red OLSR generada automáticamente.

A menudo es muy bueno para la comprensión de una red mallada poder mostrar la topología de la red gráficamente. El olsrd_dot_draw produce la topología en un archivo de formato dot en el puerto TCP 2004. Las herramientas *graphviz* pueden utilizarse para dibujar los gráficos.

Instalar la aplicación dot_draw

Compile todas las aplicaciones OLSR por separado e instálelas. Para cargarlas agregue las siguientes líneas a **/etc/olsrd.conf**

```
LoadPlugin     "olsrd_dot_draw.so.0.3"
{
       PlParam "accept" "192.168.0.5"
       PlParam "port" "2004"
}
```

El parámetro "*accept*" especifica el host que fue aceptado para visualizar la Información Topológica (por el momento, uno solo) y es el "localhost" (host local) por omisión. El parámetro "port" especifica el puerto TCP.

Luego reinicie OLSR y chequee si tiene un resultado en el Puerto TCP 2004

```
telnet localhost 2004
```

Después de un rato debe aparecer algún texto.

Puede guardar las descripciones gráficas resultantes y correr las herramientas **dot** o **neato** del paquete *graphviz* para obtener imágenes.

Bruno Randolf ha escrito un pequeño programa perl que obtiene continuamente la información topológica desde olsrd y la despliega utilizando las herramientas gráficas *graphviz* e *ImageMagick*.

Primero instale los siguientes paquetes en su estación de trabajo:

- graphviz, *http://www.graphviz.org/*
- ImageMagick, *http://www.imagemagick.org/*

Descargue el programa en:
http://meshcube.org/nylon/utils/olsr-topology-view.pl

Ahora usted puede correr el programa con **./olsr-topology-view.pl** y visualizar la topología actualizada casi en tiempo real.

Resolución de problemas

Siempre que las tarjetas WiFi pueden “verse” directamente con sus radios, la herramienta “ping” funcionará sea que olsrd esté corriendo o no. Esto es así porque las máscaras de red grandes efectivamente hacen de cada nodo un enlace local, por lo que los temas de enrutamiento son eludidos en el primer salto. Esto debe ser chequeado en primer lugar, si las cosas no funcionan

como se espera. La mayoría de los dolores de cabeza que la gente enfrenta con WiFi en el modo *ad hoc* son causados por el hecho de que este modo ha sido implementado descuidadamente en los manejadores (*drivers*) y las tarjetas. Si no es posible hacer *ping* a los nodos que están en el rango, es probable que sea un problema de las tarjetas o los manejadores, o que la configuración de la red esté mal.

Si cada máquina puede hacer *ping* a las otras, pero olsrd no encuentra las rutas, entonces deben chequearse las direcciones IP, la máscara de red y la dirección de difusión.

¿Está utilizando un cortafuego? Asegúrese de que no bloquee el puerto UDP 698.

¡Que se divierta!

Estimando la capacidad

Los enlaces inalámbricos pueden proveer a los usuarios un rendimiento real significantemente mayor que las conexiones tradicionales a Internet, tales como VSAT, discado, o DSL. El rendimiento también se denomina ***capacidad del canal***, o simplemente ***ancho de banda*** (aunque este término no está relacionado con el ancho de banda de las ondas de radio). Es importante comprender que la velocidad listada de los dispositivos inalámbricos (la tasa ***de datos***) se refiere a la tasa a la cual los radios pueden intercambiar símbolos, no al rendimiento que va a observar el usuario. Como mencionamos antes, un enlace 802.11g puede utilizar 54Mbps en el radio, pero el rendimiento real será de unos 22Mbps. El resto es la tara (*overhead*) que necesitan los radios 802.11g para coordinar sus señales.

El rendimiento es una medida de bits por tiempo. 22Mbps significa que en un segundo dado pueden ser enviados hasta 22 megabits desde un extremo del enlace al otro. Si los usuarios intentan enviar más de 22 megabits a través del enlace, va a demorar más de un segundo. Si los datos no pueden ser enviados inmediatamente, son puestos en una ***cola de espera***, y transmitidos tan pronto como sea posible. Esta cola de datos incrementa el tiempo que se necesita para que los bits puestos en la cola más recientemente atraviesen el enlace. El tiempo que le toma a los datos atravesar el enlace es denominado ***latencia***, y una latencia muy grande es denominada comúnmente demora (*lag*). El enlace va a enviar todo el tráfico en espera, pero sus clientes seguramente se quejen al incrementar la demora.

¿Cuánto rendimiento van a necesitar sus usuarios realmente? Esto depende de cuántos usuarios existen y de cómo usan su enlace

inalámbrico. Las diversas aplicaciones de Internet requieren diferentes cantidades de rendimiento.

Aplicación	Ancho de Banda/ Usuario	Notas
Mensajería de texto / IM	< 1 Kbps	Como el tráfico es infrecuente y asincrónico, IM va a tolerar mucha latencia.
Correo electrónico	1 to 100 Kbps	Al igual que IM, el correo electrónico es asincrónico e intermitente, por lo tanto va a tolerar la latencia. Los archivos adjuntos grandes, los virus y el correo no deseado aumentan significativamente la utilización del ancho de banda. Los servicios de correo web (tales como Yahoo o Hotmail) deben ser considerados como navegadores web, no como correo electrónico.
Navegadores web	50 - 100+ Kbps	Los navegadores web sólo utilizan la red cuando se solicitan datos. La comunicación es asincrónica, por lo que se puede tolerar una buena cantidad de demora. Cuando los navegadores web, buscan datos voluminosos (imágenes pesadas, descargas largas, etc.) la utilización del ancho de banda aumenta significativamente.
Flujo de audio (streaming)	96 - 160 Kbps	Cada usuario de un servicio de flujo de audio va a utilizar una cantidad constante de una relativamente gran cantidad de ancho de banda, durante el tiempo que está activo. Puede tolerar algo de latencia pasajera mediante la utilización de mucha memoria de almacenamiento temporal en el cliente (buffer). Pero extensos períodos de espera van a hacer que el audio “salte” o que se den fallos en la sesión.

Aplicación	Ancho de Banda/ Usuario	Notas
Voz sobre IP (VoIP)	24 - 100+ Kbps	Como con el flujo de audio, VoIP dedica una cantidad constante de ancho de banda de cada usuario mientras dura la llamada. Pero con VoIP, el ancho de banda utilizado es aproximadamente igual en ambas direcciones. La latencia en una conexión VoIP molesta inmediatamente a los usuarios. Para VoIP una demora mayor a unas pocas decenas de milisegundos es inaceptable.
Flujo de video (streaming)	64 - 200+ Kbps	Como el flujo de audio, un poco de latencia intermitente es superada mediante la utilización de la memoria de almacenamiento temporal del cliente. El flujo de video requiere de alto rendimiento y baja latencia para trabajar correctamente.
Aplicaciones para compartir archivos Par-a-par (BitTorrent, KaZaA, Gnutella, eDonkey, etc.)	0 - infinitos Mbps	Si bien las aplicaciones par a par (peer-to-peer) toleran cualquier cantidad de latencia, tienden a utilizar todo el rendimiento disponible para transmitir datos a la mayor cantidad de clientes y lo más rápido como les sea posible. El uso de estas aplicaciones causa latencia y problemas de rendimiento para todos los otros usuarios de la red, a menos que se utilice un conformador de ancho de banda adecuado.

Para estimar el rendimiento necesario para su red, multiplique el número esperado de usuarios por el tipo de aplicación que probablemente vayan a usar. Por ejemplo, 50 usuarios quienes están principalmente navegando en la web, en los momentos pico van a consumir entre 2.5 a 5Mbps o más de rendimiento, y se va a tolerar algo de latencia. Por otro lado, 50 usuarios simultáneos de VoIP van a requerir de 5Mbps o más de rendimiento **en ambas direcciones** sin absolutamente nada de latencia. Debido a que el equipamiento inalámbrico 802.11g es *half duplex* (esto es, sólo transmite o recibe, nunca las dos cosas a la vez) debe duplicar el rendimiento requerido por un total de **10Mbps**. Sus enlaces deben proveer esa capacidad cada segundo, o las conversaciones van a tener demora.

Ya que es poco probable que todos sus usuarios utilicen la conexión precisamente al mismo momento, una práctica normal es la de

sobresuscribir el rendimiento disponible por algún factor (esto es, permitir más usuarios de los que el máximo de ancho de banda disponible puede soportar). La sobresuscripción en un factor que va desde 2 a 5 es bastante normal. Probablemente usted utilice sobresuscripción cuando construya su infraestructura de red. Si es cuidadoso en el monitoreo del rendimiento real de su red, va a poder planificar cuándo actualizar diferentes partes de la red, y cuántos recursos adicionales va a necesitar.

Es de esperar que, sin importar cuánta capacidad provea, sus usuarios encuentren aplicaciones que utilicen la totalidad de la misma. Como veremos al final de este capítulo, las técnicas de conformación del ancho de banda pueden ayudar a mitigar algunos problemas de latencia. Mediante la conformación de ancho de banda, ***almacenamiento temporal*** (*caching*) web, así como otras técnicas, se puede reducir significativamente la latencia e incrementar el rendimiento global de su red.

Para tener una experiencia de cómo es una demora en conexiones muy lentas, el ICTP ha creado un simulador de ancho de banda. El mismo descarga una página web a toda velocidad y por otro lado a la tasa reducida que usted elija. Esa demostración le da una visión de cómo el bajo rendimiento y la alta latencia reducen la utilidad de Internet como una herramienta de comunicación. El mismo se encuentra disponible en *http://wireless.ictp.trieste.it/simulator/*

Planificar enlaces

Un sistema básico de comunicación consiste de dos radios, cada uno con su antena asociada, separados por la trayectoria que se va a cubrir. Para tener una comunicación entre ambos, los radios requieren que la señal proveniente de la antena tenga un valor por encima de cierto mínimo. El proceso de determinar si el enlace es viable se denomina cálculo del *presupuesto de potencia*. Que las señales puedan o no ser enviadas entre los radios dependerá de la calidad del equipamiento que se esté utilizando y de la disminución de la señal debido a la distancia, denominada ***pérdida en la trayectoria***.

Cálculo del presupuesto del enlace

La potencia disponible en un sistema 802.11 puede caracterizarse por los siguientes factores:

- ***Potencia de Transmisión***. Se expresa en milivatios o en dBm. La Potencia de Transmisión tiene un rango de 30mW a 200mW o más. La potencia TX a menudo depende de la tasa de transmisión. La potencia TX de un dispositivo dado debe ser especificada en los

manuales provistos por el fabricante, pero algunas veces puede ser difícil de encontrar. Algunas bases de datos en línea pueden ayudarlo, una de ellas es la provista por SeattleWireless (*http://www.seattlewireless.net/HardwareComparison*).

- **Ganancia de las Antenas**. Las antenas son dispositivos pasivos que crean el efecto de amplificación debido a su forma física. Las antenas tienen las mismas características cuando reciben que cuando transmiten. Por lo tanto, una antena de 12 dBi simplemente es una antena de 12 dBi, sin especificar si esto es en el modo de transmisión o de recepción. Las antenas parabólicas tienen una ganancia de 19-24 dBi, las antenas omnidireccionales de 5-12 dBi, y las antenas sectoriales, de 12-15 dBi.
- ***El Mínimo Nivel de Señal Recibida***, o simplemente, la sensibilidad del receptor. El RSL (*por su sigla en inglés*) mínimo es expresado siempre como dBm negativos (- dBm) y es el nivel más bajo de señal que la red inalámbrica puede distinguir. El RSL mínimo depende de la tasa de transmisión, y como regla general la tasa más baja (1 Mbps) tiene la mayor sensibilidad. El mínimo va a ser generalmente en el rango de -75 a -95 dBm. Al igual que la potencia TX, las especificaciones RSL deben ser provistas por el fabricante del equipo.
- ***Pérdidas en los Cables***. Parte de la energía de la señal se pierde en los cables, conectores y otros dispositivos entre los radios y las antenas. La pérdida depende del tipo de cable utilizado y de su longitud. La pérdida de señal para cables coaxiales cortos incluyendo los conectores es bastante baja, del rango de 2-3 dB. Lo mejor es tener cables lo más cortos como sea posible.

Cuando calculamos la pérdida en la trayectoria, se deben considerar varios efectos. Algunos de ellos son ***pérdida en el espacio libre***, ***atenuación*** y ***dispersión***. La potencia de la señal se ve disminuida por la dispersión geométrica del frente de onda, conocida comúnmente como pérdida en el espacio libre. Ignorando todo lo demás, cuanto más lejanos los dos radios, más pequeña la señal recibida debido a la pérdida en el espacio libre. Esto es independiente del medio ambiente, se debe solamente a la distancia. Esta pérdida se da porque la energía de la señal radiada se expande en función de la distancia desde el transmisor.

Utilizando los decibeles para expresar la pérdida y utilizando 2,45 GHz como la frecuencia de la señal, la ecuación para la pérdida en el espacio libre es:

```
Lfsl = 40 + 20*log(r)
```

Donde Lfsl (pérdida de señal en el espacio libre, *por su sigla en inglés*) es expresada en dB y r es la distancia en metros entre el transmisor y el receptor.

La segunda contribución para la pérdida en el camino está dada por la atenuación. Esto ocurre cuando parte de la potencia de la señal es absorbida al pasar a través de objetos sólidos como árboles, paredes, ventanas y pisos de edificios. La atenuación puede variar mucho dependiendo de la estructura del objeto que la señal está atravesando, y por lo tanto es muy difícil de cuantificar. La forma más conveniente de expresar esta contribución a la pérdida total es agregando una "pérdida permitida" a la del espacio libre. Por ejemplo, la experiencia demuestra que los árboles suman de 10 a 20 dB de pérdida por cada uno que esté en el camino directo, mientras que las paredes contribuyen de 10 a 15 dB dependiendo del tipo de construcción.

A lo largo del trayecto del enlace, la potencia de RF (radio frecuencia) deja la antena transmisora y se dispersa. Una parte de la potencia de RF alcanza a la antena receptora directamente, mientras que otra rebota en la tierra. Parte de esa potencia de RF que rebota alcanza la antena receptora. Puesto la señal reflejada tiene un trayecto más largo, llega a la antena receptora más tarde que la señal directa. Este efecto es denominado ***multitrayecto***, desvanecimiento o dispersión de la señal. En algunos casos las señales reflejadas se añaden y no causan problemas. Cuando se suman fuera de la fase, la señal recibida es prácticamente nula. En algunos casos, la señal en la antena receptora puede ser anulada por las señales reflejadas. Este fenómeno es conocido como ***anulación***. Existe una técnica simple utilizada para tratar con el multitrayecto, llamada ***diversidad de antena***. Consiste en agregar una segunda antena al radio. De hecho, el Multitrayecto es un fenómeno muy localizado. Si dos señales se suman fuera de fase en una locación, no lo harán en otra locación en las cercanías. Si tenemos dos antenas, al menos una de ellas será capaz de recibir una señal utilizable, aún si la otra está recibiendo una señal distorsionada. En aplicaciones comerciales se utiliza diversidad de antenas conmutadas: tienen múltiples antenas en múltiples entradas con un único receptor. Por lo tanto, la señal es recibida por una única antena a un mismo tiempo. Cuando se transmite, el radio utiliza la última antena usada para la recepción. La distorsión generada por el multitrayecto degrada la habilidad del receptor de recuperar la señal de manera similar a la pérdida de señal. Una forma simple de tomar en cuenta los efectos de la dispersión en el cálculo de la pérdida en el trayecto es cambiar el exponente del factor de la distancia en la fórmula de pérdida en el espacio libre. El exponente tiende a incrementarse con la distancia en un medio ambiente con mucha dispersión. En el exterior con árboles se puede utilizar un exponente de 3, mientras que en el caso de un medio ambiente interno puede usarse uno de 4.

Cuando se combinan pérdida en el espacio libre, atenuación y dispersión, la pérdida en el camino es:

```
L(dB) = 40 + 10*n*log(r) + L(permitida)
```

Donde n es el exponente mencionado.

Para realizar una estimación aproximada de la viabilidad del enlace, se puede evaluar solamente la pérdida en el espacio libre. El medio ambiente puede generar pérdida adicional de señal, y debe ser considerado para una evaluación exacta del enlace. De hecho el medio ambiente es un factor muy importante, y nunca debe ser descuidado.

Para evaluar si un enlace es viable, debemos conocer las características del equipamiento que estamos utilizando y evaluar la pérdida en el trayecto. Cuando hacemos este cálculo, la potencia TX debe ser sumada sólo en uno de los lados del enlace. Si está utilizando diferentes radios en cada lado del enlace, debe calcular la pérdida para cada dirección (utilizando la potencia TX adecuada para cada cálculo). Sumar todas las ganancias y restar las pérdidas resulta en:

```
  TX Potencia de Radio 1
+ Ganancia de la Antena de Radio 1
- Pérdida en los Cables de Radio 1
+ Ganancia de la Antena de Radio 2
- Pérdida en los Cables de Radio 2
_____________________________________

          = Ganancia Total
```

Restar la Pérdida en el trayecto de la Ganancia Total da:

```
          Ganancia Total
      - Pérdida en el trayecto
      _________________________

= Nivel de Señal en un lado del enlace
```

Si el nivel de señal resultante es mayor que el nivel mínimo de señal recibido, entonces ¡el enlace es viable! La señal recibida es suficientemente potente para que los radios la utilicen. Recuerde que el RSL mínimo se expresa siempre como dBm negativos, por lo tanto -56dBm es mayor que -70dBm. En un trayecto dado, la variación en un período de tiempo de la pérdida en el trayecto puede ser grande, por lo que se debe considerar un margen (diferencia entre el nivel de señal recibida y el nivel mínimo de señal recibida). Este margen es la cantidad de señal por encima de la sensibilidad del radio que debe ser recibida para asegurar un enlace estable y de buena calidad durante malas situaciones climáticas y otras anomalías atmosféricas. Un margen de 10-15 dB está bien. Para brindar algo de espacio para la atenuación y el multitrayecto en la señal de radio recibida, se debe tener un margen de 20dB.

Una vez que ha calculado el presupuesto del enlace en una dirección, debe hacer lo mismo en el otro sentido. Substituya la potencia de transmisión del segundo radio y compare los resultados con el nivel mínimo de señal recibido en el primer radio.

Ejemplo de cálculo del presupuesto del enlace

Como ejemplo, queremos estimar la viabilidad de un enlace de 5km con un punto de acceso y un cliente. El punto de acceso está conectado a una antena omnidireccional de 10dBi de ganancia, mientras que el cliente está conectado a una antena sectorial de 14dBi de ganancia. La potencia de transmisión del AP es 100mW (o 20dBm) y su sensibilidad es -89dBm. La potencia de transmisión del cliente es de 30mW (o 15dBm) y su sensibilidad es de -82dBm. Los cables son cortos, con una pérdida de 2dB a cada lado.

Sumar todas las ganancias y restar todas las pérdidas desde el AP hasta el cliente nos da:

```
  20 dBm (TX Potencia del Radio 1)
+ 10 dBi (Ganancia de la Antena de Radio 1)
-  2 dB  (Pérdida en los Cables de Radio 1)
+ 14 dBi (Ganancia de la Antena de Radio 2)
-  2 dB  (Pérdida en los Cables de Radio 2)
————————
  40 dB = Ganancia Total
```

La pérdida en el trayecto de un enlace de 5km, considerando sólo la pérdida en el espacio libre:

```
Pérdida en el trayecto = 40 + 20log(5000) = 113 dB
```

Restamos la pérdida en el trayecto de la ganancia total

```
40 dB - 113 dB = -73 dB
```

Ya que -73dB es mayor que la sensibilidad del receptor del cliente (-82dBm), el nivel de señal es justo el suficiente para que el cliente sea capaz de oír al punto de acceso. Solamente hay 9dB de margen (82dB - 73dB) que nos permite trabajar bien con buen tiempo, pero probablemente no sea suficiente para enfrentar condiciones climáticas extremas.

Ahora debemos calcular la ganancia desde el cliente hacia el punto de acceso:

```
   15 dBm (TX Potencia del Radio 2)
+ 14 dBi (Ganancia de la Antena de Radio 2)
-  2 dB  (Pérdida en los Cables de Radio 2)
+ 10 dBi (Ganancia de la Antena de Radio 1)
-  2 dB  (Pérdida en los Cables de Radio
_____________

   35 dB = Ganancia Total
```

Obviamente, la pérdida en el camino es la misma en el viaje de vuelta. Por lo tanto, nuestro nivel de señal recibido en el punto de acceso es:

```
35 dB - 113 dB = -78 dB
```

Si la sensibilidad de recepción del AP es -89dBm, nos deja un margen de desvanecimiento de 11dB (89dB - 78dB). En general este enlace probablemente va a funcionar pero podría utilizar un poco más de ganancia. Si usamos un plato de 24dBi en el lado del cliente en lugar de una antena sectorial de 14dBi, vamos a tener una ganancia adicional de 10dBi en ambas direcciones del enlace (recuerde que la ganancia de la antena es recíproca). Una opción más cara puede ser la de utilizar radios de más potencia en ambos extremos del enlace, pero nótese que si agregamos un amplificador o una tarjeta de más potencia en uno sólo de los extremos, esto no ayuda a mejorar la calidad global del enlace.

Existen herramientas en línea que pueden ser utilizadas para calcular el presupuesto del enlace. Por ejemplo, el Green Bay Professional Packet Radio's Wireless Network Link Analysis (*http://my.athenet.net/~multiplx/cgi-bin/wireless.main.cgi*) (Paquete Profesional de Análisis de Enlaces de Redes Inalámbricas de Radio de Green Bay) es una excelente herramienta. La Edición Super genera un archivo PDF que contiene las gráficas de la zona de Fresnel y el trayecto de las ondas de radio. El programa de cálculo también puede ser descargado desde el sitio web e instalado localmente. Veremos en más detalle una excelente herramienta en línea en la siguiente sección, ***Software de planificación de enlace***.

El sitio web de Terabeam también tiene muy buenos calculadores disponibles en línea (*http://www.terabeam.com/support/calculations/index.php*).

Tablas para calcular el presupuesto del enlace

Para calcular el presupuesto del enlace, simplemente estime la distancia y complete las siguientes tablas:

Pérdida en el espacio libre a 2,4GHz

Distancia (m)	100	500	1,000	3,000	5,000	10,000
Pérdida (dB)	80	94	100	110	114	120

Ganancia de la Antena:

Antena Radio 1 (dBi)	+ Antena Radio 2 (dBi)	= Ganancia Total de la Antena

Pérdidas:

Radio 1 + Pérdida en los Cables (dB)	Radio 2 + Pérdida en los Cables (dB)	Pérdida en el espacio libre (dB)	= Pérdida Total (dB)

Presupuesto para el enlace de Radio 1 → Radio 2:

Potencia TX de Radio 1	+ Ganancia de la Antena	- Pérdida Total	= Señal	> Sensibilidad del Radio 2

Presupuesto para el enlace de Radio 2 ➜ Radio 1:

Potencia TX de Radio 2	+ Ganancia de la Antena	- Pérdida Total	= Señal	> Sensibilidad del Radio 1

Si la señal recibida es mayor que la intensidad mínima de señal recibida en ambas direcciones del enlace, entonces el enlace es viable.

Software de planificación de enlace

Si bien calcular el presupuesto de un enlace a mano es sencillo, existen algunas herramientas que ayudan a la automatización del proceso.

Además de calcular la pérdida en el espacio libre, esas herramientas también van a tomar en cuenta otros factores relevantes (tales como absorción de los árboles, efectos del terreno, clima, y además estiman la pérdida en el trayecto en áreas urbanas). En esta sección, vamos a discutir dos herramientas gratuitas que son útiles para planificar enlaces inalámbricos: Green Bay Professional Packet Radio la de utilidades interactivas en línea de diseño de redes, y Radio Mobile.

CGIs para diseño interactivo

El grupo Profesional de Radio de Paquetes de Bahía Verde (GBPRR, *por su sigla en inglés*) ha generado una variedad de herramientas de planificación de enlaces que se encuentran gratuitas en línea. Las mismas se encuentran disponibles en *http://www.qsl.net/n9zia/wireless/page09.html*. Como están disponibles en línea, trabajan con cualquier dispositivo que tenga un navegador web y acceso a Internet.

Veremos la primera herramienta, ***Wireless Network Link Analysis*** (***Análisis de Enlaces de Redes Inalámbricas***), en detalle. La encontrará en línea en *http://my.athenet.net/~multiplx/cgi-bin/wireless.main.cgi*

Para comenzar ingrese el canal que va a ser usado por el enlace. El mismo puede ser especificado en MHz o GHz. Si no conoce la frecuencia, consulte la tabla en el Apéndice B. Tenga en cuenta que la tabla lista la frecuencia central del canal, mientras que la herramienta le solicita la frecuencia de transmisión más alta. De todos modos la diferencia es mínima, por lo que puede utilizar la frecuencia central. Para encontrar la frecuencia más alta de transmisión para un canal agregue 11MHz a la frecuencia central.

Luego ingrese los detalles del lado transmisor del enlace, incluyendo el tipo de línea de transmisión, la ganancia de la antena y otros detalles. Intente completar la mayor cantidad de datos que sepa o que pueda estimar. También puede ingresar la altura de la antena y la elevación para ese lugar. Estos datos van a ser usados para calcular el ángulo de inclinación de la antena. Para calcular el despeje de la zona de Fresnel, va a necesitar el Calculador de la Zona de Fresnel de GBPRR.

La siguiente sección es muy similar, pero incluye información acerca del otro extremo del enlace. Ingrese todos los datos disponibles en los campos apropiados.

Finalmente, la última sección describe el clima, el terreno, y la distancia del enlace. Ingrese todos los datos que conozca o que pueda estimar. La distancia del enlace la puede calcular el programa si usted especifica la latitud y la longitud de ambos lugares. Haga clic en el botón de aceptar para obtener un reporte detallado del enlace propuesto. Éste incluye todos los datos ingresados, así como las pérdidas en el trayecto proyectadas, tasas de error y tiempo que el enlace funcionará satisfactoriamente. Esos números son completamente teóricos, pero le darán una idea general de la viabilidad de enlace. Ajustando los valores de la planilla, puede jugar a "¿y qué pasa sí…?" para ver cómo cambiando los parámetros se afecta la conexión.

Además de la herramienta básica de análisis de enlaces, GBPRR provee una "edición súper" que produce un reporte en formato PDF, así como otras herramientas muy útiles (incluyendo el Calculador de la Zona de Fresnel, Calculador de Distancia y de Rumbo, y Calculador de Conversión de Decibeles, por nombrar algunos). También se provee el código fuente para la mayoría de las herramientas.

Radio Mobile

Radio Mobile es una herramienta para el diseño y simulación de sistemas inalámbricos. Predice las prestaciones de radio enlaces utilizando información acerca del equipamiento y un mapa digital del área. Es un software de dominio público que corre con Windows, pero puede utilizarse en Linux con el emulador Wine.

Radio Mobile usa el ***modelo digital de elevación del terreno*** para el cálculo de la cobertura, indica la intensidad de la señal recibida en varios puntos a lo largo del trayecto. Construye automáticamente un perfil entre dos puntos en el mapa digital mostrando el área de cobertura y la primera zona de Fresnel. Durante la simulación chequea la línea visual y calcula la Pérdida en el trayecto, incluyendo pérdidas debido a los obstáculos. Es posible crear redes de diferentes topologías, incluyendo *master/slave* (maestro/esclavo), punto a punto y punto a multipunto.

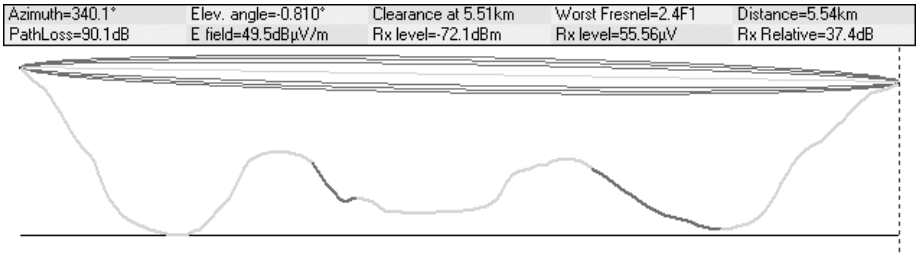


Figura 3.9: Viabilidad del enlace, incluye la zona de Fresnel y estimación de la línea visual, utilizando Radio Mobile

El software calcula el área de cobertura desde la estación de base en un sistema punto a multipunto. Trabaja para sistemas que tienen frecuencias desde 20 kHz a 200 GHz. Los ***Mapas de elevación digital*** (***DEM*** *por su sigla en inglés*) están disponibles gratuitamente desde variadas fuentes y para la mayor parte del mundo. Los DEMs no muestran las líneas costeras u otras fronteras identificables, pero pueden ser combinados fácilmente con otro tipo de datos (como fotos aéreas o cartas topográficas) en varias capas para obtener una representación más útil y rápidamente reconocible. Incluso usted puede digitalizar sus propios mapas y combinarlos con DEMs. Los mapas de elevación digitales pueden combinarse con mapas escaneados, fotos satelitales y servicios de mapas de Internet (tales como Mapquest) para producir predicciones de cobertura precisas.

Radio Mobile puede ser descargado en:
http://www.cplus.org/rmw/download.html

La página principal de Radio Mobile, con ejemplos y tutoriales está disponible en: *http://www.cplus.org/rmw/english1.html*

Radio Mobile bajo Linux

Radio Mobile también funciona utilizando Wine bajo Linux Ubuntu. Si bien las aplicaciones funcionan, algunas etiquetas de los botones pueden quedar mal ubicadas en el marco del botón, lo que puede dificultar su lectura.

Para utilizar Radio Mobile con Linux debemos tener el siguiente entorno:

- IBM Thinkpad x31
- Ubuntu Breezy (v5.10), *http://www.ubuntu.com/*
- Wine versión 20050725, desde el repositorio de Ubuntu Universe

Para instalar Radio Mobile en Windows encontrará instrucciones detalladas en *http://www.cplus.org/rmw/download.html*. Debe seguir todos los pasos excepto el paso 1 (ya que es difícil extraer un DLL desde el

archivo VBRUN60SP6.EXE bajo Linux). Va a tener que copiar el archivo MSVBVM60.DLL desde una computadora con Windows que ya tenga instalado Visual Basic 6 run-time, o buscar en Google el archivo MSVBVM60.DLL y descargarlo.

Continúe con el paso 2 desde la URL anterior, asegúrese de descomprimir los archivos descargados en el mismo directorio dentro del cual ha colocado los archivos DLL. No debe preocuparse por los pasos que siguen al 4; esos son pasos extra, necesarios sólo para los usuarios de Windows.

Finalmente puede iniciar Wine desde una terminal con el comando:

```
# wine RMWDLX.exe
```

En este punto debe ver Radio Mobile corriendo en su sesión XWindows.

Evitando el ruido

Las bandas libres de licenciamiento ISM y U-NII representan una porción muy pequeña del espectro electromagnético conocido. Debido a que esta región puede ser utilizada sin pagar costos de licenciamiento, muchos dispositivos comerciales la utilizan para un amplio rango de aplicaciones. Teléfonos inalámbricos, transmisores de video analógicos, *Bluetooth*, monitores de bebés, e incluso los hornos de microondas compiten con las redes de datos inalámbricas por el uso de la muy limitada banda de 2,4GHz. Esas señales, así como otras redes inalámbricas locales, pueden causar problemas significativos para los enlaces inalámbricos de largo alcance. Para reducir la recepción de señales no deseadas le describimos algunos pasos que puede utilizar.

- **Incremente la ganancia de la antena en ambos extremos del enlace punto a punto.** Las antenas no sólo agregan ganancia a un enlace, sino que el aumento de la directividad tiende a rechazar el ruido proveniente de los alrededores del enlace. Dos platos de alta ganancia que están enfocados uno al otro, rechazarán el ruido desde direcciones que están fuera del trayecto del enlace. Si utilizamos antenas omnidireccionales recibiremos ruido de todas las direcciones.
- **No utilice un amplificador.** Como veremos en el capítulo cuatro, los amplificadores pueden hacer que los problemas de interferencia empeoren con la amplificación indiscriminada de todas las señales recibidas. Al mismo tiempo, causan problemas de interferencia para los otros usuarios de la banda que se encuentren cerca.
- **Utilice antenas sectoriales en lugar de omnidireccionales.** Haciendo uso de varias antenas sectoriales puede reducir el ruido global recibido en un punto de distribución. Si organiza los canales utilizados en cada antena

sectorial, también puede incrementar el ancho de banda disponible para sus clientes.

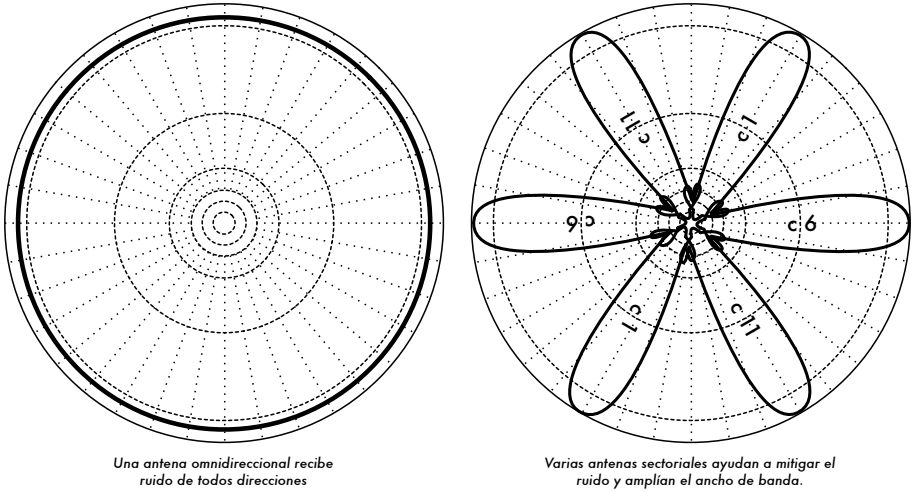


Figura 3.10: Una sola antena omnidireccional vs. múltiples antenas sectoriales.

- **Utilice el mejor canal disponible.** Recuerde que los canales 802.11b/g tienen un acho de 22MHz, pero están separados sólo por 5MHz. Realice una prospección del sitio (como se detalla en el capítulo ocho), y seleccione el canal que esté tan lejos como sea posible de las fuentes de interferencia existentes. Tenga en cuenta que el paisaje inalámbrico puede cambiar en cualquier momento ya que la gente puede agregar nuevos dispositivos (teléfonos inalámbricos, otras redes, etc.). Si de pronto su enlace tiene problemas para enviar paquetes, es posible que deba realizar otra prospección y tomar un canal diferente.
- **Utilice pequeños saltos y repetidores, en lugar de una única tirada a larga distancia. Mantenga sus enlaces punto a punto lo más corto posible.** Si bien es posible crear un enlace de 12km que cruce por el medio de una ciudad, es muy probable que tenga todo tipo de problemas de interferencia. Si puede quebrar ese enlace en dos o tres saltos más cortos, el enlace va a ser más estable. Obviamente, esto es imposible en enlaces rurales a larga distancia, donde se carece de las estructuras de montaje y de energía en los puntos intermedios, pero en estos casos los problemas de ruido son improbables.
- **Si es posible, utilice las bandas 5,8GHz, 900MHz, u otra banda sin licenciamiento.** Si bien esta es una solución a corto plazo, actualmente la mayor parte del equipamiento instalado utiliza 2,4GHz. Utilizar 802.11a, o un dispositivo de convertidor de 2,4GHz a 5,8GHz le va a permitir eludir esta congestión. Si usted puede encontrarlo, existe equipamiento 802.11 viejo que usa el espectro sin licenciamiento a 900MHz (desafortunadamente con un muy baja velocidad). Otras tecnologías tales

como Ronja (*http://ronja.twibright.com/*) usan tecnología óptica para enlaces a corta distancia libres de ruido.

- **Si todo esto falla, utilice un espectro con licenciamiento.** Hay lugares donde todo el espectro sin licenciamiento está siendo utilizado. En esos casos, puede tener sentido gastar el dinero adicional para tener un equipamiento propio que utilice una banda menos congestionada. Para enlaces punto a punto a larga distancia que requieren de muy alto rendimiento y máximo tiempo de disponibilidad, esta es, ciertamente, una opción. Por supuesto esto implica un precio mucho mayor comparado con el equipamiento sin licenciamiento.

Para identificar las fuentes del ruido, necesita herramientas que le muestren qué está sucediendo en el aire a 2,4GHz. Vamos a ver algunos ejemplos de estas herramientas en el capítulo seis.

Repetidores

El componente más crítico para construir un enlace de red a larga distancia es la existencia de ***línea visual*** (a menudo abreviada como ***LOS*** *por su sigla en inglés*). Los sistemas de microondas terrestres simplemente no pueden tolerar colinas altas, árboles, u otros obstáculos en el camino de un enlace a larga distancia. Es necesario que se tenga una idea del relieve de la tierra entre dos puntos antes de poder determinar si un enlace es posible.

Pero aún si hay una montaña entre dos puntos, debemos tener presente que los obstáculos pueden ser transformados en activos. Las montañas pueden bloquear la señal, pero suponiendo que se pueda proveer energía, también pueden actuar como muy buenos ***repetidores***.

Los repetidores son nodos que están configurados para transmitir el tráfico que no es destinado al nodo. En una red mallada, cada nodo es un repetidor. En una red de infraestructura tradicional, los nodos deben ser configurados específicamente para poder pasar el tráfico a otros nodos.

Un repetidor puede usar uno o más dispositivos inalámbricos. Cuando utiliza un sólo radio (denominado ***repetidor de una mano***), la eficiencia global es ligeramente menor que la mitad del ancho de banda disponible, puesto que el radio puede enviar o recibir datos, pero no simultáneamente. Esos dispositivos son baratos, simples y tienen bajos requerimientos de potencia. Un repetidor con dos (o más) tarjetas de radio puede operar todos los radios a toda capacidad, siempre que los mismos estén configurados para usar canales que no se superpongan. Por supuesto, los repetidores también pueden proveer una conexión Ethernet para conectividad local.

Los repetidores pueden ser adquiridos como un juego completo, o fácilmente ensamblados conectando dos o más nodos inalámbricos con un cable de Ethernet. Cuando planee usar un repetidor construido con tecnología 802.11, tenga en cuenta que cada nodo debe ser configurado en el modo maestro, administrado o *ad hoc* que le corresponda. Generalmente, ambos radios en el repetidor están configurados en el modo maestro para permitir que los múltiples clientes puedan conectarse a cualquier lado del repetidor. Pero dependiendo de su diseño de red, uno o más dispositivos van a necesitar utilizar el modo *ad hoc* o el modo cliente.

En general, los repetidores son utilizados para evitar obstáculos en el camino de un enlace a larga distancia. Los mismos pueden ser edificios en el camino, pero esos edificios contienen gente. A menudo podemos hacer acuerdos con los dueños de los edificios para proveerles de ancho de banda a cambio de utilizar la azotea y la electricidad. Si el dueño del edificio no está interesado, podemos intentar persuadir a los inquilinos de los pisos más altos para instalar equipamiento en una ventana.

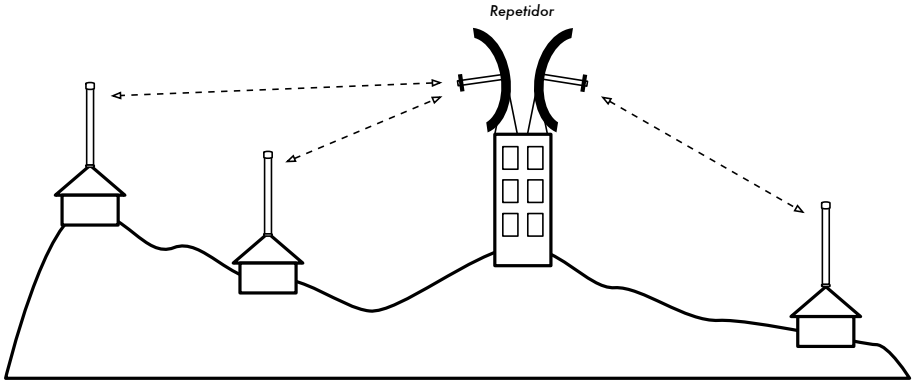


Figura 3.11: El repetidor reenvía los paquetes por el aire entre los nodos que no tienen una línea visual directa.

Si usted no puede pasar sobre, o a través de un obstáculo, a menudo lo puede rodear. En lugar de usar un enlace directo, intente hacer un salto múltiple para eludir el obstáculo.

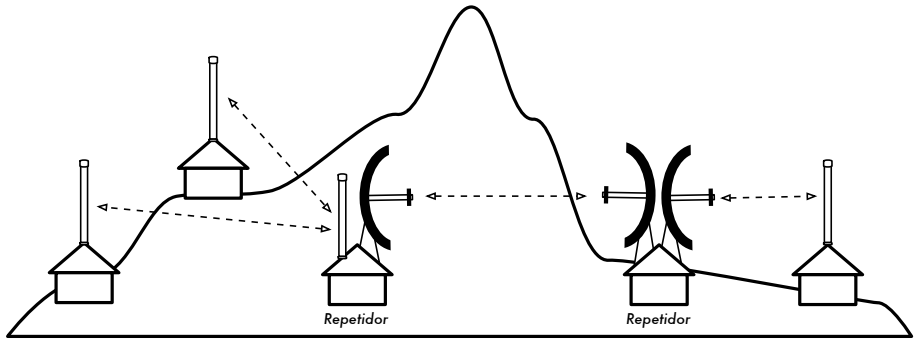


Figura 3.12: No había energía disponible en lo alto de la colina, pero fue circunvalada con el uso de múltiples repetidores ubicados alrededor de la base.

Finalmente, usted podría necesitar ir hacia atrás para poder avanzar. Si tenemos un lugar alto en una dirección diferente, y ese lugar puede ver más allá del obstáculo, se puede hacer un enlace estable a través de una ruta indirecta.

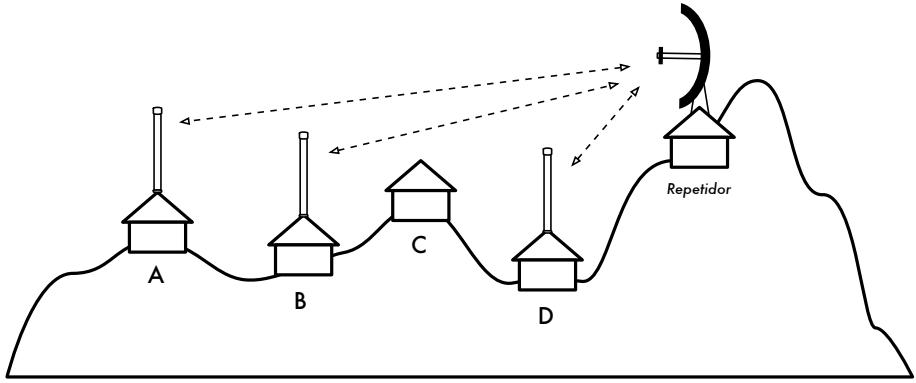


Figura 3.13: El lugar D no puede ver al lugar A o el B, porque el lugar C está en el camino y no está interesado en tener un nodo. Al instalar un repetidor en un lugar alto los nodos A, B, y D se pueden comunicar. El tráfico desde el nodo D en realidad viaja más lejos que el del resto de la red antes de que el repetidor reenvíe esos datos.

Los repetidores en la red me recuerdan el principio de “los seis grados de separación”. Esta idea dice que no importa a quién está buscando, sólo necesita contactar cinco intermediarios antes de encontrar a la persona. Los repetidores pueden “ver” una gran cantidad de intermediarios, y si su nodo está dentro del rango podrá comunicarse con cualquier nodo que el repetidor pueda alcanzar.

Optimización del Tráfico

El ancho de banda se mide como un cociente de número de bits transmitidos en un segundo. Esto significa que dado suficiente tiempo, la cantidad de información transmisible en cualquier enlace se acerca al infinito. Desafortunadamente, para un período de tiempo finito, el ancho de banda provisto por una conexión de red cualquiera no es infinito. Siempre puede descargar (o cargar) tanto tráfico como quiera; sólo que debe esperar todo lo que sea necesario. Por supuesto que los usuarios humanos no son tan pacientes como las computadoras, y no están dispuestos a esperar una infinita cantidad de tiempo para que su información atraviese la red. Por esta razón, el ancho de banda debe ser gestionado y priorizado como cualquier otro recurso limitado.

Se puede mejorar significativamente el tiempo de respuesta y maximizar el rendimiento disponible mediante la eliminación del tráfico indeseado y redundante de nuestra red. Esta sección describe varias técnicas comunes para asegurarse de que nuestra red solamente está transportando el tráfico que debe y no otro.

Almacenamiento Web temporal

Un servidor web *proxy* es un servidor en la red local que mantiene copias de lo que se ha leído recientemente, páginas web que son utilizadas a menudo, o partes de esas páginas. Cuando la siguiente persona busque esas páginas, las mismas se recuperan desde el servidor *proxy* local sin ir hasta Internet. Esto resulta, en la mayoría de los casos en un acceso al web más rápido, al mismo tiempo que se reduce significativamente la utilización del ancho de banda con Internet. Cuando se implementa un servidor *proxy*, el administrador debe saber que existen algunas páginas que no son almacenables, por ejemplo, páginas que son el resultado de programas del lado del servidor, u otros contenidos generados dinámicamente.

Otra cosa que también se ve afectada es la manera como se descargan las páginas web. Con un enlace a Internet lento, una página normal comienza a cargarse lentamente, primero mostrando algo de texto y luego desplegando los gráficos uno por uno. En una red con un servidor *proxy*, puede haber un retraso durante el cual parece que nada sucede, y luego la página se carga por completo rápidamente. Esto sucede porque la información es enviada a la computadora tan rápido que para el rearmado de la página se toma una cantidad de tiempo perceptible. El tiempo global que toma este procedimiento puede ser sólo de diez segundos (mientras que sin un servidor *proxy*, puede tomar 30 segundos cargar la página gradualmente). Pero a menos que esto se explique a algunos usuarios impacientes, estos pueden decir que el servidor *proxy* está haciendo las cosas más lentamente.

Generalmente es tarea del administrador lidiar con la percepción de los usuarios acerca de temas como éste.

Servidores *proxy*

Existen varios servidores proxy disponibles. Los que siguen son los paquetes de software utilizados más comúnmente:

- **Squid.** El software libre Squid es el estándar de facto en las universidades. Es gratuito, confiable, sencillo de utilizar y puede ser mejorado (por ejemplo, añadiendo filtros de contenido y bloqueos de publicidad). Squid produce bitácoras (*logs*) que pueden ser analizadas utilizando software como Awstats, o Webalizer, los cuales son de fuente libre y producen buenos reportes gráficos. En la mayoría de los casos, es más fácil instalarlo como parte de la distribución en lugar de descargarlo desde *http://www.squid-cache.org/* (la mayoría de las distribuciones Linux como Debian, así como otras versiones de Unix como NetBSD y FreeBSD vienen con Squid). Una buena guía de configuración de Squid se puede encontrar en: *http://squid- docs.sourceforge.net/latest/book-full.html*.
- **Servidor Proxy Microsoft 2.0.** No está disponible para instalaciones nuevas porque ha sido reemplazado por el servidor Microsoft ISA y ha dejado de tener soporte. Si bien es utilizado por algunas instituciones es mejor no considerarlo para instalaciones nuevas.
- **Servidor Microsoft ISA.** ISA es un muy buen programa de servidor *proxy*, pero demasiado caro para lo que hace. Sin embargo, con descuentos académicos puede ser accesible para algunas instituciones. Produce sus propios reportes gráficos, pero sus archivos de bitácora (log) también pueden ser analizados con el popular software Sawmill (*http://www.sawmill.net/*). Los administradores de un sitio con un Servidor MS ISA deben dedicar tiempo suficiente para obtener la configuración adecuada; por otra parte, el Servidor MS ISA Server puede utilizar gran cantidad de ancho de banda. Por ejemplo, una instalación por omisión puede consumir fácilmente más ancho de banda que lo que el sitio ha utilizado anteriormente, porque las páginas comunes con fechas de expiración cortas (tales como los sitios de noticias) se actualizan continuamente. Por lo tanto, es importante que la captura preliminar (pre-fetching) se configure correctamente, para que sea realizada durante la noche. El servidor ISA también puede ser asociado a productos de filtrado de contenidos tales como WebSense. Para más información vea el sitio: *http://www.microsoft.com/isaserver/* y *http://www.isaserver.org/*.

Evitando que los usuarios evadan el servidor proxy

Si bien eludir la censura de Internet y las políticas de acceso restrictivo a la información son un laudable esfuerzo político, los servidores *proxy* y los

firewalls son herramientas necesarias en áreas con anchos de banda extremadamente limitados. Sin ellos la estabilidad y la usabilidad de la red se ven amenazadas por los propios usuarios legítimos de la red. Las técnicas para eludir un servidor *proxy* pueden ser encontradas en: *http://www.antiproxy.com/*. Este sitio es útil para que los administradores vean cómo sus redes pueden enfrentarse a estas técnicas.

Para reforzar el uso del almacenamiento ***temporal proxy*** (*caching proxy*), puede simplemente considerarse instaurar una política de acceso a la red y confiar en sus usuarios. En el diseño que sigue, el administrador debe confiar en que los usuarios no van a eludir el servidor *proxy*.

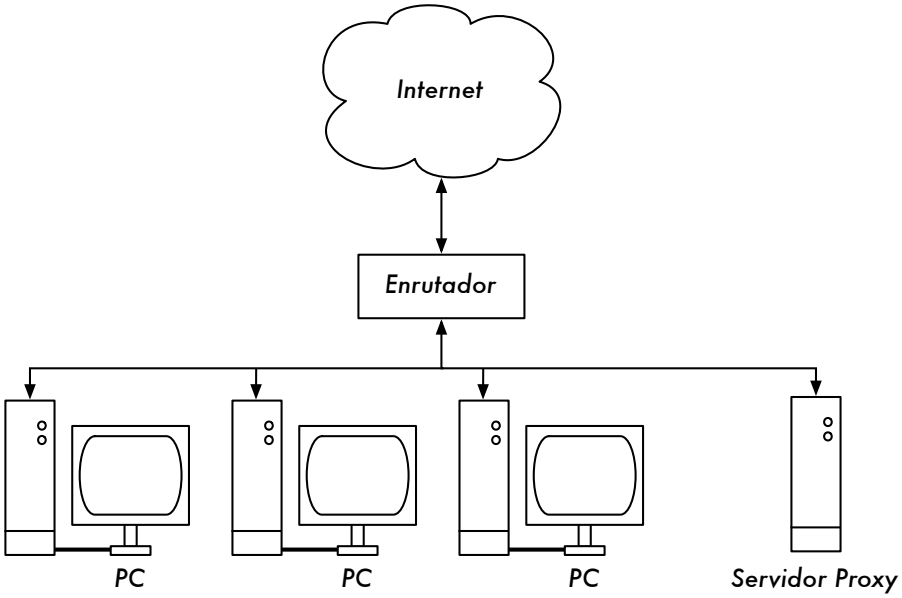


Figura 3.14: Esta red se basa en la confianza en que los usuarios van a configurar apropiadamente sus PCs para utilizar el servidor proxy.

En este caso el administrador generalmente utiliza una de las siguientes técnicas:

- **No divulgar la dirección de la pasarela por omisión (default gateway) a través de DCHP.** Esto puede funcionar por un tiempo, pero algunos usuarios que quieren eludir el proxy pueden encontrar o buscar la dirección de **la pasarela por omisión**. Una vez que esto pasa, se tiende a difundir cómo se elude el proxy.
- **Utilizar políticas de grupo o de dominio.** Esto es muy útil para configurar el servidor *proxy* adecuado para Internet Explorer en todas las computadoras del dominio, pero no es muy útil para evitar que el *proxy* sea eludido, porque se basa en el registro de un usuario en el dominio NT.

Un usuario con una computadora con Windows 95/98/ME puede cancelar su registro y luego eludir el *proxy*, y alguien que conoce la contraseña de un usuario local en su computadora con Windows NT/2000/XP puede registrarse localmente y hacer lo mismo.

- **Rogar y luchar con los usuarios.** Ésta nunca es una situación óptima para un administrador de red. La única forma de asegurarse que los *proxy* no van a ser eludidos es mediante la utilización del diseño de red adecuado, por medio de una de las tres técnicas descritas a continuación.

Cortafuego (*Firewall*)

Una de las maneras más confiable para asegurarse que las PC no van a eludir el *proxy* puede ser implementada utilizando un cortafuego.

El cortafuego puede configurarse para que solamente pueda pasar el servidor proxy, por ejemplo, para hacer solicitudes de HTTP a Internet. Todas las demás PC están bloqueadas, como se muestra en el siguiente diagrama.

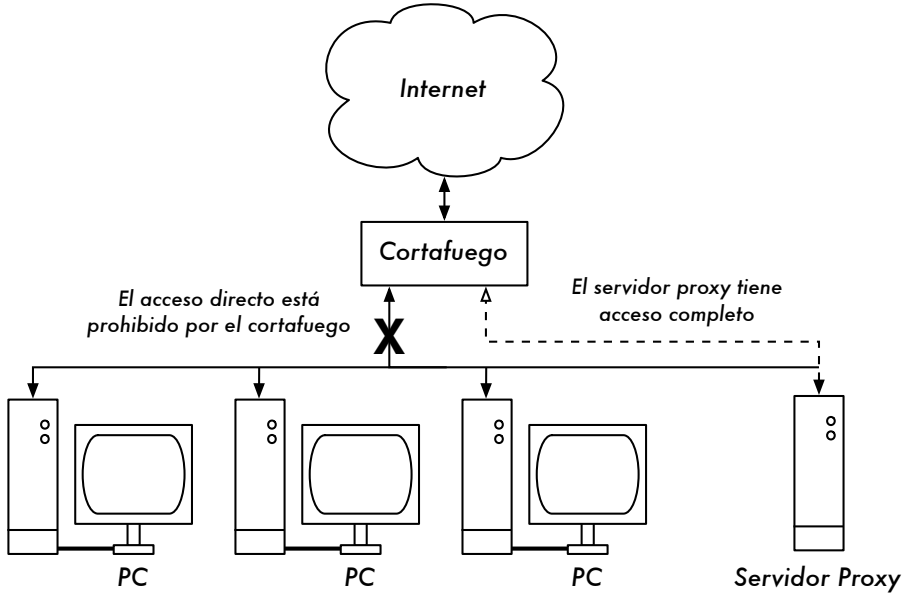


Figura 3.15: El cortafuego les impide a los PCs acceder a Internet directamente, pero les permite el acceso a través del servidor proxy.

Confiar en un cortafuego, como en el diagrama anterior, puede o no ser suficiente, dependiendo de cómo esté configurado. Si sólo bloquea el acceso desde la LAN del campus al puerto 80 en los servidores web, va a haber formas, para los usuarios inteligentes, de encontrar caminos que lo

rodeen. Aún más, van a ser capaces de utilizar protocolos sedientos de ancho de banda como Kazaa.

Dos tarjetas de red

Posiblemente, el método más confiable es el de instalar dos tarjetas de red en el servidor *proxy* y conectar la red del campus a Internet como se muestra en la siguiente figura. De esta forma, el diseño de red hace físicamente imposible alcanzar la Internet sin pasar a través del servidor *proxy*.

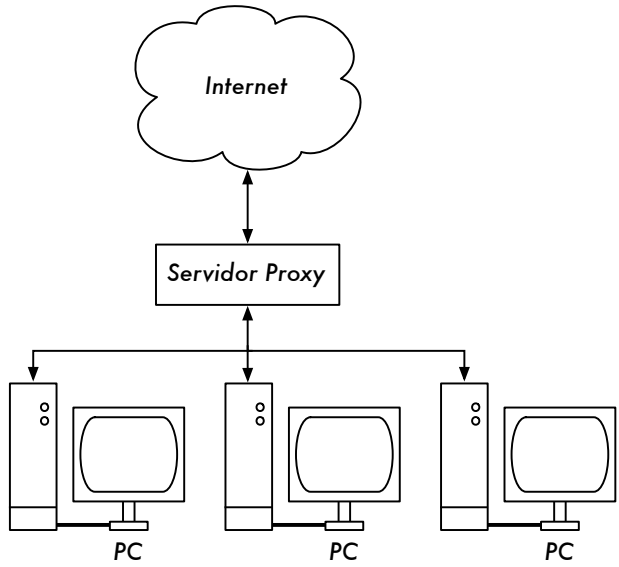


Figura 3.16: La única ruta hacia Internet es a través del proxy.

El servidor *proxy* en este diagrama no debe tener habilitado IP *forwarding*, a menos que los administradores conozcan exactamente qué es lo que quieren dejar pasar.

Una gran ventaja de este diseño es que puede utilizarse una técnica conocida como ***transparent proxying***. Utilizar *proxy* transparente significa que las solicitudes web de los usuarios son reenviadas automáticamente al servidor *proxy*, sin ninguna necesidad de configurar manualmente los navegadores web para que lo utilicen. Esto fuerza efectivamente a que todo el tráfico web sea almacenado localmente, lo que elimina muchas posibilidades de error de los usuarios, y va a trabajar incluso con dispositivos que no soportan el uso de un *proxy* manual. Para más detalles sobre cómo configurar un *proxy* transparente con Squid, diríjase a:

- *http://www.squid-cache.org/Doc/FAQ/FAQ-17.html*
- *http://en.tldp.org/HOWTO/mini/TransparentProxy-2.html*

Enrutamiento basado en políticas

Una forma de prevenir la circunvalación del *proxy* utilizando equipamiento Cisco es con una política de enrutamiento. El enrutador Cisco dirige transparentemente las solicitudes web al servidor *proxy*. Esta técnica es utilizada en la Universidad Makerere. La ventaja de este método es que, si el servidor *proxy* está caído, las políticas de enrutamiento pueden ser removidas temporalmente permitiéndoles a los clientes conectarse directamente a Internet.

Sitio web espejo (*mirror*)

Con el permiso del dueño o del administrador del sitio web, el sitio completo puede ser copiado durante la noche al servidor local, siempre que el mismo no sea demasiado grande. Esto es algo que se debe tener en cuenta para sitios web importantes, que son de interés particular para la organización, o que son muy populares entre los usuarios de la web. Si bien esto puede ser útil, tiene algunas fallas potenciales. Por ejemplo, si el sitio que es duplicado contiene programas CGI u otros contenidos dinámicos que requieren de interacción con el usuario, va a haber problemas. Un ejemplo es el sitio web que requiere que la gente se registre en línea para una conferencia. Si alguien se registra en línea en un servidor duplicado (y el programa de duplicado funciona bien), los organizadores del sitio no van a tener la información de que la persona se registró.

Debido a que un sitio duplicado puede infringir los derechos de copyright, esta técnica debe ser utilizada solamente con el permiso del sitio en cuestión. Si el sitio corre ***rsync***, puede ser duplicado utilizando rsync. Ésta es la forma más rápida y eficiente de mantener los contenidos del sitio sincronizados. Si el servidor web remoto no está corriendo rsync, se recomienda utilizar el software llamado ***wget***. Éste es parte de la mayoría de las versiones de Unix/Linux. Una versión de Windows puede encontrase en *http://xoomer.virgilio.it/hherold/*, o en el paquete de herramientas gratuito de Cygwin Unix (*http://www.cygwin.com/*).

Se puede utilizar un *script* que corra cada noche en un servidor web local y haga lo siguiente:

- Cambiar el directorio raíz del servidor web: por ejemplo, **`/var/www/`** en Unix, o **`C:\Inetpub\wwwroot`** en Windows.
- Duplicar el sitio web utilizando el siguiente comando:

```
wget --cache=off -m http://www.python.org
```

El sitio duplicado va a estar en el directorio **`www.python.org`**. El servidor web debe ser configurado para servir los contenidos de ese directorio como

un host virtual basado en nombre. Ponga en marcha el servidor local DNS para falsificar una entrada para este sitio. Para que esto funcione, las PC clientes deben ser configuradas para usar el/los servidor(es) DNS local(es) como el DNS primario. (Esto es siempre aconsejable, porque el almacenamiento intermedio (*caching*) del servidor DNS acelera los tiempos de respuesta web).

Pre-poblar la memoria intermedia (*cache*) utilizando wget

En lugar de instalar un sitio web duplicado como se describió en la sección anterior, un mejor enfoque es el de poblar el *proxy* cache utilizando un proceso automatizado. Este método ha sido descrito por J. J. Eksteen y J. P. L. Cloete del CSIR en Pretoria, Sud África, en un artículo titulado **Mejorar el Acceso a la Red de Redes en Mozambique a Través del Uso de Servidores Proxy Reflejados y Almacenados** (**Enhancing International World Wide Web Access in Mozambique Through the Use of Mirroring and Caching Proxies**). En este artículo (disponible en línea en *http://www.isoc.org/inet97/ans97/cloet.htm*) los autores describen cómo trabaja el proceso:

> "*Un proceso automatizado recupera la página inicial del sitio y especifica el número de páginas extra (siguiendo recursivamente los enlaces HTML en las páginas recuperadas) a través del uso de un proxy. En lugar de copiar las páginas recuperadas en el disco local, el proceso de duplicación descarta las páginas recuperadas. Esto se hace para conservar los recursos del sistema así como para evitar posibles problemas de copyright. Mediante el uso del proxy como intermediario, se garantiza que las páginas recuperadas están en el cache del proxy como si un cliente hubiera accedido a esa página. Cuando un cliente accede a la página recuperada, le es brindada desde el cache y no desde el enlace internacional congestionado. Este proceso puede ser corrido en momentos de poco uso de la red, para maximizar la utilización del ancho de banda y no competir con otras actividades de acceso.*"

El siguiente comando (programado para correr en la noche, o una vez al día o a la semana) es todo lo que se necesita (debe repetirse para cada sitio que necesita ser pre-poblado).

```
wget --proxy-on --cache=off --delete after -m http://www.python.org
```

Explicación:

- **-m**: Duplica el sitio completo. wget comienza en *www.python.org* y sigue todos los hiperenlaces, es decir que descarga todas las subpáginas.

- **--proxy-on**: Se asegura que wget haga uso del servidor *proxy*. Esto puede no necesitarse en aplicaciones donde se utiliza un servidor *proxy* transparente.
- **--cache=off**: Se asegura de que el contenido fresco es recuperado desde Internet, y no desde el servidor *proxy* local.
- **--delete after**: Borra la copia duplicada. El contenido duplicado permanece en el *cache* del *proxy* si hay suficiente espacio en el disco, y los parámetros del servidor *proxy* son aplicados correctamente.

Además, wget tiene muchas otras opciones; por ejemplo, proveer contraseñas para los sitios web que las requieren. Cuando utilizamos esta herramienta, Squid debe ser configurado con suficiente espacio en el disco para que contenga todos los sitios pre-poblados y más (para un uso normal de Squid que involucre otras páginas además de las pre-pobladas). Afortunadamente, el espacio de disco es cada vez más barato y su tamaño mucho más grande que nunca. Sin embargo, esta técnica puede ser utilizada solo con unos pocos sitios seleccionados. Estos sitios no deben ser muy grandes para que los procesos terminen antes de que las horas del día de trabajo comiencen, y se debe estar vigilando el espacio de disco disponible.

Jerarquías de memoria temporal (*cache*)

Cuando una organización tiene más de un servidor *proxy*, los mismos pueden compartir información *cache* entre ellos. Por ejemplo, si una página web está en el *cache* del servidor A, pero no en el cache del servidor B, un usuario conectado a través del servidor B puede acceder a la página web en el servidor A a través del servidor B. El ***Protocolo de Inter-Cache*** (Inter-Cache Protocol (***ICP***)) y el (Cache Array Routing Protocol (***CARP***)) pueden compartir información del *cache*. De éstos, el protocolo CARP es considerado el mejor. Squid soporta ambos protocolos, y el Servidor MS ISA soporta CARP. Para más información diríjase a: *http://squid-docs.sourceforge.net/latest/html/c2075.html*. El compartir información *cache* reduce el uso de ancho de banda en organizaciones donde se utiliza más de un *proxy*.

Especificaciones Proxy

En la red de un campus universitario, debería haber más de un servidor *proxy*, por razones de prestaciones y de redundancia. Con los discos actuales más baratos y más grandes, se pueden construir servidores *proxy* más poderosos, con 50 GB o más de espacio de disco asignado al *cache*. Las prestaciones del disco son importantes, por lo que los discos SCSI más rápidos se van a desempeñar mejor (aunque un *cache* basado en un IDE es

mejor que nada). RAID (Redundant Array of Independent Disks) o el uso de espejos (mirror) no son recomendados.

Se aconseja dedicar un disco exclusivamente para el cache. Por ejemplo, un disco puede ser para el *cache*, y el segundo para el sistema operativo y la bitácora del *cache*. Squid está diseñado para utilizar toda la memoria RAM que puede conseguir porque es mucho más rápido cuando los datos son recuperados desde la memoria RAM que cuando vienen desde el disco duro. Para una red en un campus, la memoria RAM debe ser de 1GB o más: Además de la memoria requerida para el sistema operativo y otras aplicaciones, Squid requiere 10 MB de RAM por cada 1 GB de disco *cache*. Por lo tanto, si tenemos un espacio de disco de 50 GB asignados al *cache*, Squid va a requerir 500 MB de memoria extra.

La máquina también va a requerir 128 MB para Linux y 128 MB para X-windows. Otros 256 MB deben agregarse para otras aplicaciones, y para que todo pueda funcionar fácilmente. Nada mejora más el rendimiento de una computadora como la instalación de una gran cantidad de memoria, porque esto reduce la necesidad de utilizar el disco duro. La memoria es miles de veces más rápida que el disco duro. Los sistemas operativos modernos frecuentemente mantienen los datos accedidos en la memoria siempre que haya suficiente RAM disponible. Pero utilizan el archivo de la página del disco duro como un área de memoria extra cuando no tienen suficiente memoria RAM.

Almacenamiento intermedio (*cache*) y optimización de DNS

Los servidores DNS con sólo la función de *cache* no son autoridades de ningún dominio, solo almacenan los resultados de solicitudes pedidas por los clientes, tal como un servidor *proxy* que almacena páginas web populares por cierto tiempo. Las direcciones DNS son almacenadas hasta que su ***tiempo de vida*** (***TTL*** *por su sigla en inglés*) expira. Esto va a reducir la cantidad de tráfico DNS en su conexión a Internet, porque el *cache* DNS puede ser capaz de satisfacer muchas de las preguntas localmente. Por supuesto que las computadoras de los clientes deben ser configuradas para utilizar el nombre del servidor solo de *cache* como su servidor DNS. Cuando todos los clientes utilicen ese servidor DNS como su servidor principal, se poblará rápidamente el *cache* de direcciones IP a nombres, por lo tanto los nombres solicitados previamente pueden ser resueltos rápidamente. Los servidores DNS que son autoridades para un dominio también actúan como cache de la conversión nombres-direcciones de hosts de ese dominio.

Bind (named)

Bind es el programa estándar de facto utilizado para servicios de nombre en Internet. Cuando Bind está instalado y corriendo, va a actuar como un servidor cache (no se necesita más configuración). Bind puede ser instalado desde un paquete como el Debian o un RPM. Instalarlo desde un paquete en general es el mejor método. En Debian, escriba

```
apt-get install bind9
```

Además de implementar *cache*, Bind también puede alojar zonas de autoridad, actuar como esclavo de zonas de autoridad, implementar *split horizon* (horizonte dividido), y todo lo demás que es posible con DNS.

dnsmasq

Un servidor DNS de cache alternativo es ***dnsmasq***. Está disponible para BSD y la mayoría de las distribuciones Linux, o desde *http://freshmeat.net/projects/dnsmasq/*. La gran ventaja de dnsmasq es la flexibilidad: actúa como un proxy DNS de *cache* y como una fuente autorizada para hosts y dominios, sin una configuración complicada de archivos de zona. Se pueden hacer actualizaciones a la zona de datos sin ni siquiera reiniciar el servicio. También actúa como servidor DHCP, e integra el servicio DNS con el de DHCP. Es liviano, estable y extremadamente flexible. Bind es, prácticamente, la mejor elección para redes muy grandes (mayores que un par de cientos de nodos), pero la simplicidad y flexibilidad de dnsmasq lo hacen atractivo para redes pequeñas y medianas.

Windows NT

Para instalar el servicio DNS en Windows NT4: seleccione Panel de Control ➞ Red ➞ Servicios ➞ Agregar ➞ Servidor DNS Microsoft. Inserte el CD de Windows NT4 CD cuando se le indique. Cómo configurar un servidor solo de memoria intermedia (*cache*) en NT se describe en el artículoKnowledge Base 167234. Una cita del artículo:

> "*Simplemente instale DNS y haga correr el Sistema Administrador de Nombres de Dominio (Domain Name System Manager). Dé un clic en DNS en el menú, seleccione Nuevo Servidor, y escriba la dirección IP de su computadora donde ha instalado DNS. Usted ahora tiene un servidor DNS solo de cache.*"

Windows 2000

Para instalar el servicio DNS: Inicio ➞Configuración ➞ Panel de Control ➞ Agregar o Quitar Programas. En Agregar o Quitar Componentes de Windows, seleccione Componentes ➞ Servicios de Red ➞ Detalles ➞

Sistema de Nombres de Dominios (DNS). Luego inicie el DNS MMC (Inicio ➜ Programas ➜ Herramientas Administrativas ➜ DNS) Desde el menú de Acción seleccione "Conectarse a la Computadora..." En la ventana de Selección de Computadora Destino, habilite "La siguiente computadora:" e ingrese el nombre del servidor DNS que usted quiere almacenar. Si hay un . [punto] en el administrador DNS (aparece por omisión), significa que el servidor DNS piensa que es el servidor DNS raíz de Internet. Ciertamente no lo es. Para que todo funcione borre el . [punto].

DNS dividido y un servidor duplicado

El objetivo de un DNS dividido (también conocido como ***horizonte dividido***) es el de presentar una visión diferente de su dominio para el mundo interno y el externo. Hay más de una forma de dividir DNS; pero por razones de seguridad se recomienda que tenga dos servidores de contenidos DNS separados; el interno y el externo (cada uno con bases de datos diferentes).

Dividir el DNS permite a los clientes de la red del campus resolver las direcciones IP para el dominio del campus a direcciones locales RFC1918, mientras que el resto de Internet resuelve los mismos nombres a direcciones IP diferentes. Esto se logra teniendo dos zonas en dos servidores DNS diferentes para el mismo dominio.

Una de las zonas es utilizada para los clientes internos de la red y la otra para los usuarios en Internet. Por ejemplo, en la red siguiente el usuario dentro del campus de Makerere verá *http://www.makerere.ac.ug/* resuelto como 172.16.16.21, mientras que un usuario en otro dominio de Internet lo verá resuelto como 195.171.16.13.

El servidor DNS en el campus, como se ve en el diagrama anterior, tiene un archivo de zona para *makerere.ac.ug* y está configurado como la autoridad para ese dominio. Además, funciona como el servidor DNS cache para el campus de Makerere, y todas las computadoras en el campus están configuradas para utilizarlo como su servidor DNS.

Los registros DNS para el servidor DNS en el campus van a verse así:

```
makerere.ac.ug
www     CNAME   webserver.makerere.ac.ug
ftp     CNAME   ftpserver.makerere.ac.ug
mail    CNAME   exchange.makerere.ac.ug
mailserver      A       172.16.16.21
webserver       A       172.16.16.21
ftpserver       A       172.16.16.21
```

Pero hay otro servidor DNS en Internet que es en realidad la autoridad para el dominio *makerere.ac.ug*. Los registros DNS para esta zona externa van a verse así:

```
makerere.ac.ug
www     A 195.171.16.13
ftp     A 195.171.16.13
mail    A 16.132.33.21
MX mail.makerere.ac.ug
```

El DNS dividido no depende de la utilización de direcciones RFC 1918. Un ISP africano puede, por ejemplo, alojar sitios web en representación de una universidad pero también puede duplicar esos mismos sitios web en Europa. Siempre que los clientes de ese ISP acceden al sitio web, éste toma la dirección IP del ISP africano, y por lo tanto el tráfico permanece en el mismo país. Cuando visitantes de otros países acceden al sitio web, reciben la dirección IP del sitio web duplicado en el servidor en Europa. De esta forma los visitantes internacionales no congestionan la conexión VSAT del ISP cuando visitan el sitio web de la universidad. Esto se está convirtiendo en una solución atractiva, ya que el alojamiento web cerca del backbone de Internet se está haciendo muy económico.

Optimización del enlace a Internet

Como mencionamos anteriormente, se pueden alcanzar rendimientos superiores a 22Mbps mediante la utilización de equipamiento 802.11g estándar para redes inalámbricas. Este valor de ancho de banda probablemente sea al menos un orden de magnitud mayor que la que le ofrece su enlace a Internet, y es capaz de soportar cómodamente muchos usuarios simultáneos de Internet.

Pero si su conexión principal a Internet es a través de un enlace VSAT, se va a encontrar con algunos problemas de desempeño si utiliza los parámetros por omisión de TCP/IP. Optimizando su enlace VSAT, se pueden mejorar significativamente los tiempos de respuesta cuando se accede a hosts de Internet.

Factores TCP/IP en una conexión por satélite

Un VSAT es concebido a menudo como una tubería de datos ***larga y gruesa***. Este término se refiere a los factores que afectan el desempeño de TCP/IP en cualquier red que tenga un ancho de banda relativamente grande, pero mucha latencia. La mayoría de las conexiones a Internet en África y otras partes del mundo en desarrollo son vía VSAT. Por lo tanto, aún si una universidad tiene su conexión a través de un ISP, esta sección puede ser aplicable si la conexión del ISP es a través de VSAT. La alta latencia en las

redes por satélite se debe a la gran distancia del satélite y la velocidad constante de la luz. Esta distancia añade aproximadamente 520 ms al tiempo de ida y retorno de un paquete (RTT –round trip time– *por su sigla en inglés*), comparado con un RTT entre Europa y Estados Unidos de alrededor de 140 ms.

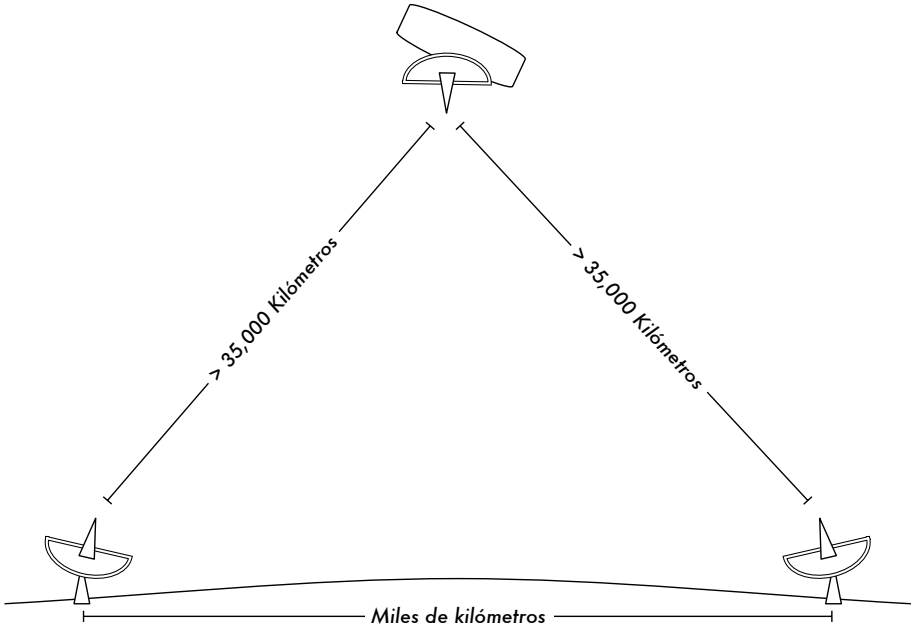


Figura 3.17: Debido a la velocidad de la luz y las largas distancias involucradas, la confirmación de recepción de un paquete ping puede tomar más de 520ms en un enlace VSAT.

Los factores que impactan más significativamente el rendimiento de TCP/IP son tiempos de propagación largos, **grandes productos de ancho de banda por retardo y errores de transmisión**.

Generalmente en una red satelital se deben utilizar sistemas operativos que soportan las implementaciones TCP/IP modernas. Estas implementaciones soportan las extensiones RFC 1323:

- La opción de ***escalado de ventana*** para soportar ventanas TCP de gran tamaño (mayores que 64KB).
- ***Recepción selectiva*** (***SACK*** *por su sigla en inglés*) para permitir una recuperación más rápida de los errores de transmisión.
- Matasellos (*Timestamps*) para calcular los valores de RTT y la expiración del tiempo de retransmisión para el enlace en uso.

Tiempos de ida y vuelta largos (RTT)

Los enlaces por satélite tienen un promedio de RTT de alrededor de 520ms hasta el primer salto. TCP utiliza el mecanismo de comienzo lento al inicio de la conexión para encontrar los parámetros de TCP/IP apropiados para la misma. El tiempo perdido en la etapa de comienzo lento es proporcional al RTT, y para los enlaces por satélite significa que TCP se encuentra en el modo de comienzo lento por más tiempo de lo que debiera. Esto disminuye drásticamente el rendimiento de las conexiones TCP de corta duración. Esto puede verse cuando descargar un sitio web pequeño sorprendentemente toma mucho tiempo, mientras que cuando se transfiere un archivo grande se obtienen velocidades de datos aceptables luego de un rato.

Además cuando se pierden paquetes, TCP entra en la fase de control de congestión y, debido al alto RTT permanece en esta fase por largo tiempo, reduciendo así el rendimiento de las conexiones TCP, sean de larga o corta duración.

Producto ancho de banda-retardo elevado

La cantidad de datos en tránsito en un enlace en un momento dado es el producto del ancho de banda por el RTT. Debido a la gran latencia del enlace satelital, este producto es grande. TCP/IP le permite a los hosts remotos enviar cierta cantidad de datos previamente sin esperar la confirmación (*acknowledgment*). Normalmente en una conexión TCP/IP se requiere una confirmación (ACK) para cada transmisión. Sin embargo el host remoto siempre puede enviar cierta cantidad de datos sin confirmación, lo que es importante para lograr una buena tasa de transferencia en conexiones con productos ancho de banda-retardo de propagación elevados. Esta cantidad de datos es denominada ***tamaño de la ventana TCP***. En las implementaciones TCP/IP modernas el tamaño de la ventana generalmente es de 64KB.

En las redes satelitales, el valor del producto ancho de banda-retardo es importante. Para utilizar el enlace en toda su capacidad, el tamaño de la ventana de la conexión debe ser igual al producto del ancho de banda-retardo. Si el tamaño de ventana máximo permitido es de 64KB, teóricamente el máximo rendimiento que se puede conseguir vía satélite es (tamaño de la ventana) / RTT, o 64KB / 520 ms. Esto da una tasa de transferencia de datos máxima de 123kB/s, correspondiente a 984 kbps, aunque la capacidad del enlace sea mucho mayor.

Cada encabezado de segmento TCP contiene un campo llamado ventana anunciada, que especifica cuantos bytes de datos adicionales está preparado para aceptar el receptor. La ***ventana anunciada*** es el tamaño actual de la memoria de almacenamiento intermedio del receptor. El emisor

no está autorizado a enviar más bytes que la ventana anunciada. Para maximizar el rendimiento, las memorias de almacenamiento intermedio del emisor y el receptor deben ser al menos iguales al producto ancho de banda-retardo. El tamaño de la memoria de almacenamiento intermedio en la mayoría de las implementaciones modernas de TCP/IP tiene un valor máximo de 64KB.

Para soslayar el problema de versiones de TCP/IP que no exceden el tamaño de la ventana de 64KB, se puede utilizar una técnica conocida como suplantación de confirmación (***TCP acknowledgment spoofing***) (vea más adelante Mejora del Rendimiento del Proxy).

Errores de transmisión

En las implementaciones de TCP/IP más viejas, siempre se consideraba que la pérdida de paquetes era causada por la congestión (en lugar de errores de enlace). Cuando esto sucede TCP adopta una defensiva contra la congestión, requiriendo tres confirmaciones duplicadas (ACK), o ejecutando un inicio lento (*slow start*) en el caso de que el tiempo de espera haya expirado.

Debido al alto valor de RTT, una vez que esta fase de control de la congestión ha comenzado, toma un largo rato para que el enlace satelital TCP/IP vuelva al nivel de rendimiento anterior. Por consiguiente, los errores en un enlace satelital tienen un efecto más serio en las prestaciones de TCP que sobre los enlaces de latencia baja. Para solucionar esta limitación, se han desarrollado mecanismos como la ***Confirmación Selectiva*** (***SACK*** por su sigla en inglés). SACK especifica exactamente aquellos paquetes que se han recibido permitiendo que el emisor retransmita solamente aquellos segmentos que se perdieron debido a errores de enlace.

El artículo sobre detalles de implementación de TCP/IP en Windows 2000 afirma:

> "*Windows 2000 introduce soporte para una importante característica de desempeño conocida como Confirmación Selectiva (SACK). SACK es especialmente importante para conexiones que utilizan ventanas TCP de gran tamaño.*"

SACK ha sido una característica estándar desde hace algún tiempo en Linux y BSD. Asegúrese de que tanto su enrutador Internet como el ISP del sitio remoto soporten SACK.

Implicaciones para las universidades

Si un sitio tiene una conexión a Internet de 512 kbps, las configuraciones por omisión de TCP/IP son suficientes, porque una ventana de 64 KB puede cubrir hasta 984 kbps. Pero si la universidad tiene más de 984 Kbps, es probable que en algunos casos no se obtenga todo el ancho de banda disponible del enlace debido a los factores de "tubería de datos larga y gruesa" discutidos anteriormente. Lo que estos factores implican realmente es que impiden que una computadora tome todo el ancho de banda. Esto no es malo durante el día, porque mucha gente está usando el ancho de banda. Pero si por ejemplo, se programan grandes descargas para la noche, el administrador puede querer hacer uso de todo el ancho de banda, y los factores de "tubería de datos larga y gruesa" pueden ser un obstáculo. Esto puede transformarse en algo crítico si una cantidad significativa de su tráfico de red se enruta a través de un túnel único o una conexión VPN hasta el otro extremo del enlace VSAT.

Los administradores pueden considerar tomar algunas medidas para asegurarse de que están aprovechando la totalidad del ancho de banda disponible, afinando las configuraciones de TCP/IP. Si una universidad ha implementado una red donde el tráfico tiene necesariamente que pasar a través de un *proxy* (impuesto por el diseño de red), entonces las únicas computadoras que pueden realizar conexiones directas a Internet serán los servidores *proxy* y de correo electrónico.

Para más información, vea: *http://www.psc.edu/networking/perf_tune.html*.

Proxy que mejora las prestaciones (PEP- Performance enhancing Proxy)

La idea de PEP se describe en la RFC 3135 (vea *http://www.ietf.org/rfc/rfc3135*), y podría ser un servidor Proxy con un disco cache grande que tiene extensiones RFC 1323, entre otras características. Una computadora portátil tiene una sesión TCP con PEP en el ISP. Ese PEP, y el que está en el proveedor de satélite se comunican utilizando diferentes sesiones TCP, inclusive, su propio protocolo privado. El PEP del proveedor de satélite toma los archivos desde el servidor web. De esta forma, la sesión TCP se divide y por lo tanto se evitan las características del enlace que afectan las prestaciones del protocolo (los factores de tubería larga y gruesa), utilizando por ejemplo suplantación de confirmaciones TCP (*TCP ACK spoofing*). Adicionalmente, PEP reactúa como proxy y realiza captura previa (*pre-fetching*) para acelerar todavía más el acceso a la web.

Este sistema puede ser construido desde cero utilizando por ejemplo Squid, o adquiriendo soluciones ofrecidas por varios vendedores.

4

Antenas y Líneas de Transmisión

El transmisor que genera la energía de RF[1] para entregar a la antena generalmente está ubicado a cierta distancia de la misma. El enlace entre ambos es la lí***nea de transmisión de RF***. Su propósito es transportar la energía de RF desde un lugar hacia el otro de la forma más eficiente posible. Del lado del receptor, la antena es responsable de captar las señales de radio desde el aire y pasarlas al receptor con la mínima cantidad de distorsión, para que el radio pueda decodificar la señal. Por estas razones el cable de RF tiene un rol muy importante en los sistemas de radio: debe mantener la integridad de las señales en ambas direcciones.

Existen dos categorías principales de líneas de transmisión: los cables y las guías de ondas. Ambos son muy buenos para transportar de forma eficiente la energía de RF a 2,4GHz.

Cables

En el caso de frecuencias mayores que HF (alta frecuencia, por su sigla en inglés) los cables utilizados son casi exclusivamente los coaxiales (o para abreviar ***coax***, derivado de las palabras del inglés “of common axis” eje en común). Los cables coaxiales tienen un ***conductor*** central recubierto por un material no conductor denominado ***dieléctrico***, o simplemente ***aislante***. El dieléctrico se recubre con una pantalla conductora envolvente a menudo en forma de malla. El material dieléctrico evita una conexión eléctrica entre el conductor central y la pantalla. Finalmente, el coaxial está protegido por un

---

1. Radio Frecuencia. Vea el capítulo dos para una discusión sobre las ondas electromagnéticas.

recubrimiento generalmente de PVC. El conductor interior transporta la señal de RF, y la pantalla evita que la señal de RF sea radiada a la atmósfera, así como impide que posibles señales externas interfieran con la que está siendo transmitida por el cable. Otro hecho interesante es que las señales eléctricas de alta frecuencia siempre viajan a lo largo de la capa exterior del conductor central: cuanto más grande el conductor central, mejor va a ser el flujo de la señal. Esto se denomina “efecto pelicular”.

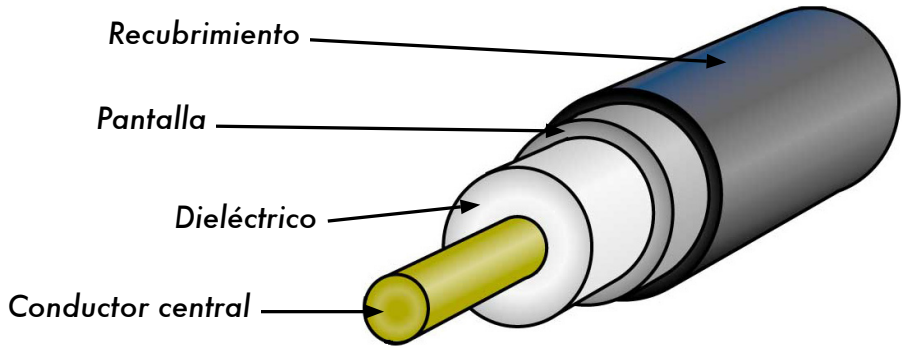


Figura 4.1: Cable coaxial con recubrimiento, pantalla, dieléctrico, y conductor central.

A pesar de que la construcción del cable coaxial es muy buena para contener la señal en el cable, presenta algo de resistencia al flujo eléctrico: a medida que la señal viaja a través del cable disminuye su intensidad. Este debilitamiento es conocido como ***atenuación***, y para las líneas de transmisión se mide en decibeles por metro (***dB/m***). El coeficiente de atenuación es una función de la frecuencia de la señal y la construcción física del cable. Si se incrementa la frecuencia de la señal, también lo hace su atenuación. Obviamente se necesita minimizar la atenuación del cable cuanto más nos sea posible, lo que puede hacerse mediante la utilización de cables muy cortos y/o de buena calidad.

Aquí les brindamos algunos puntos a considerar cuando elegimos un cable para utilizarlo con dispositivos de microondas:

1. “¡Cuanto más corto mejor!” La primer regla cuando instalamos un cable es la de hacerlo lo más corto posible. La pérdida de energía no es lineal, por lo tanto duplicar el largo del cable implica perder mucho más que el doble de energía. En el mismo sentido, si reducimos el largo del cable a la mitad vamos a tener mucho más que el doble de potencia en la antena. La mejor solución es poner el transmisor lo más cerca que podamos de la antena, incluso si esto implica colocarlo en una torre.
2. “¡Cuanto más barato peor!” La segunda regla de oro es que todo el dinero que se invierta en comprar un cable de ***buena calidad*** es un

buen negocio. Los cables baratos están pensados para ser utilizados con bajas frecuencias como VHF. Las microondas requieren de los cables de mejor calidad que haya disponibles. Todas las demás opciones no serán más que cargas fantasma para la radio[2].

3. Evite usar RG-58: fue pensado para redes Ethernet, CB o radio de VHF, no para microondas.

4. Evite usar RG-213: fue diseñado para CB y radio de HF. En este caso el diámetro del cable no implica alta calidad o baja atenuación.

5. Siempre que sea posible utilice cables ***Heliax*** (también denominados "Foam" –espuma–) para conectar el transmisor a la antena. Cuando no haya cable Heliax utilice los mejores cables LMR que pueda encontrar. Los cables Heliax tienen un centro conductor sólido o tubular con un conductor externo sólido y corrugado que lo hace flexible. Estos cables pueden construirse de dos formas, utilizando aire o espuma para el dieléctrico. Los cables Heliax con dieléctrico de aire son los más caros y garantizan la menor pérdida, pero son muy difíciles de manipular. Los de espuma tienen una pérdida ligeramente mayor, pero son más económicos y sencillos de instalar. Se requiere un procedimiento especial cuando soldamos conectores para mantener la espuma dieléctrica seca e intacta. La marca de cables coaxiales Times Microwave LMR los produce en varios diámetros, y funcionan bien en frecuencias de microondas. Los cables LMR-400 y LMR-600 se utilizan comúnmente como alternativas al Heliax.

6. Siempre que sea posible utilice cables que ya tengan los conectores, y que hayan sido probados en un laboratorio apropiado. La instalación de los conectores en el cable es una tarea delicada y se hace difícil realizarla adecuadamente aún teniendo las herramientas necesarias. A menos que tenga acceso al equipamiento que pueda verificar un cable hecho por usted mismo (como un analizador de espectro y un generador de señal, o un reflectómetro de dominio temporal), solucionar los problemas de una red que utiliza cables hechos en casa puede ser difícil.

7. No maltrate su línea de transmisión. Nunca camine sobre el cable, no lo doble demasiado, no intente desenchufar un conector halando directamente el cable. Todos esos comportamientos pueden cambiar las características mecánicas del cable y por lo tanto su impedancia, provocar un cortocircuito entre el conductor interno y la pantalla, o incluso romper la línea. Rastrear y reconocer este tipo de problemas no es tarea fácil, y esto puede llevar a un comportamiento impredecible del radioenlace.

---

2. Una carga fantasma disipa energía de RF sin radiarla. Imagínese un sumidero de calor pero a radio frecuencias.

Guías de Ondas

Por encima de los 2 GHz, la longitud de onda es lo suficientemente corta como para permitir una transferencia de energía práctica y eficiente por di-ferentes medios. Una guía de onda es un tubo conductor a través del cual se transmite la energía en la forma de ondas electromagnéticas. El tubo actúa como un contenedor que confina las ondas en un espacio cerrado. El efecto de Faraday atrapa cualquier campo electromagnético fuera de la guía. Los campos electromagnéticos son propagados a través de la guía de onda por medio de reflexiones en sus paredes internas, que son consideradas perfectamente conductoras. La intensidad de los campos es máxima en el centro a lo largo de la dimensión X, y debe disminuir a cero al llegar a las paredes, porque la existencia de cualquier campo paralelo a las mismas en su superficie causaría una corriente infinita en un conductor perfecto. Las guías de ondas, por supuesto, no pueden transportar la RF de esta forma.

En la siguiente figura pueden verse las dimensiones X, Y, y Z de una guía de ondas rectangular:

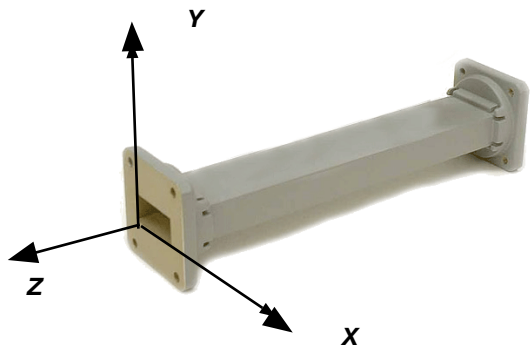


Figura 4.2: Las dimensiones X, Y, y Z de una guía de onda rectangular.

Hay un infinito número de formas en las cuales los campos eléctricos y magnéticos pueden organizarse en una guía de onda a frecuencias por encima de la frecuencia de corte. Cada una de esas configuraciones del campo se denomina ***modo***. Los modos pueden separarse en dos grupos generales. Uno de ellos es el Transversal Magnético (***TM*** *por su sigla en inglés*), donde el campo magnético es siempre transversal a la dirección de propagación, pero existe un componente del campo eléctrico en la dirección de propagación. El otro es el Transversal Eléctrico (***TE*** *por su sigla en inglés*), en el que el campo eléctrico es siempre transversal, pero existe un componente del campo magnético en la dirección de propagación.

El modo de propagación se identifica por dos letras seguido por dos subíndices numéricos. Por ejemplo el TE_{10}, TM_{11}, etc. El número de modos

posibles se incrementa con la frecuencia para un tamaño dado de guía, y existe un modo, llamado ***modo dominante***, que es el único que se puede transmitir a la frecuencia más baja que soporta la guía de onda. En una guía rectangular, la dimensión crítica es la X. Esta dimensión debe ser mayor que 0.5 λ a la frecuencia más baja que va a ser transmitida. En la práctica, generalmente la dimensión Y es igual a 0.5 X para evitar la posibilidad de que se opere en otro modo que no sea el modo dominante. Se pueden utilizar otras formas además de la rectangular, la más importante es la de tubo circular. Para éste se aplican las mismas consideraciones que para el rectangular. La dimensión de la longitud de onda para las guías rectangulares y circulares se presenta en la siguiente tabla, donde X es el ancho de la guía rectangular y r es el radio de la guía circular. Todos los valores se refieren al modo dominante.

Tipo de guía	Rectangular	Circular
Longitud de onda de corte	**2X**	**3,41r**
Longitud de onda máxima transmitida con poca atenuación	**1,6X**	**3,2r**
Longitud de onda mínima antes de que se transmita el modo siguiente	**1,1X**	**2,8r**

La energía puede introducirse o extraerse de una guía de onda por medio de un campo eléctrico o magnético. Generalmente la transferencia de energía se da a través de una línea coaxial. Dos métodos posibles para acoplar una línea coaxial son utilizar el conductor interno de la línea, o a través de una espira. Se puede introducir una sonda, constituida por una pequeña extensión del conductor interno de la línea coaxial, orientada paralelamente a las líneas de campo eléctrico. También se puede colocar un lazo o espira que encierre algunas de las líneas de campo magnético. El punto en el cual obtenemos el acoplamiento máximo depende del modo de propagación en la guía o en la cavidad. El acoplamiento es máximo cuando el dispositivo de acoplamiento está en el campo más intenso.

Si una guía de onda se deja abierta en uno de sus lados, puede radiar energía (es decir, puede ser usada como una antena en lugar de línea de transmisión). Esta radiación puede ser aumentada acampanando la guía de onda para formar una antena de bocina piramidal (*horn*). Más adelante en este capítulo veremos un ejemplo de una antena hecha con una guía de onda para WiFi.

Tipo de Cable	Núcleo	Dieléctrico	Pantalla	Recubrimiento
RG-58	0,9 mm	2,95 mm	3,8 mm	4,95 mm
RG-213	2,26 mm	7,24 mm	8,64 mm	10,29 mm
LMR-400	2,74 mm	7,24 mm	8,13 mm	10,29 mm
3/8” LDF	3,1 mm	8,12 mm	9,7 mm	11 mm

En esta tabla se contrastan los tamaños de varios tipos de líneas de transmisión. Trate de elegir el mejor cable de acuerdo con sus posibilidades, de forma de tener la menor atenuación posible a la frecuencia que vaya a utilizar para su enlace inalámbrico.

Conectores y adaptadores

Por medio de los conectores el cable puede ser conectado a otro cable o a un componente de la cadena de RF. Hay una gran cantidad de adaptadores y conectores diseñados para concordar con diferentes tamaños y tipos de líneas coaxiales. Describiremos algunos de los más populares.

Los ***conectores BNC*** fueron desarrollados a fines de los 40. La sigla BNC significa Bayoneta, Neill-Concelman, por los apellidos de quienes los inventaron: Paul Neill y Carl Concelman. El tipo BNC es un conector miniatura de conexión y desconexión rápida. Tiene dos postes de bayoneta en el conector hembra, y el apareamiento se logra con sólo un cuarto de vuelta de la tuerca de acoplamiento. Los conectores BNC son ideales para la terminación de cables coaxiales miniatura o subminiatura (RG-58 a RG-179, RG-316, etc.). Tienen un desempeño aceptable hasta unos pocos cientos de MHz. Son los que se encuentran más comúnmente en los equipamientos de prueba y en los cables coaxiales Ethernet 10base2.

Los ***conectores TNC*** también fueron inventados por Neill y Concelman, y son una versión roscada de los BNC. Debido a que proveen una mejor interconexión, funcionan bien hasta unos 12GHz. Su sigla TNC se debe a su sigla en inglés (Neill-Concelman con Rosca, por Threaded Neill-Concelman).

Los conectores ***Tipo N*** (también por Neill, aunque algunas veces atribuidos a “Navy”) fueron desarrollados originalmente durante la Segunda Guerra Mundial. Se pueden utilizar a más de 18 Ghz y se utilizan comúnmente en aplicaciones de microondas. Se fabrican para la mayoría de tipos de cable. Las uniones del cable al conector macho o hembra son impermeables, y proveen un agarre efectivo.

SMA es un acrónimo de Sub Miniatura versión A, y fue desarrollado en los 60. Los conectores SMA son unidades subminiatura de precisión que proveen excelentes prestaciones eléctricas hasta más de 18 GHz. Estos conectores de alto desempeño son de tamaño compacto y tienen una extraordinaria durabilidad.

Los ***SMB*** cuyo nombre deriva de Sub Miniatura B, son el segundo diseño subminiatura. Constituyen una versión más pequeña de los SMA con un acoplamiento a presión y funcionan hasta los 4 GHz.

Los conectores ***MCX*** se introdujeron en los 80. Aunque utilizan contactos internos y aislantes idénticos a los SMB, el diámetro exterior de la clavija es 30% más pequeño que la del SMB. Esta serie provee a los diseñadores de opciones cuando el espacio físico es limitado. MCX tiene una capacidad de banda ancha de 6GHz con un diseño de conector a presión.

Además de estos conectores estándar, la mayoría de los dispositivos WiFi utilizan una variedad de conectores patentados. A menudo son simplemente conectores de microondas estándar con las partes centrales del conductor invertidas o con roscas a contramano. Estos conectores especiales a menudo se acoplan a los otros elementos del sistema de microondas utilizando un cable delgado y corto llamado latiguillo, en inglés ***pigtail*** (***cola de cerdo***) que convierte el conector que no es estándar en uno más robusto y disponible comúnmente. Entre estos conectores especiales tenemos:

RP-TNC. Es un conector TNC con el género invertido. Éstos son los que trae el WRT54G de Linksys.

U.FL (también conocido como ***MHF***). El U.FL es un conector patentado realizado por Hirose, y el MHF es un conector mecánicamente equivalente. Probablemente es el conector de microondas más pequeño utilizado ampliamente en la actualidad. El U.FL / MHF se utiliza para conectar una tarjeta de radio mini-PCI a una antena o a un conector más grande (como un N o un TNC).

La serie ***MMCX***, también denominada MicroMate, es una de las líneas de conectores de RF más pequeñas desarrolladas en los 90. MMCX es una serie de conectores micro-miniatura con un mecanismo de bloqueo a presión que permite una rotación de 360 grados otorgándole gran flexibilidad. Los conectores MMCX se encuentran generalmente en tarjetas de radio PCMCIA, como las fabricadas por Senao y Cisco.

Los conectores ***MC-Card*** son más pequeños y más frágiles que los MMCX. Tiene un conector externo con ranuras que se quiebra fácilmente luego de unas pocas interconexiones. Generalmente están en el equipamiento Lucent / Orinoco / Avaya.

Los adaptadores coaxiales (o simplemente *adaptadores*), son conectores cortos usados para unir dos cables o dos componentes que no se pueden conectar directamente. Los adaptadores pueden ser utilizados para interconectar dispositivos o cables de diferentes tipos. Por ejemplo, un adaptador puede ser utilizado para conectar un conector SMA a un BNC. También pueden servir para unir dos conectores del mismo tipo que no pueden ha-cerlo directamente por su género (macho-macho/hembra-hembra). Por ejemplo un adaptador muy útil es el que permite unir dos conectores machos Tipo N, que tiene dos conectores hembra en ambos extremos.

Figura 4.3: Adaptador N hembra de barrilito

Elección del conector apropiado

1. "Una cuestión de género." Casi todos los conectores tienen un género bien definido que consiste en una clavija (el extremo "macho") o una toma (el extremo "hembra"). Generalmente los cables tienen conectores macho en ambos extremos y los dispositivos de RF (por ej. transmisores y antenas) tienen conectores hembra. Los acopladores direccionales y dispositivos de medición de línea pueden tener tanto conectores macho como hembra. Asegúrese de que cada conector macho en su sistema coincide con uno hembra.
2. "¡Menos es mejor!" Intente minimizar el número de conectores y adaptadores en la cadena de RF. Cada conector introduce alguna pérdida adicional (¡hasta unos pocos dB por cada conexión, dependiendo del conector!).
3. "!Compre, no lo haga usted mismo!" Como mencionamos anteriormente, siempre que pueda es mejor que compre cables que ya estén terminados con los conectores que usted necesite. Soldar los conectores no es una tarea sencilla, y en el caso de conectores pequeños como los U.FL y MMCX hacerlo bien es casi imposible. Hasta la conectorización de cables de foam (espuma) es ardua.
4. No use BNC para frecuencias de 2,4GHz o más altas. Utilice los conectores tipo N (o SMA, SMB, TNC, etc.).
5. Los conectores de microondas son componentes de precisión y se pueden dañar fácilmente si se manipulan mal. Como regla general, debe

rotar la manga exterior para apretar el conector, dejando el resto del conector (y el cable) estacionario. Si se tuercen otras partes del conector mientras estamos ajustándolo o aflojándolo es muy posible que las mismas se rompan.

6. Nunca pise, ni deje caer los conectores en el piso cuando desconecte los cables (esto sucede más a menudo de lo que usted se imagina, especialmente cuando trabajamos en un mástil sobre un techo).
7. Nunca utilice herramientas como las pinzas para apretar los conectores. Hágalo siempre con las manos. Cuando trabaje en exteriores recuerde que los metales se expanden a altas temperaturas y reducen su tamaño a baja temperatura: un conector muy apretado puede dilatarse en el verano o quebrarse en el invierno.

Antenas y diagramas (patrones) de radiación

Las antenas son un componente muy importante de los sistemas de comunicación. Por definición, una antena es un dispositivo utilizado para transformar una señal de RF que viaja en un conductor, en una onda electromagnética en el espacio abierto. Las antenas exhiben una propiedad conocida como ***reciprocidad***, lo cual significa que una antena va a mantener las mismas características sin importar si está transmitiendo o recibiendo. La mayoría de las antenas son dispositivos resonantes, que operan eficientemente sólo en una banda de frecuencia relativamente baja. Una antena debe ser sintonizada en la misma banda que el sistema de radio al que está conectada, para no afectar la recepción y transmisión. Cuando se alimenta la antena con una señal, emitirá radiación distribuida en el espacio de cierta forma. La representación gráfica de la distribución relativa de la potencia radiada en el espacio se llama ***diagrama*** o ***patrón de radiación***.

Glosario de términos de las antenas

Antes de hablar de antenas específicas, hay algunos términos que deben ser definidos y explicados:

Impedancia de entrada

Para una transferencia de energía eficiente, la ***impedancia*** del radio, la antena, y el cable de transmisión que las conecta debe ser la misma. Las antenas y sus líneas de transmisión generalmente están diseñadas para una impedancia de 50Ω. Si la antena tiene una impedancia diferente a 50Ω, hay una desadaptación, y se necesita un circuito de acoplamiento de impedancia. Cuando alguno de estos componentes no tiene la misma impedancia, la eficiencia de transmisión se ve afectada.

Pérdida de retorno

La ***pérdida de retorno*** es otra forma de expresar la desadaptación. Es una medida logarítmica expresada en dB, que compara la potencia reflejada por la antena con la potencia con la cual la alimentamos desde la línea de transmisión. La relación entre SWR (Standing Wave Ratio –Razón de Onda Estacionaria–) y la pérdida de retorno es la siguiente:

$$\text{Pérdida de Retorno (en dB)} = 20\log_{10} \frac{SWR}{SWR-1}$$

Aunque siempre existe cierta cantidad de energía que va a ser reflejada hacia el sistema, una pérdida de retorno elevada implica un funcionamiento inaceptable de la antena.

Ancho de banda

El ***ancho de banda*** de una antena se refiere al rango de frecuencias en el cual puede operar de forma correcta. Este ancho de banda es el número de hercios (Hz) para los cuales la antena va a tener una Razón de Onda Estacionaria (SWR) menor que 2:1.

El ancho de banda también puede ser descrito en términos de porcentaje de la frecuencia central de la banda.

$$\text{Ancho de Banda} = 100 \times \frac{F_H - F_L}{F_C}$$

...donde F_H es la frecuencia más alta en la banda, F_L es la frecuencia más baja, y F_C es la frecuencia central.

De esta forma, el ancho de banda porcentual es constante respecto a la frecuencia. Si fuera expresado en unidades absolutas, variaría dependiendo de la frecuencia central. Los diferentes tipos de antenas tienen variadas limitaciones de ancho de banda.

Directividad y Ganancia

La ***Directividad*** es la habilidad de una antena de transmitir enfocando la energía en una dirección particular, o de recibirla de una dirección particular. Si un enlace inalámbrico utiliza locaciones fijas para ambos extremos, es posible utilizar la directividad de la antena para concentrar la transmisión de la radiación en la dirección deseada. En una aplicación móvil donde la

antena no está fijada a un punto, es imposible predecir dónde va a estar, y por lo tanto la antena debería radiar en todas las direcciones del plano horizontal. En estas aplicaciones se utiliza una antena omnidireccional.

La ganancia no es una cantidad que pueda ser definida en términos de una cantidad física como vatios u ohmios, es un cociente sin dimensión. La ganancia se expresa en referencia a una antena estándar. Las dos referencias más comunes son la antena ***isotrópica*** y l***a antena dipolo resonante de media longitud de onda***. La antena isotrópica irradia en todas direcciones con la misma intensidad. En la realidad esta antena no existe, pero provee un patrón teórico útil y sencillo con el que comparar las antenas reales. Cualquier antena real va a irradiar más energía en algunas direcciones que en otras. Puesto que las antenas no crean energía, la potencia total irradiada es la misma que una antena isotrópica. Toda energía adicional radiada en las direcciones favorecidas es compensada por menos energía radiada en las otras direcciones.

La ganancia de una antena en una dirección dada es la cantidad de energía radiada en esa dirección comparada con la energía que podría radiar una antena isotrópica en la misma dirección alimentada con la misma potencia. Generalmente estamos interesados en la ganancia máxima, que es aquella en la dirección hacia la cual la antena está radiando la mayor potencia. Una ganancia de antena de 3dB comparada con una isotrópica debería ser escrita como **3dBi**. El dipolo resonante de media longitud de onda puede ser un estándar útil a la hora de compararlo con otras antenas a una frecuencia, o sobre una banda estrecha de frecuencias. Para comparar el dipolo con una antena sobre un rango de frecuencias se requiere de un número de dipolos de diferentes longitudes. La ganancia de una antena comparada con un dipolo debería ser escrita como **3dBd**.

El método para medir la ganancia mediante la comparación de la antena bajo prueba con una antena estándar conocida, de ganancia calibrada, es conocido como técnica de ***transferencia de*** ganancia. Otro método para medir la ganancia es el de las tres antenas, donde la potencia transmitida y recibida en las terminales de las antenas es medida entre tres antenas elegidas arbitrariamente a una distancia fija conocida.

Diagramas o Patrones de Radiación

Los ***patrones o diagramas de radiación*** describen la intensidad relativa del campo radiado en varias direcciones desde la antena a una distancia constante. El patrón de radiación es también de recepción, porque describe las propiedades de recepción de la antena. El patrón de radiación es tri-dimensional, pero generalmente las mediciones de los mismos son una porción bi-dimensional del patrón, en el plano horizontal o vertical. Estas mediciones son presentadas en coordenadas ***rectangulares*** o en

coordenadas ***polares***. La siguiente figura muestra el diagrama de radiación en coordenadas rectangulares de una antena Yagi de diez elementos. El detalle es bueno pero se hace difícil visualizar el comportamiento de la antena en diferentes direcciones.

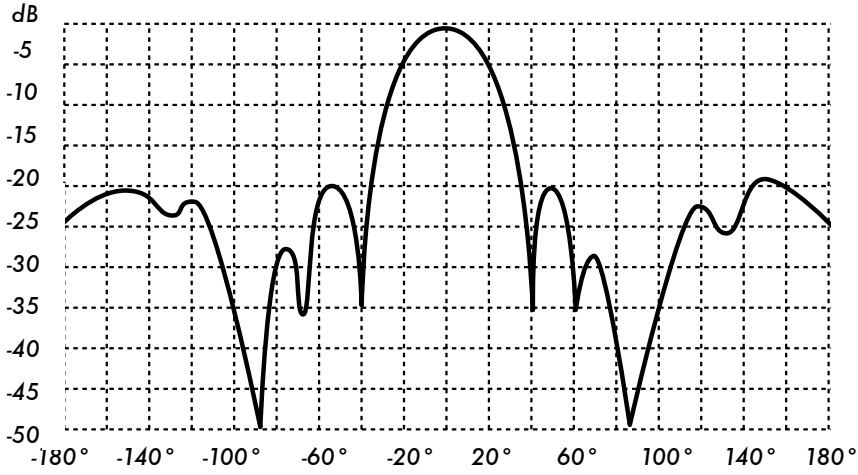


Figura 4.4: Diagrama de radiación de una antena Yagi en coordenadas rectangulares

En los sistemas de coordenadas polares, los puntos se obtienen por una proyección a lo largo de un eje que rota (radio) en la intersección con uno de varios círculos concéntricos. El siguiente es un diagrama de radiación en coordenadas polares de la misma antena Yagi de diez elementos.

Los sistemas de coordenadas polares pueden dividirse en dos clases: ***lineales*** y ***logarítmicos***. En el sistema de coordenadas polares lineal, los círculos concéntricos están uniformemente espaciados y graduados. La retícula resultante puede ser utilizada para preparar un diagrama lineal de la potencia contenida en la señal. Para facilitar la comparación, los círculos concéntricos equiespaciados pueden reemplazarse por círculos ubicados adecuadamente, representando la respuesta en decibeles, con 0 dB correspondiendo al círculo más externo. En este tipo de gráficas los lóbulos menores se suprimen. Los lóbulos con picos menores de 15 dB debajo del lóbulo principal desaparecen por su pequeño tamaño. Esta retícula mejora la presentación de las características de antenas con alta directividad y lóbulos menores pequeños. En un sistema de coordenadas lineales, se puede trazar el voltaje de la señal en lugar de la potencia, En este caso también, se enfatiza la directividad y desenfatizan los lóbulos menores, pero no en el mismo grado que en la retícula lineal de potencia.

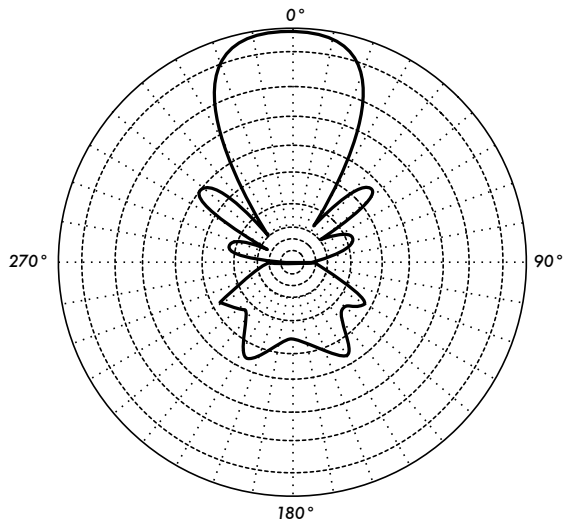


Figura 4.5: Diagrama polar lineal de la misma antena Yagi.

En el sistema de coordenadas polares logarítmico, las líneas concéntricas de la retícula son espaciadas periódicamente de acuerdo con el logaritmo de voltaje de la señal. Se pueden usar diferentes valores para la constante logarítmica de periodicidad, y esta elección va a tener un efecto en la apariencia de los diagramas trazados. Generalmente se utiliza la referencia 0 dB para el extremo externo de la gráfica. Con este tipo de retícula, los lóbulos que están 30 o 40 dB por debajo del lóbulo principal aún pueden distinguirse. El espacio entre los puntos a 0 dB y a -3 dB es mayor que el espacio entre -20 dB y -23 dB, el cual es mayor que el espacio entre -50 dB y -53 dB. Por lo tanto el espacio corresponde a la significancia relativa de dichos cambios en el desempeño de la antena.

Una escala logarítmica modificada enfatiza la forma del haz mayor mientras comprime los lóbulos laterales de muy bajo nivel (<30 dB) hacia el centro del patrón.

Hay dos tipos de diagramas de radiación: los ***absolutos*** y los ***relativos***. Los diagramas de radiación absolutos se presentan en unidades absolutas de potencia o intensidad de campo. Los diagramas de radiación relativos se referencian a unidades relativas de potencia o intensidad de campo. La mayoría de las mediciones de los diagramas de radiación son relativas a la antena isotrópica, y el método de transferencia de ganancia es utilizado para establecer la ganancia absoluta de la antena.

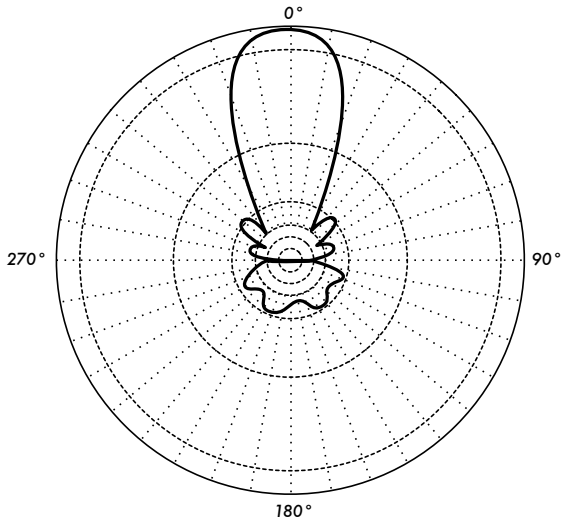


Figura 4.6: Trazado polar logarítmico

El patrón de radiación en la región cercana a la antena no es el mismo que el patrón a largas distancias. El término *campo cercano* se refiere al patrón del campo que existe cerca de la antena, mientras que el término *campo lejano* refiere a los diagramas del campo a largas distancias. El campo alejado también es denominado campo de radiación, y generalmente es el que más interesa. Normalmente el punto de interés es la potencia radiada, y por lo tanto los diagramas de la antena son medidos en la región del campo alejado. Para las medidas necesarias para confeccionar los diagramas es importante elegir una distancia suficientemente grande para estar en el campo lejano, más allá del campo cercano. La distancia mínima depende de las dimensiones de la antena con relación a la longitud de onda. La fórmula aceptada para esta distancia es:

$$r_{min} = \frac{2d^2}{\lambda}$$

…donde r_{min} es la distancia mínima desde la antena, d es la dimensión más grande de la antena, y λ es la longitud de onda.

Ancho del haz

El ***ancho del haz*** de una antena usualmente se entiende como ancho del haz a mitad de potencia. Se encuentra el pico de intensidad de radiación, luego se localizan los puntos de ambos lados de pico que representan la mitad de la potencia de intensidad del pico. La distancia angular entre los puntos de la mitad de la potencia se define como el ancho del haz. La mitad

de la potencia expresada en decibeles es de -3dB, por lo tanto algunas veces el ancho del haz a mitad de potencia es referido como el ancho del haz a 3dB. Generalmente se consideran tanto el ancho de haz vertical como horizontal.

Suponiendo que la mayor parte de la potencia radiada no se dispersa en lóbulos laterales, entonces la ganancia directiva es inversamente proporcional al ancho del haz: cuando el ancho del haz decrece, la ganancia directiva se incrementa.

Lóbulos laterales

Ninguna antena es capaz de radiar toda la energía en una dirección preferida. Inevitablemente, una parte de ella es radiada en otras direcciones. Esos picos más pequeños son denominados ***lóbulos laterales***, especificados comúnmente en dB por debajo del lóbulo principal.

Nulos

En los diagramas de radiación de una antena, una zona **nula** es aquella en la cual la potencia efectivamente radiada está en un mínimo. Un nulo a menudo tiene un ángulo de directividad estrecho en comparación al haz principal. Los nulos son útiles para varios propósitos tales como la supresión de señales interferentes en una dirección dada.

Polarización

La ***polarización*** se define como la orientación del campo eléctrico de una onda electromagnética. En general la polarización se describe por una elipse. Dos casos especiales de la polarización elíptica son la ***polarización lineal*** y la ***polarización circular***. La polarización inicial de una onda de radio es determinada por la antena.

Con la polarización lineal, el vector del campo eléctrico se mantiene en el mismo plano todo el tiempo. El campo eléctrico puede dejar la antena en una orientación vertical, horizontal, o en algún ángulo entre los dos. La radiación ***polarizada verticalmente*** se ve ligeramente menos afectada por las reflexiones en el camino de transmisión. Las antenas omnidireccionales siempre tienen una polarización vertical. Con la ***polarización horizontal***, tales reflexiones causan variaciones en la intensidad de la señal recibida. Las antenas horizontales tienen menos probabilidad de captar interferencias generadas por el hombre, normalmente polarizadas verticalmente.

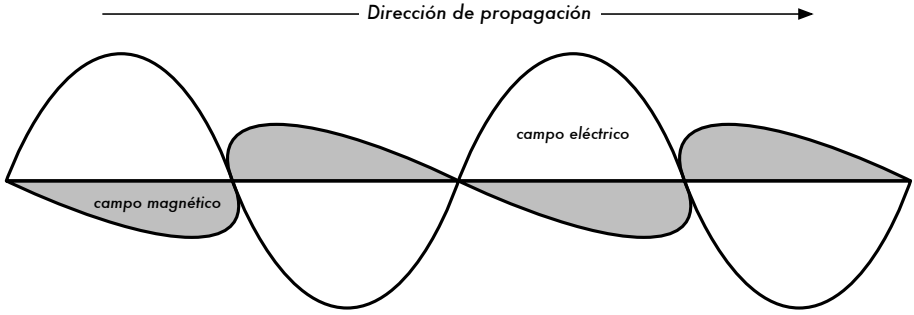


Figura 4.7: La onda senoidal eléctrica se mueve perpendicular a la onda magnética en la dirección de la propagación.

En la polarización circular el vector del campo eléctrico aparece rotando con un movimiento circular en la dirección de la propagación, haciendo una vuel-ta completa para cada ciclo de RF. Esta rotación puede ser hacia la derecha o hacia la izquierda. La elección de la polarización es una de las elecciones de diseño disponibles para el diseñador del sistema de RF.

Desadaptación de polarización

Para transferir la máxima potencia entre una antena transmisora y una receptora, ambas antenas deben tener la misma orientación espacial, el mismo sentido de polarización y el mismo coeficiente axial.

Cuando las antenas no están alineadas o no tienen la misma polarización, habrá una reducción en la transferencia de potencia entre ambas antenas. Esto va a reducir la eficiencia global y las prestaciones del sistema.

Cuando las antenas transmisora y receptora están polarizadas linealmente, una desalineación física entre ellas va a resultar en una pérdida por desadaptación de polarización, que puede ser determinada utilizando la siguiente fórmula:

$$\text{Pérdida (dB)} = 20 \log_{10} (\cos \theta)$$

...donde θ es la diferencia en el ángulo de alineación entre las dos antenas. Para 15° la pérdida es de aproximadamente 0.3dB, para 30° perdemos 1.25dB, para 45° perdemos 3dB y para 90° tenemos una pérdida infinita.

Resumiendo, cuanto más grande la desadaptación de polarización entre una antena transmisora y una receptora, más grande la pérdida aparente. En el mundo real, la pérdida debida a una desadaptación en polarización de 90° es bastante grande pero no infinita. Algunas antenas como las Yagis, o las antenas de lata, pueden rotarse 90° de forma sencilla para corresponder con la polarización del otro extremo del enlace. La polarización puede

a-provecharse en un enlace punto a punto. Use una herramienta de monitoreo para observar la interferencia desde redes adyacentes, y rote una antena hasta que se minimice la señal recibida. Luego instale su enlace utilizando la polarización en la que había medido interferencia mínima en ambos extremos. Esta técnica puede ser utilizada a veces para construir enlaces estables, aún en medio ambientes con mucho ruido RF.

Relación de ganancia adelante/atrás

A menudo es útil comparar la ***Relación de ganancia adelante/atrás*** de las antenas direccionales. Este es el cociente de la directividad máxima de una antena con relación a su directividad en la dirección opuesta. Por ejemplo, cuando se traza el patrón de radiación en una escala relativa en dB, la relación de ganancia adelante/atrás es la diferencia en dB entre el nivel de radiación máxima en la dirección delantera y el nivel de radiación a 180 grados.

Este número no tiene sentido para un antena omnidireccional, pero brinda una idea de la cantidad de potencia dirigida hacia adelante en una antena muy direccional.

Tipos de Antenas

Una clasificación de las antenas puede basarse en:

- **Frecuencia y tamaño.** Las antenas utilizadas para HF son diferentes de las antenas utilizadas para VHF, las cuales son diferentes de las antenas para microondas. La longitud de onda es diferente a diferentes frecuencias, por lo tanto las antenas deben ser diferentes en tamaño para radiar señales a la correcta longitud de onda. En este caso estamos particularmente interesados en las antenas que trabajan en el rango de microondas, especialmente en las frecuencias de los 2,4 GHz y 5 GHz. A los 2400 MHz la longitud de onda es 12,5cm, mientras que a los 5000 MHz es de 6cm.
- **Directividad.** Las antenas pueden ser omnidireccionales, sectoriales o directivas. Las ***antenas omnidireccionales*** irradian aproximadamente con la misma intensidad en todas las direcciones del plano horizontal, es decir en los 360°. Los tipos más populares de antenas omnidireccionales son los dipolos y las de plano de tierra. Las ***antenas sectoriales*** irradian principalmente en un área específica. El haz puede ser tan amplio como 180 grados, o tan angosto como 60 grados. Las ***direccionales*** o ***directivas*** son antenas en las cuales el ancho del haz es mucho más angosto que en las antenas sectoriales. Tienen la ganancia más alta y por lo tanto se utilizan para enlaces a larga distancia. Tipos de antenas

directivas son las Yagi, las biquad, las de bocina, las helicoidales, las antenas patch, los platos parabólicos, y muchas otras.

- **Construcción física.** Las antenas pueden construirse de muchas formas diferentes, desde simples mallas, platos parabólicos, o latas de café.

Cuando consideramos antenas adecuadas para el uso en WLAN de 2,4GHz, se pueden utilizar otras clasificaciones:

- **Aplicaciones.** Los puntos de acceso tienden a hacer redes punto a multipunto, mientras que los enlaces remotos son punto a punto. Esto implica diferentes tipos de antenas para el propósito. Los nodos utilizados para accesos multipunto pueden utilizar tanto antenas omni, las cuales irradian igualmente en todas direcciones, como antenas sectoriales que se enfocan en un área limitada. En el caso de los enlaces punto a punto, las antenas se usan para conectar dos lugares. Las antenas directivas son la elección principal para esta aplicación.

Ahora le presentamos una breve lista de tipos comunes de antenas para la frecuencia de 2,4GHz, con una corta descripción de la información básica acerca de sus características.

Antena de 1/4 de longitud con plano de tierra

Esta antena es muy simple en su construcción y es útil para las comunicaciones cuando el tamaño, el costo y la facilidad de construcción son importantes. Esta antena se diseñó para transmitir una señal polarizada verticalmente. Consiste en un elemento de 1⁄4 de longitud onda como medio dipolo, y tres o cuatro elementos de un 1⁄4 de longitud de onda inclinados de 30 a 45 grados hacia abajo.

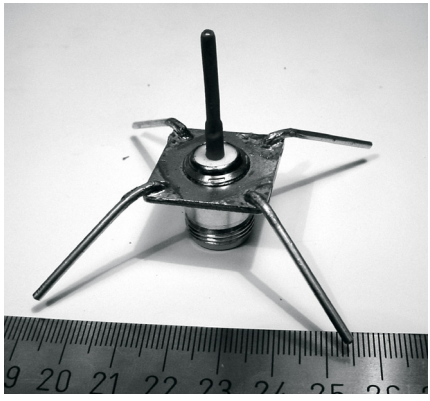


Figura 4.8: Antena de un cuarto de longitud de onda con plano de tierra.

Este conjunto de elementos, denominados radiales, constituyen el plano de tierra. Esta es una antena simple y efectiva que puede capturar una señal con igual facilidad en todas las direcciones. Para incrementar la ganancia, la señal puede hacerse más achatada para concentrar la radiación en el plano horizontal. El ancho del haz vertical representa el grado de achatamiento en el foco. Esto es útil en una situación de punto a multipunto, si todas las otras antenas se encuentran a la misma altura. La ganancia de esta antena está en el orden de 2 a 4 dBi.

Antena Yagi

La antena Yagi básica consiste en un cierto número de elementos rectos que miden cada uno aproximadamente la mitad de la longitud de onda. El elemento excitado o activo de una Yagi es el equivalente a una antena dipolo de media onda con alimentación central. En paralelo al elemento activo, y a una distancia que va de 0,2 a 0,5 longitudes de onda en cada lado, hay varillas rectas o alambres llamados reflectores y directores, o simplemente elementos pasivos. Un reflector se ubica detrás del elemento activo y es ligeramente más largo que media longitud de onda; un director se coloca en frente del elemento activo y es ligeramente más corto que media longitud de onda. Una Yagi típica tiene un reflector y uno o más directores. La antena propaga la energía del campo electromagnético en la dirección que va desde el elemento activo hacia los directores, y es más sensible a la energía electromagnética entrante en esta misma dirección. Cuantos más directores tiene una Yagi, mayor la ganancia. Cuantos más directores se agreguen a una Yagi, la misma va a ser más larga. La siguiente es una foto de una antena Yagi con 6 directores y 1 reflector.

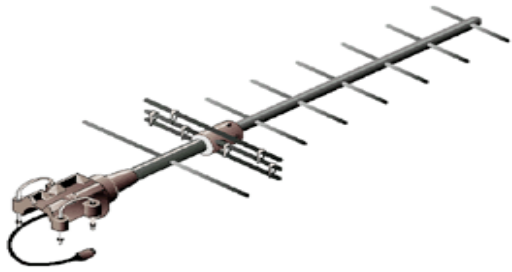


Figura 4.9: Una antena Yagi.

Las antenas Yagi son utilizadas principalmente por los enlaces Punto a Punto; tienen una ganancia desde 10 a 20 dBi y un ancho de haz horizontal de 10 a 20 grados.

Bocina

El nombre de la antena bocina deriva de su apariencia característica acampanada o de cuerno. La porción acampanada puede ser cuadrada, rectangular, cilíndrica o cónica. La dirección de máxima radiación se corresponde con el eje de la campana. Se puede alimentar sencillamente con una guía de onda, pero también puede hacerse con un cable coaxial y la transición apropiada. Las antenas bocina se utilizan comúnmente como el elemento activo en una antena de plato. La antena bocina se coloca hacia el centro del plato reflector. El uso de una bocina, en lugar de una antena dipolo o cualquier otro tipo de antena en el punto focal del plato, minimiza la pérdida de energía alrededor de los bordes del plato reflector. A 2,4GHz, una antena bocina simple hecha con una lata tiene una ganancia del orden de 10 a 15 dBi.

Figura 4.10: Antena bocina hecha con una lata de comida.

Plato Parabólico

Las antenas basadas en reflectores parabólicos son el tipo más común de antenas directivas cuando se requiere una gran ganancia. La ventaja principal es que pueden construirse para tener una ganancia y una directividad tan grande como sea requerido. La desventaja principal es que los platos grandes son difíciles de montar y están predispuestos a sufrir los efectos del viento.

Los platos de más de un metro generalmente están hechos de material sólido. Frecuentemente se utiliza el aluminio por una ventaja de peso, su durabilidad y sus buenas características eléctricas. El efecto del viento se incrementa rápidamente con el tamaño del plato y se convierte en un problema severo. A menudo se utilizan platos que tienen una superficie reflectora constituida por una malla abierta. Éstos tienen un a relación de ganancia adelante/atrás más pobre pero son seguros de utilizar y sencillos de construir. Materiales como el cobre, aluminio, bronce (latón), acero galvanizado y hierro son apropiados para una malla.

Figura 4.11: Una antena plato sólida.

BiQuad

La antena BiQuad es fácil de armar y ofrece buena directividad y ganancia para las comunicaciones punto a punto. Consiste en dos cuadrados iguales de 1⁄4 de longitud de onda como elemento de radiación y un plato metálico o malla como reflector. Esta antena tiene un ancho del haz de aproximadamente 70 grados y una ganancia en el orden de 10-12 dBi. Puede ser utilizada como una antena única o como un alimentador para un Plato Parabólico. Para encontrar la polarización, debemos observar el frente de la antena, con los cuadrados colocados lado a lado; en esa posición la polarización es vertical.

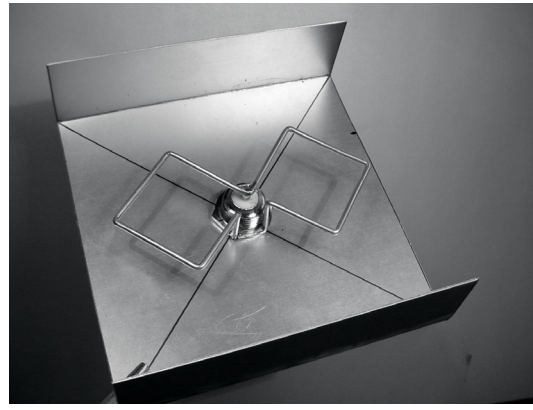


Figura 4.12: Antena BiQuad.

Otras Antenas

Existen muchos otros tipos de antenas y se crean nuevas siguiendo los avances tecnológicos.

- Antenas de Sector o Sectoriales: son muy usadas en la infraestructura de telefonía celular y en general se construyen agregando una cara reflectora a uno o más dipolos alimentados en fase. Su ancho de haz horizontal puede ser tan amplio como 180 grados, o tan angosto como 60 grados, mientras que el vertical generalmente es mucho más angosto. Las antenas compuestas pueden armarse con varios sectores para cubrir un rango horizontal más ancho (antena multisectorial).
- Antenas Panel o Patch: son paneles planos sólidos utilizados para cobertura interior, con una ganancia de hasta 20 dB.

Teoría de los Reflectores

La propiedad básica de un reflector parabólico perfecto es que convierte una onda esférica irradiada desde un punto fuente ubicado en el foco, en una onda plana. Recíprocamente, toda la energía recibida en el plato desde una fuente distante se refleja en un punto único en el foco del plato. La posición del foco, o distancia focal, está dada por:

$$f = \frac{D^2}{16 \times c}$$

...donde **D** es el diámetro del plato y **c** es la profundidad de la parábola en su centro.

El tamaño del plato es el factor más importante ya que determina la ganancia máxima que puede lograrse a una frecuencia dada y el ancho de haz resultante. La ganancia y el ancho de haz obtenidos son dados por:

$$\text{Ganancia} = \frac{(\pi \times D)^2}{\lambda^2} \times n$$

$$\text{Ancho del haz} = \frac{70\ \lambda}{D}$$

...donde **D** es el diámetro del plato y **n** es la eficiencia. La eficiencia es determinada principalmente por la efectividad de la iluminación del plato por el alimentador, pero también por otros factores. Cada vez que el diámetro del plato se duplica, la ganancia se cuadruplica o incrementa en seis dB. Si ambas estaciones duplican el tamaño de sus platos, la intensidad de la señal

puede incrementarse en 12 dB, un aumento muy sustancial. Se puede estimar una eficiencia del 50% en una antena hecha a mano.

El coeficiente f / D (longitud focal/diámetro del plato) es el factor fundamental que define el diseño del alimentador para un plato. El coeficiente está directamente relacionado con el ancho del haz del alimentador necesario para iluminar el plato de forma efectiva. Dos platos del mismo diámetro pero con diferentes longitudes focales requieren diferentes diseños del alimentador si ambos van a ser iluminados eficientemente. El valor de 0,25 corresponde al plato común de plano focal en el cual el foco está en el mismo plano que el aro del plato.

Amplificadores

Como mencionamos anteriormente las antenas no crean potencia. Ellas simplemente dirigen toda la potencia disponible en un patrón particular. Por medio de la utilización de un ***amplificador de potencia***, usted puede usar energía DC para aumentar su señal disponible. Un amplificador se conecta entre el transmisor de radio y la antena, y tiene un cable adicional que se conecta a una fuente de energía. Existen amplificadores para trabajar a 2,4GHz, que agregan varios vatios de potencia a su transmisión. Estos dispositivos detectan cuando el radio está transmitiendo, y empiezan a amplifican la señal. Cuando la transmisión termina se apagan otra vez. En recepción también agregan amplificación a la señal antes de enviarla al radio.

Desafortunadamente, el simple hecho de agregar amplificadores no va a resolver mágicamente todos los problemas de nuestra red. No discutimos acerca de los amplificadores de potencia en profundidad en este libro, porque hay varios inconvenientes en el uso de los mismos:

- **Son caros.** Los amplificadores deben trabajar a relativamente grandes anchos de banda a 2400MHz, y deben tener una conmutación lo suficientemente rápida para trabajar con aplicaciones Wi-Fi. Estos amplificadores existen pero tienden a costar varios cientos de dólares por unidad.
- **Va a necesitar por lo menos dos.** Mientras que las antenas proveen una ganancia recíproca que beneficia a ambos lados de la conexión, los amplificadores trabajan mejor amplificando una señal transmitida. Si se agrega sólo un amplificador en un extremo del enlace con una ganancia de antena insuficiente, ésta probablemente va a ser escuchada, pero usted no va a ser capaz de escuchar el otro extremo.
- **No proveen direccionalidad adicional.** Agregar ganancia a una antena provee beneficios de ganancia y direccionalidad a ambos extremos del

enlace. No solo mejoran la cantidad disponible de señal sino que tienden a rechazar ruido desde otras direcciones. Los amplificadores amplían ciegamente tanto las señales deseadas como las interferencias, y pueden hacer que los problemas de interferencia sean peores.

- L**os amplificadores generan ruido para otros usuarios de la banda.** Debido al incremento de su potencia de salida, usted está creando una alta fuente de ruido para otros usuarios en la banda sin licenciamiento. Esto puede no ser un gran tema en áreas rurales, pero puede causar grandes problemas en áreas pobladas. Por el contrario, agregar ganancia de antena va a mejorar su enlace y puede bajar el nivel de ruido para sus vecinos.
- **Utilizar amplificadores puede ser ilegal. Cada país impone límites de potencia para el espectro sin licenciamiento.** Agregar una antena a una señal altamente amplificada, probablemente provoque que se excedan los límites legales.

La utilización de amplificadores a menudo se compara con el vecino desconsiderado que quiere escuchar la radio desde afuera de su casa y por eso sube el volumen al máximo. Hasta llega a "mejorar" la recepción poniendo sus parlantes fuera de la ventana. Si bien ahora es capaz de escuchar la radio, la escuchan también todos los del edificio. Este método sirve cuando existe un solo usuario, ¿pero qué sucede cuando todos los vecinos deciden hacer lo mismo con sus radios? Utilizar amplificadores para un enlace inalámbrico causa aproximadamente el mismo efecto a 2400MHz. Su enlace puede "funcionar mejor" por el momento, pero va a tener problemas cuando otros usuarios de la banda también decidan utilizar amplificadores.

Si utiliza antenas de gran ganancia en lugar de amplificadores, se evita todos estos problemas. El costo de las antenas es mucho menor que el de los amplificadores, y puede mejorar un enlace simplemente cambiando la antena en uno de los extremos. Tener radios más sensibles y cables de buena calidad también ayuda de forma significativa en enlaces a larga distancia. Estas técnicas no causan problemas a otros usuarios de la banda, y por lo tanto las recomendamos mucho más que agregar amplificadores.

Diseños prácticos de antenas

El costo de antenas de 2400MHz ha bajado drásticamente desde la introducción del estándar 802.11b. Los diseños innovadores utilizan partes simples y pocos materiales para conseguir imponentes ganancias con pocos pasos de fabricación. Desafortunadamente, la disponibilidad de buenas antenas aún es limitada en muchas zonas del mundo, e importarlas puede

ser muy caro. Si bien diseñar una antena puede ser un proceso complejo y propenso a errores, construir antenas con componentes disponibles localmente es muy sencillo, y puede ser muy divertido. Presentamos cuatro prácticos diseños de antena que pueden armarse con muy poco dinero.

USB *dongle* como iluminador de un plato

Posiblemente el diseño de antena más simple es el uso de una parábola para dirigir la salida de un dispositivo inalámbrico USB (conocido en el ámbito de las redes como ***USB dongle***). Poniendo la antena dipolo interna presente en el dispositivo inalámbrico USB en el foco del plato parabólico, se puede obtener una ganancia significativa sin la necesidad de soldar o abrir el dispositivo inalámbrico en sí mismo. Muchos tipos de platos parabólicos pueden funcionar, incluyendo platos satelitales, antenas de televisión, y hasta implementos metálicos de la cocina (como un wok, una tapa redonda o un tamiz). Como un extra, se utilizan cables USB –baratos, libres de pérdidas de RF–, eliminando la necesidad de adquirir los cables coaxiales o heliax que son mucho más caros.

Para construir una parabólica con USB *dongle*, va a necesitar encontrar la orientación y la ubicación del dipolo dentro del *dongle*. La mayoría de los dispositivos orientan al dipolo para que el mismo esté paralelo con el borde corto del *dongle*, pero algunos montan el dipolo perpendicular al borde. Puede abrir el *dongle* y verificarlo por usted mismo, o simplemente probar el *dongle* en ambas posiciones y ver cuál provee más ganancia.

Para probar la antena, diríjala a un punto de acceso alejado varios metros, y conecte el *dongle* USB a una computadora portátil. Use el driver original del *dongle* o una herramienta como Netstumbler (vea el capítulo seis), y observe la intensidad de la señal recibida del punto de acceso. Ahora, mueva lentamente el *dongle* en relación con la parabólica y vaya mirando el medidor de intensidad de señal. Debe ver un aumento significativo en la ganancia (de 20 dB o más) cuando encuentre la posición adecuada. El dipolo generalmente se ubica de 3 a 5 centímetros de la base del disco, pero esto va a depender de la forma de la parábola. Busque varias posiciones mientras mira su medidor de intensidad de señal hasta que encuentre la posición óptima.

Una vez que encontró la mejor ubicación, fije el *dongle* en su lugar de forma segura. Va a tener que impermeabilizar el *dongle* y el cable si la antena se utiliza en exteriores. Use un compuesto de silicona o un segmento de tubo de PVC para proteger del clima los elementos electrónicos. Muchos diseños e ideas de parabólicas con alimentadores USB están documentados en línea en *http://www.usbwifi.orcon.net.nz/*.

Omni colineal

Esta antena es muy sencilla de armar; se requiere de un pedazo de alambre, un conector tipo N y una placa metálica cuadrada. Puede usarse para una cobertura punto a multipunto de corta distancia, en interiores o exteriores. La placa tiene un agujero perforado en el medio para colocar el chasis del conector tipo N el cual se atornilla en el lugar. El alambre se suelda en la clavija del conector N y tiene espiras para desfasar los elementos activos. Se pueden hacer dos versiones de la antena: una con dos elementos activos y dos espiras, y otra con cuatro elementos activos y cuatro espiras. Para la antena más corta, la ganancia ronda los 5dBi, mientras que la más larga, con cuatro elementos, va a tener de 7 a 9 dBi de ganancia. Solo vamos a describir cómo construir la antena larga.

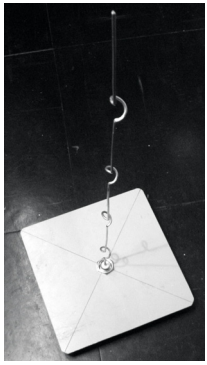


Figura 4.13: La antena omni colinear completa

Lista de componentes

- Un conector tipo N hembra de rosca
- 50 cm de alambre de bronce o de cobre de 2 mm de diámetro
- Una placa metálica cuadrada de 10x10 cm o más grande

Figura 4.14: Placa de aluminio de 10 cm x 10 cm.

Herramientas requeridas

- Regla
- Pinzas
- Lima
- Estaño y soldador
- Taladro con un juego de mechas para metal (incluyendo una mecha de 1,5 cm. de diámetro)
- Un pedazo de tubo, o una mecha con un diámetro de 1 cm.
- Prensa o abrazadera
- Martillo
- Llave inglesa

Construcción

1. Enderece el alambre utilizando la prensa.

Figura 4.15: Deje el alambre tan recto como le sea posible.

2. Con un marcador, dibuje una línea a 2,5 cm comenzando desde uno de los extremos del alambre. En esa línea doble el alambre a 90 grados con la ayuda de la prensa y el martillo.

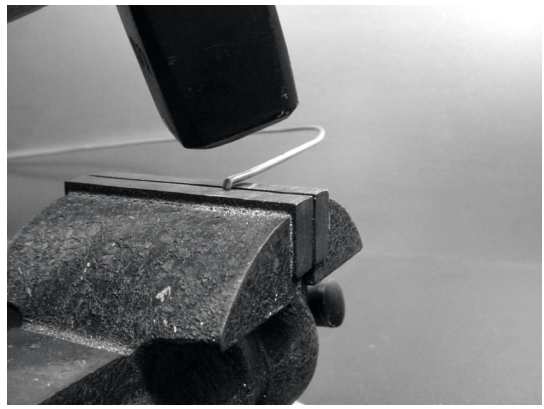


Figura 4.16: Golpee con delicadeza el alambre para hacer una curva cerrada.

3. Dibuje otra línea a una distancia de 3,6 cm desde la curva anterior. Utilice la prensa y el martillo, doble otra vez el alambre en esta segunda línea a 90 grados, en la dirección opuesta a la primera curva pero en el mismo plano. El alambre debe verse como una “Z”.

Figura 4.17: Doblar el alambre en forma de “Z”.

4. Vamos a retorcer la porción “Z” del alambre para hacer un anillo de 1 cm de diámetro. Para esto, vamos a utilizar el tubo o la mecha y curvamos el alambre a su alrededor, con la ayuda de la prensa y de las pinzas.

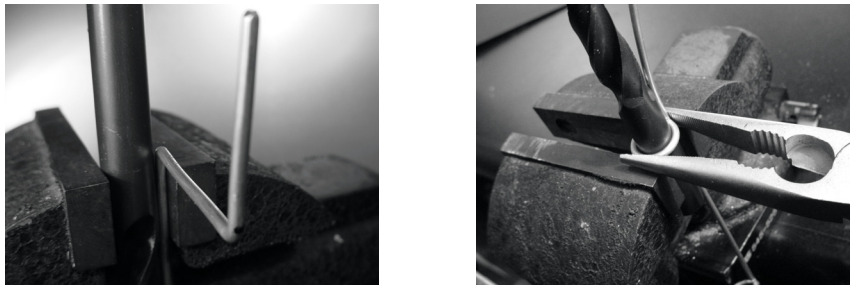


Figura 4.18: Curvar el alambre alrededor de un tubo para hacer un anillo.

El anillo va a verse así:

Figura 4.19: El anillo completo.

5. Debe hacer un segundo anillo a una distancia de 7,8 cm desde el primero. Ambos anillos deben tener la misma dirección de giro y deben ubicarse alineados del mismo lado del alambre. Haga un tercer y cuarto anillo siguiendo el mismo procedimiento, y a la misma distancia de 7,8 cm cada uno del otro. Corte el último elemento activo a una distancia de 8,0 cm desde el cuarto anillo.

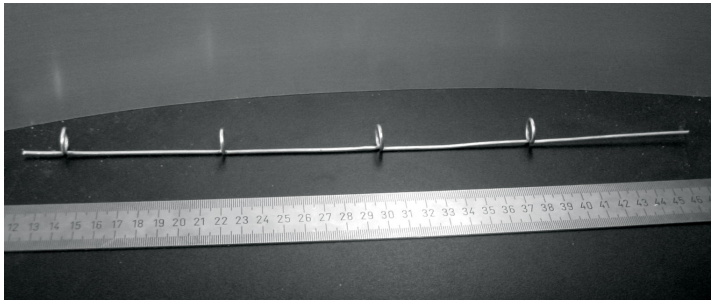


Figura 4.20: Intente mantenerlo lo más recto posible.

Si los anillos fueron hechos correctamente, ahora debe ser posible insertar un tubo a través de todos ellos como se muestra en la imagen.

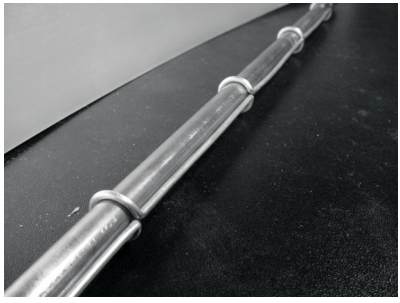


Figura 4.21: Insertar un tubo puede ayudar a enderezar el alambre.

6. Con un marcador y una regla, dibuje las diagonales en la placa metálica para encontrar su centro. Con una mecha pequeña, haga un agujero piloto en el centro de la placa. Incremente el diámetro del agujero utilizando mechas de mayor diámetro.

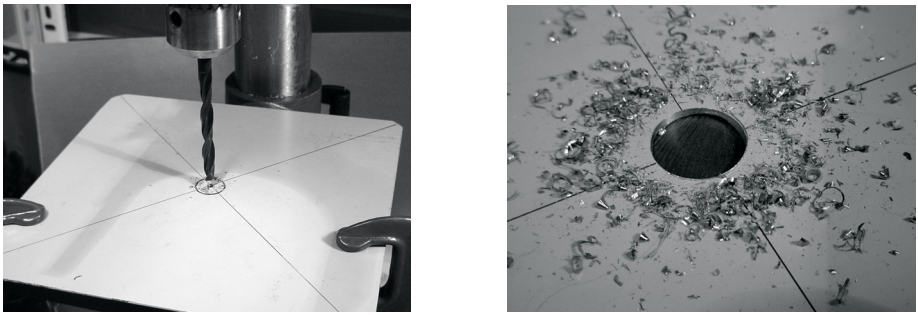


Figura 4.22: Taladrar el agujero en la placa de metal.

El conector N debe encajar exactamente en la perforación. Si es necesario use una lima.

Figura 4.23: El conector N debe encajar exactamente en la perforación.

7. Para tener una impedancia de antena de 50 Ohms, es importante que la superficie visible del aislante interno del conector (el área blanca alrededor de la clavija central) esté al mismo nivel que la superficie de la placa. Por esta razón, debe cortar 0,5 cm de un tubo de cobre con un diámetro externo de 2 cm, y colocarlo entre el conector y la placa.

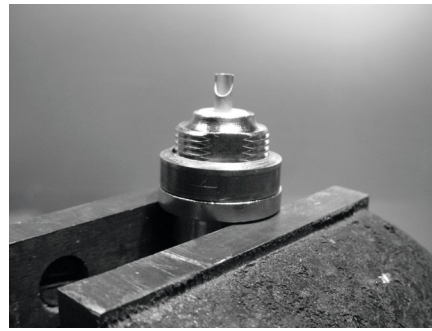


Figura 4.24: Agregar un tubo de cobre espaciador ayuda a obtener la impedancia de la antena de 50 Ohms.

8. Atornille la tuerca al conector para fijarlo firmemente en la placa utilizando la llave inglesa.

Figura 4.25: Asegure el conector N firmemente a la placa

9. Pula con la lima el lado del alambre que tiene 2,5 cm de largo desde el primer anillo. Cubra de estaño aproximadamente 0,5 cm en el extremo pulido ayudándose con la prensa.

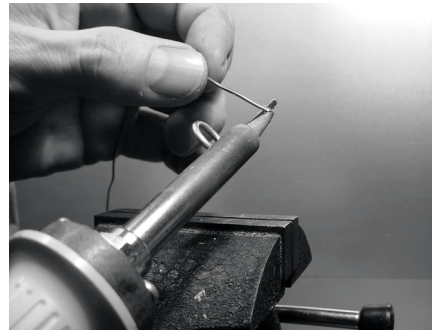


Figura 4.26: Agregue una pequeña capa de estaño al extremo del alambre para "estañearla" antes de soldarlo.

10. Con el soldador, “estañee” la clavija del conector. Mantenga el alambre en posición vertical con las pinzas y suelde el lado “con estaño” en la clavija. El primer anillo debe estar a 3,0 cm de la placa

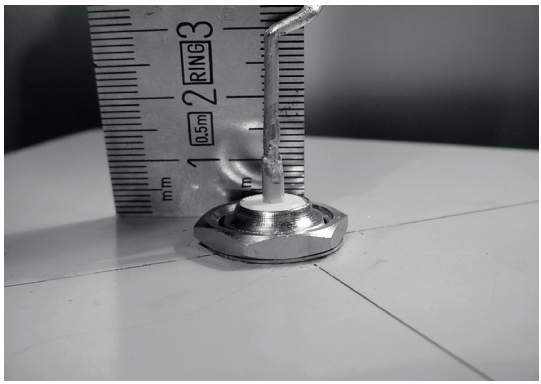


Figura 4.27: El primer anillo debe comenzar a 3,0 cm desde la superficie de la placa

11. Ahora vamos a estirar los anillos extendiendo el largo total del alambre. Usando la prensa y las pinzas estire el alambre hasta que el largo final de cada anillo sea de 2,0 cm.

Figura 4.28: Estirar los anillos. Sea muy cuidadoso y trate de no raspar la superficie del alambre con las pinzas.

12. Repita el mismo procedimiento para los otros tres anillos, llevando su longitud hasta 2,0 cm.

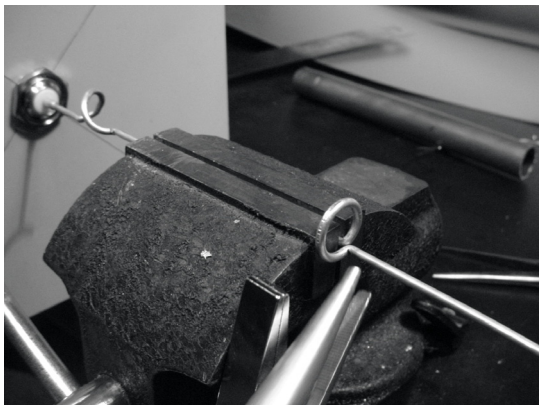


Figura 4.29: Repita el procedimiento de ajuste para todos los anillos restantes.

13. Al terminar, la antena debe medir 42,5 cm desde la placa hasta la punta.

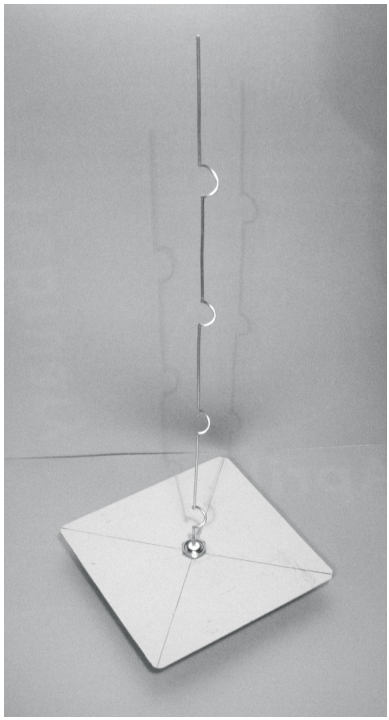


Figura 4.30: La antena terminada debe medir 42,5 cm. desde la placa hasta el final del alambre.

14. Si tiene un Analizador de Espectro con un Generador de Barrido y un Acoplador Direccional, puede chequear la curva de la potencia reflejada de la antena. La imagen que sigue muestra el despliegue del Analizador de Espectro.

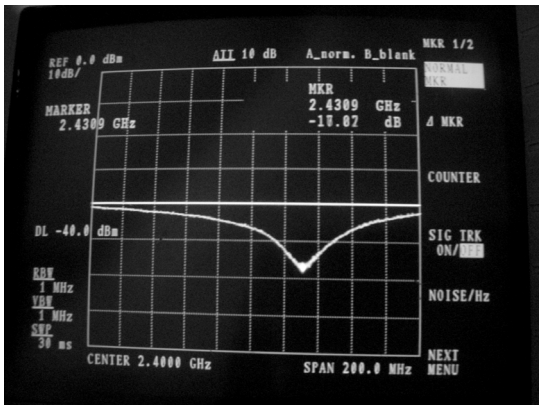


Figura 4.31: Un trazado del espectro de la potencia reflejada por la antena omnicolinear.

Si quiere utilizar esta antena en exteriores, va a necesitar impermeabilizarla. Un método simple es encerrar toda la antena en un tubo de PVC cerrado con tapas. Abra una perforación abajo para la línea de transmisión y selle la antena con silicona o pegamento.

Antena de lata o de guía-onda

Esta antena algunas veces llamada Cantenna, utiliza una lata como guía de onda y un cable corto soldado a un conector N como sonda para la transición del cable coaxial a la guía de onda. Puede construirse fácilmente al precio del conector únicamente, reciclando una lata de comida o de jugo. Es una antena direccional, útil para enlaces punto a punto de corta a media distancia. También puede utilizarse como alimentador para un plato o una malla parabólica.

No todas las latas son buenas para construir una antena porque existen algunas limitaciones en cuanto a la dimensión:

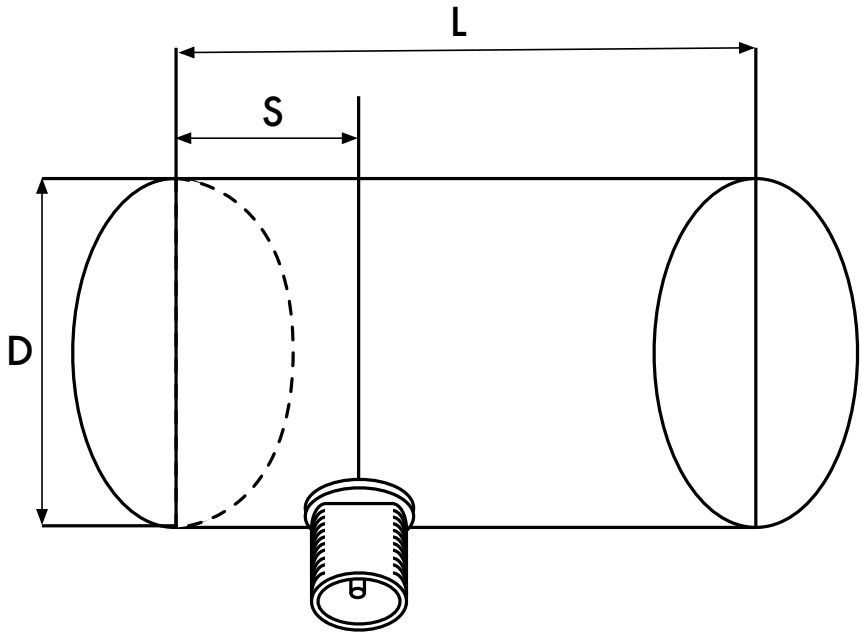


Figura 4.32: Limitaciones de dimensión en la antena guía-onda.

1. Los valores aceptables para el diámetro D del alimentador están entre 0,60 y 0,75 de longitud de onda en el aire a la frecuencia designada. A 2440 MHz la longitud de onda λ es de 12,2 cm, por lo tanto, el diámetro de la lata debe estar en el rango de 7,3 a 9,2 cm.
2. El largo L de la lata debería ser preferiblemente de al menos 0,75 λ_G, donde λ_G es la longitud de onda dentro de la guía y está dada por:

$$\lambda_G = \frac{\lambda}{\text{sqrt}(1 - (\lambda / 1.706D)^2)}$$

Cuando D sea = 7,3 cm, necesitamos una lata de al menos 56,4 cm, mientras que para D = 9,2 cm la lata debería ser de al menos 14,8 cm. Generalmente cuanto más chico el diámetro, más larga debe ser la lata. Por ejemplo, vamos a usar latas de aceite que tienen un diámetro de 8,3 cm y una altura de aproximadamente 21 cm.

3. El elemento activo para la transición del cable coaxial a la guía de onda debe posicionarse a una distancia S desde el fondo de la lata, dada por:

$$S = 0.25\ \lambda_G$$

Su largo debe ser de 0,25 λ, el cual a 2440 MHz corresponde a 3,05 cm.

La ganancia para esta antena va a estar en el orden de 10 a 14 dBi, con un ancho de haz de alrededor de 60 grados.

Figura 4.33: La antena guía-onda terminada.

Lista de componentes

- Un conector tipo N hembra atornillable
- 4 cm de alambre de bronce o de cobre de 2 mm de diámetro
- Una lata de aceite de 8,3 cm de diámetro y 21 cm. de largo

Figura 4.34: Componentes necesarios para la antena de lata.

Herramientas requeridas

- Abrelatas
- Regla
- Pinzas
- Lima
- Soldador
- Estaño
- Taladro con un juego de mechas para metal (con una mecha de 1,5 cm de diámetro)
- Prensa o abrazadera
- Llave inglesa
- Martillo
- Perforadora / Sacabocados

Construcción

1. Con el abrelatas quite cuidadosamente la parte superior de la lata.

Figura 4.35: Tenga cuidado con las puntas afiladas de los bordes al abrir la lata.

El disco circular tiene puntas muy afiladas. ¡Sea cuidadoso al manejarla! Vacíe la lata y lávela con jabón. Si la lata contenía ananás, galletitas, u otras cosas sabrosas, tenga la bondad de servir la comida a un amigo.

2. Con la regla, mida 6,2 cm desde el fondo de la lata y dibuje un punto. Tenga cuidado de medir desde el lado interior del fondo. Utilice un punzón (o una mecha pequeña o un destornillador Phillips) y un martillo

para marcar el punto. Esto hace que sea más sencillo taladrar el agujero de forma precisa. Asegúrese de no deformar la lata insertando un pequeño bloque de madera u otro objeto dentro de la lata antes de golpearla.

Figura 4.36: Marque el agujero antes de taladrar.

3. Con una mecha pequeña del taladro, haga un agujero en la posición previamente marcada. Incremente el diámetro del mismo utilizando mechas con un diámetro cada vez mayor. El conector N debe encajar exactamente en la perforación. Use la lima para alisar el borde del agujero y para remover la pintura que lo rodea para asegurar un mejor contacto eléctrico con el conector.

Figura 4.37: Taladre cuidadosamente un agujero piloto, luego use una mecha más grande para terminar el trabajo.

4. Alise con la lima uno de los extremos del alambre. Cubra con estaño el alambre alrededor de 0,5 cm en el mismo extremo ayudándose con la prensa.

Figura 4.38: Estañe el extremo del alambre antes de soldarlo.

5. Con el soldador, suelde la clavija del conector. Mantenga el alambre en posición vertical con las pinzas, suelde el lado estañado en el agujero de la clavija

Figura 4.39: Suelde el alambre a la copa dorada en el conector N.

6. Inserte una arandela y atornille suavemente la tuerca en el conector. Recorte el alambre a 3,05 cm medidos desde la base de la tuerca.

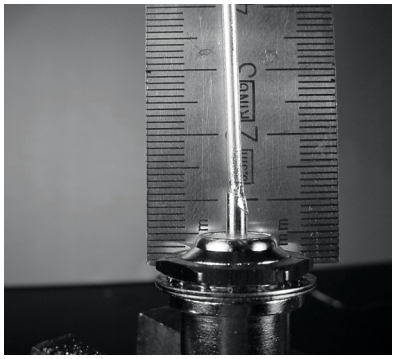


Figura 4.40: El largo del alambre es crucial.

7. Destornille la tuerca del conector, dejando la arandela en el lugar. Inserte el conector en el agujero de la lata. Atornille la tuerca al conector desde el interior de la lata.

Figura 4.41: Arme la antena.

8. Utilice las pinzas o la llave inglesa para ajustar firmemente la tuerca al conector. ¡Ha terminado!

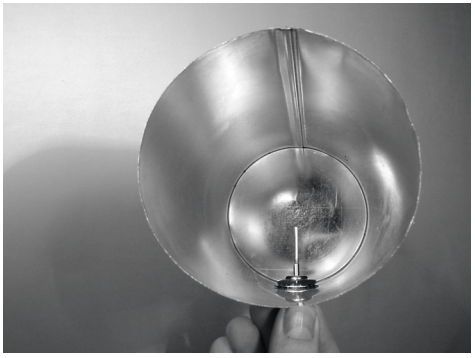


Figura 4.42: Su antena guía-onda terminada

Al igual que los otros diseños de antenas, debe hacer una cubierta a prueba de agua para la antena si quiere usarla en exteriores. El PVC funciona bien para la antena de lata. Coloque toda la antena en un tubo grande de PVC, y selle los extremos con tapas y pegamento. Va a tener que hacer una perforación en un lado del tubo en el lado de la lata para pasar el conector N con la línea de transmisión.

La antena de lata como alimentador de plato

Al igual que con la parabólica con *dongle* USB, se puede utilizar el diseño antena de lata como un alimentador para obtener una ganancia significativamente mayor. Monte la antena de lata en la parabólica con el lado abierto de la lata enfocando al centro del plato. Use la técnica descrita en el ejemplo de la antena *dongle* USB (observar cómo cambia la intensidad de la señal variando la posición del iluminador) para encontrar la ubicación óptima de la lata para el plato que está usando.

Con el uso de una antena de lata bien construida en una parabólica afinada correctamente, se puede lograr una ganancia global de la antena de 30dBi o más. Al incrementar el tamaño de la parabólica, se aumenta la ganancia y la directividad de la antena. Con parábolas muy grandes, usted puede obtener una ganancia mucho más grande.

Por ejemplo, en 2005, un equipo de estudiantes estableció exitosamente un enlace desde Nevada a Utah en los Estados Unidos. ¡El enlace cruzaba una distancia de más de 200 kilómetros! Estos entusiastas del mundo inalámbrico usaron platos de satélite de 3,5 metros para establecer un enlace 802.11b que corría a 11Mbps, sin utilizar un amplificador. Los detalles acerca de este logro pueden encontrarse en *http://www.wifi-shootout.com/*

El 13 de abril de 2006, un equipo de la Fundación EsLaRed (Ermanno Pietrosemoli y Javier Triviño), y del ICTP (Carlo Fonda) lograron transferir archivos con tecnología Wi-Fi a una distancia de 279 km usando dos enrutadores Linksys WRT54 con firmware de código abierto. Se usaron antenas satelitales recicladas, a la frecuencia de 2.412 MHz, sin emplear amplificadores. La experiencia se realizó en Venezuela, entre el Pico del Águila, a 4.100m, y el cerro El Baúl, a 125 m de altura. Detalles en *http://www.wilac.net/*

NEC2

El ***NEC2***, nombrado así por ***Numerical Electromagnetics Code***, es un paquete de modelación de antenas gratuito. NEC2 le permite construir un modelo de antena en 3D, y luego analiza la respuesta electromagnética de la misma. Fue desarrollado hace más de diez años y ha sido compilado para correr en diferentes sistemas de computadoras. NEC2 es

particularmente efectivo para analizar modelos basados en configuraciones de alambres, pero también tiene ciertas facilidades para modelar superficies planas.

El diseño de la antena se describe en un archivo de texto, y luego se construye el modelo utilizando esa descripción textual. Una antena descrita en NEC2 está dada en dos partes: su ***estructura*** y una secuencia de ***controles***. La estructura es simplemente una descripción numérica de dónde se localizan las diferentes partes de la antena y cómo están conectados los alambres. Los controles le dicen a NEC dónde está conectada la fuente de RF. Una vez definidos, se modela la antena transmisora. Debido al teorema de reciprocidad el patrón de ganancia de transmisión es el mismo que el de recepción, por lo tanto modelar las características de transmisión es suficiente para comprender el comportamiento de la antena en su totalidad.

Se debe especificar una frecuencia o rango de frecuencias de la señal de RF. El siguiente elemento importante son las características del terreno. La conductividad de la tierra varia mucho de lugar a lugar, pero en muchos casos juega un rol vital en determinar el patrón de ganancia de la antena.

Para correr NEC2 en Linux, instale el paquete NEC2 desde el URL que está abajo. Para iniciarlo, escriba **`nec2`** e ingrese los nombres de los archivos de entrada y de salida. También vale la pena instalar el paquete **`xnecview`** para verificar la estructura y el trazado del patrón de radiación. Si todo funciona bien, se debe obtener un archivo que contiene el resultado. Este puede separarse en varias secciones, pero para una rápida idea de lo que representa se puede trazar un patrón de ganancia utilizando xnecview. Usted debería ver el patrón esperado, omnidireccional horizontalmente, con un pico correspondiente al ángulo óptimo de salida. También están disponibles las versiones Windows y Mac.

La ventaja de NEC2 es que podemos tener una idea de cómo funciona la antena antes de construirla y cómo podemos modificar el diseño para tener la ganancia máxima posible. Es una herramienta compleja y requiere algo de investigación para aprender a utilizarla efectivamente, pero es invaluable para los diseñadores de antenas.

NEC2 está disponible desde los “Archivos NEC no Oficiales” de Ray Anderson en *http://www.si-list.org/swindex2.html*

Se puede obtener documentación en la “Página Principal no Oficial de NEC" en *http://www.nittany-scientific.com/nec/*

5
Equipamiento para Redes

En el último par de años, el surgimiento de un interés sin precedentes en el equipamiento para redes inalámbricas ha traído una enorme variedad de equipos económicos al mercado. Tanta variedad, que resultaría imposible catalogar cada uno de los componentes disponibles. En este capítulo, nos enfocamos en clasificar la clase de características y atributos que son deseables en los componentes inalámbricos, y vemos varios ejemplos de herramientas comerciales y DIY (hágalo usted mismo) que han funcionado bien en el pasado.

Cableado Inalámbrico

Con un nombre como el de "inalámbrico", usted podría sorprenderse de cuántos cables están involucrados en el desarrollo de un simple enlace punto a punto. Un nodo inalámbrico está conformado por varios componentes que deben estar conectados entre sí con el cableado apropiado. Obviamente, se necesita al menos una computadora conectada a una red Ethernet, un enrutador inalámbrico, o un puente en la misma red. Los componentes de radio deben conectarse a las antenas, pero en el trayecto pueden requerir un amplificador, un protector contra rayos (es un dispositivo de tres terminales, uno conectado a la antena, el otro al radio y el tercero a tierra), u otro dispositivo. Muchos de éstos requieren energía, ya sea a través de otro cable AC, o utilizando un transformador DC. Todos estos componentes utilizan varias clases de conectores, sin mencionar una amplia variedad de tipos de cable de diferentes calibres.

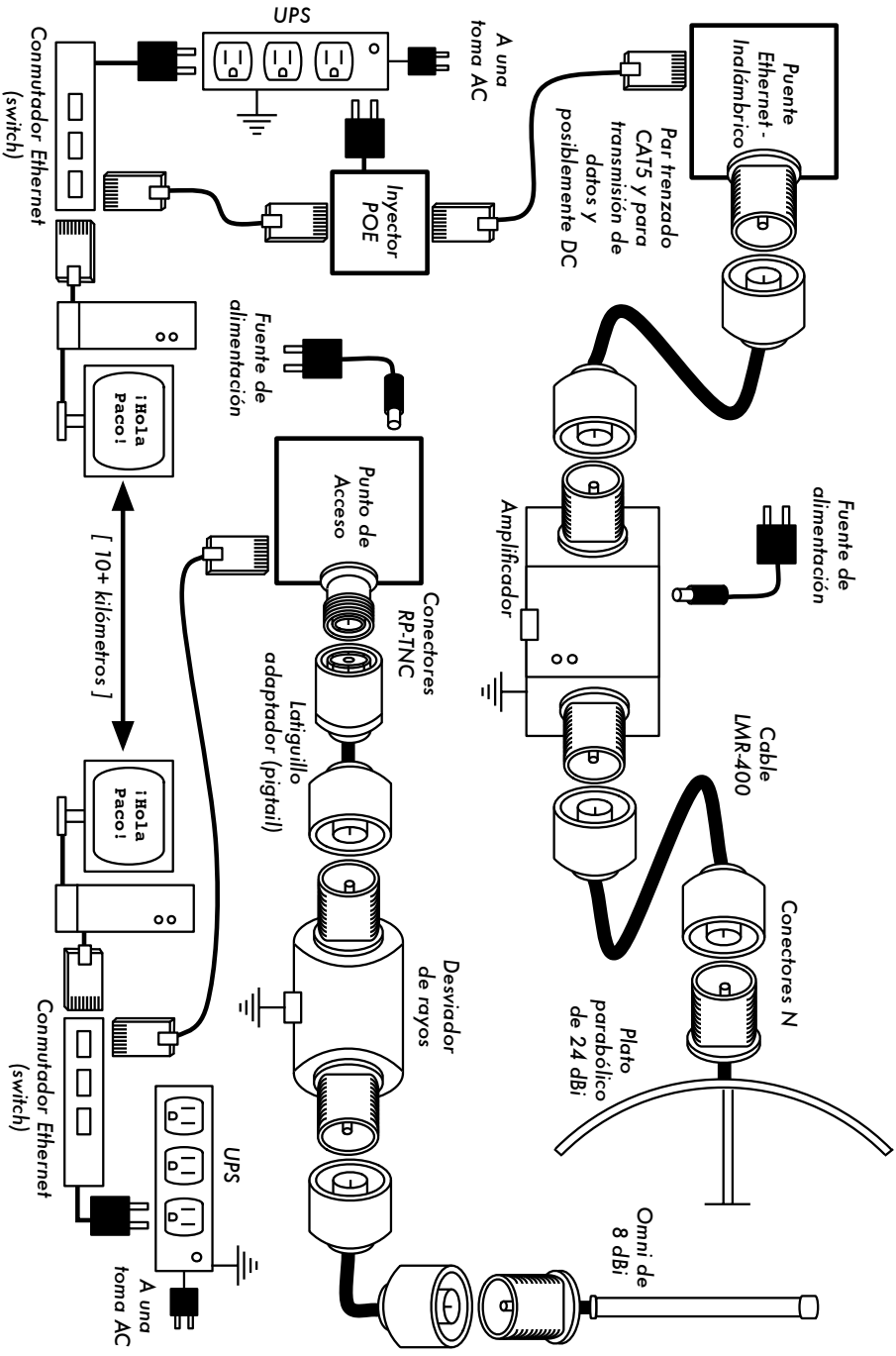


Figura 5.1: Interconexión de Componentes. .

Ahora multiplique esos cables y conectores por el número de nodos que va a instalar, y bien puede estar preguntándose porqué nos referimos a esta tecnología como "inalámbrica". El diagrama en la siguiente página le va a dar alguna idea del cableado requerido para un enlace típico punto a punto. Note que este diagrama no está a escala y no es necesariamente la mejor opción para el diseño de su red, pero le permitirá conocer en principio la variedad de conectores y componentes comunes que probablemente encontrará en el mundo real.

Aunque los componentes utilizados varían de nodo a nodo, toda instalación va incorporar estas partes:

1. Una computadora o una red conectada a un conmutador Ethernet (switch).
2. Un dispositivo que conecte esa red a un dispositivo inalámbrico (un enrutador inalámbrico, un puente o un repetidor).
3. Una antena integrada en el dispositivo inalámbrico, o conectada mediante un cable apropiado.
4. Componentes eléctricos consistentes en fuentes de alimentación, acondicionadores de energía, y protectores contra rayos.

La selección del equipamiento debe determinarse estableciendo los requerimientos del proyecto, el presupuesto disponible, y verificando que el proyecto sea viable utilizando los recursos disponibles (incluyendo provisiones para repuestos y costos de mantenimiento). Como discutimos en el capítulo uno, establecer el alcance de su proyecto es básico antes de tomar cualquier decisión de adquisiciones.

Eligiendo los componentes inalámbricos

Desafortunadamente, en un mundo de fabricantes de equipamiento que compiten entre sí y con una disponibilidad limitada de fondos, el tema del precio es el factor que generalmente recibe la mayor atención. El viejo dicho "tanto pagas, tanto obtienes" se cumple cuando compramos equipamiento de alta tecnología, pero no debe ser considerado como una verdad absoluta. Mientras que el precio es una parte importante de cualquier decisión de compra, es de vital importancia comprender precisamente qué es lo que puede obtener por su dinero, para que pueda hacer una elección que se ajuste a sus necesidades.

Cuando compare equipamiento inalámbrico para ser usado en su red, asegúrese de considerar estas variables:

- **Interoperabilidad.** ¿El equipamiento que está considerando funcionará con el de otros fabricantes? Si no es así, ¿es un factor importante para este segmento de su red? Si el equipo en cuestión soporta un protocolo abierto (como el 802.11b/g), entonces probablemente va a funcionar con equipamiento de otras fuentes.
- **Rango.** Como dijimos en el capítulo cuatro, el rango no es algo inherente a una pieza particular del equipo. El rango de un dispositivo depende de la antena conectada a él, el terreno que lo rodea, las características del dispositivo en el otro extremo del enlace, además de otros factores. En lugar de confiar en el valor del "rango" semi-ficticio provisto por el fabricante, es más útil conocer la ***potencia de transmisión*** del radio así como la ***ganancia de la antena*** (si está incluida la antena). Con esta información usted puede calcular el rango teórico como fue descrito en el capítulo tres.
- **Sensibilidad del radio.** ¿Cuán sensible es el dispositivo de radio a una tasa de transferencia dada? El fabricante debe proveer esta información, al menos a las velocidades más rápidas y más lentas. Esto puede utilizarse como una medida de la calidad del equipo, y le permite completar el cálculo del costo del enlace. Como vimos en el capítulo tres, mientras más bajo sea este valor mejor será la sensibilidad del radio.
- **Rendimiento.** Los fabricantes sistemáticamente ponen la tasa de transferencia más alta posible como la "velocidad" de su equipo. Tenga en mente que el valor de la tasa de transferencia del radio (ej. 54Mbps) nunca es el verdadero rendimiento del dispositivo (ej. aproximadamente 22Mbps para 802.11g). Si la información del rendimiento no está disponible para el dispositivo que usted está evaluando, un buen truco es dividir la "velocidad" del dispositivo por dos, y restar el 20% más o menos. Si tiene alguna duda, realice la prueba de rendimiento en una unidad de evaluación antes de comprometerse a adquirir una gran cantidad de equipamiento que no especifica una tasa de rendimiento oficial.
- **Accesorios requeridos.** Para mantener el precio inicial bajo, los vendedores a menudo quitan accesorios que se requieren para un uso normal. ¿El precio incluye todos los adaptadores de potencia? (Las fuentes DC generalmente se incluyen; pero los inyectores de potencia para Ethernet (POE) en general no. Del mismo modo, revise dos veces los voltajes de entrada, ya que el equipo normalmente viene con especificaciones de alimentación correspondiente a los estándares utilizados en los Estados Unidos. ¿Viene con los *pigtails*, adaptadores, cables, antenas, y las tarjetas de radio? Si piensa usarlo en exteriores, ¿incluye el dispositivo una caja impermeable?
- **Disponibilidad.** ¿Va a ser capaz de reemplazar los componentes que se rompan? ¿Puede ordenar esa parte en grandes cantidades? ¿Su proyecto va a requerir esas partes? ¿Cuál es el lapso de vida proyectado de este

producto en particular, en términos de tiempo de funcionamiento en el campo y probabilidad de que el vendedor lo siga suministrando?

- **Otros factores.** Asegúrese de que se provean otras características importantes para satisfacer sus necesidades particulares. Por ejemplo, ¿incluye el dispositivo un conector para una antena externa? Si lo hace, ¿de qué tipo es? ¿Existen limitaciones en número de usuarios o en el rendimiento impuestas por software, y si las hay, cuál es el costo de extender esos límites? ¿Cuál es la forma física del dispositivo? ¿Cuánta potencia consume? ¿Soporta POE como fuente de potencia? ¿Provee encriptación, NAT, herramientas de monitoreo de ancho de banda, u otras características críticas para el diseño de la red?

Contestando estas preguntas primero, va a poder tomar decisiones de compra inteligentes cuando sea el momento de elegir el equipamiento de la red. Es casi imposible que usted pueda contestar todas las dudas posibles antes de comprar el equipo, pero si le da prioridad a estas preguntas y presiona al vendedor para que las conteste antes de comprometerse a comprar, hará un mejor uso de su presupuesto y va a construir una red con componentes que se adecuen a sus necesidades.

Soluciones comerciales vs. Soluciones DIY (hágalo usted mismo)

Lo más seguro es que su proyecto de red incluya componentes adquiridos a través de proveedores externos así como otros conseguidos o fabricados localmente. Esta es una verdad económica en la mayor parte del mundo. En este estadio de la tecnología humana, la distribución global de la información es algo trivial en comparación a la distribución global de bienes. En muchas regiones, importar cada componente necesario para construir la red es prohibitivamente caro para la mayoría, aún para los grandes presupuestos. Se puede ahorrar mucho dinero a corto plazo encontrando fuentes locales para partes y mano de obra, e importar sólo aquellos componentes que lo ameriten.

Por supuesto que hay un límite a lo que puede ser hecho por una persona o un grupo en un tiempo determinado. Para ponerlo de otra forma, mediante la importación de tecnología, se intercambia dinero por equipamiento que le puede solucionar un problema particular en un periodo comparativamente inferior de tiempo. El arte de construir infraestructuras de comunicaciones locales está en encontrar el correcto balance entre el dinero y el esfuerzo que se necesita para resolver un problema dado.

Algunos componentes como las tarjetas de radio y los cables de antenas, son definitivamente muy complejos como para considerar fabricarlos

localmente. Sin embargo, otros elementos como las antenas y las torres son relativamente simples y pueden hacerse a nivel local por una fracción del costo de importación. Entre estos dos extremos se encuentran los dispositivos de comunicación en sí.

Utilizando componentes disponibles como las tarjetas de radio, placas madre, y otros, se pueden construir dispositivos que provean características comparables (o aún superiores) a la mayoría de las implementaciones comerciales. Combinar plataformas de equipamiento abiertas con software de fuente abierta puede resultar en una verdadera ganga, porque provee soluciones robustas y a la medida por muy bajo costo.

Esto no quiere decir que el equipamiento comercial sea inferior a una solución "hágalo usted mismo". Al proveernos las conocidas "llave en mano", los fabricantes no sólo nos ahorran tiempo de desarrollo, sino que también permiten que personas relativamente no calificadas puedan instalar y mantener el equipamiento. La fortaleza principal de las soluciones comerciales es que ellas proveen ***soporte*** y ***garantía de equipamiento*** (usualmente limitada). También tienen una ***plataforma consistente*** que tiende a que las instalaciones de red sean muy estables y a menudo intercambiables.

Si una parte del equipamiento no funciona, es difícil de configurar, o tiene problemas, un buen fabricante lo va a asistir. Si en uso normal el equipamiento falla (excluyendo daños extremos, como los ocasionados por la caída de un rayo), el fabricante lo va a reemplazar. La mayoría ofrecen esos servicios por un tiempo limitado como parte del precio de compra, y otros brindan soporte y garantía por un período de tiempo extendido mediante el pago de una cuota mensual. Teniendo una plataforma consistente es sencillo tener los repuestos a mano y simplemente "cambiar" el equipo que falla sin la necesidad de un técnico que configure el equipo. Evidentemente esto viene de la mano de un costo inicial más alto si lo comparamos con los componentes disponibles localmente.

Desde el punto de vista de un arquitecto de red, los tres grandes riesgos ocultos al elegir soluciones comerciales son: ***quedar atrapado con un proveedor***, las ***líneas de productos descontinuadas***, y ***los costos de licenciamiento futuro***.

Puede ser muy costoso dejar que las mal denominadas nuevas "características" dirijan el desarrollo de su red. Los fabricantes frecuentemente van a ofrecerle características que son incompatibles por su diseño con los de la competencia, y luego usan elementos de mercadeo para convencerlo de que usted no puede vivir sin éstas, sin importar que la característica contribuya a solucionar sus problemas de comunicación o no. Al empezar a contar con esas características, probablemente en el futuro

decidirá continuar comprando equipamiento del mismo fabricante. Esa es la esencia de quedar atrapado con el proveedor. Si una gran institución utiliza una cantidad significante de equipamiento patentado, es improbable que simplemente vaya a abandonarlo para considerar un proveedor diferente. Los equipos de venta saben esto (y de hecho, algunos cuentan con ello) y utilizan esto como estrategia para la negociación de precios.

Un fabricante puede eventualmente decidir descontinuar una línea de productos sin importar su popularidad. Esto asegura que los clientes, que ya confiaban en las características del producto patentado del fabricante, van a comprar los nuevos modelos (casi siempre más caros). Los efectos a largo plazo de quedar atrapado con el proveedor y con los productos descontinuados, son difíciles de estimar cuando planificamos un proyecto de red, pero deben tenerse en mente.

Finalmente, si una pieza en particular del equipamiento utiliza un código de computadora patentado, usted va a tener que licenciar el uso de ese código en contratos futuros. El costo de esas licencias puede variar dependiendo de las características que brinda, el número de usuarios, la velocidad de la conexión u otros factores. ¡Si no se paga el costo de la licencia, algunos equipos están diseñados para simplemente dejar de funcionar hasta que se provea una licencia válida! Asegúrese de que comprende los términos de uso de cualquier equipamiento que adquiera, incluyendo las futuras cuotas de licenciamiento.

Usando equipamiento genérico que soporta estándares abiertos y software de fuente abierta, se pueden evitar algunos de estos riesgos. Por ejemplo, es muy difícil verse atrapado por un proveedor que utiliza protocolos abiertos (tales como TCP/IP sobre 802.11a/b/g). Si tiene un problema con el equipo o con el proveedor, siempre puede adquirirlo de otro proveedor, ya que va a funcionar con lo que usted ya compró. Es por estas razones que recomendamos utilizar protocolos patentados y espectro con licenciamiento **sólo** en casos donde el equivalente abierto (como el 802.11a/b/g) no es viable técnicamente.

Si bien los productos individuales pueden discontinuarse en cualquier momento, usted puede limitar el impacto que esto va a tener en su red utilizando componentes genéricos. Por ejemplo, si una *placa madre* particular ya no está disponible en el mercado, puede tener a mano varias *placas madre* de PC que van a desempeñarse efectivamente en la misma tarea. Más adelante en este capítulo vamos a ver algunos ejemplos de cómo utilizar esos componentes genéricos para construir un nodo inalámbrico completo.

Obviamente, no va a haber costos de licenciamiento en cuanto al software libre (con la excepción de un proveedor que ofrezca soporte u otros servicios sin cobrar por el uso del software en sí mismo). Ha habido ocasionalmente

vendedores que se aprovechan indebidamente del regalo que los programadores de fuente abierta le han dado al mundo, exigiendo el pago de licencias, violando de ese modo los términos de distribución acordados por los autores originales. Sería bueno evitar a dichos vendedores, y desconfiar de aquellas afirmaciones de "software libre" que, sin embargo, estipulan una cuota de licenciamiento a futuro.

La desventaja de utilizar software libre y equipamiento genérico es claramente una cuestión de soporte. Cuando lleguen los problemas a la red, va a tener que resolverlos por usted mismo. Esto a veces se logra consultando recursos gratuitos en línea y motores de búsqueda, y aplicando los parches al código directamente. Si no tiene ningún miembro de su equipo que sea competente en el tema y se dedique a diseñar soluciones a sus problemas de comunicación, entonces poner en marcha un proyecto de red puede tomar una cantidad considerable de tiempo. Por supuesto que tampoco hay garantías de que simplemente "a punta de dinero" se resuelva el problema. Si bien damos varios ejemplos de cómo hacer el trabajo usted mismo, seguramente le va a resultar un gran desafío. Necesita encontrar el balance entre el enfoque de las soluciones comerciales y las hechas por usted mismo, que funcionen de forma adecuada a su proyecto.

En resumen, siempre defina primero el objetivo de su red, identifique los recursos que puede tener para lidiar con el problema, y permita que la selección del equipamiento emerja naturalmente de esos resultados. Considere las soluciones comerciales así como los componentes abiertos, manteniendo siempre en mente los costos a largo plazo de ambas.

Productos inalámbricos profesionales

En el mercado existe equipamiento en abundancia para enlaces punto a punto (P2P) a larga distancia. La mayoría ya está listo para ponerse en funcionamiento al sacarlo de la caja; solamente debemos conectar y sellar los cables de la antena. Cuando pensamos en un enlace a larga distancia, existen tres factores principales que debemos considerar: la distancia total del enlace, los requerimientos de tiempo de puesta en funcionamiento, y por supuesto los requerimientos de velocidad.

La mayoría de los productos comerciales disponibles en la actualidad para enlaces de largo alcance, utilizan tecnología OFDM y operan en la banda ISM de 5800 MHz. Existen algunos productos que utilizan estándares abiertos, pero la mayoría tienen protocolos propietarios de algún tipo. Esto significa que para formar un enlace, las radios de ambos lados deben ser del mismo fabricante. Para el caso de un enlace crítico es una buena idea elegir un sistema que utilice equipamiento idéntico en ambos extremos del enlace. De esta forma se necesita tener almacenado solamente un repuesto, y si se

tiene que usar puede reemplazarse en cualquier lado del enlace. Hay algunos productos buenos en el mercado que usan diferentes equipamientos en los extremos del enlace. Los mismos pueden usarse en una red siempre que se haga con cuidado, de lo contrario se van a necesitar más repuestos para ambos tipos de radios.

Lo que sigue no intenta ser propaganda de venta de un radio, ni tampoco una queja acerca de otros. Son simplemente algunas notas generadas durante más de cinco años de experiencia de campo alrededor de todo el mundo, con productos comerciales sin licenciamiento. Desafortunadamente, no hay forma de considerar todos los productos, por esa razón sólo algunos de los favoritos se listan a continuación.

Redline Communications

Redline llegó al mercado en primera instancia con la línea de productos AN-50. Este fue el primer producto punto a punto disponible con tasas de transferencia de datos sobre los 50 Mbps, al alcance de los pequeños operadores. Sólo utiliza 20 MHz del espectro por canal. Hay tres modelos diferentes en la línea AN-50. Los tres tienen el mismo grupo de características básicas, sólo cambia el ancho de banda total. El modelo estándar tiene 36 Mbps de rendimiento, el modelo económico tiene 18 Mbps, y la versión completa 54 Mbps. Los controles del ancho de banda son a través de un programa y pueden acomodar la demanda de ancho de banda.

Los radios Redline están compuestos de una unidad interna, una externa y una antena. La unidad interna entra en un estante estándar de 19 pulgadas y ocupa 1U (1,5 pulgadas de altura). La unidad externa se monta en el mismo soporte que mantiene la antena en su lugar. Esta unidad es el radio. Las dos unidades están unidas por un cable coaxial. Se utiliza el cable Beldon RG6 o el RG11. Es el mismo que se utiliza para las instalaciones satelitales de TV. No es caro, se encuentra fácilmente y elimina la necesidad de adquirir cables caros de baja pérdida, como la serie de *Times Microwave LMR* o *Andrew Corporation Heliax*. El hecho de montar el radio tan cerca de la antena mantiene la pérdida del cable en un mínimo absoluto.

Debemos destacar dos características de los radios Redline. La primera es el ***Modo de Alineación General***, que utiliza una alarma sónica (*beeper*) que cambia el tono cuando cambia la técnica de modulación. Un beep más rápido significa una conexión más rápida. Esto permite un alineamiento mucho más sencillo porque el enlace puede ser alineado por los tonos únicamente. Sólo se necesita una sintonización final, y para ayudarnos tenemos una aplicación gráfica de Windows. Otra característica es el botón de ***Prueba***. Si realizamos cambios al radio, y no estamos seguros de que sean los correctos, presionando el botón de prueba en lugar del botón

Guardar, activará los nuevos cambios por cinco minutos. Después de esos cinco minutos, la configuración vuelve a la configuración anterior a apretar el botón de ***Prueba***. Esto permite que se prueben los cambios, y si las cosas no funcionan y el enlace cae, el mismo se recobrará después de cinco minutos. Una vez que los cambios hayan sido probados, simplemente se confirma la nueva configuración, y se presiona el botón de guardar en lugar del de prueba.

Redline tiene otros modelos disponibles. El AN-30 tiene cuatro puertos T1/E1, además de una conexión a Ethernet de 30 Mbps. El AN-100 sigue el estándar 802.16a, y el próximo RedMax promete adherir a WiMax.

Por más información acerca de estos los productos vea *http://www.redlinecommunications.com/*

Alvarion

Una de las grandes ventajas de trabajar con los productos Alvarion es su bien establecida red de distribución mundial. También tienen una de las cuotas del mercado mundial más grande para toda clase de equipamiento de conectividad inalámbrica a Internet. Tiene distribuidores y revendedores en la mayoría de las regiones. Para los enlaces a larga distancia ofrece dos productos de interés: La serie VL, y el Link Blaster.

Si bien la serie VL es en realidad un sistema punto a multi-punto, un solo radio cliente conectado a un punto de acceso funcionará bien para establecer un enlace punto a punto. Lo único que debe considerarse es utilizar una antena con mayor direccionalidad en el punto de acceso, a menos que haya un enlace planeado a futuro que puede conectarse a ese punto de acceso. Hay dos velocidades disponibles para la serie VL, 24 Mbps y 6 Mbps. Los requerimientos de costo, tiempo de la señal y velocidad van a guiar la decisión de cuál CPE (*Customer Premises Equipment*- equipo de usuario) usar.

El Link Blaster se parece muchísimo al Redline AN-50. Esto se debe a que de hecho son el mismo aparato. Casi enseguida después de que el Redline AN-50 llegó al mercado, se firmó un acuerdo OEM (Original Equipment Manufacturer) entre las dos compañías y así nació el Link Blaster. A pesar de que la caja del modelo para interiores es diferente, y de que las antenas están marcadas de forma distinta, los componentes electrónicos internos de estos modelos son idénticos. El Link Blaster cuesta más que un Redline; este valor adicional se justifica por un diseño más robusto así como un nivel de soporte adicional. En muchos casos, a un revendedor de Alvarion le es sencillo conseguir productos de revendedores de Redline. Esto debe ser investigado a nivel local. Puede valer más la pena el dinero extra para tener un producto que esté disponible y tenga soporte local.

Alvarion tiene algunos productos para enlaces punto a punto de 2400 MHz. La mayoría de sus productos usan la banda ISM en los 2400 MHz con la tecnología de espectro esparcido de salto de frecuencia (*FHSS por su sigla en inglés*) y generan mucho ruido que puede afectar otras aplicaciones sobre el espectro esparcido que usen secuencias directas (*DSSS por su sigla en inglés*) y que se encuentren en la misma torre. Si se está planeando una red basada en un sistema de distribución DSSS, un transporte (*backhaul*) FHSS no es una opción efectiva.

Para más información acera de los productos Alvarion, vea *http://www.alvarion.com/*

Rad Data Communications

La línea de productos Rad Airmux es relativamente nueva en el Mercado, y tiene un potencial grande. El Airmux 200 es una radio de 48 Mbps, usa el cable CAT5, y tiene uno de los mejores precios para cualquier solución comercial. Las unidades son pequeñas y fáciles de manipular en una torre. La única contra con la que nos podemos enfrentar es la falta de un sistema distribución local en el mundo en desarrollo. Tenemos dos modelos disponibles dentro de la línea Airmux. Uno usa antenas internas, y el otro externas.

La experiencia con los radios Airmux a principios del 2005 mostró la existencia de un problema con la temporización. Sólo se ve cuando la distancia del enlace es mayor a 12 millas, o 19 km. No importa qué tipo de antena se esté usando. Mientras que este problema no sea solucionado, esos radios sólo deberían utilizarse para enlaces de hasta 19 km. Si se sigue este consejo los radios van a desempeñarse muy bien, especialmente desde el punto de vista de su precio.

Para más información acerca de los productos Rad, vea *http://www.rad.com/*

Cisco Systems

Las soluciones inalámbricas de Cisco tienen dos grandes ventajas a su favor. Tienen una distribución muy bien establecida, soporte y entrenamiento en redes por casi todo el mundo. Esto puede ser de gran ayuda cuando debemos procurarnos el equipamiento, y aún más importante, si el mismo se rompe y necesitamos reemplazarlo. La siguiente gran ventaja es que utilizan estándares abiertos para la mayoría de las partes, siguiendo los estándares 802.11a/b/g.

La experiencia ha mostrado que sus herramientas de configuración vía web no son tan sencillas de comprender como las que encontramos en muchos

otros productos, y el equipamiento tiende a tener un precio que hace que otras soluciones no comerciales de estándares abiertos sean más viables.

Más información acerca de Cisco se puede encontrar en *http://www.cisco.com/*

¿Algunas otras?

Actualmente hay muchas más soluciones disponibles en el mercado y siguen llegando otras todo el tiempo. Buenas soluciones se encuentran en compañías como Trango Broadband (*http://www.trangobroadband.com/*) y Waverider Communications (*http://www.waverider.com/*). Cuando consideremos qué solución utilizar, siempre debemos recordar los tres factores principales; distancia, tiempo de puesta en funcionamiento y velocidad. Debe chequear y asegurarse de que las radios operan en una banda sin licenciamiento donde usted las va a instalar.

Protectores profesionales contra rayos

La única amenaza natural del equipamiento inalámbrico son los rayos eléctricos. Hay dos formas diferentes mediante las cuales un rayo puede dañar el equipo: con un impacto directo o uno inducido. Los impactos directos son cuando el rayo realmente alcanza la torre o la antena. El impacto inducido se produce cuando el rayo cae cerca de la torre. Imagine un relámpago cargado negativamente. Como las cargas se repelen entre sí, hará que los electrones en el cable se alejen del rayo, creando corriente en las líneas. Esta es mucha más corriente de la que el sensible radio puede manejar. En general, cualquier tipo de rayo va a destruir el equipo que esté sin protección.

Proteger las redes inalámbricas de los relámpagos no es una ciencia exacta, y no hay garantías de que no vaya a caer un rayo, aún si se toman todas las precauciones. Muchos de los métodos utilizados van a ayudar a prevenir los impactos directos y los generados por inducción. Si bien no es necesario utilizar todos los métodos de protección contra rayos, tener más de uno va a ayudarnos a cuidar mejor el equipo. La cantidad de rayos observados históricamente en un área de servicio es la mejor guía para saber que debemos hacer.

Comience en la base misma de la torre. Recuerde que la base de la torre está bajo tierra. Después de colocados los cimientos de la torre, pero antes de que el pozo se llene nuevamente, se debe instalar un aro de alambre trenzado grueso para hacer tierra, extendido bajo la superficie y sobresaliendo de la misma cerca de la pata de la torre. El alambre debe ser por lo menos AWG #4 (*American Wire Gauge*) o más grueso.

Adicionalmente, se debe enterrar una jabalina, y conectarla también a la torre en el mismo punto.

Figura 5.2: Torre con un cable de cobre grueso conectado a tierra.

Es importante tener en cuenta que no todos los metales conducen la electricidad de la misma forma. Algunos metales actúan como conductores eléctricos mejor que otros, y las diferentes capas existentes en la superficie también pueden afectar cómo el metal de la torre maneja la corriente eléctrica. El acero inoxidable es uno de los peores conductores, y las capas contra la herrumbre como los galvanizados o la pintura reducen la conductividad del metal. Por esta razón se coloca un alambre de tierra trenzado desde la base de la torre hasta la cima. La base necesita estar apropiadamente unida a los conductores provenientes del aro y de la jabalina. La cima de la torre debe tener una jabalina pararrayos, terminada en punta. Cuanto más fina y aguda sea la punta, más efectivo será el pararrayos. El alambre de tierra trenzado desde la base tiene que terminarse en esta jabalina. Es muy importante asegurarse de que el alambre de tierra esté conectado al propio metal. Cua-lquier tipo de capa, como la pintura, debe removerse antes de que se coloque el alambre. Una vez que se hizo la conexión, si es necesario, el área expuesta puede repintarse, cubriendo el alambre y los conectores para proteger a la torre de la herrumbre y la corrosión.

La solución anterior detalla la instalación de un sistema básico de tierra. El mismo provee protección para la torre contra los impactos directos, y representa el sistema de base al que se conectará todo lo demás.

La protección ideal para los impactos indirectos son protectores de gas contra rayos ubicados en ambos extremos del cable. Estos protectores contra rayos deben ser conectados directamente al alambre de tierra instalado en la torre si este está en el extremo más alto. El extremo en la base debe también conectarse a una buena tierra, como una placa de tierra o una tubería metálica que esté llena de agua. Es importante asegurarse de que el protector contra rayos externo esté impermeabilizado. Muchos protectores contra rayos para los cables coaxiales son impermeables, mientras que los de cable CAT5 no lo son.

En el caso de que no se usen los protectores contra rayos, y el cableado esté basado en coaxiales, se conecta el revestimiento del cable coaxial al cable de tierra instalado en las torres, y de esta forma proveerá algo de protección. Esto proporciona un camino a tierra a las corrientes inducidas, y si la descarga no es muy fuerte no va a afectar el cable coaxial. Si bien este método no da una protección tan buena como la utilización de los protectores de gas, es mejor que nada.

Construyendo un AP con una PC

A diferencia de los sistemas operativos para consumidores (como Microsoft Windows), el sistema operativo GNU/Linux le brinda al administrador de red acceso completo a muchos elementos del trabajo en redes. Podemos acceder y manipular paquetes de red a cualquier nivel, desde la capa de enlace de datos hasta la capa de aplicación. Se pueden tomar decisiones de enrutamiento con base a cualquier información contenida en el paquete de red, desde la dirección de enrutamiento y puertos, hasta los contenidos de los segmentos de datos. Un punto de acceso basado en Linux puede actuar como enrutador, puente, corta fuego, concentrador VPN, servidor de aplicaciones, monitor de la red, o virtualmente cualquier otro rol de la red en el que usted pueda pensar. Es un software libre, y no requiere pagos de licenciamiento. Linux/GNU es una herramienta muy poderosa que puede ajustarse a una amplia variedad de roles en una infraestructura de red.

Agregar una tarjeta inalámbrica y un dispositivo Ethernet a una PC corriendo Linux le dará una herramienta muy flexible que puede ayudarlo a repartir el ancho de banda y administrar su red a un costo muy bajo. El equipamiento puede ser desde una computadora portátil reciclada, o una computadora de escritorio, hasta una computadora embebida, tales como un equipo de red Linksys WRT54G o Metrix.

En esta sección veremos cómo configurar Linux en las siguientes configuraciones:

- Como punto de acceso inalámbrico utilizando Masquerading/NAT y una conexión cableada a Internet (también denominada *gateway*).
- Como punto de acceso inalámbrico que actúa como puente transparente. El puente puede usarse tanto como un simple punto de acceso, o como un repetidor con dos radios.

Considere estas recetas como un punto de inicio. Construyendo estos ejemplos simples, puede crear un servidor que se ajuste de forma precisa a su infraestructura de red.

Pre-requisitos

Antes de comenzar, debe estar familiarizado con Linux desde la perspectiva del usuario, y ser capaz de instalar la distribución Linux/Gnu de su elección. También se requiere una comprensión básica de la interfaz de línea de comando (*terminal*) en Linux.

Va a necesitar una computadora con una o más tarjetas inalámbricas instaladas previamente, así como una interfaz Ethernet estándar. Estos ejemplos utilizan una tarjeta y un manejador (*driver*) específicos, pero hay varios tipos diferentes de tarjetas que pueden funcionar igualmente bien. Las tarjetas inalámbricas basadas en los grupos de chips Atheros y Prism lo hacen particularmente bien. Estos ejemplos se basan en la versión de Linux Ubuntu 5.10 (Breezy Badger), con una tarjeta inalámbrica soportada por los manejadores HostAP o MADWiFi.

Para más información acerca de estos manejadores vea *http://hostap.epitest.fi/* y *http://madwifi.org/*.

Para completar estas instalaciones se requiere del siguiente software, el cual debe estar incluido en su distribución Linux:

- Herramientas Inalámbricas (comandos iwconfig, iwlist)
- Cortafuego iptables
- dnsmasq (servidor cache DNS y servidor DHCP)

La potencia de CPU que se requiere depende de cuánto trabajo se tiene que hacer más allá de un simple enrutamiento y NAT. Para muchas aplicaciones una 486 de 133MHz es perfectamente capaz de enrutar paquetes a las velocidades inalámbricas. Si piensa usar mucha encriptación (como WEP o un servidor VPN), entonces necesita algo más rápido. Si también quiere correr un servidor de almacenamiento intermedio (como Squid, vea el capítulo tres) necesitará una computadora con mucha más rapidez, espacio de disco y memoria RAM. Un enrutador típico que solo

esté realizando NAT puede operar con tan solo 64MB de RAM y almacenamiento.

Cuando armamos una máquina que está pensada para ser parte de una infraestructura de red, debemos tener en cuenta que los discos duros tienen una vida útil limitada en comparación con la mayoría de los otros componentes. A menudo puede utilizar almacenamiento de estado sólido, como un disco *flash*, en lugar de un disco duro. Este puede ser un manejador *flash* USB (suponiendo que su PC va a cargarse desde USB), o una tarjeta Compact Flash utilizando un adaptador de CF a IDE. Estos adaptadores son bastante económicos, y permiten que una tarjeta CF actúe en apariencia como un disco duro IDE. Pueden usarse en cualquier PC que soporte discos duros IDE. Como no tienen partes móviles, funcionarán por muchos años en un rango mucho más alto de temperaturas de las que puede tolerar un disco duro.

Escenario 1: punto de acceso con Enmascaramiento

Este es el más simple de los escenarios, y es especialmente útil en situaciones donde usted quiere un único punto de acceso para una oficina. Es el más fácil en una situación donde:

1. Existen un cortafuego y una pasarela (*gateway*) dedicados corriendo Linux, y usted sólo quiere agregar una interfaz inalámbrica.
2. Usted dispone de una vieja computadora común o portátil restaurada y prefiere utilizarla como un punto de acceso.
3. Requiere de más potencia en términos de monitoreo, registro y/o seguridad de lo que la mayoría de los puntos de acceso comerciales le proveen, pero no quiere derrochar en un punto de acceso empresarial.
4. Le gustaría que una única computadora actuara como dos puntos de acceso (y cortafuego) para poder ofrecer un punto de acceso seguro a la intranet, así como acceso abierto a los invitados.

Configuración inicial

Comience con una computadora ya configurada corriendo Linux/Gnu. Puede ser una instalación de Servidor Ubuntu, o Fedora Core. Para su funcionamiento, la computadora debe tener al menos dos interfaces, y al menos una de ellas debe ser inalámbrica. El resto de esta descripción supone que su puerto Ethernet (eth0) está conectado a la Internet, y que hay una interfaz inalámbrica (wlan0) que va a proveer la funcionalidad del punto de acceso.

Para saber si su grupo de chips soporta el modo maestro, pruebe con el siguiente comando en modo raíz (root):

```
# iwconfig wlan0 mode Master
```

...reemplazando wlan0 con el nombre de su interfaz.

Si obtiene un mensaje de error, su tarjeta inalámbrica no soporta el modo de punto de acceso. De todas formas puede probar la misma configuración en el modo ad hoc, que es soportado por todos los grupos de chips. Esto re-quiere configurar todas las computadoras portátiles que están conectadas al "punto de acceso" en el modo ad hoc, y puede que no funcione del modo que usted espera. En general es mejor encontrar una tarjeta inalámbrica que soporte el modo AP. Para obtener una lista de las tarjetas soportadas vea los sitios web HostAP y MADWiFi mencionados anteriormente.

Antes de continuar asegúrese de que dnsmasq está instalado en su computadora. Puede utilizar la herramienta de configuración gráfica de su distribución para instalarlo. En Ubuntu puede simplemente correr lo siguiente en modo raíz (root):

```
# apt-get install dnsmasq
```

Configurar las interfaces

Configure su servidor para que eth0 esté conectada a Internet. Utilice la herramienta de configuración gráfica que viene con su distribución.

Si su red Ethernet usa DHCP, puede probar con el siguiente comando como raíz:

```
# dhclient eth0
```

Debe recibir una dirección IP y una pasarela por defecto. Luego arranque su interfaz inalámbrica en el modo Maestro y póngale un nombre de su elección:

```
# iwconfig wlan0 essid "my network" mode Master enc off
```

El comando **`enc off`** desconecta la encriptación WEP. Para habilitar WEP agregue la clave hexagesimal del largo correcto:

```
# iwconfig wlan0 essid "my network" mode Master enc 1A2B3C4D5E
```

Como una alternativa, puede utilizar una clave legible comenzando con "**`s:`** "

```
# iwconfig wlan0 essid "my network" mode Master enc "s:apple"
```

Ahora déle a su interfaz inalámbrica una dirección IP en una sub red privada, pero asegúrese de que no sea la misma sub red de la de su adaptador Ethernet:

```
# ifconfig wlan0 10.0.0.1 netmask 255.255.255.0 broadcast 10.0.0.255 up
```

Configurar enmascarado en el kernel

Para ser capaces de traducir direcciones entre dos interfaces en la computadora, debemos habilitar el enmascarado (NAT) en el kernel linux. Primero cargamos el módulo kernel pertinente:

```
# modprobe ipt_MASQUERADE
```

Ahora vamos a desactivar todas las reglas del cortafuego existente para asegurarnos que las mismas no van a bloquearnos al reenviar paquetes entre las dos interfaces. Si tiene un cortafuego activado, asegúrese de que sabe cómo restaurar las reglas existentes antes de proceder.

```
# iptables -F
```

Habilite la funcionalidad de NAT entre las dos interfaces

```
# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Finalmente tenemos que habilitar el kernel para reenviar paquetes entre las interfaces:

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

En las distribuciones de Linux basado en Debian como Ubuntu, este cambio también puede hacerse editando el archivo **`/etc/network/options`**, y cambiando la línea

```
ip_forward=no
```

a

```
ip_forward=yes
```

y luego reiniciar las interfaces de red con:

```
# /etc/init.d/network restart
```

o

```
# /etc/init.d/networking restart
```

Configurar el servidor DHCP

En este momento deberíamos tener un punto de acceso en funcionamiento. Puede probarlo conectándose a la red inalámbrica "my network" desde otra computadora a la que le haya asignado una dirección en el mismo rango de direcciones que su interfaz inalámbrica en el servidor (10.0.0.0/24 si siguió los ejemplos). Si ha habilitado WEP, tenga cuidado de utilizar la misma clave que especificó en el AP.

Para que sea más sencillo para las personas conectarse al servidor sin conocer el rango de direcciones IP, vamos a configurar un servidor DHCP para que maneje automáticamente las direcciones de los clientes inalámbricos.

Con este propósito utilizamos el programa dnsmasq. Como su nombre lo indica, provee un servidor DNS interino (*caching*) así como un servidor DHCP. Este programa fue desarrollado específicamente para el uso con cortafuegos que realizan NAT. Si su conexión a Internet tiene una alta latencia y/o un ancho de banda bajo, como conexión por discado (*dial-up*) o un VSAT, el tener un servidor DNS interino es de mucha utilidad. Esto significa que muchas consultas DNS pueden resolverse localmente, ahorrándole mucho tráfico a la conexión a Internet, y al mismo tiempo hace que la conexión se sienta notablemente más rápida.

Instale dnsmasq con el paquete de administración de la distribución. Si dnsmasq no está disponible como un paquete, descargue el código fuente e instálelo manualmente. Lo puede obtener en: *http://thekelleys.org.uk/dnsmasq/doc.html*.

Todo lo que necesitamos para correr dnsmasq es editar unas pocas líneas de su archivo de configuración, **`/etc/dnsmasq.conf`**.

El archivo de configuración está bien documentado, y tiene muchas opciones para varios tipos de configuración. Para tener el servidor básico DHCP en funcionamiento debemos quitar los comentarios y/o editar dos líneas.

Encuentre las líneas que comienzan de este modo:

```
interface=
```

...y asegúrese de que digan:

```
interface=wlan0
```

...cambiando wlan0 para que corresponda con el nombre de su interfaz inalámbrica. Luego encuentre las líneas que comienzan con:

```
#dhcp-range=
```

Quite el indicador de comentario de la línea y edítela para abarcar las direcciones pertinentes, por ej.

```
dhcp-range=10.0.0.10,10.0.0.110,255.255.255.0,6h
```

Luego salve el archivo e inicie dnsmasq:

```
# /etc/init.d/dnsmasq start
```

En este momento, debe ser capaz de conectarse al servidor como un punto de acceso, y obtener una dirección IP utilizando DHCP. Esto le debe permitir conectarse a Internet a través del servidor.

Agregando seguridad extra: Configurar un cortafuego

Una vez configurado y probado, se pueden agregar reglas de cortafuego utilizando la herramienta de cortafuego incluida en su distribución. Algunos gestores para configurar reglas del cortafuego son:

- ***firestarter*** – un cliente gráfico para Gnome, que requiere que su servidor corra en Gnome
- ***knetfilter*** – un cliente gráfico para KDE, el cual requiere que su servidor corra en KDE
- ***Shorewall*** – un conjunto de guiones y archivos de configuración que van a facilitar la configuración de los cortafuegos iptables. También hay gestores para shorewall, como el webmin-shorewall
- ***fwbuilder*** - una herramienta gráfica poderosa, pero ligeramente compleja que le permite crear guiones iptables en otra computadora, y luego transferirlos al servidor. Esto evita la necesidad de una interfaz gráfica en el servidor, y es una opción de seguridad aún más fuerte.

Una vez que todo está configurado de forma correcta, revise que todas las configuraciones estén reflejadas en el guión de arranque del sistema. De esta forma sus cambios seguirán funcionando aunque la computadora deba ser reiniciada.

Escenario 2: Hacer del punto de acceso un puente transparente

Este escenario puede utilizarse tanto para un repetidor de dos radios, o para un punto de acceso conectado a una Ethernet. Utilizamos un puente en lugar de un enrutador cuando queremos que ambas interfaces en el punto de acceso compartan la misma sub red. Esto puede ser particularmente útil en redes con múltiples puntos de acceso donde preferimos tener un único cortafuego central y tal vez un servidor de autentificación. Dado que todos los clientes comparten la misma sub red, pueden ser manejados fácilmente con un único servidor DHCP y un cortafuego sin la necesidad de un relevador DHCP.

Por ejemplo, usted puede configurar un servidor como en el primer escenario, pero utiliza dos interfaces Ethernet cableadas en lugar de una cableada y una inalámbrica. Una interfaz sería su conexión a Internet, y la otra conecta a un conmutador. Luego conecte tantos puntos de acceso como sean requeridos al mismo conmutador, configurándolos como puentes transparentes, y cada uno pasará a través del mismo cortafuego y utilizará el mismo servidor DHCP.

La simplicidad de puentear tiene un costo en cuanto a eficiencia. Ya que todos los clientes comparten la misma sub red, el tráfico de difusión se repite a través de la red. Esto funciona bien con redes pequeñas, pero cuando el número de clientes se incrementa, se desperdicia mucho ancho de banda en el tráfico de difusión.

Configuración inicial

La configuración inicial para un punto de acceso puenteado es similar al del punto de acceso enmascarado, sin requerir de dnsmasq. Siga las instrucciones de configuración inicial del ejemplo anterior.

Además, para la función de puente se requiere el paquete *bridge-utils* (***utilidades*** puente). Este paquete está disponible para Ubuntu y otras distribuciones basadas en Debian, y también para Fedora Core. Asegúrese de que éste esté instalado y de que el comando **`brctl`** esté disponible antes del procedimiento.

Configurando las Interfaces

En Ubuntu o en Debian configuramos las interfaces editando el archivo **`/etc/network/interfaces`**

Agregue una sección como la que sigue, pero cambie los nombres de las interfaces y las direcciones IP que correspondan. La dirección IP y la máscara de red deben concordar con la de su red. Este ejemplo supone que está construyendo un repetidor inalámbrico con dos interfaces inalámbricas, wlan0 y wlan1. La interfaz wlan0 va a ser un cliente de la red "*office*", y wlan1 va a crear una red llamada "*repeater*".

Agregue lo siguiente a **`/etc/network/interfaces`**:

```
auto br0
iface br0 inet static
  address 192.168.1.2
  network 192.168.1.0
  netmask 255.255.255.0
  broadcast 192.168.1.255
  gateway 192.168.1.1
  pre-up ifconfig wlan 0 0.0.0.0 up
  pre-up ifconfig wlan1 0.0.0.0 up
  pre-up iwconfig wlan0 essid "office" mode Managed
  pre-up iwconfig wlan1 essid "repeater" mode Master
  bridge_ports wlan0 wlan1
  post-down ifconfig wlan1 down
  post-down ifconfig wlan0 down
```

Ponga una marca de comentario a todas las líneas que se refieran a wlan0, o a wlan1 para asegurarse de que no van a interferir con nuestra configuración.

Esta sintaxis para configurar los puentes mediante el archivo **`interfaces`** es específico para distribuciones basadas en Debian, y los detalles de la configuración del puente son manejados por un par de guiones: **`/etc/network/if-pre-up.d/bridge`** y **`/etc/network/if-post-down.d/bridge`**. La documentación para estos guiones se encuentra en **`/usr/share/doc/bridge-utils/`**.

Si dichos programas no existen en su distribución (como Fedora Core), aquí hay una configuración alternativa para **`/etc/network/interfaces`** que logrará lo mismo:

```
iface br0 inet static
  pre-up ifconfig wlan 0 0.0.0.0 up
  pre-up ifconfig wlan1 0.0.0.0 up
  pre-up iwconfig wlan0 essid "office" mode Managed
  pre-up iwconfig wlan1 essid "repeater" mode Master
  pre-up brctl addbr br0
  pre-up brctl addif br0 wlan0
  pre-up brctl addif br0 wlan1
  post-down ifconfig wlan1 down
  post-down ifconfig wlan0 down
  post-down brctl delif br0 wlan0
  post-down brctl delif br0 wlan1
  post-down brctl delbr br0
```

Arrancar el puente

Una vez que el puente esté definido como una interfaz, arranque el puente escribiendo:

```
# ifup -v br0
```

La "-v" significa salida verbosa y proporciona información acerca de lo que está pasando.

En Fedora Core (y otras distribuciones no Debian) también debe darle a su interfaz puenteada una dirección de IP y agregar una ruta por omisión al res-to de la red:

```
#ifconfig br0 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
#route add default gw 192.168.1.1
```

En este momento debería poder conectar a este nuevo punto de acceso una computadora portátil inalámbrica, y a través de ésta conectarse a Internet (o al menos con el resto de su red).

Si quiere más información sobre su puente y lo que está haciendo, utilice el comando ***brctl***. Intente por ejemplo:

```
# brctl show br0
```

Esto debería darle e información sobre lo que está haciendo el puente.

Escenarios 1 y 2 de la forma sencilla

En lugar de configurar su computadora como un punto de acceso desde cero, usted puede aprovechar una distribución Linux armada especialmente para este propósito. Estas distribuciones pueden hacernos la tarea tan simple como arrancar la computadora desde un CD preconfigurado con el sistema operativo para interfaz inalámbrica. Para más información diríjase a la sección, "Sistemas operativos amigables con la tecnología inalámbrica".

Como puede ver es fácil proveer servicios de punto de acceso desde un enrutador Linux estándar. Usar Linux le da un control mucho más significativo sobre cómo se enrutan los paquetes a través de su red, y tiene algunas características que simplemente son imposibles de encontrar en un equipamiento para consumidores.

Así, puede comenzar con cualquiera de los dos ejemplos anteriores e implementar una red inalámbrica privada donde los usuarios son autentificados utilizando un navegador web estándar. Mediante el uso de un portal cautivo como el ***Chillispot***, se pueden verificar las credenciales de los

usuarios inalámbricos en una base de datos (por ejemplo, un servidor de dominios Windows accesible vía RADIUS). Este arreglo puede permitir un acceso preferencial a los usuarios existentes en la base de datos, al mismo tiempo que se permite un nivel de acceso muy limitado para el público en general.

Otra aplicación muy popular es el modelo comercial preparado. En el mismo, los usuarios deben adquirir un pase antes de acceder a la red. Este pase provee una contraseña que tiene validez por una cantidad de tiempo limitada (generalmente un día). Cuando el pase expira, el usuario debe comprar otro. Esta característica solamente está disponible en equipamientos de redes relativamente caros, pero puede implementarse usando un software libre como el Chillispot y el phpMyPrePaid. Vamos a ver más sobre la tecnología de portal cautivo y los sistemas de pase en la sección **Autentificación** del capítulo seis.

Sistemas operativos amigables con la tecnología inalámbrica

Existen varios sistemas operativos de fuente abierta que proveen herramientas muy útiles para trabajar en redes inalámbricas. Estos fueron pensados para utilizarse en PCs recicladas con otro propósito, o con otro equipamiento de red (en lugar de una computadora portátil o un servidor), y están bien afinados para trabajar en la implementación de redes inalámbricas. Algunos de estos proyectos incluyen:

- **Freifunk.** Basado en el proyecto OpenWRT (*http://openwrt.org/*), el *firmware* Freifunk brinda un soporte a OLSR para puntos de acceso tipo consumidor basados en MIPS, tales como Linksys WRT54G / WRT54GS / WAP54G, Siemens SE505, y otros. Simplemente sustituyendo el *firmware* estándar de uno de esos AP con el *firmware* de Freifunk, podrá construir rápidamente una red *mesh* OLSR auto-formada. En este momento Freifunk no está disponible para arquitecturas de computadoras x86. Es mantenido por Sven Ola del grupo inalámbrico Freifunk en Berlín. Puede descargar el *firmware* desde *http://www.freifunk.net/wiki/FreifunkFirmware* .
- **Metrix Pebble.** El projecto Linux Pebble fue iniciado en el 2002 por Terry Schmidt del grupo NYCwireless. Originalmente, fue una versión de la distribución Linux Debian que incluye herramientas inalámbricas, cortafuego, administración del tráfico, y enrutamiento. Desde 2004, Metrix Communication ha estado extendiendo Pebble para incluir manejadores actualizados, monitoreo de ancho de banda, y herramientas de configuración basadas en la web. El objetivo de Metrix Pebble es proveer una plataforma completa para el desarrollo inalámbrico. Trabaja con equipamiento x86 con al menos 64MB de memoria *flash* o

almacenamiento de disco duro. Puede descargar Metrix Pebble desde *http://metrix.net/metrix/howto/metrix-pebble.html*.

- **m0n0wall.** Basado en FreeBSD, m0n0wall es un paquete cortafuego pequeño, pero muy completo, que provee servicios de AP. Se configura desde una interfaz web y la configuración completa del sistema es almacenada en un único archivo XML. Su reducido tamaño (menos de 6MB) lo hace atractivo para el uso en sistemas embebidos pequeños. Su objetivo es proveer un cortafuego seguro, y como tal no incluye herramientas para el espacio del usuario (no es posible registrarse en la máquina desde la red). Más allá de esta limitación, es una buena elección para los administradores de redes inalámbricas, particularmente aquellos con un conocimiento previo en FreeBSD. Puede descargar m0n0wall desde *http://www.m0n0.ch/*.

Todas estas distribuciones están diseñadas para adecuarse a computadoras con un almacenamiento limitado. Si usted está utilizando un disco *flash* muy grande o un disco duro, ciertamente puede instalar un SO más completo (como Ubuntu o Debian) y utilizar la computadora como enrutador o punto de acceso. De todas formas le va a tomar cierta cantidad de tiempo de desarrollo asegurarse de que todas las herramientas necesarias estén incluidas, evitando instalar paquetes innecesarios. Por medio de la utilización de uno de estos proyectos como punto de inicio para construir un nodo inalámbrico, ahorrará considerable tiempo y esfuerzo.

El Linksys WRT54G

En el mercado actual uno de los puntos de acceso más popular es el Linksys WRT54G. Este punto de acceso tiene dos conectores de antena externos RP-TNC, un conmutador Ethernet con cuatro puertos, y un radio 802.11b/g. Se configura a través de una simple interfaz web. Si bien no está diseñado para exteriores, puede instalarse en una caja adecuada para tal fin, o en un tubo de plástico, a un costo relativamente bajo. En este momento el WRT54G cuesta aproximadamente U$S 60.

En el 2003, los *hackers* se dieron cuenta de que el *firmware* que se vendía con WRT54G en realidad era una versión de Linux. Esto lprodujo un tremendo interés en construir un *firmware* adaptable que extendiera las capacidades del enrutador de forma significativa. Algunas de esas nuevas características incluyen el soporte del modo cliente en el radio, portales cautivos, y redes *mesh*. Dos buenas alternativas de paquetes de *firmware* para WRT54G son OpenWRT (http://openwrt.org/) y Freifunk (*http://www.freifunk.net/wiki/FreifunkFirmware*).

Desafortunadamente, a fines del 2005, Linksys sacó la versión 5 de WRT54G. Esta nueva versión del equipamiento eliminaba algo de memoria

RAM y de almacenamiento *flash* en la placa madre, haciendo prácticamente imposible correr Linux (se vende con VxWorks, un sistema operativo mucho más pequeño que no permite una fácil adaptación). Puesto que el WRT54G v5 no corre con el *firmware* adaptado basado en Linux, se volvió menos atractivo para los desarrolladores de redes. Linksys también desarrolló el WRT54GL, el cual es esencialmente el WRT54G v4 (que corre con Linux) con un precio ligeramente más alto.

Otros puntos de acceso Linksys corren Linux, incluyendo el WRT54GS y el WAP54G. Si bien también tienen unos precios relativamente bajos, las especificaciones de equipamiento pueden cambiar en cualquier momento. Sin abrir el paquete es difícil saber qué versión del equipamiento es usada, lo que hace riesgoso adquirirlos en una tienda y prácticamente imposible ordenarlos en línea. A pesar de que WRT54GL tiene garantía de correr con Linux, Linksys ha hecho saber que no espera vender este modelo en grandes volúmenes, y no queda claro por cuánto tiempo el mismo va a estar en venta.

Si puede encontrar una revisión anterior de WRT54G, o de WRT54GL, estos enrutadores son versátiles y baratos. Con un *firmware* de código abierto, pueden configurarse para funcionar como una *mesh* OLSR o en el modo cliente, y trabajan muy bien como una solución económica del lado del cliente. Aunque el nuevo modelo v5 funciona como punto de acceso, no puede ser configurado como cliente, y los usuarios que han publicado sus opiniones respecto a estos equipos han expresado reservas en comparación con el v4 y modelos anteriores.

Para más información, diríjase a uno de estos sitios web:

- *http://linksysinfo.org/*
- *http://seattlewireless.net/index.cgi/LinksysWrt54g*

6
Seguridad

En una red cableada tradicional, el control del acceso es muy sencillo: si una persona tiene acceso físico a una computadora o a un *hub* (concentrador) de la red, entonces pueden usar (o abusar) de los recursos de la red. Si bien los mecanismos a través de software son un componente importante de la seguridad de la red, el mecanismo decisivo es limitar el acceso físico a los dispositivos de la red. Es simple: si todas las terminales y los componentes de la red son accedidos sólo por personas de confianza, entonces la red puede ser considerada confiable.

Las reglas cambian significativamente en las redes inalámbricas. A pesar de que el alcance aparente de su punto de acceso puede ser de unos pocos cientos de metros, un usuario con una antena de gran ganancia puede ser capaz de hacer uso de su red aunque esté a varias manzanas de distancia. Aún cuando un usuario no autorizado sea detectado, es imposible "rastrear el cable" hasta el lugar donde está esa persona. Sin transmitir ni un sólo paquete, un usuario malintencionado puede registrar todos los datos de la red a un disco. Más adelante estos datos pueden utilizarse para lanzar un ataque más sofisticado contra la red. Nunca suponga que las ondas de radio simplemente "se detienen" en el límite de su propiedad.

Por supuesto, aún en las redes cableadas es casi imposible confiar por completo en todos los usuarios de la red. Un empleado descontento, un usuario con poca capacitación, así como una simple equivocación de un usuario honesto pueden causar daño significativo en las operaciones de la red. Como arquitecto de la red, su objetivo debe ser facilitar la comunicación privada entre los usuarios legítimos de la misma. Aunque en una red se necesita una cierta cantidad de control de acceso y de autenticación, habrá fallado en su función si a los usuarios legítimos de la red se les hace difícil utilizarla para comunicarse.

Según un viejo dicho, la única forma de mantener completamente segura una computadora es desenchufarla, ponerla dentro de una caja fuerte, destruir la llave y enterrarla bajo concreto. Si bien dicho sistema puede ser completamente "seguro", no es útil para la comunicación. Cuando tome decisiones de seguridad para su red, recuerde que por encima de todo, la red existe para que los usuarios puedan comunicarse unos con otros. Las consideraciones de seguridad son importantes, pero no deben interponerse en el camino de los usuarios.

Seguridad física

Cuando instala una red, usted está construyendo una infraestructura de la cual la gente dependerá y por lo tanto, la red debe ser confiable. Para la mayoría de los casos, las interrupciones en el servicio ocurren a menudo debido a alteraciones hechas por las personas, accidentalmente o no. Las redes son físicas, son cables y cajas, cosas que pueden ser modificadas fácilmente. En muchas instalaciones, puede ser que la gente no sepa qué tipo de equipamiento se ha instalado, o experimentan por pura curiosidad. Puede que no se den cuenta de la importancia de que un cable llegue a un puerto. Es posible que muevan un cable Ethernet para conectar su computadora portátil durante 5 minutos, o cambien de posición al conmutador porque les estorba. Un enchufe puede ser desconectado de una regleta porque alguien más necesita esa conexión. Asegurar la seguridad física de la instalación es un asunto prioritario. Las señales y las etiquetas le serán útiles a aquellos que saben leer, o que hablan su mismo idioma. Colocar el equipo fuera del camino, y limitar el acceso al mismo es el mejor medio para asegurarse de que no ocurran accidentes o se manipule el equipamiento.

En las economías menos desarrolladas no va a ser fácil encontrar los sujetadores, amarres o cajas apropiados. Sin embargo, podrá encontrar productos eléctricos equivalentes que funcionen igualmente bien. Los cerramientos a la medida también son sencillos de fabricar, y deben considerarse esenciales para cualquier instalación. A menudo es más económico pagar a un albañil para que haga las perforaciones e instale los conductos; a pesar de que ésta puede ser una opción cara en el mundo desarrollado, este tipo de actividad es accesible en los países del Sur. Se puede incrustar tubería de PVC en las paredes de cemento para pasar el cable de una habitación a otra, evitando hacer perforaciones cada vez que tenemos que pasar un cable. Para el aislamiento, se pueden rellenar los conductos alrededor del cable con bolsas de plástico.

El equipamiento pequeño debe montarse en la pared y el grande se debe colocar en un closet o en un armario.

Conmutadores (*switches*)

Los conmutadores, *hubs* o los puntos de acceso interiores pueden atornillarse directamente a la pared. Lo mejor es poner el equipo lo más alto posible para reducir las posibilidades de que alguien toque los dispositivos o sus cables.

Cables

Los cables deben esconderse y atarse. Es mejor enterrarlos que dejarlos colgando en un patio donde puedan ser usados para secar la ropa o simplemente enganchados con una escalera, etc. Para evitar alimañas o insectos consiga conductos plásticos para electricidad. El costo adicional le evitará molestias. Los conductos deben enterrarse aproximadamente a 30 cm de profundidad (o más abajo si el suelo se congela a mayor profundidad en climas extremos). También es recomendable comprar conductos de un calibre superior al mínimo necesario para que en el futuro otros cables que se requieran puedan pasarse por la misma tubería. Cuando se hacen instalaciones en edificios, también es posible encontrar conductos de plástico que pueden ser utilizados para pasar cables. De lo contrario, simplemente sujete los cables a la pared para asegurarse de que no queden expuestos en lugares donde puedan ser enganchados, pinchados o cortados.

Energía

Lo mejor es tener las zapatillas eléctricas (alargues, regletas, múltiples) dentro de un armario cerrado. Si esto no es posible colóquelas debajo de un escritorio o en la pared y utilice cinta adhesiva fuerte para asegurar el enchufe a la conexión de la pared. No deje espacios libres en la zapatilla eléctrica ni en la UPS, tápelas con cinta si es necesario. La gente va a tender a utilizar la conexión que esté más a su alcance, por lo tanto hágalas difíciles de usar. Si no lo hace, puede encontrarse con un ventilador o una lámpara enchufada en su UPS; aunque es bueno tener luz ¡es aún más importante mantener su servidor en funcionamiento!

Agua

Proteja su equipo del agua y de la humedad. En todos los casos asegúrese de que su equipo, incluida su UPS, está al menos a 30cm. del piso para evitar daños por posibles inundaciones. También intente tener una cubierta sobre su equipo, para que de esta forma el agua y la humedad no caigan sobre él. En los climas húmedos es importante que el equipamiento tenga la ventilación adecuada para asegurarse de que se va a eliminar la humedad.

Los armarios pequeños deben tener ventilación, o de lo contrario la humedad y el calor pueden degradar o aún destruir su equipamiento.

Mástiles y torres

El equipo instalado en un mástil o torre a menudo está a salvo de los ladrones. No obstante, para disuadirlos y mantener su equipo a salvo del viento es bueno sobre-estructurar estos montajes. Los equipos que se monten sobre la torre o mástil deben pintarse de colores apagados, blanco o gris mate para reflejar el sol, así como para desviar la atención, haciéndolo lucir poco interesante. Las antenas tipo panel son mucho más sutiles que los platos y por eso debemos preferirlas. Todas las instalaciones en las paredes deberán estar a una altura tal, que se requiera de una escalera para alcanzarlas. Intente elegir lugares bien iluminados pero no muy prominentes para poner el equipo. También evite las antenas que se parezcan a las de televisión, porque esas pueden atraer el interés de los ladrones, mientras que una antena WiFi no va a ser de utilidad para la mayoría de ellos.

Amenazas a la red

Una diferencia esencial entre las redes Ehernet y las inalámbricas es que estas últimas se construyen en un ***medio compartido***. Se parecen más a los viejos concentradores de red que a los conmutadores modernos, en ellas cada computadora conectada a la red puede "ver" el tráfico de todos los otros usuarios. Para monitorear todo el tráfico de la red en un punto de acceso, uno puede simplemente sintonizar el canal que se está utilizando, colocar la tarjeta de red en el modo de monitoreo, y registrar cada paquete. Estos datos pueden ser de mucho valor para alguien que los escucha a escondidas (incluyendo datos como el correo electrónico, datos de voz o registros de conversaciones en línea). Esto también puede proveer contraseñas y otros datos de gran valor, posibilitando que la red se vea comprometida en el futuro. Como veremos más adelante en este capítulo, este problema puede mitigarse con el uso de la encriptación.

Otro problema serio de las redes inalámbricas es que los usuarios son relativamente ***anónimos***. Todos los dispositivos inalámbricos incluyen una dirección MAC única, la cual es asignada por el fabricante, pero esas direcciones a menudo pueden ser modificadas con ciertos programas. Aún teniendo la dirección MAC, puede ser muy difícil identificar donde está localizado físicamente un usuario inalámbrico. Los efectos del eco, las antenas de gran ganancia, y una amplia variedad de características de los transmisores de radio, pueden hacer que sea imposible determinar si un usuario malintencionado está en el cuarto de al lado o en un lujar muy alejado.

Si bien el espectro sin licenciamiento implica grandes ahorros económicos para el usuario, por otro lado tiene el desafortunado efecto colateral de que los ataques de ***denegación del servicio*** (***DoS*** *por su sigla en inglés*) son extremadamente simples. Simplemente con encender un punto de acceso de alta potencia, un teléfono inalámbrico, un transmisor de video, o cualquier otro dispositivo de 2.4 GHz, una persona con malas intenciones puede causar problemas significativos a la red. Muchos dispositivos de red son vulnerables también a otras formas de ataques de denegación del servicio, tales como una avalancha de desasociaciones (*disassociation flooding*) y el desborde de las tablas ARP.

Les presentamos varias categorías de personas que pueden causar problemas a una red inalámbrica:

- ***Usuarios involuntarios.*** Como la mayoría de las redes inalámbricas están instaladas en áreas muy pobladas, es común que los usuarios de computadoras portátiles se asocien accidentalmente a la red equivocada. La mayoría de los clientes va a elegir cualquier red disponible si la de su preferencia no lo está. Los usuarios pueden hacer uso de esta red como lo hacen habitualmente, ignorando completamente que pueden estar transmitiendo datos importantes en la red de alguien más. Las personas malintencionadas pueden aprovechar esta situación instalando puntos de acceso en lugares estratégicos, para intentar atacar usuarios desprevenidos y capturar sus datos.

  El primer paso para evitar este problema es educar a sus usuarios, y subrayar la importancia de conectarse solamente a redes conocidas y de confianza. Muchos clientes inalámbricos pueden configurarse para conectarse solamente a redes confiables, o para pedir permiso antes de incorporarse a una nueva red. Como veremos más adelante en este capítulo los usuarios pueden conectarse de forma segura a redes públicas abiertas utilizando una encriptación fuerte.

- W***ar drivers.*** El fenómeno de los "*war drivers*" (buscadores de redes) basa su nombre en la famosa película sobre piratas informáticos de 1983, "Juegos de Guerra" (*War Games*). Ellos están interesados en encontrar la ubicación física de las redes inalámbricas. En general se mueven por la ciudad equipados con una computadora portátil, un GPS, y una antena omnidireccional, registrando el nombre y la ubicación de cada red que localizan. Luego se combinan esos registros con los de otros buscadores de redes transformándose en mapas gráficos describiendo las "huellas" inalámbricas de una ciudad.

  La amplia mayoría de los buscadores de redes no representa una amenaza directa a la red, pero los datos que recolectan pueden ser de interés para aquellos que se dedican a *atacar* redes. Por ejemplo, un punto de acceso desprotegido detectado de esta manera, puede estar

ubicado en un edificio importante, como una oficina de gobierno o de una empresa. Una persona con malas intenciones puede utilizar esta información para acceder a esa red ilegalmente. La instalación de ese AP nunca debió haber sucedido en primer lugar, pero los buscadores de redes hacen más urgente la solución de este problema. Como veremos más adelante en este capítulo, los buscadores de redes que utilizan el famoso programa NetStumbler pueden ser detectados con otros programas como el Kismet. Para más información acerca de los buscadores de redes, vea los sitios *http://www.wifimaps.com/*, *http://www.nodedb.com/*, o *http://www.netstumbler.com*.

- ***Puntos de acceso deshonestos.*** Hay dos clases generales de puntos de acceso deshonestos: aquellos instalados incorrectamente por usuarios legítimos, y los instalados por gente malintencionada que piensa en recolectar datos o dañar la red. En el caso más sencillo, un usuario legítimo de la red, puede querer una mejor cobertura inalámbrica en su oficina, o puede que encuentre demasiado difíciles de cumplir las restricciones de seguridad de la red inalámbrica corporativa. Al instalar un punto de acceso sin autorización, el usuario abre la red desde el interior de la misma a los ataques potenciales. Si bien existe la posibilidad de rastrear a través de la red puntos de acceso no autorizados, es muy importante tener una política clara que los prohíba.

  Puede que sea muy difícil lidiar con la segunda clase. Al instalar un AP de gran potencia que utilice el mismo ESSID de la red, una persona puede engañar a la gente para que use este equipo y registrar o manipular todos los datos que pasan por él. Repetimos, si sus usuarios están entrenados para usar una fuerte encriptación, este problema se va a reducir de forma significativa.

- ***Escuchas Subrepticias.*** Como mencionamos antes, este es un problema muy difícil de manejar en las redes inalámbricas. Utilizando una herramienta de monitoreo pasiva (como Kismet), un fisgón puede registrar todos los datos de la red desde lejos sin que ni siquiera se note su presencia. Los datos encriptados pobremente simplemente pueden registrarse y luego descifrarse, mientras que los datos sin encriptación se pueden leer fácilmente en tiempo real.

  Si a usted le es difícil convencer a otros de este problema, puede realizar una demostración con herramientas como Etherpeg o Driftnet (*http://www.etherpeg.org/* o *http://www.ex-parrot.com/~chris/driftnet/*). Estas herramientas buscan datos gráficos en redes inalámbricas, tales como archivos GIF y JPEG. Mientras que los usuarios están navegando en Internet, estas herramientas despliegan todos los gráficos encontrados en un collage. A menudo utilizo estas herramientas cuando estoy dando una charla de seguridad inalámbrica. Usted le puede decir a un usuario que su correo electrónico es vulnerable si no tiene encriptación, pero nada les hace llegar mejor el mensaje que mostrarles las imágenes que están

buscando en su navegador web. Si bien no puede ser prevenido por completo, el uso de una fuerte encriptación va a desalentar las escuchas ***subrepticias***.

Esta introducción está pensada para darle una idea de los problemas a los que usted tiene que enfrentarse cuando diseña una red inalámbrica. Más adelante, vamos a presentarle herramientas y técnicas que lo ayudarán a mitigarlos.

Autenticación

Antes de tener acceso a los recursos de la red, los usuarios deben ser ***autenticados***. En un mundo ideal, cada usuario inalámbrico debería tener un identificador personal que fuera único, inmodificable e imposible de suplantar por otros usuarios. Este es un problema muy difícil de resolver en el mundo real.

Lo más cercano a tener un identificador único es la dirección MAC. Este es un número de 48-bits asignado por el fabricante a cada dispositivo inalámbrico y Ethernet. Empleando un ***filtro mac*** en nuestro punto de acceso, podemos autentificar a los usuarios mediante su dirección MAC. Con este método el punto de acceso, mantiene una tabla de direcciones MAC aprobadas. Cuando un usuario intenta asociarse a un punto de acceso, la dirección MAC del cliente debe estar en la lista aprobada, o de lo contrario la asociación va a ser rechazada. Como una alternativa, el AP puede tener una tabla de direcciones MAC "prohibidas", y habilitar a todos los dispositivos que no están en esa lista.

Desafortunadamente, este no es un mecanismo de seguridad ideal. Mantener las tablas MAC en cada dispositivo puede ser muy engorroso, requiriendo que todos los dispositivos cliente tengan su dirección MAC grabadas y cargadas en los AP. Además, las direcciones MAC a menudo pueden modificarse mediante software. Si un atacante determinado observa las direcciones MAC que están en uso en una red inalámbrica, él puede "suplantar" una dirección MAC aprobada y asociarse con éxito al AP. A pesar de que el filtro MAC va a evitar que los usuarios involuntarios y los curiosos accedan a la red, el filtro MAC por si solo no puede proteger su red de los atacantes empecinados.

Los filtros MAC son útiles para limitar temporalmente el acceso de usuarios que actúan de forma incorrecta. Por ejemplo, si una computadora portátil tiene un virus que envía grandes cantidades de tráfico no deseado, su dirección MAC puede agregarse a la tabla de filtrado para detener el tráfico de forma inmediata. Esto le dará tiempo para ubicar al usuario y arreglar el problema.

Otra forma popular de autenticación de las redes inalámbricas es la llamada ***red cerrada***. En una red común, los AP transmiten sus ESSID muchas veces por segundo, permitiéndoles a los clientes (así como a las herramientas como NetStumbler) encontrar la red y mostrar su presencia al usuario. En una red cerrada, el AP no transmite el ESSID, y los usuarios deben conocer el nombre completo de la red antes de que el AP les permita asociarse. Esto evita que los usuarios casuales descubran la red y la seleccionen en su cliente de red inalámbrica.

Con esta característica hay varios inconvenientes. Forzar a los usuarios a escribir el ESSID completo antes de conectarse a la red, amplía las posibilidades de error y a menudo resulta en solicitudes de soporte y quejas. La red no será detectada por herramientas como NetStumbler, y esto puede prevenir que la misma aparezca en los mapas de los *war drivers*. Pero esto también significa que otros instaladores de redes tampoco pueden encontrar su red con facilidad, y no van a saber que usted está usando un canal dado. Un vecino podría realizar un estudio del lugar, y al no detectar redes cercanas podría instalar su propia red en el mismo canal que usted está utilizando, lo cual va a provocarle problemas de interferencia tanto a usted como a su vecino.

Finalmente, utilizar redes cerradas ofrece poca seguridad adicional a su red. Utilizando herramientas de monitoreo pasivas (como Kismet), un usuario experimentado puede detectar paquetes enviados desde sus clientes legítimos al AP. Esos paquetes necesariamente contienen el nombre de la red. Y por lo tanto, un malintencionado puede usarlo luego para asociarse, al igual que lo haría un usuario normal.

Probablemente la encriptación sea la mejor herramienta que tenemos para autenticar a los usuarios de la red. Mediante una fuerte encriptación, podemos identificar a un usuario de una forma única difícil de suplantar, y usar esa identidad para determinar accesos futuros a la red. La encriptación también tiene el beneficio de ofrecer una capa de privacidad adicional ya que evita que los fisgones tengan un acceso fácil al tráfico de la red.

El método de encriptación más utilizado en las redes inalámbricas es el llamado ***encriptación WEP***. WEP ***significa privacidad equivalente*** a la cableada (*del inglés Wired Equivalent Privacy*), y es soportada por casi todo el equipamiento 802.11a/b/g. WEP utiliza una clave compartida de 40-bits para encriptar los datos entre el punto de acceso y el cliente. La clave debe ingresarse en los AP así como en cada uno de los clientes. Cuando se habilita WEP, los clientes no pueden asociarse con el AP hasta que utilicen la clave correcta. Un fisgón oyendo una red con WEP igual puede ver el tráfico y las direcciones MAC, pero los mensajes de los datos de cada paquete están encriptados. Esto provee a la red de un buen mecanismo de autenticación, además de darle un poco de privacidad.

WEP definitivamente no es la mejor solución de encriptación que haya disponible. Por un lado, la clave WEP se comparte entre todos los usuarios, y si la misma está comprometida (es decir, si un usuario le dice a un amigo la contraseña, o se va un empleado) entonces cambiar la contraseña puede ser extremadamente difícil, ya que todos los AP y los dispositivos cliente deben cambiarla. Esto también significa que los usuarios legítimos de la red pueden escuchar el tráfico de los demás, ya que todos conocen la clave.

A menudo la clave es seleccionada sin mucho cuidado, haciendo posibles los intentos de ataques fuera de línea. Aún peor, varias versiones de WEP son vulnerables mediante técnicas conocidas, haciendo aún más fácil atacar algunas redes. Algunos fabricantes han implementado varias extensiones a WEP (como claves más largas y esquemas rápidos de rotación), pero esas extensiones no son parte del estándar, de tal manera que no van a funcionar correctamente entre equipamientos de diferentes fabricantes. Actualizando al *firmware* más reciente en todos sus dispositivos inalámbricos, puede prevenir alguno de los primeros ataques conocidos a WEP.

Pese a lo anterior, WEP puede ser una herramienta útil de autenticación. Confiando en que sus usuarios no van a difundir la contraseña, puede estar casi seguro de que sus clientes de red inalámbrica son legítimos. Los ataques a WEP están fuera del alcance de la mayoría de los usuarios. WEP es extremadamente útil para asegurar enlaces punto a punto a larga distancia, aún en redes abiertas. Si utiliza WEP en dicho enlace, desalentará que otras personas se asocien al enlace, y probablemente escojan otro AP. Definitivamente WEP es una señal de "manténgase afuera" para su red. Cualquiera que detecte la red va a ver que se requiere una clave, dejándole claro que no es bienvenido.

La mayor fortaleza de WEP es su interoperabilidad. Para cumplir con los estándares, todos los dispositivos inalámbricos soportan un WEP básico. Si bien no es el método más fuerte disponible, ciertamente es la característica implementada más comúnmente. Más adelante vamos a ver otras técnicas de encriptación más avanzadas.

Para obtener más detalles sobre el estado de la encriptación WEP, vea estos artículos:

- *http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html*
- *http://www.cs.umd.edu/~waa/wireless.pdf*
- *http://www.crypto.com/papers/others/rc4_ksaproc.ps*

Otro protocolo de autenticación en la capa de enlace de datos es el **Acceso Protegido Wi-Fi**, o ***WPA*** (***Wi-Fi Protected Access*** *por su sigla en inglés*). WPA se creó específicamente para lidiar con los problemas de WEP que

mencionamos antes. Provee un esquema de encriptación significativamente más fuerte, y puede utilizar una clave privada compartida, claves únicas asignadas a cada usuario, o inclusive un certificado SSL para autenticar el punto de acceso y el cliente. Las credenciales de autenticación se chequean usando el protocolo 802.1X, el cual puede consultar una base de datos externa como RADIUS. Mediante el uso de un Protocolo de Integridad Temporal de la Clave (*TKIP –Temporal Key Integrity Protocol*), las claves se pueden rotar rápidamente, reduciendo la posibilidad de que una sesión en particular sea descifrada. En general, WPA provee una autenticación y privacidad significativamente mejor que el estándar WEP.

El problema con WPA, a la fecha de publicación de este libro, es que la interoperabilidad entre los vendedores es aún muy baja. WPA requiere equipamiento de última generación para los puntos de acceso, y *firmware* actualizado en todos los clientes inalámbricos, así como una configuración laboriosa. Si usted controla la totalidad de la plataforma de equipamiento del lugar donde está realizando la instalación, WPA puede ser ideal. La autenticación de los clientes y de los AP, resuelve los problemas de puntos de acceso deshonestos y provee muchas más ventajas que WEP. Pero en la mayoría de las instalaciones de red donde el equipamiento es variado y el conocimiento de los usuarios es limitado, instalar WPA puede ser una pesadilla. Por esta razón es que la mayoría continua utilizando WEP, si es que usa algún tipo de encriptación.

Portales cautivos

Una herramienta común de autenticación utilizada en las redes inalámbricas es el ***portal cautivo***. Este utiliza un navegador web estándar para darle al usuario la posibilidad de presentar sus credenciales de registro. También puede utilizarse para presentar información (como Política de Uso Aceptable) a los usuarios antes de permitir el acceso. Mediante el uso de un navegador web en lugar de un programa personalizado de autenticación, los portales cautivos funcionan en prácticamente todas las computadoras portátiles y sistemas operativos. Generalmente se utilizan en redes abiertas que no tienen otro método de autenticación (como WEP o filtros MAC).

Para comenzar, el usuario abre su computadora portátil y selecciona la red. Su computadora solicita una dirección mediante DHCP y le es otorgada. Luego usa su navegador web para ir a cualquier sitio en Internet.

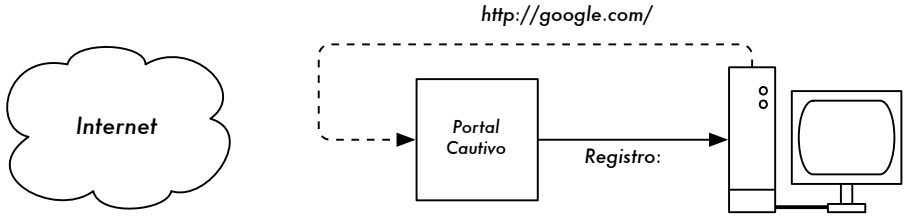


Figura 6.1: El usuario solicita una página web y es redireccionado.

En lugar de recibir la página solicitada, al usuario se le presenta una pantalla de registro. Esta página puede solicitarle al usuario que ingrese su nombre de usuario y una contraseña, simplemente oprime el botón de "registro"(*login*), escribe los números de una tarjeta prepago, o ingresa cualquier otra credencial que solicite el administrador de red. El punto de acceso u otro servidor en la red verifica los datos. Cualquier otro tipo de acceso a la red se bloquea hasta que se verifiquen las credenciales.

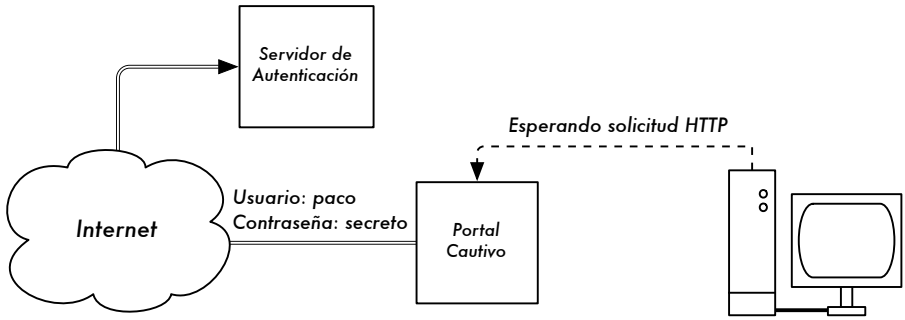


Figura 6.2: Las credenciales se verifican antes de brindar acceso al resto de la red. El servidor de autenticación puede ser el punto de acceso mismo, otra computadora en la red local, o un servidor en cualquier lugar del Internet.

Una vez que el usuario ha sido autenticado, se le permite el acceso a los recursos de la red, y en general es redireccionado al sitio web que solicitó originalmente.

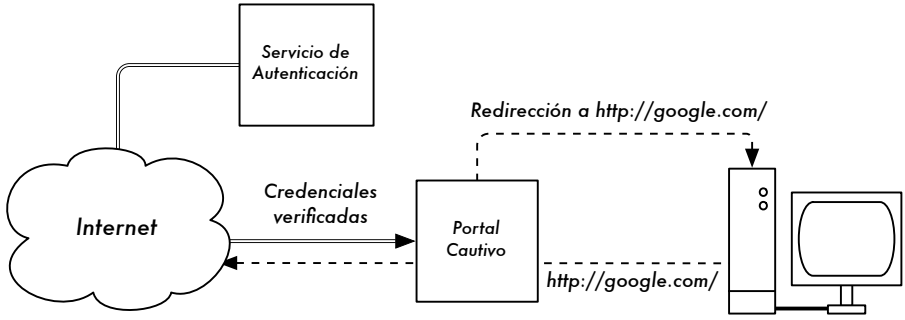


Figura 6.3: Después de que el usuario es autenticado, se le permite el acceso al resto de la red.

Los portales cautivos no proveen encriptación para los usuarios de redes inalámbricas, en su lugar confían en las direcciones MAC e IP del cliente como identificadores únicos. Si bien esto no es necesariamente muy seguro, muchas implementaciones van a solicitar que el usuario se re-autentique periódicamente. Esto puede hacerse automáticamente, minimizando una ventana emergente (*pop-up*) del navegador, cuando el usuario se registra por primera vez.

Debido a que no proveen una fuerte encriptación, los portales cautivos no son una buena elección para aquellas redes que requieren una protección fuerte y limiten el acceso solamente a usuarios confiables. En realidad se adaptan mejor para cafés, hoteles y otros lugares de acceso público donde se esperan usuarios casuales de la red.

En redes públicas o semipúblicas, las técnicas de encriptación como WEP y WPA son realmente inútiles. Simplemente no hay forma de distribuir claves públicas o compartidas para el público en general sin comprometer la seguridad de esas claves. En esas instalaciones, una simple aplicación como un portal cautivo provee un nivel de servicio intermedio entre completamente abierto y completamente cerrado.

Dos implementaciones de portales cautivos de fuente abierta son NoCatSplash y Chillispot.

NoCatSplash

Si usted simplemente necesita proveer a los usuarios de una red abierta con información y la política de uso aceptable, preste atención a NoCatSplash. El mismo está disponible en *http://nocat.net/download/NoCatSplash/*.

NoCatSplash provee una página de ingreso modificable, solicitándoles a sus usuarios presionar el botón de “registro” antes de utilizar la red. Esto es útil para identificar los operadores de la red y mostrar las reglas de acceso a la misma.

NoCatSplash está escrito en C, y va a correr en casi cualquier sistema operativo tipo Unix incluidos Linux, BSD, y también plataformas embebidas como OpenWRT. Tiene un archivo de configuración muy simple y puede usar cualquier archivo HTML personalizado como la página de ingreso. En general se corre directamente en un punto de acceso, pero también funciona en un enrutador o un servidor *proxy*. Para más información, vea la página *http://nocat.net/*.

Otros proyectos populares relacionados con *hotspots*

NoCatSplash es una implementación simple de portal cautivo. Existen muchas otras implementaciones gratuitas que soportan diversos rangos de funcionalidad. Algunas de ellas incluyen:

- Chillispot (*http://www.chillispot.org/*). Chillispot es un portal cautivo diseñado para autenticar verificando los datos contra una base de datos de credenciales de usuarios, tal como RADIUS. Si lo combinamos con la aplicación phpMyPrePaid, se puede implementar fácilmente un sistema de autenticación basado en pre-pago. phpMyPrePaid se puede descargar desde *http://sourceforge.net/projects/phpmyprepaid/*.
- WiFi Dog (*http://www.wifidog.org/*). WiFi Dog provee un paquete muy completo de autenticación vía portal cautivo, en muy poco espacio (generalmente menos de 30kB). Desde la perspectiva del usuario, no requiere de una ventana emergente (*pop-up*) ni de soporte javascript, permitiéndole trabajar en una amplia variedad de dispositivos inalámbricos.
- m0n0wall (*http://m0n0.ch/wall/*). Como mencionamos en el capítulo cinco, m0n0wall es un sistema operativo embebido completo basado en FreeBSD. Este incluye un portal cautivo con soporte RADIUS, así como un servidor web PHP.

Privacidad

La mayoría de los usuarios son dichosamente ignorantes de que su correo electrónico privado, conversaciones en línea, y aún sus contraseñas a menudo son enviados “al descubierto” por docenas de redes inseguras antes de llegar a su destino en Internet. No obstante lo errados que pueden estar, en general, los usuarios tienen expectativas de un poco de privacidad cuando usan redes de computadoras.

La privacidad se puede lograr, aún en redes inseguras como los puntos de acceso público e Internet. El único método efectivo probado para proteger la privacidad es el uso de una ***encriptación*** fuerte ***de extremo a extremo***.

Las técnicas de encriptación como WEP y WPA intentan mantener la privacidad en la capa dos, la capa de enlace de datos. Aunque éstas nos protegen de los fisgones en la conexión inalámbrica, la protección termina en el punto de acceso. Si el cliente inalámbrico usa protocolos inseguros (como POP o SMTP para recibir y enviar correos electrónicos), entonces los usuarios que están más allá del AP pueden registrar la sesión y ver los datos importantes. Como mencionamos antes, WEP también tiene la debilidad de

utilizar claves privadas compartidas. Esto significa que los usuarios legítimos de la red pueden escucharse unos a otros, ya que todos conocen la clave privada.

Utilizando encriptación en el extremo remoto de la conexión, los usuarios pueden eludir completamente el problema. Estas técnicas funcionan muy bien aún en redes públicas, donde los fisgones están oyendo y posiblemente manipulando los datos que vienen del punto de acceso.

Para asegurar la privacidad de los datos, una buena encriptación de extremo a extremo debe ofrecer las siguientes características:

- ***Autenticación verificada del extremo remoto.*** El usuario debe ser capaz de conocer sin ninguna duda que el extremo remoto es el que dice ser. Sin autenticación, un usuario puede darle datos importantes a cualquiera que afirme ser el servicio legítimo.
- ***Métodos fuertes de encriptación.*** El algoritmo de encriptación debe ser puesto al escrutinio del público, y no debe ser fácil de descifrar por un tercero. El uso de métodos de encriptación no publicados no ofrece seguridad, y una encriptación fuerte lo es aún más si el algoritmo es ampliamente conocido y sujeto a la revisión de los pares. Un buen algoritmo con una clave larga y adecuadamente protegida, puede ofrecer encriptación imposible de romper aunque hagamos cualquier esfuerzo utilizando la tecnología actual.
- ***Criptografía de clave pública.*** Aunque no es un requerimiento absoluto para la encriptación de extremo a extremo, el uso de criptografía de clave pública en lugar de una clave compartida, puede asegurar que los datos personales de los usuarios se mantengan privados, aún si la clave de otro usuario del servicio se ve comprometida. Esto también resuelve ciertos problemas con la distribución de las claves a los usuarios a través de una red insegura.
- ***Encapsulación de datos.*** Un buen mecanismo de encriptación de extremo a extremo protege tantos datos como sea posible. Esto puede ir desde encriptar una sencilla transacción de correo electrónico, a encapsular todo el tráfico IP, incluyendo búsquedas en servidores DNS y otros protocolos de soporte. Algunas herramientas de encriptación proveen un canal seguro que también pueden utilizar otras aplicaciones. Esto permite que los usuarios corran cualquier programa que ellos quieran y aún tengan la protección de una fuerte encriptación, aunque los programas no la soporten directamente.

Note que la legislación sobre el uso de encriptación varía ampliamente de lugar en lugar. Algunos países pueden llegar a equiparar el uso de encriptación con el uso de armamento o municiones, y pueden requerir un

permiso, exigir la custodia de las claves privadas o prohibir su uso por completo. Antes de implementar cualquier solución que implique encriptación verifique que el uso de esta tecnología esté permitido en su comunidad.

En las siguientes secciones vamos a examinar algunas herramientas específicas que proveen una buena protección para los datos de sus usuarios.

SSL

La tecnología de encriptación de extremo a extremo más accesible es ***Secure Socket Layer*** conocida simplemente como ***SSL*** *por su sigla en inglés*. Incluida en casi todos los navegadores web, SSL utiliza criptografía de clave pública e ***infraestructura de clave pública confiable*** (***PKI*** *por su sigla en inglés*), para asegurar las comunicaciones de datos en la web. Cada vez que visita la URL de una web que comienza con https, está usando SSL.

La implementación SSL provista en los navegadores web incluye un conjunto de certificados de fuentes confiables, denominados ***autoridades certificadoras*** (***CA***). Estos certificados son claves criptográficas que se utilizan para verificar la autenticidad de los sitios web. Cuando usted navega en un sitio que utiliza SSL, el navegador y el servidor primero intercambian certificados. Luego el navegador verifica que el certificado brindado por el servidor concuerde con el nombre en su servidor DNS, que no haya expirado, y que esté firmado por una autoridad certificadora confiable. Opcionalmente el servidor verifica la identidad del certificado del navegador. Si los certificados son aprobados, el navegador y el servidor negocian la clave de sesión maestra utilizando los certificados intercambiados anteriormente para protegerla. Dicha clave se usa para encriptar todas las comunicaciones hasta que el navegador se desconecte. Este tipo de encapsulamiento de datos es conocido como ***túnel***.

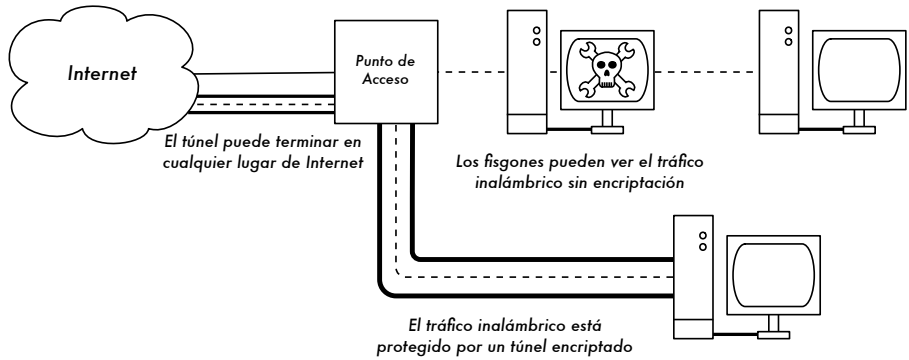


Figura 6.4: Los fisgones deben romper la encriptación para monitorear el tráfico dentro de un túnel encriptado. La conversación dentro del túnel es igual a cualquier otra conversación sin encriptar.

El uso de certificados con una PKI no solo protege a la comunicación de los fisgones, sino que también evita los ataques del llamado ***hombre en el medio*** (***MITM*** *por su sigla en inglés*). En un ataque del hombre en el medio, un usuario mal intencionado intercepta una comunicación entre el navegador y el servidor. Presentándoles certificados falsos a ambos, puede mantener dos sesiones encriptadas al mismo tiempo. Puesto que este usuario conoce el secreto de ambas conexiones, es trivial observar y manipular los datos que están pasando entre el servidor y el navegador.

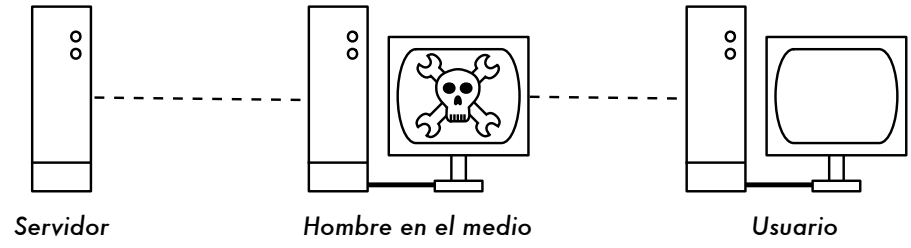


Figura 6.5: El hombre en el medio controla de forma efectiva todo lo que el usuario ve, y puede grabar y manipular todo el tráfico. Sin una infraestructura de clave pú-blica para verificar la autenticidad de las claves, la encriptación fuerte por si sola no podría protegernos de este tipo de ataque.

El uso de una buena PKI previene este tipo de ataque. Para tener éxito el usuario con malas intenciones debería presentar un certificado al cliente, que estuviera firmado por una autoridad certificadora. A menos que la CA haya sido comprometida (muy poco probable) o que el usuario pueda ser engañado para aceptar el certificado falso, este tipo de ataque es infructuoso. Es por esto que es de vital importancia que los usuarios comprendan que ignorar los avisos sobre los certificados vencidos o falsos es muy peligroso, especialmente cuando usamos redes inalámbricas. Pulsando el botón “ignorar” cuando son avisados por su navegador, los usuarios se abren a una cantidad de ataques potenciales.

SSL no sólo se utiliza para navegar en la web. Los protocolos de correo electrónico como IMAP, POP, y SMTP (que son bastante inseguros) pueden asegurarse envolviéndolos en un túnel SSL. La mayoría de los clientes de correo electrónico actuales soportan IMAPS y POPS (IMAP y POP seguros), así como SMTP protegido con SSL/TLS. Si su servidor de correo no provee soporte SSL, de todas formas puede asegurarlo con SSL utilizando un paquete como Stunnel (*http://www.stunnel.org/*). SSL puede utilizarse para asegurar de forma efectiva casi cualquier servicio que corra sobre TCP.

SSH

La mayoría de la gente considera SSH como un sustituto para **`telnet`** que provee seguridad, porque **`scp`** y **`sftp`** son los equivalentes seguros de rcp y

ftp. Pero SSH es mucho más que un acceso remoto a consola encriptado. Al igual que SSL, utiliza una fuerte criptografía de clave pública para verificar el servidor remoto y encriptar los datos. En lugar de PKI, utiliza una clave de impresión digital almacenada que se chequea antes de permitir la conexión. Puede usar contraseñas, claves públicas u otros métodos de autenticación de usuarios.

Mucha gente no sabe que SSH también puede actuar como un túnel de encriptación general o como un servidor proxy de encriptación. Estableciendo una conexión SSH en un lugar confiable cerca de (o en) un servidor remoto, los protocolos inseguros pueden protegerse de los fisgones y los ataques.

Esta técnica puede resultar algo avanzada para muchos usuarios, pero los desarrolladores de redes pueden utilizar SSH para encriptar el tráfico en enlaces inseguros, como los enlaces inalámbricos punto a punto. Como las herramientas son gratuitas y funcionan sobre el estándar TCP, los usuarios avanzados pueden implementar conexiones SSH por sí mismos, obteniendo su propia encriptación de extremo a extremo sin la intervención del administrador.

Probablemente OpenSSH (*http://openssh.org/*) sea la implementación más popular en las plataformas tipo Unix. Para Windows tenemos disponibles implementaciones gratuitas como Putty (*http://www.putty.nl/*) y WinSCP (*http://winscp.net/*). OpenSSH también corre en Windows bajo el paquete Cygwin (*http://www.cygwin.com/*). Los ejemplos a continuación suponen que usted está utilizando una versión reciente de OpenSSH.

Para establecer un túnel encriptado desde un puerto en la computadora local hasta un puerto en el extremo remoto se debe utilizar el parámetro **-L**. Por ejemplo, supongamos que usted quiere reenviar el tráfico del *proxy* web en un enlace encriptado al servidor squid en *squid.example.net*. El puerto de reenvío 3128 (el puerto *proxy* por omisión) utiliza este comando:

```
ssh -fN -g -L3128:squid.example.net:3128 squid.example.net
```

Las opciones **-fN** le ordenan a ssh que permanezca abierto en segundo plano después de conectarse. La opción **-g** permite a otros usuarios en su segmento local que se conecten a la computadora local, y la utilicen para la encriptación sobre el enlace inseguro. OpenSSH utilizará una clave pública para la autenticación si usted ya ha configurado una, o va a solicitarle su contraseña para conectarse al extremo remoto. Luego usted puede configurar su navegador web para conectarse al servidor local puerto 3128 como su servicio de proxy. Todo el tráfico web será encriptado antes de la transmisión al sitio remoto.

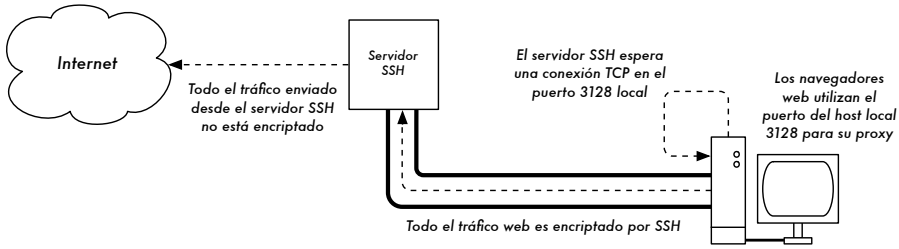


Figura 6.6: El túnel SSH protege el tráfico web hasta llegar al servidor SSH remoto.

SSH también puede funcionar como un proxy dinámico SOCKS4 o SOCKS5. Esto le permite crear un proxy web encriptador sin la necesidad de instalar squid. Tenga en cuenta que éste no será un proxy con memoria intermedia (cache), simplemente encripta todo el tráfico.

```
ssh -fN -D 8080 remote.example.net
```

Configure su navegador web para utilizar SOCKS4 o SOCKS5 en el puerto local 8080, y listo.

SSH puede encriptar datos en cualquier puerto TCP, incluyendo puertos utilizados para el correo electrónico. También puede comprimir los datos, lo que puede hacer disminuir el tiempo de recuperación de datos (latencia) en enlaces de baja capacidad.

```
ssh -fNCg -L110:localhost:110 -L25:localhost:25 mailhost.example.net
```

La opción **-C** habilita la compresión. Especificando múltiples veces la opción **-L** se pueden agregar tantas reglas de redirección de puertos como quiera. Tenga en cuenta que para vincularse a un puerto local inferior a 1024, debe tener privilegios de administrador (root) en la máquina local.

Estos son solo algunos ejemplos de la flexibilidad de SSH. Al implementar claves públicas y utilizar el agente de reenvío ssh, puede automatizarse la creación de túneles encriptados a través de la red inalámbrica, y proteger nuestras comunicaciones con una fuerte encriptación y autenticación.

OpenVPN

OpenVPN es una implementación VPN gratuita de fuente abierta construida con encriptación SSL. Existen versiones para un amplio rango de sistemas operativos, incluyendo Linux, Windows 2000/XP y superiores, OpenBSD, FreeBSD, NetBSD, Mac OS X, y Solaris. Una VPN encapsula todo el tráfico (incluyendo DNS y todos los otros protocolos) en un túnel encriptado, no un solo puerto TCP. La mayoría de la gente lo encuentra considerablemente más sencillo de comprender y configurar que IPSEC.

OpenVPN también tiene algunas desventajas, como por ejemplo una latencia bastante alta. Cierta cantidad de latencia no se puede evitar porque toda la encriptación/desencriptación se hace en el entorno de usuario, pero si se utilizan computadoras relativamente nuevas en cada extremo del túnel puede minimizarla. Si bien puede usar las tradicionales claves compartidas, OpenVPN se destaca realmente cuando se usa con certificados SSL y una autoridad certificadora confiable. OpenVPN tiene algunas ventajas que lo hace una buena opción para proveer seguridad de extremo a extremo.

- Se basa en un protocolo de encriptación robusto y probado (SSL y RSA)
- Es relativamente fácil de configurar
- Funciona en muchas plataformas diferentes
- Está bien documentado
- Es gratuito y de fuente abierta

Al igual que SSH y SSL, OpenVPN necesita conectarse a un puerto TCP único en el extremo remoto. Una vez establecido, puede encapsular todos los datos en la capa de red, o en la capa de enlace de datos, según sus requerimientos. Lo puede utilizar para crear conexiones VPN robustas entre máquinas individuales o simplemente utilizarlo para conectar enrutadores en redes inalámbricas inseguras.

La tecnología VPN es un campo complejo, y está un poco más allá del alcance de esta sección. Es importante comprender dónde encajan las VPN en la estructura de su red, para proveer la mejor protección posible sin exponer a su organización a problemas involuntarios. Existen varios recursos en línea que se dedican a la instalación de OpenVPN en un servidor y un cliente, personalmente recomiendo este artículo del Linux Journal: *http://www.linuxjournal.com/article/7949*, así como el sitio oficial de CÓMO HACERLO: *http://openvpn.net/howto.html*

Tor y Anonimizadores

Básicamente, Internet es una red abierta basada en la confianza. Cuando usted se conecta a un servidor web en Internet, su tráfico pasa a través de muchos enrutadores diferentes, pertenecientes a una gran variedad de instituciones, corporaciones y personas. En principio, cualquiera de esos enrutadores tiene la posibilidad de observar de cerca sus datos, mirando como mínimo las direcciones de origen y destino, y muy a menudo el contenido de los datos. Aún si sus datos están encriptados por medio de un protocolo seguro, su proveedor de Internet puede monitorear la cantidad de datos y el origen y destino de los mismos. A menudo esto es suficiente para tener una idea clara de sus actividades en línea.

La privacidad y el anonimato son importantes y están unidas estrechamente. Hay muchas razones válidas para considerar proteger su privacidad ***ha-ciendo anónimo*** su tráfico en la red. Supongamos que usted quiere ofrecer conectividad a Internet a su comunidad, instalando varios puntos de acceso para que la gente se conecte. Tanto si usted les cobra por el acceso como si no, existe siempre el riesgo de que la gente utilice la red para alguna actividad ilegal en su país o región. Usted podría argumentar luego, en caso de verse envuelto en problemas legales, que esa acción ilegal no fue realizada por usted sino por cualquiera conectado a su red. Sin embargo, el problema legal puede evadirse elegantemente si no es técnicamente factible determinar adónde fue realmente dirigido su tráfico. ¿Y qué pasa con la censura en Internet? Publicar páginas web anónimamente puede ser necesario para evitar la censura del gobierno.

Existen herramientas que le permiten hacer anónimo su tráfico de formas relativamente sencillas. La combinación de ***Tor*** (*http://tor.eff.org/*) y ***Privoxy*** (*http://www.privoxy.org/*) es una forma poderosa de correr un servidor *proxy* local que pasa su tráfico de Internet a través de varios servidores dispersos por la red, dificultando seguir el rastro de la información. Tor puede activarse en un PC local bajo Microsoft Windows, Mac OSX, Linux y una variedad de BSDs, donde el tráfico se hace anónimo desde el navegador a esa máquina en particular. Tor y Privoxy también pueden instalarse en una pasarela (*gateway*), o también en un pequeño punto de acceso embebido (como el Linksys WRT54G) donde se provee anonimato automáticamente para todos los usuarios de la red.

Tor funciona haciendo rebotar repetidamente sus conexiones TCP a través de varios servidores esparcidos en Internet, y envuelve la información de enrutamiento en varias capas encriptadas (de ahí el término enrutamiento ***cebolla***), que se van quitando cuando el paquete se mueve por la red. Esto significa que, en cualquier punto en la red, la dirección de la fuente y la del destino no pueden relacionarse una con la otra. Esto hace que el análisis del tráfico sea extremadamente difícil.

La necesidad del proxy de privacidad Privoxy en combinación con Tor se debe al hecho de que las solicitudes de nombre del servidor (solicitudes DNS) en la mayoría de los casos no pasan a través del servidor proxy, y alguien que esté analizando su tráfico puede ser capaz de ver que usted está intentando acceder a un sitio específico (por ejemplo google.com) por el hecho de que envía una solicitud DNS para traducir google.com a la dirección IP apropiada. Privoxy se conecta a Tor como un proxy SOCKS4a, el cual usa nombres de servidores (no direcciones IP) para entregar sus paquetes en el destino deseado.

En otras palabras, utilizar Privoxy con Tor es una forma simple y efectiva de prevenir el análisis del tráfico que relaciona su dirección IP con los servicios

que utiliza en línea. Combinado con protocolos de encriptación seguros (como los que hemos visto en este capítulo), Tor y Privoxy proveen un alto nivel de anonimato en Internet.

Monitoreo

Las redes de computadoras (y las inalámbricas en particular) son invenciones increíblemente entretenidas y útiles. Excepto, por supuesto, cuando no funcionan. Sus usuarios se pueden quejar de que la red es "lenta" o "no funciona" ¿pero qué significa esto realmente? Sin comprender qué es lo que realmente está pasando, administrar una red puede ser muy frustrante.

Para ser un administrador de red efectivo, necesita tener acceso a herramientas que le muestren exactamente qué es lo que está sucediendo en su red. Existen varias clases diferentes de herramientas de monitoreo. Cada una le muestra un aspecto diferente de lo que "está pasando", desde la interacción física del radio a las formas en que las aplicaciones de los usuarios interactúan entre ellas. Al observar el desempeño de la red a través del tiempo se puede tener una idea de lo que es "normal" para ella, y ser notificado automáticamente cuando las cosas están fuera de orden. Las herramientas que presentamos en esta sección son bastante poderosas, y se pueden descargar gratuitamente de las fuentes listadas.

Detección de redes

Las herramientas de monitoreo comunes, simplemente proveen una lista de redes disponibles con información básica (tales como intensidad de la señal y canal). Le permiten detectar rápidamente redes cercanas y determinar si están dentro de su alcance o si están causando interferencia.

- **Las incorporadas en el cliente.** Todos los sistemas operativos modernos proveen soporte incorporado para redes inalámbricas. En general este incluye la habilidad de explorar en búsqueda de redes disponibles, permitiéndole al usuario elegir una red de la lista. Si bien prácticamente todos los dispositivos inalámbricos incluyen una utilidad simple de exploración, las funcionalidades puede variar ampliamente entre implementaciones. En general, son útiles solamente para configurar una computadora en su hogar o en la oficina. Tienden a proveer poca información además de los nombres de las redes y la señal disponible para el punto de acceso en uso actualmente.
- **Netstumbler** (*http://www.netstumbler.com/*). Es la herramienta más popular para detectar redes inalámbricas utilizando Microsoft Windows. Soporta una variedad de tarjetas inalámbricas, y es muy sencilla de utilizar. Detecta redes abiertas y encriptadas, pero no puede detectar

redes inalámbricas “cerradas”. También ofrece un medidor de señal/ruido que grafica la señal recibida a lo largo del tiempo. También se puede integrar con una variedad de dispositivos GPS, para registrar ubicaciones precisas e información sobre la potencia de la señal. Todo esto hace que Netstumbler sea una herramienta accesible para realizar una prospección informal de la zona.

- **Ministumbler** (*http://www.netstumbler.com/*). De los realizadores de Netstumbler, Ministumbler provee muchas de las mismas funcionalidades que la versión de Windows, pero funciona en las plataformas Pocket PC. Ministumbler se puede correr en PDAs portátiles con una tarjeta inalámbrica para detectar puntos de acceso en la zona.
- **Macstumbler** (*http://www.macstumbler.com/*). Si bien no está relacionado directamente con Netstumbler, Macstumbler brinda muchas de sus funcionalidades pero para la plataforma Mac OS X. Funciona con todas las tarjetas Apple Airport.
- **Wellenreiter** (*http://www.wellenreiter.net/*). Wellenreiter es un buen detector gráfico de redes inalámbricas para Linux. Requiere Perl y GTK, y soporta tarjetas inalámbricas Prism2, Lucent, y Cisco.

Analizadores de protocolos

Los analizadores de protocolos de redes una gran cantidad de detalles de la información que fluye por una red, permitiendo inspeccionar paquetes individualmente. Para las redes cableadas, pueden inspeccionar paquetes en la capa de enlace de datos o en una superior. Para el caso de las redes inalámbricas, se puede inspeccionar información hasta las tramas 802.11. Aquí hay varios analizadores de protocolos de redes populares (y gratuitas):

- **Ethereal** (*http://www.ethereal.com/*). Ethereal probablemente sea el analizador de protocolos más popular de los que tenemos a disposición. Funciona con Linux, Windows, Mac OS X, y con varios sistemas BSD. Ethereal capturara los paquetes directamente “del cable” y los despliega en una interfaz gráfica intuitiva. Puede decodificar más de 750 protocolos, desde las tramas 802.11 a los paquetes HTTP. Fácilmente reensambla los paquetes fragmentados y sigue las sesiones TCP por completo, aún si otros datos se han intercalado en la muestra. Ethereal es muy importante para resolver problemas difíciles de la red, y averiguar que es exactamente lo que está sucediendo cuando dos computadoras conversan “en el cable”.
- **Kismet** (*http://www.kismetwireless.net/*). Kismet es un poderoso analizador de protocolos inalámbrico para Linux, Mac OS X, y la distribución Linux embebida OpenWRT. Funciona con cualquier tarjeta inalámbrica que soporte el modo monitor pasivo. Además de la detección

básica de redes, Kismet registra pasivamente todas las tramas 802.11 al disco o la red en el formato estándar PCAP, para su futuro análisis con herramientas como Ethereal. Kismet también ofrece información asociada del cliente, impresión digital del modelo del AP, detección con Netstumbler, e integración GPS.

Como es un monitor pasivo de la red también puede detectar redes inalámbricas "cerradas", analizando el tráfico enviado por los clientes. Se puede instalar Kismet en varias computadoras al mismo tiempo, y hacer que todas reporten a través de la red a una misma interfaz de usuario. Esto permite realizar un monitoreo inalámbrico sobre grandes áreas, tales como un campus universitario o corporativo. Como utiliza el modo de monitoreo pasivo, hace todo esto sin transmitir ningún dato.

- **KisMAC** (*http:///kismac.binaervarianz.de/*). Desarrollado exclusivamente para la plataforma Mac OS X, KisMAC puede hacer mucho de lo que Kismet hace, pero con una interfaz gráfica Mac OS X muy elaborada. Es un rastreador pasivo que registra datos al disco en un formato PCAP compatible con Ethereal. No soporta un rastreo pasivo con tarjetas AirportExtreme (debido a las limitaciones en el manejador inalámbrico), pero soporta el modo pasivo con una variedad de tarjetas inalámbricas USB.
- **Driftnet y Etherpeg**. Estas herramientas decodifican datos gráficos (como los archivos GIF y JPEG) y los despliegan como un collage. Como mencionamos anteriormente, herramientas como ésta tienen un uso limitado en la resolución de problemas, pero tienen mucho valor para demostrar la inseguridad de los protocolos sin encriptación. Etherpeg está disponible en http://www.etherpeg.org/, y Driftnet puede descargarse en *http://www.ex-parrot.com/~chris/driftnet/*.

Monitoreo del ancho de banda

La red está lenta. ¿Quién está acaparando todo el ancho de banda? Utilizando una buena herramienta de monitoreo, puede determinar fácilmente la fuente que inunda su red de correo no deseado y de virus. Dichas herramientas también lo pueden ayudar a planificar los incrementos de capacidad requeridos para mantener los usuarios satisfechos. Al mismo tiempo le dan una representación visual de cómo fluye el tráfico en la red, incluyendo el que proviene de una computadora o servicio en particular.

- **MRTG** (*http://people.ee.ethz.ch/~oetiker/webtools/mrtg/*). La mayoría de los administradores de red se han encontrado con MRTG en algún punto de su carrera. Escrito originalmente en 1995, MRTG posiblemente sea la aplicación de monitoreo de ancho de banda más usada. Utilizando Perl y C, construye una página web llena de gráficos detallando el tráfico saliente y entrante en un dispositivo de red en particular. Con MRTG es muy

sencillo consultar conmutadores de red, puntos de acceso, servidores, así como otros dispositivos, y desplegar los resultados como gráficos en función del tiempo.

- **RRDtool** (*http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/*). Desarrollado por la misma gente que escribió mrtg, rrdtool es una aplicación de monitoreo genérica más poderosa. RRD es una abreviatura de base de datos de recorrido circular (*Round-Robin Database por su nombre en inglés*). Este es un formato de datos genérico que le permite seguir cualquier punto de datos como un conjunto promediado en el tiempo. Si bien rrdtool no monitorea directamente interfaces o dispositivos, muchos paquetes de monitoreo confían en él para almacenar y desplegar los datos que colectan. Con unos pocos programas de consola, puede monitorear fácilmente los conmutadores y puntos de acceso de su red, y trazar de forma gráfica en una página web el ancho de banda utilizado.
- **ntop** (*http://www.ntop.org/*). Para realizar un análisis histórico del tráfico y del uso de la red, seguramente usted va a querer investigar ntop. Este programa construye un reporte detallado en tiempo real de lo que observa en el tráfico de la red, y lo despliega en su navegador web. Se integra con rrdtool, y realiza gráficos y cuadros visuales que representan cómo está siendo usada la red. En redes muy pesadas ntop puede consumir mucha capacidad de la CPU y espacio del disco, pero le brinda un extensivo análisis de cómo está siendo utilizada su red. Funciona en Linux, BSD, Mac OS X, y Windows.
- **iptraf** (*http://iptraf.seul.org/*). Si necesita tomar una instantánea de la actividad de la red en un sistema Linux, inténtelo con iptraf. Ésta es una utilidad de línea de comando que le brinda en segundos una mirada sobre las conexiones y el flujo de su red, incluyendo puertos y protocolos. Puede ser muy buena para determinar quién está usando un enlace inalámbrico en particular, y cuanta carga se le está imponiendo. Por ejemplo, al mostrar una estadística detallada acerca de una interfaz, usted puede encontrar instantáneamente los usuarios de programas de intercambio entre pares (*P2P o peer-to-peer como se les conoce en inglés*) y determinar exactamente cuánto ancho de banda están utilizando en cierto momento.

Resolución de problemas

¿Qué hace cuando la red se daña? Si no puede acceder a una página web o a un servidor de correo electrónico, y el problema no se soluciona presionando el botón de “actualizar”, ustedes hace necesario aislar la ubicación exacta del problema. Estas herramientas lo van a ayudar a determinar dónde se encuentra exactamente un problema de la conexión.

- **ping**. Casi todos los sistemas operativos (incluyendo Windows, Mac OS X, y por supuesto Linux y BSD) incluyen una versión de la utilidad *ping*. Utiliza paquetes ICMP para intentar contactar un servidor específico y le informa a usted cuánto tiempo lleva obtener una respuesta.

  Saber qué contactar es tan importante como saber cómo hacerlo. Si usted no puede conectarse a un servicio en su navegador web (por ejemplo, *http://yahoo.com/*), puede intentar contactarlo:

```
$ ping yahoo.com
PING yahoo.com (66.94.234.13): 56 data bytes
64 bytes from 66.94.234.13: icmp_seq=0 ttl=57 time=29.375 ms
64 bytes from 66.94.234.13: icmp_seq=1 ttl=56 time=35.467 ms
64 bytes from 66.94.234.13: icmp_seq=2 ttl=56 time=34.158 ms
^C
--- yahoo.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 29.375/33.000/35.467/2.618 ms
```

Presione control-C cuando haya terminado de colectar datos. Si los paquetes se toman mucho tiempo en regresar, puede haber una congestión en la red. Si el retorno de los paquetes de contacto tiene un ttl inusualmente bajo, puede que haya problemas de enrutamiento entre su computadora y el extremo remoto. ¿Pero qué sucede si el contacto no regresa ningún dato? Si está contactando un nombre en lugar de una dirección IP, puede que tenga problemas de DNS.

Intente contactar una dirección IP en Internet. Si no puede acceder a ella, es una buena idea observar si puede contactar su enrutador por omisión:

```
$ ping 216.231.38.1
PING 216.231.38.1 (216.231.38.1): 56 data bytes
64 bytes from 216.231.38.1: icmp_seq=0 ttl=126 time=12.991 ms
64 bytes from 216.231.38.1: icmp_seq=1 ttl=126 time=14.869 ms
64 bytes from 216.231.38.1: icmp_seq=2 ttl=126 time=13.897 ms
^C
--- 216.231.38.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 12.991/13.919/14.869/0.767 ms
```

Si no puede contactar a su enrutador por omisión, entonces lo más probable es que tampoco pueda acceder a Internet. Si tampoco puede contactar otras direcciones IP en su LAN local, es tiempo de verificar su conexión. Si está utilizando cable Ethernet, ¿está enchufado? Si está utilizando una conexión inalámbrica, ¿esta usted conectado a la red correcta, y está la red dentro de su alcance?

El diagnóstico de problemas de la red con *ping* es casi un arte, pero es muy útil. Ya que probablemente usted va a encontrar *ping* en casi cualquier

computadora con la que trabaje, es una buena idea aprender cómo usarlo apropiadamente.

- **traceroute** y **mtr** (*http://www.bitwizard.nl/mtr/*). Como sucede con *ping*, *traceroute* está en la mayoría de los sistemas operativos (en algunas versiones de Microsoft Windows se le denomina **tracert**). Si corre *traceroute*, puede rastrear la ubicación de los problemas entre su computadora y cualquier punto en Internet:

```
$ traceroute -n google.com
traceroute to google.com (72.14.207.99), 64 hops max, 40 byte packets
 1  10.15.6.1  4.322 ms  1.763 ms  1.731 ms
 2  216.231.38.1  36.187 ms  14.648 ms  13.561 ms
 3  69.17.83.233  14.197 ms  13.256 ms  13.267 ms
 4  69.17.83.150  32.478 ms  29.545 ms  27.494 ms
 5  198.32.176.31  40.788 ms  28.160 ms  28.115 ms
 6  66.249.94.14  28.601 ms  29.913 ms  28.811 ms
 7  172.16.236.8  2328.809 ms  2528.944 ms  2428.719 ms
 8  * * *
```

La opción **-n** le dice a *traceroute* que no se preocupe por resolver los nombres en el DNS, y hace que el programa corra más rápido. Usted puede ver que en el salto siete, el tiempo de recorrido de ida y vuelta se dispara a más de dos segundos, mientras que los paquetes parece que se desechan en el salto ocho. Esto puede indicar un problema en ese punto de la red. Si esta parte de la red está bajo su control, vale la pena comenzar sus esfuerzos para resolver el problema por allí.

My TraceRoute (mtr) es un programa que combina *ping* y *traceroute* en una sola herramienta. Corriendo mtr, puede obtener un promedio de la latencia y la pérdida de paquetes hacia un servidor en cierto lapso, en lugar de la visión instantánea que ofrecen *ping* y *traceroute*.

```
                          My traceroute  [v0.69]
tesla.rob.swn (0.0.0.0)        (tos=0x0 psize=64 bitpatSun Jan  8 20:01:26 2006
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                  Packets               Pings
 Host                           Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. gremlin.rob.swn              0.0%     4    1.9   2.0   1.7   2.6   0.4
 2. er1.sea1.speakeasy.net       0.0%     4   15.5  14.0  12.7  15.5   1.3
 3. 220.ge-0-1-0.cr2.sea1.speakeasy.  0.0%     4   11.0  11.7  10.7  14.0   1.6
 4. fe-0-3-0.cr2.sfo1.speakeasy.net   0.0%     4   36.0  34.7  28.7  38.1   4.1
 5. bas1-m.pao.yahoo.com         0.0%     4   27.9  29.6  27.9  33.0   2.4
 6. so-1-1-0.pat1.dce.yahoo.com  0.0%     4   89.7  91.0  89.7  93.0   1.4
 7. ae1.p400.msr1.dcn.yahoo.com  0.0%     4   91.2  93.1  90.8  99.2   4.1
 8. ge5-2.bas1-m.dcn.yahoo.com   0.0%     4   89.3  91.0  89.3  93.4   1.9
```

Los datos van a ser actualizados y promediados continuamente. Al igual que con *ping*, cuando haya terminado de observar los datos debe presionar control-C. Tenga en cuenta que para usar mtr debe tener privilegios de administrador (root).

Si bien estas herramientas no van a revelar exactamente qué es lo que está funcionando mal en una red, pueden darle información suficiente para saber por dónde continuar en la resolución de problemas.

Prueba de rendimiento

¿Cuán rápido puede funcionar la red? ¿Cuál es la capacidad real utilizable en un enlace específico de la red? Puede obtener una muy buena estimación de su capacidad de rendimiento inundando el enlace con tráfico y midiendo cuánto demora en transferir los datos. Aunque existen páginas web que pueden hacer una "prueba de velocidad" en su navegador (como *http://www.dslreports.com/stest*), esas pruebas son altamente inexactas si usted está lejos de la fuente de prueba. Aún peor, no le permiten medir la velocidad de un enlace en particular, sino solamente la velocidad de su enlace a Internet. Le presentamos dos herramientas que le van a permitir realizar una prueba de rendimiento en su propia red.

- **ttcp** (*http://ftp.arl.mil/ftp/pub/ttcp/*). Actualmente es una parte estándar de la mayoría de los sistemas tipo Unix. ttcp es una simple herramienta de prueba de red. Se corre en cualquier lado del enlace que usted quiera probar. El primer nodo actúa en modo receptor, y el otro transmite:

```
node_a$ ttcp -r -s

node_b$ ttcp -t -s node_a
ttcp-t: buflen=8192, nbuf=2048, align=16384/0, port=5001  tcp -> node_a
ttcp-t: socket
ttcp-t: connect
ttcp-t: 16777216 bytes in 249.14 real seconds = 65.76 KB/sec +++
ttcp-t: 2048 I/O calls, msec/call = 124.57, calls/sec = 8.22
ttcp-t: 0.0user 0.2sys 4:09real 0% 0i+0d 0maxrss 0+0pf 7533+0csw
```

  Después de recolectar los datos en una dirección, debe invertir el par de transmisión y recepción para probar el enlace en la otra dirección. Puede probar flujos UDP así como TCP, alterar varios parámetros TCP y el largo de la memoria intermedia (*buffer*) para probar la red bajo fuertes exigencias. Además, el usuario puede especificar los datos a enviar en la prueba, en lugar de enviar datos generados aleatoriamente. Recuerde que la velocidad de lectura está en kilobytes, no en kilobits. Multiplique el resultado por 8 para encontrar la velocidad en kilobits por segundo.

  La única desventaja real de ttcp, es que hace años que no ha sido actualizado. Afortunadamente, el código es de dominio público y está disponible gratuitamente. Al igual que *ping* y *traceroute*, ttcp es una herramienta estándar en muchos sistemas.

- **iperf** (*http://dast.nlanr.net/Projects/Iperf/*). Al igual que ttcp, iperf es una herramienta de línea de comandos para estimar el rendimiento de una

conexión de red. Soporta muchas de las mismas características que ttcp, pero utiliza un modelo "cliente" y uno "servidor" en lugar del par "receptor" y "transmisor". Para correr iperf, inicie un servidor en un lado y un cliente en el otro:

```
node_a$ iperf -s

node_b$ iperf -c node_a
------------------------------------------------------------
Client connecting to node_a, TCP port 5001
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[  5] local 10.15.6.1 port 1212 connected with 10.15.6.23 port 5001
[ ID] Interval       Transfer     Bandwidth
[  5]  0.0-11.3 sec   768 KBytes   558 Kbits/sec
```

El lado del servidor continuará escuchando y aceptando conexiones del cliente en el puerto 5001 hasta que usted presione control-C para detenerlo. Esto puede ser útil si corremos varias tandas de pruebas desde di-ferentes lugares.

La mayor diferencia entre ttcp e iperf es que iperf está siendo desarrollado activamente, y tiene muchas características nuevas (incluyendo soporte IPv6). Esto lo hace una buena elección cuando construimos redes nuevas.

Salud de la red

Siguiendo la información a través del tiempo, usted puede tener una idea general de la salud de la red y sus servicios. Estas herramientas muestran las tendencias de su red y pueden incluso notificar a las personas cuando se presenten problemas. Muy a menudo, los sistemas van a notar el problema aún antes de que una persona llame solicitando soporte técnico.

- **cacti** (*http://www.cacti.net/*). Como mencionamos anteriormente, muchas herramientas utilizan RRDtool como programa de soporte (*back-end*) para armar gráficos con los datos que ellas recolectan. Cacti es una herramienta de ese tipo. Es una herramienta de gestión de redes basada en PHP que simplifica la recolección de datos y la generación de gráficos. Almacena su configuración en una base de datos MySQL, y está integrada con SNMP. Cacti hace muy sencillo el mapeo de todos los dispositivos en su red y monitorea todo, desde el flujo de la red hasta la carga del CPU. Tiene un esquema extensible de recolección de datos que le permite captar casi cualquier tipo de datos que se le ocurra (tales como señales de radio, ruido, o usuarios asociados) y desplegarlos en un gráfico en función del tiempo. Representaciones pequeñas (*thumbnails*) de sus gráficos pueden combinarse en una única página. Esto le permite observar el estado global de su red de una sola ojeada.

- **SmokePing** (*http://people.ee.ethz.ch/~oetiker/webtools/smokeping/*). Otra de las herramientas desarrollada por Tobias Oetiker es SmokePing. Está escrita en Perl y muestra la pérdida de paquetes y la latencia en un único gráfico. Es muy útil correr SmokePing en un servidor con buena conectividad a toda su red. Con el tiempo, revela tendencias que pueden apuntar a todo tipo de problemas de red. Combinado con MRTG o Cacti, puede observar el efecto que tiene la congestión de la red en la pérdida de paquetes y en la latencia. SmokePing puede enviar alertas cuando se encuentran ciertas condiciones, como cuando se observa una pérdida excesiva de paquetes en un enlace por un período de tiempo largo.
- **Nagios** (*http://www.nagios.org/*). Nagios es una herramienta de monitoreo de servicio. Además de seguir el desempeño de simples contactos (como con SmokePing), Nagios puede observar el desempeño de los servicios reales en varias máquinas. Por ejemplo, puede consultar periódicamente su servidor web, y estar seguro de que devuelve una página web válida. Si una verificación falla, Nagios puede notificar a una o varias personas vía correo electrónico, mensaje de texto al celular (SMS) o mensajería instantánea (IM).

  Aunque Nagios ciertamente ayuda a un único administrador a monitorear una red grande, sus funciones se destacan cuando usted tiene personal de soporte, con responsabilidades divididas entre varios de sus miembros. La detección de problemas puede ser configurada para ignorar problemas pasajeros, y sólo cuando se amerite enviar las notificaciones únicamente a las personas responsables de solucionarlos. Si el problema sigue por un período de tiempo predeterminado sin ser atendido, se puede notificar adicionalmente a otras personas. Esto permite que los problemas temporales sean simplemente registrados sin molestar al personal, y que sólo los problemas reales tengan que ser atendidos por el equipo.

7
Construyendo un Nodo en Exteriores

Se deben tener en cuenta muchas consideraciones prácticas cuando instalamos equipamiento electrónico en exteriores. Obviamente, debe protegerse de la lluvia, el viento, el sol y otros elementos dañinos. Debemos proveer energía, y la antena tiene que estar montada a una altura suficiente. Sin la puesta a tierra adecuada, los rayos que puedan caer cerca, las fluctuaciones de tensión eléctrica, y hasta el viento pueden destruir nuestro enlace ina-lámbrico. Este capítulo le dará una idea de los problemas prácticos a los que va a tener que enfrentarse cuando instale equipamiento inalámbrico en exteriores.

Cajas herméticas

Las cajas herméticas vienen en muchas variedades. Para crear un contenedor hermético para equipamiento de uso en exteriores se puede usar metal o plástico.

Por supuesto, el equipo necesita energía para funcionar, y debe ser conectado a una antena y a un cable Ethernet. Cada vez que usted perfora un contenedor hermético, crea un nuevo lugar por el cual puede ingresar el agua.

La Asociación Nacional de Fabricantes Eléctricos de USA (*NEMA - National Electrical Manufacturers Association*) estipula normativas para proteger el equipamiento eléctrico de la lluvia, la nieve, el polvo y otros contaminantes. Una caja que cumpla la clasificación ***NEMA 3*** o superior es adecuada para el uso en climas benignos. Una ***NEMA 4X*** o ***NEMA 6*** provee una excelente protección aún cuando sea expuesta al hielo o a un chorro de agua. En el caso de los elementos que perforan el cuerpo de la caja (como los cables y

los conectores), NEMA les asigna un índice de protección del ingreso (IP). Un índice de protección de ingreso de ***IP66*** o ***IP67*** protege esas perforaciones de un chorro muy fuerte de agua. Una buena protección para exteriores también debe proveer bloqueo contra las radiaciones UV para prevenir la rotura del precinto por la exposición al sol, así como para proteger el equipamiento que está adentro.

Claro que puede que sea un desafío encontrar en su región cajas clasificadas por NEMA. A menudo se pueden reciclar materiales locales para usarlos como recipientes herméticos. Se pueden utilizar cajas de plástico o de metal, conductos eléctricos para las casas y hasta contenedores de plástico para comida. Cuando perforamos una caja, debemos utilizar juntas de buena calidad o sellos toroidales (*o rings*) para sellar la abertura. En el caso de instalaciones temporales se puede utilizar como sellador un compuesto de silicona estabilizada para soportar rayos UV, o algún compuesto adhesivo flexible, pues recuerde que los cables se mueven con el viento y si el adhesivo es rígido al cabo de un tiempo empezará a resquebrajarse y permitir la entrada de humedad.

La vida de una caja de plástico se puede extender mucho dándole alguna protección al sol. Colocar la caja a la sombra, así sea bajo otro equipamiento, un panel solar, o una lámina delgada de metal específicamente para ese propósito, extenderá la vida de la caja así como la del equipo que está contenido en su interior.

Antes de colocar cualquier dispositivo electrónico en una caja sellada, asegúrese de satisfacer los requerimientos mínimos de disipación del calor. Si su placa madre requiere un ventilador o un difusor de calor muy grande, recuerde que allí no va a haber corriente de aire y probablemente su equipamiento vaya a recalentarse hasta dañarse. Utilice solamente componentes electrónicos que estén diseñados para ser usados en un medio ambiente sin circulación de aire.

Suministro de energía

La corriente DC puede ser provista simplemente haciendo una perforación en su caja y pasando un cable. Si su caja es lo suficientemente grande (como por ejemplo una caja eléctrica para exteriores) puede dotarla de un tomacorriente AC, pero los fabricantes están adoptando una solución muy práctica que elimina la necesidad de una perforación adicional en la caja: Energía a través de Ethernet (***PoE*** por su sigla en inglés).

El estándar 802.3af define un método para proveer energía a los dispositivos usando los pares que no se utilizan en un cable Ethernet estándar. En un cable CAT5 se pueden suministrar cerca de 13 vatios de forma segura y sin

interferir con la transmisión de datos en el mismo cable. Los nuevos conmutadores Ethernet que soportan 802.3af (denominados *end span injectors*) entregan energía directamente a los dispositivos conectados. Estos conmutadores pueden proveer energía en los mismos cables que son utilizados para los datos (pares 1-2 y 3-6) o en los no usados (pares 4-5 y 7-8). Una alternativa que no requiere conmutadores especiales es utilizar los llamados inyectores de DC (*mid span injectors*,) que se colocan entre los conmutadores Ethernet y el dispositivo a alimentar. Estos inyectores proveen energía mediante los pares no utilizados para transmitir datos.

Si su enrutador inalámbrico o su CPE incluyen soporte para 802.3af, en teoría podría simplemente conectarlo a un inyector. Desafortunadamente, algunos fabricantes (particularmente Cisco) utilizan otra polaridad de corriente, y conectar unos equipos no compatibles puede dañar el inyector y el equipamiento al que debíamos alimentar. Lea con cuidado las instrucciones y asegúrese de que su inyector y el equipamiento inalámbrico coinciden en los conectores y la polaridad que debe utilizarse para alimentarlos.

Si su equipamiento inalámbrico no soporta alimentación por Ethernet, puede sin embargo aprovechar los pares libres en el cable CAT5 para transportar la energía. Puede utilizar un ***inyector pasivo PoE*** comercial, o construir uno usted mismo. Estos dispositivos aplican la corriente continua (DC) a los pares libres en un extremo del cable, mientras que en el otro extremo los pares se aplican mediante un conector apropiado al receptáculo del dispositivo a alimentar. El par de dispositivos pasivos PoE se pueden adquirir por menos de $20.

Para hacerlo usted mismo, tiene que saber cuánta potencia requiere el dispositivo para funcionar, y además suministrar una corriente y voltaje lo suficientemente grandes para cubrir la pérdida en el cable Ethernet. No debe aplicar demasiada potencia porque la baja resistencia del cable constituye un riesgo de incendio. Puede encontrar un programa que calcula la pérdida de voltaje en un cable CAT5, en el siguiente sitio:
http://www.gweep.net/~sfoskett/tech/poecalc.html

Una vez que conoce la potencia y la polaridad eléctrica adecuadas para abastecer su equipamiento inalámbrico, aplique el conector al cable CAT5 utilizando solamente los hilos de datos (pares 1-2 y 3-6). Luego conecte la fuente de alimentación de corriente continua a los pares 4-5 (en general azul / azul-blanco) y 7-8 (marrón / marrón-blanco) en un extremo, y a la clavija tubular de alimentación en el otro. Una guía completa de cómo construir su propio inyector POE desde cero, está en: *http://nycwireless.net/poe/*

Consideraciones de montaje

En muchos casos, el equipamiento está ubicado en un edificio donde hay una ventana con vidrios comunes a través de los cuales pasan los rayos de luz. Los vidrios normales producen poca atenuación, pero los coloreados generan una atenuación inaceptable. El montaje en interiores simplifica mucho los temas de energía y resistencia al agua, pero evidentemente es útil solo en áreas muy pobladas.

Cuando colocamos antenas en torres, es muy importante utilizar soportes separadores, y no adosarlas directamente en la torre. Los soportes ayudan en muchas funciones incluyendo separación, alineación y protección de la antena.

Los soportes deben ser lo suficientemente fuertes para aguantar el peso de la antena, y también mantenerla en su lugar en los días ventosos. Recuerde que las antenas pueden actuar como pequeñas velas y cuando hay vientos fuertes pueden hacer mucha fuerza sobre sus montajes. Cuando estimamos la resistencia al viento, se debe considerar la superficie total de la antena, así como la distancia desde el centro de la antena al punto en el que está pegada al edificio. Las antenas grandes como los platos o los paneles sectoriales de gran ganancia pueden tener una considerable carga de viento. Si utilizamos una parabólica grillada o en malla, en lugar de un plato sólido, ayudaremos a reducir la carga del viento sin afectar mucho la ganancia de la antena. Asegúrese de que los soportes de montaje y la estructura de soporte en general sean sólidos, de otra forma su antena se va a desalinear con el tiempo (o aún peor, ¡se va a caer toda a torre!).

Los soportes deben tener una separación suficiente de la torre para permitir la alineación, pero no tanta que pueda impedir alcanzarla si se necesita mantenimiento o servicio.

El tubo del soporte de la antena debe ser circular, para que la antena pueda girar a fin de alinearla. Además, el tubo debe ser vertical. Si se está colocando en una torre de sección variable, el soporte de separación debe diseñarse para ser colocado verticalmente. Esto se logra utilizando brazos de diferente longitud, o combinaciones de varillas roscadas y placas de acero.

Figura 7.1: Una antena con un soporte de separación instalándose en una torre.

Como el equipamiento va a estar en exteriores durante toda su vida de servicio, es importante asegurarse de que el acero utilizado sea a prueba de herrumbre. El acero inoxidable a menudo tiene un precio demasiado alto para instalaciones en torres, por eso se prefiere el galvanizado al calor, pero es posible que no esté disponible en algunas áreas. Una buena pintura antióxido también puede servir. Si se elige esta opción, debe que planificar una inspección anual del montaje y si es necesario repintarlo.

Torres Venteadas o Atirantadas

Una torre venteada a la que se pueda trepar es una excelente elección para muchas instalaciones, pero en el caso de estructuras muy altas se necesita una torre autosoportada.

En el caso de las torres venteadas, colocar una polea en la cima del mástil facilita su instalación. El mástil se asegura a la sección más baja ya colocada, mientras que las dos secciones de la torre se acoplan con una unión articulada. Una cuerda pasada por la polea facilita el levantamiento de la siguiente sección. Luego de que esa sección esté vertical, sujétela a la sección más baja del mástil. El mástil (denominado en inglés gin pole) se retira, y si es necesario se puede repetir la operación. Apriete los cables de

vientos cuidadosamente, deben tener todos la misma tensión. Elija los puntos de anclaje para que los ángulos, vistos desde el centro de la torre, estén tan equiespaciados como sea posible.

Figura 7.2: Una torre venteada escalable.

Torres autosoportadas

Las torres autosoportadas son caras pero algunas veces son necesarias, particularmente cuando se requiere una gran altura. Pueden ser tan simples como un mástil robusto enterrado en una fundación de concreto, o tan complicadas como una torre de radio profesional.

Figura 7.3: Una torre autosoportada sencilla.

Algunas veces se puede utilizar una torre ya existente, aunque se deben evitar las antenas de transmisión AM porque toda la estructura es activa. Las torres de estaciones FM son aceptables si se mantiene por lo menos algunos metros de separación entre las antenas. Tenga en cuenta que si bien las antenas de transmisión adyacentes pueden no interferir con su conexión inalámbrica, una FM de alta potencia puede causar interferencia en el cable Ethernet. Siempre que utilice una torre ocupada por muchas antenas, tenga mucho cuidado con la puesta a tierra y considere la conveniencia de utilizar cable apantallado para los datos.

Figura 7.4: Una torre mucho más complicada.

Montajes sobre el techo

En los techos planos se pueden utilizar montajes para la antena que no penetren el piso. Consisten de un trípode colocado en una base de metal o de madera. Luego la base se carga con ladrillos, bolsas de arena, bidones de agua, o con cualquier otra cosa pesada. Utilizando este montaje eliminamos la necesidad de perforar el techo con tornillos, evitando potenciales goteras.

Figura 7.5: Esta base de metal puede cargarse con bolsas de arena, rocas o botellas de agua para lograr una plataforma estable sin penetrar el techo.

Cuando ya existe alguna estructura, como chimeneas o las paredes de los edificios, podemos utilizar montajes en la pared o soportes metálicos. Si las antenas se deben colocar a más de cuatro metros sobre el nivel del techo, una torre escalable puede ser la mejor solución para permitir el acceso más sencillo al equipamiento y para prevenir los movimientos de la antena durante fuertes vientos.

Metales diferentes

Para minimizar la corrosión electrolítica cuando dos metales diferentes están en contacto en presencia de humedad, sus potenciales electrolíticos deben ser lo más cercanos posible. Utilice grasa dieléctrica en la conexión entre dos metales de tipo diferente para prevenir el efecto de electrólisis.

El cobre no debe tocar nunca los materiales galvanizados de forma directa sin una protección adecuada de la unión. El agua en contacto con el cobre incorpora iones que atacan la cobertura galvanizada (*zinc*) de la torre. El acero inoxidable puede usarse como material separador, pero debe tener en cuenta que éste no es un buen conductor. Si se utiliza como separador entre el cobre y los metales galvanizados, la superficie de contacto debe ser grande y la longitud a atravesar, corta. Debe utilizarse un compuesto protector de juntas para cubrir la conexión, y para que el agua no pueda pasar entre los diferentes metales.

La humedad en los conectores es sin duda la causa de fallos más observada en los radioenlaces. Debe apretar los conectores firmemente, pero nunca utilice una llave inglesa u otra herramienta para hacerlo. Recuerde que los metales se expanden y contraen con los cambios de temperatura, y que un conector demasiado ajustado se puede romper en climas extremos.

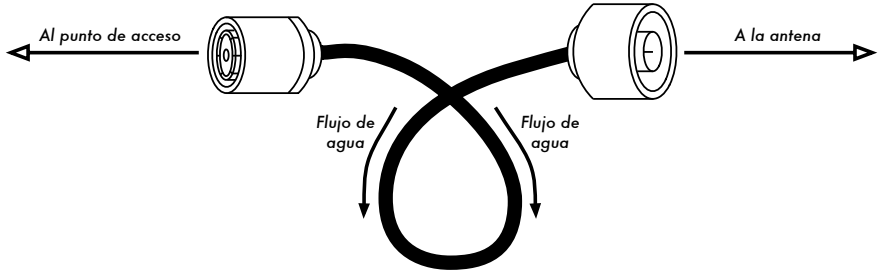


Figura 7.6: Un bucle en forma de gota fuerza al agua de lluvia a alejarse de sus conectores.

Una vez ajustados, los conectores se deben proteger aplicando una capa de cinta aisladora, luego una capa de cinta o mastique sellador y luego otra capa de cinta aisladora. El sellador protege el conector de la filtración del agua, y la capa de cinta protege el sellador del daño por los rayos UV. Los cables deben tener un bucle en forma de gota extra para evitar que el agua ingrese dentro del radio.

Seguridad

Cuando esté trabajando en las alturas utilice siempre arneses de seguridad amarrados a la torre. Si nunca ha trabajado en una torre, contrate a un profesional que lo haga por usted. En muchos países se requiere entrenamiento especial para estar autorizado a trabajar en torres por encima de cierta altura.

Evite trabajar en las torres cuando haya fuertes vientos o tormentas. Cuente siempre con un compañero, y suba sólo cuando haya buena luz. Trabajar en una torre puede llevar más tiempo del que usted piensa y es ***extremadamente*** peligroso trabajar en la oscuridad. Tómese todo el tiempo necesario para completar el trabajo antes de que se oculte el sol, y si el tiempo no le alcanza recuerde que la torre estará allí en la mañana, cuando usted pueda retomar el problema después de haber tenido una buena noche de descanso.

Alineación de antenas en un enlace a larga distancia

La clave para lograr una alineación exitosa de las antenas en un enlace a larga distancia es la comunicación. Si modifica muchas variables al mismo tiempo (es decir, un equipo comienza a mover la antena mientras el otro intenta tomar una lectura de la intensidad de la señal), el proceso tomará todo el día y probablemente va a terminar con las antenas desalineadas.

Deben utilizarse dos equipos. Idealmente, cada equipo estará conformado al menos por dos personas: una que tome las lecturas de la señal y se comunique con el extremo remoto, y la otra que manipule la antena. Éstos son puntos que debe tener en mente cuando trabaje con enlaces a larga distancia.

1. **Pruebe todo el equipamiento con anterioridad.** Antes de dirigirse al campo, configure los dispositivos, conecte las antenas con los cables apropiados y haga una prueba completa de conectividad de extremo a extremo. Desarme pare el transporte con la convicción de que en el campo sólo deberá conectar y energizar sin tener que modificar ningún parámetro. Este es un buen momento para acordar la polarización de las antenas (vea el capítulo dos si no comprende lo que significa polarización).
2. **Consiga equipo de comunicaciones de respaldo.** Si bien los teléfonos celulares usualmente son lo suficientemente buenos como para funcionar en las ciudades, la recepción móvil puede ser muy mala o

inexistente en áreas rurales. Puede utilizar radios de dos vías para comunicación de voz como los FRS o GMRS, o si sus equipos tienen licencias para radio amateurs, utilice un par de radios VHF o UHF en bandas de radioaficionado. Trabajar a cierta distancia puede ser frustrante sobre todo si usted le está preguntando constantemente al otro equipo "¿pueden escucharme ahora?" Seleccione sus canales de comunicación y pruebe sus radios (incluyendo las baterías) antes de separarse.

3. **Lleve una cámara.** Tómese cierto tiempo para documentar la ubicación de cada enlace, incluyendo los edificios que lo rodean y las obstrucciones. Más adelante esto puede ser muy útil para determinar la viabilidad de otro enlace en ese lugar sin tener que viajar en persona hasta allí. En su primera visita al lugar, registre las coordenadas con un GPS así como la elevación.

4. **Comience por estimar la orientación y elevación adecuadas.** Para comenzar, ambos equipos deben utilizar triangulación (utilizando las coordenadas del GPS o un mapa) para tener una idea general de la dirección hacia la cual apuntar. Utilice una brújula para alinear la antena en la orientación deseada. Los accidentes notables del terreno también son aprovechables para la orientación. Si puede utilizar binoculares para ver el otro extremo será aún mejor. Una vez que haya hecho sus conjeturas, tome una lectura de la intensidad de la señal recibida. Si ha hecho un buen estimado de la dirección, es probable que ya tenga señal.

5. **Si todo falla, construya su propia referencia de alineación.** Algunos tipos de terrenos hacen difícil juzgar la ubicación del otro extremo del enlace. Si está construyendo un enlace en un área con pocas marcas, una referencia hecha por usted mismo como una cometa, un globo, una lámpara de destello, una antorcha de emergencia o inclusive una señal de humo pueden ayudar. No necesariamente debe tener un GPS para alinear su antena.

6. **Pruebe la señal en ambas direcciones, pero una a la vez.** Una vez que ambos extremos han alineado lo mejor que pueden, el extremo con menos ganancia de antena debe dejarla fija. Utilizando una buena herramienta de monitoreo (como Kismet, Netstumbler, o la incluida en un buen cliente inalámbrico), el equipo con la antena de mayor ganancia debe girarla lentamente en el plano horizontal observando el medidor de señal. Una vez conseguida la mejor posición en el plano, intente modificar la elevación de la antena. Luego que se encuentra la mejor elevación, fije la antena en su lugar y avise al otro equipo para que realice el mismo procedimiento en el otro extremo. Repita este procedimiento un par de veces hasta encontrar la mejor posición para ambas antenas.

7. **No toque la antena cuando esté tomando una lectura.** Su cuerpo afecta el patrón de radiación de la antena. No la toque y no permanezca en el camino del haz cuando tome lecturas de la intensidad de la señal. Lo mismo se aplica para el equipo en el otro extremo del enlace.
8. **No vacile en seguir explorando después de obtener el máximo de señal recibida.** Como vimos en el capítulo cuatro, los patrones de radiación presentan muchos lóbulos laterales con sensibilidad inferior a la del lóbulo principal. Si la señal que recibe es menor que lo calculado puede que haya encontrado un lóbulo lateral. Continúe moviéndose lentamente más allá de ese lóbulo para ver si puede encontrar el lóbulo principal.
9. **El ángulo de la antena puede parecer errado.** El lóbulo principal de la antena a menudo irradia ligeramente hacia un lado o el otro del eje visual de la antena. No se preocupe de como luce la antena; la posición óptima es aquella que produce la mejor señal.
10. **Revise la polarización.** Puede ser frustrante intentar alinear un plato para descubrir que el otro equipo está utilizando la polarización opuesta. Repetimos, esto debe acordarse antes de dejar la base, pero si un enlace presenta una señal débil en todas las orientaciones, un nuevo chequeo de la polarización no va a hacer daño.
11. **Si nada funciona, pruebe todos los componentes uno a la vez.** ¿Están encendidos los dispositivos en ambos extremos? ¿Los pigtails y los conectores están conectados correctamente, sin partes dañadas o que generen sospecha? Como subrayamos en el capítulo ocho, una buena técnica de resolución de problemas le evita pérdida de tiempo y frustración. Trabaje lentamente y comunique frecuentemente su estado al otro equipo

Si trabaja metódicamente y con una buena comunicación, puede completar la alineación de antenas de gran ganancia en poco tiempo. Además si lo hace de forma apropiada, ¡será divertido!

Protección contra rayos y fluctuaciones de tensión eléctrica

La energía es un gran desafío para la mayoría de las instalaciones en el mundo en desarrollo. Donde hay redes eléctricas, a menudo carecen del mantenimiento adecuado, fluctúan dramáticamente y son susceptibles a los rayos. Una buena protección contra las fluctuaciones de tensión eléctrica es fundamental no sólo para proteger su equipamiento inalámbrico sino también para todo el equipo que está conectado a él.

Fusibles y cortacircuitos

Los fusibles son básicos pero se descuidan muy a menudo. En áreas rurales, y también en muchas zonas urbanas de los países en desarrollo, se hace difícil encontrar fusibles. A pesar del costo adicional, es preferible usar cortacircuitos (interruptores automáticos termomagnéticos). Probablemente haya que importarlos, pero vale la pena considerarlos. A menudo los fusibles quemados son reemplazados por monedas para restablecer el contacto. En un caso reciente, se destruyó todo el equipamiento electrónico en una estación de radio rural cuando cayó un rayo y atravesó el cableado que carecía de cortacircuito o fusible para protegerlo.

Puesta a tierra

Realizar una instalación de tierra adecuada no tiene por qué ser una tarea complicada. Se persiguen dos objetivos: proveer un cortocircuito a tierra en caso de que caiga un rayo, y proveer un circuito para que la energía estática excesiva sea disipada.

El primer objetivo es proteger el equipo de la caída directa o casi directa de un rayo, mientras que el segundo provee un camino para disipar el exceso de energía debida a la acumulación de electricidad estática. La estática puede causar una degradación significante de la calidad de la señal, particularmente en receptores sensibles (VSATs por ejemplo). Establecer un cortocircuito a tierra es sencillo. El instalador simplemente debe proveer un camino lo más corto posible desde la superficie conductora más alta (un pararrayos) hasta la tierra. Cuando un rayo impacta el pararrayos, la energía viaja por el camino más corto, y por lo tanto va a eludir el equipamiento. Este cable a tierra debe ser capaz de manejar corrientes grandes (se necesita un cable grueso, como un cable de cobre trenzado AWG 8).

Para poner a tierra al equipamiento, instale un pararrayos más arriba del equipo a proteger en una torre u otra estructura. Luego utilice un cable conductor grueso para conectar el pararrayos a algo que esté sólidamente conectado a tierra. Los caños o tuberías metálicas subterráneas pueden ser una muy buena tierra (dependiendo de su profundidad, la humedad, salinidad, cantidad de metal y contenido orgánico del suelo). En muchos lugares de África del Oeste las tuberías no están enterradas, y el equipamiento de tierra mencionado a menudo es inadecuado debido a la mala conductividad del suelo (típico de suelos tropicales estacionalmente áridos). Existen dos formas muy sencillas de medir la eficiencia de la puesta a tierra:

1. La menos precisa es conectar un UPS (Unidad de alimentación ininterruptible) de buena calidad o un multi-enchufe (regleta), que tenga un indicador de tierra (un ***LED –Diodo Emisor de Luz–***). Este LED es

encendido por la energía que está siendo disipada por el circuito a tierra. Una tierra efectiva disipa pequeñas cantidades de energía a la tierra. Algunas personas utilizan esto para piratear un poco de corriente gratuita ¡ya que esta corriente no activa el contador de energía eléctrica!

2. Tome un bombillo de pocos vatios (30 W) con su receptáculo, conecte un cable a tierra y el segundo a la fase. Si la tierra está funcionando bien, el bombillo debería encenderse levemente.
3. La forma más sofisticada es simplemente medir la impedancia entre la fase y tierra.

Si su tierra no es eficiente va a tener que enterrar una jabalina (estaca) a mayor profundidad (donde el suelo es más húmedo, y tiene más materia orgánica y metales), o mejorar la conductividad de la tierra. Un enfoque común en donde hay poco suelo es excavar un pozo de 1 metro de diámetro y 2 metros de profundidad, y colocar en él una pieza de metal conductor que tenga mucha masa. Esto a menudo se denomina ***plomo*** pero puede ser cualquier pieza de metal que pese 0,5 kg o más, tales como un yunque de hierro o una rueda de acero. Luego rellene el agujero con carbón mezclado con sal, y después llénelo hasta el tope con tierra. Humedezca el área, y el carbón y la sal se difundirán generando un zona conductora alrededor del plomo, mejorando de esta forma la eficiencia de la tierra.

Si usa cable coaxial entre la antena y el radio también puede aprovecharse para poner a tierra la torre, sin embargo un diseño más confiable usa un cable separado para la puesta a tierra de la torre. Para conectar a tierra el cable coaxial, simplemente pele un poco del revestimiento del cable en el punto más cercano a la tierra antes de que entre en el edificio, conecte un cable de tierra en ese punto, usando un buen conector o soldadura. No olvide impermeabilizar el sitio de la conexión.

Estabilizadores y reguladores de tensión

Hay muchas marcas de estabilizadores de tensión, pero la mayoría son digitales o electromecánicos. Los últimos son mucho más baratos y más comunes, usan el voltaje de 220V, 240V, o 110V de entrada para alimentar un motor que a su vez acciona un generador de corriente alterna (alternador), que produce el voltaje deseado (normalmente 220V). En general son efectivos, pero estas unidades ofrecen poca protección contra los rayos u otras fluctuaciones de tensión. A menudo se queman luego del primer rayo. Una vez quemados, pueden quedar fusionados a un determinado voltaje de salida (usualmente errado).

Los reguladores digitales controlan la energía utilizando resistencias u otros componentes de estado sólido. Son más caros, pero mucho menos susceptibles de quemarse.

Siempre que le sea posible utilice un regulador digital. Se justifica el costo adicional ya que ofrecen mejor protección para el resto de su equipo. Después de una tormenta eléctrica, inspeccione todos los componentes de su sistema de potencia (incluido el estabilizador).

Energía solar y eólica

Las aplicaciones descritas en este capítulo utilizan voltaje DC (corriente continua) que tiene una polaridad. ¡Confundir la polaridad genera daños inmediatos e irreversibles para su equipo! Vamos a suponer que usted sabe usar un multímetro digital (DMM por su sigla en inglés) para chequear la polaridad. Los voltajes DC que se utilizan en las aplicaciones descritas no son dañinos al tocar los conductores –pero las baterías de plomo grandes pueden erogar muy altas corrientes–. Un cable que ocasione un corto entre las terminales va a comenzar inmediatamente a ponerse al rojo vivo y a quemar su aislamiento. Para prevenir el fuego, siempre debe haber un fusible cerca de la terminal positiva de la batería. De esta forma el fusible se quemará antes que lo hagan los cables.

Las baterías de plomo contienen ácido sulfúrico que puede causar quemaduras graves. Cuando están cargadas o se cortocircuitan sus terminales, liberan hidrógeno –aún cuando sean del tipo hermético–. Se requiere una ventilación apropiada para prevenir explosiones, especialmente si las baterías son del tipo de plomo-electrolito ácido. Cuando manipule estas baterías es una buena idea proteger sus ojos con lentes de seguridad. Una vez conocí a un “experto” en baterías que hizo explotar tres de ellas durante su carrera. El plomo es tóxico, por lo que asegúrese de deshacerse de sus baterías gastadas de forma adecuada, aunque esto puede ser algo difícil en los países que no tienen ninguna infraestructura de reciclaje.

Sistemas de energía autónomos

Hay muchas situaciones en las cuales se quiere instalar un nodo inalámbrico en una zona donde la red de distribución eléctrica es inestable, como ocurre a menudo en países en desarrollo, o simplemente no existe, como en una colina donde quiera instalar un repetidor.

Un sistema de energía autónomo consiste básicamente en una batería que almacena energía eléctrica producida por un generador que funciona con el viento, la luz solar y/o la gasolina. Además se necesita un circuito electrónico que controle el proceso de carga y descarga.

Cuando diseñamos un sistema para operar con energía solar o eólica, es importante elegir un dispositivo que gaste un mínimo de energía. Cada vatio desperdiciado en la carga causa grandes costos en el suministro de energía.

Más consumo de energía significa que se van a necesitar paneles solares más grandes y más cantidad de baterías para proveer la energía suficiente. Si ahorramos energía eligiendo el equipamiento adecuado también vamos a ahorrarnos mucho dinero y problemas. Por ejemplo, un enlace a larga distancia, no necesariamente precisa de un amplificador que gaste mucha energía. Una tarjeta Wi-Fi con una buena sensibilidad de recepción y un despeje de al menos el 60% de la zona de Fresnel va a funcionar mejor que un amplificador, y al mismo tiempo ahorra energía. Un dicho muy conocido de los radioaficionados también se puede aplicar aquí: El mejor amplificador es una buena antena. Otras medidas para reducir el consumo de energía incluyen disminuir la velocidad del CPU y reducir la potencia de transmisión al valor mínimo que se necesite para proveer un enlace estable, incrementar la longitud de los intervalos de beacon, y apagar el sistema en los momentos que no se necesite.

La mayoría de los sistemas solares funcionan a 12 o 24 voltios. Preferiblemente, se debe utilizar un dispositivo inalámbrico que funcione con voltaje DC, operando a los 12 V que la mayoría de las baterías de plomo-ácido proveen. Si transformamos el voltaje de la batería a AC, o si utilizamos un voltaje diferente al de la batería para alimentar el punto de acceso, estamos desperdiciando energía. Un enrutador, o un punto de acceso que acepte de 8 a 20 voltios DC es perfecto.

La mayoría de los puntos de acceso económicos, tienen un regulador de voltaje de modo conmutado que funciona bien en un rango de voltaje sin recalentarse (aunque la fuente que traiga de fábrica sea de 5 o 12 voltios).

CUIDADO: Si opera su punto de acceso con una fuente de alimentación diferente de la suministrada por el fabricante, va a anular cualquier garantía y puede causar daño a su equipamiento. Si bien la técnica que describimos a continuación en general funciona como le decimos, recuerde que debe probarla, y si lo hace es bajo su propio riesgo.

Abra su punto de acceso y busque cerca de la entrada de DC dos grandes condensadores y un inductor (un toroide con un alambre de cobre enrollado a su alrededor). Si están presentes, entonces el dispositivo utiliza una fuente conmutada, y el voltaje de operación debe ser algo menor que el voltaje impreso en la etiqueta de los condensadores. Usualmente el voltaje de esos condensadores es de 16 o 25 voltios. Tenga en cuenta que una fuente de alimentación no regulada produce picos de voltaje muy superiores al voltaje nominal escrito en la etiqueta. Por lo tanto, conectar una fuente no regulada de 24 voltios a un dispositivo con condensadores de 25 voltios no es una buena idea. Por supuesto, abrir su dispositivo elimina cualquier garantía. No intente operar un punto de acceso a voltajes mayores si no usa un regulador conmutado, pues se calentaría, funcionaría mal o, inclusive, podría incendiarse.

El famoso Linksys WRT54G funciona en cualquier voltaje entre 5 y 20 voltios DC, consume cerca de 6 vatios, y tiene un conmutador Ethernet integrado. Tener un conmutador es por supuesto mejor y más práctico, pero consume energía extra. Linksys también ofrece un punto de acceso Wi-Fi denominado WAP54G que consume solamente 3 vatios y que puede correr OpenWRT y el firmware Freifunk. El Accesscube 4G Systems consume aproximadamente 6 vatios, cuando está equipado con una sola interfaz Wi-Fi. Si 802.11b es suficiente, las tarjetas mini-PCI Orinoco se desempeñan muy bien, y gastan una cantidad de energía mínima.

Otra estrategia importante para ahorrar energía es que los cables de DC sean cortos, gruesos y de buena calidad. Esto minimiza la pérdida de voltaje.

Calcular y medir el consumo de energía

El diseño de sistemas autónomos siempre comienza con el cálculo de cuánta energía se consume. La forma más sencilla de medir el consumo de su dispositivo es emplear una fuente de alimentación variable dotada de voltímetro y amperímetro. El voltaje nominal de una batería de plomo en general varía entre 11 V (descargada) y aproximadamente 14.5 V (límite superior del voltaje de carga). Usted puede variar el voltaje de su fuente de alimentación y ver cuánta corriente consume el dispositivo en diferentes voltajes. Si no tenemos esta herramienta, se puede realizar la medida utilizando la fuente de alimentación incluida en el dispositivo. Interrumpa el cable que va a la entrada DC de su dispositivo e inserte un amperímetro. Tenga en cuenta que un ***amperímetro*** se quemará, o quemará la fuente si lo conecta entre la terminal positiva y la negativa de ésta porque el amperímetro producirá un cortocircuito. La entrada de muchos amperímetros no está protegida por fusible, por lo tanto tenga mucho cuidado porque pueden dañarse muy fácilmente.

La cantidad de potencia consumida puede calcularse con esta fórmula:

```
P = U * I
```

P es la potencia en vatios, U es el voltaje en voltios, I es la corriente en amperios. Por ejemplo:

```
6 W = 12 V * 0,5 A
```

El resultado es el consumo del dispositivo. Si el dispositivo del ejemplo opera por una hora, la energía consumida es de 6 vatios-hora (Wh), ó 0.5 amperios-hora (Ah). Por lo tanto el dispositivo consumirá 144 Wh o 12 Ah al día.

Para simplificar las cosas voy a utilizar el voltaje nominal de las baterías para los cálculos, sin tener en cuenta que el voltaje provisto por la batería varía dependiendo de su cantidad de carga. La baterías son clasificadas por su capacidad en Ah, por lo tanto es más sencillo calcular utilizando Ah en lugar de Wh. La batería de un gran camión en general tiene 170 Ah, por lo tanto una batería cargada al 100% daría energía al dispositivo por aproximadamente 340 horas, con un ciclo de descarga del 100%.

Características de descarga - Regla práctica

El voltaje suministrado por una batería de plomo de 12 voltios depende de su estado de carga. Cuando la batería está cargada al 100% tiene un voltaje de 12.8 V el cual cae rápidamente a 12.6 V al extraerle corriente. Dado que la batería debe proveer una corriente constante, el voltaje de salida desciende linealmente de 12.6 V a 11.6 V en un período largo de tiempo. Por debajo de los 11.6 V el voltaje de salida cae rápidamente. Como la batería provee aproximadamente el 95% de su energía dentro de esta caída lineal del voltaje, el estado de la carga puede estimarse midiendo el voltaje bajo carga. La suposición es que la batería está cargada al 100% a 12.6 voltios y tiene 0% de carga a 11.6 voltios. Por lo tanto, cuando medimos una batería bajo carga, el estatus puede estimarse con un multímetro digital. Por ejemplo una lectura de 12.5 voltios corresponde a una carga del 90%, 12.3 voltios corresponde a una carga del 70%, etc.

Las baterías de plomo se degradan rápidamente cuando se descargan al 0%. Una batería de camión perderá el 50% de su capacidad de diseño dentro de los 50 a 150 ciclos si es cargada y descargada completamente durante cada ciclo. A 0% de la carga la batería todavía tiene 11 V en las terminales (cuando se extrae corriente). Nunca descargue una batería de plomo de 12 voltios por debajo de ese valor, porque eso le haría perder una grandísima cantidad de capacidad de almacenamiento, y descargarla hasta 0 V va a arruinarla por completo. Para evitar esta situación, en la construcción de un sistema de energía basado en baterías se debe utilizar un sistema LVD (Low Voltaje Disconnect) que a bajo voltaje desconecta el circuito. No es aconsejable descargar una batería de plomo por debajo del 70%. Evitar bajar del 80% incrementa significativamente su durabilidad. Por lo tanto una batería de camión de 170 Ah ¡tiene solamente una capacidad utilizable de 34 a 51 Ah!

Una batería de auto o de camión debe permanecer por encima de los 12.3 voltios. En raros casos se puede permitir bajar más de ese valor, por ejemplo un inesperado y largo período de mal clima. Esto puede hacerse siempre que la batería se cargue completamente después de este tipo de incidentes. Cargar al 100% tarda bastante tiempo porque el proceso de carga es más lento cuando se aproxima al final, aún si se dispone de toda la energía posible de la fuente. Una fuente de energía muy débil raramente pueda

completar la carga y debido a eso va gastar las baterías rápidamente. Por esta razón se recomienda hacer cargas a corrientes altas para evitar más costos. En este sentido nos pueden ayudar un regulador de carga eólica o solar, o un cargador automático de batería (con características de carga avanzadas). Las mejores son las características IUIa y las IU son la segunda elección.

Las baterías de arranque de automóviles son las más baratas, pero no son la mejor opción. En el mercado hay algunas baterías solares especiales, diseñadas para ser utilizadas en sistemas solares. Ellas permiten ciclos de recarga profundos (dependiendo del tipo pueden llegar a hasta por debajo del 50%) y tienen una baja corriente de autodescarga. Lo mismo se aplica a las baterías selladas de plomo, son más caras pero más seguras de manipular.

Las baterías de auto o de camión que tienen las etiquetas ***libres de mantenimiento*** deberían tener una corriente de autodescarga insignificante. De todas formas las baterías libres de mantenimiento todavía lo necesitan. Por ejemplo, se debe chequear frecuentemente el nivel del electrolito, especialmente en climas calientes. Si hay una pérdida de electrolito, se debe usar agua destilada para reponerlo ya que si no lo hacemos arruinaremos la batería.

¡Si carga demasiado sus baterías también las destruirá! En un sistema de alimentación con baterías se debe regular la corriente de carga porque la carga excesiva e ilimitada la va a dañar. Si el voltaje en la batería es demasiado alto, el componente de agua de la solución de ácido sulfúrico produce electrólisis, provocando una atmósfera que contiene una cantidad concentrada de oxígeno. El oxígeno es muy corrosivo y destruirá los conectores internos.

Diseñar un sistema con baterías de reserva

Las cosas son menos complicadas si existe una red de distribución eléctrica, aunque sea inestable y funcione esporádicamente. En ese caso, todo lo que necesitamos es un cargador automático que sea capaz de cargar la batería completamente. Sería deseable tener un cargador de modo conmutado, con un amplio rango de voltajes de entrada y características de carga sofisticadas. Estos ayudan a protegernos de las fluctuaciones de voltaje de la red de distribución. Los cargadores baratos que tienen un simple transformador, puede que nunca carguen su batería por completo si el voltaje de la red es demasiado bajo. Un cargador sencillo diseñado para 230 voltios AC suministra muy poca corriente cuando opera a 200 V o menos. No importa cuánto tiempo esté en funcionamiento, nunca va a llegar a completar la carga. Por otro lado, se quemará si el voltaje es un poco más alto que el esperado –o simplemente arruinará las baterías después de un tiempo. Un

estabilizador de voltaje AC que evite la quema de su cargador por altos voltajes puede ser realmente una muy buena idea en muchas situaciones.

Un sistema de alimentación con batería de respaldo es el siguiente:

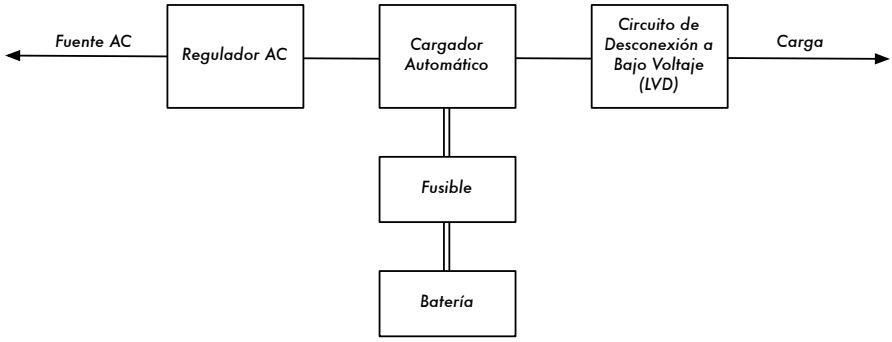


Figura 7.7: El sistema completo de alimentación con batería de respaldo.

Suponga que su dispositivo consume 7 W a 12 voltios. Necesitamos el servicio 24 horas al día, por lo tanto el dispositivo va a consumir:

```
168 Wh = 24h * 7 W
```

A 12 voltios la capacidad en amperios-hora sería:

```
14 Ah = 168 Wh / 12 V
```

Ahora, supongamos que, ocasionalmente, tenemos una situación donde el suministro de energía falla por una semana.

```
98 Ah = 14 Ah/día * 7 días
1176 Wh = 98 Ah * 12 V
```

Si dejamos que nuestra batería se descargue de 100% a 30%, consumiendo el 70% de la capacidad, necesitamos una capacidad de almacenamiento de:

```
140 Ah = 98 Ah / 0,7
```

Una batería de camión tiene esta capacidad.

Generalmente la energía está disponible durante 5 horas al día, por lo tanto el sistema va a funcionar por 19 horas con batería.

```
133 Wh = 19h * 7 W
```

Cargar y descargar una batería nunca es 100% eficiente. Siempre va a haber pérdida de energía en la batería, por lo tanto tenemos que cargarla

con más energía de la requerida. La eficiencia de carga y descarga en general es de aproximadamente el 75%.

```
177,4 Wh = 133 Wh / 0,75
```

Queremos cargarla completamente en 5 horas.

Consideremos la eficiencia de carga:

```
166 Wh = 148 Wh / 0,75
```

La convertimos a Ah:

```
14,8 Ah = 177,4 Wh / 12 V
```

Consideramos el tiempo de carga:

```
2,96 A = 14,8 Ah / 5h
```

Mientras estamos cargando, el punto de acceso/enrutador continúa consumiendo energía. 7 W equivalen a 0.6 A a 12 V:

```
3,56 A = 2,96 A + 0,6 A
```

Debemos considerar que el proceso de carga se torna más lento cuado está llegando al final del período de carga. Es mejor disponer de una corriente de carga inicial más alta para asegurarnos que alcanzamos el 100% de la carga. Un tiempo de carga de 5 horas es algo corto, por lo tanto es una buena inversión el tener un cargador IUIa de 8 amperios o más.

Hasta una batería de camión económica debe durar por lo menos 5 años, siempre que el electrolito sea chequeado frecuentemente. No se olvide de utilizar LVD. Es aconsejable sobredimensionar el sistema hasta cierto grado. Pero las baterías siempre se van a desgastar y deben ser reemplazadas, por lo que conviene sobredimensionar el alimentador en lugar de las baterías.

Diseñando un sistema alimentado por energía solar o eólica

La cantidad de energía que puede cosechar con un sistema alimentado por energía solar o eólica depende del área en donde se encuentra y la época del año. Usualmente, puede encontrar información acerca de la cantidad de radiación solar o la velocidad del viento de organizaciones administrativas competentes en asuntos climáticos. Éstas colectan información a través de los años y le pueden decir qué debe esperar para cada estación del año. Hay varios programas de simulación y cálculo para sistemas solares, entre

ellos está PVSOL, un programa comercial (bastante caro). Existe una versión de demostración en varios idiomas.

Calcular exactamente cuánta energía va a producir un sistema solar en un lugar dado da mucho trabajo. En el cálculo están involucrados varios factores como la temperatura, número de horas de sol, intensidad de la radiación, reflexiones en el medioambiente, alineamiento de los paneles solares y muchos más. Un programa de simulación y datos climáticos es un punto para comenzar, pero recuerde que en el mundo real, algo tan simple como la suciedad en los paneles puede estropear completamente los resultados de sus cálculos teóricos.

Estimar la cantidad de energía producida por un generador de viento es algo difícil y más aún si hay obstáculos alrededor del mismo. El enfoque empírico sería medir la velocidad del viento en el lugar por el período de un año –algo bastante impráctico.

Esto debería ser una guía práctica. Si en su país no se dispone de datos climáticos detallados y un programa sofisticado para el cálculo, le sugerimos construir un sistema piloto. Si la batería no logra cargarse lo suficiente, es hora de incrementar el número o tamaño de los paneles solares. Como mencionamos antes, mantener el consumo de energía al mínimo es realmente importante para evitar costos innecesarios.

Si su sistema necesita tener un tiempo de funcionamiento del 100%, las consideraciones comenzarán tomando en cuenta el peor clima del año. Tie-ne que decidir si el sistema utilizará una capacidad de almacenamiento o fuente de energía más grandes para proveer energía en los períodos críticos. Puede ser mucho más barato utilizar un generador a gasolina durante estas eventualidades.

Combinar energía solar y eólica puede ser lo más sensato en zonas con estaciones que proveen energía eólica cuando la energía solar es débil. Por ejemplo, en Alemania el sol provee sólo 10% de la energía en invierno comparado con el verano. En primavera y otoño no hay mucha energía solar tampoco, pero hay bastante viento. Durante el invierno se necesitan grandes baterías ya que es posible que ni los paneles solares o los generadores de viento provean suficiente energía durante ese período.

Bajo dichas condiciones, un sistema diseñado para un 100% de tiempo de funcionamiento necesita un margen decente de seguridad y una gran capacidad de almacenamiento. La carga debe ser vigorosa para lograr una carga total tan a menudo como sea posible durante los períodos de buen clima. Los paneles solares pueden necesitar un reemplazo cada 25 años, ¡mientras que una batería en un sistema que no tiene suficiente potencia de carga puede tener que ser reemplazada cada año!

Circuito

Un sistema de suministro autónomo consiste de:

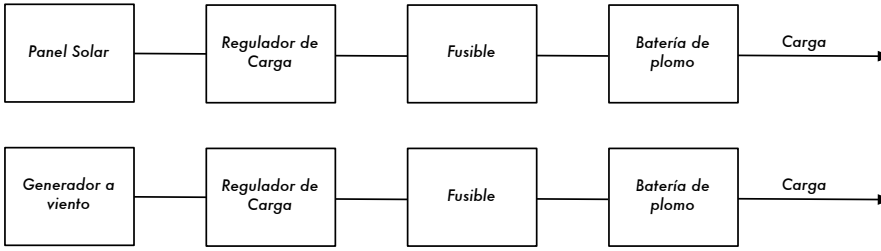


Figura 7.8: Sistema alimentado con energía eólica o solar.

Si se combinan ambos sistemas se conectan a la misma batería.

Energía eólica

Un generador a viento es una opción clara cuando se diseña un sistema autónomo para un transmisor inalámbrico que se va a construir en una colina o montaña. Una consideración a tener en cuenta con la energía eólica, es que la velocidad del viento debe ser lo suficientemente alta en un sitio que puede estar rodeado por objetos. La velocidad promedio durante el año debe ser por lo menos de 3 a 4 metros por segundo, y el generador a viento debe estar 6 metros más alto que otros objetos en una distancia de 100 me-tros. Una ubicación muy alejada de la costa usualmente no cuenta con suficiente energía eólica para cumplir con estos requerimientos.

Energía Solar

En la mayoría de los casos, la mejor solución es un sistema que utilice solamente energía solar. Usualmente. es bastante fácil encontrar una ubicación adecuada para los paneles solares, y ellos no contienen partes mecánicas móviles que precisen mantenimiento.

Es importante que los paneles estén montados con el mejor alineamiento y ángulo hacia el sol. El mejor ángulo puede variar a través del año y es dependiente de la ubicación del lugar. Es una buena idea tomar en cuenta que el polvo, las hojas o los pájaros pueden ensuciar un panel solar. El ángulo de montaje óptimo puede ser demasiado horizontal, favoreciendo que el polvo se aloje en el panel solar, requiriendo una limpieza frecuente.

No se debe permitir sombra sobre el panel durante el día, porque los paneles consisten en varias células solares que están conectadas en serie. Una cadena es tan fuerte como su eslabón más débil. Si algo cubre completamente una célula del panel solar –por ejemplo una hoja– el panel

entero deja de producir energía. ¡Hasta la sombra de un cable reduce significativamente la cantidad de energía generada por el sistema solar!

Reguladores de carga

Los reguladores de carga para los generadores a viento son diferentes a los reguladores para paneles solares. Si el sistema tiene energía solar y eólica, se van a necesitar dos reguladores. Cada regulador tiene que estar conectado a las terminales de la batería directamente (¡a través de un fusible por supuesto!)

Influencia del seguimiento del punto de insolación máxima

Los fabricantes de paneles son optimistas cuando calculan la potencia máxima de energía de sus paneles. Por lo tanto, la energía producida efectivamente por un panel es significativamente menor que la que se declara en la hoja de datos. La potencia máxima de energía sólo se logra a cierto voltaje, a una temperatura de panel de 20 grados Celsius y a una radiación solar de 1000 vatios por metro cuadrado. Esto no es realista ya que un panel se calienta mucho a 1000 W de radiación por metro cuadrado. Las altas temperaturas reducen la generación efectiva de energía de un panel. No hay mucho que hacer aparte de recordar que un panel nunca logra la potencia publicitada.

La influencia del voltaje de salida del panel es lo más importante para considerar en un sistema autónomo. Si se utiliza un regulador de carga simple, el voltaje en el panel cae al nivel del voltaje de la batería. Un panel solar puede tener la máxima eficiencia a 18 voltios –producir 1 amperio con insolación de 1000 W/m2 a 30 grados Celsius. Este punto de eficiencia máxima es llamado ***punto de máxima potencia*** (o ***MPP*** por su sigla en inglés).

Nuestro panel podría producir:

```
18 W = 18 V * 1 A
```

Si el panel está conectado a una batería de 12.3 voltios, la corriente es un poco mayor que a MPP, quizás 1.1 A, pero el voltaje del panel caería al nivel del de la batería:

```
13,5 W = 12,3 V* 1,1 A
```

La eficiencia en nuestro ejemplo sería solo de un 75% con un regulador de carga simple. Este problema puede ser solucionado usando un regulador solar con seguimiento del punto de máxima potencia. Un regulador de MPP bien diseñado logra una eficiencia de 90%. Un sistema con un regulador simple nunca logra más de 70% del la potencia declarada por el fabricante.

Incrementar la capacidad de la batería y el panel solar

Si quiere combinar dos o más baterías para incrementar la capacidad, interconéctelas en paralelo, es decir, interconecte ambas terminales positivas con un cable grueso. En el cable debe haber un fusible cercano a cada terminal positiva. Interconecte las terminales negativas sin fusibles. Para interconectar paneles solares tampoco se necesitan fusibles.

Circuitos de desconexión a bajo voltaje

Las cargas (su punto de acceso, enrutador u otro dispositivo) estarán conectadas al regulador de carga. La mayoría de éstos viene con circuitos de desconexión por bajo voltaje. Estos circuitos nunca deberían activarse, pues indicaría un serio error de diseño o la presencia de un daño. Si sucede que hay dos reguladores en el sistema que tienen circuitos de desconexión a bajo voltaje, conecte las cargas a un solo regulador, de otra forma éstos podrían dañarse.

Cálculo

El cálculo de un panel solar no es muy diferente al de un sistema con batería de reserva (detallado anteriormente). Obviamente los períodos en los que no hay energía disponible para la carga pueden ser muy largos, y la corriente de carga no es fija lo que complica el cálculo.

Un sistema bien diseñado debe ser capaz de recargar completamente una batería descargada en unos pocos días soleados, al mismo tiempo que provee de energía al equipamiento.

8
Resolución de Problemas

La forma en que usted establezca la infraestructura de soporte de su red es tan importante como el tipo de equipamiento que utilice. A diferencia de las conexiones cableadas, los problemas con las redes inalámbricas a menudo son invisibles, y pueden requerir más capacidades y más tiempo para diagnosticarlos y remediarlos. La interferencia, el viento y otras obstrucciones físicas pueden causar que una red que estaba en funcionamiento desde hace tiempo falle. Este capítulo detalla una serie de estrategias para ayudarlo a formar un equipo de gente que pueda dar soporte a su red de forma efectiva.

Formando su equipo

Cada pueblo, compañía o familia, tiene algunas personas que están intrigadas por la tecnología. Son aquellos a quienes encontramos empalmando el cable de televisión, reparando un televisor roto o soldando una nueva pieza a una bicicleta. Este tipo de gente se va a interesar por su red y querrá aprender tanto como le sea posible. Aunque estas personas son recursos invalorables, debe evitar impartir todo el conocimiento especializado sobre las redes inalámbricas a una sola persona, porque si su único especialista pierde interés o encuentra un trabajo mejor remunerado en otro lugar, se va a llevar el conocimiento consigo cuando se vaya.

También puede haber muchos adolescentes jóvenes y ambiciosos o adultos jóvenes que se interesan por el tema y tienen tiempo para escuchar, ayudar y aprender acerca de la red. Ellos son de gran ayuda y van a aprender rápidamente, pero el equipo debe enfocar su atención en aquellos que sean los mejores para dar soporte a la red en los meses y años siguientes. Lo más probable es que los adultos jóvenes y los adolescentes se marchen a la universidad o a encontrar empleo, especialmente los ambiciosos, que son a los que les gustaría involucrarse. Estos jóvenes también tienen poca

influencia en la comunidad, donde una persona mayor es probable que tenga más capacidad para tomar decisiones que afecten a la red positivamente. A pesar de que estas personas puedan tener menos tiempo para aprender y parezcan menos interesados, su contribución y educación adecuada acerca del sistema puede ser significativa.

Por lo tanto, una estrategia clave para armar un equipo de soporte es balancear y distribuir el conocimiento entre aquellos que son los más capacitados para darle soporte a la red a largo plazo. Si bien debe involucrar a los jóvenes, no les debe dejar capitalizar el uso o el conocimiento de estos sistemas. Encuentre gente que esté comprometida con la comunidad, que tenga sus raíces en ella, que puedan ser motivados, y enséñeles. Una estrategia complementaria es repartir funciones y obligaciones y documentar toda la metodología y procedimientos. De esta forma la gente puede ser entrenada fácilmente y sustituida con poco esfuerzo.

Por ejemplo, en un proyecto el equipo de entrenamiento seleccionó a un brillante joven recién graduado de la universidad que había vuelto a su pueblo; él estaba muy motivado y aprendió rápidamente. Como aprendió tan rápido, se le enseñó más de lo que se había previsto, y era capaz de lidiar con una variedad de problemas, desde arreglar una computadora a rearmar el cable Ethernet. Desafortunadamente, dos meses después de emprender el proyecto le llegó una oferta para un trabajo en el gobierno y dejó la comunidad. Ni siquiera con la oferta de un salario similar se le pudo retener, ya que la perspectiva de un trabajo estable en el gobierno era más atractiva. Todo el conocimiento de la red y cómo realizar su soporte se fue con él. El equipo de entrenamiento tuvo que volver y comenzar el entrenamiento otra vez. La siguiente estrategia fue dividir funciones y entrenar gente que estuviera establecida de forma permanente en la comunidad: gente que tuviera hijos y casas, y que ya tuvieran trabajo. Llevó el triple de tiempo enseñarles a tres personas hasta que alcanzaron el nivel de entrenamiento del joven universitario, pero la comunidad retuvo ese conocimiento por mucho más tiempo.

Con esto queremos sugerirle que seleccionar por usted mismo a quien se va a involucrar en el proyecto a menudo no es el mejor enfoque. En general es mejor encontrar una organización local o un administrador local, y trabajar con ellos para encontrar el equipo técnico adecuado. Los valores, la historia, las políticas locales y muchos otros factores pueden ser importantes para ellos, mientras que pueden ser completamente incomprensibles para gente que no es de esa comunidad. El mejor enfoque es entrenar a su socio local para darle cierto criterio (asegurándose de que lo comprenden) y para marcar límites firmes. Dichos límites deben incluir reglas acerca del favoritismo y clientelismo, aunque éstas deben considerar la situación local. Probablemente sea imposible decir que usted no puede contratar familiares,

pero deben existir inspecciones y balances. Si tenemos un candidato que sea un familiar, debe haber un criterio claro, y una segunda autoridad que decida sobre su candidatura. También es importante que el socio local tenga esa autoridad y que no sea influido por los organizadores del proyecto, porque de otro modo se compromete su habilidad gerencial. Los socios locales deben ser capaces de determinar quién va a ser la mejor persona para trabajar con ellos. Si son bien instruidos sobre este proceso, entonces los requerimientos de personal serán cumplidos a cabalidad.

La resolución de problemas y el soporte técnico son como el arte abstracto. La primera vez que usted ve una pintura abstracta puede que le parezca un conjunto de pinceladas al azar. Luego de reflexionar en la composición durante un tiempo, puede que comience a apreciar la obra como un conjunto, y la coherencia "*invisible*" se vuelva real. La mirada de un neófito a una red inalámbrica puede identificar antenas, cables y computadoras, pero le puede tomar bastante tiempo apreciar el objetivo de la red "*invisible*". En áreas rurales, es posible que la gente de la localidad deba hacer una inmensa evolución en su comprensión antes de que pueda apreciar una red invisible que fue instalada en su pueblo. Por lo tanto se necesita una introducción paulatina que les haga más fácil aceptar y apropiarse de la tecnología. El mejor método es fomentar el involucramiento de la comunidad. Una vez que los participantes han sido seleccionados y se han comprometido con el proyecto, involúcrelos tanto como sea posible. Déjelos "manejar". Entrégueles la pinza crimpeadora o el teclado y muéstreles cómo hacer el trabajo. Aunque usted no tenga tiempo para explicar cada detalle, y a sabiendas de que haciéndolo de esta manera va a tomar mucho más tiempo, ellos necesitan involucrarse físicamente y ver no sólo lo que ha sido hecho, sino también cuánto trabajo se ha hecho.

El método científico se enseña prácticamente en todas las escuelas occidentales. Mucha gente lo aprende durante sus clases de ciencia en la secundaria. Para decirlo simplemente, se toma un conjunto de variables, luego se eliminan lentamente dichas variables a través de pruebas binarias hasta quedarse con una o pocas posibilidades. Con esas posibilidades en mente, se completa el experimento. Luego se prueba si el experimento produce algo similar al resultado esperado, de lo contrario se calcula nuevamente el resultado esperado y se intenta de nuevo. Al campesino típico se le pudo haber explicado este concepto, pero probablemente no haya tenido la oportunidad de aplicarlo para resolver problemas complejos. Aunque estén familiarizados con el método científico, es probable que no hayan pensado en aplicarlo para resolver problemas reales.

Este método es muy efectivo a pesar de que puede llegar a consumir mucho tiempo. Se puede acelerar haciendo suposiciones lógicas. Por ejemplo, si un punto de acceso que venía funcionando hace mucho, deja de hacerlo repentinamente luego de una tormenta, se puede sospechar que hay un

problema con el abastecimiento eléctrico y por lo tanto obviar la mayor parte del procedimiento. Las personas que han sido adiestradas para dar soporte deben aprender como resolver los problemas utilizando este método, ya que va a haber momentos en los que el problema no es ni conocido ni evidente. Se pueden hacer simples árboles de decisión, o diagramas de flujo, e intentar eliminar las variables para aislar el problema. Por supuesto, esos cuadros no deben ser seguidos ciegamente.

A menudo es más sencillo enseñar este método utilizando primero un problema no tecnológico. Digamos, haga que su estudiante desarrolle un procedimiento de resolución para un problema sencillo y familiar, como por ejemplo, un televisor a batería. Para empezar, sabotee el aparato: póngale una batería sin carga, desconecte la antena e inserte un fusible roto. Pruebe al estudiante, dejándole en claro que cada problema muestra síntomas específicos, e indíquele la manera de proceder. Una vez que haya reparado el televisor, hágalo aplicar este procedimiento a un problema más complicado. En una red, usted puede cambiar una dirección IP, cambiar o dañar cables, utilizar el ESSID equivocado u orientar la antena en la dirección equivocada. Es importante que ellos desarrollen una metodología y un procedimiento para resolver estos problemas.

Técnicas adecuadas para la resolución de problemas

Ninguna metodología de resolución de problemas puede cubrir por completo todos aquellos con los que se va a encontrar cuando trabaja con redes inalámbricas, pero a menudo los problemas caen dentro de uno de los pocos errores comunes. Aquí hay algunos simples puntos a tener en mente que pueden hacer que su esfuerzo para resolver el problema vaya en la dirección correcta.

- **No entre en pánico.** Si usted está arreglando un sistema, significa que el mismo estaba funcionando, con seguridad muy recientemente. Antes de sobresaltarse y hacer cambios impulsivamente, analice la escena y determine exactamente lo que está roto. Si tiene un registro histórico o estadísticas de funcionamiento, mucho mejor. Asegúrese de recolectar la información en primer lugar para poder tomar una decisión bien informada antes de hacer cambios.
- **¿Está conectado?** Este paso a menudo es pasado por alto hasta que muchas otras posibilidades son exploradas. Los enchufes pueden desconectarse muy fácilmente, ya sea accidental o intencionalmente. ¿El cable está conectado a una buena fuente de energía? ¿El otro extremo está conectado a su equipo? ¿La luz de energía está encendida? Esto puede sonar algo tonto, pero usted se verá aún más tonto si pierde mucho

tiempo en probar la línea de alimentación de la antena sólo para comprobar que el AP estuvo desenchufado todo ese tiempo. Confíe en nosotros, esto sucede más a menudo de lo que la mayoría de nosotros queremos admitir.

- **¿Cuál fue la última cosa que cambiamos?** Si usted es la única persona con acceso a sistema, ¿cuál fue el último cambio que hizo? Si otros tienen acceso a él, ¿cuál fue el último cambio que hicieron y cuándo? ¿Cuándo fue el último momento en el que el sistema funcionó? A menudo los cambios tienen consecuencias imprevistas que pueden no ser notadas inmediatamente. Deshaga ese cambio y vea el efecto que tiene en el problema.
- **Haga una copia de seguridad.** Esto se debe hacer antes de que usted detecte problemas y le servirá después. Si va a hacer una actualización compleja de software al sistema, tener una copia de seguridad significa que puede restaurarlo rápidamente a la configuración previa y comenzar de nuevo. Cuando resolvemos problemas muy complejos, tener una configuración que "más o menos funciona" puede ser mucho mejor que tener una que no funciona para nada (y que no puede restaurar fácilmente desde la memoria).
- **El bueno conocido.** Esta idea se aplica tanto al equipamiento como a los programas. Un ***bueno conocido*** es cualquier componente que se pueda reemplazar en un sistema complejo para verificar que sus contrapartes están en buenas condiciones de funcionamiento. Por ejemplo, puede llevar junto con sus herramientas, un cable Ethernet previamente probado. Si sospecha que hay problemas con el cable que está en la instalación, sencillamente puede intercambiar el cable sospechoso con el bueno conocido y ver si las cosas mejoran. Esto es mucho más rápido y menos propenso a los errores que rearmar un cable, y le dice inmediatamente si el cambio solucionó el problema. De la misma forma usted puede tener una batería de repuesto, un cable de antena, o un CD-ROM con una buena configuración conocida para el sistema. Cuando solucionamos problemas complicados, guardar su trabajo en un punto dado nos permite retornar a un estado bueno conocido, aún si el problema no se ha solucionado por completo.
- **Cambie una variable por vez.** Cuando estamos bajo presión para poner un sistema de nuevo en línea, tendemos a actuar impulsivamente y cambiar muchas variables al mismo tiempo. Si lo hace, y sus cambios arreglan el problema, entonces no va a comprender exactamente qué fue lo que ocasionó el problema en primer lugar. Peor aún, sus cambios pueden solucionar el problema original, pero al mismo tiempo generar consecuencias imprevistas que pueden dañar otras partes del sistema. Si cambia sus variables una a la vez, puede entender con precisión qué fue lo que se dañó en primera instancia, y ser capaz de ver los efectos directos de los cambios que va haciendo.

- **No lo dañe.** Si no comprende en su totalidad cómo funciona un sistema, no dude en llamar a un experto. Si no está seguro de si un cambio en particular va a dañar otras partes del sistema, entonces encuentre a alguien con más experiencia, o busque una forma de probar su cambio sin hacer daño. Poner una moneda en lugar de un fusible puede resolver el problema inmediato, pero también puede incendiar el edificio.

Es poco probable que la gente que diseñó su red esté disponible veinticuatro horas al día para resolver los problemas cuando aparecen. Aunque su equipo de soporte sea muy capaz de resolver problemas, puede que no sea lo suficientemente competente como para configurar un enrutador desde cero o poner el conector a un cable LMR-400. A menudo es mucho más eficiente tener varios componentes de respaldo a mano, y entrenar a su equipo para reemplazar por completo la pieza rota. Esto puede significar tener un punto de acceso o un enrutador preconfigurado, guardados en un gabinete cerrado, claramente etiquetado y almacenado junto con los cables de respaldo y las fuentes de alimentación. Su equipo puede cambiar el elemento que funciona mal y enviarlo a un experto para que lo repare o coordinar para que se envíe otro equipo de respaldo. Mantener los respaldos seguros y reemplazarlos cuando los usamos puede ahorrarnos mucho tiempo a todos.

Problemas comunes de las redes

A menudo los problemas de conectividad provienen de la rotura de componentes, un clima adverso o simplemente un problema de configuración. Una vez que su red esté conectada a Internet o abierta al público en general, van a aparecer una gran cantidad de amenazas provenientes de los mismos usuarios. Esas amenazas pueden estar en un rango desde las benignas hasta las indiscutiblemente malévolas, pero todas van a tener impacto en su red si no está configurada correctamente. Esta sección se enfoca en algunos problemas comunes encontrados una vez que su red es utilizada por seres humanos reales.

Sitios web alojados localmente

Si una universidad aloja su sitio web localmente, los visitantes del sitio desde fuera del campus y del resto del mundo van a competir con los trabajadores de la universidad por el ancho de banda. Esto incluye el acceso automatizado desde los motores de búsqueda que periódicamente ***escanean*** su sitio por completo. Una solución para este problema es dividir el DNS y reflejar el sitio. La universidad refleja una copia de sus sitios web en un servidor que puede ser una compañía de almacenamiento web europea, y utiliza el DNS dividido para direccionar a todos los usuarios de fuera de la universidad hacia el sitio reflejado, mientras que los usuarios de

la universidad acceden al mismo sitio pero a nivel local. Los detalles sobre cómo configurar esto se proveen en el capítulo tres.

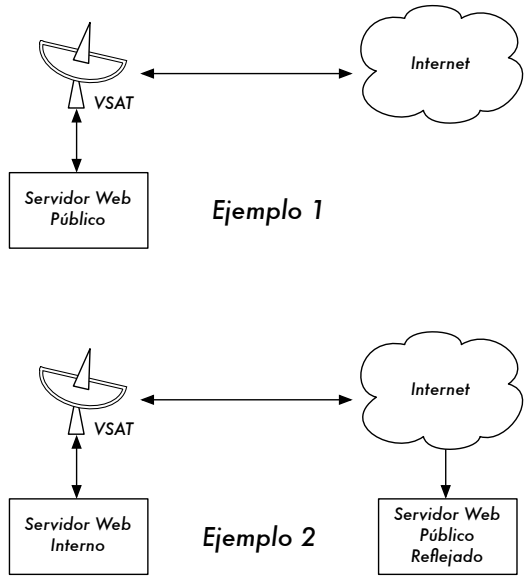


Figura 8.1: En el ejemplo 1, todo el tráfico del sitio web que viene desde Internet debe atravesar el VSAT. En el ejemplo 2, el sitio web público es alojado en un servicio europeo rápido, mientras que en el servidor interno se mantiene una copia para tener un acceso local muy rápido. Esto mejora la conexión del VSAT y reduce los tiempos de carga para los usuarios del sitio web.

Proxis abiertos

Un servidor proxy debe ser configurado para aceptar solamente conexiones desde la red de la universidad, no desde el resto de Internet. Esto se debe a que gente de todos lados se va a conectar y utilizar los proxis abiertos por una variedad de razones, como por ejemplo evitar pagar por ancho de banda internacional. La forma de configurarlo depende del servidor proxy que usted use. Por ejemplo, puede especificar el rango de direcciones IP para la red del campus en su archivo **`squid.conf`** de manera que esta sea la única red que puede utilizar Squid. Alternativamente, si su servidor proxy está detrás del límite de un cortafuego, puede configurar el cortafuego para que le permita solamente a los servidores internos que se conecten al puerto proxy.

Servidores de retransmisión abiertos

Un servidor de correo electrónico configurado incorrectamente puede ser encontrado por gente inescrupulosa, y usado como un servidor de retransmisión para enviar grandes cantidades de mensajes y de correo no

deseado. Ellos lo hacen para ocultar la verdadera fuente del correo no deseado y para evitar ser atrapados. Para detectar esta vulnerabilidad, haga la siguiente prueba en su servidor de correo electrónico (o en el servidor SMTP que actúa como servidor de retransmisión en el perímetro de la red del campus). Use ***telnet*** para abrir una conexión al puerto 25 del servidor en cuestión (con algunas versiones Windows de telnet, puede ser necesario escribir '*set local_echo*' antes de que el texto sea visible):

```
telnet mail.uzz.ac.zz 25
```

Si se permite conversación de línea de comando interactiva (como el ejemplo que sigue), el servidor está abierto para retransmitir:

```
MAIL FROM: spammer@waste.com
250 OK - mail from <spammer@waste.com>
RCPT TO: innocent@university.ac.zz
250 OK - rcpt to spammer@waste.com
```

En su lugar, la respuesta después del primer **`MAIL FROM`** debe ser algo así:

```
550 Relaying is prohibited.
```

Una prueba en línea como esta, así como información acerca de este problema, están disponibles en sitios como *http://www.ordb.org/*. Como aquellos que envían correos masivos tienen métodos automatizados para encontrar los servidores de retransmisión abiertos, una institución que no protege sus sistemas de correo es casi seguro que va a ser víctima de abusos. Configurar el servidor de correo para que no sea un relevador abierto consiste en especificar las redes y hosts que están autorizados para transmitir mensajes a través de él en el MTA (por ejemplo, Sendmail, Postfix, Exim, o Exchange). Éste probablemente va a ser el rango de direcciones IP de la red del campus.

Redes entre pares (P2P - peer-to-peer)

El abuso del ancho de banda a través de programas entre pares (P2P) para compartir archivos como Kazaa, Morpheus, WinMX y BearShare se puede prevenir de las siguientes formas:

- **No permita la instalación de nuevos programas en las computadoras del campus.** Para prevenir la instalación de programas como el Kazaa, no debe darse a los usuarios comunes acceso de administrador a las estaciones de trabajo. Muchas instituciones también estandarizan la configuración de sus máquinas, instalando el sistema operativo requerido en una computadora, luego instalan todas las aplicaciones y las configuran de una forma óptima, incluyendo la imposibilidad de que los usuarios instalen nuevas aplicaciones. Una imagen del disco de esta PC se clona a

todas las otras PCs utilizando un programa como Partition Image (vea *http://www.partimage.org/*) o Drive Image Pro (vea *http://www.powerquest.com/*).

Es probable que de vez en cuando los usuarios puedan eludir el control y consigan instalar nuevo software o dañar el que ya tenía instalado la computadora (provocando por ejemplo que esta se "cuelgue" a menudo). Cuando esto pasa, un administrador simplemente puede restablecer la imagen del disco, logrando que el sistema operativo y todo el software en la computadora sean exactamente como se especificó originalmente.

- **Bloquear esos protocolos no es una solución.** Esto pasa porque Kazaa y otros protocolos son lo suficientemente hábiles como para eludir los puertos bloqueados. Por omisión Kazaa utiliza para la conexión inicial el puerto 1214, pero si no está disponible intentará utilizar los puertos 1000 al 4000. Si también están bloqueados, utiliza el puerto 80, haciéndose ver como tráfico de consultas web. Por esta razón los ISPs no lo bloquean, pero sí lo "limitan", utilizando un administrador de ancho de banda (vea el capítulo tres).
- **Si limitar el ancho de banda no es una opción, cambie el diseño de la red.** Si el servidor proxy y los servidores de correo están configurados con dos tarjetas de red (como se describe en el capítulo tres), y esos servidores no están configurados para reenviar ningún paquete, entonces van a bloquear todo el tráfico P2P. También van a bloquear todos los otros tipos de tráfico como Microsoft NetMeeting, SSH, software VPN, y todos los otros servicios no permitidos específicamente por el servidor proxy. En redes con un ancho de banda escaso se puede decidir que la simplicidad de este diseño prepondera sobre las desventajas que tiene. Esta decisión puede ser necesaria, pero no debe tomarse a la ligera. Los administradores no pueden predecir las formas innovadoras en las que los usuarios van a hacer uso de la red. Si bloqueamos preventivamente todos los accesos, también impediremos que los usuarios puedan hacer uso de cualquier servicio (aún los servicios de ancho de banda lento) que su proxy no soporte. Si bien esto puede ser deseable en circunstancias de ancho de banda muy lento, en general nunca debe ser considerada como una buena política de acceso.

Programas que se instalan a sí mismos (desde Internet)

Existen programas que se instalan a sí mismos y luego utilizan ancho de banda –por ejemplo el denominado Bonzi-Buddy, el Microsoft Network, y otros tipos de "gusanos". Algunos programas son espías, y permanecen enviando información sobre los hábitos de búsqueda (y de consumo) de un usuario hacia una compañía en algún lugar de Internet. Estos programas se previenen, hasta cierto punto, educando a los usuarios y cerrando las PCs para evitar el acceso como administrador a los usuarios normales. En otros

casos, tenemos soluciones de software para encontrar y remover estos programas problemáticos, como Spychecker (*http://www.spychecker.com/*), Ad-Aware (*http://www.lavasoft.de/*), o xp-antispy (*http://www.xp-antispy.de/*).

Actualizaciones de Windows

Los últimos sistemas operativos de Microsoft Windows suponen que una computadora con una conexión LAN tiene un buen enlace a Internet, y descarga automáticamente parches de seguridad, correctores de fallas y mejoradores, desde el sitio web de Microsoft. Esto puede consumir grandes cantidades de ancho de banda en un enlace a Internet costoso. Los dos posibles enfoques a este problema son:

- **Deshabilitar las actualizaciones de Windows en todas las estaciones de trabajo.** Las actualizaciones de seguridad son muy importantes para los servidores, pero que las estaciones de trabajo en una red privada protegida como la red de un campus las necesiten, es algo debatible.
- **Instalar un Servidor de Actualización de Software.** Este es un programa gratuito de Microsoft que le permite descargar todas las actualizaciones de Microsoft durante la noche al servidor local y luego distribuirlas desde allí a las estaciones de trabajo cliente. De esta forma las actualizaciones de Windows utilizarán el ancho de banda del enlace a Internet durante el día. Desafortunadamente, para que esto funcione, todos los PCs cliente deben ser configurados para utilizar el Servidor de Actualización de Software. Si usted tiene un servidor DNS flexible, también puede configurarlo para que responda todas las solicitudes al sitio web *windowsupdate.microsoft.com*, y lo redireccione hacia su servidor de actualización. Esta es una buena opción sólo para redes muy grandes, pero puede ahorrar una incalculable cantidad de ancho de banda de Internet.

Bloquear el sitio de actualizaciones de Windows en el servidor proxy no es una buena solución porque el servicio de actualización de Windows (Actualización Automática) va a continuar intentando más agresivamente, y si todas las estaciones de trabajo lo hacen, se produce una pesada carga en el servidor proxy. El extracto de abajo es del registro del proxy (registro de acceso Squid) donde esto fue hecho bloqueando los archivos de gabinete Microsoft (.cab).

La mayoría del registro Squid lucía así:

```
2003.4.2 13:24:17 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
  *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:18 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:18 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab HEAD 0
2003.4.2 13:24:19 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:19 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:20 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:21 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:21 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab GET 0
2003.4.2 13:24:21 192.168.1.21 http://windowsupdate.microsoft.com/ident.cab
 *DENIED* Banned extension .cab HEAD 0
```

Si bien esto puede ser tolerable cuando tenemos unos pocos PC cliente, el problema crece significativamente cuantos más nodos se agregan a la red. En lugar de forzar al servidor proxy a procesar solicitudes que siempre van a fallar, tiene más sentido redireccionar los clientes del Software de Actualización a un servidor local de actualización.

Programas que suponen un enlace de gran ancho de banda

Además de las actualizaciones de Windows, muchos otros programas y servicios dan por sentado que el ancho de banda no es un problema, y por lo tanto lo consumen por razones que el usuario no puede predecir. Por ejemplo, los paquetes anti-virus (como el Norton AntiVirus) se actualizan a sí mismos directamente desde Internet, automática y periódicamente. Sería mejor si esas actualizaciones se distribuyeran desde el servidor local.

Otros programas como el reproductor de video RealNetworks, descarga actualizaciones y publicidad automáticamente, así como envía información sobre los hábitos de uso a un sitio en Internet. Pequeñas aplicaciones (conocidas como *applets*) aparentemente inocuas (como Konfabulator y miniaplicaciones que crean accesos directos desde el escritorio del usuario, conocidas como *Dashboard widgets*) sondean continuamente los servidores de Internet buscando información actualizada. Esta información puede requerir poco ancho de banda (como las actualizaciones del estado del tiempo o de noticias), o mucho ancho de banda (como las cámaras web). Estas aplicaciones deben ser limitadas o bloqueadas por completo.

Las últimas versiones de Windows y Mac OS X tienen un servicio de sincronización horaria. Este mantiene el reloj de la computadora en la hora exacta conectándose a dos servidores de sincronización en Internet. Para

eso es mejor instalar un servidor local de hora y distribuir la hora exacta desde allí, en lugar de ocupar el enlace de Internet con esas solicitudes.

Tráfico de Windows en el enlace a Internet

Las computadoras que tienen el sistema operativo Windows se comunican entre ellas usando ***Network Basic Input/Output System - NetBIOS*** (es una interfaz de programación que permite a las aplicaciones instaladas en computadores diferentes dentro de una red local comunicarse) y ***Server Message Block - SMB*** (un protocolo para compartir archivos, impresoras, puertos y otros servicios y dispositivos entre computadores). Estos protocolos operan sobre TCP/IP y otros protocolos de transporte. SMB es un protocolo que realiza ***elecciones*** para determinar cuál computadora va a ser el ***buscador maestro***. El buscador maestro es una computadora que mantiene una lista de todas las computadoras, recursos compartidos e impresoras que usted puede ver en el ***Entorno de Red.*** La información sobre recursos compartidos también es transmitida a intervalos regulares.

El protocolo SMB fue diseñado para redes LAN y causa problemas cuando la computadora con Windows está conectada a Internet. A menos que el tráfico SMB sea filtrado, se esparcirá por el enlace a Internet, desperdiciando el ancho de banda de la organización. Para prevenirlo se pueden tomar los siguientes pasos:

- Bloquear el tráfico SMB/NetBIOS saliente en el enrutador perimetral o en el cortafuego. Este tráfico consume ancho de banda, y peor aún, presenta un riesgo de seguridad. Muchos “gusanos” en Internet y herramientas de penetración buscan activamente SMB abiertos, y explotan dichas conexiones para ganar ulterior acceso a su red.
- **Instale ZoneAlarm en todas las estaciones de trabajo (no en el servidor).** Una versión gratuita se puede encontrar en *http://www.zonelabs.com/*. Este programa le permite al usuario determinar cuáles aplicaciones pueden hacer conexiones a Internet y cuáles no. Por ejemplo, Internet Explorer necesita conectarse a Internet, pero el Explorador de Windows no. ZoneAlarm puede bloquear el Explorador de Windows para que no lo haga.
- **Reduzca los recursos compartidos de la red.** Idealmente, sólo el servidor de archivos debería tener recursos compartidos. Puede utilizar una herramienta como SoftPerfect Network Scanner (disponible en *http://www.softperfect.com/*) para identificar fácilmente todos los recursos compartidos en su red.

Gusanos y virus

Los gusanos y los virus pueden generar una gran cantidad de tráfico. Por ejemplo el gusano W32/Opaserv aún prevalece, a pesar de que es muy viejo. Se esparce a través de los recursos compartidos de Windows y es detectado por otras personas en Internet porque intenta esparcirse aún más. Por esta razón es esencial que haya una protección anti-virus instalada en todas las PCs. Más esencial aún es la educación de los usuarios en cuanto a no ejecutar archivos adjuntos, así como no dar respuesta a correos no deseados. De hecho debería haber una política de que ni las estaciones de trabajo, ni el servidor, puedan correr servicios que no están utilizándose. Una computadora no debería tener recursos compartidos a menos que fuera un servidor de archivos; y un servidor no debería correr servicios innecesarios. Por ejemplo, los servidores Windows y Unix generalmente corren un servicio de servidor web por omisión. Éste debería deshabilitarse si dicho servidor tiene una función diferente; cuantos menos servicios corra una computadora, menos posibilidades tiene de ser atacada.

Lazos de reenvío de correo electrónico

Ocasionalmente, un error cometido por un único usuario puede llegar a causar un problema serio. Por ejemplo, un usuario cuya cuenta universitaria está configurada para reenviar todo el correo a su cuenta personal en Yahoo. El usuario se va de vacaciones, y todos los correos que le fueron enviados se siguen reenviando a su cuenta en Yahoo la cual puede crecer sólo hasta 2 MB. Cuando la cuenta de Yahoo se llene, va a comenzar a rebotar los correos para la cuenta de la universidad, la cual inmediatamente los va a reenviar a la cuenta de Yahoo. Un lazo de correo electrónico se forma cuando se envían y re-envían cientos de miles de correos, generando un tráfico masivo y congestionando los servidores de correo.

Existen opciones dentro de los servidores de correo que son capaces de reconocer los lazos. Estas opciones deben activarse por omisión. Los administradores también deben tener cuidado de no apagarlas por error. Debe también evitar instalar un sistema de re-envío SMTP que modifique los encabezados de los correos de tal forma que el servidor de correo no pueda reconocer el lazo que se ha formado.

Descargas pesadas

Un usuario puede iniciar varias descargas simultáneas, o descargar grandes archivos tales como 650MB de imágenes, acaparando la mayor parte del ancho de banda. La solución a este tipo de problemas está en el entrenamiento, hacer descargas diferidas, y monitoreo (incluyendo monitoreo en tiempo real, como se subrayó en el capítulo seis). La descarga diferida se puede implementar al menos de dos formas:

En la Universidad de Moratuwa, se implementó un sistema utilizando el direccionamiento URL. A los usuarios que acceden a direcciones **ftp://** se les ofrece un directorio donde cada archivo listado tiene dos enlaces: uno para la descarga normal, y otro para la descarga diferida. Si se selecciona la descarga diferida, el archivo especificado se pone en cola para descargarlo más tarde, y al usuario se le notifica por correo electrónico cuando la descarga está completa. El sistema mantiene una memoria intermedia (*cache*) de archivos descargados recientemente, y cuando los mismos se solicitan de nuevo, los recupera inmediatamente. La cola de descarga se ordena según el tamaño del archivo, por lo tanto los archivos pequeños se descargan primero. Como una parte del ancho de banda se dedica para este sistema aún en las horas pico, los usuarios que solicitan archivos pequeños pueden recibirlos en minutos, algunas veces hasta más rápido que una descarga en línea.

Otro enfoque puede ser crear una interfaz web donde los usuarios ingresan el URL del archivo que quieren descargar. El mismo se descarga durante la noche utilizando una tarea programada (o ***cron job*** por su nombre en inglés). Este sistema funciona solamente para usuarios que no sean impacientes, y que estén familiarizados con los tamaños de archivos que pueden ser problemáticos para descargarlos durante las horas de trabajo.

Envío de archivos pesados

Cuando los usuarios necesitan transferir archivos grandes a colaboradores en cualquier lugar en Internet, se les debe enseñar cómo programar la subida (*upload*) del archivo. En Windows, subir archivos a un servidor FTP remoto se puede hacer utilizando un guión (*script*) FTP, que es un archivo de texto con comandos FTP similares a los siguientes (guardado como **`c:\ftpscript.txt`**):

```
open ftp.ed.ac.uk
gventer
mysecretword
delete data.zip
binary
put data.zip
quit
```

Para ejecutarlo, escriba esto desde la línea de comando:

```
ftp -s:c:\ftpscript.txt
```

En computadoras con Windows NT, 2000 y XP, el comando puede guardarse en un archivo como **`transfer.cmd`**, y ser programado para correr en la noche utilizando las Tareas Programadas (Inicio ➔ Configuración ➔ Panel

de Control ➜ Tareas Programadas). En Unix, se puede hacer lo mismo utilizando las opciones ***at*** o ***cron***.

Usuarios enviándose archivos unos a otros

Los usuarios a menudo necesitan enviarse archivos grandes. Si el receptor es local, es un gasto innecesario de ancho de banda enviarlos vía Internet. Para eso se debe crear un recurso compartido en el servidor web local Windows / Samba / Novell, donde un usuario puede colocar archivos grandes para que otros los descarguen.

Como una alternativa se puede escribir una interfaz web para que un servidor web local acepte un archivo pesado y lo coloque en un área de descarga. Después de cargarlo al servidor web, el usuario recibe un URL cor-respondiente al archivo, que puede transmitir a sus colaboradores locales o internacionales para que accedan al archivo. Esto es lo que ha hecho la Universidad de Bristol con su sistema FLUFF. La universidad ofrece una facilidad para la carga de archivos pesados (FLUFF por su sigla en inglés) disponible en *http://www.bristol.ac.uk/fluff/*. Esos archivos pueden se accedidos por cualquiera al que se le haya dado su ubicación. La ventaja de este enfoque es que los usuarios pueden brindar acceso a sus archivos a usuarios externos, mientras el método de archivos compartidos funciona sólo para los usuarios dentro de la red del campus. Un sistema como este se puede implementar fácilmente como un guión (*script*) CGI utilizando Python y Apache.

9
Voz sobre IP

Este capítulo fue escrito por Alberto Escudero-Pascual y Louise Berthilson, originalmente publicado como “VoIP para el desarrollo, - Una guía para crear una infraestructura de voz en regiones en desarrollo”, gracias al apoyo de la Iniciativa Acacia del Centro Internacional de Investigaciones para el Desarrollo bajo licencia Creative Commons Attribution NonCommercial-ShareAlike 2.5.

No fue hasta la primavera del año 2004 cuando descubrí un programa libre * que era capaz de hacer exactamente lo que necesitaba. Por aquel tiempo vivía en Tanzania y tuve que sufrir, no sólo que la línea telefónica era inestable, sino que, además, las tarifas telefónicas eran totalmente desorbitantes. Tan pronto como conseguí un acceso a la Internet empecé a usar una de esas aplicaciones, tan propietaria como conocida, para hacer mis llamadas a Europa. Pronto me di cuenta que el programa no me daba la flexibilidad que yo quería porque lo que realmente necesitaba era poder hacer llamadas a través de mi línea telefónica en Suecia y poder ofrecer esa conexión de voz a mis vecinos.

La idea de usar la Internet como si fuera una red telefónica no era nueva, pero el proyecto que me daba toda esa flexibilidad era, desde luego, “revolucionario”. El programa que permitía que mi computadora se convirtiera en una centralita telefónica se llamaba “*Asterisk*.” *Asterisk* es un proyecto de código libre basado en las ideas del “Proyecto de Telefonía Zapata”.

No necesité demasiado tiempo para descubrir que Asterisk era capaz de hacer mucho más de lo que nunca me pude imaginar. Mientras lo exploraba me daba cuenta del mundo de posibilidades y oportunidades que ofrecía, especialmente en las regiones en desarrollo. La sensación de aquel

momento era muy parecida a la de mi primera conexión a la World Wide Web en 1994.

Sin duda aprender a poner en marcha un sistema con *Asterisk* fue una tarea que requirió gran perseverancia (sí, algunos me llaman obcecado). Empecé a escribir estas líneas de introducción a la voz IP porque, aunque ya existen algunos libros muy buenos sobre el tema, no he encontrado un documento que describa los conceptos más básicos en palabras que la mayoría de los mortales puedan entender. Esta "guía" pretende describirte los conceptos esenciales de la telefonía sobre IP y darte unos ejemplos concretos de su potencialidad en regiones en desarrollo. Como el reto al escribir este documento era crear un documento breve sin pecar de simplismo, una gran parte del esfuerzo ha sido intentar ser lo más pedagógico posible.

Ten paciencia. La persistencia es la clave del aprendizaje de un autodidacta.

Antes de describir cómo puedes crear tu propio sistema de telefonía, introducimos lo conceptos básicos de telefonía sobre Internet. Dedícale tiempo a leerlos – a largo plazo, entender los conceptos es mucho más importante que instalar un programa u otro.

Las dos siguientes secciones están dedicadas a aquellos que quieran poner la teoría en práctica: montar tu propia centralita e instalando y configurando los programas.

En lugar de listar todas las órdenes y configuraciones posibles, hemos seleccionado tres escenarios prácticos como ejemplos ilustrativos. Recuerda que el objetivo de este documento es ayudarte en tus primeros pasos. Los tres escenarios que hemos elegido son:

- Telefonía privada en una comunidad rural
- Conectando una red local telefónica a la RTB
- Interconectando dos comunidades remotas

Para terminar hemos incluido algunas referencias útiles a algunos recursos que te ayudarán a aprender más.

La poción mágica

Tres son los elementos que te permitirán desplegar una infraestructura de telefonía: **VoIP**, **estándares abiertos** y **los programas libres y abiertos**.

VoIP

Una definición general de Voz sobre IP (también conocida como telefonía IP) es la posibilidad de transportar conversaciones telefónicas en paquetes IP. Cuando hablamos de "VoIP", nos referimos a "la telefonía en Internet" en el sentido más amplio de la expresión. El término VoIP no se refiere a ninguno de los mecanismos concretos que existen para llevar las señales de voz de un sitio a otro en la red. Existen docenas de tecnologías que permiten hablar por la red. Las alternativas tecnológicas de VoIP se pueden dividir de una manera sencilla en dos grandes grupos: tecnologías cerradas-propietarias y sistemas abiertos. En el primer grupo de tecnologías nos encontramos con el conocido Skype o el ya legendario Cisco Skinny (SCCP). Skinny es un protocolo de control para terminales. Originalmente desarrollado por Selsius Corporation y ahora bajo el control y diseño de Cisco Systems, Inc. Uno de los clientes más famosos de Skinny es la serie Cisco 7900 de teléfonos IP.

En el segundo grupo de tecnologías nos encontramos con los estándares abiertos basados en SIP, H.323 o IAX. El protocolo de inicio de sesión (SIP) es el resultado del trabajo del IETF y define el manejo de sesiones entre uno o más participantes. H.323 es un conjunto de recomendaciones de la UIT-T que define un grupo de protocolos para ofrecer sesiones audiovisuales en una red conmutada de paquetes. El H.323 se usa en el famoso programa Netmeeting. IAX2 es un protocolo de comunicación de voz IP que se usa en *Asterisk*, una centralita de código abierto y libre. IAX2 permite conexiones entre servidores *Asterisk* y clientes IAX2.

H.323 es un protocolo desarrollado por la UIT que cobró cierta fama porque era el más usado por los grandes operadores en sus redes troncales. SIP ha incrementado su popularidad cuando las tecnologías de VoIP se han hecho más presentes en el "bucle local." El bucle de área local es un enlace físico que conecta al cliente con la terminación de la red de telefonía del proveedor de servicios de telecomunicaciones.

Últimamente hemos presenciado el nacimiento y el fuerte crecimiento de una nueva alternativa conocida como IAX. IAX2 (por ser la versión 2) está fuertemente influido por el modelo comunitario de desarrollo abierto y tiene la ventaja de haber aprendido de los errores de sus predecesores. IAX2 resuelve muchos de los problemas y limitaciones de H.323 y SIP. Aunque IAX2 no es un estándar en el sentido más oficial de la palabra, no sólo tiene el gran reconocimiento de la comunidad sino todos los pre-requisitos para convertirse en el remplazo (de facto) de SIP. Aún es un RFC, - Request for Comments, en castellano: solicitud de comentarios. Los RFC son una serie de documentos numerados e informales que buscan construir consensos en favor de la estandarización de protocolos y servicios para la Internet.

Una de las características esenciales de todos los protocolos tradicionales de voz sobre IP es el derroche de ancho de banda. Ese exceso de bits en la red es debido a la necesidad de enviar información adicional en cada una de las cabeceras de los paquetes IP. Este problema tiene especial importancia en regiones en desarrollo donde el acceso a ancho de banda es limitado y los costes de conexión a Internet pueden llegar a ser hasta 100 veces mayor que en Europa o Norteamérica. Por ejemplo, 1 Mbps en el Este de África cuesta más de 1000 USD/mes mientras que la misma capacidad en Suecia cuesta menos de 10 USD/mes.

Para que te hagas una idea del gasto adicional de ancho de banda necesario para enviar voz sobre Internet podemos citar como ejemplo que un audio comprimido de 5.6 kbit/seg necesita de hasta 18 kbit/seg. La diferencia entre los 5.6 y los 18 kbit/seg son esos bits en las cabeceras de los paquetes. Las cabeceras son toda esa información adicional que es necesaria para encaminar correctamente cada uno de los paquetes de voz al receptor. Una de las ventajas de IAX2 es que ha sido capaz de reducir considerablemente ese exceso de bits por paquete. Además, es capaz de agrupar los paquetes de distintas conversaciones, que van en una misma dirección en la red, en uno sólo. Al ser capaz de agregar múltiples paquetes de distintas conversaciones dentro de uno sólo, el exceso de información introducido por las cabeceras se reduce en cada una de las conversaciones.

Como resultado de las pruebas realizadas durante la elaboración de esta guía (usando una conexión telefónica a la red), evidenciamos las ventajas de utilizar IAX2 frente a la misma conversación usando SIP. Una conversación de voz IP usando un codec como el G.729 (8 Kbps) requiere unos 30 Kbps usando SIP y tan sólo 24 Kbps con IAX2. Si agregamos cinco llamadas simultáneas cada llamada se reduce a 13 Kbps.

Estándares Abiertos y Código Libre

No podríamos estar hablando de la libertad de construir nuestra propia red telefónica sin la existencia de los estándares abiertos y el código libre. Los estándares abiertos permiten que cualquiera pueda implementar un sistema con garantías de interoperabilidad. Gracias a esa interoperabilidad de nuestro diseño no sólo podemos crear nuestra red telefónica sino que, además, podemos conectarla a la red telefónica global. Con el código libre podemos aprender de experiencias parecidas, integrar sus soluciones y compartir nuestros propios resultados con los demás.

Una de la primeras preguntas que merece una respuesta es: ¿por qué deberías crear tu propia infraestructura de voz sobre IP y no seguir usando servicios gratuitos como Skype?

La respuesta es simple: sostenibilidad y flexibilidad. Los servicios gratuitos te pueden solucionar una necesidad a corto plazo pero nunca garantizar tu independencia o el control de tu propio proceso de aprendizaje y desarrollo. No se trata de una cuestión puramente técnica. El problema no es decidir cuál es la mejor de las tecnologías sino cuál es la que permite que las comunidades sean dueñas de su propio desarrollo y que puedan adaptarla a sus propias necesidades.

Es muy difícil imaginar un desarrollo sostenible sin transferencia de conocimiento y reapropiamiento tecnológico. Una solución basada en estándares abiertos y código libre no es sólo una buena solución desde un punto de vista puramente técnico sino que además permite la posibilidad de adaptación para mejorarse a la realidad local.

Para ser conscientes de la importancia de los estándares abiertos quizás sea bueno empezar presentando una definición de "estándar." Un estándar es un conjunto de reglas, condiciones o requerimientos que describen materiales, productos, sistemas, servicios o prácticas. En telefonía, los estándares garantizan que todas las centrales de telefonía sean capaces de operar entre sí. Sin ese conjunto de reglas comunes un sistema de telefonía de una región sería incapaz de intercambiar llamadas con otro que esté, tan sólo, unos kilómetros más allá. Aunque muchos de los estándares de telefonía son públicos, los sistemas siempre han estado bajo el control de un grupo muy limitado de fabricantes. Los grandes fabricantes de sistemas de telefonía son los únicos capaces de negociar contratos a nivel regional o incluso nacional. Ésta es la razón que puede explicar porqué es muy común encontrar siempre el mismo tipo de equipos a lo largo de un mismo país.

Los equipos de telefonía tradicionales, además, tienen la particularidad de haber sido diseñados para realizar un conjunto de tareas muy concretas. Normalmente, son equipos informáticos con aplicaciones muy específicas. Aunque las reglas que gobiernan la telefonía (los estándares) son relativamente abiertas, no es el caso de los equipos informáticos que los implementan. Al contrario de los estándares, el funcionamiento interno siempre se mantiene en secreto.

Dentro de la "poción mágica de la telefonía" los estándares abiertos son un ingrediente necesario, pero lo que realmente ha permitido esta nueva "revolución" ha sido la posibilidad de emular la funcionalidad de los sistemas de telefonía tradicionales con un programa funcionando en un computador personal. Todos los elementos necesarios están a tu alcance:

- tienes el acceso a los programas y a los equipos que permiten el intercambio de conversaciones telefónicas.
- tienes una red abierta y pública para intercambiar esas llamadas (la Internet).

- tienes la posibilidad de modificar cada uno de los elementos para adaptarlos a tus propias necesidades.

Asterisk

Asterisk es una implementación libre de una centralita telefónica. El programa permite tanto que los teléfonos conectados a la centralita puedan hacer llamadas entre ellos como servir de pasarela a la red telefónica tradicional. El código del programa fue originalmente creado por Mark Spencer (Digium) basado en las ideas y el trabajo previo de Jim Dixon (proyecto de telefonía Zapata). El programa, sus mejoras y correcciones, es el resultado del trabajo colectivo de la comunidad del software (programas) libre. Aunque *Asterisk* puede funcionar en muchos sistemas operativos, GNU/Linux es la plataforma más estable y en la que existe un mayor soporte.

Para usar *Asterisk* sólo se necesita un computador personal (PC), pero si quieres conectarte a la red telefónica tradicional debes añadir el correspondiente periférico dedicado.

La receta

Esta sección resume los conceptos principales de VoIP. Entender cada uno los conceptos te va a ser muy útil cuando configures cualquier tipo de programa relacionado con telefonía IP. Aunque VoIP es una área enorme de conocimiento, hemos seleccionado cuidadosamente siete conceptos esenciales: PBX, PSTN – RTB, Señalización en telefonía tradicional, Señalización en telefonía IP, Señalización en telefonía IP, Equipamiento para VoIP, Codecs y Calidad de Servicio. Esta sección incluye una descripción, básica pero sólida, de lo que necesitas saber para dar tus primeros pasos en la creación de un sistema de telefonía.

PBX

El término PBX o PABX es una de esas siglas que dicen bastante poco. PBX son las primeras letras del término inglés Private (Automatic) Branch Exchange. En palabras simples, el uso más común de una PBX es compartir de una a varias líneas telefónicas con un grupo de usuarios. Una PBX se emplaza entre las líneas telefónicas y los teléfonos (terminales de voz). La PBX tiene la propiedad de ser capaz de redirigir las llamadas entrantes a uno o varios teléfonos. De una manera similar, una PBX permite a un teléfono escoger una de las líneas telefónicas para realizar una llamada telefónica al exterior. De la misma forma que un enrutador (router) en Internet es responsable de dirigir los paquetes de un origen a su destino, una PBX es responsable de dirigir “llamadas telefónicas”.

La palabra “private” en la sigla PBX significa que el dueño del sistema tiene todo el control y decide como compartir los líneas exteriores con los usuarios. Una PBX no sólo permite compartir un conjunto de líneas con un grupo de usuarios sino que también ofrece la posibilidad de crear servicios de valor añadido como transferencia de llamadas, llamadas a tres , pasarela de voz a correo o servicios basados en una respuesta de voz interactiva (IVR), etc.

A manera de aclaración de los términos utilizados anteriormente:

- Llamada-a-tres es la posibilidad de tener a más de dos personas hablando simultáneamente en la misma conversación.
- Una pasarela de voz a e-mail permite grabar un mensaje de voz en un adjunto de correo electrónico (como si fuera un contestador automático). El mensaje se graba en un archivo de audio y se envía a una cuenta de correo.
- Un sistema de voz interactivo (Interactive Voice Response) permite seleccionar una opción de un menú a través de la voz o del teclado del terminal.

Una PBX puede ser de gran utilidad en múltiples escenarios. Piensa en las regiones donde el acceso a la red telefónica implica caminar varias horas (sino días) a una cabina o Telecentro. Además, una situación muy común es que sólo exista una línea telefónica por edificio o por población. Una PBX (tu centralita) permitirá compartir esa línea e incluso extender la red telefónica a lugares remotos.

PSTN - RTB

PSTN es la Red Pública Telefónica Conmutada (Public Switched Telephone Network), “la red de redes telefónicas” o más conocida como “la red telefónica.” En castellano la PSTN es conocida como la red pública conmutada (RTC) o red telefónica básica (RTB). De la misma forma que Internet es la red global IP, la RTB es la amalgama de todas las redes conmutadas de teléfono. Una diferencia muy importante entre la RTB e Internet es la noción de “flujo de información”. En telefonía los flujos de información son cada una de las llamadas o conversaciones mientras que en Internet es cada uno de los paquetes de datos. Desde el punto de vista conceptual la RTB e Internet son muy diferentes y representan dos mundos y filosofías casi antagónicas. Si una conversación se efectúa en una RTB se tiene que reservar un canal (circuito) dedicado de 64 Kbps, pero en Internet la misma conversación puede coexistir con otros servicios de manera simultánea. Aunque esta diferencia pueda parecer irrelevante a primera vista, tiene grandes implicaciones de cara a la implementación de las tecnologías de la información tanto en regiones desarrolladas como en

desarrollo. En el modelo tradicional, un "cable de cobre" proporciona acceso a la RTB y ofrece un sólo tipo de servicio: un canal analógico. Si ese mismo cable se usa para conectarse a una red conmutada de paquetes como Internet, se puede implementar cualquier tipo de servicio basado en el protocolo IP.

La RTB ha estado históricamente gobernada por estándares creados por la UIT, mientras que Internet es gobernada por los estándares del IETF.

La ITU o UIT en castellano es la Unión Internacional de Telecomunicaciones, una organización internacional responsable de estandarización, gestión del radio espectro y de la organización de acuerdos de interconexión entre países que permitan el intercambio de llamadas internacionales. La UIT es parte de la ONU y tiene una estructura de miembros formal.

El IETF (*Internet Engineering Task Force*) es un conjunto de grupos de trabajo responsables de estandarización de Internet. La organización es abierta, formada por voluntarios y sin ningún requerimiento formal para ser miembro.

Ambas redes, la RTB e Internet usan direcciones para encaminar sus flujos de información. En la primera se usan números telefónicos para conmutar llamadas en las centrales telefónicas, en Internet se usan direcciones IP para conmutar paquetes entre los enrutadores (*routers*).

Señalización en telefonía tradicional

Las centrales telefónicas son los "routers" de la RTB. Un Foreign Exchange Office (FXO) es cualquier dispositivo que, desde el punto de vista de la central telefónica, actúa como un teléfono tradicional. Un FXO debe ser capaz de aceptar señales de llamada o ring, ponerse en estado de colgado o descolgado, y enviar y recibir señales de voz. Asume que un FXO es como un "teléfono" o cualquier otro dispositivo que "suena" (como una máquina de fax o un módem).

Un Foreign Exchange Station (FXS) es lo que está situado al otro lado de una línea telefónica tradicional (la estación). Un FXS envía el tono de marcado, la señal de llamada que hace sonar los teléfonos y los alimenta. En líneas analógicas, un FXS alimenta al FXO. El FXS utiliza alrededor de 48 voltios DC para alimentar al teléfono durante la conversación y hasta 80 voltios AC (20 Hz) cuando genera el tono de llamada (ring).

Una PBX que integra periféricos FXO y FXS puede conectarse a la RTB y incorporar teléfonos analógicos. Las líneas telefónicas que vienen del operador se tienen que conectar a una interfaz FXO. Los teléfonos se deben conectar a las interfaces FXS de la centralita.

En resumen, dos reglas fáciles que debes recordar son:

4. Un FXS necesita estar conectado a un FXO (como una línea telefónica necesita estar conectada a un teléfono) o viceversa.
5. Un FXS suministra energía (elemento activo) a un teléfono FXO (elemento pasivo)

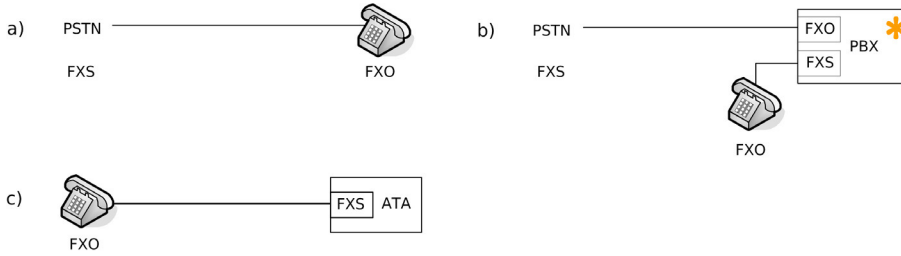


Figura 9.1: a) Un teléfono analógico es un dispositivo FXO conectado a una línea telefónica (RTB) actuando como FXS b) Una PBX puede incorporar tanto interfaces FXS como FXO. c) Un adaptador telefónico o ATA actúa como un FXS.

Señalización analógica

Cada vez que usas una línea telefónica se intercambian un conjunto de "señales". Las señales sirven para ofrecer información del estado de la llamada al usuario. Algunas de esas señales son el tono de marcado o el tono de línea ocupada. Estas señales se transmiten entre el FXS y el FXO haciendo uso de un protocolo conocido como "señalización".

Por desgracia, existen muchas maneras de generar este tipo de señales. Cada uno de los mecanismos es conocido como "método de señalización". Los métodos de señalización son diferentes de un lugar a otro, así que debes conocer de antemano el método de señalización que se usa en tus líneas telefónicas. Dos de los métodos de señalización más conocidos son el "loop start" y el "ground start". Si desconoces el método de señalización que debes usar puedes empezar probando con "loop start". Una consecuencia de configurar tu PBX con un método de señalización equivocado es que la línea telefónica se cuelga de manera inesperada.

Señalización entre centrales telefónicas

SS7 es un grupo de estándares desarrollados originalmente por la AT&T y la UIT que, entre otras cosas, se encargan de la gestión del establecimiento de llamadas y su encaminamiento entre centrales telefónicas en la RTB. Una cosa muy importante que debes entender es que en la red telefónica tradicional, la voz y las señales auxiliares (señalización) están claramente separadas. Esto significa que existe un "circuito" dedicado a voz y otro circuito independiente para el intercambio de las señales encargadas del

establecimiento de las llamadas. Esta información "adicional" necesaria en cada llamada se intercambia usando un protocolo conocido como SS7.

El hecho de que la voz y la señalización están separadas significa que los flujos de información pueden tomar caminos físicos totalmente diferentes. Imagínate que las "conversaciones" pueden viajar por un cable mientras que los números de teléfono de los comunicantes se envían por otro. Este concepto es importante para entender la siguiente sección: señalización en telefonía IP.

Señalización en telefonía IP

Por herencia histórica, la señalización en voz sobre IP sigue unos principios muy parecidos a la señalización en RTB. Las señales y las conversaciones están claramente diferenciadas. En esta sección introducimos dos protocolos de VoIP que vamos a integrar en nuestra futura PBX: SIP e IAX2.

Session Initiation Protocol (SIP)

El protocolo de señalización de inicio de sesión, del inglés Session Initiation Protocol (SIP), es una especificación para Internet para ofrecer una funcionalidad similar al SS7 pero en una red IP. El protocolo SIP, desarrollado por el IETF, es responsable de establecer las llamadas y del resto de funciones de señalización. Recuerda que, cuando hablamos de señalización en el contexto de llamadas de voz, estamos hablando de la indicación de línea ocupada, los tonos de llamada o que alguien ha contestado al otro lado de la línea.

SIP hace tres cosas importantes:

1. Encargarse de la autentificación.
2. Negociar la calidad de una llamada telefónica (Una de las grandes diferencias entre la telefonía tradicional y la IP es que la calidad de servicio de una conversación se puede negociar).
3. Intercambiar las direcciones IP y puertos que se van utilizar para enviar y recibir las "conversaciones de voz".

Servidores Proxy

Aunque dos dispositivos SIP (teléfonos IP) pueden comunicarse directamente, SIP normalmente hace uso de algunos elementos adicionales llamados "proxies" para facilitar el establecimiento de las llamadas. Un "proxy" opera como un representante (apoderado) que se encarga de negociar entre dos partes. Con la ayuda de un "proxy" puedes mover físicamente tu número de teléfono en Internet. Los números no están asociados a un sitio concreto sino que se pueden mover siempre y cuando

notifiquemos al “proxy” de nuestra (nueva) ubicación. Como el “proxy” funciona como un intermediario es capaz de indicar a las partes dónde se encuentran los teléfonos. Este servidor intermedio en SIP aprende la posición de sus usuarios durante un proceso que se conoce como “registro”.

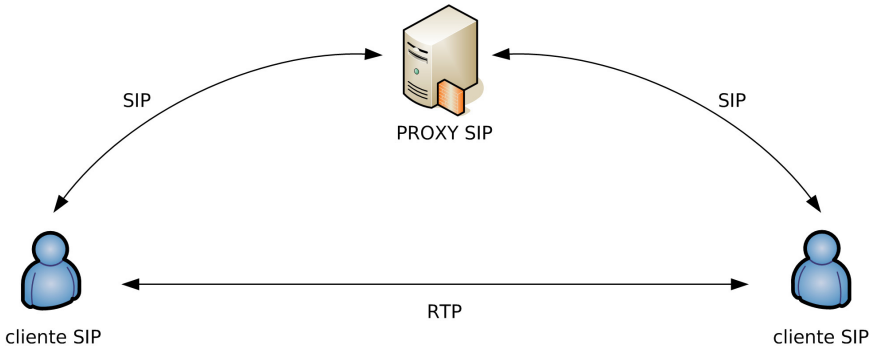


Figura 9.2: El proceso de registro entre clientes y el servidor “proxy”. La señalización (SIP) y las conversaciones de voz (RTP) viajan por caminos diferentes.

Protocolos en tiempo real y el NAT

En Internet, las conversaciones que usan señalización de tipo SIP resultan en flujo constante de paquetes de pequeño tamaño entre los comunicantes. Estos paquetes de voz hacen uso de otro protocolo llamado RTP. El protocolo de transporte de tiempo real o Real-time Transport Protocol (RTP) es el encargado de llevar las conversaciones (la voz) de un lado a otro. En el RTP se define un mecanismo estándar para enviar audio y vídeo en Internet. De la misma forma que en una conversación existen dos flujos de voz, en una conversación en una red IP tenemos dos flujos de paquetes RTP.

Los Network Address Translators (NATs) son los grandes enemigos del RTP. Una red con un NAT consiste en varios computadores compartiendo, con el mundo exterior, una sóla dirección IP pública. Las máquinas situadas dentro de la red NAT usan direcciones “privadas”. Aunque el NAT permite conectar más fácilmente computadores a la red, lo hace al precio de no permitir una conexión puramente bi-direccional. El efecto de un NAT en voz sobre IP es que no se pueden recibir conexiones iniciadas desde el exterior.

Existen varios problemas relacionados con NAT y VoIP. El más común de los problemas es conocido como “audio en una sola dirección” (one-way audio). Como recordarás, una conversación está compuesta por dos flujos de paquetes RTP distintos. En presencia de un NAT, sólo el flujo de dentro a fuera no es bloqueado; el flujo de fuera a dentro no tiene la misma suerte y puede atravesar el NAT. La consecuencia: el que inicia la llamada desde dentro del NAT no puede escuchar a la otra parte. Si los dos comunicantes

se encuentran dentro de NATs las cosas se complican aún más, hasta el punto de que ningún flujo de audio llega a su destino final.

Por desgracia, las direcciones IP privadas y los NAT están especialmente presentes en todos los lugares de las regiones en desarrollo. Configurar una red con señalización SIP y NATs no es trivial. Esta guía incluye algunos consejos generales en la sección que describe los escenarios prácticos.

Inter-Asterisk eXchange (IAX)

La segunda versión del protocolo de comunicación entre *Asterisks* (Inter-*Asterisk* eXchange) se conoce como IAX2. IAX2 es un protocolo de telefonía IP que utiliza un reducido número de bits en las cabeceras y que está diseñado para permitir la comunicación entre centralitas y clientes *Asterisk*. El contenido de voz en los paquetes se envía usando una cabecera de tan solo 4 octetos (32 bits). Una cabecera más compleja de 12 octetos se utiliza con los paquetes de control y en algunos paquetes especiales de voz (uno por minuto aproximadamente).

IAX2 es una alternativa al protocolo de señalización SIP. IAX2 fue creado como parte del desarrollo de la PBX *Asterisk*. A diferencia del SIP, que usa dos flujos de datos para voz y otros dos para señalización, IAX2 usa sólo un par de flujos donde voz y datos coexisten. Esta forma de enviar tanto las conversaciones como la señalización por el mismo canal se conoce como *in-band*, en contraste con el método que usa SIP, el *out-of-band*. La idea de enviar la señalización dentro del canal de voz (*in-band*) obliga a separar los paquetes de voz de los paquetes de señalización. Aunque este diseño requiere más gasto de procesamiento (CPU) ofrece mejores propiedades en presencia de cortafuegos y NATs.

Debido a su diseño, IAX2 es la opción más adecuada en regiones en desarrollo donde existen gran presencia de NATs. Además, IAX2 es capaz de empaquetar llamadas simultáneas en un sólo flujo de paquetes IP. Este mecanismo es conocido como “trunking” y su implementación resulta en ahorros en el consumo de ancho de banda.

El concepto de “trunking” se puede explicar con la siguiente metáfora: imagínate que necesitas mandar cinco cartas a gente que vive en otro país. Una posibilidad es usar un sobre por cada una de las cartas; la otra es usar un único sobre e incluir el nombre del destinatario final en la cabecera de cada una de las cartas. La agregación de llamadas en telefonía IP funciona de la misma forma y permite enviar múltiples cartas (llamadas) en un único sobre (paquete IP).

En resumen, el diseño de IAX2 es más adecuado para regiones en desarrollo por tres razones:

1. Reduce el uso de ancho de banda por llamada.
2. Está diseñado para operar en presencia de NATs (soporte nativo) y es más fácil de usar detrás de los cortafuegos.
3. Reduce aún más el ancho de banda cuando se realizan varias llamadas simultáneas (como resultado del "trunking")

Equipamiento para VoIP

Teléfonos VoIP

Un teléfono de VoIP o teléfono IP es un equipo especialmente diseñado para conectarse a una red de telefonía IP. Los teléfonos IP pueden implementar uno o varios protocolos de voz sobre IP.En Septiembre del 2006 ya existen varias compañías que han fabricado teléfonos IP con soporte IAX2.

Algunas de las características que debes tener en cuenta cuando compres un teléfono IP son:

- Ancho de banda reducido: inclusión de codecs de alta compresión (e.g. G.729, gsm, speex).
- Buena interfaz de administración: inclusión de interfaz web.
- Salida de audio: inclusión de salida externa de audio y soporte de manos-libres (para educación a distancia).

Existen muchos modelos en rango de precios de 100-120 USD que hacen mucho más de lo que vas a necesitar y funcionan perfectamente con Asterisk. Como parte del trabajo de investigación que inspiró el desarrollo de la guía de donde surgió este capítulo, hemos evaluado de manera positiva los siguientes modelos con Asterisk: SwissVoice IP10S (150 USD), Thomson ST2030 (100 USD), Gulfstream Budgetome (75 USD) y el Cisco 7940 (300 USD).

Telefonía con Software – Soft Phones

Una alternativa al uso de equipos dedicados (físicos) de VoIP es el uso de programas para emularlos. Estos programas se conocen como "soft phones" y funcionan en cualquier computador personal. El único requerimiento es tener una tarjeta de sonido en funcionamiento y estar seguro de que el cortafuegos instalado en tu máquina no está bloqueando a la aplicación. Los siguientes teléfonos "softphones" han sido evaluados como parte de este trabajo: IAXClient (IAX2), X-Lite (SIP).

Si quieres reducir el ancho de banda usado por tus conversaciones elige un "soft phone" que tenga soporte para el protocolo IAX2 y activa un codec de alta compresión.

Tarjetas de interfaz a la RTB

Si quieres encaminar las llamadas de tus terminales de VoIP a la red telefónica tradicional (RTB) necesitas un periférico especializado en la PBX. Una solución modular para *Asterisk*, que permite conectar líneas y teléfonos analógicos, es una tarjeta PCI fabricada por Digium: *TDM400P wildcard* (la palabra inglesa wildcard significa "comodín").

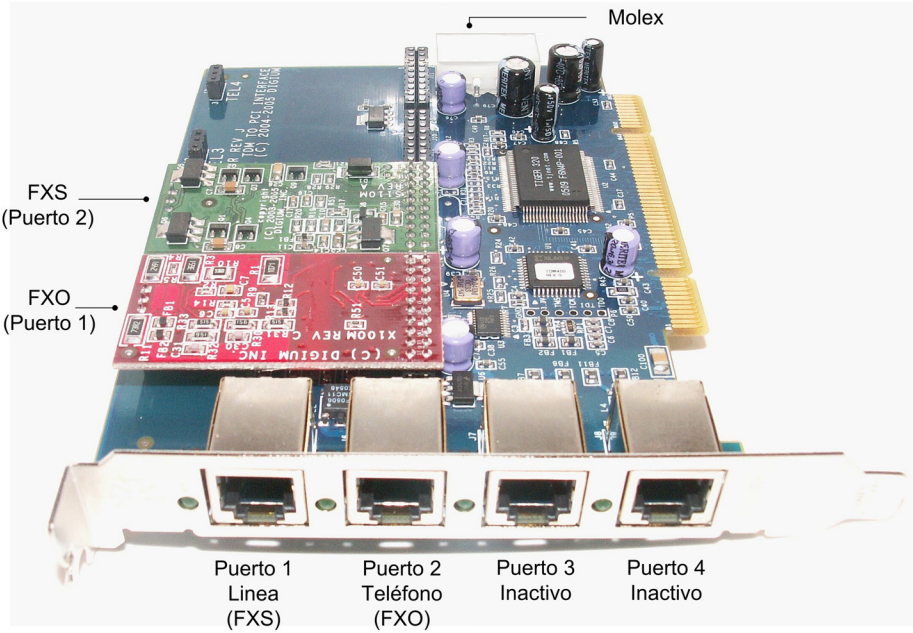


Figura 9.3: Un tarjeta TDM400P con sus cuatro puertos. Los dos primeros puertos (Puerto 1: FXO, Puerto 2: FXS) están ocupados mientras que los dos últimos puertos (Puerto 3 y 4) están inactivos.

La tarjeta, conocida como "TDM wildcard" o simplemente "TDM", tiene cuatro puertos y se llama "wildcard" porque permite insertar un máximo de cuatro expansiones. Las expansiones son módulos de unidades FXO o FXS. Desde el punto de vista práctico esto significa que a la TDM se le pueden conectar hasta cuatro líneas telefónicas (4 módulos FXO), o dos líneas entrantes (2 FXO) y dos teléfonos analógicos (2 FXS modules), etc.

Una buena idea es comprar inicialmente la versión de la TDM400P con dos módulos. Un módulo FXO (para conectar una línea telefónica) y un FXS (para conectar un teléfono analógico). Si en el futuro necesitas expandir la tarjeta siempre puedes añadir módulos extra más tarde.

Adaptador para Teléfonos Analógicos (ATA)

Un adaptador para teléfonos analógicos (ATA) o en breve, adaptador telefónico (TA) conecta un teléfono ordinario a una red de VoIP. Un ATA tiene un conector RJ-11 (el conector de teléfono) y un RJ-45 (el conector de red o Ethernet). Un ATA funciona como si fuera un adaptador FXS, por un lado habla con el teléfono analógico y por el otro opera en modo digital con la red de voz IP. Si quieres implementar una red en una región en desarrollo no es una mala opción utilizar ATAs en lugar de teléfonos IP. Los ATAs suelen ser más baratos y al ser más pequeños suelen ser más fáciles de "nacionalizar" en las aduanas. Otra de las ventajas de usar un ATAs es que puedes conectar cualquier tipo de aparato telefónico a la red IP, por ejemplo, se pueden conectar una cabina telefónica (de monedas o tarjeta), un fax o un teléfono inalámbrico (DECT). Los siguientes adaptadores telefónicos (ATA) han sido evaluados como parte de este trabajo: Sipura SPA-3000, GlobelTex IAD.

Una de las opciones tipo ATA que usa el protocolo IAX2 es el módelo s101i de Digium. Este ATA también se le conoce con el nombre de IAXy. El IAXy es una ATA de reducido tamaño con soporte IAX2. El ATA no soporta codecs de alta compresión.

Codecs

Un algoritmo compresor/de-compresor (codec) es un conjunto de transformaciones utilizadas para digitalizar la voz. Los codecs convierten tanto la voz en datos (bits) como los datos en voz. Un codec toma una señal analógica y la convierte en una señal digital en un formato binario (0s y 1s). Existen muchas formas de digitalizar audio y cada una de esas formas resulta en un tipo de codec. En general puedes asumir que a mayor compresión vas a obtener mayor distorsión (peor calidad). Un codec se considera mejor que otro cuando es capaz de ofrecer mejor calidad de voz usando la misma cantidad de ancho de banda.

Un circuito de la RTB (el teléfono de siempre) usa un codec conocido como Modulación por Impulsos Codificados (MIC) del inglés Pulse Code Modulation (PCM). El MIC es un codec de alta calidad que necesita 64 kbps. Dos estándares de compresión MIC son el micro-law (u-law) y el a-law. A estos estándares se les conoce también como G711u y G711a respectivamente. El micro-law se usa normalmente en Norteamérica y el a-law en Europa. La familia de codecs G711 no requieren de gran procesamiento y por eso están disponibles en la mayoría (si no todos) los equipos de voz IP.

En países en desarrollo, el uso del G.711 no es viable porque requiere demasiado ancho de banda. Debes considerar otro tipo de codecs que hagan un uso más efectivo del los recursos disponibles en la red.

Unas buenas opciones de codecs libres y que usan poco ancho de banda son el codec de GSM y el Speex. El G.729 es un codec propietario altamente robusto pero requiere de una licencia para su uso comercial. G.729 es un codec de 8 kbps (aprox. 30 Kbps por conversación usando SIP). El codec fue desarrollado por un consorcio de organizaciones: France Telecom, Mitsubishi Electric Corporation, Nippon Telegraph and Telephone Corporation (NTT) y la Universidad de Sherbrooke. El precio del codec es de 10 USD. Ver *http://www.digium.com/en/products/voice/g729codec.php*.

Calidad de Servicio

La calidad de servicio o Quality of Service (QoS) es la capacidad de la red para ofrecer mejoras en el servicio de cierto tipo de tráfico de red. Uno de los grandes retos al implementar VoIP, especialmente en regiones en desarrollo, es garantizar que exista un ancho de banda constante para las conversaciones. Para ofrecer una buena calidad en la conversación, el ancho de banda que necesitan los dos flujos de tráfico se debe garantizar con independencia del estado del resto de las conexiones (incluso si la conexión a Internet está altamente ocupada). Cuando diseñes una red de voz IP debes intentar optimizar el ancho de banda, controlar las fluctuaciones de la red (jitter), y minimizar la latencia. Debes prestar atención especial a los casos donde vayas a usar VoIP en redes inalámbricas, como las que están basadas en IEEE 802.11b/g/a. En estas redes tienes que asegurarte que les das prioridad al tráfico de voz.

Latencia

Latencia es sinónimo de retraso, y mide el tiempo que tarda un paquete en viajar de un punto a otro. Para mejorar la calidad de las conversaciones de voz sobre IP es necesario reducir los retrasos al máximo, dando la máxima prioridad al tráfico de voz. Dar más prioridad a los paquetes de voz significa que se les deja “saltarse la cola” de salida y así ocupar una mejor posición que el resto de los paquetes que están esperando para ser transmitidos.

Si la comunicación requiere el uso de un enlace por satélite vas a tener que contar con, al menos, una latencia de 300 ms (0.3 segundos). Para poder reducir el retraso tienes que implementar buenas políticas de calidad de servicio en los enrutadores (routers) y conmutadores (switches) por los que atraviesa tu tráfico de voz. Aunque una conversación es técnicamente posible si existen dos o más enlaces de satélite entre los comunicantes, tienes que estar preparado para esperas del orden de un segundo. Una

regla de oro para minimizar la latencia es colocar tu centralita (PBX) en el segmento menos congestionado o saturado de la red.

Jitter – Fluctuaciones de velocidad

En VoIP, el jitter es la variación del tiempo entre la llegada de distintos paquetes. Estas variaciones son debidas a la saturación de la red, la falta de sincronismo o los cambios dinámicos en las rutas. En redes con grandes cambios de velocidad se puede usar un "*jitter buffer*" para mejorar la calidad de la conversación. Un buffer es un espacio intermedio donde se almacenan los paquetes hasta su procesamiento. La idea básica del "*jitter buffer*" es retrasar deliberadamente la reproducción del sonido para garantizar que los paquetes más "lentos" hayan llegado. Los paquetes se almacenan en el buffer, se reordenan si es necesario y se reproducen a una velocidad constante. La calidad de voz mejora al precio de incrementar la latencia total.

Muchos equipos de VoIP te dejan ajustar el tamaño del "*jitter buffer*". El buffer es ese área donde los paquetes se almacenan para luego ser enviados al procesador de voz en intervalos constantes. El tamaño del buffer se mide en milisegundos. Si el buffer es de 200 ms significa que introducimos un retraso (esperamos) ese tiempo antes de reproducir la voz.

Existen dos tipos de jitter buffers: estático y dinámico. Un buffer estático está implementado como parte del equipo y configurado de manera fija por el fabricante. El dinámico se configura usando un programa y lo puede cambiar el usuario. Un valor común del jitter buffer es de 100 ms. Al incrementar el buffer vamos a mejorar la calidad de la conversación pero no olvides que lo que estás haciendo es incrementar el retardo total (latencia). Debes buscar un valor de compromiso. Ten en cuenta que un retraso total muy por encima de 300 ms hace muy difícil tener una conversación.

Manos a la obra
Puesta en práctica–Creando tu propia PBX

¿Qué es lo que necesito?

Lo primero que vas a necesitar es una computadora personal. Cualquier máquina fabricada después del año 2000 debe tener suficiente potencia para hacer funcionar *Asterisk*. A medida que tu sistema crece (especialmente si usas codecs de alta compresión) tendrás que considerar un buen procesador y memoria, pero para empezar cualquier máquina es buena. La computadora debe funcionar con cualquier distribución del sistema operativo Linux.

La manera más barata de empezar es utilizar "softphones". El primer ejercicio es aprender a configurar *Asterisk* para poder establecer una llamada entre dos "softphones" a través de tu PBX. Tus primeros ensayos los puedes hacer con dos computadores con tarjetas de sonido. Instala dos clientes de VoIP en cada uno de los computadores y usa un tercero para instalar y configurar *Asterisk*.

En el caso de que quieras usar equipos físicos de voz IP (teléfonos VoIP o ATA), o conectarte con la RTB vas a necesitar algunos de los componentes descritos más adelante.

Si quieres construir una PBX portátil y de bajo consumo de energía consulta las soluciones basadas en placa base mini-ITX. Como parte de esta guía construimos una centralita usando el modelo EPIA M10000 (también conocida como Nehemiah). La placa base tiene dos ranuras PCI donde puedes conectar la tarjeta multiuso Digium TDM400P que es compatible con el estándar PCI 2.2. Un "centralita portátil" te permitirá demostrar la tecnología y al mismo tiempo te ofrece la posibilidad de transportar tu propio demostrador como equipaje de mano.

Consejos de instalación

Ésta es una lista de consejos de instalación si necesitas instalar una tarjeta PCI TDM400P:

- Asegúrate de que tu máquina tiene una ranura PCI 2.2 libre.
- Si vas a usar un módulo FXS en la tarjeta TDM400P tienes que tener un cable de alimentación con un conector "*molex*" libre. Un conector del tipo Molex es un conector de alimentación de 4-pin de uso común en PCs. Los cables amarillos y rojos dan una tensión de +12V y +5V respectivamente, el cable negro es tierra.
- Si vas a usar una placa base de tamaño reducido como las mini-ITX vas a necesitar una "*raiser PCI*". La tarjeta "*raiser*" gira la posición de la TDM400P 90 grados. Es necesario girar la tarjeta para que entre dentro de la caja.
- ¡No conectes una línea telefónica a un puerto FXS! Al conectar un puerto FXS con otro FXS se puede quemar el módulo.

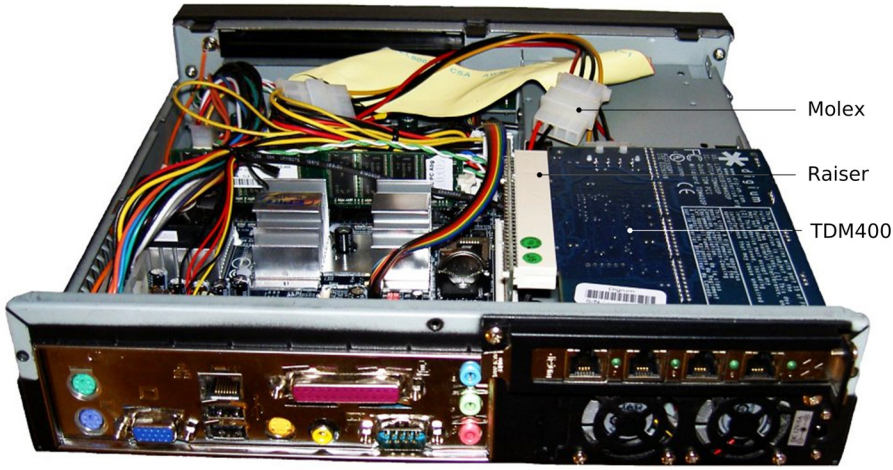


Figura 9.4: Una central telefónica portátil basada en una placa mini-ITX con una tarjeta Digium TDM400P

Instalando Asterisk

Asterisk no es sólo un programa de gran tamaño sino que, además, sigue creciendo al integrar más funcionalidades cada día. Su diseño y arquitectura es tan potente como flexible. La flexibilidad de *Asterisk* también implica cierta complejidad debido a las numerosas posibilidades y opciones. El programa es una herramienta tan potente que puede hacer probablemente todo lo que te puedes imaginar, pero los primeros pasos no son fáciles. Aprender a configurar *Asterisk* me recuerda a esas largas noches de hace diez años delante de la pantalla intentando configurar las primeras versiones del servidor web *Apache* o el *Sendmail*. *Asterisk* puede hacer tantas cosas que tu reto va a ser aprender a hacer bien tan sólo unas pocas.

La metodología que hemos tomado en esta guía no es la de listar todas los posibles órdenes, sino la de citar algunas durante la descripción de tres escenarios prácticos. Los escenarios han sido elegidos para que te sirvan de referencia en tus propias instalaciones. Los ejemplos, aunque básicos, te permitirán la creación de sistemas telefónicos mucho más complejos. Hemos decidido (intencionadamente) simplificar las configuraciones al máximo. Somos conscientes de que algunos de los ejemplos se pueden resolver de otras maneras, no olvides que eres libre de experimentar y explorar tú mismo.

Compilando Asterisk

Como cualquier programa libre, existen *dos* formas principales de instalarlo. El primer método consiste en descargar el código fuente de la red y compilar

tu propia versión binaria. El segundo método consiste en descargar una versión ya compilada en forma de paquete.

Si decides compilar *Asterisk* desde su código fuente los siguientes consejos te pueden ser de utilidad:

- Descarga el código fuente de Asterisk de http://www.asterisk.org. A septiembre del 2006, la última versión estable de Asterisk es la 1.2.12. La última versión del controlador de la familia de tarjetas Zapata es la 1.2.9.
- Para una versión básica no necesitas bajarte los paquetes de "add ons" o "sounds".
- Para poder compilar Asterisk desde el código fuente es necesario tener un entorno de compilación en tu sistema. Asegúrate que tienes los siguientes paquetes instalados:
    - bison (un generador de analizadores sintácticos)
    - zlib y zlib-devel (bibliotecas de compresión – desarrollo)
    - ncurses y ncurses-dev (bibliotecas de utilidades de consola - desarrollo)
    - openssl y openssl-dev (libssl-dev) (SSL – bibliotecas de desarrollo)
    - libc6-dev (cabeceras y bibliotecas de desarrollo GNU C)
    - gcc y make (el compilador C de gnu y la utilidad make)

La compilación de Asterisk no es diferente de otro programa de código libre en Linux:

Para compilar:

```
# make
```

Para instalar:

```
# make install
```

Para instalar los "scripts" de arranque:

```
# make config
```

Para instalar los archivos de configuración de ejemplo:

```
# make samples
```

Para instalar la documentación de desarrollo:

```
# make progdocs
```

Si quieres usar una tarjeta *Digium Wildcard*(tm) con Asterisk vas a tener que compilar e instalar un controlador llamado zaptel (módulo del kernel).

- Descarga el código fuente del Zaptel de *http://www.asterisk.org*. Por desgracia, el controlador de zaptel no forma parte del núcleo (kernel) de Linux y tienes que crearte tus propios módulos.
- Asegúrate de que las cabeceras del núcleo del kernel (paquete kernel-headers) está instalado en tu sistema. Puedes consultar la versión del núcleo/kernel de tu máquina usando la orden **`# uname -a`**. Por ejemplo si estas usando un sistema con Ubuntu Dapper (x386) tienes que instalar el siguiente paquete de cabeceras: **`headers linux-headers-2.6.15-25-386`**.

Descargando Asterisk

También es posible descargar *Asterisk* ya compilado. El programa compilado (binario ejecutable) se obtiene en la forma de "paquete." Un paquete contiene todos los archivos necesarios para ejecutar un programa. Dependiendo de la distribución de Linux que estés usando existen paquetes en distintos formatos (rpm, deb o tgz). Si estás usando una distribución basada en Debian, puedes descargar e instalar *Asterisk* usando la utilidad **`apt`**. Ejecuta la orden **`apt-get install`** con los siguientes paquetes:

Paquete	Descripción
Asterisk-classic (obligatorio)	PBX en código libre – versión original de Digium
Asterisk-config (sugerido)	archivos de configuración para Asterisk
Asterisk-dev (opcional)	archivos de desarrollo para Asterisk
Asterisk-doc (sugerido)	documentación para Asterisk
Asterisk-sounds-extra (opcional)	archivos adicionales de sonido para Asterisk
Asterisk-sounds-main (opcional)	archivos de sonido para Asterisk

A día de hoy, no existe una versión binaria (compilada) del controlador del núcleo "zaptel". No tienes más opción que seguir el método descrito en la sección anterior. Descarga el código fuente del controlador del núcleo (zaptel kernel drive) y crea el módulo con la utilidad **`make`** y **`make install`**. No

olvides que antes de compilar el controlador necesitas tener instaladas las cabeceras del núcleo (kernel) de Linux.

Paquete	Descripción
zaptel (obligatorio)	Utilidades para Zaptel
zaptel-source (obligatorio)	Código fuente del controlador del núcleo Zaptel
linux-headers-2.6.15-25-386 (depende tu distribución)	Cabeceras del núcleo de Linux para Ubuntu Dapper x386 Kernel

Órdenes Básicas en Asterisk

Asterisk tiene dos componentes internos: un servidor que normalmente funciona en segundo plano y un cliente (CLI) que supervisa el servidor. Tanto el servidor como el cliente se invocan usando la orden "*Asterisk*" pero utilizando distintos argumentos.

Una vez que tengas *Asterisk* instalado, tienes que aprender algunas órdenes básicas:

Arrancar/Parar Asterisk desde el arranque (run level)

```
# /etc/init.d/asterisk (start|stop)
```

Arrancar Asterisk desde la línea de órdenes

```
# asterisk
```

Arrancar el servidor en modo de depuración

```
# asterisk -vvvc
```

Arranca en modo de depuración o "verbose" (-vvv) y abre un cliente en modo consola (-c) (con un cliente en modo consola (CLI) puedes supervisar lo que esta pasando en el servidor.

Si el servidor está funcionando en segundo plano te puedes conectar usando el cliente con el argumento (-r).

```
# asterisk -r
```

CLI órdenes básicas

Recarga la configuración

```
#CLI> reload
```

Activa el modo de depuración para SIP o SIP o IAX2

```
#CLI> IAX2 debug
#CLI> SIP debug
```

Desactiva el modo de depuración para SIP o IAX2

```
#CLI> IAX2 no debug
#CLI> SIP no debug
```

Muestra el estado de "usuarios", "peers" y "canales" para SIP o IAX2. El término "peer" se traduce al castellano como "compañero". En el caso concreto de Asterisk los términos "user" and "peer" se usan para clasificar los tipos de conexiones IP al sistema.

```
#CLI> sip show users
#CLI> sip show peers
#CLI> sip show channels
#CLI> iax2 show peers
#CLI> iax2 show users
#CLI> iax2 show channels
```

Archivos de configuración

El número de archivos de configuración que tienes que modificar para hacer funcionar *Asterisk* depende del tipo de tecnologías VoIP que quieras usar en tu instalación actual de manera simultánea. La lógica básica para configurar *Asterisk* se puede resumir en los dos pasos siguientes:

Paso 1: Define y Configura los canales de comunicación

Primero, tienes que definir y configurar el tipo de canales de comunicación que quieres usar. Una manera muy fácil de entender lo que es un canal de comunicación es imaginarse un "cable". Los canales en telefonía IP no son los cables físicos, sino cables lógicos. Como Internet te permite tener muchas sesiones concurrentes en el mismo cable físico, podemos definir múltiples canales lógicos que operan simultáneamente en el mismo medio.

Recuerda que *Asterisk* te permite interconectar distintos dispositivos usando diferentes protocolos de VoIP. Los archivos de configuración que necesitas preparar están asociados al tipo de tecnología VoIP que vayas a usar. No es mala idea instalar los archivos "ejemplo" (*samples*) como referencia.

Paso 2: Define reglas para tus extensiones (Crear un plan de marcado)

El segundo paso es definir cómo van a interactuar cada uno de los canales entre sí. Una vez que has definido un canal garantizas que las conversaciones puedan entrar y salir de tu PBX pero además tienes que definir cómo se encaminan cada una de esas conversaciones. Por ejemplo, puedes preferir que una llamada entrante desde la RTB se envíe automáticamente a un teléfono IP o, puedes definir una conexión entre dos teléfonos IP separados 20 kms a través de una red inalámbrica. Todo ese tipo de "inteligencia" entre los canales se debe crear en un archivo de configuración conocido como **`extensions.conf`**. El archivo de extensiones contiene todas esas reglas de gestión de llamadas a las que se conoce como el ***plan de marcado*** o ***dial plan***.

Para que te hagas una idea más intuitiva de este tipo de conceptos, piensa en los sistemas de telefonía más antiguos. En esos sistemas, existía una persona (el operador) que era responsable de conectar físicamente los cables telefónicos entre dos terminales. Para que una llamada fluyera entre dos líneas de comunicación (canales) se necesitaba contactar primero con el operador (PBX) e informarle de nuestras intenciones. El archivo de extensiones en nuestra PBX suplanta el rol del operador tradicional.

En nuestros tres escenarios vamos a usar cinco archivos de configuración:

archivo de Configuración	Descripción
/etc/asterisk/extensions.conf (siempre obligatorio)	Contiene el plan de marcado (dialplan). Interconecta los canales.
/etc/asterisk/sip.conf	Se usa para configurar canales tipo SIP (teléfonos SIP y proveedores SIP)
/etc/asterisk/iax.conf	Se usa para configurar canales tipo IAX2 (teléfonos IAX2 y proveedores IAX2)
/etc/asterisk/zapata.conf	Se usa para configurar las tarjetas de interfaz RTB tipo Zapata. Asterisk usa la configuración para habilitar el canal(es) de la tarjeta en el arranque

archivo de Configuración	Descripción
/etc/zaptel.conf	Configuración de bajo nivel de la tarjeta zaptel. Indica que dispositivo del tipo zaptel estamos usando. La utilidad Zaptel Configurator tool "ztcfg" usa este archivo de configuración antes de arrancar Asterisk

Peers, Users y Friends

Uno de los temas más complicados de *Asterisk* (o al menos lo ha sido para mí durante mucho tiempo) es el del uso de la opción ***peer***, ***user*** y ***friend*** en los archivos **`iax.conf`** y **`sip.conf`**.

Los términos *peer*, *user* y *friend* se usan para clasificar las llamadas entrantes y salientes. Mientras que un "user" es una conexión que se autentifica con nuestra PBX (i.e. una llamada entrante), un "peer" es una llamada saliente. Los "users" nos llaman y nosotros llamamos a los "peers."

Tienes que tener en cuenta una de las excepciones a esta clasificación quizás simplista. Cuando uno de nuestros "peers" actúa como proxy de otros terminales IP, las llamadas entrantes desde ese "peer" se asocian a la sección "peer" correspondiente (en lugar de usar una sección tipo "user"). Esto es debido que cuando un "peer" actúa como proxy, no puede autentificar en favor de sus clientes. El proxy puede redirigir las llamadas a tu centralita pero no puede autentificarse como el cliente final. Asterisk utiliza la dirección IP del "peer" para seleccionar la sección adecuada del archivo de configuración. En resumen, una llamada saliente siempre es tipo "peer", una llamada entrante puede ser tipo "user", o tipo "peer" cuando la llamada entrante procede de un proxy.

Un "friend" es una conexión que se puede comportar tanto como "user" o como "peer", es decir una conexión saliente o entrante.

Cuando nos llega una conexión entrante del tipo "user" o "friend" tenemos que decidir qué hacer con la conexión. El término "contexto" se usa para definir qué reglas o grupo de reglas del plan de marcado (**`extensions.conf`**) se deben aplicar a esa llamada concreta. El "contexto" de una llamada entrante se encarga de asociarla con un conjunto de reglas presentes en el plan de marcado. El "contexto" representa el punto de entrada de la llamada en el plan de marcado.

El archivo **`extensions.conf`** incluye todos los "números" que se pueden acceder desde la PBX en distintas secciones (contextos). Cada uno de los múltiples canales entrantes definidos en cada uno de los archivos de configuración (iax.conf, sip.conf, zapata.conf) se asocian a cierta sección (contexto) del plan de marcado.

ESCENARIOS

Escenario A:
Red telefónica privada en una comunidad rural

En nuestro primer escenario queremos instalar una PBX en el Telecentro de una comunidad rural y ofrecer telefonía IP a cuatro organizaciones de los alrededores. Después de completar la instalación, cada organización debe ser capaz de hacer llamadas telefónicas gratuitas al Telecentro y a todos los socios conectados. Una vez que la infraestructura de comunicaciones se ha desplegado podemos establecer tarifas reducidas para las llamadas internas que permitan cubrir los costos de ampliación y mantenimiento. El uso de voz sobre IP nos permite trabajar en modelos de desarrollo comunitario en donde se puede considerar las llamadas internas como gratuitas.

La siguiente tabla resume la información de cada una de las cuatro organizaciones y lista las cuatro tecnologías diferentes que se pueden usar para conectarse a la centralita. Con el objetivo de presentar un ejemplo lo más ilustrativo posible, hemos elegido una gran variedad de tecnologías de voz IP. En una implantación real debes considerar reducir el número de tecnologías con el fin de facilitar el soporte y mantenimiento.

Organización	Tecnología	Extensión
Biblioteca Comunitaria	Teléfono VoIP con protocolo SIP	462
Hospital Regional	ATA usando el protocolo SIP	463
Escuela de Primaria	ATA usando el protocolo IAX2	464
Asociación Ganaderos	Dos teléfonos "Soft Phones" usando SIP y IAX2	465, 466

Configurando los clientes VoIP

Antes de describir como configurar la PBX empezamos con una descripción de la instalación de cada uno de los clientes de VoIP.

Biblioteca Comunitaria

El primer cliente está situado en la biblioteca pública de la zona. La biblioteca está situada alrededor de 1 km del Telecentro. En esta organización vamos a instalar un terminal de voz IP con soporte para el protocolo SIP. El terminal está conectado directamente a nuestra PBX a través de una pasarela inalámbrica dedicada (enlace punto-a-punto en modo transparente o "bridge"). La dirección IP del terminal IP (192.168.46.2) está en el mismo segmento de red que nuestra PBX (192.168.46.1). Como el enlace inalámbrico está en modo transparente, la PBX y el terminal IP se comunican directamente y no tenemos que preocuparnos de los problemas relacionados con el NAT.

Para configurar cualquier tipo de terminal de voz IP consulta el manual del equipo y busca la manera de activar la interfaz de administración por Web. Existen tres mecanismos básicos para configurar la dirección IP de un teléfono. Teclado: configurar la dirección IP de teléfono a través del teclado del terminal. DHCP: conectar el teléfono a una red con DHCP y extraer la dirección de la información ofrecida por el servidor DHCP. IP de fábrica: leer la documentación para conocer la dirección IP que viene por defecto en el terminal. Una vez que entres en la zona de administración busca cómo configurar por Web los siguientes parámetros básicos:

Parámetro	Valor
Dirección IP del teléfono VoIP	192.168.46.2
Dirección IP de la PBX (proxy SIP)	192.168.46.1
Registrar/Register	SI/YES
Nombre de Usuario (User/Auth name)	462
Caller ID	462
Clave/Password	462pass
Codec	G.711 (u-law)

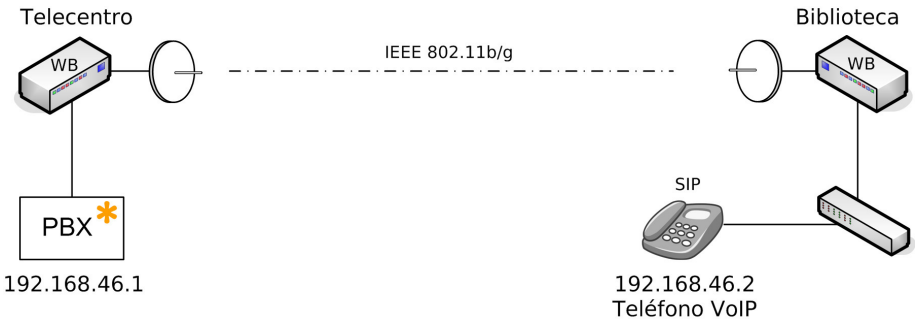


Figura 9.5: La biblioteca comunitaria está conectada a la PBX a través de una pasarela inalámbrica. El enlace punto a punto permite al terminal de VoIP hacer y recibir llamadas.

Hospital Regional

El segundo cliente de nuestra red interna es un ATA situado en el hospital. El hospital local está situado al otro lado de la calle, en frente del Telecentro. La conexión entre el Telecentro y el hospital es un cable de par trenzado de 100 metros (ethernet Cat5). La manera de configurar un ATA no es muy diferente a la de configurar un teléfono VoIP. Siguiendo los mismos pasos que en el ejemplo anterior vamos a usar la interfaz de administración web y completar los siguientes parámetros.

Parámetro	Valor
Dirección IP del ATA	192.168.46.3
Dirección IP de la PBX (SIP proxy)	192.168.46.1
Registrar/Register	SI/YES
Nombre de Usuario (User/Auth name)	463
Caller ID	463
Clave/Password	463pass
Codec	G.711 (u-law)

En lugar de conectar al ATA un teléfono tradicional decidimos usar un teléfono inalámbrico de tecnología DECT. DECT, del inglés Digital Enhanced (formerly European) Cordless Telecommunications, es un estándar de comunicación inalámbrica para teléfonos portátiles que opera en 1.9 Ghz. La

estación base se conecta al puerto RJ-11 del ATA. El resultado es que podemos tener cobertura telefónica DECT en cualquier parte del hospital. El ATA hace de puente entre el teléfono sin cables y la red de voz sobre IP.

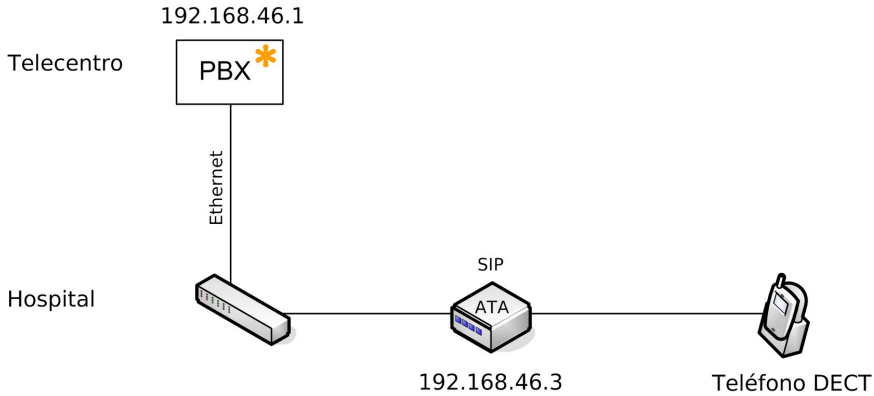


Figura 9.6: El Hospital está conectado al Telecentro a través de un cable de par trenzado de 100 m. Un teléfono sin hilos (DECT) está conectado al ATA. El ATA se registra con la PBX usando el protocolo SIP.

Escuela Primaria

El tercer cliente de nuestra red es la escuela de primaria. La escuela está en un edificio adjunto al Telecentro y también se puede conectar con cable de par trenzado. En la escuela se coloca otro equipo ATA, en este caso el equipo usa el protocolo IAX2 en lugar de SIP.

En la escuela usamos el modelo de ATA (interfaz FXS) s101i o IAXy. En este cliente conectamos un teléfono ordinario al puerto RJ11 del adaptador telefónico.

El IAXy no incluye un interfaz de configuración por web. La manera más fácil y cómoda de configurar la unidad es utilizar el propio *Asterisk*. La primera vez que conectas el ATA a la red intenta obtener una dirección IP por DHCP. Mira la información (logs) que te da tu servidor DHCP y toma buena nota de la dirección IP del IAXy. El siguiente paso es editar el archivo **`/etc/asterisk/iaxprov.conf`** incluyendo una sección parecida a la siguiente:

```
[iaxy_school]
ip: 192.168.46.4
netmask: 255.255.255.0
gateway: 192.168.46.1
codec: ulaw
server: 192.168.46.1.2
user: 464
pass: 464pass
register
```

Supongamos que tu servidor DHCP le asignó la dirección IP 192.168.46.100 al ATA. Para actualizar la configuración de la unidad escribe desde la consola de *Asterisk* la siguiente orden:

```
#asterisk -r
#CLI> iax2 provision 192.164.46.100 iaxy_school
```

Si no quieres usar el propio *Asterisk* para actualizar el IAXy puedes usar un programa de administración bajo Windows. Existe un programa para sistema operativo Windows para gestionar un teléfono de voz IP IAXy disponible en: *http://dacosta.dynip.com/asterisk*.

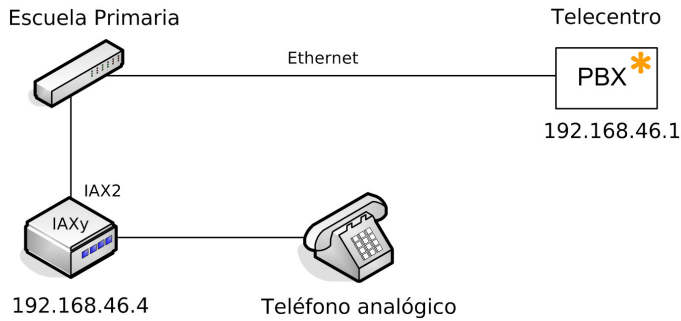


Figura 9.7: La escuela primaria está conectada a la PBX a través de un cable de par trenzado. Un ATA con soporte de IAX2 conecta un teléfono analógico a la centralita.

Asociación de agricultores

El cuarto cliente de nuestra red es la asociación de agricultores que está situada en un edificio a 20 kms de nuestras oficinas centrales (Telecentro). La asociación ya tiene dos computadoras conectadas al Telecentro a través de un router NAT inalámbrico. El equipo inalámbrico tiene la dirección IP 192.168.46.5 y sirve una red interna (via NAT) con un rango de IPs (10.10.46.0/24). En las oficinas de la asociación vamos a instalar dos "*Soft phones*", uno usando el protocolo SIP y otro el protocolo IAX2.

El elemento que requiere más atención es el "*Soft Phone*" que usa SIP. Tenemos que asegurar que el audio funciona en las dos direcciones.

En el "*Soft phone*" SIP:

- Activar el registro con la PBX (register).
- Activar los mensajes que mantienen la conexión activa con la PBX (keep-alive packets). Los paquetes "*Keep-alive*" son paquetes "vacíos" cuya única finalidad es asegurar que la conexión NAT se mantiene abierta/viva para recibir llamadas entrantes.

- Activar la posibilidad de recibir audio por el mismo puerto que lo enviamos.

En la PBX:

- Configurar en *Asterisk* que el teléfono está dentro de un NAT.

Un buen "*Soft Phone*" que usa SIP y que funciona bien dentro de los NATs es el programa X-Lite de Xten. Hay disponible una versión gratuita del programa X-ten en: *http://www.xten.com/index.php?menu=download*.

El "*Soft Phone*" que usa IAX2 no necesita una configuración especial para funcionar dentro de un NAT. Lo único que tienes que asegurar es que el puerto de comunicaciones de IAX2, el UDP puerto 4569, no está bloqueado. Una buena opción de "*Soft Phone*" con soporte para IAX2 es iaxcomm. IaxComm se puede descargar desde: *http://iaxclient.sourceforge.net*.

Desde el punto de vista conceptual no existen diferencias entre la configuración de un programa cliente de telefonía IP en un computador y un terminal físico. Usa los valores de usuario/clave 465/465pass y 466/466pass en cada uno de los programas. Asegúrate que el codec G711 (u-law) está activado y que la dirección de la PBX (proxy) es la 192.168.46.1.

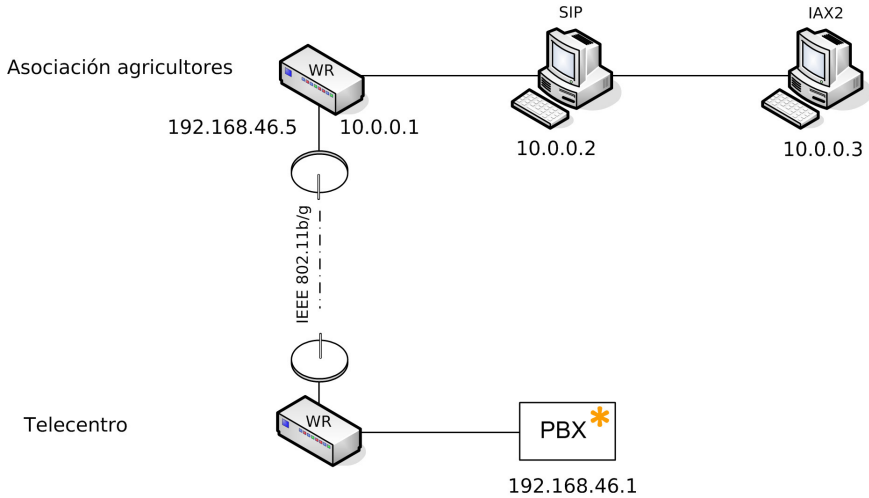


Figura 9.8: La asociación de agricultores está conectada a la centralita a través de un NAT inalámbrico. Un programa de telefonía "soft phone" está instalado en cada uno de los computadores. El primer cliente usa el protocolo SIP mientras que el segundo usa IAX2.

Configurando Asterisk

Paso 1: Definir y configurar los canales de comunicación

Es nuestro primer escenario vamos a usar dos tipos de canales de comunicación: SIP y IAX2. Por lo tanto, tenemos que editar los archivos **sip.conf** y **iax.conf**.

Ten en cuenta que los comentarios dentro de los archivos de comunicación en Asterisk comienzan por punto y coma (;).

En el archivo **sip.conf**, incluye los siguientes datos:

```
[462]
type=friend                    ; Hacemos y recibimos llamadas
secret=462pass
context=internal_calls         ; Todas las "llamadas entrantes"
                               ; están asociadas
                               ; al contexto internal_calls
host=dynamic
callerid=Library
disallow=all                   ; Primero desactivamos todos los codecs
allow=ulaw                     ; Luego activamos el/los codecs que
                               ; podemos usar

[463]
type=friend
secret=463pass
context=internal_calls
host=dynamic
callerid=Hospital
disallow=all
allow=ulaw

[465]
type=friend
secret=465pass
context=internal_calls
host=dynamic                   ; No sabemos la IP por adelantado.
                               ; Aprendemos la IP cuando el usuario
                               ; ser registra
callerid=Farmers1
disallow=all
allow=ulaw
                               ; Opciones específicas para soporte NAT
nat=yes                        ; Se usan la IP,puerto del NAT
qualify=yes                    ; Tráfico "dummy" para mantener la
                               ; conexión viva
```

Y en **iax.conf**, tenemos las siguientes opciones:

```
[464]
type=friend
secret=464pass
context=internal_calls
host=dynamic
callerid=School
disallow=all
allow=ulaw

[466]
type=friend
secret=466pass
context=internal_calls
host=dynamic
callerid=Farmers2
disallow=all
allow=ulaw
```

Paso 2: Definir las reglas en el plan de marcado (crear las extensiones)

En el primer escenario tenemos todos los canales (users) asociados al mismo contexto (internal calls). Por lo tanto, sólo tenemos que definir un contexto en el plan de marcado en **extensions.conf** (ver más abajo).

```
[internal_calls]
exten => 462,1,Dial(SIP/462)
exten => 463,1,Dial(SIP/463)
exten => 465,1,Dial(SIP/465)
exten => 464,1,Dial(IAX2/464)
exten => 466,1,Dial(IAX2/466)
exten => t,1,Hangup()         ; Extensión especial (Timeout)
exten => i,1,Hangup()         ; Extensión especial (Inválido)
exten => s,1,Hangup()         ; Extensión especial (Sin Destino)
```

La sintáxis del archivo de extensiones **extensions.conf** es muy intuitiva.

- Los corchetes **[nombre_contexto]** indican dónde empieza el contexto y su nombre de identificación. Los nombres de los contextos se han definido en los archivos de canales de comunicación **sip.conf** y **iax.conf**. (**Paso 1**)
- Cada una de las secciones del plan de marcado está asociada a un contexto. Cada una de las líneas dentro del contexto tienen el formato:

  exten => ***numero***, ***prioridad***, ***acción***

En el ejemplo anterior estamos creando todas las extensiones (462 a 466) y poniéndolas disponibles dentro del contexto [*internal_calls*]. La orden Dial() crea un canal SIP o IAX2 con los “peers” de nombre 462 a 466.

Escenario B. Conectando la RTB

Nuestro segundo escenario es el resultado de añadir al Escenario A un nuevo canal de comunicaciones. El objetivo es incluir en la red privada anterior un canal hacia la red telefónica tradicional (RTB). Para ello, es necesario añadir a la PBX una interfaz hacia la red telefónica.

En este ejemplo proponemos el uso de una tarjeta PCI TDM400P de *Digium* con un puerto FXO. Como recordarás la tarjeta TDM400P es un interfaz al que se le pueden incluir hasta cuatro módulos FXS/FXO. El uso de un módulo FXO te permitirá conectar la PBX a una línea telefónica analógica.

Figura 9.9: El Telecentro usa una tarjeta TDM400P wildcard para (1) conectar la PBX a la RTB (módulo FXO) y (2) añadir una extensión al teléfono analógico (FXS module).

Incluir el soporte para la tarjeta TDM400P

Los pasos necesarios para poner en funcionamiento el interfaz TDM son cuatro.

Paso 1: Insertar la tarjeta PCI

El primer paso es conectar la tarjeta PCI de medio-tamaño en una de las ranuras libres de tu placa madre. Asegúrate que el conector de tipo *molex* (12/5 volt) del interfaz TDM está conectado a la fuente de alimentación de tu computador. La tarjeta TDM recibe corriente a través de un conector hembra conocido como *molex* (es el mismo tipo de conector de 4-hilos con el que se alimentan los discos duros IDE). Si tu fuente de alimentación no tiene un conector macho disponible tendrás que añadir un divisor de corriente (power splitter).

Paso 2: Instalar los controladores del dispositivo

El segundo paso es asegurarse que los controladores del dispositivo están disponibles (se compilaron correctamente y están cargados). Ejecuta el comando **`lsmod`**, deberías ver el controlador **`wctdm`** cargado. Observa que

el controlador **wctdm** depende del zaptel que a su vez depende del **crc_ccitt**.

```
# lsmod
zaptel                191748  7 wctdm
crc_ccitt               2304  3 hisax,zaptel,irda
```

Paso 3: Configurar la tarjeta TDM400P con la utilidad ztcfg

El tercer paso es configurar el dispositivo. Los controladores **wctdm** han sido diseñados para funcionar con una combinación cualquiera de módulos FXS y FXO. Para indicar al controlador que estamos usando un módulo del tipo FXO en el primer puerto de la tarjeta editamos el archivo **/etc/zaptel.conf** con la configuración más básica:

```
fxsls=1
loadzone=us    ; loadzone=es para España
defaultzone=us ; defaultzone=es
```

La primera línea **fxsls=1** significa que estamos usando señalización FXS del tipo **Loopstart** en el puerto 1. Recuerda que un módulo FXO necesita señalización FXS.

La segunda y tercera línea del archivo de configuración indican el tipo de "tonos" usados en la línea. El sonido y cadencia de los tonos de marcado o de línea ocupada varían de un país a otro.

La lista completa de las especificaciones de tonos por países está disponible en: *http://www.itu.int/ITU-T/inr/forms/files/tones-0203.pdf*

Usamos **ztcfg**, una utilidad de configuración de dispositivos zaptel que se instala como parte del código fuente de *Asterisk* o el paquete zaptel. Ejecutamos **/sbin/ztcfg** para cargar y ejecutar el archivo de configuración **/etc/zaptel.conf**.

Al ejecutar la utilidad deberías obtener el siguiente resultado:

```
# ztcfg -vv
Zaptel Configuration
========================

Channel map:
Channel 01: FXS Loopstart (Default) (Slaves: 01)
1 channels configured.
```

Paso 4: Configurar Asterisk para usar el equipamiento Zapata

El cuarto y último paso es configurar *Asterisk* para que reconozca y use la tarjeta interfaz TDM. Esto creará un nuevo canal de comunicaciones. Editamos el archivo de configuración **`/etc/asterisk/zapata.conf`** de la forma:

```
[channels]
usecallerid=yes
hidecallerid=no
callwaiting=no
threewaycalling=yes
transfer=yes
echocancel=yes
echotraining=yes

context=incoming_pstn
signalling=fxs_ls
channel => 1
```

Las tres últimas líneas del archivo **`zapata.conf`** son las más importantes para una configuración básica. La línea **context=incoming_pstn** indica que todas las llamadas entrantes por el canal de RTB se asociarán a ese contexto. Las siguientes dos líneas indican el tipo de señalización: **`fxs_ls`** (FXS con Loopstart) y que las llamadas llegan por el canal/puerto 1 de la TDM, **channel => 1**.

Una vez que tengas configurado este nuevo tipo de canal (TDM zapata) sólo te queda decidir cómo gestionar las llamadas entrantes y salientes de la RTB.

Gestión de llamadas entrantes desde la RTB.

En nuestro segundo escenario decidimos que el comportamiento ideal para las llamadas entrantes desde la RTB es el siguiente: una vez que una llamada entra por la línea analógica, queremos que se descuelgue un sistema automático de atención por tonos (IVR). El sistema (nuestro *Asterisk*) preguntará por la extensión deseada, una vez que el número de extensión se introduzca por el terminal (tonos DTMF) la llamada se encaminará a una de las extensiones.

La idea principal es permitir compartir un sólo número de la RTB con todas las extensiones. Esta "inteligencia" se implementa en el archivo **`extensions.conf`**. Añadimos una nueva sección (contexto) **[incoming_pstn]** de la siguiente forma:

```
[incoming_pstn]
exten => s,1,Answer()                 ; Contestamos la llamada entrante
exten => s,2,DigitTimeout(10)         ; Configuramos los valores
                                      ; máximos para introducir el
                                      ; número de extensión
exten => s,3,ResponseTimeout(20)
exten => s,4,Background(vm-extension) ; Un mensaje de voz
                                      ; pregunta: ¿extensión?

exten => i,1,Goto(incoming_pstn,s,1)  ; Repetir preguntar si
                                      ; extensión inválida
exten => t,1,Hangup()                 ; Colgar
include =>  internal_calls            ; Pone a disposición todas las
                                      ; extensiones internas
```

Nota: la versión final completa del archivo **`extensions.conf`** está disponible más adelante.

Gestión de llamadas salientes por la RTB

Para que cada uno de los teléfonos IP puedan usar la línea analógica de salida creamos un nuevo contexto **[outgoing_calls]**.

```
[outgoing_calls]
exten => _0.,1,Dial(Zap/1/${EXTEN:1})
exten => t,1,Hangup()
```

La extensión especial "_0." significa que para alcanzar la RTB se debe empezar marcando el numero "0". La orden **Dial()** crea el puente entre la llamada IP desde los terminales y el canal analógico **Zap/1** (canal 1). Por último **${EXTEN:1}** significa que el número que se marcará por el canal analógico es el número marcado desde los terminales internos IP sin el primer dígito. En nuestro caso se quita el "**0**" inicial al marcar por la RTB.

Una vez que hemos creado un nuevo contexto en el plan de marcado **[outgoing_calls]**, es necesario que los terminales tengan acceso a la extensión de salida. La manera más fácil de conseguirlo es añadir una línea del tipo **include => outgoing_calls** al final del contexto **[internal_calls]**:

```
include => outgoing_calls
```

Añadiendo un terminal analógico a la PBX

En nuestro primer escenario hemos configurado cinco terminales de VoIP en cuatro organizaciones, pero el Telecentro que aloja la PBX no tiene ninguna extensión de voz. La manera más simple de añadir al Telecentro su extensión de voz es instalar un módulo FXS en la PBX. La tarjeta TDM400P tiene 3 puertos libres, usamos el segundo puerto de la PCI para incluir el módulo FXS. Una vez que tengamos el módulo FXS configurado podemos conectar un terminal analógico (FXO) al puerto 2 de la PBX.

El proceso es simple; después de apagar la PBX, insertamos el módulo FXS en el segundo puerto de la tarjeta TDM. Después de arrancar el sistema, añadimos una línea más **fxo_ls=2** al archivo de configuración **/etc/zaptel.conf**.

```
fxsls=1
fxols=2
loadzone=us    ; loadzone=es para españa
defaultzone=us ; defaultzone=es
```

Para asegurar que el segundo puerto (FXS) ha sido detectado tienes que usar la herramienta **ztcfg** (o incluirla en el arranque) con el siguiente resultado:

```
#ztcfg -vv
Zaptel Configuration
========================

Channel map:

Channel 01: FXS Loopstart (Default) (Slaves: 01)
Channel 02: FXO Loopstart (Default) (Slaves: 02)

2 channels configured.
```

Una vez que el sistema operativo puede hacer uso del nuevo puerto en la TDM, configuramos *Asterisk* en **/etc/asterisk/zapata.conf** para que pueda hacer uso de un nuevo canal analógico (el teléfono). En el mismo archivo de configuración indicamos que las llamadas entrantes desde el teléfono analógico (puerto 2 de la tarjeta TDM) se deben asociar al contexto **[internal_calls]**:

```
[channels]
usecallerid=yes
hidecallerid=no
callwaiting=no
threewaycalling=yes
transfer=yes
echocancel=yes
echotraining=yes

context=incoming_pstn
signalling=fxs_ls
channel => 1

;Añadimos un módulo FXS
context=internal_calls
signalling=fxo_ls
channel => 2
```

Actualización del plan de marcado

Necesitamos un nuevo plan de marcado con dos nuevas funcionalidades:

1. Permitir tanto llamadas entrantes como salientes por la RTB (canal zapata 1).
2. Incluir el nuevo terminal (canal zapata 2) a nuestro plan de marcado. El terminal analógico (FXO) en el Telecentro debe poder hacer y recibir llamadas.

El archivo **`extensions.conf`** para nuestro segundo escenario tiene el siguiente aspecto:

```
[incoming_pstn]
exten => s,1,Answer()
exten => s,2,DigitTimeout(10)
exten => s,3,ResponseTimeout(20)
exten => s,4,Background(vm-extension)
exten => i,1,Goto(incoming_pstn,s,1)
exten => t,1,Hangup()
include =>  internal_calls

[internal_calls]
exten => 461,1,Dial(Zap/2) ; Extensión 461 llama por el canal Zap 2
exten => 462,1,Dial(SIP/462)
exten => 463,1,Dial(SIP/463)
exten => 465,1,Dial(SIP/465)
exten => 464,1,Dial(IAX2/464)
exten => 466,1,Dial(IAX2/466)
exten => t,1,Hangup()
exten => s,1,Hangup()
exten => i,1,Hangup()
include => outgoing_calls  ; Salida RTB disponible a todos los clientes

[outgoing_calls]
exten => _0.,1,Dial(Zap/1/${EXTEN:1}) ; Quita 0 antes de marcar por RTB
exten => t,1,Hangup()
```

Escenario C. Conectando comunidades usando VoIP

En nuestro tercer y último escenario queremos conectar nuestro Telecentro con un centro de capacitación a distancia situado en otro país. La conexión de datos se realizará a través de un enlace de satélite tipo VSAT. Una vez que tengamos funcionando la conexión a Internet podemos usarla para realizar tanto llamadas internacionales al centro de capacitación como a otros destinos.

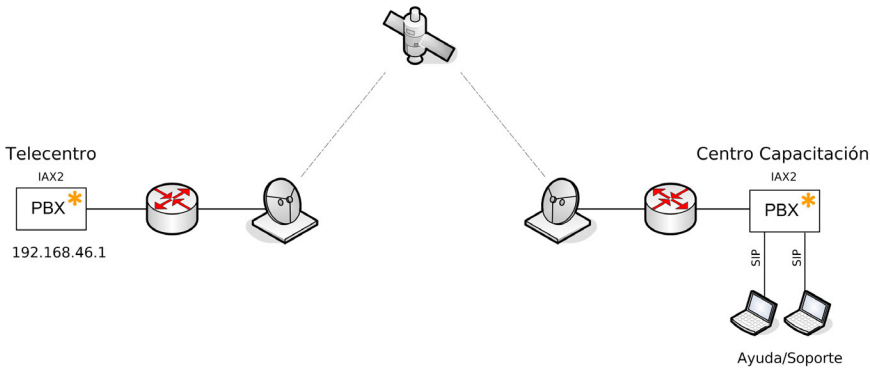


Figura 9.10: Tanto el Telecentro como el Centro de Capacitación tienen su centralita Asterisk. Las centralitas están interconectadas gracias a un enlace de satélite tipo VSAT.

Problemas más comunes en enlaces vía satélite

La conexión a Internet desde el Telecentro tiene un ancho de banda muy limitado (128/64 Kbps) por lo que debemos diseñar una solución que haga un uso óptimo del ancho de banda disponible. En el siguiente ejemplo proponemos conectar dos centralitas usando *Asterisk* y el protocolo IAX2 de voz sobre IP. Además de usar IAX2 en lugar de SIP, utilizaremos un codec de alta compresión como el G.729. Para terminar, activaremos el "trunking" de llamadas que permite agregar varias llamadas simultáneas en el mismo flujo de paquetes IP.

Un escenario muy común en entornos con VSATs es la escasez de direcciones IP públicas que se ofrecen en la conexión a Internet. Si no tienes ninguna dirección pública IP disponible para tu centralita tienes que asegurarte de que el puerto de comunicaciones IAX2 es visible desde el exterior. Para hacer visible el puerto debes redirigir las conexiones al puerto UDP 4569 a la PBX.

- Si tu conexión usa un enrutador del tipo Cisco con NAT tienes que usar una configuración parecida a la siguiente.

```
#ip nat inside source static udp 192.168.46.1 4569 interface \
fastEthernet 0/0 4569
```

- Si tu enrutador usa Linux puedes redirigir las conexiones al puerto 4569 a tu máquina Asterisk (192.168.46.1) usando el programa de gestión de rutas: **`iptables`**

```
#/sbin/iptables -t nat -A PREROUTING -p udp --dport 4569 -i eth0 \
-j DNAT --to-destination  192.168.46.1:4569
```

Independientemente del tipo de equipo que estés usando para encaminar tu tráfico a Internet, lo realmente importante es recordar que tu centralita tiene

que ser accesible desde el exterior. El puerto por defecto de comunicaciones IAX2 es UDP 4569.

Interconectando dos servidores con Asterisk

Telecentro

El archivo de configuración iax.conf en el Telecentro debería parecerse al siguiente:

```
[general]
bindaddr = 0.0.0.0
tos = lowdelay
disallow = all
allow = ulaw
allow = g729          ; Permitimos el uso del codec G.729

register => server2:server2pass@training_voip.org
                      ; server2:server2pass es el usuario
                      ; y clave que usamos para registrarnos

                      ; Cuenta de usuario que usará el Centro de
                      ; Capacitación para registrarse con nosotros
[server1]
type=friend
user=server1
secret=server1pass
host=dynamic          ; Aprendemos la dirección IP
                      ; cuando se registran con nosotros

context=incoming_training_centre_calls
auth=md5              ; Añadimos seguridad en autentificación
disallow=all
allow=g729
trunk=yes             ; Activamos el "trunking"
```

Para alcanzar el Centro de Capacitación desde nuestro Telecentro añadimos un nuevo contexto en el archivo **`extensions.conf`**. Cuando una llamada empieza por "99", redirigimos la conexión al centro de capacitación **[server1]** a través de Internet.

```
[outgoing_training_centre_calls]
exten => _99.,1,Dial(IAX2/server2:server2pass@server1/${EXTEN:2})
exten => _99.,2,Congestion          ; En caso de fallo, sonido
                                    ; de congestionado
```

El siguiente paso es decidir lo que hacemos con las llamadas provenientes del Centro de Capacitación. En el ejemplo hacemos sonar el teléfono analógico (**Zap/2**) en el Telecentro.

```
[incoming_training_centre_calls]
exten => _X.,1,Dial(Zap/2)
                                        ; Llamadas desde el centro de
                                        ; capacitación con cualquier
                                        ; número hacen sonar el teléfono
                                        ; analog. del Telecentro
```

Centro de capacitación

El archivo **iax.conf** del centro de capacitación es similar:

```
[general]
bindaddr = 0.0.0.0
tos = lowdelay
disallow = all
allow = g729                    ; Usamos G.729
register => server1:server1pass@rural.telecentres.org

                                ; Nos registramos como usuario server1
[server2]
type=friend
user=server2
secret=server2pass
host=dynamic

context=incoming_telecentres_calls
auth=md5
disallow=all
allow=g729
trunk=yes
```

Después de configurar el canal IAX2 en el Centro de Capacitación, vamos a añadir el contexto **[outgoing_telecentres_calls]** y **[incoming_telecentres_calls]** para gestionar las llamadas salientes y entrantes al/desde el Telecentro.

Creamos una regla en el plan de marcado para que las llamadas que empiecen por 88 se envíen al Telecentro (peer **[server2]** en **iax.conf**).

```
[outgoing_telecentres_calls]
exten => _88.,1,Dial(IAX2/server1:server1pass@server2/${EXTEN:2})
exten => _88.,2, Congestion
```

Las llamadas entrantes al Centro de Capacitación se redirigen a un centro de atención de usuario. En el siguiente ejemplo, las llamadas entrantes se reenvían al personal de ayuda usando un canal SIP (**SIP/support-desk**)

```
[incoming_telecentres_calls]
exten => _X.,1,Dial(SIP/support-desk)
; Llamadas entrantes se envían al centro
; de atención de usuario (Support Desk)
```

La canal SIP que se ejecuta con Dial() hacia el *support-desk* (servicio de atención de usuario) tiene que configurarse en la centralita del Centro de Capacitación.

La función de registro

No se pueden realizar llamadas a un "peer" hasta que se conozca su dirección IP. Imagínate la situación donde sólo una de las dos centralitas tiene la dirección IP fija. El proceso de registro permite al "peer" hacer pública su dirección IP actual. En nuestro ejemplo anterior hemos usado dos órdenes de registro aunque la función de registro no sea estrictamente necesaria porque los comunicantes tienen IP fijas. Para usar las direcciones fijas en lugar del proceso de registro sustituimos la opción **host=dynamic** por la opción **host=<ip_address or domain>**.

Para aprender más

- Uno de los mejores libros sobre Asterisk es: Asterisk, The Future of Telephony, Jim Van Meggelen, Jared Smith, Leif Madsen. O'Really 2005. Licencia Creative Commons.
- *http://www.oreilly.com/catalog/asterisk/*
- Descarga libre en: *http://www.asteriskdocs.org/modules/tinycontent/index.php?id=11*
- Para no perder de vista lo que está pasando en el mundo de la telefonía IP puedes consultar: *http://www.oreillynet.com/etel/*
- El sitio "VoIP info" es una wiki enorme con cientos de consejos y ayudas; aunque encontrar lo que uno realmente necesita puede llevarte un poco de tiempo *http://www.voip-info.org/wiki-Asterisk+tips+and+tricks*

Conclusión

Este capítulo es un intento de introducirte en el mundo de la telefonía IP. Esperamos que a través de algunos escenarios, haber sido capaces de hacerte consciente de las infinitas posibilidades que ofrece la telefonía IP en regiones en desarrollo. La unión de la telefonía IP con las tecnologías inalámbricas de bajo costo permite ofrecer servicios de voz y datos a regiones excluidas. Estas tecnologías promueven la creación de nuevas redes comunitarias, redes operadas y mantenidas por las comunidades.

Los archivos incluidos como ejemplos pretender servir de guía para ayudarte a poner en marcha tu primer sistema de telefonía. Ningún documento puede compararse con la experiencia personal; ¡ten paciencia!, tu perseverancia es la clave para tu aprendizaje. Y recuerda que no estás solo – siempre puedes pedir ayuda en los foros de discusión y compartir tu experiencia con otros.

¡Bienvenido/a a la una comunidad imparable de entusiastas de la telefonía IP!

¡Esperamos tu llamada!

Tabla de Abreviaturas

Abreviatura	Descripción
ATA	Adaptador Telefónico Analógico
DECT	Comunicación Digital Inalámbrica Mejorada *Digital Enhanced Cordless Telecommunications*
FXO	*Foreign Exchange Office*
FXS	*Foreign Exchange Station*
GSM	Sistema Global para Comunicaciones Móviles *Global System for Mobile communication*
IAX(2)	Protocolo de Intercambio de Asterisk (versión 2)
IETF	Grupo de Trabajo de Ingeniería de la Internet *Internet Engineering Task Force*
ITU/UIT	Unión Internacional de Telecomunicaciones *International Telecommunications Union*
IVR	Respuesta de Voz Interactiva Respuesta Vocal Interactiva, *Interactive Voice Response*
NAT	Traductor de Direcciones de Red *Network Address Translation*
PBX (PABX)	Centralita Telefónica (Automática) Privada *Private (Automatic) Branch Exchange*
PCM/MIC	Modulación por Impulsos Codificados *Pulse Code Modulation*
PSTN/RTB(C)	Red de Telefonía Básica (Conmutada) *Public Switched Telephone Network*

Abreviatura	Descripción
QoS	Calidad de Servicio *Quality of Service*
RFC	Documento de Trabajo de Estandarización (Internet) *Request For Comment*
RTP	Protocolo de Tiempo Real *Real-time Transport Protocol*
SCCP	Protocolo de Control de Llamadas Skinny *Skinny Call Control Protocol*
SIP	Protocolo de Señalización de Sesión(es) *Session Initiation Protocol*
SS7	Sistema de Señalización (versión) 7 *Signalling System 7*
TA/ATA	Adaptador Telefónico *Telephone Adapter*
UDP	User Data Protocol
VoIP	Voz sobre IP. Telefonía IP
VSAT	Terminal de Pequeña Apertura (Comunicaciones por Satélite), *Very Small Aperture Terminal*

Descripción de las ilustraciones de este capítulo

Centralita (PBX) con Asterisk

ATA

IAXy

Enrutador inalámbrico (wireless router)

Pasarela inalámbrica (wireless bridge)


Switch


Router


Teléfono analógico


Teléfono DECT


Teléfono VoIP


Softphone


Antena parabólica


VSAT terminal satélite


Satélite

10
Estudios de Casos

No importa cuánto planeemos el montaje de un enlace o nodo, inevitablemente, vamos a tener que lanzarnos a instalar algo. Ese es el momento de la verdad que demuestra cuán acertadas eran nuestras estimaciones y predicciones.

Es un día muy fuera de lo común, cuando todo ocurre precisamente como lo planeamos. Aún después de instalar su primer nodo, el décimo o el número cien, se va a encontrar que las cosas no funcionan como las planeó. Este capítulo describe algunos de nuestros más memorables proyectos de redes. Si está pronto a embarcarse en su primer proyecto inalámbrico o es un veterano en esto, es reconfortante recordar que siempre hay algo para aprender.

Consejos generales

Las economías de los países en desarrollo son muy diferentes de la del mundo desarrollado, y por lo tanto un proceso o solución diseñada para un país más desarrollado puede no ser adecuada en el Oeste de África, o en Asia del Sur. Específicamente, el costo de los materiales producidos localmente y el costo de la mano de obra van a ser insignificantes, mientas los bienes importados pueden ser mucho más caros, comparados con su costo en los países desarrollados. Por ejemplo, uno puede construir e instalar una torre por el 10% del costo de la torre en los Estados Unidos, pero el precio de la antena puede llegar a ser el doble. Las soluciones que capitalizan las ventajas competitivas locales, mano de obra barata y materiales locales, van a ser las más fáciles de replicar.

Encontrar el equipamiento adecuado es una de las tareas más difíciles en lo países en desarrollo. Debido a que el transporte, las comunicaciones y los

sistemas económicos no están desarrollados, los materiales y el equipamiento pueden ser difíciles de encontrar. Un fusible, por ejemplo, puede no ser fácil de conseguir en algunos países, por lo que es una gran ventaja que pueda ser sustituido por un cable que se queme e interrumpa la corriente cuando ésta alcance un cierto amperaje. Encontrar sustitutos para los materiales también estimula al desarrollo de la capacidad empresarial local, así como al sentido de apropiación del sistema, además de ahorrar dinero.

Recipientes para el equipamiento

Objetos de plástico de bajo costo se encuentran por cualquier lado en el mundo en desarrollo, pero están hechos con materiales de mala calidad, generalmente muy delgados, haciéndolos inadecuados para proteger el equipamiento. Los tubos de PVC son sin duda más resistentes, y están diseñados para ser impermeables. En el oeste de África, el PVC más común se encuentra en los almacenes de venta de productos para plomería, con calibres que oscilan entre los 90mm y los 220 mm. Los puntos de acceso como el Routerboard 500 y 200 pueden entrar en dichos tubos, que, sellados con tapas en los extremos, pueden crear una cubierta a prueba de agua muy robusta. También tienen la ventaja de ser aerodinámicos y poco interesantes para los transeúntes, además de que el espacio dejado alrededor del equipamiento asegura una adecuada circulación de aire. A menudo es bueno dejar un agujero de ventilación en la parte inferior de la cubierta de PVC, aunque he aprendido que dejar agujeros abiertos puede ser un problema. En una ocasión las hormigas decidieron construir su hormiguero a 25 metros sobre el piso, adentro del tubo de PVC que contenía un punto de acceso, por eso se aconseja que si queremos evitar infestaciones utilicemos una malla de alambre para cubrir el agujero de ventilación.

Mástiles para antena

Recuperar materiales usados se ha transformado en una industria importante en los países más pobres. Desde autos viejos hasta televisores, cualquier material que tenga valor será desarmado, vendido y reutilizado. Por ejemplo, los autos son desmantelados pieza por pieza, día a día, el metal resultante es clasificado y luego cargado a un camión para ser vendido. Los trabajadores metalúrgicos locales estarán ya familiarizados con la construcción de un mástil para televisión con metal desechado. Con unas pequeñas adaptaciones, esos mismos mástiles pueden ser rediseñados para redes inalámbricas.

El mástil típico es el poste de 5 metros, compuesto por un único tubo de 30mm de diámetro enterrado en el cemento. Es mejor construir el mástil en dos partes, con una parte removible que encastra en una base con un

diámetro levemente más grande. Alternativamente, el mástil puede ser hecho con brazos empotrados de forma segura a un muro. Este proyecto es fácil, pero requiere el uso de escalera para poder completarlo por lo que se sugiere tener precaución.

Este tipo de mástil puede ser aumentado varios metros con la ayuda de cables tensores. Para fortalecer el poste, plante 3 líneas separadas 120 grados, con una caída de por lo menos 33 grados desde la punta de la torre.

Por sobre todas las cosas: involucre a la comunidad

El involucramiento de la comunidad es imperativo para asegurar el éxito y la sustentabilidad del proyecto. Involucrar a la comunidad en el proyecto puede ser el desafío más grande, pero si se hace, la tecnología no cubrirá sus necesidades, ni será aceptada. Más aún, la comunidad puede atemorizarse y menoscabar la iniciativa. Sin importar cuán complejo sea un emprendimiento, un proyecto exitoso necesita apoyo de aquellos a los que va a servir.

Una estrategia efectiva para ganar apoyo es encontrar una persona influyente y respetada cuyas motivaciones sean buenas. Encuentre a la persona o personas que más se puedan interesar por el proyecto. A menudo, va a necesitar involucrar a personas influyentes como consejeras, o como miembros del comité directivo. Esta gente ya cuenta con la confianza del resto, sabe a quién contactar y puede hablar el lenguaje de la comunidad. Tómese su tiempo y sea selectivo en encontrar la gente adecuada para su proyecto. Ninguna decisión afecta más a su proyecto que tener en su equipo personas de la comunidad, eficaces y de confianza.

Tome también en cuenta a los actores clave en una institución o comunidad. Identifique aquella gente que probablemente se oponga o apoye su proyecto. Tan temprano como sea posible, intente obtener el apoyo de los defensores potenciales y mantenga al margen a los detractores. Esto es una tarea difícil que requiere un conocimiento íntimo de la institución o comunidad. Si el proyecto no tiene un aliado local, puede requerir un tiempo para adquirir este conocimiento y confianza de la comunidad.

Sea cuidadoso cuando elige sus aliados. Una reunión "del municipio" es útil para observar la política, alianzas y feudos locales en acción. Después de eso es más fácil elegir con quien aliarse y a quien mantener al margen. Trate de no generar un entusiasmo sin garantías, es importante ser honesto, franco y no hacer promesas que no puede cumplir.

En comunidades con altos índices de analfabetismo, enfóquese en servicios de transformación de digitales a analógicos, tales como Internet para estaciones de radio, imprimir artículos y fotos en línea, y otras aplicaciones

no textuales. No intente introducir una tecnología en una comunidad sin comprender qué aplicaciones realmente le van a servir. A menudo la comunidad no va a tener idea acerca de qué nuevas tecnologías ayudarán a solucionar sus problemas, por lo tanto, proveer nuevas características es inútil si no comprendemos cómo se va a beneficiar la comunidad.

Cuando recolecte información, verifique los datos que le dan. Si quiere saber el estado financiero de una compañía/organización, pida ver una factura de electricidad o de teléfono. ¿Han pagado sus cuentas? A veces los beneficiarios potenciales van a comprometer sus propios valores deseando ganar fondos y equipos. Pero mucho más a menudo, los socios locales que confían en usted, serán francos, honestos y serviciales.

Otro error común es lo que yo llamo síndrome de “padres divorciados”, donde las ONGs, donantes y socios no se informan entre sí sobre su involucramiento con el beneficiario. Los beneficiarios astutos pueden ganar atractivas recompensas permitiendo que las ONGs y los donantes derrochen equipos, capacitación y fondos. Es importante conocer qué otras organizaciones están involucradas de manera que pueda comprender como impactan sus actividades a la suya. Por ejemplo, una vez diseñé un proyecto para una escuela rural en Mali; mi equipo instaló un sistema de fuente abierta con computadoras usadas, y pasó varios días capacitando a la gente en cómo usarlo. El proyecto fue catalogado como un éxito, pero muy poco después de su instalación, otro donante llegó con nuevas computadoras Pentium 4 corriendo Windows XP, y los estudiantes rápidamente abandonaron las viejas computadoras y se prepararon para usar las nuevas. Hubiera sido mejor negociar con la escuela de antemano, para conocer su compromiso con el proyecto. Si hubieran sido francos, las computadoras que ahora están sin uso podrían haber sido entregadas a otra escuela donde sí serían utilizadas.

En muchas comunidades rurales de economías no desarrolladas, las leyes y políticas son débiles, y los contratos pueden no tener valor alguno, aunque a veces se pueden encontrar otras maneras de asegurarse. Aquí es donde los servicios pre-pago son ideales, porque no requieren un contrato legal; se asegura el compromiso por la inversión de fondos antes de que se brinde el servicio.

Cuando se hacen adquisiciones también se requiere que los involucrados inviertan en el proyecto. Siempre se debe pedir el compromiso recíproco de la comunidad.

Cancelar la implementación, es una opción que debe evaluarse siempre. Si no se puede tener un aliado y una comunidad convencida, el proyecto debe considerar seleccionar a una comunidad o beneficiario diferente. Es decir, que debe haber una negociación; el equipamiento, el dinero y la

capacitación no pueden ser simples obsequios, la comunidad debe estar involucrada y contribuir.

--Ian Howard

Nota aclaratoria: Los estudios de caso que fueron incluidos en la primera edición de este libro han sido removidos en aras de ofrecer información sobre la región de América Latina y el Caribe. Los estudios de caso que aparecen en la primera edición pueden consultarse en www.wndw.net.

Sistema de Información Agraria del Valle de Chancay-Huaral

La problemática - La realidad de Huaral

El valle de Chancay-Huaral está ubicado 80 kilómetros al Norte de Lima, la capital del Perú. Es una de las principales despensas de Lima, abasteciéndola de frutas, hortalizas y carne. Al igual que en todos los valles de la costa peruana, en Huaral no hay lluvias, por lo que la agricultura es totalmente dependiente del sistema de canales de riego que toma las aguas del río. El valle agrícola está dividido en 17 Comisiones de Regantes, cada una encargada de la gestión del riego en su zona, y todas agrupadas en la Junta de Usuarios del Distrito de Riego del río Chancay-Huaral. Estas organizaciones están compuestas enteramente por los agricultores del valle.

El valle de Huaral es un típico entorno rural peruano en donde la mayoría de los agricultores practican una economía tencia orientada totalmente hacia el mercado, con propiedades pequeñas, escasez de servicios básicos como agua potable, aguas negras y luz, y un bajo desarrollo de los servicios de telecomunicaciones: la telefonía es escasa y el acceso a Internet prácticamente inexistente.

Un problema fundamental del agricultor peruano es la situación de desventaja con la que compite en el mercado a causa de deficiencias en el acceso a información relevantes a su quehacer. En la historia reciente del agro nacional han sido frecuentes los problemas de las pérdidas de cultivos y de las inversiones debido a la sobreproducción de algún cultivo, es decir, muchos agricultores siembran a la vez un mismo producto y lo hacen desconociendo cuál es la demanda en el mercado. Por otra parte, las Juntas de Usuarios encargadas de la administración de los recursos hídricos dedicados a la agricultura no cuentan con las herramientas necesarias para gestionar de manera rápida y eficaz todas sus responsabilidades en el

manejo del agua (distribución, mantenimiento, gestión económica, etc.), lo que a la postre significa mayores inconvenientes para el pequeño agricultor.

La solución planteada

Con el fin de avanzar hacia la solución de los problemas causados por la escasez de información, necesaria para que los agricultores tomen decisiones en cada etapa de sus procesos productivos, el Centro Peruano de Estudios Sociales (CEPES) y la Junta de Usuarios de Huaral iniciaron el proyecto "Sistema de Información Agraria de Huaral". El proyecto busca recolectar/producir y difundir información relevante y actualizada sobre las tendencias del mercado, precios de venta, información técnica agropecuaria, reportes y estadísticas de las áreas cultivadas, entre otros temas, utilizando a la Internet en este medio rural. Este propósito hizo absolutamente necesario el diseño de una infraestructura distribuida de telecomunicaciones en el valle que permitiera la transferencia de información entre todas las zonas y comunidades del valle.

Wireless vs. VSAT

Para llevar la conexión de Internet y el servicio telefónico hasta los locales de las Comisiones de Regantes de Huaral, ubicados en zona rural y distribuidos a lo largo y ancho del valle, se analizaron dos opciones de conectividad: enlaces satelitales de conexión a Internet independientes para cada uno de los puntos o una red inalámbrica que interconectase a todas las Comisiones con un punto central, ubicado en el área urbana del valle, donde ya se contaba con la provisión de servicios de acceso a Internet. En el siguiente cuadro se encuentra el análisis de costos realizado durante la etapa inicial del proyecto (2003):

Resumen comparativo de costos: red inalámbrica vs. enlaces satelitales

	Red inalámbrica (US $)	Enlaces satelitales (US $)
Inversión inicial	53,566	11,505
Costos de operación del primer año	19,800	103,368
Costos de operación del segundo año	31,800	103,368
Costo total al terminar el segundo año	105,166	218,241
Equipamiento propio	47,600	0

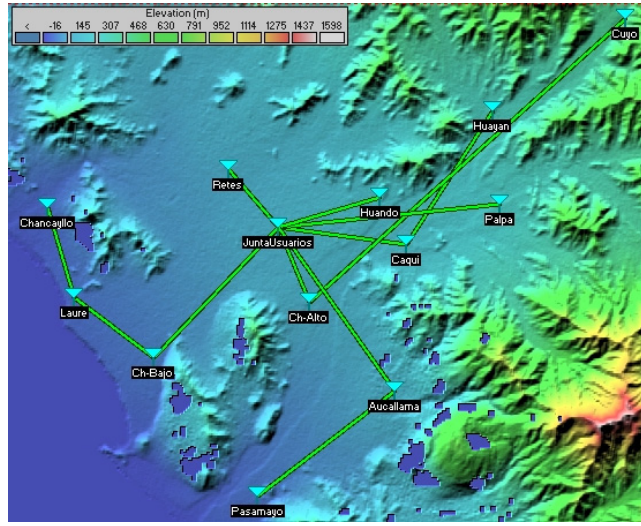
El contraste técnico y económico de ambas soluciones permitió la elección de una red inalámbrica como la solución a implementar. Entre las ventajas de esta solución destacan los bajos costos de operación independiente, la alta velocidad de interconexión entre los telecentros del valle y la posibilidad de acceder al sitio web del Sistema de Información Agraria sin necesidad de transitar por Internet. Adicionalmente, el uso de una conexión a Internet vía ADSL, un tipo de conexión muy popular en el Perú, permitió reducir aún más los costos recurrentes.

Otra característica negativa de la solución satelital fue la reducida disponibilidad local de proveedores que generaba una dependencia en la que el aumento de tarifas o la suspensión de operaciones del proveedor constituía un riesgo inminente para la columna vertebral del proyecto: su red de interconexión.

Interconectando inalámbricamente las Comisiones de Regantes

El valle de Huaral tiene la topografía típica del valle costero peruano, relativamente plana y rodeada por altos cerros. El objetivo entonces era interconectar inalámbricamente la oficina de la Junta de Usuarios de Huaral, ubicada en la zona urbana donde se cuenta con acceso regular a Internet y a los servicios de telefonía, con 11 de las Comisiones de Regantes del valle, distribuidas geográficamente en la zona rural.

Durante los estudios de sitio, realizados primordialmente mediante el paquete de software RadioMobile, se encontró el esquema de conexión óptimo para cada uno de los puntos de la red. Nuestro resultado se muestra en la siguiente figura:



Todos los enlaces están basados en equipos para interiores que cumplen con el estándar 802.11b y trabajan en la frecuencia de 2.4 GHz, adaptados para trabajar en ambientes exteriores y protegidos contra la humedad con cajas a prueba de lluvias Nema 4. La potencia de transmisión que usan los radios es de 100 y 200 mW, y las antenas utilizadas son de 24 dBi y 18 dBi. Un enlace particular de la red es el que une a la Comisión de Regantes de Chancay Alto con la de Cuyo, en la que, usando los mismos equipos 802.11b y agregando convertidores de frecuencia, se trabaja con 900 MHz a fin de aminorar la pérdida en el espacio libre que en este caso era considerable debido a la distancia de 18.9 km y a la línea de vista parcialmente obstruida.

Con este esquema de radios y antenas obtuvimos una red estable y de buenas características, con un margen de operación superior a los 20 dB en todos los enlaces, tal como se puede apreciar en el siguiente cuadro:

N°	Enlace	Distancia	Canal	Margen Operación
1	Junta de Usuarios – Retes	3.38 km	13	28.2 dB
2	Junta de Usuarios – Huando	4.71 km	13	25.6 dB
3	Junta de Usuarios – Chancay Alto	3.56 km	13	24.8 dB
4	Junta de Usuarios – Palpa	9.86 km	3	31.4 dB
5	Junta de Usuarios – Caqui	5.73 km	3	31.2 dB
6	Caqui – Huayan	7.06 km	8	25.1 dB
7	Junta de Usuarios – Aucallama	8.88 km	13	24.0 dB
8	Aucallama – Pasamano	7.67 km	8	28.6 dB
9	Junta de Usuarios – Chancay Bajo	7.99 km	8	28.1 dB
10	Chancay Bajo – Laure	4.39 km	3	30.4 dB
11	Laure – Chancayllo	4.14 km	13	27.3 dB
12	Chancay – Alto Cuyo	18.86 km	904– 926 MHz	19.6 dB

Resumen de los enlaces y sus márgenes de operación.

El impacto de la red.

Cada uno de los telecentros interconectados cuenta con una red local de computadoras, con sistemas operativos y aplicaciones de software libre, que permiten el acceso a los servicios provistos a los agricultores, sus familias y, en general, a las comunidades locales. Sobre la red inalámbrica se han implementado los servicios de transmisión de datos, acceso web al Sistema de Información Agraria y a todos los servicios provistos a través de Internet, y el de telefonía de voz sobre IP que actualmente permite a la Junta de Usuarios de Huaral una comunicación fluida con las Comisiones de Regantes, lo que a significado el mejoramiento constante de la coordinación entre las oficinas de la organización y de la gestión del riego. En general, todas las funciones de la Junta se realizan de una forma mucho más dinámica que en los años anteriores.

Mediante el uso de formularios interactivos diseñados para la fácil publicación de contenidos en línea, la Junta de Usuarios publica diariamente información relacionada con la distribución del agua de riego que es constantemente consultada en los telecentros de las Comisiones de Regantes y que sirve de insumo básico para todo el proceso de distribución del recurso hídrico en cada zona.

La comunidad de pobladores rurales ha iniciado su apropiación de las TICs y las utilizan dándole distintos usos a los recursos dependiendo de sus necesidades particulares: consulta de información educativa, comunicación con sus familiares y amigos que viven en el extranjero y la publicación de contenidos locales en Internet.

El servicio de telefonía VoIP prepago ha generado un impacto importante en la zona. Este servicio ha logrado cubrir la demanda insatisfecha de telefonía que existía en el valle, principalmente en las Comisiones de Regantes más alejadas del centro urbano.

Finalmente, un impacto especial y no esperado del proyecto es la aparición constante de nuevos emprendedores locales que inspirados por la experiencia de la red de la organización de agricultores han empleado la tecnología WiFi para proveer servicios de ciber cafés en otras zonas rurales, con notable éxito y cubriendo un área más amplia del valle.

Chilesincables.org

Una comunidad abierta a las redes inalámbricas libres y su implementación.

Resumen

El fin de esta agrupación es la instauración de una comunidad abierta en torno a las redes inalámbricas libres y su implementación, en la cual el espíritu sea compartir las experiencias y conocimientos adquiridos, siempre bajo las **normas legales vigentes** y en lo posible poner este conocimiento a disposición de entidades o comunidades de bajos ingresos económicos, con el fin de mejorar su calidad de vida proveyéndoles de acceso a sistemas de conectividad y de paso cooperar con la disminución de la brecha digital en Chile e incentivar la utilización de software libre (Open Source).

Antecedentes

Las nuevas tecnologías inalámbricas de transmisión de datos y su relativo bajo costo, permiten crear redes de alta velocidad separadas geográficamente. Sí estas redes se desarrollan organizadamente bajo el concepto de no restringir al acceso a sus datos, obtenemos redes libres[1] las cuales pueden ser explotadas y desarrolladas por cualquier persona, permitiendo el acceso a nuevas tecnologías digitales y a todos sus beneficios sin importar la condición económica, social y/o política de los usuarios, lo cual es una respuesta al modelo comercial restrictivo imperante en la sociedad occidental moderna.

Para que este modelo de redes inalámbricas libres prospere, es necesaria la apropiación de tecnologías, lo cual se lleva a cabo a través de grupos de "hackers" asociados en comunidades, quienes se encargan de investigar, desarrollar e implementar proyectos, y permiten el acceso libre al conocimiento adquirido.

Justificación

Chilesincables.org busca promover y organizar redes inalámbricas libres en Chile de forma profesional; educar al respecto, tanto es sus aspectos técnicos y legales; apropiar nuevas tecnologías, mediante la investigación, adaptándolas a las necesidades de la comunidad y la sociedad.

---

[1] Entiéndase el concepto de libertad más allá de una falta de retribución o costo económico por algún servicio o creación, sino como un concepto filosófico mucho más amplio.

Descripción de la tecnología implementada

Actualmente se utiliza tecnología asociada con las especificaciones IEEE 802.11 en sus estándares a ,b y g[2] más conocida como WiFi, sin descartar la expansión a nuevas innovaciones en el área, como por ejemplo Wimax. Este equipamiento es modificado para ser adaptado a antenas externas de manufactura propia, las cuales se encuentran en norma con la legislación de telecomunicaciones vigente en el país.

Aunque la mayoría del hardware que cumple con el estándar es útil para los objetivos, se fomenta la utilización e investigación de ciertos manufacturadores que permiten un mayor control e integración a nuestras necesidades (sin necesariamente aumentar los costos), los cuales están basados en chipsets Atheros, Prism, Orinoco, RT2500, RT2400, por nombrar algunos, y ciertos modelos de Access Points Linksys, Netgear, Motorola, etc. que cuentan con soporte de firmware por diversas comunidades de hackers que le dan nuevas funcionalidades a estos equipos

En lo referente a la construcción de la red, se utilizan Sistemas operativos Open Source, especialmente plataformas GNU/Linux u otros sistemas inspirados en Unix como FreeBSD, OpenBSD, Minix, etc., los cuales se adaptan a nuestras necesidades en el área de ruteo (enrutamiento) e implementación de servicios, como proxies, servidores web, servidores FTP, etc. Además poseen en común la filosofía del proyecto ya que es tecnología libre y de código abierto.

Usos y aplicaciones

Las diversas redes implementadas permiten:

1. Transferencia de datos mediante servidores FTP o WEB.
2. Servicios de VozIP.
3. Streaming (flujo contnuo) de audio y video.
4. Mensajería instantánea.
5. Investigación: Investigar e implementar nuevos servicios como LDAP, resolución de nombres, seguridad, mejora de las prestaciones, etc.
6. Adaptación de la red por parte de los clientes[3], esto significa que los usuarios pueden utilizar la infraestructura de la red para crear sus propios servicios.

---

[2] Actualmente se esta empezando a realizar estudios con equipamiento pre estándar “n”, el cual correspondería a un avance sobre todo en la velocidad de transmisión de datos permitiendo tasas de transmisión inalámbrica superiores a 100 Mbps.

[3] Entiéndase el término “Cliente” como el usuario que utiliza libremente la red comunitaria.

Administración y mantenimiento

La unidad operacional de red corresponde al "nodo", cuyas funciones son:

1. Permitir que los clientes se asocien a él y prestarles servicios básicos
2. Un nodo debe estar asociado a lo menos a otro nodo, de esa manera crece la red y existen más servicios disponibles para los clientes.

Un nodo es mantenido por un administrador, que en nuestro caso es un miembro de la comunidad que ha adquirido el compromiso de:

1. Mantener un tiempo de operatividad adecuado (superior a un 90%)
2. Mantener algunos servicios básicos (por lo general un servidor Web)
3. Mantener algún sistema que informe a los clientes sobre los servicios que el nodo presta, indicando cómo acceder a ellos, esto generalmente se lleva a cabo mediante un portal cautivo.

La administración general de la red, específicamente lo relacionado con la implementación de nuevos nodos, selección de su ubicación, topología de la red, etc. es llevada a cabo por la directiva de la comunidad o por los comités técnicos formados para tal efecto.

Chilesincables.org actualmente se encuentra realizando los últimos trámites para obtener una personalidad jurídica, lo cual permitiría protocolizar los procedimientos administrativos internos y formalizar la comunidad ante la sociedad.

Entrenamiento y capacitación

Chilesincables.org considera vital capacitar a sus miembros y clientes debido a que:

1. Se debe mantener el espectro radioeléctrico lo mas limpio posible, de esa manera se asegura que los enlaces inalámbricos sean de la calidad adecuada. Por lo tanto es necesario instruir en técnicas de radio-comunicaciones.
2. Se debe utilizar materiales y métodos aprobados por la legislación vigente, de esa manera la actividad puede desarrollarse sin problemas.
3. La red debe crecer de forma armoniosa y con ciertos requisitos, por lo tanto es necesario que nuestros administradores posean conocimientos sobre redes TCP/IP que permitan cumplir con lo anterior.

4. La tecnología debe ser traspasada a los usuarios de esa manera la actividad se perpetúa.

Para cumplir con lo anterior Chilesincables.org realiza periódicamente las siguientes actividades:

1. Talleres de antenas: donde se capacita en la construcción de antenas y se enseñan conceptos básicos de radio-comunicaciones.
2. Talleres de Sistemas operativos: Se capacita respecto a la implementación de enrutadores y servicios basados en plataformas GNU/Linux u otros especialmente desarrollados para la actividad como m0n0wall o pfsense y además se enseñan conceptos básicos de redes.
3. Se fomenta y publicita actividades desarrolladas por otras comunidades que guarden relación con nuestros objetivos como por ejemplo talleres universitarios, charlas, encuentros de software libre, etc.
4. Se mantienen documentación actualizada y libremente accesible a quienes les interese la actividad.

Material Gráfico

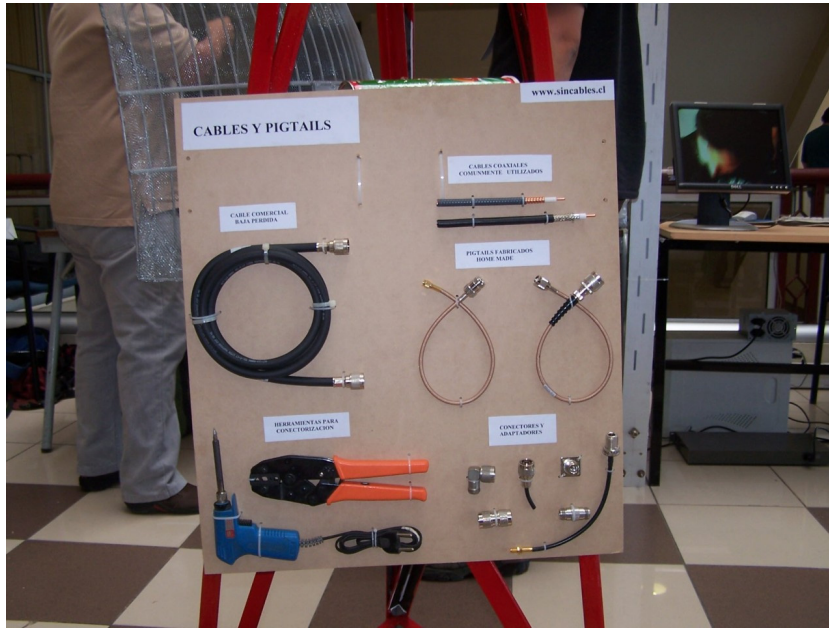
Las siguientes fotografías son un resumen de algunas de las actividades que hemos realizado a lo largo de nuestra historia como comunidad:

Charla dirigida a nuestros miembros por un especialista en telecomunicaciones.

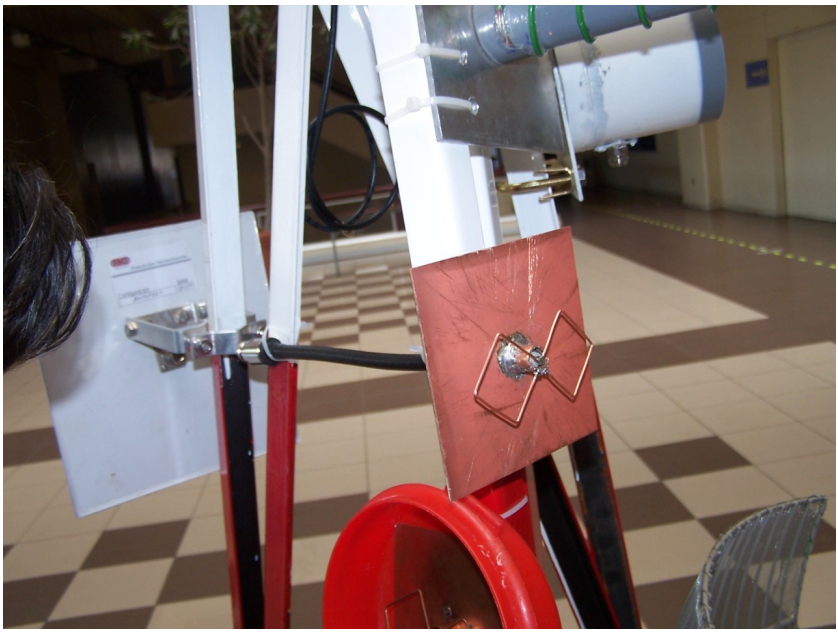
Taller de antenas ranuradas omnidireccionales, en esta ocasión se les enseñó a los asistentes como confeccionar una antena y la teoría de su funcionamiento.

Uno de nuestros miembros realizando una charla acerca de la implementación de un enrutador basado en m0n0wall en la administración de un nodo.

Stand de nuestra comunidad en la FLISOL Santiago 2006, puede observarse la mini torre realizada para el evento la cual contenía una muestra de antenas y de conectores y pigtails (latiguillos).



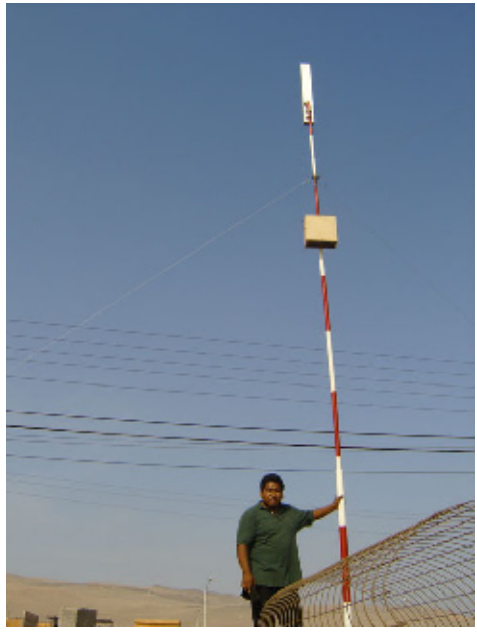
Detalle de la mini torre con la exposición de cables, pigtails y antenas.



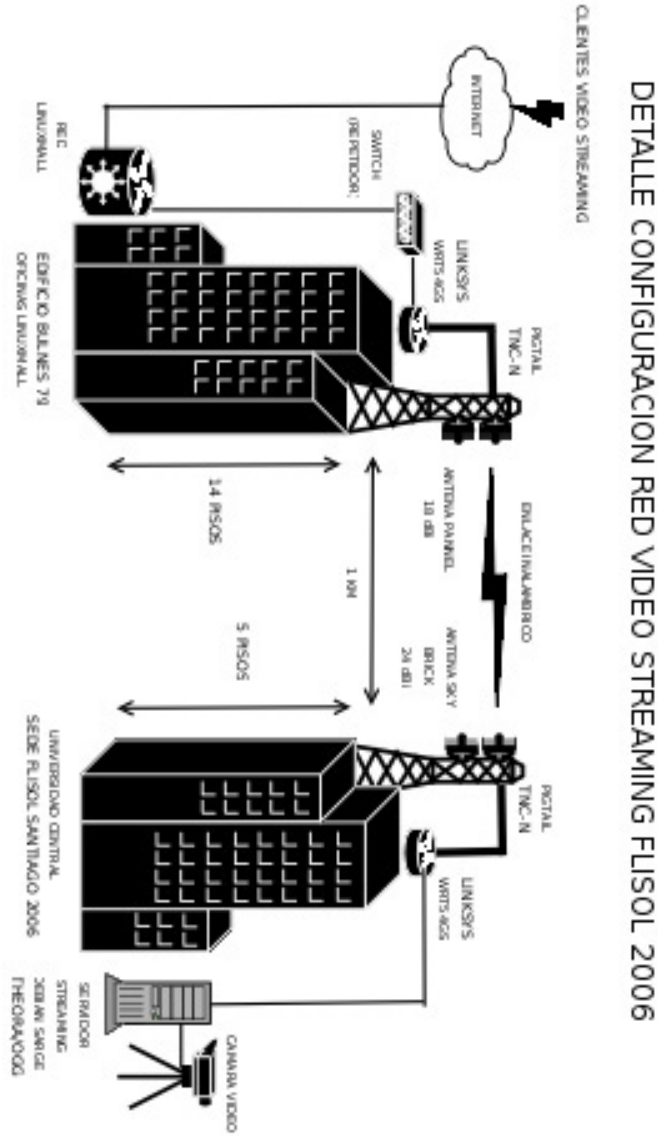
Detalle de la mini torre con la exposición de cables, pigtails y antenas.

Estación wireless con antena parabólica cuya misión era enlazar el sector marcado con el pequeño círculo para transmitir la FLISOL santiago 2006 mediante flujo continuo de video (streaming) con software libre.

Instalaciones donde se encontraba la antena panel a la cual se enlazaba la parabólica (corresponde al lugar marcado por el círculo).



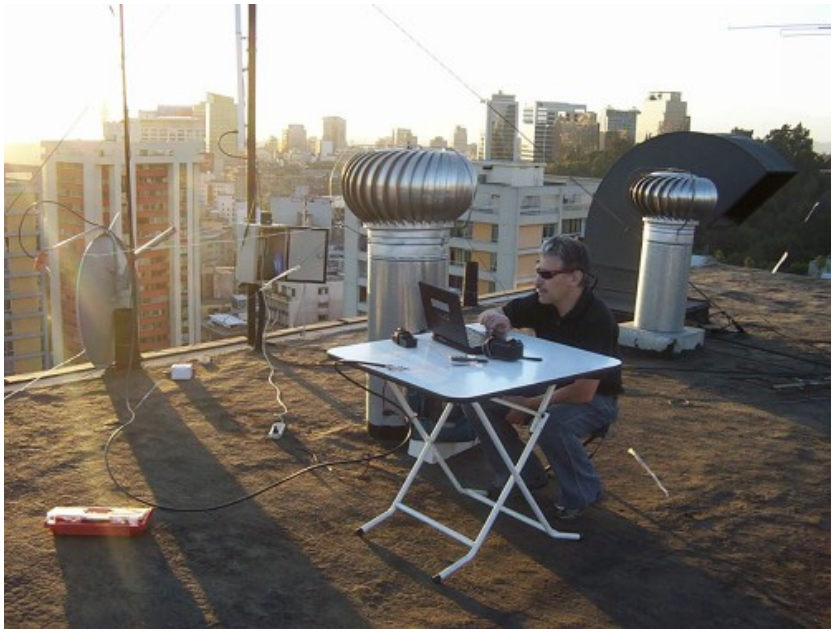
Nodo Quiani, Primera región de Chile, Arica, este nodo es uno de los más alto del mundo a 4000 m de altura y a 2000 s al Norte de la capital del país.



Esquema del proyecto de transmisión de la FLISOL Santiago 2006 por video streaming con software libre a través de un enlace inalámbrico de 1, la velocidad real de transmisión obtenida fue de 36 Mbps.

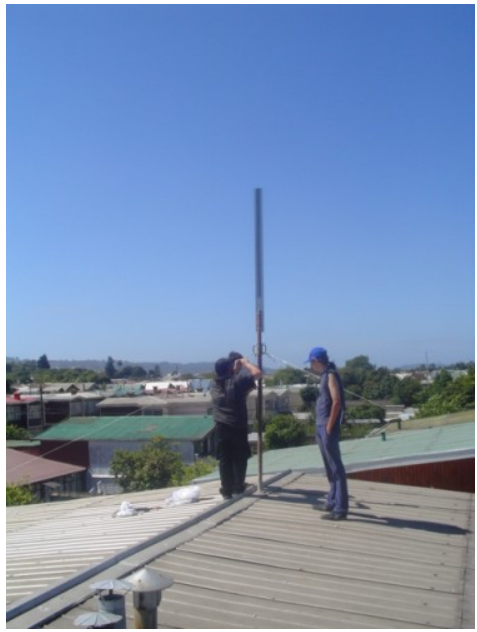
Nodo en la zona sur de Santiago, altura de la torre 15 m, antena: Trevor Marshall 16 + 16, clientes 30, enlazado con nodo en zona centro a mas de 12.

Vista Panorámica Nodo desde la cima de la torre



Nodo zona centro enlazado con nodo zona sur en Santiago, puede observarse antena parabólica que realiza el enlace y antena ranurada para captar clientes.

Nodo Blue, VIII Región, a mas de 500 al sur de la capital enlazado a nodo Campano en la ciudad de Talcahuano a 4 de distancia.



Nodo Campano en Talcahuano VIII Región de Chile.

Nodo en la comuna de la Granja Santiago, enlazado a nodo Santiago Centro (10 s), se observa una antena parrilla.

Implementación de Nodo Independencia en la zona Norte de Santiago.

Implementación de Nodo sobre torre de agua de 20 m en la zona de Batuco, Región Metropolitana, lo cual correspondía a trabajos relacionados con enlace de telecentro Cabrati.

Taller de antenas Yagi realizado por nuestra comunidad, puede observarse a los asistentes fabricando las antenas.

Taller de antenas Yagi realizado por nuestra comunidad, puede observarse a los asistentes fabricando las antenas.

Créditos

Nuestra comunidad se compone de un grupo de activistas desinteresados entre quienes se destacan:

Felipe Cortez (Pulpo), Felipe Benavides (Colcad), Mario Wagenknecht (Kaneda), Daniel Ortiz (Zaterio), Cesar Urquejo (Xeuron), Oscar Vasquez (Machine), Jose San Martin (Packet), Carlos Campano (Campano), Christian Vasquez (Crossfading), Andres Peralta (Cantenario), Ariel Orellana (Ariel), Miguel Bizama (Picunche), Eric Azua (Mr. Floppy), David Paco (Dpaco), Marcelo Jara (Alaska).

Transmisión inalámbrica de datos en Los Andes: Construyendo la red del estado Mérida.

Resumen

La ciudad de Mérida, en los Andes del norte, alberga una universidad bicentenaria que ha mostrado un gran compromiso con la actividad en redes como se evidencia en la instalación de una red de fibra óptica TDM de 100 Mbps luego complementada con una ATM (Asynchronous Transfer Mode) de 155 Mbps y en la organización de 3 reuniones de la Escuela Latinoamericana de Redes en los pasados seis años[4].

El deseo de extender los beneficios del acceso a Internet a las comunidades adyacentes, sin embargo, se vió coartado por las dificultades del terreno y las limitaciones de la infraestructura telefónica. Estos retos fueron superados usando tecnologías de radio, comenzando con *packet radio* en las bandas de VHF (Very High Frequency) y de UHF (Ultra High Frequency), que sin embargo se hicieron obsoletas debido a los requerimientos de ancho de banda del acceso a la Web. Se pasó luego a velocidades más altas gracias a las microondas usando tanto soluciones de espectro esparcido como de banda estrecha.

---

4. Este artículo fue escrito en 1999. Para 2006, el número de eventos de entrenamiento asciende a 8.

La red de avanzada que se está instalando permite transmisión de datos *full duplex* a 10 Mbs y abarca una región de unos 200 por 100 km que se extiende desde el nivel del mar hasta 5.000 m de altura. Novedosas antenas multisectoriales permiten el uso eficiente del espectro de 6 MHz por canal, a la vez que facilitan aplicaciones tales como videoconferencias y telefonía IP.

Las escuelas, los hospitales, las bibliotecas y los centros comunitarios constituyen el principal objetivo de la conectividad, pero varias oficinas gubernamentales ahora también tienen la capacidad de interactuar con los ciudadanos con una eficiencia novedosa, con lo cual se promueven cambios sociales profundos.

El presente artículo aborda los obstáculos técnicos y culturales que han debido superarse para que el proyecto cumpla con su cometido.

Contenidos:

Introducción

Mérida es uno de los tres estados montañosos de Venezuela donde los Andes alcanzan los 5.000 m.

La ciudad del mismo nombre yace al pie de la montaña más alta, en una meseta de unos 1.600 m. Es la capital del estado, y alberga una universidad bicentenaria de unos 35.000 estudiantes. La Universidad de Los Andes (ULA) instaló la primera red de computación académica en 1.989, la cual, a pesar de limitaciones económicas, ha crecido para albergar un cable de fibra óptica de 26 km sobre el cual se han tendido tanto redes TDM como ATM (Asynchronous Transfer Mode)[5].

No obstante, muchos lugares de la ciudad, sin mencionar los pueblos aledaños, quedan fuera del alcance del anillo de fibra óptica. La universidad también cuenta con un servidor de comunicaciones con líneas telefónicas para proporcionar acceso remoto a su red, pero las llamadas locales se cobran por minuto y muchos pueblos ni siquiera tienen líneas telefónicas.

Por las razones antes expuestas, se han hecho esfuerzos desde el comienzo para desarrollar acceso inalámbrico para la red universitaria

5. Para el año 2006, sobre el mismo cable de fibra óptica, se ha desplegado una red Gigabit Ethernet de 50 km.

RedULA. El primer intento aprovechó las redes de paquetes existentes operados por radioaficionados quienes, ya desde 1.987, tenían una pasarela (gateway) con una estación HF (High Frequency) operando a 300 bps para contactos internacionales, y varias estaciones VHF (Very High Frequency) conectadas a 1.200 bps que interconectaban el país.

Las abruptas montañas de la región son grandes obstáculos para construir carreteras y tender cables pero pueden ser útiles para la instalación de radio enlaces.

Esta tarea es facilitada por la existencia de un teleférico que tiene la fama de ser el más alto del mundo y que une la ciudad con un pico de 4.765 m. En la ruta hacia este pico, el teleférico toca una estación intermedia —La Aguada— con una altitud de 3.450 m y una espectacular vista de la ciudad de Mérida y otros pueblos a una distancia de hasta 50 km.

Packet Radio

Los radioaficionados locales operan una red de paquetes. Inicialmente funcionaba a 1.200 bps en VHF y usaba radios FM de voz para aficionados conectados a un computador personal (PC) por medio de un TNC (Terminal Node Controller). El TNC es la interfaz entre el radio analógico y la señal digital del PC, abre el circuito *Push to Talk* en el radio para cambiar de transmisión a recepción, ejecuta la modulación/demodulación y el ensamblaje/desensamblaje de los paquetes usando una variación del protocolo X.25 conocida como AX.25. Se construyeron gateways entre los

radios VHF y HF conectando dos módems al mismo TNC y al mismo computador. Normalmente, un *gateway* conectaría la red de paquetes VHF local a nodos internacionales por medio de estaciones HF que podrían cubrir miles de kilómetros aunque la velocidad sea de sólo 300 bps. Se construyó también una red de paquetes nacional basada en *digipeaters* (repetidoras digitales: básicamente un TNC conectado a dos radios con antenas apuntando en diferentes direcciones) para extender la red desde Mérida a Caracas por medio de sólo dos estaciones repetidoras de este tipo. Los *digipeaters* operaban a 1.200 bps y permitían compartir programas y algunos archivos de texto entre los aficionados.

Phil Karn[6], un radioaficionado con sólidos conocimientos de redes de computación escribió el programa KA9Q que implementa TCP/IP (protocolo de transmisión de control/protocolo de Internet) sobre AX.25. Con el uso de este programa, bautizado con las siglas de su inventor, los aficionados de todo el mundo se pudieron conectar muy pronto a Internet usando diferentes tipos de radios. KA9Q limita las funciones del TNC a un nivel mínimo, aprovechando el poder de la PC conectada para la ejecución de la mayoría de las funciones. Este enfoque permite una gran flexibilidad y actualizaciones fáciles. También en Mérida pudimos muy pronto actualizar nuestra red a 9600 bps con el uso de módems más avanzados, y varios radioaficionados tuvieron acceso a Internet a través de la red cableada RedULA, operada por la Universidad de Los Andes. El reducido ancho de banda disponible en la banda VHF limitó la velocidad obtenible. Para incrementarla, hubo que moverse a portadoras de más alta frecuencia. En UHF (Ultra-High Frequency), a los aficionados se les permite el uso de canales de 100 kHz de ancho. Radios digitales, acoplados con módems de 19.2 kbps permitieron doblar los anchos de banda de la transmisión. Con el uso de esta tecnología y antenas construidas en el Laboratorio de Comunicaciones de la ULA, LabCom, se desarrolló un proyecto para conectar la Casa de Ciencia en la ciudad de El Vigía, con Mérida y con Internet.

---

6. Karn, Phil, "The KA9Q Internet (TCP/IP) Package: A Progress Report," Sixth ARRL Computer Networking Conference, Redondo Beach, CA, 29 August 1987.

A pesar de que El Vigía dista sólo 100 km de Mérida por carretera, el terreno montañoso demanda el uso de dos repetidores, uno colocado en La Aguada, a 3.450 m de altitud, y otro en Tusta, a 2.000 m. El proyecto fue financiado por FUNDACITE-MERIDA, una institución gubernamental que promueve la ciencia y la tecnología en el estado. FUNDACITE también opera un grupo de módems telefónicos de 56 kbps que proveen acceso a Internet, tanto a instituciones como a individuos. La necesidad de dos estaciones repetidoras subraya las limitaciones impuestas por el uso de portadoras de alta frecuencia que requieren de línea de vista para establecer transmisiones confiables, mientras que en la banda VHF las señales se reflejan fácilmente superando las montañas. A veces, es posible usar repetidores pasivos que se construyen conectando dos antenas direccionales espalda a espalda con un cable coaxial sin necesidad de radio. Este esquema fue probado para conectar mi residencia con el LabCom, a sólo 11 km de distancia, pero con una colina en el medio que bloquea las señales de radio. Este obstáculo se salvó aprovechando la reflexión en La Aguada, donde se instalaron dos antenas orientadas con 40 grados de separación.

Aunque este esquema era muy interesante y, ciertamente, mucho más económico que el acceso por módems que proporcionaban el mismo ancho de banda para ese entonces, se necesitó un medio más rápido cuando nos enfrentamos a la tarea de construir un *backbone* inalámbico para conectar poblaciones remotas.

Exploramos, entonces, el uso de los módems de 56 kbps desarrollados por Dale Heatherington[7], albergados en una tarjeta PI2 construida por aficionados de Ottawa, conectados directamente en el bus del PC, y usando LINUX como sistema operativo de red. Aunque este sistema funcionaba muy bien, el surgimiento de la World Wide Web con su plétora de imágenes y otras aplicaciones consumidoras de ancho de banda, hizo patente que si queríamos satisfacer las necesidades de escuelas y hospitales, teníamos que implementar una solución de mayor ancho de banda, por lo menos en el *backbone*. Esto significó el uso de frecuencias portadoras más elevadas, en el rango de las microondas, lo cual implica costos altos. Afortunadamente, una alternativa tecnológica usada comúnmente por los militares, se puso a la disposición para usos civiles a precios razonables. Esta tecnología llamada ***espectro esparcido*** encontró por primera vez aplicación civil como red inalámbrica de área local de corto alcance (LAN), y mostró pronto su gran utilidad en lugares donde el espectro electromagnético no está sobresaturado, permitiendo salvar distancias de varios kilómetros.

Espectro esparcido

La técnica de espectro esparcido utiliza señales de baja potencia expandiendo el espectro hasta abarcar el ancho de banda asignado, permitiendo así que un número de usuarios compartan el medio a través de la utilización de códigos diferentes para cada suscriptor.

Hay dos maneras de lograr esto: Espectro esparcido de secuencia directa (DSSS) y espectro esparcido de salto de frecuencia (FHSS).

- En DSSS, la información que se va a transmitir se multiplica digitalmente por una secuencia de alta frecuencia, aumentando, por lo tanto, el ancho de banda de transmisión. A pesar de que esto pueda parecer un desperdicio de ancho de banda, el sistema de recuperación es tan eficiente que puede descodificar señales muy débiles permitiéndoles a varias estaciones el uso simultáneo del mismo espectro.
- En FHSS, el transmisor está constantemente cambiando la frecuencia de la portadora dentro del ancho de banda asignado, de acuerdo con un código específico. El receptor debe conocer este código para rastrear la frecuencia de la portadora. Ambas técnicas, en efecto, intercambian potencia por ancho de banda, permitiendo que muchas estaciones compartan una cierta porción del espectro.

Durante la Primera Escuela Latinoamericana de Redes (EsLaRed´92), realizada en Mérida en 1992, mostramos esta técnica estableciendo

---

7. Heatherington, D., "A 56 kilobaud RF modem," Sixth ARRL Computer Networking Conference, Redondo Beach, CA, 29 August 1987.

algunas redes de prueba utilizando antenas externas construidas en el LabCom, lo que permitió una transmisión a varios kilómetros.

En 1993[8] el Ministerio de Comunicaciones de Venezuela abrió cuatro bandas para uso con espectro esparcido:

- 400 - 512 MHz
- 806 - 960 MHz
- 2,4 – 2,4835 GHz
- 5,725 – 5,850 GHz

Para cualquiera de las bandas anteriores la potencia máxima del transmisor se restringió a 1 vatio y la ganancia máxima de antena a 6 dBi, para una PIRE (potencia isotrópica radiada equivalente) total de 36 dBm.

Esta reglamentación echó las bases para el desarrollo de una red DSSS con un ancho de banda nominal de 2 Mbps en la banda de 900 MHz que cumpliera los requerimientos impuestos por el nacimiento de la actividad de la World Wide Web. Partiendo del LabCom, donde existía conexión a RedUla, una antena Yagi casera orientada hacia La Aguada se enlazaba a un reflector de esquina, el cual, con un ancho de haz de 90 grados, iluminaba la mayor parte de la ciudad de Mérida. Varios suscriptores que compartían el ancho de banda nominal de 2 Mbps pudieron intercambiar archivos, incluyendo imágenes y video clips. Algunos sitios que requerían cables más largos entre la antena y el radio fueron acomodados por medio del uso de amplificadores bilaterales.

Estos alentadores resultados se comunicaron a un grupo conformado con miras a resolver los problemas de conectividad de la universidad de Ile-Ife, en Nigeria, en el International Centre for Theoretical Physics (ICTP) de Trieste, Italia, en 1995. Más tarde, en ese mismo año, la red propuesta fue instalada por personal del ICTP con fondos de la Universidad de las Naciones Unidas. Dicha red conecta el Centro de Computación, el Edificio de Ciencias Físicas y el Edificio de Tecnología, tres instalaciones separadas aproximadamente 1 km en la universidad nigeriana. Esta conexión ha venido funcionando satisfactoriamente desde entonces, demostrando ser una solución mejor, en su relación costo-efectividad, que la red de fibras ópticas originalmente planeada[9].

---

8. Conatel, Comision Nacional de Comunicaciones, Ministerio de Transporte y Comunicaciones, "NORMAS PARA LA OPERACION DE SISTEMAS DE TELECOMUNICACIONES CON TECNOLOGIA DE BANDA ESPARCIDA (SPREAD SPECTRUM)," Caracas, 17 Noviembre1993.

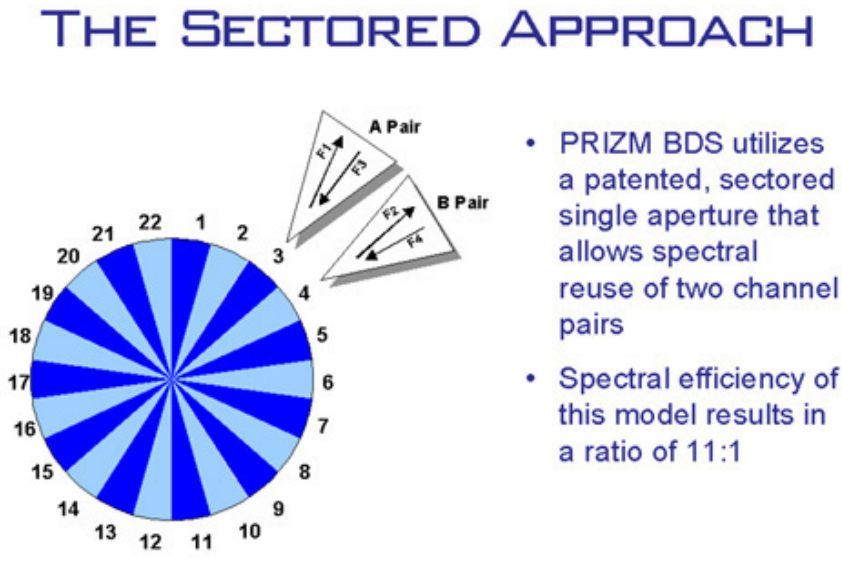
9. International Centre For Theoretical Physics, "Programme of Training and System Development on Networking and Radiocommunications," Trieste, Italy, 1996, http://www.ictp.trieste.it

Volviendo a Mérida, a medida que el número de sitios crecía, el rendimiento observado por usuario descendía, así que comenzamos a examinar la banda de 2.4 GHz para proporcionar una nueva solución al tráfico adicional. Esta banda puede transportar simultáneamente tres flujos independientes de 2 Mbps, pero la distancia cubierta es menor que la permitida por la banda de 900MHz. Mientras planeábamos la extensión del *backbone* usando esta banda, nos enteramos de una compañía naciente que ofrecía una solución novedosa con mejores prestaciones: distancias mayores, rendimientos considerablemente altos, y la posibilidad de re-uso de frecuencias utilizando microondas de banda estrecha.

Sistema de acceso de banda ancha

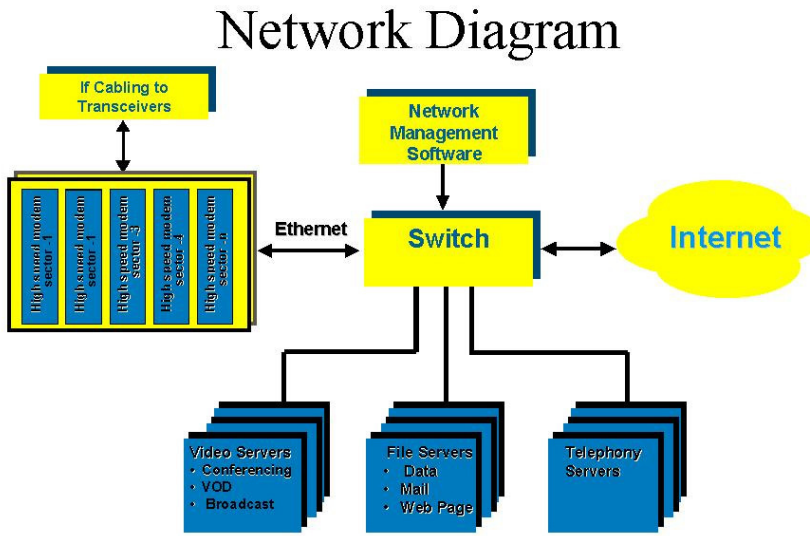
Después de visitar las instalaciones de Spike Technologies en Nashua, New Hampshire[10], nos convencimos de que su antena patentada y su sistema de radio eran la mejor solución para los requerimientos de nuestra red del estado por las razones siguientes:

Este sistema de acceso de banda ancha emplea una antena multisectorial con una ganancia de 20 dBi que permite hasta 22 sectores independientes, cada uno transmitiendo y recibiendo en canales separados a 10 Mbps, full duplex, para un rendimiento agregado de 440 Mbps. El re-uso de frecuencias en los sectores no adyacentes permite una gran eficiencia espectral.

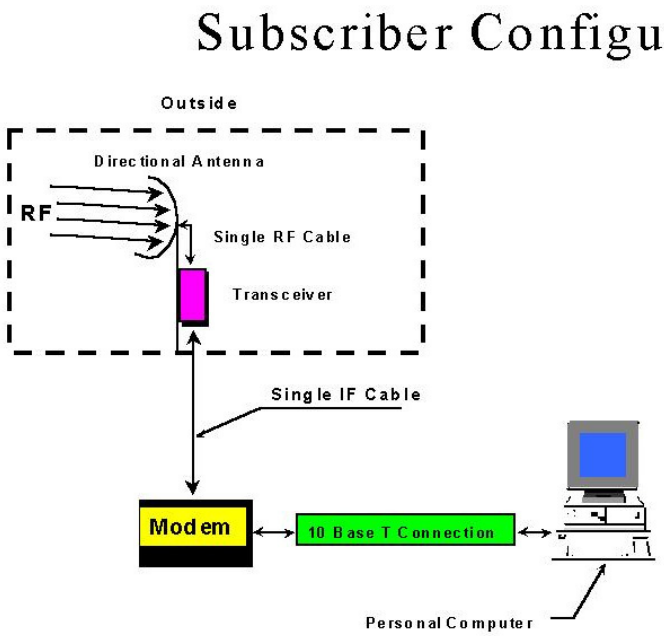


10. Spike Technologies, Inc. http://www.spike.com

Los radios digitales de banda estrecha pueden operar indistintamente en frecuencias desde 1 a 10 GHz, con un alcance de hasta 50 km. Los radios pueden funcionar con una variedad de módems de TV por cable, suministrándole al suscriptor una conexión estándar 10Base-T para LAN. En la estación base, los diferentes sectores están interconectados con un interruptor de alta velocidad y pequeña latencia, permitiendo aplicaciones de video de alta calidad de 30 tramas/s. Cada sector se comporta como un LAN Ethernet independiente.



En el sitio del suscriptor un radio similar y un módem proveen una conexión 10Base T a la Ethernet local.



Con financiamiento de Fundacite, un sistema de prueba se instaló muy pronto en Mérida, con la estación base situada justo encima de la estación del teleférico, La Aguada, a una altura de 3.450 m.

Inicialmente, se instalaron sólo 5 sectores, cada uno con un ancho de haz de 16 grados. El primer sitio estaba en el sector 1, en las instalaciones de Fundacite, donde un sistema satelital proporcionaba acceso a Internet. El sector 2 daba servicio al Palacio de Gobierno. El sector 3, a FUNDEM, una organización de prevención de desastres del gobierno local. El sector 4 daba servicio a un centro penitenciario cerca de la población de Lagunillas, a unos 35 km de Mérida. El sector 5 transmitía a una repetidora en la cima de una montaña cerca del pueblo de La Trampa, a 40 km de La Aguada. Desde La Trampa, otro enlace de 41 km extendía la red hasta la Casa de Ciencia de Tovar.

La figura 9 muestra un mapa de la ciudad de Mérida. Las líneas negras muestran el backbone inicial, y las rojas, el extendido.

En enero de 1.998, una video-conferencia entre el centro penitenciario y el Palacio de Justicia en Mérida, demostró que, aparte del acceso a Internet, el sistema podía también utilizarse en video de tiempo real, en este caso, empleado para que el juez pudiera entrevistar a los internos, evitándose así las inconveniencias y riesgos de su transporte fuera del local.

El éxito de esta prueba estimuló al gobierno local en la búsqueda de los fondos necesarios para la instalación de un sistema completo de acceso a Internet de alta velocidad para el sistema de salud, educación, bibliotecas, centro comunitarios, y varias agencias gubernamentales. En enero de 1.999 teníamos 3 hospitales, 6 centros educativos, 4 institutos de investigación, 2 diarios, 1 estación de TV, 1 biblioteca pública, y 20 instituciones sociales y

gubernamentales compartiendo información y acceso a Internet. Se planeaba en este año la conexión de 400 sitios a una velocidad 10Mbps full duplex, y los fondos para este propósito ya se habían conseguido. Entre las varias actividades apoyadas por esta red vale la pena mencionar las siguientes:

- Educativas: Las escuelas encontraron un extenso reservorio de materiales de gran calidad para alumnos y profesores especialmente en las áreas de geografía, idiomas y ciencias, así como herramientas para comunicarse con otros grupos de intereses comunes. Las bibliotecas tienen salas con computadores accesibles al público general conectadas a Internet. Los periódicos y las estaciones de TV cuentan con un inagotable caudal de información disponible para su audiencia.
- Salud: El hospital universitario tiene una conexión directa a la unidad de cuidados intensivos donde una planta de médicos especialistas está siempre de guardia. Estos médicos están disponibles para consultas de parte de colegas que se encuentren en poblaciones distantes para discutir casos específicos. Un grupo de investigadores de la universidad está desarrollando varias aplicaciones de telemedicina basadas en la red.
- Investigación: Además de la universidad y Fundacite, el observatorio astronómico de Llano del Hato, situado en una montaña a 3.600 m y a 8 grados del ecuador, será conectado pronto, lo que permitirá a los astrónomos de todo el mundo el acceso a las imágenes allí almacenadas. Investigadores de campo de poblaciones remotas podrán disfrutar de acceso a Internet.
- Gobierno: La mayoría de las agencias gubernamentales están conectadas y comienzan a colocar información en línea para los ciudadanos. Esperamos que esto tenga un gran impacto para la relación entre los ciudadanos y el gobierno. Las agencias de ayuda y las fuerzas policiales hacen también uso frecuente de la red.
- Entretenimiento y Productividad: Para la gente que vive fuera de la ciudad las oportunidades ofrecidas por la Red tienen un impacto significativo en su calidad de vida. Esperamos que esto ayude a revertir la tendencia al éxodo de las zonas rurales aliviando, por ende, la sobrepoblación de las ciudades. Los campesinos tienen acceso a la información sobre los precios de sus cultivos y materiales, así como a información que ayude a mejorar sus prácticas de agricultura.

Durante el evento SUPERCOMM´98, realizado en Atlanta, en junio de ese año, la red de acceso de banda ancha de Mérida fue elegida como ganadora del premio SUPERQuest en la categoría de Acceso Remoto.

Entrenamiento

Desde nuestros primeros esfuerzos por establecer una red de computadoras, nos dimos cuenta de que el entrenamiento de las personas

involucradas en la construcción, gerencia y mantenimiento de la misma, era de vital importancia para el éxito y supervivencia del proyecto. Dadas las limitaciones de nuestro presupuesto, decidimos que teníamos que unir nuestros recursos con los de otras personas que también requirieran entrenamiento. En 1990, el ICTP organizó la First International School on Computer Network Analysis and Management, a la que asistieron los profesores José Silva y Luis Núñez de nuestra universidad. A su regreso a Mérida, ellos propusieron que se implementara una actividad semejante en nuestra institución. Para este fin, y aprovechando mi sabático, pasé tres meses en Bellcore, en Morristown, New Jersey, y tres más en el ICTP, secundado por mi colega, Profesor Edmundo Vitale, en la preparación de la Second Networking School realizada en ese instituto, en 1992. El resto de mi sabático lo pasé en SURANET, en College Park, Maryland, bajo la guía del Dr. Glenn Ricart, quien me presentó al Dr. Saul Hahn, de la organización de Estados Americanos. Posteriormente, el Dr. Hahn ofreció respaldo financiero para una actividad de entrenamiento en Latinoamérica. Estas experiencias nos permitieron el lanzamiento de la Primera Escuela Latinoamericana de Redes (EsLaRed´92) en Mérida[11], a la que asistieron 45 participantes de 8 países, con instructores de Europa, Estados Unidos y Latinoamérica. Este entrenamiento teórico-práctico duró tres semanas y en él se enfatizaron las tecnologías inalámbricas. EsLaRed´95 tuvo lugar de nuevo en Mérida, con 110 participantes y 20 instructores. EsLaRed´97 contó con 120 participantes y fue respaldada por la Internet Society, que también apoyó el Primer Taller de Redes en español y portugués para Latinoamérica y el Caribe realizado en Río de Janeiro, en 1998, con EsLa Red como responsable de los contenidos de los entrenamientos. EsLaRed´99 se fundirá este año con Walc´99, el segundo taller de Internet para Latinoamérica y el Caribe que se realizará en Junio, en nuestra universidad.

Comentarios finales

Este artículo ha descrito algunos de los esfuerzos emprendidos en el campo de las redes de computadoras en el estado Mérida. La Internet en los países en desarrollo tiene un impacto aún más profundo que en otras partes debido al alto costo de las llamadas internacionales, faxes, revistas y libros, aún más crítico tomando en cuenta el bajo ingreso promedio de la población. Algunos habitantes de poblaciones remotas que no tienen teléfonos están experimentando la transición del siglo 19 al siglo 21 gracias a las redes inalámbricas. Es de esperar que esto contribuya a mejorar el nivel de vida en los campos de salud, educación, entretenimiento y productividad, así como a crear una relación más equitativa entre los ciudadanos y sus gobiernos.

--Ermanno Pietrosemoli

---

11. Escuela Latinoamericana de Redes, http://www.eslared.org.ve

EHAS- Enlace hispanoamericano de Salud

Instalación de una red Wi-Fi para la mejora de la atención primaria de salud en una zona rural aislada de Cusco, Perú

Andrés Martínez, Javier Simó, Joaquín Seoane, Esther Senso, Valentín Villarroel, Arnau Sánchez, Sandra Salmerón, Silvia Lafuente, Pablo Osuna, David Chávez, Jaime Vera, David Espinoza, River Quispe, Luis Camacho, César Córdova, Leopoldo Liñán, Juan Paco Fernández, Yvanna Quijandria, Paola Sanoni, Humberto Guerra, Carlos Kiyán, José Luis Rojas, Jamine Pozú y Norma Rodríguez

Contacto: *info@ehas.org*
Sitio Web: *http://www.ehas.org*

RESUMEN

En el marco del Programa @LIS - Alianza para la Sociedad de la Información -, ejecutado por el Programa de Cooperación de la Unión Europea, la Fundación EHAS - Enlace Hispano Americano de Salud -, culminó en Febrero de 2006 la implementación y puesta en marcha de una Red de Telecomunicaciones en la Región de Cusco, Perú. Esta red, concebida como una red piloto, nació con el objetivo de mejorar los procesos de atención de salud primaria de esta zona. El proyecto permitió la interconexión de 12 establecimientos de salud rurales, antes totalmente aislados entre sí tanto del Hospital Regional de Salud de Cusco y la Red de Salud Cusco Sur. La tecnología empleada en esta red ha sido Wi-Fi, adaptada para un escenario de distancias largas con enlaces de hasta 40km. Además, dadas las altas prestaciones obtenidas (6.5Mbps obtenidos en los enlaces de 40km), se ha instalado un sistema de telefonía sobre IP (VoIP) que permite la comunicación de voz gratuita entre todos los establecimientos y la interconexión de todos ellos con la red telefónica conmutada exterior.

Una vez puesta en marcha la red de comunicaciones se ha procedido a implementar servicios que, entre otros, permitan la formación remota del personal de salud, promuevan la mejora del sistema de vigilancia epidemiológica, y apoyen el sistema de referencia y contra-referencia de pacientes. De forma adicional, teniendo como base la infraestructura de la red y los servicios de comunicaciones brindados, se está ejecutando en la actualidad un proyecto piloto de Telemedicina que permitirá evaluar la viabilidad técnica e institucional de la implementación de algunos servicios de telemedicina como estetoscopía, cardiología, dermatología y tele-consulta para primera y segunda opinión.

ANTECEDENTES

La atención sanitaria en establecimientos de salud rurales de países en desarrollo suele ser muy deficiente debido a la falta de medios materiales, la insuficiente cualificación de los técnicos de salud y la incomunicación con el resto de la red de salud; todo ello da lugar a serias dificultades para prevenir las enfermedades, realizar diagnósticos y tratamientos adecuados o atender de forma debida las emergencias médicas.

Ante esta situación el Grupo de Bioingeniería y Telemedicina (GBT) de la Universidad Politécnica de Madrid (UPM), y la ONG Ingeniería sin Fronteras (ISF) crearon en 1997 el Programa EHAS (Enlace Hispano Americano de Salud), con el objetivo de introducir sistemas de comunicación y telemedicina para el personal sanitario rural, de forma que permitieran un mejor uso de los recursos ya existentes y una mejor coordinación del sistema completo de atención de salud.

Después de un periodo inicial de investigación realizado en Madrid por el grupo GBT-UPM se obtuvo una importante conclusión: el acceso a Internet a través de radio VHF/HF en zonas rurales aisladas de países en desarrollo era viable tanto tecnológica como económicamente. Con el objetivo de implementar un primer proyecto piloto en Perú, dos instituciones locales de Lima se unieron al Programa EHAS: la Facultad de Telecomunicaciones de la Pontificia Universidad Católica del Perú (PUCP), actuando como contraparte tecnológica, y la Universidad Peruana Cayetano Heredia (UPCH) como contraparte médica y de salud. Este equipo multidisciplinar comenzó a trabajar en el desarrollo de dos líneas principales de acción: la tecnología EHAS y los servicios EHAS.

Fruto de esta colaboración llegó la primera experiencia piloto: una red de voz y datos (correo electrónico) para comunicar 39 establecimientos de salud en la zona de Huallaga en Alto Amazonas, Perú. Los primeros resultados obtenidos en una evaluación posterior (2001) arrojaron un balance muy positivo sobre el impacto del proyecto, a partir de lo cual se decidió ampliarlo a otras regiones en Perú y a países como Colombia y Cuba. Durante los años posteriores nuevos proyectos pilotos son desarrollados en cada uno de estos países, gracias al apoyo financiero de instituciones como el Banco Mundial, el Ayuntamiento de Madrid, Greenpeace o la Unión Europea.

La estructura jerárquica propuesta para EHAS Perú (un socio tecnológico y otro médico) fue también replicada para los casos de Colombia y Cuba. De esta manera, en Colombia el Departamento de Telemática y el Departamento de Medicina Social, ambos de la Universidad del Cauca, se convierten respectivamente en el socio tecnológico y el socio médico. En el caso de Cuba las instituciones implicadas son INFOMED y CEDISAP, ambas pertenecientes al Ministerio de Salud de Cuba.

De manera simultánea a estos proyectos pilotos, el equipo de EHAS sigue trabajando en la adaptación de tecnologías de comunicación para su aplicación a zonas rurales aisladas. Algunos de los resultados conseguidos son: el desarrollo de modems software VHF/HF de altas prestaciones, la adaptación de la tecnología Wi-Fi para enlaces de larga distancia, y el uso de la tecnología VoIP en una red Wi-Fi con una arquitectura de calidad de servicio.

En el 2004, gracias a la importante dimensión adquirida por EHAS, tanto ISF como UPM crearon la Fundación EHAS, una organización sin ánimo de lucro con entidad legal independiente pero bajo la supervisión de ambas instituciones.

JUSTIFICACIÓN

Estructura de los establecimientos de salud

La atención primaria de salud en las zonas rural de Cusco, y en general de cualquier país latinoamericano, se organiza principalmente a través de dos tipos de establecimientos, los Centros (CS) y los Puestos de Salud (PS). Los CS son los establecimientos de mayor jerarquía y están situados en las capitales de provincia (en localidades medianamente pobladas, entre 1.000 y 5.000 habitantes), donde suele llegar la línea telefónica. Son centro de referencia de varios PS, están siempre dirigidos por médicos, poseen cierta infraestructura y equipamiento para realizar algunas pruebas diagnósticas y suelen contar con laboratorio. Algunos de ellos permiten la hospitalización y son el lugar desde el que se coordinan las actividades de los PS asociados (distribución de medicamentos, envío y recepción de informes administrativos y epidemiológicos, capacitaciones al personal, etc.).

Los PS dependen de los CS y están situados en poblaciones, en la mayoría de los casos, aisladas, en áreas de baja densidad de población y generalmente con menos de 500 habitantes. No cuentan con línea telefónica y están mal dotados de infraestructura de carreteras y suministro eléctrico. Estos establecimientos están normalmente a cargo de personal de enfermería o técnicos sanitarios. Este personal depende asistencialmente del médico jefe del CS de referencia.

Variables de contorno del escenario de trabajo

La insuficiente formación del personal sanitario rural, las dificultades para la coordinación de emergencias médicas, la falta de información epidemiológica o los problemas de calidad en la misma, los excesivos viajes necesarios para la coordinación de actividades, su excesivo coste y la cantidad de horas de inactividad o de falta de atención que producen,

justifica la necesidad de una intervención como la propuesta por el programa EHAS.

Sin embargo, existen unos condicionantes que plantea la zona rural que impiden una actuación clásica para la instalación de sistemas de comunicación y servicios de información. Nos referimos a que:

- Los ingresos de los establecimientos de salud rurales son tan bajos que descartan cualquier solución tecnológica con altos costes de operación.
- La mayoría de estos establecimientos no cuentan con sistemas de suministro de energía eléctrica.
- Algunos Centros de Salud cuentan con línea telefónica, pero prácticamente todos los Puestos de Salud carecen de teléfono y carecerán por al menos diez años.
- En los sistemas rurales de salud hay poca formación y experiencia en el uso, mantenimiento y gestión de tecnologías de la información.

Por todo esto se justifica una intervención que utilice tecnología de comunicación apropiada, robusta pero a su vez fácil de manejar, de bajo consumo y bajo coste, pero sobre todo con unos gastos de operación (costes de comunicación) mínimos. Además, lo inadecuado de los materiales formativos clásicos para responder a las necesidades del sector salud rural, fundamenta la necesidad de crear contenidos específicos con el doble fin de mejorar la capacitación y evitar la sensación de aislamiento, principal causante de la alta rotación del personal sanitario rural.

El programa EHAS propone además un esquema de trabajo con los socios locales que supone, en primer lugar, un proceso de transferencia tecnológica a los agentes nacionales para que conozcan y dominen la tecnología a emplear y la generación y provisión de servicios de información electrónicos para salud; luego, en segundo lugar, la constitución de una red de colaboración transnacional sur–sur que permita aprovechar las sinergias en las labores de investigación y desarrollo de servicios; y por último, una actividad que genere capacidades locales para poder asumir el modelo de desarrollo del programa en su propio país.

Finalmente, con vistas a asegurar la aceptación de la intervención entre los agentes locales involucrados y su sostenibilidad, el proyecto asume un procedimiento participativo e integrador de los grupos beneficiarios, que presta especial atención a los aspectos de capacitación y gestión del cambio.

Problemática de la salud en el Perú

En las últimas décadas, aún subsisten indicadores de salud alarmantes que ubican al Perú en una situación desfavorable en comparación con la mayoría de los países latinoamericanos.

En la Región Cusco en los últimos años se ha presentado en general una reducción sostenida de la mortalidad, especialmente a expensas de las enfermedades infecciosas y transmisibles. Sin embargo las múltiples carencias de las instalaciones de salud con que cuenta es un factor que pone en riesgo a la población beneficiaria.

En la Dirección Regional de Salud (DIRESA) de Cusco no se cuenta con información actualizada que permita conocer el estado actual de infraestructura en los establecimientos de salud; ni información sobre el equipamiento y tecnología disponibles. Sin embargo, es evidente que un importante porcentaje de los establecimientos de salud requieren rehabilitación, ampliación, conclusión y/o construcción. El equipamiento médico es insuficiente, en otros es obsoleto y con escaso mantenimiento, al igual que los medios de transporte y comunicación.

El sistema de referencia y contrarreferencia es importante porque solo en la ciudad del Cusco se encuentran los 2 Hospitales Referenciales a nivel regional, por ende se transfieren solamente los casos más graves. La inaccesibilidad a los servicios de salud es uno de los factores asociados a la mortalidad, así como la organización de los servicios de salud y su capacidad de respuesta en términos de resolutividad y calidad de atención.

Por otra parte la Mortalidad Perinatal representa un problema pendiente de resolución, considerado como uno de los marcadores que refleja el nivel de desarrollo así como un indicador de la pobreza de los pueblos. Al analizar la información sobre las muertes maternas en un 42% se cataloga que si hubo demora en llegar al Establecimiento de Salud, asociado a la inaccesibilidad geográfica así como a dificultades para trasladar a la paciente a un servicio de salud.

Justificación sobre la tecnología empleada

Las condiciones particulares ya vistas de este escenario condiciona grandemente las tecnologías de comunicación que se pueden usar: la falta de recursos hace inapropiadas las redes de operador tales como la telefonía móvil, las infraestructuras cableadas y las redes satelitales; la inaccesibilidad de muchos lugares y la dispersión de la población sugiere el uso de tecnologías inalámbricas de largo alcance, y la falta de energía eléctrica y de técnicos cualificados también incide en qué tipo de tecnologías se pueden usar de forma sostenible.

En EHAS se han empleado con éxito redes radio operando en las bandas HF y VHF, ampliamente utilizadas para las comunicaciones de voz semi-dúplex, y que pueden ser aprovechadas también para comunicaciones de datos. No obstante, esta solución presenta algunos inconvenientes como la lentitud en la comunicación de datos, el alto consumo de los equipos, el alto coste de las instalaciones, la difícil adaptación a la red telefónica y el uso de frecuencias con licencia.

Una nueva línea de investigación que se abrió en los últimos años en EHAS se basó en la tecnología inalámbrica IEEE 802.11 (Wi-Fi). Con esta tecnología se ha dado un fenómeno de apropiación por parte de los países en vías de desarrollo; la carencia de infraestructuras de comunicación apropiadas para las comunicaciones de datos, incluso en los núcleos urbanos de muchos países, ha dado lugar a numerosas experiencias de adaptación de Wi-Fi para distribuir el acceso a Internet con la mayor cobertura posible en exteriores. El enorme éxito de Wi-Fi en todos los ámbitos ha dado lugar a una gran cantidad de productos en el mercado, a precios extremadamente bajos y mucha flexibilidad de uso en combinación con desarrollos de software abierto.

Entre tanto, se está a la espera de la consolidación definitiva de Wimax o IEEE 802.16, tecnología emergente pensada para la distribución inalámbrica de la conectividad de datos con QoS a largas distancias. Pero se sabe que se tardará en tener soluciones Wimax tan accesibles como lo son las Wi-Fi, sobre todo en términos de costo.

En los países en desarrollo, Wi-Fi presenta varias ventajas importantes: hay mucho equipamiento a costos muy reducidos, suele ser de muy bajo consumo y emplea una banda de frecuencias de uso libre, aunque con ciertas restricciones. Además con esas limitaciones y las sensibilidades de los equipos Wi-Fi del mercado, se pueden realizar enlaces tanto PtP (punto a punto) como punto a multipunto (PtMP) de muchas decenas de kilómetros. No obstante, Wi-Fi no deja de ser una tecnología pensada para redes locales inalámbricas, y el MAC presenta importantes limitaciones en enlaces largos, si bien mediante algunas modificaciones es posible adaptarlo a este último escenario.

Otro punto de interés es la búsqueda de la arquitectura de red idónea para el despliegue de este tipo de redes. Hemos apostado por la arquitectura mesh, cuya popularidad es cada vez mayor. Las redes mesh se forman de forma espontánea sin ninguna infraestructura, constituyendo mallas que conectan un cierto número de nodos entre sí, y en que cada nodo puede ser al mismo tiempo pasarela a Internet, repetidor o nodo cliente.

La gran limitación de Wi-Fi, ya sea en infraestructuras o en redes mesh, es la necesidad de línea de vista para establecer enlaces que excedan de

algunos centenares de metros. Esta condición puede ser imposible o muy difícil de conseguir en muchos casos, lo que llevará en muchas instalaciones prácticas a la necesidad de instalar nodos repetidores para comunicar a los nodos clientes. Este ha sido el caso de la red Wi-Fi de Cusco.

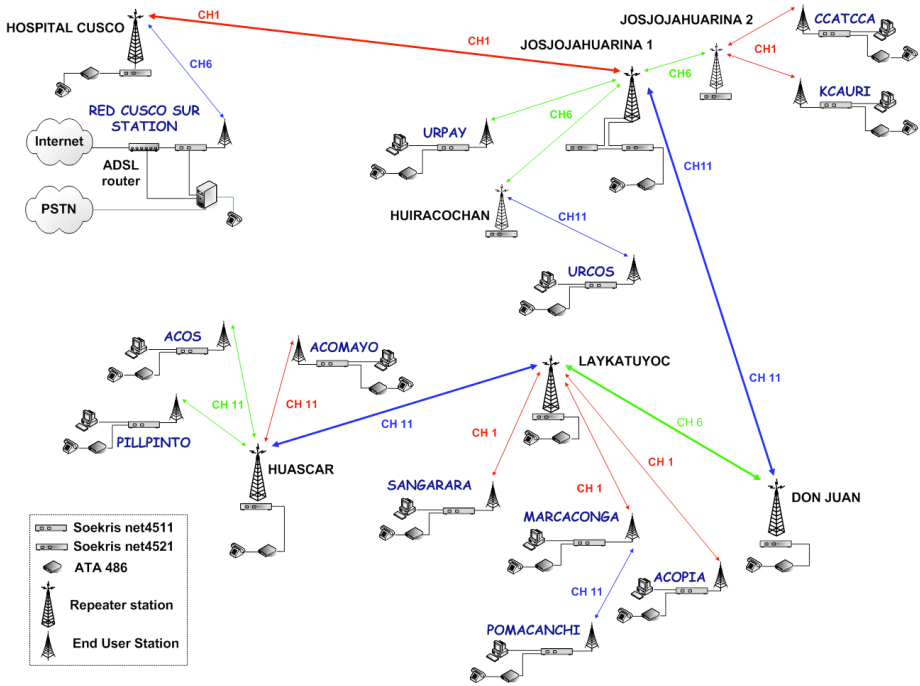
USOS Y APLICACIONES

Descripción de la Red

La Red EHAS implementada en Cusco interconecta a 12 establecimientos de salud del Ministerio de Salud de Perú (MINSA) ubicados en las provincias de Quispicanchi y Acomayo con la Red de Servicios Cusco Sur (perteneciente a la DIRESA) y el Hospital Regional del Cusco.

En la siguiente Figura se detalla de manera esquemática el diseño de la Red Wi-Fi de Cusco. Los establecimientos de salud son: DIRESA de Cusco, Ccatcca, Kcaury, Urpay, Urcos, Acopia, Pomacanchi, Marcaconga, Sangarará, Acomayo, Acos y Pillpinto.

Los repetidores, que se eligieron por tener línea de vista directa con los centros/puestos de salud de su respectiva zona, son: Hospital Cusco, Josjojahuarina1, Josjojahuarina2, Huiracochán, Don Juan, Laykatuyoc y Huascar.



Servicios de comunicación

Los servicios básicos que ofrece el proyecto a los usuarios son:

- **Acceso a Internet.** El acceso se realiza de forma transparente para el usuario a través de su PC. Los dos principales servicios de los que hacen uso los usuarios de los establecimientos de salud son el navegador Web (Mozilla Firefox) y los programas de mensajería (Gaim).
- **Correo electrónico.** Se ha instalado un servidor de correo en Cusco encargado de gestionar las cuentas de correo de cada uno de los usuarios. Una de las principales ventajas de manejar cuentas de correo electrónico siguiendo este esquema es que el servicio podrá seguir usándose aún cuando no exista conectividad con la red exterior. Mientras que si se usaran direcciones de correo de otros proveedores (yahoo, gmail, etc) o correo Web, sería necesario tener acceso a Internet para poder usar el correo.
- **Ofimática y aplicaciones de usuario.** Se ha instalado el Sistema Operativo Linux Ubuntu en cada una de las computadoras. Para las aplicaciones de ofimática se cuenta con la aplicación OpenOffice. De manera adicional se ha instalado en cada establecimiento una impresora con la que poder imprimir documentos e informes.
- **Comunicación de voz mediante telefonía IP (VoIP).** Se ha diseñado un sistema de VoIP basado en Asterisk, una centralita de software abierto. Este sistema de VoIP proporciona un servicio de comunicación de voz entre 13 establecimientos de salud. Todos tienen la posibilidad de realizar llamadas entre ellos y además de poder hacer llamadas al exterior (telefonía pública) a través de tarjetas prepago y recibir llamadas del exterior. Se brinda la posibilidad de servicios adicionales como voicemail y conferencia. La arquitectura de telefonía IP de la red Wi-Fi de Cusco está formada por dos elementos: servidores Asterisk y teléfonos IP; el servidor Asterisk administra los teléfonos IP. Se han instalado cinco servidores Asterisk para administrar 13 teléfonos. El servidor principal está ubicado en el servidor del Hospital de Cusco, mientras que los otros servidores son secundarios y están instalados en los nodos repetidores (en placas Soekris net4521): Josjojahuarina1, Laykatuyoc y Huascar. Cada uno de estos servidores es responsable de las llamadas de una cierta parte de la red. La primera idea fue instalar un único servidor en Cusco. Pero en caso de que algunos puntos de la red perdieran su conectividad con Cusco no se podrían seguir realizando llamadas hasta que la red fuera restablecida de nuevo. Debido a eso se decidió seguir un sistema basado en múltiples servidores.

  En cuanto a los teléfonos IP utilizados por los establecimientos de salud de esta red se trata de teléfonos analógicos a los que se les ha añadido un

ATA (Adaptador para teléfonos analógicos). Se decidió optar por este esquema para que en caso de avería los teléfonos pudieran ser más fácilmente sustituibles.

Servicios y Procesos de Gestión en Salud

En cuanto a las herramientas y servicios brindados han sido:

- Plataforma de edición de cursos.
- Plataforma de educación a distancia.
- Sistema de gestión de información epidemiológica.
- Material docente para personal de salud rural.
- Cursos a distancia para personal de salud rural.

Así mismo se ha apoyado a los sistemas locales de salud en el aprovechamiento de los sistemas y servicios instalados para mejorar algunos de sus procesos de gestión en salud: gestión de emergencias, segunda opinión, gestión de información de stock de farmacia, dispensarización de la población y referencia-contrarreferencia de pacientes.

Usos futuros

El personal médico y gerencial de los establecimientos de salud, a partir de su propia experiencia con los sistemas de comunicación EHAS, ha ido generando nuevos usos espontáneos de la red. Entre otros se destacan el seguimiento de pacientes contrarreferidos desde el Hospital Regional de Cusco, la realización de los petitorios de farmacia o el envío de requerimientos de almacén. Además en la actualidad se está trabajando en la instalación de equipos que permitan añadir nuevos servicios a la red: electrocardiografos digitales, escáner, webcam y cámara digital. Estos elementos permitirán ayudar principalmente tanto en la consulta remota de pacientes como en el diagnóstico remoto de enfermedades.

ADMINISTRACIÓN Y MANTENIMIENTO

Administración: Sistema de Gestión de Red

Las primeras redes de comunicaciones que EHAS desplegó en zonas rurales aisladas carecían de un sistema de gestión de red. Como consecuencia directa, en ocasiones pasaban semanas e incluso meses hasta que el administrador local de la red era consciente de que se había producido una falla en algún punto. Para corregir esta problemática, en la red de Cusco se desarrolló un Sistema de Gestión propio que permitiera monitorizar la red de comunicaciones, de manera que se pudiera conocer con detalle la disponibilidad y estado en tiempo real de los nodos, así como prevenir posibles problemas o averías con la antelación suficiente. La

información que se quiere monitorizar de cada nodo de la red es generada y recogida por el propio nodo de manera local, dando lugar a una serie de logs que son enviados a un nodo gestor (situado en el Hospital de Cusco) a través del correo electrónico. El nodo gestor procesa la información que recibe de cada nodo de la red y la presenta al administrador local en forma de interfaz Web a través de la aplicación Zabbix. Esta aplicación cuenta con funcionalidades como mapas con el estado de los nodos de la red, servicio de alarmas y envío de alertas a los administradores de la red, estadísticas con variables locales a cada nodo (nivel de la señal Wi-Fi de los enlaces, estado de la batería del subsistema solar, estado de la memoria, etc). Varios problemas que han ido surgiendo en la red (desalineamiento de las antenas, falla en la batería de algún repetidor) han podido ser monitorizados y subsanados de manera eficiente gracias al empleo de este Sistema de Gestión de Red.

Mantenimiento

El adecuado mantenimiento de los Sistemas EHAS requiere que algunos miembros del Ministerio de Salud adquieran las competencias necesarias para resolver los posibles problemas y fallas que se puedan presentar en la Red, así como efectuar las tareas básicas de mantenimiento preventivo programadas. En este sentido, se vio indispensable la realización de cursos presenciales de capacitación técnica que permitieran la asimilación de los conocimientos requeridos. Este cursos perseguían como objetivos especificos:

1. Dar a conocer las características técnicas básicas de los Sistemas radio instalados en el marco del Proyecto EHAS - @LIS.
2. Promover la identificación del personal sanitario con el uso y cuidado de los componentes de la Red EHAS.
3. Conocimiento y compresión, de parte de los técnicos de apoyo designados en cada micro red, de los componentes y sub sistemas que componen a los Sistemas de Comunicaciones instalados, así como de los principios de funcionamiento, procedimientos y actividades de mantenimiento preventivo de los Sistemas EHAS.
4. Conocimiento y compresión, de parte de los técnicos especialistas de la Red de Salud del funcionamiento, configuración, procedimientos y actividades de mantenimiento preventivo y correctivo de los Sistemas EHAS.

Las sesiones fueron teórico-prácticas y como refuerzo al aprendizaje en aula, se realizaron visitas técnicas a instalaciones de Sistemas clientes y a repetidores, realizándose pruebas de implementación de un enlace en la red troncal.

Con el fin de certificar las competencias adquiridas se realizó un proceso de evaluación al finalizar cada curso en el cual se evaluó tanto el grado de asimilación y comprensión de los conceptos como la capacidad de resolver problemas prácticos que son típicos en el mantenimiento.

En cuanto a las responsabilidades generadas por la Red, corresponde a los Jefes de los Centros de Salud el hacer cumplir las tareas básicas de mantenimiento a los técnicos capacitados en cada micro red y definidas en los manuales correspondientes. La Red de Servicios Cusco Sur tiene la responsabilidad de supervisar y registrar todas las actividades de mantenimiento, así como de organizar y ejecutar las de mayor complejidad. También es responsabilidad de la Red asegurar la previsión de los gastos dentro del Presupuesto Anual de la institución beneficiaria. En relación al mantenimiento correctivo (reporte y detección de averías) de la Red EHAS instalada, la institución beneficiaria asume el compromiso de planificar y gestionar, dentro de sus procedimientos formales, las actividades necesarias para este fin.

Sostenibilidad

El objetivo principal de las actividades de mantenimiento es garantizar la sostenibilidad de la Red de Comunicaciones instalada en Cusco. Sin embargo, un efectivo mantenimiento no es la única estrategia que puede implementarse para este fin, siendo conveniente y hasta necesario complementar estas actividades con la formación de un contexto favorable en el ámbito institucional y a nivel local, con el fin de involucrar a los beneficiarios directos y a otros actores que podrían colaborar o participar en los procesos iniciados.

- **Convenios**: Se ha propuesto la formalización de adendas a los convenios bipartitos de colaboración existentes entre la DISA Cusco y la Universidad Nacional San Antonio Abad de Cusco (UNSAAC), y entre esta última y la Pontificia Universidad Católica del Perú, con el fin de asegurar que el soporte tecnológico y de recursos humanos especializados se encuentre siempre disponible ante las necesidades de los beneficiarios, tanto en temas de mantenimiento correctivo como en la implementación de nuevos servicios sobre la infraestructura existente.
- **Financiamiento**: La piedra angular de todo esfuerzo para lograr la sostenibilidad de un proyecto es la existencia de financiamiento para la ejecución de las actividades propuestas en el mismo. En este aspecto desde la planificación del Proyecto se estableció como una meta fundamental la inserción de los costos asociados al mantenimiento de la Red dentro del presupuesto oficial elaborado por la Red de Servicios Cusco Sur. Como resultado de estas gestiones la DISA Cusco ha aprobado la ampliación del presupuesto asignado en la partida mantenimiento de la Red Sur en forma global, considerando de esta

manera los nuevos gastos a generarse debido al mantenimiento de la Red EHAS instalada.

ENTRENAMIENTO Y CAPACITACIÓN

Se establece como un requisito para la operación de los Sistemas EHAS que el personal encargado haya sido capacitado previamente en esta actividad. Los cursos de capacitación de usuarios han sido realizados durante el periodo de ejecución del proyecto. Sin embargo, en caso se efectúen rotaciones de personal o contrataciones nuevas, la Unidad de Estadística de la Red Cusco Sur se encargará de efectuar una primera inducción a los nuevos usuarios, la que debe ser reforzada luego por el jefe del establecimiento de salud o el funcionario que haya sido directamente capacitado.

La capacitación de los usuarios, a partir de manuales confeccionados por nuestro equipo, se ha centrado principalmente en el manejo general del ordenador y de un paquete básico de programas ofimáticos (procesador de textos, hoja de cálculo, etc.). También se ha impartido formación en el manejo del resto de equipos: impresora, teléfono de VoIP, etc. Además, la capacitación ha incluido mantenimiento preventivo de los equipos.

El proceso de formación informática suele tener dos momentos claros: la capacitación y el autoaprendizaje a través del uso. Durante esa segunda fase de autoaprendizaje el usuario afianza sus conocimientos a través de la exploración de las posibilidades del computador. Los usuarios del proyecto se encuentran en zonas muy aisladas donde lo normal es que no haya personas que sepan manejar el computador y por tanto, donde es difícil encontrar personas que puedan apoyarlas en caso de dudas. De las declaraciones en entrevistas y talleres se ha comprobado que en muchos casos el personal de salud no cuenta con mucho tiempo para utilizar el computador. Estos dos factores contribuyen a que sea más lenta la segunda fase de autoaprendizaje. Es por esta razón que se hace más importante asegurar una sólida formación de la que se ha recibido con una mirada hacia el futuro.

Desde el punto de vista de los usuarios las capacitaciones suponen un elemento de importante motivación laboral y han resultado muy satisfactorias en contenido y metodología. Según el Dr. Carlos Vega, Director de Servicios de la DIRESA Cusco "*La idea de adquirir capacitación por medio del computador motiva de manera especial al personal de salud*".

EVALUACIÓN DEL PROYECTO

Las redes han demostrado tener una buena fiabilidad, sobre todo si se tiene en cuenta el entorno rural en el que se encuentran, con dificultades de acceso y con escasez de infraestructuras de todo tipo. La principal causa de pérdida de servicio en todos los casos han sido caída de rayos y descargas eléctricas. En las redes WiFi el servicio de correo electrónico e Internet ha demostrado ser bastante robusto, pero el de telefonía presenta aún algunas dificultades que están siendo subsanadas por nuestro equipo con el uso de una arquitectura de QoS que permita priorizar las comunicaciones de voz sobre las de datos.

Los usuarios consideran que los sistemas son fáciles de usar. Si se desagrega por sistemas, estiman que el sistema más fácil de usar es el de VoIP, después el ordenador y finalmente Internet. Se ha identificado la preferencia por el uso de sistemas de VoIP para las comunicaciones locales con otros establecimientos de salud y con la autoridad local, mientras que el Internet es un recurso que se emplea para las comunicaciones hacia el exterior.

Las mejoras en la gestión de salud y la capacidad resolutiva de los centros y establecimientos de salud se refleja en los cambios surgidos en la gestión de urgencias con la aplicación de las nuevas tecnologías, el incremento y mejora de la solicitud de segunda opinión por parte del personal de periferia hacia profesionales de mayor experiencia, intercambio de información por escrito y envío de información de índole administrativa por correo electrónico, sin embargo una de las dificultades que se han identificado es la necesidad de que vayan firmados por el emisor.

Desde los puestos de salud, se realizaron más de 700 inter-consultas sobre dudas diagnósticas de tratamiento que fueron contestadas inmediatamente por los médicos de los centros de referencia. Lo cual ha tenido un impacto en los números de traslado de pacientes. En los casos en que el traslado no pudo evitarse, se logró reducir en 40% tiempo de traslado de los pacientes debido a una mejor coordinación. Además se ha logrado reducir el número de viajes para la entrega de informes, que se redujo a la cuarta parte solamente en el primer año de uso.

Las actividades de comunicación se realizan manera diaria, y así muchas otras actividades comunes de los establecimientos de salud se hacen de manera coordinada y sinérgica. La comunicación entre el personal de la microrred es diaria, con lo cual se ha vencido la sensación de aislamiento profesional y personal de los trabajadores del sistema de salud y los miembros de la comunidad.

Por otro lado, el sistema de comunicación del proyecto ha facilitado que las dudas de carácter administrativo sean dirigidas a la Red de Salud en lugar de a los Centros de atención primaria. Por tanto, el proyecto ha contribuido

además con facilitar la formulación de consultas sobre temas administrativos a la fuente correspondiente.

Finalmente, también consideramos en este apartado como usuarios a personas no vinculadas a salud: principalmente del gobierno local y educación, que utilizan el computador principalmente como herramienta de trabajo y del acceso a Internet aún cuando la demanda de éste grupo es, de hecho, poco frecuente.

REPETIDORES

HOSPITAL CUSCO. De izquierda a derecha y arriba abajo: Antena directiva de 19dBi apuntando a la Red Sur, Antenas montadas en tejado, Caja de equipos montada en el interior del tejado y antena directiva de 24dBi apuntada al repetidor Josjojahuarina1.

JOSJOJAHUARINA1. De izquierda a derecha y arriba abajo: Antenas y paneles solares montados en torre ventada de 12 metros, Equipos de telecomunicaciones y proteccion electrica en caja metalica, Caja metalica de bateria, Paneles solares montados en la torre ventada.

ESTACIONES CLIENTE

URCOS. De izquierda a derecha: Antena directiva de 24dBi montada en poste de 6 metros, Estación de cómputo y equipo de telecomunicaciones en Urcos

KCAURY. De izquierda a derecha: Antena directiva de 24dBi montada en brazo mecánico y Estación de cómputo y caja de equipos de telecomunicaciones.

ACOPIA. De izquierda a derecha: Estación de cómputo y caja de equipo de telecomunicaciones, Antena de 24dBi montada en poste de 6 metros y Caja de equipo de telecomunicaciones.

CRÉDITOS

- Fundación Enlace Hispanoamericano de Salud (EHAS)
- Universidad Politécnica de Madrid (UPM)
- Ingeniería sin Fronteras (ISF)
- Pontificia Universidad Católica del Perú (PUCP)
- Universidad Peruana Cayetano Heredia (UPCH)
- Programa @LIS de la Unión Europea

Apéndice A: Recursos

Recomendamos estos recursos para que quienes lo deseen, puedan aprender más acerca de los variados aspectos de las redes inalámbricas (los mismos están disponibles solamente en inglés). Si quiere conocer más enlaces y recursos, visite nuestro sitio web en *http://wndw.net/.*

Antenas y diseño de antenas

- Cushcraft technical papers on antenna design and radio propagation, *http://www.cushcraft.com/comm/support/technical-papers.htm*
- Free antenna designs, *http://www.freeantennas.com/*
- Hyperlink Tech, *http://hyperlinktech.com/*
- Pasadena Networks LLC, *http://www.wlanparts.com/*
- SuperPass, *http://www.superpass.com/*
- Unofficial NEC-2 code archives, *http://www.si-list.org/swindex2.html*
- Unofficial NEC-2 radio modeling tool home page, *http://www.nittany-scientific.com/nec/*
- USB WiFi dish designs, *http://www.usbwifi.orcon.net.nz/*

Herramientas para la resolución de problemas de redes

- Cacti network monitoring package, *http://www.cacti.net/*
- DSL Reports bandwidth speed tests, *http://www.dslreports.com/stest*
- Ethereal network protocol analyzer, *http://www.ethereal.com/*
- Iperf network performance testing tool, *http://dast.nlanr.net/Projects/Iperf/*
- iptraf network diagnostic tool, *http://iptraf.seul.org/*
- MRTG network monitoring and graphing tool, *http://people.ee.ethz.ch/~oetiker/webtools/mrtg/*
- My TraceRoute network diagnostic tool, *http://www.bitwizard.nl/mtr/*

- Nagios network monitoring and event notification tool, *http://www.nagios.org/*
- Ntop network monitoring tool, *http://www.ntop.org/*
- RRDtool round robin database graphing utility, *http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/*
- SmokePing network latency and packet loss monitor, *http://people.ee.ethz.ch/~oetiker/webtools/smokeping/*
- SoftPerfect network analysis tools, *http://www.softperfect.com/*
- Squid transparent http proxy HOWTO, *http://en.tldp.org/HOWTO/mini/TransparentProxy-2.html*
- ttcp network performance testing tool, *http://ftp.arl.mil/ftp/pub/ttcp/*

Seguridad

- AntiProxy http proxy circumvention tools and information, *http://www.antiproxy.com/*
- Anti-spyware tools, *http://www.spychecker.com/*
- Driftnet network monitoring utility *http://www.ex-parrot.com/~chris/driftnet/*
- Etherpeg network monitoring utility, *http://www.etherpeg.org/*
- Introduction to OpenVPN, *http://www.linuxjournal.com/article/7949*
- Lavasoft Ad-Aware spyware removal tool, *http://www.lavasoft.de/*
- OpenSSH secure shell and tunneling tool, *http://openssh.org/*
- OpenVPN encrypted tunnel setup guide, *http://openvpn.net/howto.html*
- Privoxy filtering web proxy, *http://www.privoxy.org/*
- PuTTY SSH client for Windows, *http://www.putty.nl/*
- Sawmill log analyzer, *http://www.sawmill.net/*
- Security of the WEP algorithm, *http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html*
- Spyware prevention for Windows XP (German), *http://www.xp-antispy.de/*
- Stunnel Universal SSL Wrapper, *http://www.stunnel.org/*
- TOR onion router, *http://tor.eff.org/*
- Weaknesses in the Key Scheduling Algorithm of RC4, *http://www.crypto.com/papers/others/rc4_ksaproc.ps*
- Windows SCP client, *http://winscp.net/*

- Your 802.11 Wireless Network has No Clothes, *http://www.cs.umd.edu/~waa/wireless.pdf*
- ZoneAlarm personal firewall for Windows, *http://www.zonelabs.com/*

Optimización del ancho de banda

- Cache hierarchies with Squid, *http://squid-docs.sourceforge.net/latest/html/c2075.html*
- dnsmasq caching DNS and DHCP server, *http://thekelleys.org.uk/dnsmasq/doc.html*
- Enhancing International World Wide Web Access in Mozambique Through the Use of Mirroring and Caching Proxies, *http://www.isoc.org/inet97/ans97/cloet.htm*
- Fluff file distribution utility, *http://www.bristol.ac.uk/fluff/*
- Microsoft Internet Security and Acceleration Server, *http://www.microsoft.com/isaserver/*
- Microsoft ISA Server Firewall and Cache, *http://www.isaserver.org/*
- Pittsburgh Supercomputing Center's guide to Enabling High Performance Data Transfers, *http://www.psc.edu/networking/perf_tune.html*
- RFC 3135: Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations, *http://www.ietf.org/rfc/rfc3135*
- Squid web proxy cache, *http://squid-cache.org/*

Redes mesh

- Champaign-Urbana Community Wireless Network software, *http://cuwireless.net/download*
- Freifunk OLSR mesh firmware for the Linksys WRT54G, *http://www.freifunk.net/wiki/FreifunkFirmware*
- MIT Roofnet Project, *http://pdos.csail.mit.edu/roofnet/doku.php*
- OLSR mesh networking daemon, *http://www.olsr.org/*
- Real-time OLSR topology viewer, *http://meshcube.org/nylon/utils/olsr-topology-view.pl*

Sistemas operativos y manejadores

- HostAP wireless driver for the Prism 2.5 chipset, *http://hostap.epitest.fi/*
- m0n0wall wireless router OS, *http://m0n0.ch/wall/*
- MadWiFi wireless driver for the Atheros chipset, *http://madwifi.org/*

- Metrix Pebble wireless router OS, *http://metrix.net/metrix/howto/metrix-pebble.html*
- OpenWRT wireless router OS for Linksys access points, *http://openwrt.org/*
- Pebble Linux, *http://nycwireless.net/pebble/*

Herramientas inalámbricas

- Chillispot captive portal, *http://www.chillispot.org/*
- Interactive Wireless Network Design Analysis Utilities, *http://www.qsl.net/n9zia/wireless/page09.html*
- KisMAC wireless monitor for Mac OS X, *http://kismac.binaervarianz.de/*
- Kismet wireless network monitoring tool, *http://www.kismetwireless.net/*
- MacStumbler wireless network detection tool for Mac OS X, *http://www.macstumbler.com/*
- NetStumbler wireless network detection tool for Windows and Pocket PC, *http://www.netstumbler.com/*
- NoCatSplash captive portal, *http://nocat.net/download/NoCatSplash/*
- PHPMyPrePaid prepaid ticketing system, *http://sourceforge.net/projects/phpmyprepaid/*
- RadioMobile radio performance modeling tool, *http://www.cplus.org/rmw/*
- Terabeam wireless link calculation tools, *http://www.terabeam.com/support/calculations/index.php*
- Wellenreiter wireless network detection tool for Linux, *http://www.wellenreiter.net/*
- WiFiDog captive portal, *http://www.wifidog.org/*
- Wireless Network Link Analysis tool by GBPRR, *http://my.athenet.net/~multiplx/cgi-bin/wireless.main.cgi*

Información general relacionada a redes inalámbricas

- DefCon long distance WiFi shootout, *http://www.wifi-shootout.com/*
- Homebrew wireless hardware designs, *http://www.w1ghz.org/*
- Linksys wireless access point information*, http://linksysinfo.org/*
- Linksys WRT54G resource guide, http://seattlewireless.net/index.cgi/LinksysWrt54g
- NoCat community wireless group, *http://nocat.net/*

- POE guide by NYCWireless, *http://nycwireless.net/poe/*
- Ronja optical data link hardware, *http://ronja.twibright.com/*
- SeattleWireless community wireless group, *http://seattlewireless.net/*
- SeattleWireless Hardware comparison page, *http://www.seattlewireless.net/HardwareComparison*
- Stephen Foskett's Power Over Ethernet (PoE) Calculator, *http://www.gweep.net/~sfoskett/tech/poecalc.html*

Vendedores de equipamiento de redes

- Alvarion wireless networking equipment, *http://www.alvarion.com/*
- Cisco wireless networking equipment, *http://www.cisco.com/*
- Metrix outdoor wireless networking kits, *http://metrix.net/*
- Mikrotik wireless network equipment, *http://www.mikrotik.com/routers.php#linx1part0*
- PowerNOC outdoor wireless networking equipment, *http://powernoc.us/outdoor_bridge.html*
- RAD Data Communications networking hardware, *http://www.rad.com/*
- Redline Communications WiMax wireless networking equipment, *http://www.redlinecommunications.com/*
- Trango wireless networking hardware, *http://www.trangobroadband.com/*
- WaveRider wireless hardware, *http://www.waverider.com/*

Servicios de redes

- Access Kenya ISP, *http://www.accesskenya.com/*
- Broadband Access Ltd. wireless broadband carrier, *http://www.blue.co.ke/*
- Virtual IT outsourcing, http://www.virtualit.biz/
- wire.less.dk consultancy and services, *http://wire.less.dk/*

Entrenamiento y educación

- Association for Progressive Communications wireless connectivity projects, *http://www.apc.org/wireless/*
- International Network for the Availability of Scientific Publications, *http://www.inasp.info/*
- Makere University, Uganda, *http://www.makerere.ac.ug/*

- Radio Communications Unit of the Abdus Salam International Center for Theoretical Physics, *http://wireless.ictp.trieste.it/*
- World Summits on Free Information Infrastructures, *http://www.wsfii.org/*

Miscelánea de enlaces

- Cygwin Linux-like environment for Windows, *http://www.cygwin.com/*
- Graphvis graph visualization tool, *http://www.graphviz.org/*
- ICTP bandwidth simulator, *http://wireless.ictp.trieste.it/simulator/*
- NodeDB war driving map database, *http://www.nodedb.com/*
- Open Relay DataBase, *http://www.ordb.org/*
- Partition Image disk utility for Linux, *http://www.partimage.org/*
- RFC 1918: Address Allocation for Private Internets, *http://www.ietf.org/rfc/rfc1918*
- Ubuntu Linux, *http://www.ubuntu.com/*
- wget web utility for Windows, *http://xoomer.virgilio.it/hherold/*
- WiFiMaps war driving map database, *http://www.wifimaps.com/*

Books

- *802.11 Networks: The Definitive Guide, 2nd Edition*. Matthew Gast, O'Reilly Media. ISBN #0-596-10052-3
- *802.11 Wireless Network Site Surveying and Installation.* Bruce Alexander, Cisco Press. ISBN #1-587-05164-8
- The *ARRL Antenna Book, 20th Edition.* R. Dean Straw (Editor), American Radio Relay League*.* ISBN #0-87259-904-3
- The *ARRL UHF/Microwave Experimenter's Manual*. American Radio Relay League*.* ISBN #0-87259-312-6
- *Building Wireless Community Networks, 2nd Edition.* Rob Flickenger, O'Reilly Media. ISBN #0-596-00502-4
- *Deploying License-Free Wireless Wide-Area Networks.* Jack Unger, Cisco Press. ISBN #1-587-05069-2
- TCP/IP Illustrated, Volume 1. W. Richard Stevens, Addison-Wesley. ISBN #0-201-63346-9
- *Wireless Hacks, 2nd Edition*. Rob Flickenger and Roger Weeks, O'Reilly Media. ISBN #0-596-10144-9

Apéndice B: Asignación de Canales

Las siguientes tablas listan los números de los canales y frecuencias centrales utilizadas para 802.11a y 802.11b/g. Si bien todas estas frecuencias están en las bandas sin licenciamiento ISM y U-NII, no todos los canales están disponibles en los diferentes países. Muchas regiones imponen restricciones en la potencia de salida y el en uso interno / externo de algunos canales. Esas regulaciones cambian rápidamente, por lo tanto revise las regulaciones locales antes de transmitir.

Estas tablas le muestran la frecuencia central de cada canal. Los canales son de un ancho de 22MHz en 802.11b/g, y de 20MHz en 802.11a.

802.11b / g			
Canal #	Frecuencia Central (GHz)	Canal #	Frecuencia Central (GHz)
1	2,412	8	2,447
2	2,417	9	2,452
3	2,422	10	2,457
4	2,427	11	2,462
5	2,432	12	2,467
6	2,437	13	2,472
7	2,442	14	2,484

802.11a	
Canal #	Frecuencia Central (GHz)
34	5,170
36	5,180
38	5,190
40	5,200
42	5,210
44	5,220
46	5,230
48	5,240
52	5,260
56	5,280
60	5,300
64	5,320
149	5,745
153	5,765
157	5,785
161	5,805