Redes Inalámbricas en los Países en Desarrollo

Tercera Edición

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
Tercera edición, septiembre de 2008

ISBN: 978-0-9778093-7-0

Tabla de Contenido

Sobre este Libro

Este libro es parte de un conjunto de materiales sobre el mismo tema: Redes Inalámbricas en los Países en Desarrollo (Wireless Networking in the Developing World: WNDW). El proyecto WNDW incluye:

- Libros impresos
- Traducciones al español, francés, italiano, portugués, árabe, entre otras.
- Una versión electrónica gratuita del texto en formatos PDF y HTML 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/*

El sitio Web incluye más casos de estudio, referencias a páginas externas, así como actualizaciones del equipamiento. Aquellos voluntarios que quieran

aportar ideas son bienvenidos. Por favor suscríbanse a la lista de correo electrónico y envíen 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. Hay también material adicional adaptado de How to Accelerate Your Internet, *http://www.bwmo.net/*

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. Añada su propia contribución y actualizaciones en el wiki de WNDW: *http://www.wndw.net/*

Grupo Central

- **Rob Flickenger** fue el autor principal, editor e ilustrador de este libro. Escribió y editó varios libros sobre redes inalámbricas y Linux, incluyendo, Building Wireless Community Networks y Wireless Hacks (O'Reilly Media) de los cuales existen las versiones en español. Está orgulloso de sus condiciones de hacker, científico aficionado, y propulsor de redes libres en todas partes.
- **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*
- **Sebastián Büttrich** *(http://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. Es 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. Es también músico con varias grabaciones en su haber.

- **Laura M. Drewett** es Co-fundadora de Adapted Consulting Inc., una empresa social que se especializa en adaptar tecnología y soluciones comerciales para el mundo en desarrollo. Como Laura vivió en Mali en los 90, y escribió su tesis sobre programas de educación para niñas, se ha esforzado en encontrar soluciones sostenibles para el desarrollo. Como experta en sostenibilidad para proyectos de TIC en los países en desarrollo, ha diseñado y dirigido proyectos para una diversidad de clientes en África, Medio Oriente, y Europa oriental. Tiene una Licenciatura en Arte con mención en Relaciones Exteriores y Francés de la Universidad de Virginia, y un Certificado de Maestría en Gerencia de Proyectos de la George Washington University School of Business.
- **Alberto Escudero-Pascual** y **Louise Berthilson** son los fundadores de IT +46, una compañía consultora sueca especializada en tecnología de la información en países en desarrollo. IT+46 es conocida internacionalmente por impulsar e implementar infraestructura inalámbrica de Internet en zonas rurales de África y América Latina. Desde 2004, la compañía ha entrenado a más de 350 personas en 14 países y liberado más de 600 páginas bajo Creative Commons License. Más información en *http://www.it46.se/*
- **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 principalmente 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 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.
- **Kyle Johnston,** *http://www.schoolnet.na/*

- **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://www.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 dedicadas 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.

- **Gina Kupfermann,** es ingeniera graduada en gerencia de energía y en Ingeniería y Administración. Aparte de su profesión como contralora de finanzas, ha trabajado para varios proyectos comunitarios auto-organizados y organizaciones sin fines de lucro. Desde 2005 es miembro de la junta ejecutiva de la asociación de desarrollo para las redes libres, la entidad legal de freifunk.net.

- **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 ISP (Proveedores de Servicios de Internet) de África. Como 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.

- **Juergen Neumann** *(http://www.ergomedia.de/)* comenzó a trabajar con tecnologías de la información en 1984, y desde entonces ha estado en busca de maneras de implementar redes de TIC que sean útiles a las organizaciones y a la sociedad. Como consultor de estrategias e implementación de TIC ha trabajado para importantes compañías en Alemania y proyectos sin fines de lucro. En 2002 fue co-fundador de *www.freifunk.net*, una campaña para difundir conocimiento y redes sociales sobre redes libres y abiertas. Freifunk es considerada globalmente como uno de los proyectos comunitarios más exitosos en este campo.

- **Ermanno Pietrosemoli** tiene un MSc en telecomunicaciones de la Universidad de Stanford. Ha estado involucrado en la planificación y construcción de redes de computadoras durante los últimos veinte años, primero en la universidad de los Andes, donde es profesor de telecomunicaciones desde 1970 y luego, en su calidad de presidente de la Fundación Escuela Latinoamericana de Redes ("EsLaRed"

www.eslared.org.ve) y consultor, ha expandido sus actividades para incluir la planificación, diseño e instalación de redes de transmisión de datos en Argentina, Colombia, Ecuador, Italia, Nicaragua, Perú, Uruguay, Trinidad y Venezuela manteniendo su base en Mérida, Venezuela. Ha dictado cursos de redes inalámbricas también en Brasil, India, Kenya, México y República Dominicana. Desde 1996 colabora con el ICTP de Trieste en las actividades de formación y desarrollo en redes inalámbricas que realiza esta institución con el apoyo de la UIT. Esta fructífera colaboración condujo a demostrar la factibilidad de enlaces WiFi a 279 km de distancia en 2006 y a 382 km en 2007.

- **Frédéric Renet** es uno de los co-fundadores de Soluciones Técnicas de Adapted Consulting, Inc. Frédéric se ha involucrado por más de 10 años en TIC y ha trabajado con computadores desde su infancia. Inició su carrera en TIC a comienzo de los 90 con un bulletin board system (BBS) que usaba módems analógicos, y desde entonces ha continuado creando sistemas que mejoran la comunicación. Recientemente, Frédéric pasó más de un año en IESC/Geekcorps, Mali, como consultor. En este cargo desarrolló muchas soluciones innovadoras para transmisión de radio FM, laboratorios escolares de comunicación y sistemas de iluminación para comunidades rurales.
- **Marco Zennaro,** también conocido como marcusgennaroz, es un ingeniero electrónico que trabaja en el ICTP en Trieste, Italia. Un radioaficionado que ha estado utilizando BBS y radios de comunicaciones 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.

Brindaron su Apoyo

- **Lisa Chan** *(http://www.cowinanorange.com/)* fue la editora principal.
- **Casey Halverson** *(http://seattlewireless.net/~casey/)* realizó revisiones técnicas y sugerencias.
- **Jessie Heaven Lotz** *(http://jessieheavenlotz.com/)* proporcionó varias ilustraciones actualizadas para esta edición.
- **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.
- **Catherine Sharp** *(http://odessablue.com/)* colaboró en la edición.
- **Lara Sobel** (*lara@hackerfriendly.com*) diseñó la cubierta de la segunda edición de WNDW, y realizó la cubierta y la diagramación de la tercera edición en español.

- **Matt Westervelt** *(http://seattlewireless.net/~mattw/)* realizó revisiones técnicas y colaboró en la edición. Es el fundador de *SeattleWireless (http://seattlewireless.net)*, y un apóstol de FreeNetworks por todo el mundo.

La traducción de esta tercera edición en español fue realizada por Lourdes G. de Pietrosemoli, profesora de la Universidad de Los Andes, y la revisión técnica, por Ermanno Pietrosemoli.

Acerca de Voz sobre IP

Por favor, note que el capítulo Voz sobre IP (Capítulo 9 en versión previa) no aparece en esta edición, pero puede consultarlo en línea en: *http://wndw.net/*

Acerca de la guía de energía solar

El material de base para el capítulo de Energía Solar fue desarrollado por Alberto Escudero-Pascual. En 1998, la organización Ingenieros sin Fronteras (Federación Española) publicó la primera edición de un manual titulado “Manual de Energía Solar Fotovoltaica y Cooperación al Desarrollo”. El manual fue escrito y publicado por miembros de la ONG y expertos del Instituto de Energía Solar de la Universidad Politécnica de Madrid. Por azares de la vida, ninguno de los miembros del equipo editorial conservó una versión electrónica del documento por lo que no fueron hechas más ediciones. Han pasado casi diez años desde esa primera edición, y este documento es un esfuerzo para rescatar y expandir el manual.

Como parte de esa operación de rescate, Alberto quisiera agradecer a los coordinadores de la edición original y los tutores de sus años universitarios: Miguel Ángel Eguido Aguilera, Mercedes Montero Bartolomé y Julio Amador. Este nuevo trabajo ha sido producido bajo la licencia Creative Commons ***Attribution-ShareAlike 3.0.*** Esperamos que este nuevo material sea un punto de partida para nuevas ediciones incluyendo nuevas contribuciones por parte de la comunidad.

La segunda edición ampliada de la guía de energía solar ha recibido un valioso apoyo de Fréderic Renet y Louise Berthilson.

Agradecimientos especiales

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 tiempo y energía para alcanzar la promesa de una Internet global. Sin ustedes, las redes comunitarias no podrían existir.

La publicación de este trabajo ha sido financiada por el International Development Research Centre, *http://www.idrc.ca/* de Canadá con ayuda adicional por parte de *NetworktheWorld.org.*

IDRC CRDI

ICTP The Abdus Salam International Centre for Theoretical Physics

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 en 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. Al involucrar 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 ayudarle a construir tecnologías de comunicación accesibles para su comunidad por medio del buen uso de todos los recursos disponibles. Utilizando equipo económico ampliamente disponible, es posible 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/la a usted y a sus vecinos a Internet. Utilizando materiales locales y fabricando partes usted mismo/a, se pueden armar enlaces de red confiables con muy poco presupuesto. Y al trabajar 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 computadora portátil o seleccionar los productos adecuados a la red de su hogar, sino que trata sobre el armado de infraestructuras de red para que sean utilizadas como dorsales de redes inalámbricas de amplio alcance. Con este objetivo en mente, la información se presenta desde varios puntos de vista, incluyendo factores técnicos, sociales y económicos. Los estudios de casos analizados muestran los intentos hechos por varios grupos para la instalación de esas redes, los recursos utilizados, y los resultados obtenidos en dichos intentos.

Desde los primeros experimentos de transmisión de chispas a fines del siglo antepasado, la tecnología inalámbrica ha sido un área que ha evolucionado rápidamente. Si bien en este libro proporcionamos ejemplos específicos de cómo construir enlaces de datos de alta velocidad, las técnicas descritas en el mismo no intentan reemplazar las infraestructuras de cableado existentes (tales como el sistema telefónico y las dorsales de 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.

Incorporar una red inalámbrica a una red preexistente

Si usted es el/la administrador/a 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 ampliación del alcance de una red Ethernet cableada a 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.

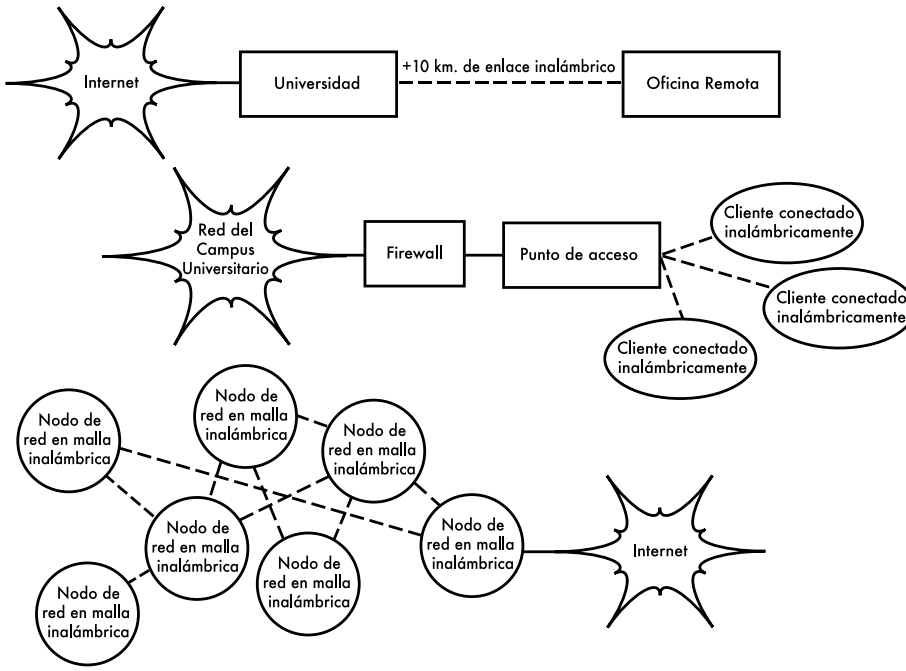


Figura 1.1: Algunos ejemplos de redes inalámbricas.

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, y 802.11g) ha adquirido gran popularidad en Estados Unidos y Europa. Mediante la implementación de un conjunto común de protocolos, los fabricantes de todo el mundo han producido equipos interoperables. Esta decisión ha demostrado ser de gran ayuda para la industria y los consumidores. Los consumidores pueden utilizar equipo que implementa el estándar 802.11 sin miedo a "quedar atrapado con el vendedor". Como resultado, pueden comprar

equipo 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 utilizan WiMAX apenas están entrando al mercado al momento en que se escribe este libro, nos vamos a concentrar 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 la IEEE el 16 de septiembre 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 11 Mbps, con una velocidad real de datos utilizable mayor a 5 Mbps.

- **802.11g.** Como no estuvo finalizado 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 en los radios incorporados en virtualmente todas las laptops y muchos de los dispositivos portátiles manuales (handheld). Utiliza el mismo rango ISM que el 802.11b, pero con el esquema de modulación denominado ***Multiplexaje por División de Frecuencias Ortogonales*** **–Orthogonal Frequency Division Multiplexing (OFDM)**. Tiene una tasa de transmisión máxima de 54 Mbps (con un caudal real de hasta 25 Mbps), y mantiene compatibilidad con el altamente popular 802.11b porque soporta también 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 caudal real (throughput) de hasta 27 Mbps. El 802.11a opera en la banda ISM entre 5725 y 5850 MHz, y en una porción de la banda UNII entre 5,15 y 5,35 GHz. Esto lo hace incompatible con el 802.11b o el 802.11g, y su frecuencia de transmisión más elevada implica un alcance menor comparado con el 802.11b/g al mismo nivel de potencia. Si bien esta porción del espectro es relativamente inutilizada comparada con la 2,4 GHz, 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 108 Mbps, mejor encriptación, y mayor rango. Desafortunadamente, esas extensiones no funcionan entre productos de diferentes fabricantes, y adquirirlos lo/la va a atar a un vendedor específico para la compra de cada parte de su red. 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, el tener un mejor rango, y la exención 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/a en el armado de redes inalámbricas seguramente tenga varias preguntas acerca de lo que la tecnología puede hacer, así como cuánto cuesta. Mencionamos a continuación 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? ***Página 209***

¿Debo colocar un cable eléctrico hasta la punta de la torre? ***Página 246***

¿Cómo puedo utilizar paneles solares para dar energía a mi nodo inalámbrico manteniéndolo activo durante la noche? ***Página 215***

¿Por cuánto tiempo va a funcionar mi punto de acceso (access point) con una batería? ***Página 235***

¿Puedo usar un generador eólico para darle energía a mi equipo en la noche? ***Página 210***

Administración

¿Cuánto ancho de banda necesito comprar para mis usuarios? ***Página 65***

¿Cómo puedo monitorear y gestionar puntos de acceso remotos desde mi oficina? ***Página 174***

¿Qué debo hacer cuando la red falla? ***Páginas 174, 263***

¿Cuáles son los problemas más comunes encontrados en las redes inalámbricas y cómo puedo solucionarlos? ***Página 263***

Distancia

¿Cuál es el alcance de mi punto de acceso? ***Página 68***

¿Existe alguna fórmula que me permita saber cuán lejos puedo llegar con un punto de acceso determinado? ***Página 68***

¿Cómo puedo saber si un lugar alejado puede ser conectado a Internet utilizando un enlace inalámbrico? ***Página 68***

¿Existe un software que me ayude a estimar la factibilidad de un enlace inalámbrico de larga distancia? ***Página 75***

El fabricante dice que mi punto de acceso tiene un rango de alcance de 300 metros. ¿Es eso cierto? ***Página 68***

¿Cómo puedo proveer de conectividad inalámbrica a muchos clientes remotos esparcidos alrededor de la ciudad? ***Página 53***

¿Es verdad que puedo aumentar el alcance utilizando una lata o añadiendo papel de aluminio a la antena de mi AP? ***Página 117***

¿Puedo utilizar una red inalámbrica para conectarme con un sitio remoto y compartir la misma conexión central a Internet? ***Página 52***

Parece que mis enlaces inalámbricos son demasiado largos para garantizar un buen funcionamiento. ¿Puedo colocar un repetidor en el medio para mejorarlos? ***Página 78***

¿Debería utilizar un amplificador? ***Página 115***

Instalación

¿Cómo puedo instalar mi AP para uso interior en un mástil externo sobre mi techo? ***Página 245***

¿Realmente es útil agregar un "protector de rayos" y una puesta a tierra al mástil de mi antena, o no es tan necesario? ***Página 260***

¿Puedo construir el mástil por mí mismo? ¿Cómo puedo hacerlo? ***Página 247***

¿Por qué mi antena funciona mucho mejor cuando la coloco en otra orientación? ***Página 12***

¿Qué canal debo utilizar? ***Página 15***

¿Las ondas de radio atraviesan edificios y árboles? ¿Qué pasa con las personas? ***Página 15***

¿Las ondas de radio atraviesan una colina que esté en el camino? ***Página 17***

¿Cómo construyo una red en malla? ***Página 56***

¿Qué tipo de antena es la mejor para mi red? ***Página 102***

¿Puedo construir un punto de acceso utilizando un PC reciclado? ***Página 145***

¿Cómo puedo instalar Linux en mi AP? ¿Por qué debería hacerlo? ***Página 153***

Dinero

¿Cómo puedo saber si un enlace inalámbrico puede obtenerse con una cantidad limitada de dinero? ***Página 277***

¿Cuál es el mejor AP por el menor precio? ***Página 139***

¿Cómo puedo monitorear y cobrar a los clientes por el uso de mi red inalámbrica? ***Páginas 165, 189***

Socios y Clientes

¿Si suministro la conexión, aún necesito el servicio de un ISP? ¿Por qué? ***Página 27***

¿Con cuántos clientes puedo cubrir mis costos? ***Página 283***

¿Cuántos clientes va a soportar mi red inalámbrica? ***Página 65***

¿Qué debo hacer para que mi red inalámbrica funcione más rápido? ***Página 80***

¿Es mi conexión a Internet tan rápida como pudiera serlo? ***Página 90***

Seguridad

¿Cómo puedo proteger mi red inalámbrica del acceso no autorizado? ***Página 157***

¿Es cierto que una red inalámbrica siempre es insegura y está abierta al ataque de piratas informáticos (hackers)? ***Página 160***

¿Es cierto que el uso de software libre hace que mi red sea menos segura? ***Página 167***

¿Cómo puedo ver qué está sucediendo en mi red? ***Página 174***

Información y Licencias

¿Qué otros libros puedo leer para mejorar mis conocimientos acerca de redes inalámbricas? ***Página 367***

¿Dónde puedo encontrar más información en línea? ***Página 361***

¿Puedo utilizar partes de este libro para mi propia práctica docente? ***Sí.***

¿Puedo imprimir y vender copias de este libro? ***Sí.*** *Para más detalles, vea la sección* ***Sobre este Libro.***

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/segundos, la frecuencia en ciclos por segundos (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.**

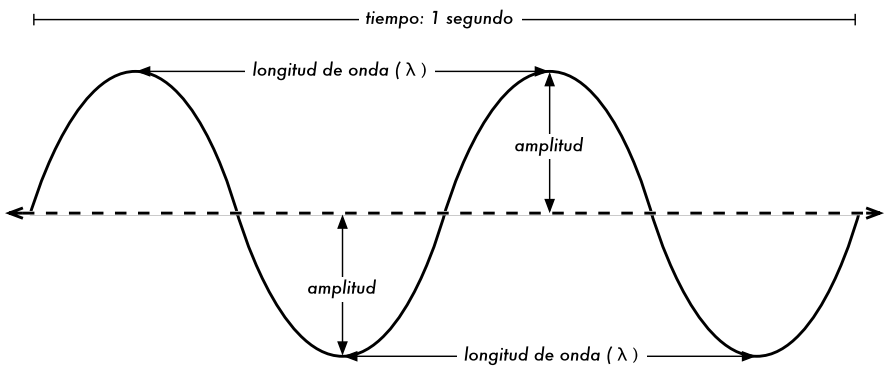


Figura 2.1: Longitud de onda, amplitud, y frecuencia.
En este caso la frecuencia es 2 ciclos por segundo, o 2 Hz.

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.

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, la velocidad **c** es la velocidad de la luz.

$$c = 300{,}000 \text{ km/s} = 300{,}000{,}000 \text{ m/s} = 3*10^8 \text{ m/s}$$
$$c = f * \lambda$$

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
Mili-	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 lambda (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.

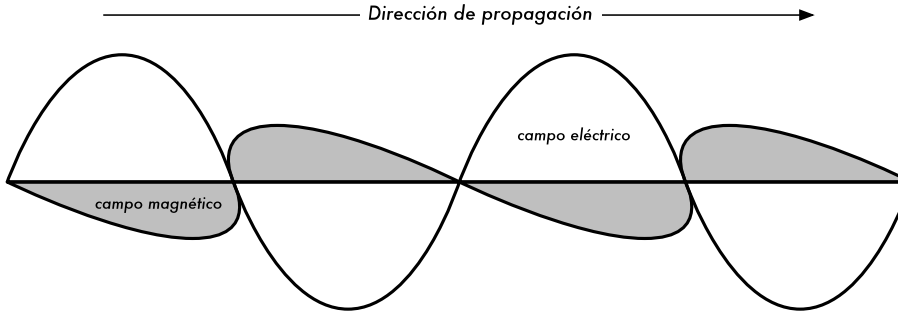


Figura 2.2: El campo eléctrico y el campo magnético complementario de una onda electromagnética. La polarización describe la orientación del campo eléctrico.

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 y $3{,}8*10^{14}$ 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.

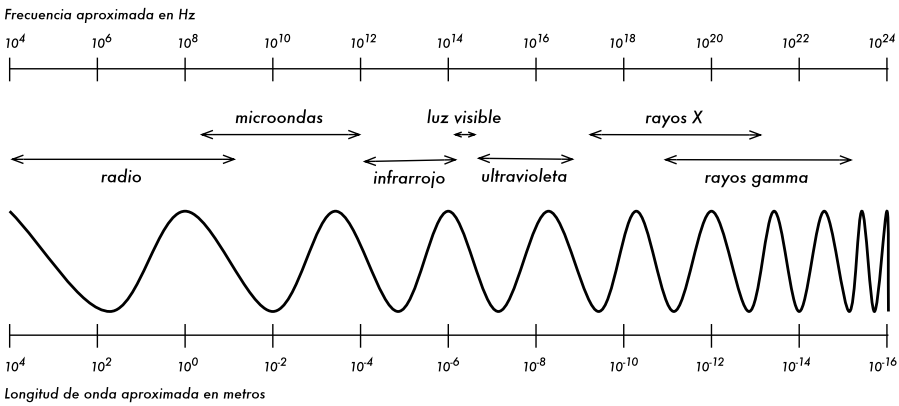


Figura 2.3: El espectro electromagnético.

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 – 5850 MHz (correspondiente a longitudes de onda de alrededor de 5 a 6 cm).

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 cómo 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 22 MHz, pero están separados sólo por 5 MHz. Esto significa que los canales adyacentes se superponen, y pueden interferir unos con otros. Esto es representado visualmente en la **Figura 2.4**.

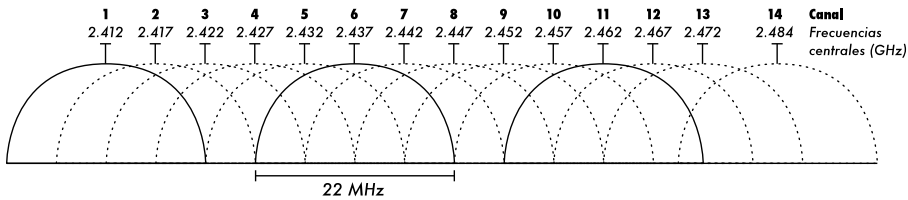


Figura 2.4: Canales y frecuencias centrales para 802.11b. Note que los canales 1, 6, y 11 no se superponen.

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

Comportamiento de las ondas de radio

Aquí 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 (88-108 MHz) puede atravesar edificios y otros obstáculos fácilmente, mientras que las ondas más cortas (cómo los teléfonos GSM operando a 900 MHz ó 1800 MHz) 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.

Imagine 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, las partículas vecinas harán 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 de Fresnel, la necesidad de línea visual así como el hecho de que algunas veces las ondas cruzan 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.

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 2,4 GHz. Un método simple de medir la absorción del plástico a 2,4 GHz es

---

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.

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 2,4 GHz, una rejilla metálica con separación de un cm (1 cm) entre sus elementos va a actuar igual que una placa de metal.

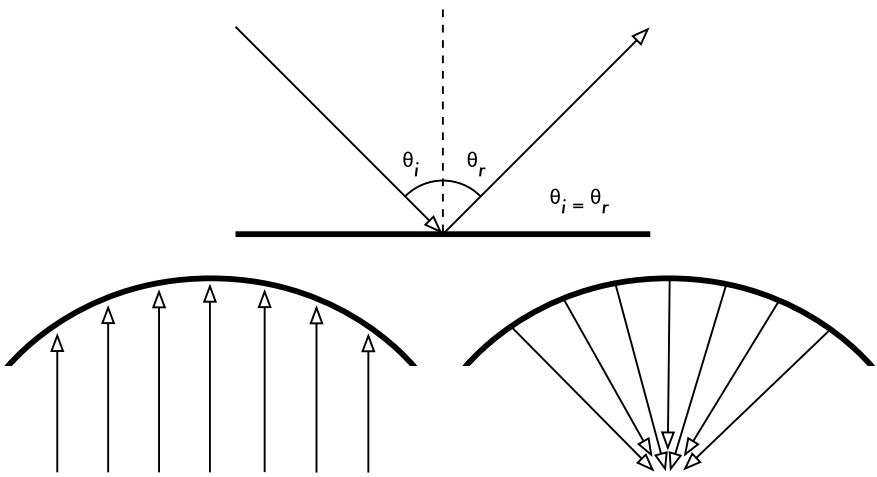


Figura 2.5: Reflexión de ondas de radio. El ángulo de incidencia es siempre igual al ángulo de reflexión. Una antena parabólica utiliza este efecto para concentrar las ondas de radio que caen sobre su superficie en una dirección común.

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.

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

Utilizamos la reflexión en ventaja nuestra en la construcción de las antenas: por ejemplo, colocando 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, interponemos en su camino una barrera sólida, como una cerca de madera, para bloquearla. Luego practicamos una estrecha rendija en esa barrera, 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.

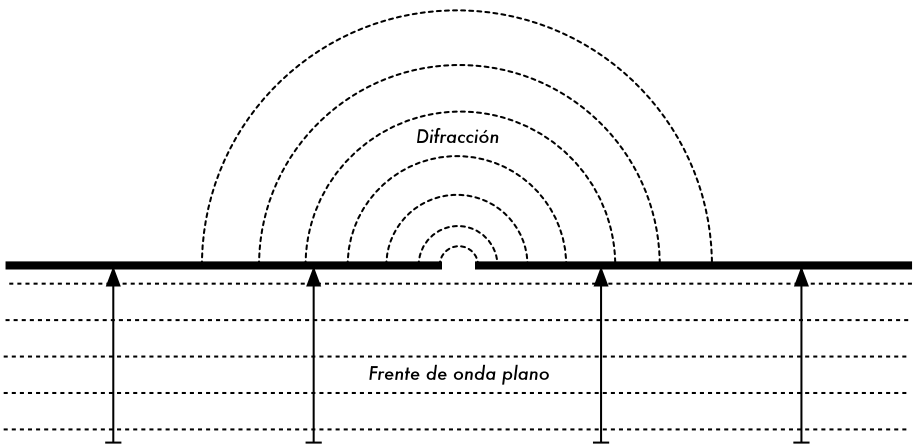


Figura 2.6: Difracción a través de una ranura pequeña.

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 o no adecuadamente el fenómeno, todavía es tema de debate. Pero para nuestros propósitos, el modelo de Huygens describe el efecto bastante bien.

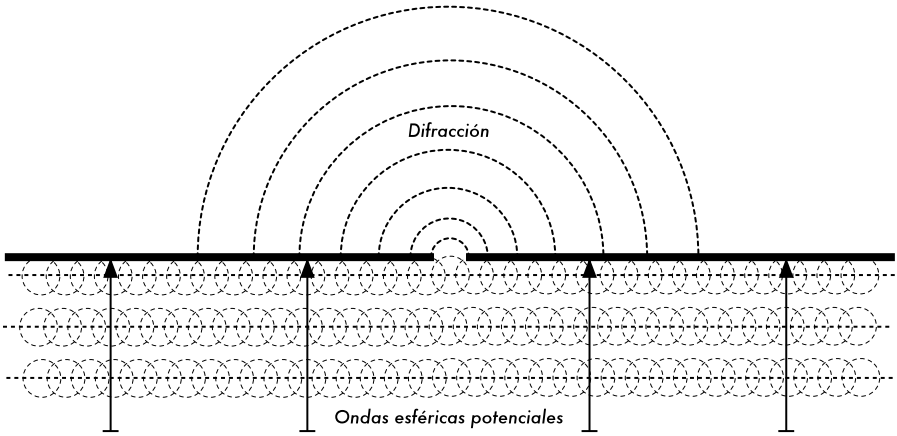


Figura 2.7: El Principio de Huygens.

Es por medio del efecto de difracción, que las ondas van a “doblar” en 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.

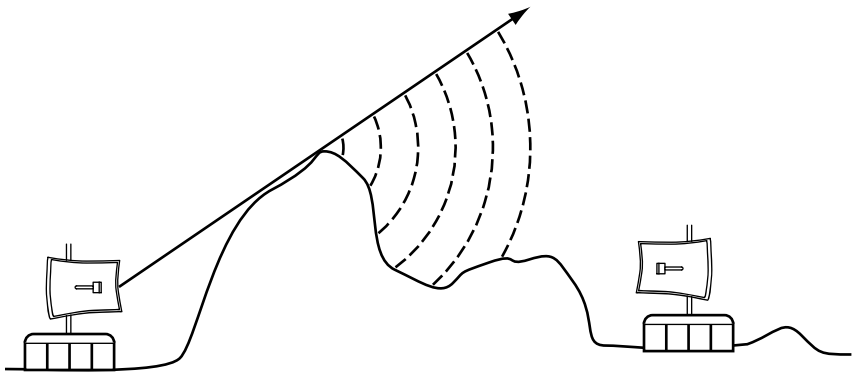


Figura 2.8: Difracción en la cima de una montaña.

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 ***interferencia constructiva***. Cuando un pico coincide con un valle, tenemos una completa aniquilación (1 + (-)1 = 0), y 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 los trenes de ondas se sumen o se 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.

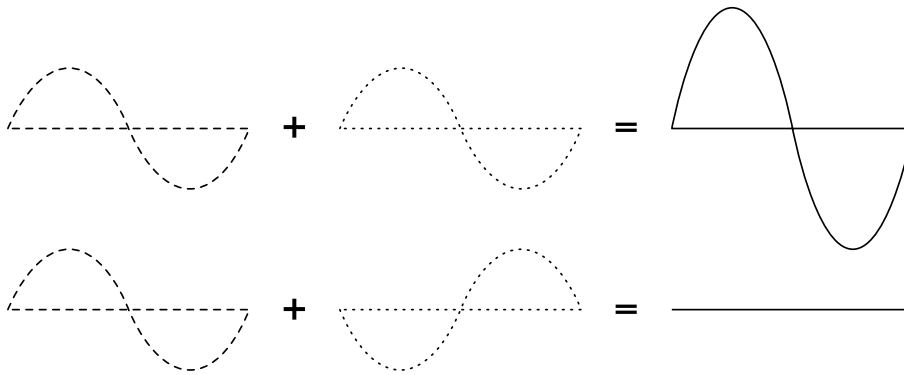


Figura 2.9: Interferencia constructiva y destructiva.

En la tecnología inalámbrica, la palabra Interferencia es usada comúnmente 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 ayudan a manejar el problema de la interferencia, pero no lo eliminan 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. Recuerde 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/a utilizando un apuntador láser económico y un par de binoculares en una noche clara. En lugar de apuntar a la luna, hágalo hacia 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, una elipse. Su ancho puede ser descrito por medio del concepto de zonas de Fresnel.

Para entender 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 el 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 la señal llega al punto B.

Tenga en cuenta que existen muchas zonas de Fresnel, pero a nosotros nos interesa principalmente la zona 1. Si esta fuera bloqueada por un obstáculo,

como 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.

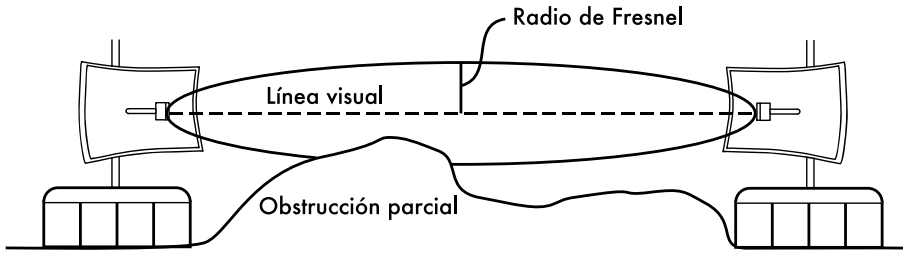


Figura 2.10: La zona de Fresnel es bloqueada parcialmente en este enlace, aunque la línea visual no está obstruida.

Aquí hay una fórmula 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 sustraer 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 2 km, transmitiendo a 2437 MHz (802.11b canal 6):

```
r = 17,31 sqrt ((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.

Potencia

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 3**. 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.

Cálculo en dB

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, esto es, define la relación entre dos medidas de potencia. Se define como:

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

…donde **P1** y **P0** pueden ser dos valores cualesquiera que queramos comparar. Normalmente, 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 llamamos exponencial. Por ejemplo, el oído humano escucha un sonido dos veces más fuerte que otro si el primero tiene diez veces la intensidad física del segundo.

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. Las 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/la lector/a 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 por aprender acerca de la física de radio de lo que nosotros podemos explicar aquí. Para encontrar más información acerca de este campo del conocimiento en constante desarrollo, consulte los recursos mencionados 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/a 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 los problemas de comunicación que desea resolver. 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 su implementación 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 ubicaciones fijas, o se va a expandir para incluir cientos de computadoras portátiles itinerantes y otros dispositivos?

En este capítulo, comenzaremos revisando los conceptos que definen TCP/IP, la principal familia de protocolos de red actualmente usados en Internet. Luego veremos cómo otras personas han construido redes inalámbricas para resolver sus problemas de comunicación, incluyendo diagramas de la estructura esencial de la red. Finalmente, mostraremos varios métodos sencillos para hacer que la información fluya eficientemente por su red y por la del resto del mundo.

Fundamentos de redes

TCP/IP hace referencia a una serie de protocolos que permiten mantener conversaciones en la Internet global. Al entender TCP/IP, usted podrá construir redes que pueden virtualmente alcanzar cualquier tamaño, y que a la postre formen parte de la Internet global.

Si usted ya está familiarizado/a con los conceptos esenciales de redes TCP/IP (incluyendo manejo de direcciones, enrutamiento, conmutadores, cortafuegos, y enrutadores), podría adelantar hasta la sección **Diseño de la red física**, en la **página 51**. Ahora revisaremos los fundamentos de las redes de Internet.

Introducción

Venecia, Italia, es una ciudad fantástica para perderse. Las calles son simples pasos peatonales que cruzan las aguas de los canales en cientos de sitios, y nunca van en línea recta. Los carteros venecianos son de los más entrenados del mundo, especializados en hacer entregas a sólo uno o dos de los seis *sestieri* (distritos) de Venecia. Esto es necesario debido a la intrincada disposición de la antigua ciudad. Mucha gente encuentra que conocer la ubicación del sol y el agua es mucho más útil que tratar de encontrar el nombre de una calle en un mapa.

Figura 3.1: Otro tipo de máscara de red.

Imagine un turista que encuentra una máscara de papel-maché como recuerdo y quiere enviarla desde la galería en S. Polo, Venecia, a una oficina en Seattle, EUA. Esto parece una tarea ordinaria (o incluso trivial), pero veamos lo que pasa realmente.

El artista, en primer lugar, empaca la máscara en una caja de cartón para despacharla a la oficina de Seattle, EUA. Esta caja es recogida por un empleado de correos quien le añade una serie de formularios oficiales, y la envía a una oficina de acopio central para envíos internacionales. Después de algunos días, el paquete pasa la aduana italiana y está listo para un vuelo trasatlántico y llega a un sitio central de procesamiento de importaciones en EUA. Una vez que pasa la aduana de EUA, el paquete se envía al punto de distribución regional del noroeste de los EUA, y luego al centro de procesamiento de Seattle. El paquete finalmente es transportado en un vehículo de reparto que tiene una ruta que lo llevará a la dirección apropiada, en la calle indicada, en el vecindario apropiado. Un empleado en la oficina postal recibe el paquete y lo coloca en el buzón de entradas apropiado. Una vez que llega, el paquete se recupera y la máscara es, finalmente, recibida.

El empleado de la oficina de Seattle ni sabe, ni le interesa cómo llegar al *sestiere* de S.Polo en Venecia. Su trabajo es, simplemente, recibir los paquetes cuando llegan, y entregarlos a la persona indicada. Igualmente, la compañía postal, en Venecia, no tiene por qué preocuparse de cómo llegar a la vecindad apropiada en Seattle. Su trabajo es recoger los paquetes en la vecindad local y reenviarlos al próximo centro de acopio en la cadena de entrega.

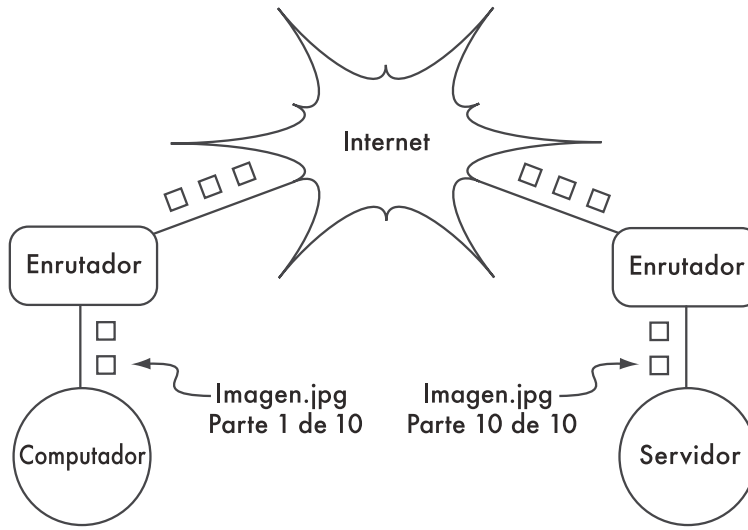


Figura 3.2: Red de Internet.
Los paquetes se remiten entre los enrutadores hasta que llegan al destino final.

El ejemplo anterior sirve para ilustrar cómo funciona el enrutamiento en Internet. Un mensaje es fragmentado en múltiples ***paquetes*** individuales, cada uno etiquetado con su origen y destino. El computador, entonces, envía estos paquetes a un ***enrutador*** (*router*), que decide dónde va a enviarlos a continuación. El enrutador sólo necesita recordar un número pequeño de rutas, por ejemplo, cómo llegar a la red local, la mejor ruta hacia algunas otras redes locales, y una ruta hacia una pasarela (*gateway*) que lo comunica al resto de Internet. Esta lista de posibles rutas se denomina ***tabla de enrutamiento*** (*routing table*). A medida que los paquetes llegan al enrutador, la dirección del destinatario es examinada y comparada con su tabla de enrutamiento interna. Si el enrutador no tiene una ruta explícita para el destino en cuestión, manda el paquete hacia la que más se le aproxime, que es, a menudo, su propia pasarela a Internet (a través de su ***ruta por defecto—default route***). El próximo enrutador hace lo mismo, y así sucesivamente, hasta que el paquete finalmente llega a su destino.

Los paquetes de mercancía pueden ser enviados a través del sistema postal internacional sólo porque hemos establecido un sistema de direcciones estandarizado para este fin. Por ejemplo, la dirección del destinatario debe estar escrita en el frente del paquete de forma legible, e incluir toda la información

crítica (nombre del destinatario, calle, ciudad, país, código postal). Sin esta información, los paquetes o son devueltos al remitente, o se pierden en el sistema.

Los paquetes de datos fluyen a través de la Internet global sólo en virtud de que hemos convenido sobre un sistema común de direcciones y un protocolo para el envío de los mismos. Estos protocolos de comunicación estándar hacen posible el intercambio de información a una escala global.

Comunicaciones cooperativas

La comunicación es sólo posible cuando los participantes hablan una lengua común. Pero una vez que la comunicación se hace más compleja que una simple conversación entre dos personas, el protocolo se vuelve tan importante como la lengua. Puede que toda la gente de un auditorio hable español, pero sin un conjunto de reglas establecidas para decidir quién tiene el derecho de usar el micrófono, la comunicación de las ideas de una sola persona a la audiencia completa es casi imposible. Ahora, imagínese un auditorio tan grande como el mundo, lleno de todos los computadores existentes. Sin un conjunto común de protocolos de comunicación para regular cuándo y cómo puede hablar cada computador, Internet sería un desastre caótico donde todas las máquinas tratan de hablar al mismo tiempo.

El modelo OSI

El estándar internacional para Sistemas Abiertos de Interconexión, OSI (por su sigla en inglés: *Open Systems Interconnection*), se define en el documento ISO/IEC 7498-1, emanado de la *International Standards Organization* y la *International Electrotechnical Comission*. El estándar completo está disponible como publicación "ISO/IEC 7498-1: 1994", en *http://standards.iso.org/ittf/PubliclyAvailableStandards/*x

El modelo OSI divide el tráfico de la red en una cantidad de ***capas***. Cada capa es independiente de las capas que la rodean y cada una se apoya en los servicios prestados por la capa inferior mientras que proporciona sus servicios a la capa superior. La separación entre capas hace que sea fácil diseñar una ***pila de protocolos*** (*protocol stack*) muy elaborada y confiable, tal como la difundida pila ***TCP/IP***. Una pila de protocolos es una implementación real de un marco de comunicaciones estratificado. El modelo OSI no define los protocolos que van a usarse en una red en particular, sino que simplemente delega cada "trabajo" de comunicaciones a una sola capa dentro de una jerarquía bien definida.

Mientras que la especificación ISO/IEC 7498-1 determina cómo deberían interactuar las capas, los detalles de la implementación real se dejan al fabricante. Cada capa puede implementarse en el hardware (es más común para las capas inferiores), o en el software. Siempre y cuando la interfaz entre capas se adhiera al estándar, los instaladores son libres de usar cualquier medio a su disposición para construir su pila de protocolos. Esto quiere decir que cualquier capa de un fabricante A puede operar con la misma capa de un fabricante B (suponiendo que las especificaciones relevantes se implementen e interpreten correctamente).

A continuación se presenta un breve bosquejo del modelo de redes OSI de siete capas.

Capa	Nombre	Descripción
7	Aplicación	La ***Capa de Aplicación*** es la capa con la que la mayoría de los usuarios tiene contacto, y es el nivel en el que ocurre la comunicación humana. HTTP, FTP, y SMTP son todos protocolos de la capa de aplicación. El usuario se ubica por encima de esta capa, interactuando con la aplicación
6	Presentación	La ***Capa de Presentación*** tiene que ver con representación de datos, antes de que lleguen a la aplicación. Esto incluye codificación MIME, compresión de datos, comprobación del formato, ordenación de los bytes , etc.
5	Sesión	La ***Capa de Sesión*** maneja la sesión de comunicación lógica entre aplicaciones. NetBIOS y RPC son dos ejemplos de protocolos de la capa 5.
4	Transporte	La ***Capa de Transporte*** provee un método para obtener un servicio particular en un nodo de red específico. Algunos ejemplos de protocolos que operan en esta capa son TCP y UDP. Algunos protocolos de la capa de transporte (como TCP), garantizan que todos los datos lleguen a destino y se reorganicen y entreguen a la próxima capa en el orden apropiado. UDP es un protocolo “no orientado a conexión” comúnmente usado para señales de video y audio de flujo continuo.
3	Red	IP (el protocolo de Internet) es el más común de la ***Capa de Red***. Esta es la capa donde ocurre el enrutamiento. Se encarga de transferir los paquetes desde la capa de enlace local a la de otras redes. Los enrutadores cumplen esta función en una red por medio de, al menos, dos interfaces de red, una en cada una de las redes que se van a interconectar. Cada nodo en Internet tiene una dirección IP exclusiva. Otro protocolo crítico de Capa de Red es ICMP, que es un protocolo especial que proporciona varios mensajes necesarios para la adecuada operación de IP. Esta capa a menudo se denomina la ***Capa de Internet.***

Capa	Nombre	Descripción
2	Enlace de datos	Cada vez que dos o más nodos comparten el mismo medio físico (por ejemplo, varios computadores conectados a un concentrador (hub), o una habitación lleno de dispositivos inalámbricos que usan el mismo canal de radio), usan la ***Capa de Enlace de Datos*** para comunicarse. Los ejemplos más comunes de protocolos de enlace de datos son Ethernet, Token Ring, ATM, y los protocolos de redes inalámbricas (802.11a/b/g). La comunicación en esta capa se define como de enlace-local porque todos los nodos conectados a esta capa se comunican directamente entre sí. Esta capa también se conoce como capa de Control de Acceso al Medio (MAC en inglés). En redes modeladas de acuerdo con Ethernet, los nodos se identifican por su dirección MAC. Esta es un número exclusivo de 48 bits asignado de fábrica a todo dispositivo de red.
1	Física	***La Capa Física*** es la capa más baja en el modelo OSI, y se refiere al medio físico real en el que ocurre la comunicación. Este puede ser un cable CAT5 de cobre, un par de fibras ópticas, ondas de radio, o cualquier otro medio capaz de transmitir señales. Cables cortados, fibras partidas, e interferencia de RF constituyen, todos, problemas de capa física.

Las capas de este modelo están numeradas del 1 al 7, con el 7 en el tope. Esto se hace para reforzar la idea de que cada capa está basada y depende de la capa de abajo. Imagine el modelo OSI como un edificio, con sus bases en la capa 1. Las próximas capas, como los pisos sucesivos, y el techo, como la capa 7. Si se remueve una sola capa, el edificio no se sostiene. De manera semejante, si se incendia el piso 4, nadie podría atravesarlo en ninguna de las dos direcciones.

Las primeras tres capas (Física, Enlace de Datos y Red) ocurren todas “en la red”. Es decir, la actividad en estas capas va a estar determinada por la configuración de los cables, conmutadores, enrutadores y otros dispositivos semejantes. Un conmutador (*switch*) de red puede distribuir paquetes usando sólo direcciones MAC, así que necesita implementar sólo las capas 1 y 2. Un enrutador sencillo puede enrutar paquetes usando sólo sus direcciones IP, así que necesita implementar sólo las capas 1 a 3. Un servidor web o un computador portátil (*laptop*) ejecutan aplicaciones, así que deben implementar las siete capas. Algunos enrutadores avanzados pueden implementar desde la capa 4 en adelante lo que les permite tomar decisiones basadas en la información de alto nivel contenida en un paquete, como el nombre de un sitio web, o los adjuntos de un correo electrónico.

El modelo OSI es internacionalmente reconocido, y es considerado como el modelo de red definitivo y completo. Proporciona un esquema para los

fabricantes e implementadores de protocolos de red que puede ser usado para construir dispositivos inter-operacionales en cualquier parte del mundo.

Desde la perspectiva de un ingeniero de redes, o una persona que trate de localizar una falla, el modelo OSI puede parecer innecesariamente complejo. En particular, la gente que construye o localiza fallas en redes TCP/IP rara vez se encuentra con problemas en las capas de Sesión o Presentación. Para la mayor parte de las implementaciones de redes, el modelo OSI puede ser simplificado en un conjunto menor de cinco capas.

El modelo TCP/IP

A diferencia del modelo OSI, el modelo TCP/IP no es un estándar internacional, y su definición varía. Sin embargo, es usado a menudo como un modelo práctico para entender y resolver fallas en redes Internet. La mayor parte de Internet usa TCP/IP, así que podemos plantear algunas premisas sobre las redes que las harán de más fácil comprensión. El modelo de redes TCP/IP describe las siguientes cinco capas:

Capa	Nombre
5	Aplicación
4	Transporte
3	Internet
2	Enlace de Datos
1	Física

En términos del modelo OSI, las capas cinco a siete quedan comprendidas en la capa superior (la Capa de Aplicación). Las primeras cuatro capas de ambos modelos son idénticas. Muchos ingenieros de redes consideran todo lo que está por encima de la capa cuatro como “sólo datos”, que van a variar de aplicación a aplicación. Ya que las primeras tres capas son inter-operables para los equipos de casi todos los fabricantes, y la capa cuatro trabaja entre todos los anfitriones que usan TCP/IP, y todo lo que está por arriba de la capa cuatro es para aplicaciones específicas, este modelo simplificado funciona bien cuando se construyen o detectan fallas en redes TCP/IP. Vamos usar el modelo TCP/IP cuando hablemos de redes en este libro.

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 arribar 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). Una vez entregada la carta, el mensajero queda libre.

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, **E**nlace de **D**atos, **I**nternet, **T**ransporte, y **A**plicación, o en inglés "*Please Don't Look In The Attic*," que se usa por "*Physical* / *Data Link* / *Internet* / *Transport* / *Application*".

Los protocolos de Internet

TCP/IP es la pila de protocolos más comúnmente usada en la Internet global. El acrónimo se lee en inglés ***Transmission Control Protocol***, e ***Internet Protocol***, respectivamente, pero en realidad se refiere a una familia completa de protocolos de comunicaciones relacionados. TCP/IP también se conoce como ***grupo de protocolo Internet***, y opera en las capas tres y cuatro del modelo TCP/IP.

En la presente discusión nos concentraremos en la versión cuatro del protocolo IP (IPv4), ya que en este momento es el protocolo más implementado en Internet.

Direccionamiento IP

En una red IPv4, la dirección es un número de 32 bits, normalmente escrito como cuatro números de 8 bits expresados en forma decimal y separados por puntos. Ejemplos de direcciones IP son: 10.0.17.1; 192.168.1.1; ó 172.16.5.23.

Si se enumeraran todas las direcciones IP posibles, estas irían desde 0.0.0.0 hasta 255.255.255.255. Esto arroja un total de más de cuatro mil millones de direcciones IP posibles (255 x 255 x 255 x 255 = 4.228.250.625). Sin embargo, muchas de estas están reservadas para propósitos especiales y no deberían ser asignadas a anfitriones. Cada una de las direcciones IP usables, es un identificador exclusivo que diferencia un nodo de red de otro.

Las redes interconectadas deben convenir sobre un plan de direcciones IP. Las direcciones IP deben ser únicas y generalmente no pueden usarse en diferentes puntos de la Internet al mismo tiempo; de lo contrario, los enrutadores no sabrían cuál es la mejor manera de enrutarles los paquetes.

Las direcciones IP son asignadas por una autoridad central de numeración que proporciona un método de numeración consistente y coherente. Esto evita la posibilidad de duplicar direcciones. La autoridad central asigna grandes bloques de direcciones consecutivas a las autoridades locales, las cuales asignan, a su vez, bloques consecutivos más pequeños dentro de esos rangos a otras autoridades, o a sus clientes. Estos grupos de direcciones se llaman ***subredes***. Subredes grandes pueden, a su vez, dividirse en subredes menores. Un grupo de direcciones relacionadas se denomina ***espacio de direcciones***.

Subredes

Aplicando una ***máscara de subred*** (también llamada máscara de red, o simplemente *netmask*, en inglés) usted puede especificar tanto al anfitrión (*host*), como a la red a la que pertenece. Tradicionalmente, las máscaras de subred se expresan utilizando formas decimales separadas por puntos, a la manera de una dirección IP. Por ejemplo, 255.255.255.0 sería una máscara común. Usted

encontrará que esta notación se usa al configurar interfaces de redes, al crear rutas, etc. Sin embargo, las máscaras de subred se expresan más sucintamente utilizando ***notación CIDR***, la que simplemente enumera la cantidad de bits en la máscara después de la barra ascendente (/). De esta manera, 225.225.225.0 puede simplificarse en /24. CIDR es la sigla en inglés de ***Classless Inter-Domain Routing—Enrutamiento entre dominios sin referencia a la clase***—y está definida en RFC1518[1].

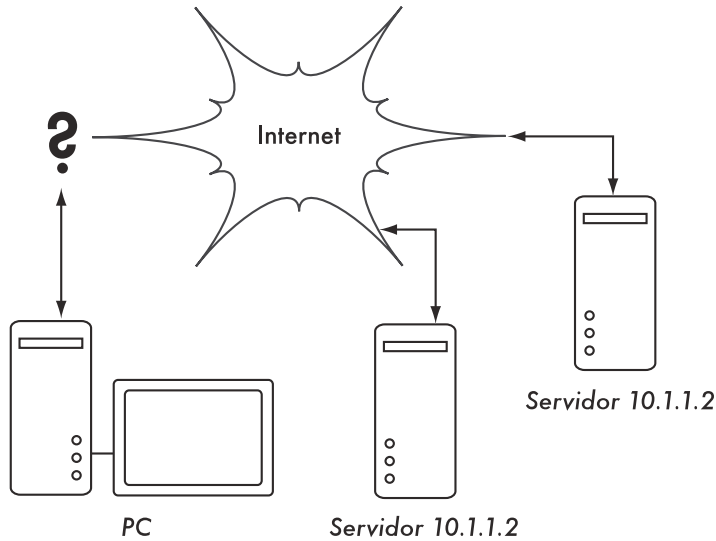


Figura 3.3: Si las direcciones IP no son únicas, un enrutamiento global inequívoco es imposible. Si el PC solicita una página web desde 10.1.1.2, ¿con cuál servidor se va a conectar?

Una máscara de subred determina el tamaño de una red dada. Al usar una máscara de red /24, hay 8 bits reservados para anfitriones: (32 bits en total—24 bits de máscara de red = 8 bits para anfitriones). Esto permite hasta 256 direcciones de anfitrión ($2^8 = 256$). Por convención, el primer valor se toma como la ***dirección de la red*** (.0 ó 00000000), y el último se toma como la ***dirección de difusión*** (.255 ó 11111111). Esto deja 254 direcciones libres para anfitriones en esta red.

Las máscaras de subred funcionan aplicando lógica AND al número IP de 32 bits. En notación binaria, los bits "1" de la máscara indican la porción de la dirección de red, y los "0", la porción de la dirección del anfitrión. Un AND lógico se efectúa comparando los dos bits. El resultado es "1" si los dos bits comparados son también "1". De lo contrario, el resultado es "0". A continuación exponemos todos los resultados posibles de la operación AND binaria entre dos bits.

1. RFC: Request For Comments, es una serie numerada de documentos sobre Internet, publicados por la Internet Society. No todas las RFC son estándares. Pueden verse en línea en *http://rfc.net/*

Bit 1	Bit 2	Resultado
0	0	0
0	1	0
1	0	0
1	1	1

Para entender cómo una máscara de red se aplica a una dirección IP, primero convierta todo a binario. La máscara de red 255.255.255.0 en binario contiene veinticuatro bits “1”.

```
255      .255      .255      .0
11111111 .11111111 .11111111 .00000000
```

Cuando esta máscara de red se combina con la dirección IP 10.10.10.10, podemos aplicar el AND lógico a cada uno de los bits para determinar la dirección de red.

```
  10.10.10.10: 00001010.00001010.00001010.00001010
255.255.255.0: 11111111.11111111.11111111.00000000
               ----------------------------------
   10.10.10.0: 00001010.00001010.00001010.00000000
```

Esto da como resultado la red 10.10.10.0/24. Esta red comprende desde los anfitriones 10.10.10.1 hasta 10.10.10.254, con 10.10.10.0 como la dirección de red, y 10.10.10.255 como la dirección de difusión.

Las máscaras de subred no están limitadas a octetos enteros. También se pueden especificar máscaras de subred como 255.254.0.0 (ó /15 CIDR). Este es un bloque grande que contiene 131.072 direcciones, desde 10.0.0.0 hasta 10.1.255.255. Podría continuar dividiéndose, por ejemplo, en 512 subredes de 256 direcciones cada una. La primera sería 10.0.0.0-10.0.0.255, luego 10.0.1.0 -10.0.1.255, y así sucesivamente, hasta 10.1.255.0-10.1.255.255. Alternativamente, podría ser dividido en dos bloques de 65.536 direcciones, u 8.192 bloques de 16 direcciones, o de muchas otras maneras diferentes. Incluso, podría dividirse en una combinación de diferentes tamaños de bloques, siempre y cuando ninguno se solape con otro, y que cada uno sea una subred válida cuyo tamaño sea una potencia de dos.

Aunque muchas máscaras de red son posibles, las más comunes son:

CIDR	Decimal	# de Anfitriones
/30	255.255.255.252	4
/29	255.255.255.248	8
/28	255.255.255.240	16
/27	255.255.255.224	32
/26	255.255.255.192	64
/25	255.255.255.128	128
/24	255.255.255.0	256
/16	255.255.0.0	65 536
/8	255.0.0.0	16 777 216

Con cada decremento en el valor de CIDR, el espacio de direcciones IP se duplica. Recuerde que en cada red hay dos direcciones IP reservadas para las direcciones de red y de difusión.

Hay tres máscaras de red comunes que tienen nombres especiales. Una red /8 (con una máscara de red de 255.0.0.0) define a una red ***Clase A***. Una /16 (255.255.0.0) es una ***Clase B***, y una /24 (255.255.255.0) se llama ***Clase C***. Estos nombres se usaban mucho antes de la notación CIDR, y se usan todavía a menudo por razones históricas.

Direcciones IP globales

¿Se ha preguntado usted quién controla las asignaciones del espacio IP? Las ***Direcciones IP enrutables globalmente*** son asignadas y distribuidas por los ***Administradores Regionales de Internet*** (*RIR*, por la sigla en inglés) a los Proveedores de Servicios de Internet (*ISP*, en inglés). El ISP, entonces, les asigna a los clientes pequeños bloques, a medida que los solicitan. En la práctica, todos los usuarios de Internet obtienen sus direcciones IP de un ISP.

Los cuatro mil millones de direcciones IP disponibles son administrados por la ***IANA***, que es la ***Autoridad de Asignación de Números de Internet — Internet Assigned Numbers Authority*** (IANA, *http://www.iana.org*). IANA ha dividido el espacio Internet en grandes subredes, normalmente del tipo /8 con 16 millones de direcciones cada una. Estas subredes se delegan a uno de los cinco registros regionales de Internet (*RIR*, en inglés), a los que se ha asignado autoridad sobre áreas geográficas extensas.

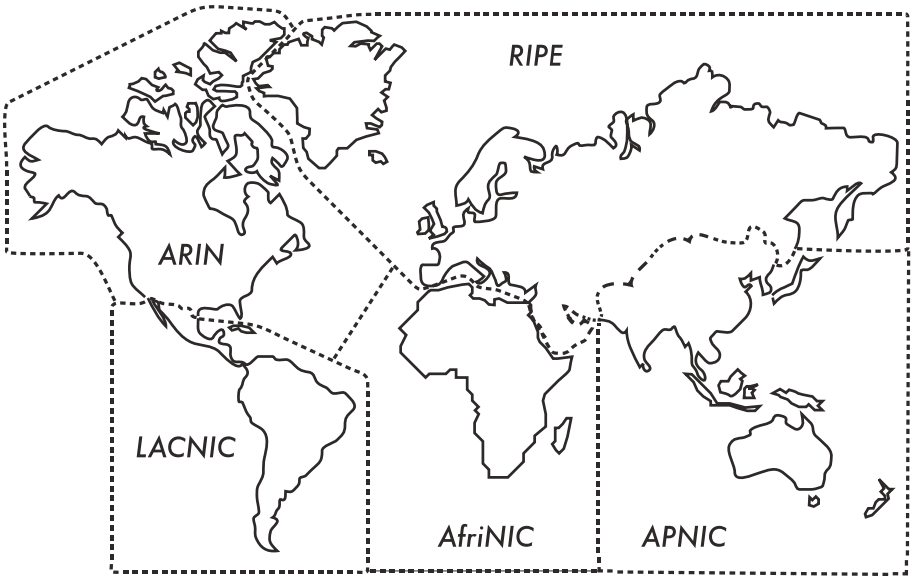


Figura 3.4: La autoridad para la asignación de direcciones IP se delega en cinco Administradores Regionales de Internet - Regional Internet Registrars (RIR).

Los cinco Administradores Regionales de Internet—Regional Internet Registrars (RIR), son:

- Centro de Información de la Red de África
  (AfriNIC, *http://www.afrinic.net/*)
- Centro de Información de la Red de Asia del Pacífico
  (*APNIC, http://www.apnic.net/*)
- Registro Americano de Número de Internet
  (ARIN, *http://www.arin.net/*)
- Registro de Direcciones IP para Latinoamérica y el Caribe
  (LACNIC, *http://www.lacnic.net/*)
- Red IP de Europa
  (RIPE NCC, *http://www.ripe.net/*)

Su Proveedor de Servicios de Internet le asignará un espacio de direcciones IP enrutables globalmente, tomadas de las que le asigne el Administrador Regional de Internet.

Una vez que se llegue a un acuerdo sobre las asignaciones de direcciones IP, es posible transmitir paquetes entre diferentes redes y participar en la Internet global. El proceso de mover paquetes entre las diferentes redes se conoce como ***enrutamiento***, ***ruteo***, o ***encaminamiento***.

Direcciones IP estáticas

Una dirección IP estática es una dirección asignada que no cambia nunca. Las direcciones IP estáticas son importantes porque los servidores que las usan son alcanzables por los servidores DNS y comúnmente ofrecen servicios a otras máquinas (por ejemplo, servicio de correo electrónico, servidores web, etc).

Los bloques de direcciones IP estáticas pueden ser asignados por su ISP, bajo pedido, o automáticamente, dependiendo de sus medios de conexión a Internet.

Direcciones IP dinámicas

Las direcciones IP dinámicas son asignadas por un ISP para nodos no permanentes conectados a Internet, tales como computadores caseros conectados por discado.

Las direcciones IP dinámicas pueden ser asignadas automáticamente usando el ***Protocolo Dinámico de Configuración de Anfitrión—Dynamic Host Configuration Protocol*** (***DHCP***), dependiendo del tipo de conexión a Internet. Un nodo que usa DHCP, en primer lugar le solicita a la red una dirección IP y automáticamente configura su interfaz de red. Las direcciones IP las puede asignar aleatoriamente su ISP a partir del bloque de direcciones que posee, o puede asignarse de acuerdo con una determinada política. Las direcciones IP asignadas por el DHCP son válidas por un período determinado (llamado ***período de adjudicación—lease time***). El nodo debe renovar la adjudicación DHCP antes de su expiración. Al renovarla, el nodo puede recibir la misma dirección IP o una diferente de la reserva de direcciones disponibles.

Las direcciones dinámicas son muy populares entre los proveedores de servicios de Internet, porque les permite usar menos direcciones IP que el número total de clientes. Se necesita sólo una dirección por cada cliente que esté ***activo en un momento dado***. Las direcciones IP globalmente enrutables son caras, y algunas autoridades que realizan la adjudicación de direcciones (como RIPE, el RIR europeo) son muy estrictas en cuanto al uso de direcciones IP por parte de los ISP. Asignar direcciones dinámicas le permite al ISP ahorrar dinero, por lo que usualmente exigen un pago adicional a los clientes que deseen una dirección IP estática.

Direcciones IP privadas

La mayor parte de las redes privadas no requieren la adjudicación de direcciones IP públicas, globalmente enrutables, para cada computador en la organización. En particular, los computadores que no son servidores no necesitan ser direccionables desde la Internet pública. Las organizaciones comúnmente utilizan, para los computadores internos, direcciones IP tomadas del ***espacio de direcciones privadas***.

Hoy en día existen tres bloques de espacio de direcciones privadas reservados por IANA: 10.0.0.0/8; 172.16.0.0/12; y 192.168.0.0/16. Estas están definidas en el RFC1918. Estas direcciones no son enrutables en la Internet, y usualmente son exclusivas solamente en el ámbito de una organización o grupo de organizaciones, que hayan escogido seguir el mismo esquema de numeración.

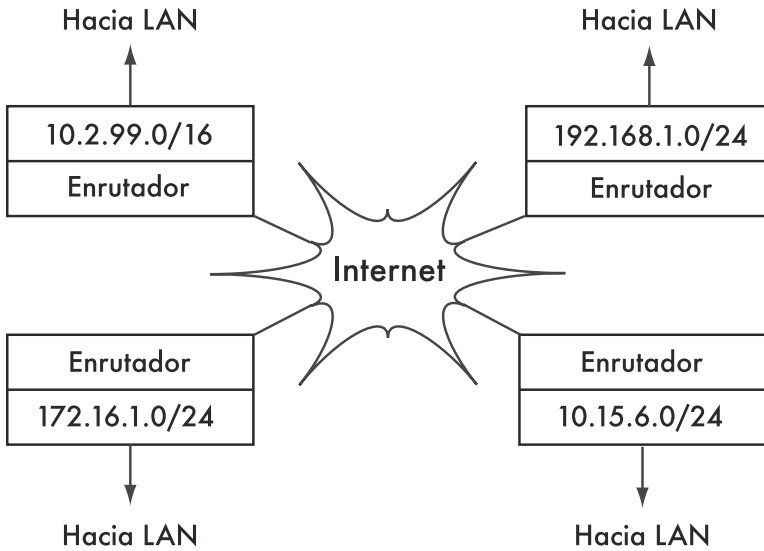


Figura 3.5: Las direcciones privadas RFC1918 pueden ser usadas dentro de una organización, y no son difundidas hacia la Internet global.

Si usted alguna vez tiene la intención de interconectar redes privadas que usan espacio de direcciones RFC1918, asegúrese de no repetir direcciones en ninguna de las redes. Por ejemplo, podría fragmentar el espacio de direcciones 10.0.0.0 /8 en múltiples redes Clase B (10.1.0.0/16, 10.2.0.0/16, etc). Un bloque podría asignarse a cada red de acuerdo con su ubicación física (parte central del campus, primer grupo de oficinas, segundo grupo de oficinas, residencias estudiantiles, etc.). Los/las administradores/as de red de cada ubicación pueden, a su vez, volver a fragmentar la red en múltiples redes Clase C (10.1.1.0/24, 10.1.2.0/24, etc.), o en bloques de cualquier otro tamaño lógico. En el futuro, en el caso en que la red esté alguna vez conectada (sea físicamente, por enlace inalámbrico o VPN), todas las máquinas van a ser alcanzables desde cualquier punto en la red sin tener que volver a numerar los dispositivos de red.

Algunos proveedores de Internet pueden adjudicarles a sus clientes direcciones privadas como éstas, en lugar de direcciones públicas, a pesar de que hay serias desventajas. Puesto que estas direcciones no pueden ser enrutadas en Internet, los computadores que las usan no son en verdad “parte” de Internet y no son directamente asequibles desde ella. Para poder conectarlos con Internet sus direcciones privadas deben ser convertidas en direcciones públicas. Este proceso de conversión se conoce como ***Traducción de Direcciones de Red*** (***NAT***, en inglés), y se ejecuta normalmente en la pasarela (gateway) entre la red privada e Internet. Veremos más detalles en la **página 44**.

Enrutamiento

Imagínese una red con tres anfitriones: A, B y C. Estos usan las direcciones IP 192.168.1.1; 192.168.1.2; y 192.168.1.3, respectivamente. Estos anfitriones son parte de una red /24 (su máscara de red es 255.255.255.0). Para que dos anfitriones se comuniquen en una red local, deben conocer las direcciones MAC respectivas. Es posible configurar manualmente cada anfitrión con una tabla de mapeo desde una dirección IP a una dirección MAC, pero normalmente el ***Protocolo de Resolución de Direcciones*** (ARP, en inglés) se usa para determinar esto de manera automática.

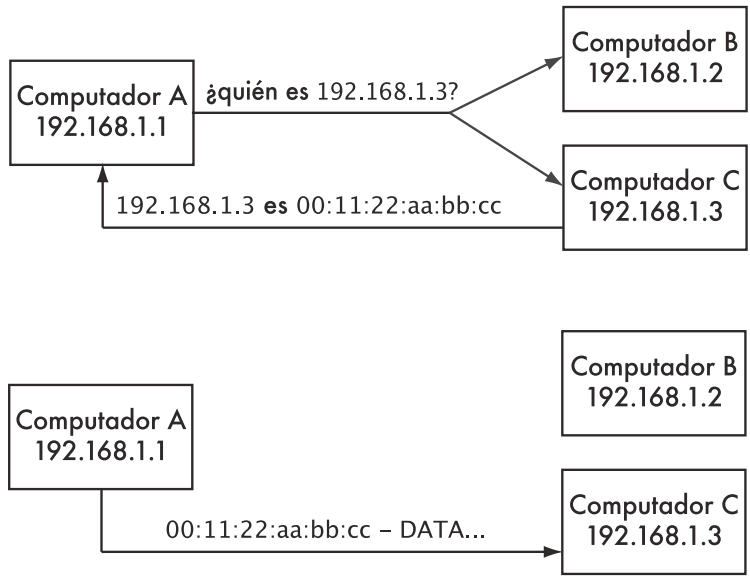


Figura 3.6: El computador A necesita enviar datos a 192.168.1.3. Pero debe primero preguntar por toda la red cuál es la dirección MAC que responde a 192.168.1.3.

Cuando se usa ARP, el anfitrión A transmite a los otros anfitriones la pregunta: "¿Quién tiene la dirección MAC para la IP 192.168.1.3?" Cuando el anfitrión C ve una solicitud ARP de su propia dirección IP, le responde con su dirección MAC.

Considere ahora otra red con 3 anfitriones: D, E y F, con las direcciones IP 192.168.2.1; 192.168.2.2; 192.168.2.3, respectivamente. Esta es otra red /24, pero no en el mismo rango que la red anterior. Los tres anfitriones pueden conectarse entre sí directamente (primero, usando ARP para transformar la dirección IP en una dirección MAC, y luego enviando los paquetes a esa dirección MAC).

Ahora añadimos el anfitrión G. Este tiene dos tarjetas de red, una de ellas conectada a cada red. La primera tarjeta de red usa la dirección IP 192.168.1.4, y la otra usa 192.168.2.4. El anfitrión G tiene presencia física en ambas redes, y puede enrutar paquetes entre ellas.

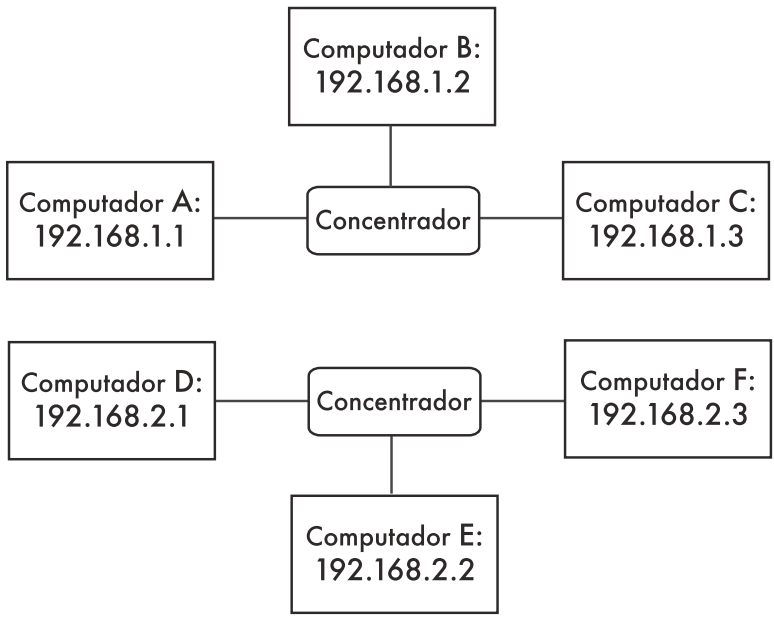


Figura 3.7: Dos redes IP separadas.

Pero, ¿qué pasa si los anfitriones A, B y C quieren conectar con D, E y F? Necesitarían añadir una ruta a la otra red por intermedio de G. Por ejemplo, A y C añadirían una ruta a través de 192.168.2.4. En Linux, esto se logra con la instrucción:

```
# ip route add 192.168.2.0/24 via 192.168.1.4
```

Y los anfitriones D-F añadirían la siguiente:

```
# ip route add 192.168.1.0/24 via 192.168.2.4
```

El resultado se muestra en la **Figura 3.8**. Note que la ruta se añade a través de la dirección IP en el anfitrión G que tiene una conexión local para la red respectiva. El anfitrión A no podría añadir esta ruta a través de 192.168.2.4, a pesar de que físicamente sea la misma máquina que 192.168.1.4 (anfitrión G), porque esa dirección IP corresponde a otra interfaz de red. Recuerde que las direcciones IP se asignan a la interfaz, que es la que está físicamente conectada a la red respectiva.

La ruta le dice al sistema operativo que la red deseada no se encuentra en la red local inmediata, y que debe ***reenviar*** el tráfico a través del enrutador especificado. Si el anfitrión A quiere enviar un paquete a F, este sería primero enviado a G. Entonces G buscaría a F en su tabla de enrutamiento para ver si

tiene conexión directa con la red de F. Finalmente, el anfitrión G resolvería la dirección física (MAC) de F y le remitiría el paquete.

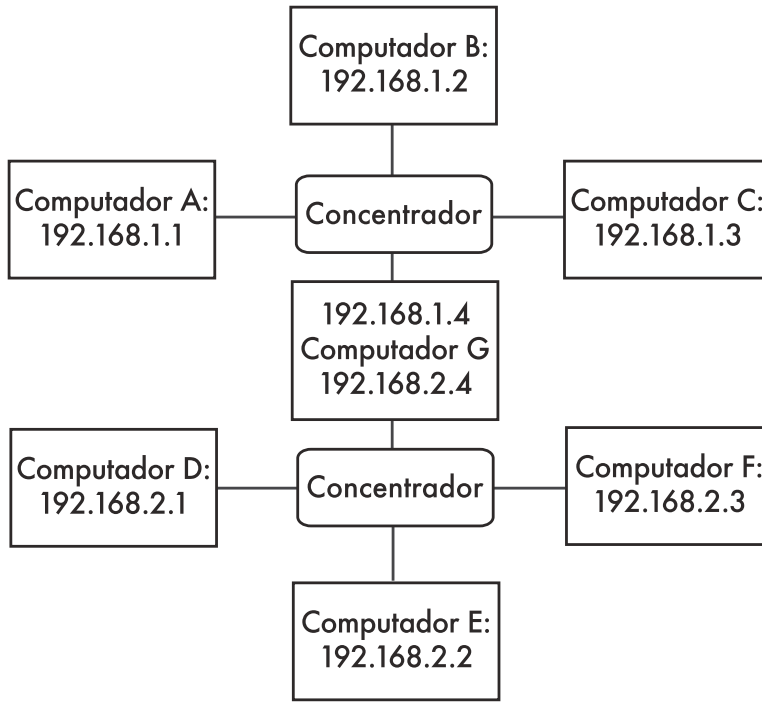
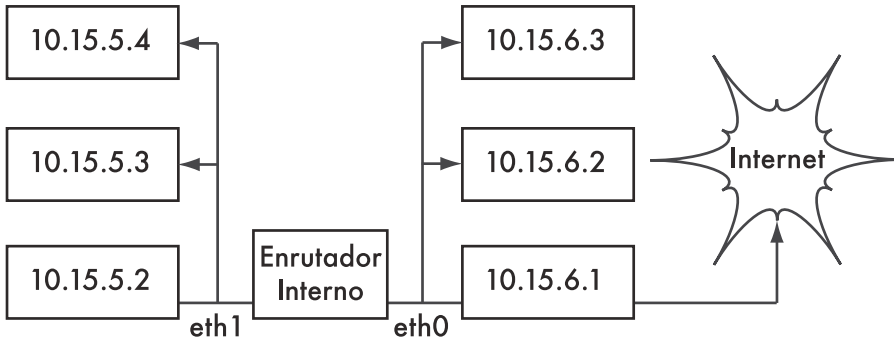


Figura 3.8: El anfitrión G actúa como enrutador entre las dos redes.

Este es un ejemplo de enrutamiento muy sencillo donde el destino final está a un solo ***salto*** (*hop*) desde el origen. A medida que las redes se hacen más complejas, se necesitarán muchos saltos para alcanzar el destino final. Puesto que no sería práctico que cada máquina de Internet "conociera" la ruta hacia todas las demás, hacemos uso de una entrada de enrutamiento que se conoce como la ***ruta por defecto*** (también conocida como la ***pasarela por defecto***). Cuando un enrutador recibe un paquete destinado a una red para la cual no se ha especificado una ruta, el paquete se remite a su pasarela por defecto.

La pasarela (*gateway*) por defecto es comúnmente la mejor ruta hacia el exterior de su red, usualmente en la dirección de su ISP. Un ejemplo de un enrutador que usa una pasarela por defecto se muestra en la **Figura 3.9**.

Las rutas pueden ser actualizadas manualmente, o pueden reaccionar dinámicamente ante una falla de red, u otra eventualidad. Algunos ejemplos de protocolos de enrutamiento dinámico más populares son RIP, OSPF, BGP, y OLSR. Enseñar a configurar enrutamiento dinámico está más allá de los objetivos de este libro, pero para información sobre lecturas al respecto puede consultar el **Apéndice A**.




```
Tabla de enrutamiento para enrutador interno:

Destino         Gateway     Genmask         Flags  Metric  Iface
10.15.5.0       *           255.255.255.0   U      0       eth1
10.15.6.0       *           255.255.255.0   U      0       eth0
por defecto     10.15.6.1   0.0.0.0         UG     0       eth0
```

Figura 3.9: Cuando no existe una ruta explícita para un destino particular, un anfitrión usa la entrada de la pasarela por defecto en su tabla de enrutamiento.

Traducción de Direcciones de Red (NAT)

Para contactar con los anfitriones en la Internet, las direcciones RFC1918 deben convertirse en direcciones IP globales, enrutables. Esto se logra por medio de una técnica que se llama ***Traducción de Direcciones de Red—Network Address Translation***, o ***NAT***. Un dispositivo NAT es un enrutador que manipula las direcciones de paquetes en lugar de simplemente remitirlas. En un enrutador NAT, la conexión a Internet usa una (o más) direcciones IP enrutadas globalmente, mientras que la red privada usa una dirección IP del rango de las direcciones privadas del RFC1918. El enrutador NAT permite que la/las direcciones IP sean compartidas con todos los usuarios internos, que usan todos direcciones privadas. Convierte los paquetes desde una forma de direcciones a otra, a medida que los paquetes se transmiten. Desde la perspectiva de los usuarios/as, estos/as van a estar directamente conectados a Internet sin necesidad de software o *drivers* especiales. Simplemente usan el enrutador NAT como la pasarela por defecto, y direccionan los paquetes, como lo harían normalmente. El enrutador NAT traduce los paquetes dirigidos hacia afuera para que puedan usar las direcciones IP globales a medida que salen de la red, y los vuelve a traducir cuando se reciben desde Internet.

La consecuencia más importante cuando se usa NAT es que las máquinas desde Internet no pueden contactar con servidores dentro de la organización sin fijar reglas explícitas de envío en el enrutador. Las conexiones iniciadas desde el interior del espacio privado de dirección generalmente no presentan problemas, sin embargo, ciertas aplicaciones (tales como Voz sobre IP y cierto software para VPN) pueden tener dificultades con el uso de NAT.

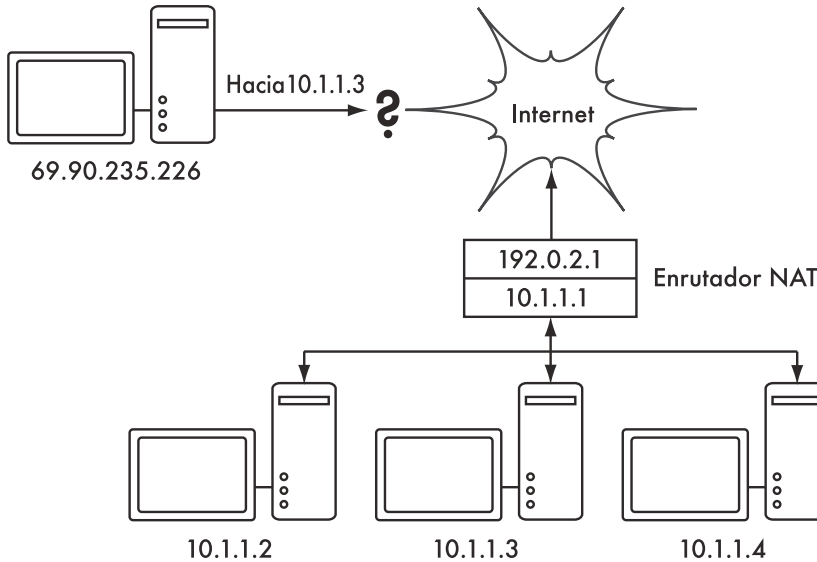


Figura 3.10: La Traducción de Direcciones de Red le permite compartir una sola dirección IP con muchos anfitriones internos, pero puede interferir con el funcionamiento apropiado de algunos servicios.

Dependiendo de su punto de vista, esto puede ser considerado un problema (puesto que hace que sea más difícil establecer una comunicación bidireccional), o una característica ventajosa, puesto que en realidad le proporciona un cortafuego "gratis" a toda la organización. Las direcciones RFC1918 deberían filtrarse en el borde de su red para evitar que tráfico RFC1918, de manera accidental, o malintencionada, entre o salga de su red. Mientras que NAT realiza algunas funciones de cortafuego, no es nunca un sustituto de uno verdadero.

Conjunto de Protocolos de Internet

Las máquinas en Internet usan el Protocolo de Internet (IP) para establecer contacto unas con otras, incluso cuando están separadas por múltiple máquinas intermediarias. Hay un conjunto de protocolos que se ejecutan conjuntamente con IP y que proporcionan características tan esenciales a las operaciones normales como el mismo protocolo IP. Cada paquete contiene un número de protocolo que identifica el protocolo utilizado. Los protocolos más comúnmente usados son el ***Transmission Control Protocol*** (***TCP***, número 6), el ***User Datagram Protol*** (***UDP***, número 17) y el ***Internet Control Message Protocol*** (***ICPM***, número 1). En conjunto, estos protocolos (y otros) se conocen como el ***Conjunto de Protocolos de Internet***, o simplemente ***TCP/IP***.

Los protocolos TCP y UDP introducen el concepto de número de puerto. Los números de puerto permiten que se ejecuten múltiples servicios bajo la misma dirección IP y que todavía se distingan unos de otros. Cada paquete tiene un número de puerto de procedencia y de destino. Algunos números de puerto son estándares bien definidos que se usan para acceder a servicios bien conocidos, tales como servidores de correo electrónico y web. Por ejemplo, los servidores

web normalmente ***escuchan*** TCP en el puerto 80, y los servidores de correo electrónico SMTP escuchan TCP en el puerto 25. Cuando decimos que un determinado servicio "escucha" en un puerto (como el 80), queremos decir que aceptará paquetes que usen su IP como dirección IP de destino, y 80 como el puerto de destino. A los servidores normalmente les es indiferente la IP de procedencia o el puerto de procedencia, sin embargo, a veces se valen de esta información para establecer la identidad de la otra parte. Cuando se envía una respuesta a estos paquetes, el servidor va a usar su propia IP como IP de procedencia, y 80 como puerto de procedencia.

Cuando un cliente se conecta a un servicio, puede usar de su lado cualquier número de puerto de procedencia que no esté en uso, pero debe conectar con el puerto apropiado del servidor (p. ej. 80 para web, 25 para correo electrónico). TCP es un protocolo ***orientado a sesión*** con características de transmisión y entrega garantizadas (tales como detección y minimización de congestión de la red, repetición de pruebas, reordenamiento y reensamblado de paquetes, etc). UDP está diseñado para flujo de información ***sin conexión***, y no garantiza entrega, ni ordenamientos específicos.

El protocolo ICMP está diseñado para depuración y mantenimiento de la Internet. En lugar de números de puerto, usa tipos de mensaje, que también son números. Diferentes tipos de mensaje se usan para solicitar una simple respuesta de otro computador (solicitud de eco), para notificar al remitente de otro paquete sobre un posible lazo de enrutamiento (se excede el tiempo previsto para la transmisión), o informarle al remitente que un paquete no ha podido enviarse debido a reglas de cortafuego u otros problemas (destino inalcanzable).

En este momento, usted debería tener un conocimiento sólido sobre cómo se direccionan los computadores en la red, y de cómo fluye la información entre ellos. Examinemos ahora brevemente el equipamiento físico que implementa estos protocolos de red.

Ethernet

Ethernet es el nombre del estándar más popular para conectar computadores en una ***Red de Área Local—Local Area Network*** (***LAN***). Se usa a menudo para conectar computadores individuales a Internet a través de un enrutador, módem ADSL, o dispositivo inalámbrico. Sin embargo, si usted conecta un solo computador a Internet, puede que no use Ethernet. Su nombre viene del concepto físico de "éter", el medio que se suponía, en otros tiempos, que transportaba las ondas luminosas a través del espacio libre. El estándar oficial se denomina IEEE 802.3.

El estándar Ethernet más común se llama 100baseT. Este define una tasa de datos de 100 megabits por segundo, sobre cable de par trenzado con conectores modulares RJ-45 en el extremo. La topología de red es una estrella con conmutadores y concentradores en el centro de cada estrella, y nodos finales en los extremos.

Direcciones MAC

Cada dispositivo conectado a una red Ethernet tiene una dirección MAC única asignada por el fabricante de la tarjeta de red. Su función se parece a la de

la dirección IP, puesto que sirve como un identificador único que les permite a los dispositivos "hablar" entre sí. Sin embargo, el alcance de una dirección MAC se limita al dominio de difusión que va a estar definido por todos los computadores unidos a través de cables, concentradores, conmutadores y puentes, pero sin atravesar enrutadores ni pasarelas de Internet. Las direcciones MAC nunca se usan directamente en la Internet y no son transmitidas entre enrutadores.

Concentradores (hubs)

Los concentradores Ethernet interconectan dispositivos Ethernet de par trenzado. Funcionan en la capa física (las más baja, la primera). Repiten las señales recibidas por cada puerto hacia el resto de los puertos. Los concentradores pueden, por lo tanto, ser considerados como simples repetidores. Debido a su diseño, sólo uno de los puertos transmite a la vez con éxito. Si dos dispositivos transmiten al mismo tiempo, las transmisiones se interfieren, y ambos se retiran para tratar de retransmitir los paquetes más tarde. A esto se le conoce como ***colisión***, y cada anfitrión es responsable de detectar las colisiones que se producen durante la transmisión, y de retransmitir sus propios paquetes cuando sea necesario.

Cuando en un puerto se detectan problemas como número excesivo de colisiones, algunos concentradores pueden desconectar (***segmentar o particionar)*** ese puerto por un tiempo para limitar su impacto en el resto de la red. Mientras un puerto está segmentado, los dispositivos conectados con ese puerto no pueden comunicarse con el resto de la red. Las redes basadas en concentradores son generalmente más robustas que el Ethernet coaxial (también conocido como 10base2, o ThinNet), donde un dispositivo con problemas puede incapacitar el segmento completo. Pero los concentradores están limitados respecto a su utilidad ya que pueden fácilmente convertirse en puntos de congestionamiento en redes de mucho tránsito.

Conmutadores

Un ***conmutador o switch*** es un dispositivo que funciona de manera muy parecida a un concentrador, pero proporciona una conexión dedicada entre puertos. En lugar de repetir todo el tráfico en cada puerto, el *conmutador* determina cuáles puertos se están comunicando directamente y los interconecta temporalmente. Los conmutadores proporcionan, en general, mejores prestaciones que los concentradores, especialmente en redes de mucho tráfico con numerosos computadores. No son mucho más caros que los concentradores y los reemplazan en muchas ocasiones.

Los conmutadores funcionan en la capa de enlace de datos (la segunda capa) puesto que interpretan y actúan sobre las direcciones MAC en los paquetes que reciben. Cuando un paquete llega a un puerto de un conmutador, éste determina la dirección MAC de procedencia, que está asociada a ese puerto. Luego almacena esta información en una ***tabla MAC*** interna, y transmite el paquete en el puerto que se corresponda. Si la dirección MAC de destino no aparece en la tabla MAC, el paquete se envía a todas las interfaces conectadas. Si el puerto de destino se corresponde con el puerto entrante, el paquete se filtra y no se remite.

Concentradores versus conmutadores

Los concentradores son considerados como dispositivos bastante elementales puesto que retransmiten de manera ineficiente todo el tráfico en cada puerto. Esta simplicidad acarrea a la vez un defecto de rendimiento y un problema de seguridad. El rendimiento general es más lento ya que el ancho de banda disponible debe compartirse entre todos los puertos. Y, puesto que todo el tráfico es "visto" por todos los puertos, cualquier anfitrión de la red puede fácilmente monitorizar todo el tráfico de red.

Los conmutadores crean conexiones virtuales entre los puertos receptores y transmisores. Esto genera una mejor prestación porque se pueden hacer muchas conexiones virtuales simultáneamente. Los conmutadores más costosos pueden cambiar el tráfico inspeccionando los paquetes a niveles más altos (en la capa de transporte, o en la de aplicación), permitir la creación de VLAN, e implementar otras características avanzadas.

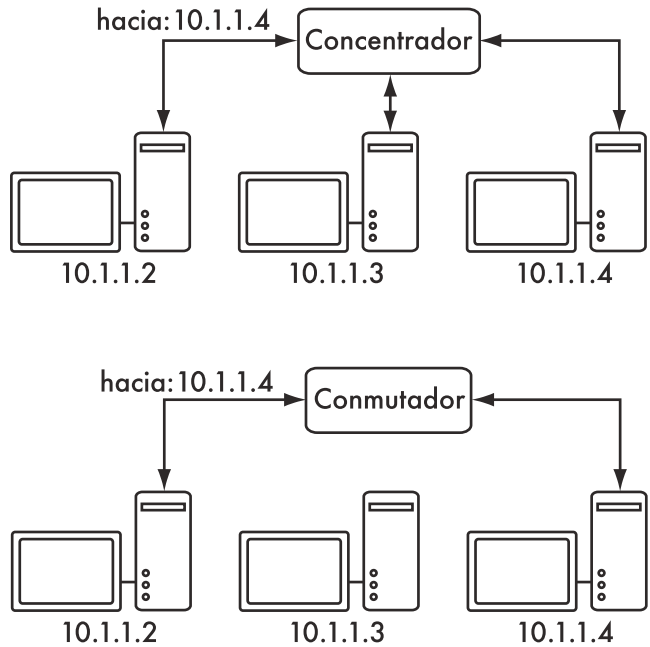


Figura 3.11: Un concentrador simplemente repite todo el tráfico en cada puerto, mientras que un conmutador establece una conexión dedicada temporal entre los puertos que necesitan comunicarse.

Un concentrador puede usarse cuando la repetición del tráfico en todos los puertos es deseable; por ejemplo, cuando usted quiere permitir explícitamente que una máquina monitora vea todo el tráfico de la red. La mayoría de los conmutadores tienen un ***puerto monitor***, que permite la repetición únicamente en un puerto designado específicamente para este propósito.

Los concentradores solían ser más económicos que los conmutadores. Sin embargo, el precio de los conmutadores ha bajado considerablemente con el

tiempo. Por lo tanto, las redes con concentradores deberían reemplazar estos con conmutadores, en la medida de lo posible.

Tanto los concentradores como los conmutadores pueden ofrecer *servicios administrados*. Algunos de estos servicios incluyen la capacidad de establecer la velocidad del enlace (10baseT, 100baseT, 1000basT, *full* o *half duplex*) por puerto, de permitir que se disparen alarmas cuando ocurren incidentes de red (como cambios en las direcciones MAC, o paquetes malformados), y normalmente incluyen ***contadores de puerto*** para facilitar la generación de informes sobre ancho de banda. Un conmutador administrado que proporciona conteo de bytes de carga y descarga para cada puerto físico, puede simplificar mucho la tarea de monitorizar la red. Estos servicios están normalmente disponibles por SNMP, o se puede acceder a ellos por telnet, ssh, una interfaz web, o una herramienta especial de configuración.

Enrutadores y cortafuegos

Mientras que los concentradores y los conmutadores proporcionan conectividad para un segmento de una red local, el trabajo de un enrutador es el de remitir paquetes entre diferentes segmentos de la red. Un enrutador normalmente tiene dos o más interfaces físicas de red. Puede incluir respaldo para diferentes tipos de medios de red tales como Ethernet, ATM, DSL, o discado (*dial-up*). Los enrutadores pueden ser dispositivos dedicados de *hardware* (como los enrutadores Cisco o Juniper), o pueden construirse a partir de un PC estándar con múltiples tarjetas de red y software apropiado.

Los enrutadores se encuentran en el ***borde*** de dos o más redes. Por definición, tienen una conexión con cada red, y en tanto máquinas de borde pueden asumir otras responsabilidades además del enrutamiento. Muchos enrutadores tienen capacidad de cortafuego que proporciona un mecanismo para filtrar o redirigir paquetes que no cumplen con las exigencias de seguridad o de políticas de acceso. También pueden suministrar servicios de Traducción de Direcciones de Red (NAT).

Los enrutadores varían considerablemente en precios y prestaciones. Los más económicos y menos versátiles son dispositivos simples de hardware dedicado, a menudo con función de NAT utilizada para compartir una conexión a Internet entre pocos computadores. El siguiente nivel es un enrutador de software, que consiste en un sistema operativo que opera en un PC estándar con múltiples interfaces de red. Los sistemas operativos estándares como Microsoft Windows, Linux y BSD tienen, todos ellos, la capacidad de enrutar, y son mucho más versátiles que los dispositivos de hardware más baratos. Sin embargo, presentan el mismo problema que las PC convencionales: alto consumo de energía, gran número de piezas muy complejas y poco confiables y configuración más engorrosa.

Los dispositivos más costosos son enrutadores *high-end* de hardware dedicado, fabricados por compañías como Cisco y Juniper. Usualmente ofrecen mejor rendimiento, más características, y mayor confiabilidad que el software de enrutamiento de las PC. También es posible comprar apoyo técnico y contratos de mantenimiento para estos dispositivos.

La mayor parte de los enrutadores modernos ofrecen posibilidades de monitorizar y grabar remotamente el rendimiento, normalmente a través de SNMP—*Simple Network Managment Protocol*. Sin embargo, algunos de los dispositivos más sencillos no tienen esta característica.

Otros equipamientos

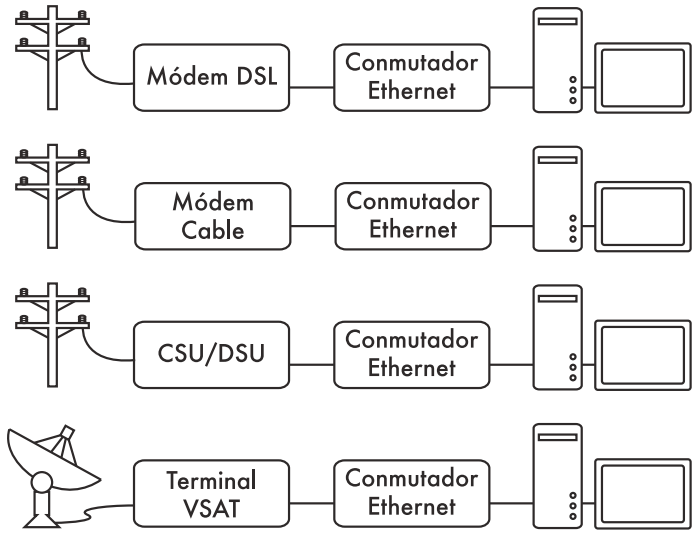


Figura 3.12: Muchos módems DSL, módems para cable, CSU / DSU, puntos de acceso inalámbricos, y terminales VSAT, terminan en un jack Ethernet

.

Cada red física tiene una pieza asociada de equipo terminal. Por ejemplo, las conexiones VSAT consisten en una antena parabólica conectada a un terminal que, o bien va enchufado a una tarjeta dentro de la PC, o termina en una conexión Ethernet estándar. Las líneas DSL utilizan un ***módem DSL*** que hace puente entre la línea telefónica y un dispositivo local, sea una red Ethernet, o un único computador a través de USB. Los ***cable modems*** hacen puente entre el cable de televisión y Ethernet, o un bus PC Card interno. Algunos tipos de circuito telecom (como un T1, o un T3) usan un CSU / DSU para hacer puente entre el circuito y un puerto serial o Ethernet. Las líneas estándares de discado usan módems para conectar el computador al teléfono, normalmente a través de una tarjeta de enchufar, o de un puerto serial. Y también hay diferentes tipos de equipo de red inalámbrico que conectan con una variedad de radios y antenas, pero casi todos terminan en un jack Ethernet.

La funcionalidad de estos dispositivos puede variar significativamente de acuerdo con el fabricante. Algunos proporcionan mecanismos de monitorizar el rendimiento, mientras que otros no. Puesto que su conexión a Internet, en última instancia procede de su ISP, usted debería seguir sus recomendaciones en lo que respecta a la selección de equipos que hagan puente entre la red de su ISP y su propia red Ethernet.

Ensamblar todas las partes

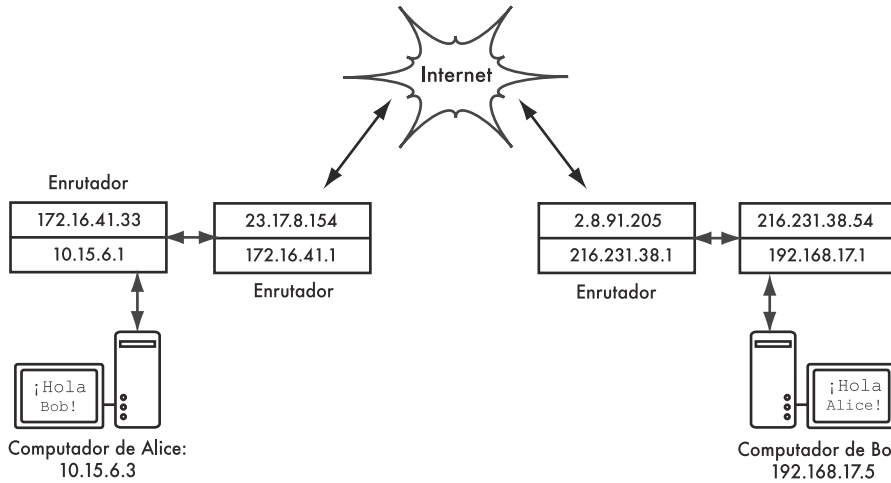


Figura 3.13: Redes Internet. Cada segmento de la red tiene un enrutador con dos direcciones IP, y realiza un "enlace-local" con dos redes diferentes. Los paquetes son remitidos entre enrutadores hasta que alcanzan su destino final.

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.

En el ejemplo de 3.13 se puede ver el camino que toman los paquetes cuando Alicia habla con Bob utilizando un servicio de mensajería instantánea. Cada flecha 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 remitan 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.

Diseño de 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 en que usted pueda alcanzar a sus clientes inalámbricos? Sea que deba llegar hasta una oficina en un edificio o extenderse

a lo largo de muchos kilómetros, las redes inalámbricas se organizan naturalmente en estas tres configuraciones lógicas: ***enlaces punto a punto***, ***enlaces punto a multipunto***, y ***nubes multipunto a multipunto***. Si bien las diferentes partes de su red pueden aprovechar las tres configuraciones, los enlaces individuales van a estar dentro de una de esas topologías.

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 a ella. Por ejemplo, una universidad puede tener una conexión *Frame Relay* rápida, o una conexión VSAT dentro del campus, pero difícilmente podrá justificar otra conexión de la misma índole para un edificio importante fuera del campus. Si el edificio principal tiene una visión libre de obstáculos al lugar remoto, una conexión punto a punto puede ser utilizada para unirlos. Ésta puede complementar o incluso remplazar enlaces de discado existentes. Con antenas apropiadas y existiendo línea visual, se pueden hacer enlaces punto a punto confiables de más de cien kilómetros.

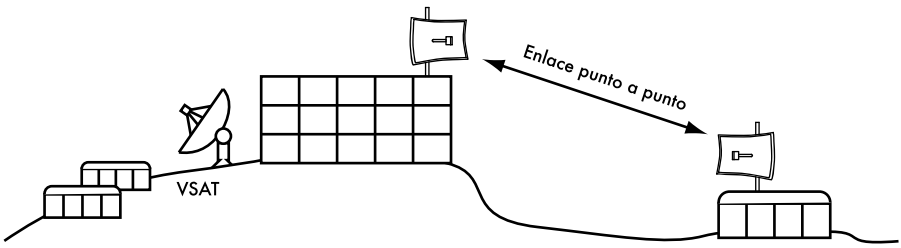


Figura 3.14: Un enlace punto a punto le permite a un lugar remoto compartir una conexión central a Internet.

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

Los enlaces punto a punto no necesariamente tienen que estar relacionados con el acceso a Internet. Supongamos que usted debe desplazarse hasta una estación meteorológica 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 red ***punto a multipunto***. Cada vez que tenemos varios nodos[2] hablando con un punto de acceso central estamos en presencia de una aplicación punto a multipunto. El ejemplo típico de un trazado punto a multipunto es el uso de un ***punto de acceso*** (***Access Point***) 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.

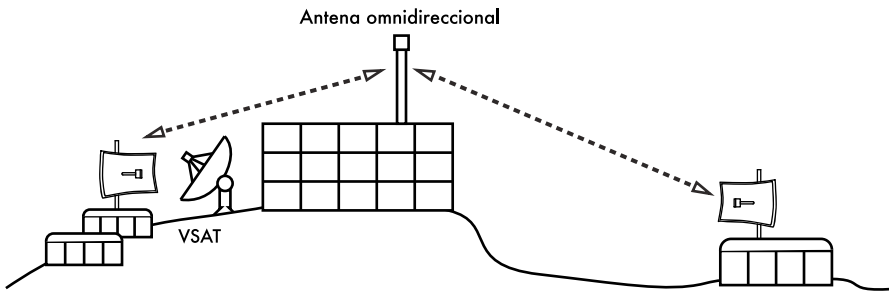


Figura 3.15: La conexión VSAT central es compartida por múltiples sitios remotos. Estos tres lugares también pueden comunicarse directamente entre sí a velocidades mucho más rápidas que las ofrecidas por VSAT.

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 la 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 enlaces 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

2. 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.

tráfico de tantos otros como sea necesario, y todos los nodos se comunican directamente entre sí.

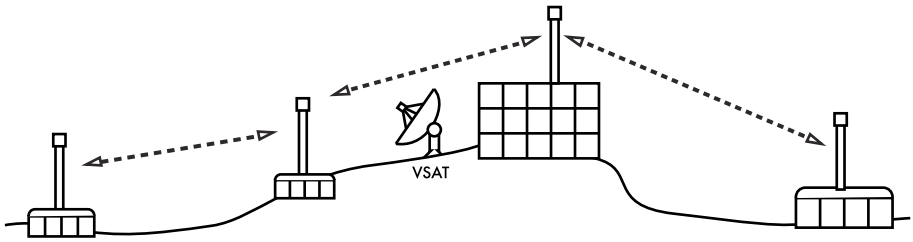


Figura 3.16: Una red en malla (mesh) multipunto a multipunto. Cada punto puede acceder a otro a gran velocidad, o utilizar la conexión central VSAT para acceder a Internet.

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 redes multipunto a multipunto generalmente no tienen la misma capacidad que las redes punto a punto, o las punto a multipunto, debido a la sobrecarga adicional de administrar el enrutamiento de la red y el 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 pueden suplementarse con técnicas tradicionales de redes cableadas. 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 difunda 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.

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 2**, esto significa que los radios 802.11a se comunican con otro radio 802.11a en frecuencias de 5 GHz, y que los radios 802.11b/g hablan con otros 802.11b/g en 2,4 GHz, 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 a 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***) es utilizado 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 6**) 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.

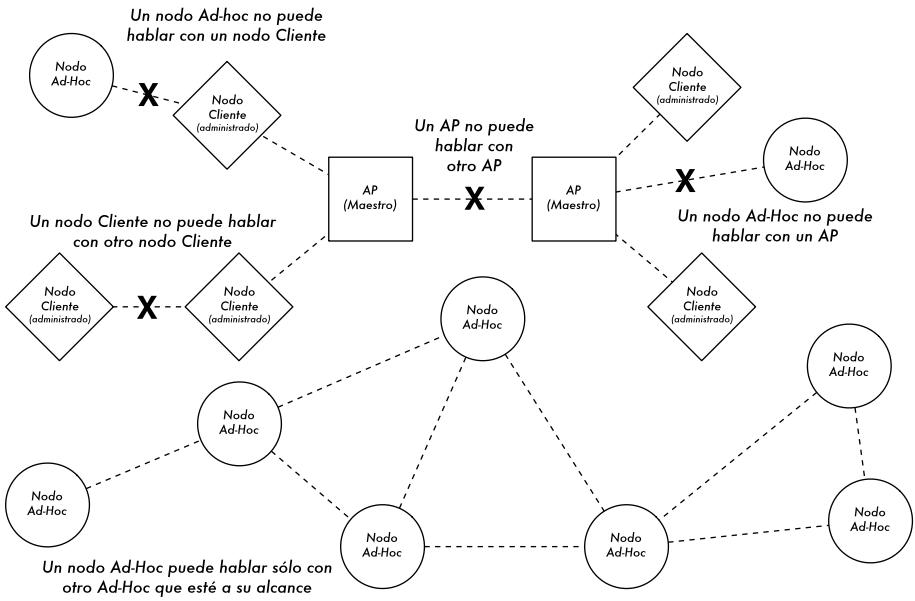


Figura 3.17: AP, clientes, y nodos Ad-Hoc.

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.

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.

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 varios kilómetros 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.

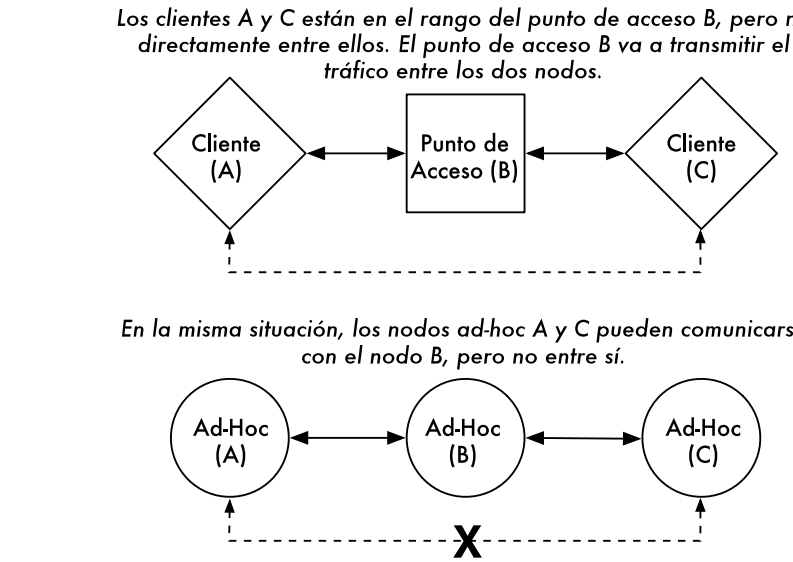


Figura 3.18: El punto de acceso B va a transmitir el tráfico entre los clientes A y C. En el modo Ad-Hoc, el nodo B no va a transmitir el tráfico entre A y C por defecto.

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.

Los nodos *ad-hoc* no repiten datos por defecto, 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 crítico 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 pero 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 casi no se encuentran en el mundo real. Los nodos pueden fallar, los dispositivos WiFi pueden desorientarse, y la interferencia puede hacer que los radio enlaces estén inutilizados en cualquier momento. Además, nadie quiere actualizar varias tablas de enrutamiento a mano cada vez que 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 Optimizado) 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 (*open-source*) que admite Mac OS X, Windows 98, 2000, XP, Linux, FreeBSD, OpenBSD y NetBSD. **Olsrd** está disponible para puntos de acceso que ejecutan Linux, como Linksys WRT54G, Asus WI500g, AccessCube, o Pocket PC que ejecutan Linux Familiar, y viene incluido en los equipos Metrix que ejecutan Metrix Pyramid. Olsrd puede manejar interfaces múltiples y puede extenderse con diferentes *plug-ins*. Admite 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 con el

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 concordancia con otras implementaciones.

Teoría

Después de haber ejecutado 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 600 interfaces. El promedio de carga del CPU causada por olsrd en un Linksys WRT54G funcionando 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 que depende de cuántas interfaces estén involucradas y cuán a menudo se actualicen 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 ejecuta 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 transmisores 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 son transmisores 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 Pyramid. Si 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* tenga 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 desde 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 ejecutando el demonio OLSR puede funcionar bastante bien para este propósito. No existe una manera sencilla de automatizar el proceso cuando se utilza 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 sean las mismas en todos lados. Olsrd puede hacer esto por sí mismo. Cuando se establece un archivo de configuración olsrd por defecto, esta característica debe ser habilitada para eliminar confusiones del tipo “¿por qué los otros nodos no pueden ver mi máquina?"

Configuremos 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 haya 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 use el mismo canal inalámbrico, el mismo nombre de red inalámbrica ESSID (Extended Service Set IDentifier) y de que tenga 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 celda. 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 esté 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 transmitir. Si bien implica una sobrecarga, en un medio ambiente ruidoso, esto reduce la penalización por los errores y les permite a los paquetes afrontar 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 encuentre y utilice las interfaces sobre las cuales debe trabajar.

Para Mac OS-X y Windows se dispone de una buena guía para configurar y monitorizar el 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 comprobadas.

```
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 ejecutarlo con la opción de depuración -d 2, especialmente la primera vez. Puede ver qué es lo que hace olsrd y monitorizar cómo están funcionando los enlaces con 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
```

Uso de OLSR en Ethernet y en interfaces múltiples

No es necesario tener una interfaz inalámbrica para probar o utilizar olsrd, aunque fue diseñado para estas. 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 estén 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 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 que todavía les funcione. De hecho, la idea de tener un protocolo que haga 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 revisar el sitio web *olsr.org*. Aquí hay unas instrucciones resumidas para la aplicación de visualización de la topología de la red olsrd_dot_draw.

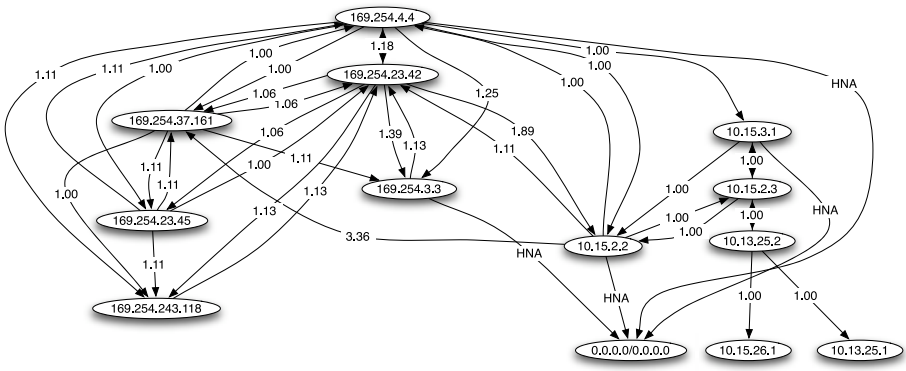


Figura 3.19: Una topología de red OLSR generada automáticamente.

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.

Para 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 defecto. El parámetro "port" especifica el puerto TCP.

Luego reinicie olsr y compruebe 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 ejecutar 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 ejecutar el programa con **./olsr-topology-view.pl** y visualizar la topología actualizada casi en tiempo real.

Resolución de problemas

Siempre y cuando las tarjetas WiFi puedan "verse" directamente con sus radios, la herramienta "*ping*" funcionará, esté o no funcionando olsrd. 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 comprobado 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 revisarse 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 caudal real significativamente mayor que las conexiones tradicionales a Internet, tales como VSAT, discado, o DSL. El caudal también se denomina ***capacidad del canal***, o simplemente ***ancho de banda*** (aunque este término no es diferente al 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 caudal que va a observar el usuario. Como mencionamos antes, un enlace 802.11g puede transmitir a 54 Mbps en el radio, pero el caudal real será de unos 22 Mbps. El resto es la tara (*overhead*) que necesitan los radios 802.11g para coordinar sus señales.

El caudal es una medida de bits por unidad de tiempo. 22 Mbps 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 les 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 si se incrementa la demora.

¿Cuánto caudal van a necesitar sus usuarios realmente? Esto depende de cuántos usuarios haya, y de cómo usan su enlace inalámbrico. Las diversas aplicaciones de Internet requieren diferentes caudales.

Para estimar el caudal necesario para su red, multiplique el número esperado de usuarios por el tipo de aplicación que probablemente vayan a usar. Por ejemplo, 50 usuarios principalmente navegando en la web, en los momentos pico van a consumir un caudal entre 2,5 a 5 Mbps o más, y toleran algo de latencia. Por otro lado, 50 usuarios simultáneos de VoIP van a requerir un caudal de 5 Mbps o más **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 caudal requerido, hasta un total de 10 Mbps. Sus enlaces deben proveer esa capacidad, o las conversaciones van a tener demora.

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 a 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.

Aplicación	Ancho de Banda/ Usuario	Notas
Flujo de audio (*streaming)*	96 - 160 kbps	Cada usuario de un servicio de flujo de audio va a utilizar una cantidad constante de un ancho de banda relativamente grande durante el tiempo que esté activo. Puede tolerar algo de latencia pasajera mediante la utilización de mucha memoria de almacenamiento temporal en el cliente (*buffer*). Pero los períodos de espera prolongados van a hacer que el audio "salte" o que se den fallos en la sesión.
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 superado 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 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 (*bandwidth shaper*) adecuado.

Ya que es poco probable que todos sus usuarios utilicen la conexión precisamente en el mismo momento, una práctica normal es la de ***sobresuscribir*** el caudal disponible por algún factor (esto es, permitir más usuarios de los que el máximo de ancho de banda disponible puede admitir). 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/a al monitorizar el 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 web (*caching*), 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 caudal 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 comprende 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 una potencia por encima de cierto mínimo. El proceso de determinar si el enlace es viable se denomina cálculo del ***presupuesto de potencia***. El 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, denominado ***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 30 mW a 600 mW, 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 ayudar. 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 entre 19 y 32 dBi, las antenas omnidireccionales de 5-17 dBi, y las antenas sectoriales tienen una ganancia de 12-19 dBi.

- **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 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 que sean lo más corto 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:

$$L_{fsl} = 40 + 20*\log(r)$$

Donde L_{fsl} (pérdida de señal en el espacio libre, (*Free Space Loss*, 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 esté 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 que la señal reflejada tiene un trayecto más largo, llega a la antena receptora más tarde que la señal directa. Este efecto es denominado ***multitrayectoria***, desvanecimiento, o dispersión de la señal. En algunos casos las señales reflejadas se añaden y no causan problemas. Cuando se suman en contrafase, la señal recibida es muy baja llegando inclusive a anularse por las señales reflejadas. Este fenómeno es conocido como ***anulación***. Existe una técnica simple utilizada para tratar con la multitrayectoria, llamada ***diversidad de antena***. Consiste en agregar una segunda antena al radio. De hecho, la multitrayectoria es un fenómeno muy localizado. Si dos señales se suman fuera de fase en una determinada ubicación, no lo harán en otra ubicación 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. Los equipos más modernos usan varias cadenas independientes de transmisión, cada una conectada a su propia antena y la correspondiente configuración en el receptor, en lo que se conoce como ***MIMO*** (***Multiple Input, Multiple Output***), lo que consigue mejorar notablemente el caudal neto recibido. Esta es una de las tecnologías utilizadas en el estándar IEEE 802.11n. La distorsión generada por la multitrayectoria 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 para el cálculo de la pérdida en el trayecto es cambiar el exponente del factor 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 considerar 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 del 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 lo suficientemente potente como para que los radios la utilicen. Recuerde que el RSL mínimo se expresa siempre en dBm negativos, por lo tanto -56 dBm es mayor que -70 dBm. 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 la multitrayectoria en la señal de radio recibida, se debe tener un margen de 20 dB.

Una vez que haya 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 recibida en el primer radio.

Ejemplo de cálculo del presupuesto del enlace

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

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

Restamos la pérdida en el trayecto de la ganancia total:

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

Ya que -73dBm es mayor que la sensibilidad del receptor del cliente (-82 dBm), el nivel de señal es justo el suficiente para que el cliente sea capaz de oír al punto de acceso. Solamente hay 9 dB de margen (82 dB–73 dB) 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 1)
 ————————————————————————————————————————
  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 dBm
```

Si la sensibilidad de recepción del AP es -89 dBm, nos deja un margen de desvanecimiento de 11dB (89 dB–78 dB). En general este enlace probablemente va a funcionar pero podría utilizar un poco más de ganancia. Si usamos una antena de 24 dBi en el lado del cliente en lugar de una antena sectorial de 14 dBi, vamos a tener una ganancia adicional de 10 dBi 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, 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*—Paquete Profesional de Análisis de Enlaces de Redes Inalámbricas de Radio de Green Bay—es una excelente herramienta: (*http://my.athenet.net/~multiplx/cgi-bin/wireless.main.cgi*). 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 2,4 GHz

Distancia (m)	100	500	1000	3000	5000	10000
Pérdida (dB)	80	94	100	110	113	120

Para más información sobre distancias en el espacio libre, vea el **Apéndice C**.

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 del 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 que tiene utilidades interactivas en línea para diseño de redes, y Radio Mobile.

Herramientas CGI para Diseño interactivo

El grupo Profesional de Radio Paquete 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 están 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. Se encuentra 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 11 MHz 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. Pulse el botón de aceptar para obtener un informe 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 informe 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 funciona con Windows, pero puede utilizarse en Linux con el emulador Wine.

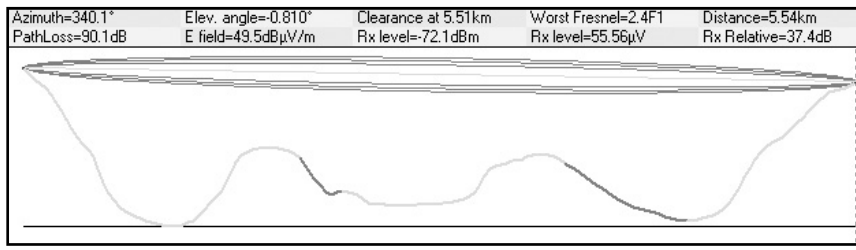


Figura 3.20: Viabilidad del enlace, incluye estimación de la zona de Fresnel y de la existencia de línea visual, utilizando Radio Mobile.

Radio ***Mobile*** usa el ***modelo digital de elevación del terreno*** para el cálculo de la cobertura, e 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 comprueba la línea visual y calcula la Pérdida en el Espacio Libre, 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. 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 100 kHz a 200 GHz. Los ***Mapas de elevación digital (Digital Elevation Maps—DEM***, por su sigla en inglés) están disponibles gratuitamente desde variadas fuentes y para la mayor parte del mundo. Los DEM no muestran las líneas costeras u otras fronteras identificables, pero pueden combinarse fácilmente con otro tipo de datos (como fotos aéreas, cartas topográficas y las imágenes satelitales de Google Earth y otras) en varias capas para obtener una representación más útil y rápidamente reconocible. Incluso puede digitalizar sus propios mapas y combinarlos con DEM. Los mapas de elevación digitales pueden combinarse con mapas escaneados, fotos satelitales y servicios de mapas de Internet (tales como Mapquest) para producir predicciones precisas de cobertura.

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 x 31
- 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 un terminal con el comando:

```
# wine RMWDLX.exe
```

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

Cómo evitar 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 analógicos de video, *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 2,4 GHz. Esas señales, así como las de 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 antenas de alta ganancia que están enfocadas entre sí, rechazarán el ruido desde direcciones aledañas. Si utilizamos antenas omnidireccionales recibiremos ruido de todas las direcciones.

- **Utilice antenas sectoriales en lugar de omnidireccionales**. Haciendo uso de varias antenas sectoriales puede reducir el ruido global recibido en un punto de distribución (**AP**). Si traslapa los canales utilizados en cada antena sectorial, también puede incrementar el ancho de banda disponible para sus clientes.
- **No utilice un amplificador**. Como veremos en el **Capítulo 4**, 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.

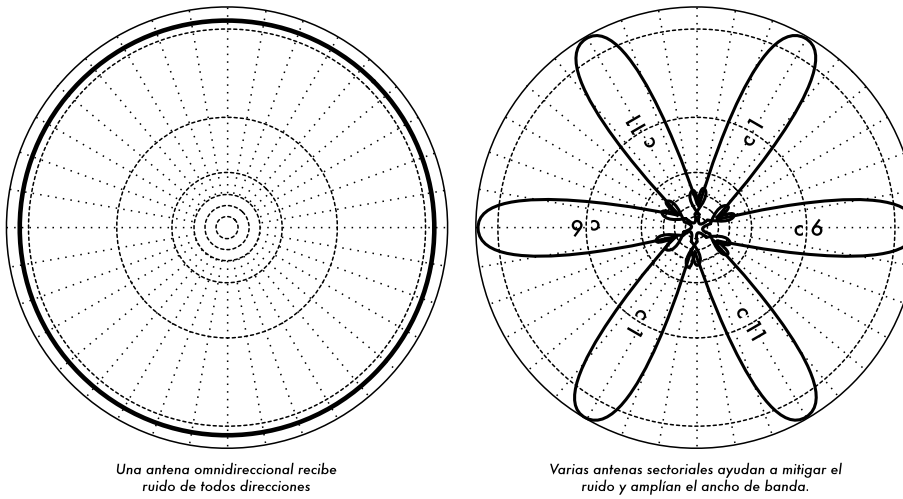


Figura 3.21: Una sola antena omnidireccional versus múltiples antenas sectoriales.

- **Utilice el mejor canal disponible**. Recuerde que los canales 802.11b/g tienen un ancho de 22 MHz, pero están separados sólo por 5 MHz. Realice una prospección del sitio, 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 repente su enlace presenta 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 factible crear un enlace de 12 km 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 5,8G Hz, 900 MHz, u otra banda sin licenciamiento**. Si bien esta es una solución a corto plazo, actualmente la mayor parte del equipamiento instalado utiliza 2,4 GHz. Utilizar 802.11a, o un dispositivo de convertidor de 2,4 GHz a 5,8 GHz le va a permitir eludir esta congestión. Si usted puede encontrarlo, existe equipamiento 802.11 viejo que usa el espectro sin licenciamiento a 900 MHz (desafortunadamente con una velocidad muy baja). 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 ocupado. 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 2,4 GHz. Vamos a ver algunos ejemplos de estas herramientas en el **Capítulo 6**.

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—*Line of Sight)*. 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 puede proveer energía, también pueden actuar como muy buenos ***repetidores***.

Los repetidores son nodos que están configurados para transmitir el tráfico no 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***), el caudal 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 bajo consumo 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.

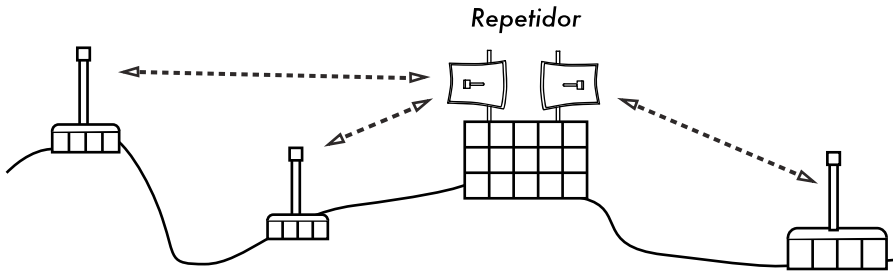


Figura 3.22: El repetidor remite los paquetes por el aire entre los nodos que no tienen línea visual directa.

En general, los repetidores son utilizados para evitar obstáculos en el camino de un enlace a larga distancia, como edificios en el camino; pero esos edificios contienen gente. A menudo podemos hacer acuerdos con los dueños de los edificios para proporcionarles 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.

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.

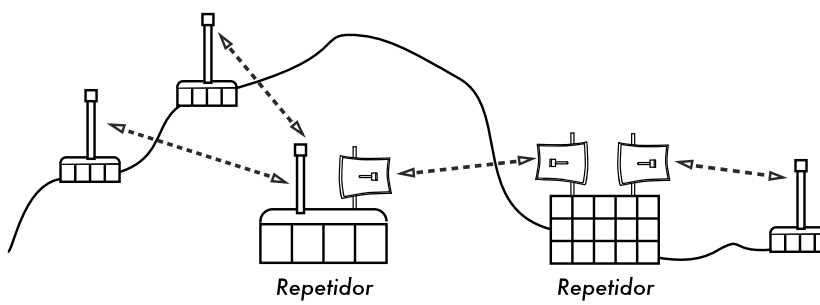


Figura 3.23: No había energía disponible en lo alto de la colina, pero fue circunvalada con el uso de múltiples repetidores ubicados alrededor de la base.

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.

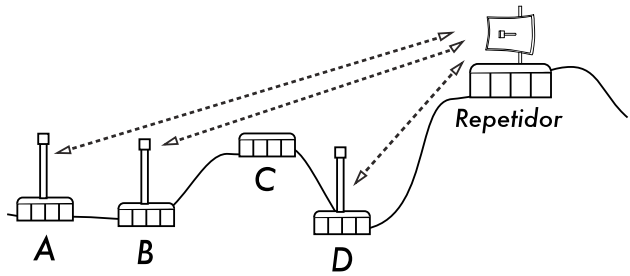


Figura 3.24: El lugar D no puede ver al lugar A o el B, porque el lugar C está en el camino y no está interesado en tener un nodo. Al instalar un repetidor en un lugar alto, los nodos A, B, y D se pueden comunicar. El tráfico desde el nodo D en realidad viaja más lejos que el del resto de la red antes 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 esté 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 el 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 esté transportando el tráfico que debe y no otro.

Almacenamiento Web temporal (Web caching)

Un servidor web *proxy* es un servidor en la red local que mantiene copias de lo que ha sido 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 a la 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, pueden interpretarlo como que el servidor proxy está haciendo las cosas 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 modificado (por ejemplo, añadiendo filtros de contenido y bloqueos de publicidad). Squid produce bitácoras (*logs*) que pueden ser analizadas utilizando software como Awstats, o Webalizer, que son de fuente libre y producen buenos informes 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 informes 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 defecto 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 previa (*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/*

Cómo evitar 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 las *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 midan qué tan susceptibles son sus redes a estas técnicas.

Para reforzar el uso del almacenamiento temporal *proxy* (*caching proxy*), usted puede simplemente considerar 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*.

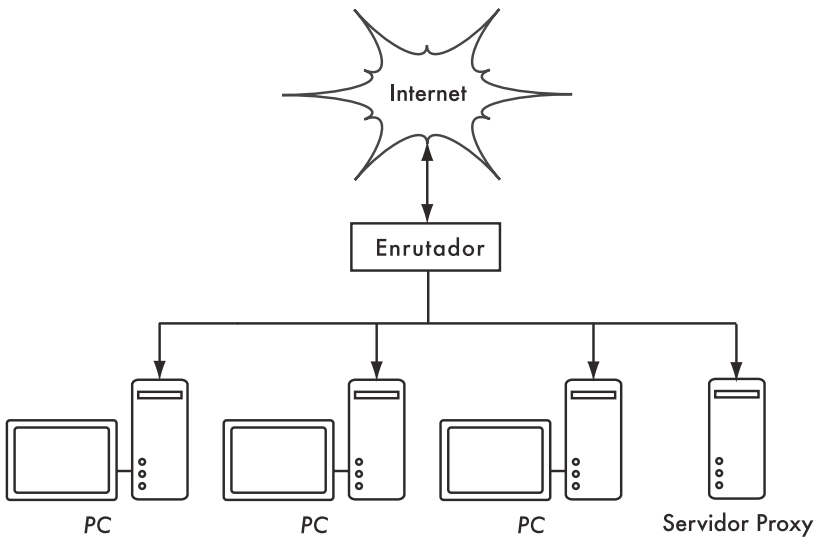


Figura 3.25: Esta red se basa en la confianza de que los usuarios van a configurar apropiadamente sus PC para utilizar el servidor proxy.

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

- **No divulgar la dirección de la pasarela por defecto** (***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 defecto**. 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 conozca 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/a administrador/a de red. La única forma de asegurar 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 asegurar 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 la **Figura 3.26**.

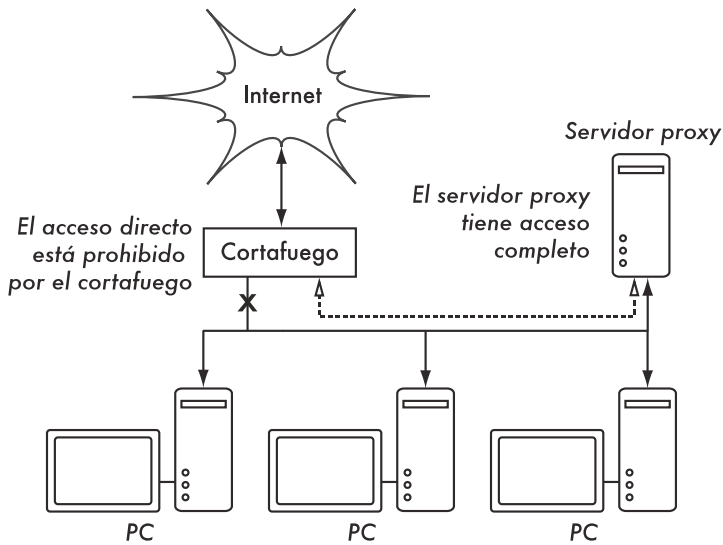


Figura 3.26: El cortafuego les impide a los PC acceder a Internet directamente, pero les permite el acceso por el servidor proxy.

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 consumidores de ancho de banda como Bit Torrent, o 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*.

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

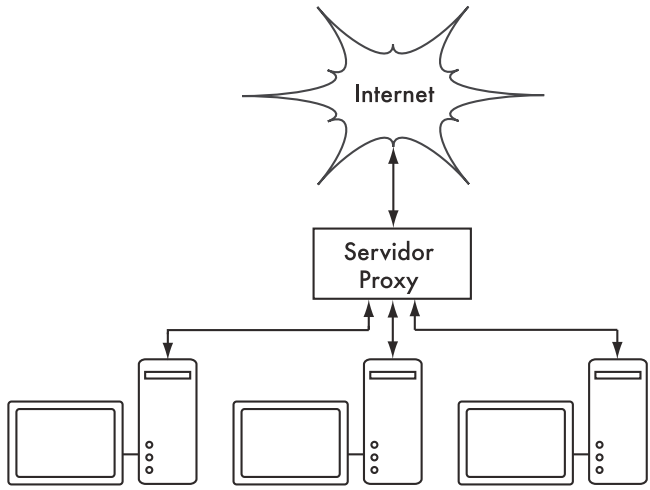


Figura 3.27: La única ruta hacia Internet es a través del proxy.

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 admiten 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/a o del/la administrador/a del sitio web, el sitio completo puede ser copiado durante la noche al servidor local, siempre que el mismo no sea demasiado grande. Esto se debe tener en cuenta para sitios web importantes, que son de interés particular para la organización, o 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 necesita 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 ejecuta ***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 ejecutando 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 funcione 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 temporal (*caching*) del servidor DNS acelera los tiempos de respuesta web).

Pre-poblar la memoria caché 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 caché 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*) 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 caché del proxy como si un cliente hubiera accedido a esa página. Cuando un cliente accede a la página recuperada, le es brindada desde el caché y no desde el enlace internacional congestionado. Este proceso puede ser implementado 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 ejecutarse en la noche, 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
```

Estas opciones permiten lo siguiente:

- **-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 de que wget haga uso del servidor *proxy*. Esto puede no necesitarse en aplicaciones donde se utiliza un servidor *proxy* transparente.
- **--c cache-off**: Se asegura de que el contenido nuevo sea recuperado desde Internet, y no desde el servidor *proxy* local.
- **--delete after**: Borra la copia duplicada. El contenido duplicado permanece en el caché 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 requieran. Cuando utilizamos esta herramienta, Squid debe ser configurado con suficiente espacio en el disco para que contenga todos los sitios pre-poblados y otros (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 caché

Cuando una organización tiene más de un servidor proxy, los mismos pueden compartir información caché entre ellos. Por ejemplo, si una página web está en el caché del servidor A, pero no en el caché del servidor B, un usuario conectado a través del servidor B puede acceder a la página web en el servidor A por el servidor B. El ***Protocolo de Inter-caché*** (***Inter-caché Protocol***, ***ICP***) y el ***Caché Array Routing Protocol***, ***CARP*** pueden compartir información de la caché. De éstos, el protocolo CARP es considerado el mejor. Squid admite ambos protocolos, y el Servidor MS ISA admite CARP. Para más información diríjase a: *http://squiddocs.sourceforge.net/latest/html/c2075.html*. El compartir información caché 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 a la *caché*. Las prestaciones del disco son importantes, por lo que los discos SCSI más rápidos se van a desempeñar mejor (aunque una *caché* basado en un IDE es mejor que nada). Ni RAID (Redundant Array of Independt Disks), ni el uso de espejos (*mirror*) son recomendados.

Se aconseja dedicar un disco exclusivamente para la *caché*. Por ejemplo, un disco puede ser para la *caché*, y el segundo para el sistema operativo y la bitácora de la caché. 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 la red de un campus, la memoria RAM debe ser de 1 GB o más:

- Además de la memoria requerida para el sistema operativo y otras aplicaciones, Squid necesita 10 MB de RAM por cada 1 GB de caché de disco. Por lo tanto, si tenemos un espacio de disco de 50 GB asignados a la caché, Squid va a necesitar 500 MB de memoria extra.
- La máquina también va a precisar 128 MB para Linux y 128 MB para Xwindows.
- 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 mantienen los datos de acceso frecuente en la memoria siempre que haya suficiente RAM disponible. Pero utilizan el archivo de página del disco duro como un área de memoria extra cuando no tienen suficiente memoria RAM.

Caché y optimización de DNS

Los servidores DNS con sólo la función de *caché* no son autoridades de ningún dominio, solo almacenan los resultados de solicitudes hechas 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 ***Time To Live***) expira. Esto va a reducir la cantidad de tráfico DNS en su conexión a Internet, porque la caché de DNS puede ser capaz de satisfacer muchas de las solicitudes localmente. Por supuesto que las computadoras de los clientes deben ser configuradas para utilizar *sólo* el *servidor de DNS caché* como su servidor DNS. Cuando todos los clientes utilicen ese servidor DNS como su servidor principal, se poblará rápidamente la caché de direcciones IP a nombres, de esta manera, los nombres solicitados previamente pueden ser resueltos de manera rápida. Los servidores DNS que son autoridades para un dominio también actúan como caché de la conversión nombres-direcciones de anftriones (*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 ejecutándose, va a actuar como un servidor caché (no se necesita más configuración). Bind puede ser instalado desde un paquete como el Debian, o un RPM. Instalarlo desde un paquete es, en general, el mejor método. En Debian, escriba:

```
apt-get install bind9
```

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

dnsmasq

Un servidor DNS de caché 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 caché *proxy* de DNS y como una fuente de autoridad para anfitriones (*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 a 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. En el artículo Knowledge Base 167234

se describe cómo configurar un servidor que sólo implementa caché en NT. Una cita del artículo:

> "*Simplemente instale DNS y ejecute el Sistema Administrador de Nombres de Dominio (Domain Name System Manager). Pulse DNS en el menú, seleccione Nuevo Servidor, y escriba la dirección IP de la computadora donde ha instalado DNS. Usted ahora tiene un servidor DNS sólo de caché*".

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 defecto), 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 caché 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 22 Mbps 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 el que le ofrece su enlace a Internet, y es capaz de admitir 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 defecto de TCP/IP. Optimizando su enlace VSAT, se pueden mejorar significativamente los tiempos de respuesta cuando se accede a *hosts* de Internet.

Factores que afectan 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 VSAT. La alta latencia en las redes por satélite se debe a la gran distancia del satélite y a 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 a través de fibra óptica.

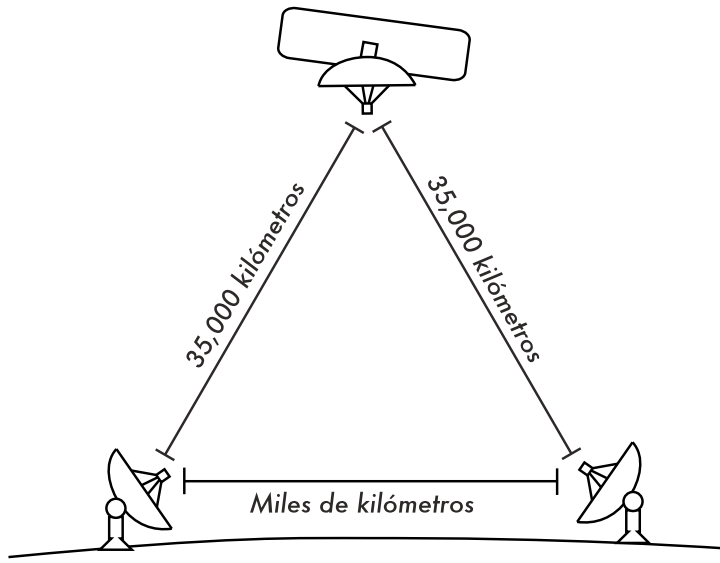


Figura 3.28: Debido a la velocidad de propagación finita y las largas distancias involucradas, la confirmación de recepción de un paquete ping puede tomar más de 520 ms en un enlace VSAT.

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

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

- La opción de **escalado de ventana**, para permitir 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 520 ms hasta el primer salto. TCP utiliza el mecanismo de comienzo lento (*slow start*) 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 después 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 elevados

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 host 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 buen 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 64 KB.

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 64 KB, teóricamente el máximo rendimiento que se puede conseguir vía satélite es (tamaño de la ventana) / RTT, ó 64 KB / 520 ms. Esto da una tasa de transferencia de datos máxima de 123 KB/s, correspondiente a 984 Kbps (1008246 bps), aunque la capacidad del enlace sea mucho mayor.

Cada encabezado de segmento TCP contiene un campo llamado ***ventana anunciada***, que especifica cuántos bytes de datos adicionales está el receptor preparado para aceptar. La ventana anunciada es el tamaño actual de la memoria de almacenamiento temporal 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 64 KB.

Para soslayar el problema de versiones de TCP/IP que no exceden el tamaño de la ventana de 64 KB, 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 y exige tres confirmaciones duplicadas (ACK), o ejecuta 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 Microsoft 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 admitan SACK.

Implicaciones para las universidades

Si un sitio tiene una conexión a Internet de 512 kbps, las configuraciones por defecto 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/la administrador/a 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/las administradores/as pueden considerar tomar algunas medidas para asegurarse de que estén 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 caché grande que tenga 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 actúa como proxy y realiza captura previa (*pre-fetching*) para acelerar todavía más el acceso al web.

Este sistema puede ser construido desde cero utilizando por ejemplo Squid, o adquiriendo soluciones prefabricadas (*off the shelf*) ofrecidas por varios vendedores.

Más información

Aunque la optimización del ancho de banda es un asunto complejo y a menudo difícil, las técnicas ofrecidas en este capítulo deberían ayudar a reducir las fuentes obvias de malgasto de ancho de banda. Para hacer el mejor uso posible del ancho de banda disponible, usted necesita definir buenas políticas de acceso, establecer herramientas confiables para analizar y monitorizar, e implementar una arquitectura de red que imponga límites deseables de uso.

Para más información sobre optimización de ancho de banda, vea el libro gratuito How to Accelerate your Internet (*http://bwmo.net*).

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 ***línea 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 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

1. Radio Frecuencia. Vea el Capítulo 2 para una discusión sobre las ondas electromagnéticas.

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”.

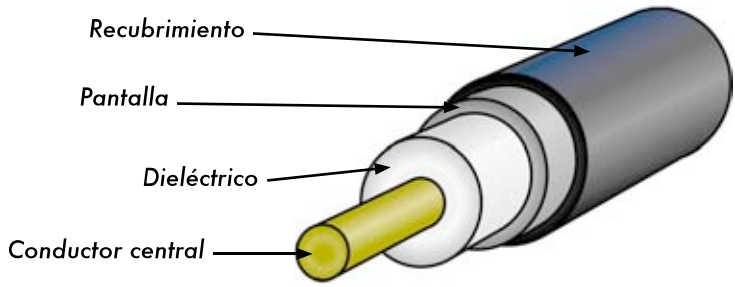


Figura 4.1: Cable coaxial con recubrimiento, pantalla, dieléctrico, y conductor central.

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, esto puede hacerse mediante la utilización de cables muy cortos y/o de buena calidad.

Aquí les presentamos algunos puntos que se deben 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].

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

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 permita verificar un cable hecho por usted mismo/a (como un analizador del 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.

Guías de Ondas

Arriba de los 2 GHz, la longitud de onda es lo suficientemente corta como para permitir una transferencia de energía práctica y eficiente por diferentes 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:

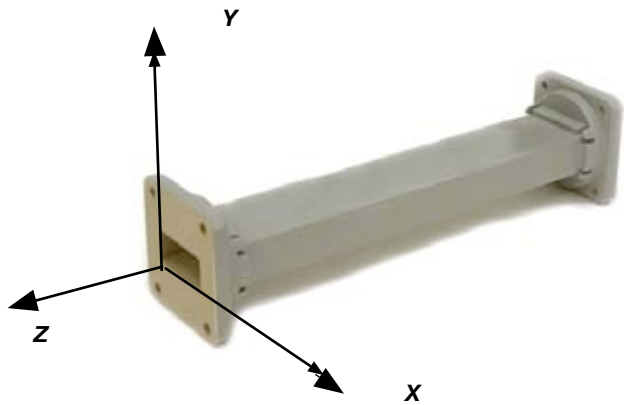


Figura 4.2: Las dimensiones X, Y, y Z de una guía de onda rectangular.

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 seguidas 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 presentan 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 12 GHz. Su sigla TNC se debe al 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 60s. 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 proporciona opciones a los diseñadores cuando el espacio físico es limitado. MCX tiene una capacidad de banda ancha de 6 GHz 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 hacerlo 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 2,4 GHz 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 sus 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:

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

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 ubicaciones 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 con referencia a una antena estándar. Las dos referencias más comunes son la ***antena isotrópica*** y la ***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 tridimensional, pero generalmente las mediciones de los mismos son una porción bidimensional 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.

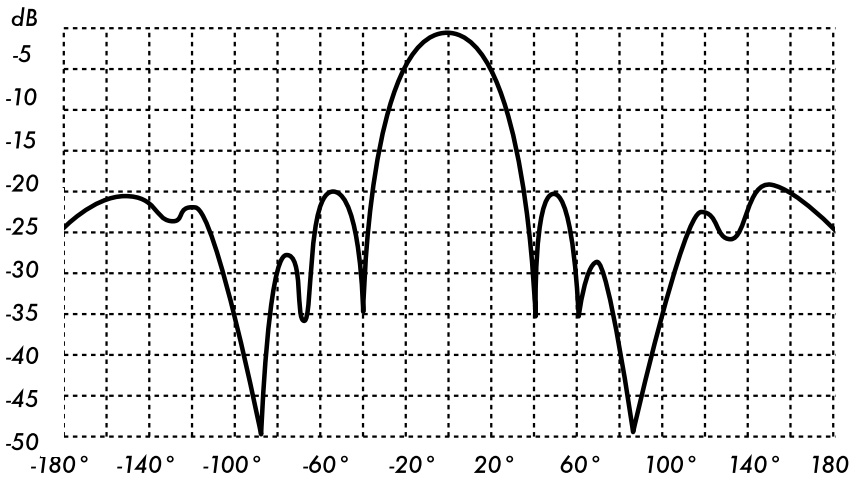


Figura 4.4: Diagrama de radiación de una antena Yagi en coordenadas rectangulares

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. En la *Figura 4.5* presentamos 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 lineal de coordenadas polares, 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 como el 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 se desenfatizan los lóbulos menores, pero no en el mismo grado que en la retícula lineal de potencia.

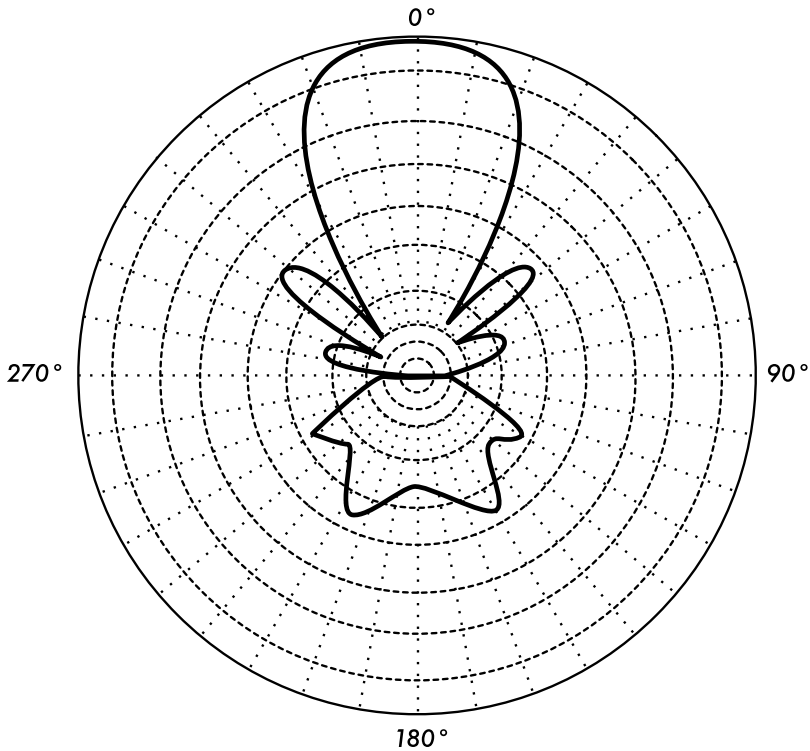


Figura 4.5: Diagrama polar lineal de la misma antena Yagi.

En el sistema logarítmico de coordenadas polares, 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 margen externo del cuadro. Con este tipo de retícula, los lóbulos que están 30 ó 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.

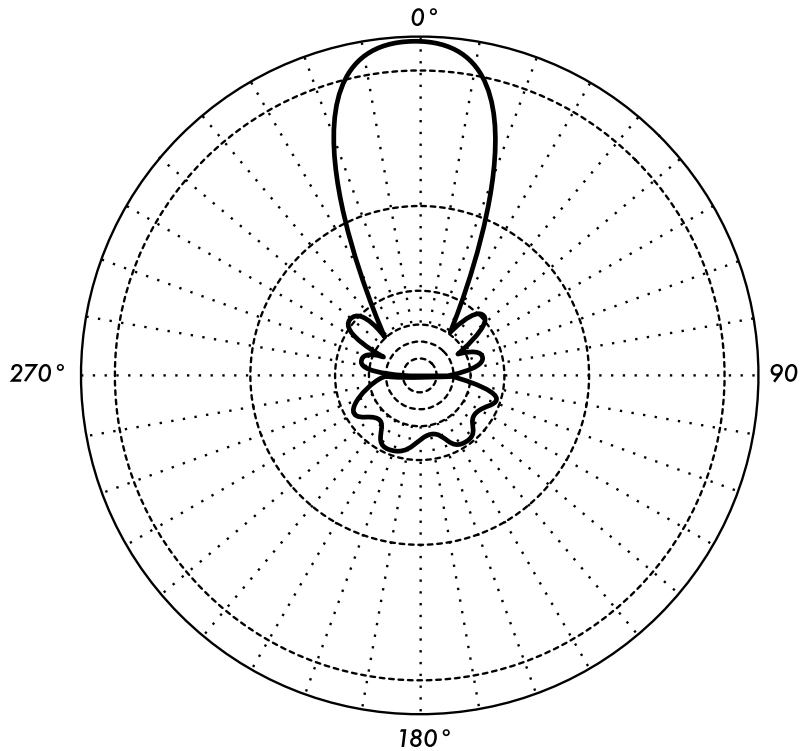


Figura 4.6: Trazado polar logarítmico

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 del pico que representan la mitad de la potencia de intensidad del pico. La distancia angular entre los puntos de mitad 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 mayoría 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.

En la polarización circular el vector del campo eléctrico aparece rotando con un movimiento circular en la dirección de la propagación, haciendo una vuelta 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.

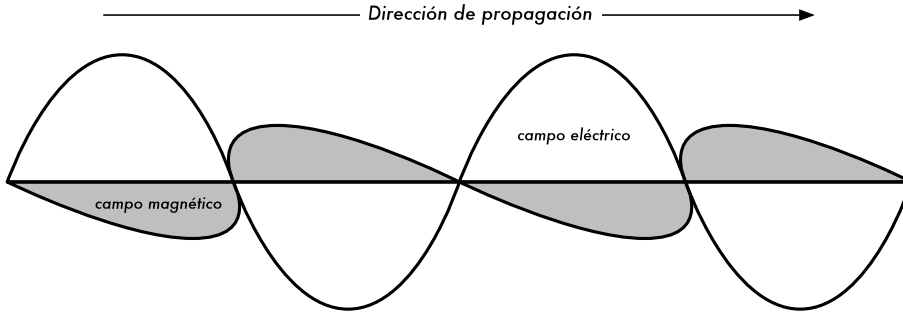


Figura 4.7: La onda senoidal eléctrica se mueve perpendicular a la onda magnética en la dirección de la propagación.

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 0.3 dB, para 30° perdemos 1.25 dB, para 45° perdemos 3 dB 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 aprovecharse 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 12,5 cm, mientras que a los 5000 MHz es de 6 cm.
- **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 2,4 GHz, 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 2,4 GHz, con una corta descripción de la información básica acerca de sus características.

Antena de ¼ 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 ¼ de longitud de onda como medio dipolo y tres o cuatro elementos de ¼ de longitud de onda inclinados de 30 a 45 grados hacia abajo. 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.

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

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 longitud 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.

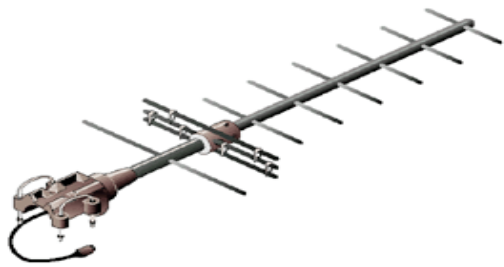


Figura 4.9: Una antena Yagi.

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 2,4 GHz, una antena bocina simple hecha con una lata tiene una ganancia del orden de 10 a 15 dBi.

Plato Parabólico

Las antenas basadas en reflectores parabólicos son el tipo más común de antenas directivas donde 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 una 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 4.10: Antena bocina hecha con una lata de comida.

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 ¼ de longitud de onda como elemento de radiación y de 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 2,4 GHz, 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 2400 MHz, y deben tener una conmutación lo suficientemente rápida para trabajar con aplicaciones Wi-Fi. Estos amplificadores existen pero suelen 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 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 sólo mejoran la cantidad disponible de señal sino que tienden a rechazar ruido desde otras direcciones. Los amplificadores amplían ciegamente las señales deseadas y 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 2400 MHz. 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 2400 MHz 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/a, 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 encontrada 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 los elementos electrónicos del clima. 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 5 dBi, mientras que la más larga, con cuatro elementos, va a tener de 7 a 9 dBi de ganancia. Sólo vamos a describir cómo construir la antena larga.

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 4.13: 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 (caño), o una mecha con un diámetro de 1 cm.
- Prensa o abrazadera
- Martillo
- Llave inglesa

Construcción

1. Enderece el alambre utilizando la prensa.

Figura 4.14: 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 4.15: 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 4.16: 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 4.17: Curvar el alambre alrededor de un tubo para hacer un anillo.

El anillo va a verse así:

Figura 4.18: 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.

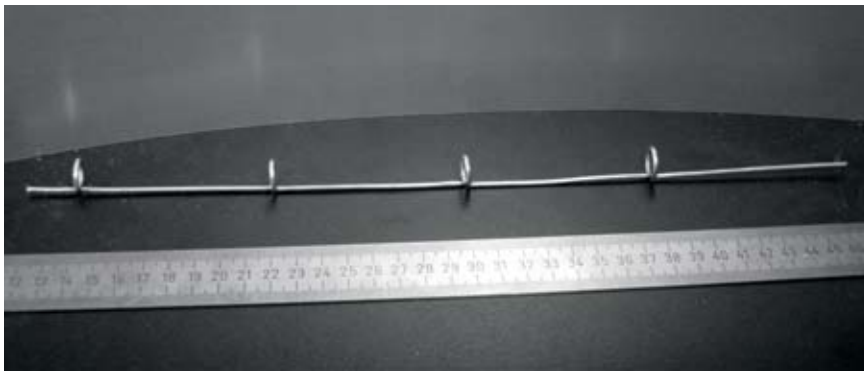


Figura 4.19: Intente mantenerlo lo más recto posible.

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

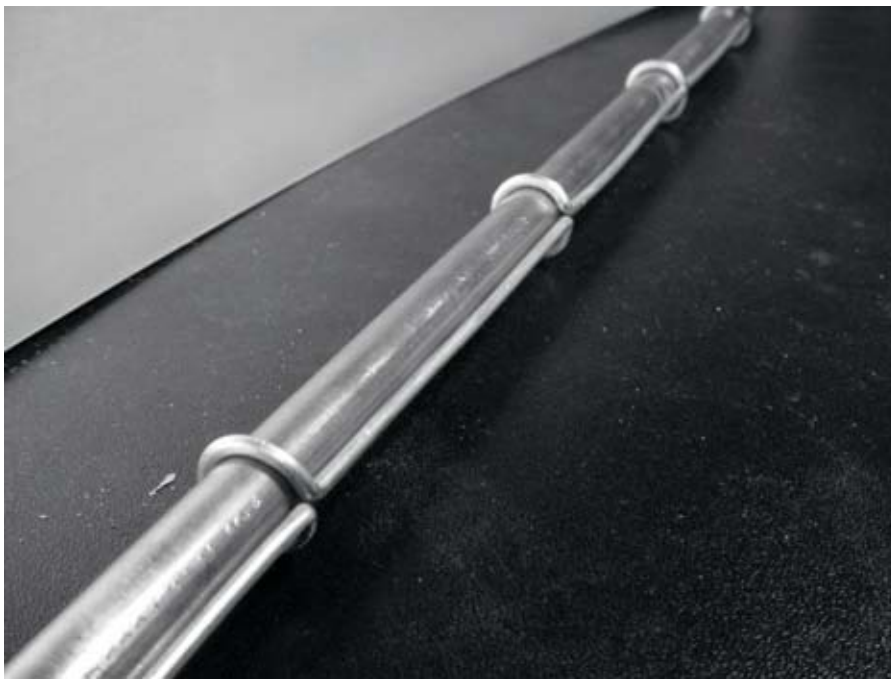


Figura 4.20: Insertar un tubo puede ayudar a enderezar el alambre.

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.

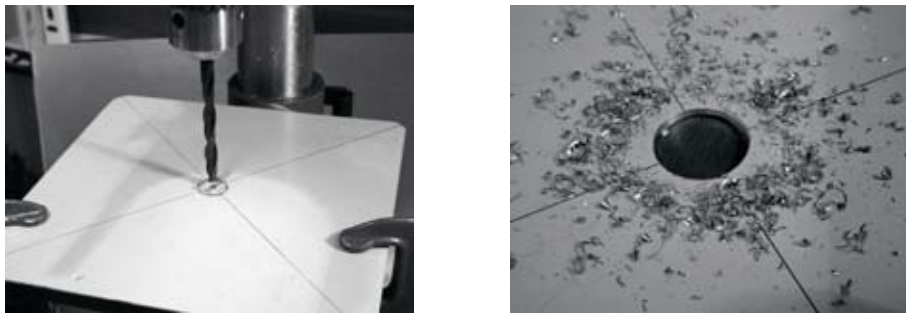


Figura 4.21: Taladrar el agujero en la placa de metal.

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

Figura 4.22: 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.

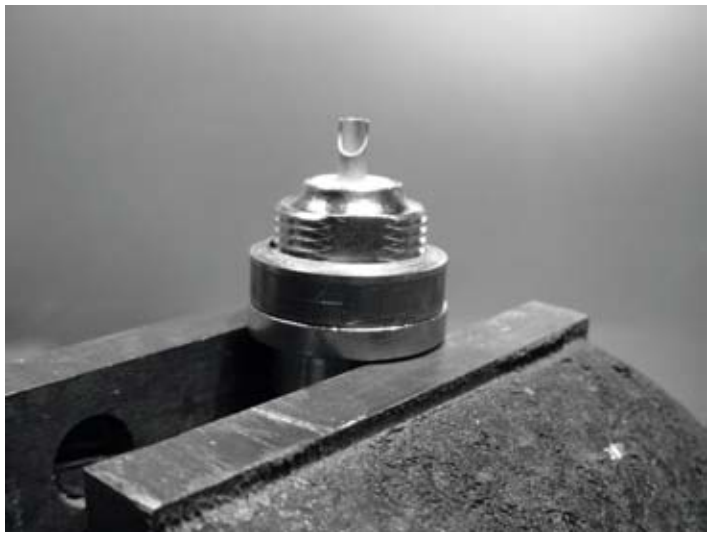


Figura 4.23: Agregar un tubo de cobre espaciador ayuda a obtener la impedancia de la antena de 50 Ohms.

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

Figura 4.24: 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.

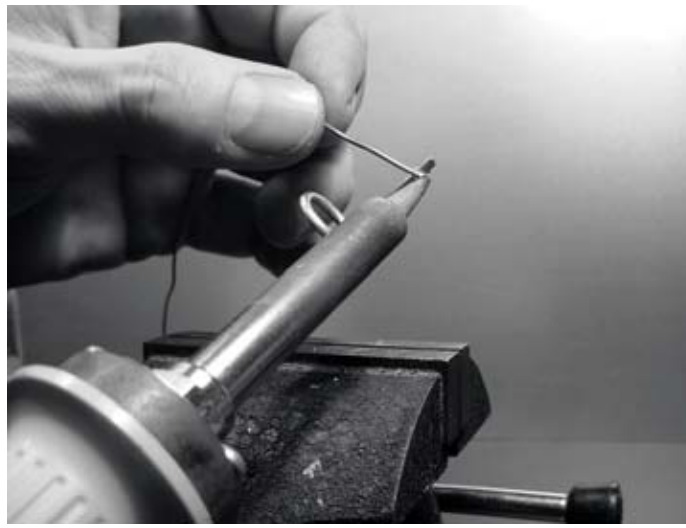


Figura 4.25: Agregue una pequeña capa de estaño al extremo del alambre antes de soldarlo.

10. Con el soldador, estañe 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 4.26: 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 4.27: 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 a 2,0 cm.

Figura 4.28: 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 4.29: La antena terminada debe medir 42,5 cm. desde la placa hasta el final del alambre.

14. Si tiene un Analizador del 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 del Espectro.

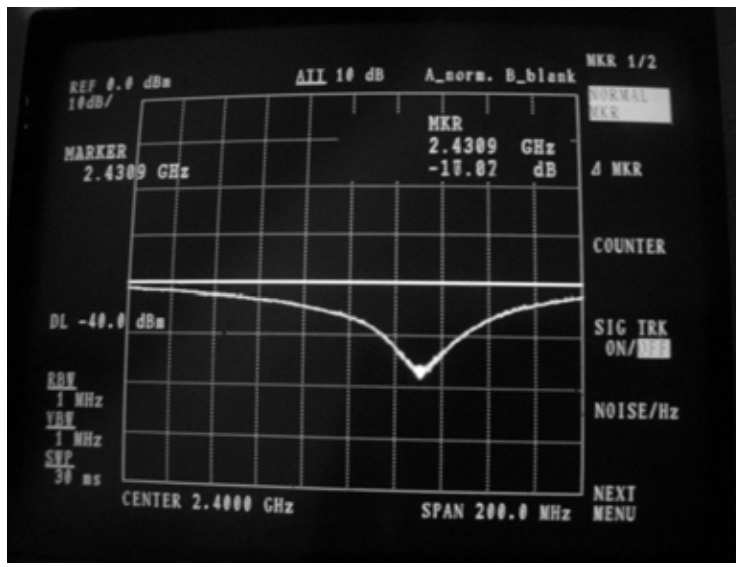


Figura 4.30: Un trazado del espectro de la potencia reflejada por la antena omnicolinear.

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:

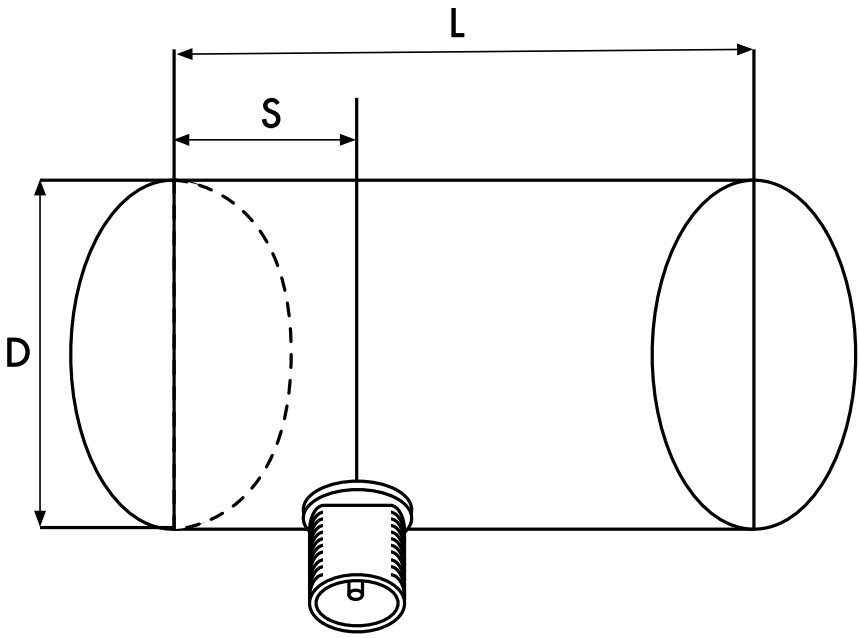


Figura 4.31: Limitaciones de dimensión en la antena guía-onda.

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, necesitaremos 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 4.32: La antena guía-onda terminada.

Lista de componentes

- Un conector tipo N hembra, de rosca
- 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 4.33: 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 4.34: Tenga cuidado con las puntas afiladas de los bordes al abrir la lata.

El disco circular tiene puntas muy afiladas. ¡Sea cuidadoso/a al manejarla! Vacíe la lata y lávela con jabón. Si la lata contenía ananás, galletitas, u otras cosas sabrosas, tenga la bondad de compartirlas con sus compañeros/as.

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 una perforadora (o un pequeño taladro, 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 4.35: 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 4.36: 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.

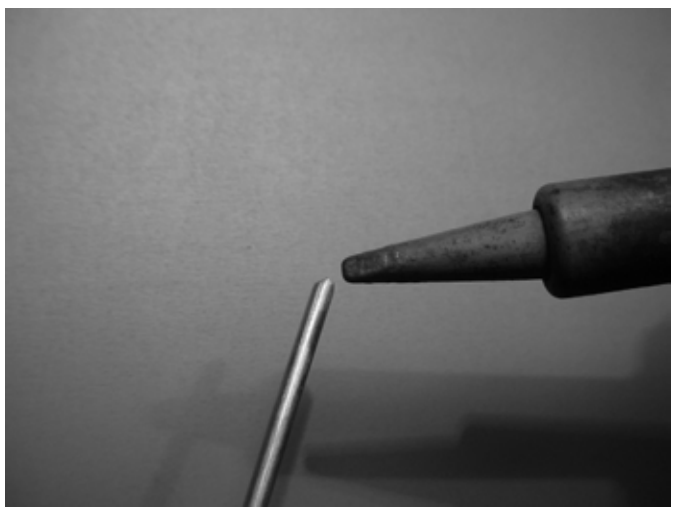


Figura 4.37: Estañe el extremo del alambre antes de soldarlo.

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 4.38: 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.

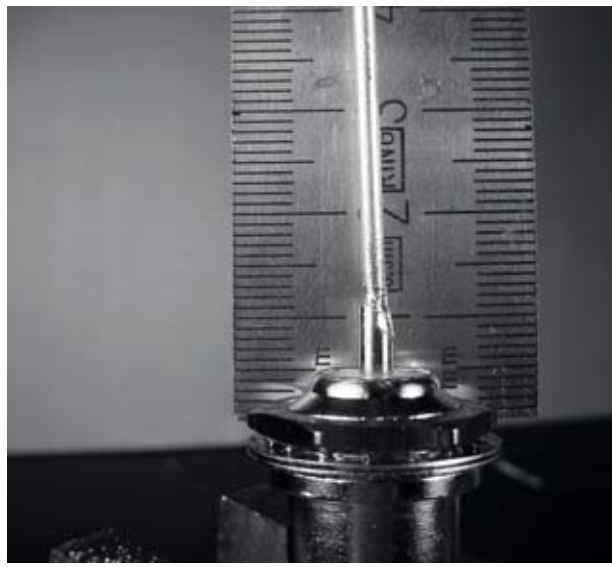


Figura 4.39: El largo del alambre es crucial.

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 4.40: Arme la antena.

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

Figura 4.41: 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 (observe 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, 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, 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 esta 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 el Capítulo 11: Estudio de casos.

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 varía 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 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
Equipamientos 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 de bajo costo al mercado. Tanta variedad, que resultaría imposible catalogar cada uno de los componentes disponibles. En este capítulo, nos enfocamos en señalar la clase de características y atributos que son deseables en los componentes inalámbricos, y revisar 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.

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.

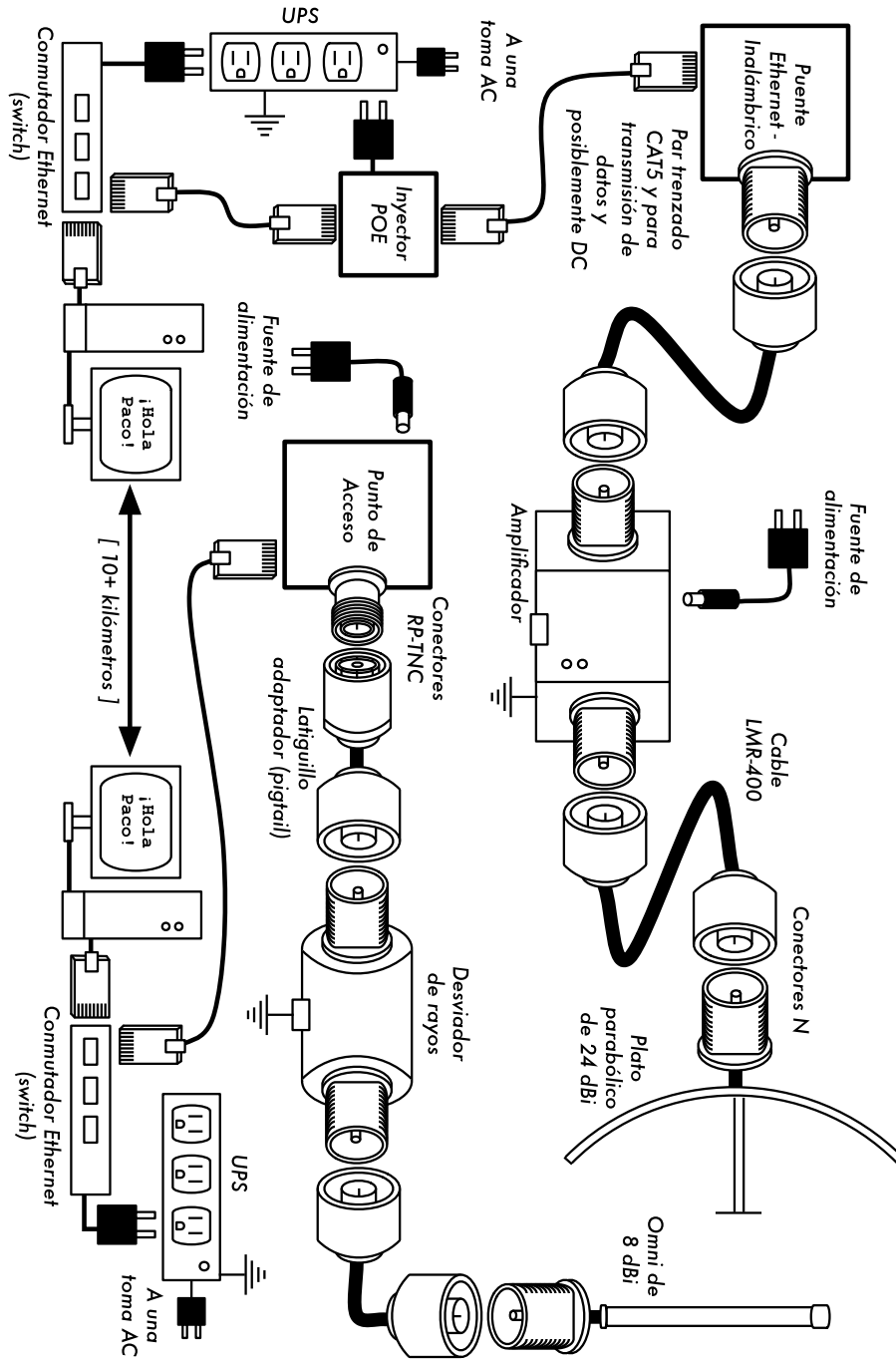


Figura 5.1: Interconexión de Componentes.

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 (*switch*) Ethernet.
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 constituidos por fuentes de alimentación, acondicionadores de energía, y protectores contra rayos.

La selección del equipamiento debe determinarse estableciendo las exigencias 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 1**, establecer el alcance de su proyecto es básico antes de tomar cualquier decisión de adquisiciones.

Cómo elegir 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 usar 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 acepta un protocolo abierto (como el 802.11b/g), entonces probablemente va a funcionar con equipamiento de otras fuentes.
- **Rango**. Como dijimos en el **Capítulo 4**, el alcance no es algo inherente a una pieza particular del equipo. El alcance de un dispositivo depende de la antena conectada a él, el terreno que lo rodea, y las características del dispositivo en el otro extremo del enlace, además de otros factores. En lugar de confiar en el valor del "alcance" 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 alcance teórico como fue descrito en el **Capítulo 3**.

- **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 presupuesto del enlace. Como vimos en el **Capítulo 3**, mientras más bajo sea este valor mejor será la sensibilidad del radio.
- **Caudal neto** (**throughput**). 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. 54 Mbps) nunca es el verdadero caudal neto del dispositivo (ej. aproximadamente 22 Mbps para 802.11g). Si la información del caudal neto no está disponible para el dispositivo que usted está evaluando, un buen truco es dividir la "velocidad" del dispositivo entre dos, y restar el 20%, más o menos. Si tiene alguna duda, realice la prueba de caudal neto en una unidad de evaluación antes de comprometerse a adquirir una gran cantidad de equipamiento que no especifica una tasa oficial de caudal neto.
- **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 energía? (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 latiguillos (*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, usted va a poder tomar decisiones de compra inteligentes cuando sea el momento de elegir el equipamiento de la red. Es casi imposible poder resolver 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 versus 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 sustituir el equipo que falla sin la necesidad de un técnico que lo configure. 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 l***os costos de licenciamiento futuro***.

Puede ser muy costoso dejar que las mal denominadas nuevas "prestaciones" dirijan el desarrollo de su red. Los fabricantes frecuentemente van a ofrecerle prestaciones 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 prestación contribuya a solucionar sus problemas de comunicación o no.

Al empezar a contar con esas prestaciones, 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 lo utilizan 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 descontinuarse 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 estipulan una cuota de licenciamiento 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/a, 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/a, 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.

Cuando considere cuál es el equipamiento que va a usar recuerde siempre comparar la distancia útil esperada, confiabilidad y caudal neto (throughput), además del precio. Asegúrese de incluir cualquier cuota de licenciamiento futuro cuando calcule el costo total del equipamiento. Finalmente, asegure que los radios que va a comprar operan en una banda exenta de licencia donde los va a instalar, o si debe usar espectro sujeto a licencia, que tiene los recursos y los permisos para pagar las licencias requeridas.

Protección profesional 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 por inducción. 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 la descarga de un rayo 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 mucho mayor que la que el receptor de radio puede manejar. En general, cualquier tipo de rayo va a destruir el equipo que esté sin protección.

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

Proteger las redes inalámbricas de los rayos 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 qué 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

(diámetro *mayor de 5,19 mm*) o más grueso. Adicionalmente, se debe enterrar una jabalina, y conectarla también a la torre en el mismo punto.

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. Cualquier tipo de capa, como la pintura, debe removerse antes de conectar 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 contra rayos de gas 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 en 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. GNU/Linux 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 que ejecuta Linux le dará una herramienta muy flexible que puede ayudarlo/a 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 Mikrotik.

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 pasarela inalámbrica —*wireless 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. Extendiendo estos ejemplos simples, puede crear un servidor que se ajuste de forma precisa a su infraestructura de red.

Prerrequisitos

Antes de comenzar, debe estar familiarizado con Linux desde la perspectiva del usuario, y ser capaz de instalar la distribución GNU/Linux 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 compatible con 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 caché 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 133 MHz 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 implementar un servidor de almacenamiento intermedio (como Squid), 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 una unidad *flash* USB (suponiendo que su PC pueda arrancar 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 admita 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 ejecutando 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 para ejecutar GNU/Linux. Puede ser una instalación de Ubuntu Servidor, 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 admite 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 admite el modo de punto de acceso. De todas formas puede probar la misma configuración en el modo ad hoc, que es permitido por todos los grupos de chips. Esto requiere 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 admita el modo AP. Para obtener una lista de las tarjetas compatibles, 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:

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

Para 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 de 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 asegurándose de que **ip_forward** indique **yes**:

```
ip_forward=yes
```

y luego reiniciar las interfaces de red con:

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

ó:

```
# /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 les sea más sencillo a 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 ejecutar 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 guarde 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.

Agregue seguridad extra: Configure 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 ejecute Gnome.
- ***Knetfilter***: un cliente gráfico para KDE, el cual requiere que su servidor ejecute KDE.
- ***Shorewall***: 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 más robusta.

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 subred. 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 subred, 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 necesite, 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 subred, 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. 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 específica 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 es el caso de Fedora Core), aquí hay una configuración alternativa para **/etc/network/interfaces** que logrará lo mismo con sólo un poco más de complicación:

```
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 basadas en Debian) también debe darle a su interfaz puenteada una dirección IP y agregar una ruta por defecto al resto 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).

Use el comando ***brctl*** para ver lo que está haciendo el puente:

```
# brctl show br0
```

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 completo sobre cómo se enrutan los paquetes a través de su red, dotándolo de 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 un tiempo limitado (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 6**.

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 PC 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*
- **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 6 MB) 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 cierto tiempo de desarrollo para 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 US$ 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 produjo 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*. Algunas buenas alternativas de paquetes de *firmware* para WRT54G son: OpenWRT (*http://openwrt.org/*), Tomato (*http://www.polarcloud.com/tomato*), y Freifunk (*http://www.freifunk.net)*.

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 ejecutar Linux (se vende con VxWorks, un sistema operativo mucho más pequeño que no permite una fácil adaptación). Linksys también desarrolló el WRT54GL, el cual es esencialmente el WRT54G v4 (que funciona con Linux) a 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 utiliza, 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.

Afortunadamente, los *hackers* han logrado sortear las dificultades que impedían instalar *firmware* modificado en las versiones 5 y 6 y las revisiones posteriores (v7 y v8) de WRT54G .

Para información actualizada acerca de la modificación de los enrutadores inalámbricos Linksys, consulte: *http:///linksysinfo.org/*

6
Seguridad y Monitoreo

En una red cableada tradicional, el control del acceso es muy sencillo: si una persona tiene acceso físico a una computadora o a un concentrador (*hub*) en la red, entonces puede usar (o abusar) de los recursos de la red. Si bien los mecanismos 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. En pocas palabras: si sólo las personas de confianza tienen acceso a los terminales y los componentes de la red, entonces la red puede considerarse 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 siempre cierto grado 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 experimenten 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 un tomacorriente porque alguien más necesita esa conexión. Asegurar la seguridad física de la instalación es un asunto prioritario. Los letreros y las etiquetas les serán útiles a aquellos que saben leer, o que hablan su mismo idioma. Colocar el equipo donde no estorbe 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. La fabricación local de cajas para contener el equipo puede se económicamente viable. 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 bloque 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

De ser posible, los cables deberían estar ocultos y atados. Es posible encontrar conductos de plástico para cables que pueden usarse en edificios. Si no los encuentra, sujete los cables a la pared para que queden fijos, y asegúrese de que no queden expuestos en lugares donde puedan ser enganchados, pinchados o cortados. Es preferible enterrar los cables en lugar de dejarlos colgando en espacios donde puedan ser usados para colgar ropa o ser tropezados con una escalera, etc. Para evitar alimañas e insectos use ductos

eléctricos plásticos. El costo adicional vale la pena pues evitará molestias. El ducto debería enterrarse aproximadamente a 30 cm de profundidad, o por debajo del nivel de congelamiento en climas fríos. Es aconsejable comprar ductos de un calibre superior al mínimo necesario de manera que en el futuro se puedan pasar otros cables por el mismo ducto. Considere señalizar los cables enterrados con un aviso de "llame por teléfono antes de excavar" para evitar apagones accidentales.

Energía

Lo mejor es poner los multienchufes (regletas, zapatillas) dentro de un armario cerrado. Si esto no es posible colóquelos 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 el multienchufes ni en la UPS, tápelos 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 30 cm 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

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 sobredimensionar 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 imperceptibles que los reflectores parabólicos 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 destacados 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 Ethernet y las inalámbricas es que estas últimas constituyen 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 monitorizar todo el tráfico de la red en un punto de acceso, se 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 acceso a contraseñas y otros datos de gran valor, facilitando 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, 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 lugar 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 de 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 causarle problemas serios a la red. Muchos dispositivos de red son también vulnerables a otras formas de ataques de denegación del servicio, tales como una inundación 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.

- ***War 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*). Los *war drivers* 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 gran 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/*, ó *http://www.netstumbler.com*

- ***Puntos de acceso piratas***. Hay dos clases generales de puntos de acceso piratas: 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 (*http://www.etherpeg.org/*), o Driftnet (*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 encriptación fuerte 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 a cada interfaz 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 sólo 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 este mecanismo 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 encriptación fuerte, 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 está disponible en 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 escuchando en 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 un buen mecanismo de autenticación, además de darle un poco de privacidad.

WEP definitivamente no es la mejor solución de encriptación 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 un empleado abandona la organización) 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 de rotación rápida), 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 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 ofrecen un WEP básico. Si bien no es el método más fuerte disponible, ciertamente es el implementado 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 revisan usando el protocolo 802.1X, que 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.

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 piratas 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.

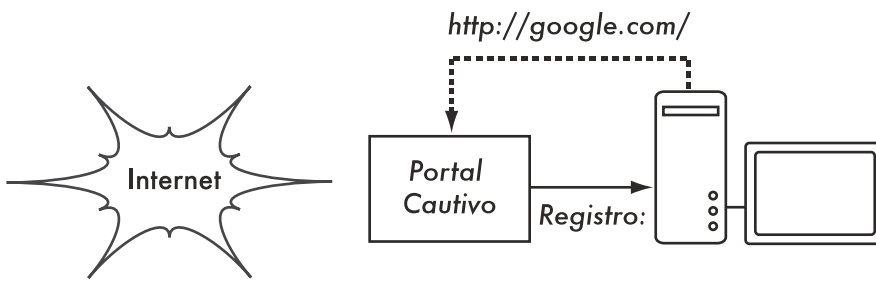


Figura 6.1: El usuario solicita una página web y es redireccionado.

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.

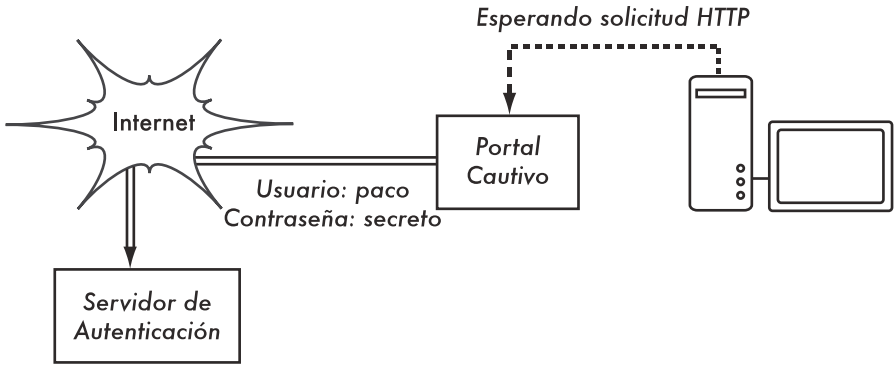


Figura 6.2: Las credenciales se verifican antes de brindar acceso al resto de la red. El servidor de autenticación puede ser el punto de acceso mismo, otra computadora en la red local, o un servidor en cualquier lugar del Internet.

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.

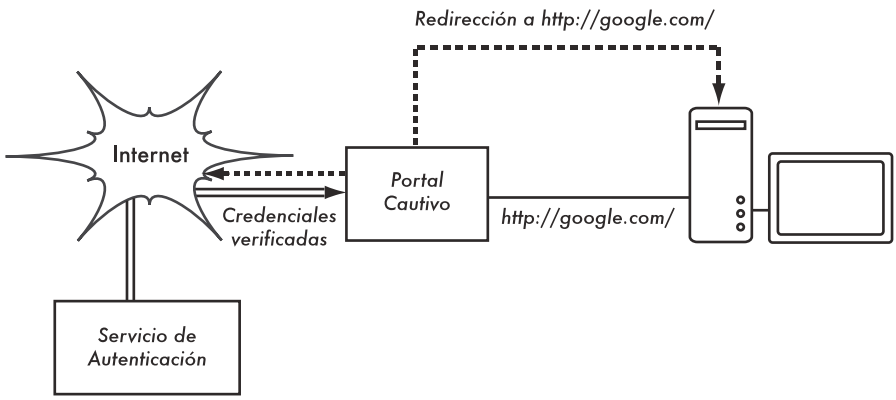


Figura 6.3: Después de que el usuario es autenticado, se le permite el acceso al resto de la red.

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 único identificador. 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.

Proyectos populares de servicios WiFi locales (hotspots)

- Chillispot (*http://www.chillispot.info/*). 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/*). Es un sistema operativo embebido completo basado en FreeBSD. Este incluye un portal cautivo con soporte RADIUS, así como un servidor web PHP.
- **NoCatSplash** (*http://nocat.net/downloas/NoCatSplash/)* les presenta a los usuarios una página de inicio (***splash***) personalizable que les pide pulsar sobre el botón de registro (*login*) antes del acceso a Internet. Esto es útil para identificar a los operadores de la red y desplegar las reglas de acceso a la red. Es una solución fácil en situaciones donde se necesita proporcionarles a los usuarios una red abierta con información y una política de uso aceptable.

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.
- ***Encapsulado 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 y ***PKI*** (***Public Key Infrastructure***), para asegurar las comunicaciones de datos en la web. Cada vez que visita una URL 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 encapsulado de datos es conocido como ***túnel***.

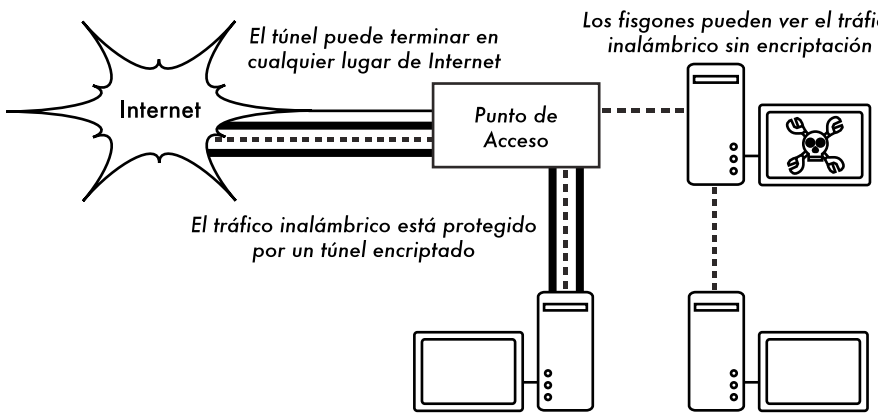


Figura 6.4: Los fisgones deben romper la encriptación para monitorizar el tráfico dentro de un túnel encriptado. La conversación dentro del túnel es igual a cualquier otra conversación sin encriptar.

El uso de certificados con PKI no sólo 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, le resulta fácil observar y manipular los datos que están pasando entre el servidor y el navegador.

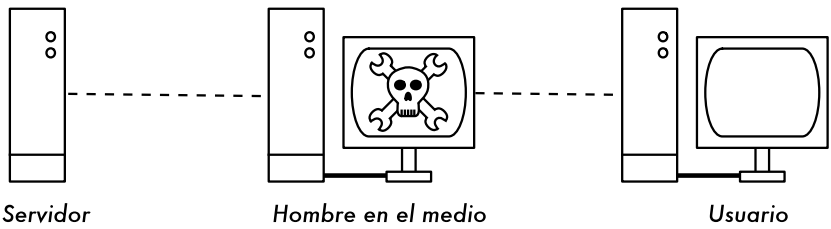


Figura 6.5: El hombre en el medio controla de forma efectiva todo lo que el usuario ve, y puede grabar y manipular todo el tráfico. Sin una infraestructura de clave pública para verificar la autenticidad de las claves, la encriptación fuerte por si sola no podría protegernos de este tipo de ataque.

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 mediante un túnel SSL. La mayoría de los clientes de correo electrónico actuales ofrecen 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 tiene además funcionalidades adicionales. Al igual que SSL, utiliza criptografía fuerte de clave pública para verificar el servidor remoto y encriptar los datos. En lugar de PKI, utiliza una caché de clave que se verifica 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.

Es poco conocido que SSH también puede funcionar como un túnel de encriptación para usos generales, o incluso *web proxy* de encriptación. Estableciendo primero 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.

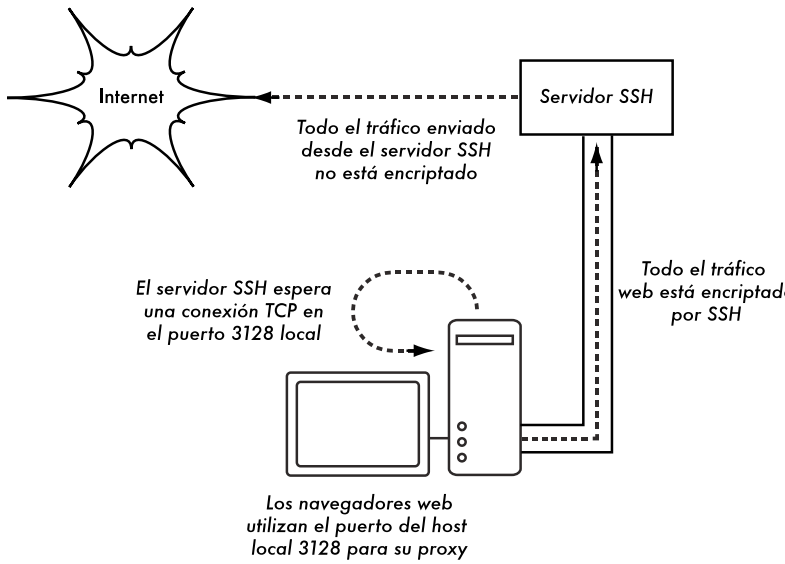


Figura 6.6: El túnel SSH protege el tráfico web hasta llegar al servidor SSH remoto.

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 *web proxy* 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.

SSH también puede funcionar como un proxy dinámico SOCKS4 o SOCKS5. Esto le permite crear un encriptador web proxy sin la necesidad de instalar squid. Tenga en cuenta que éste no será un proxy con memoria caché, 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 la 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 sólo 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 autenticación y una encriptación fuerte.

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 solamente un 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.

Algunas de estas ventajas son:

- 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 del How To: *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 monitorizar 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 ***haciendo 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 al 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 de la red

El monitoreo de la red es el uso de registro (*logging*) y herramientas de análisis para determinar con precisión el flujo de tráfico, la utilización y otros indicadores de desempeño característicos de una red. Buenas herramientas para monitorizar le proporcionarán cifras numéricas y representaciones gráficas del estado de la red. Esto le va a ayudar a visualizar en detalle lo que está ocurriendo, de manera que sepa cuáles son los ajustes que necesita hacer. Estas herramientas le ayudarán a responder preguntas básicas, como las siguientes:

- ¿Cuáles son los servicios más populares usados en la red?
- ¿Quiénes hacen uso más intenso de la red?
- ¿Qué otros canales inalámbricos se usan en el área?
- ¿Hay usuarios que estén instalando puntos de acceso inalámbricos en mi red cableada de uso privado?
- ¿A que hora del día es más utilizada la red?
- ¿Cuáles son los sitios más visitados por sus usuarios?

- ¿Está el tráfico entrante y saliente cerca de la capacidad disponible de nuestra red?
- ¿Hay indicaciones de alguna situación inusual en la red que esté consumiendo ancho de banda o causando otros problemas?
- ¿El Proveedor de Servicios de Internet (ISP) está dándonos el servicio por el que estamos pagando? Esto debe responderse en términos de ancho de banda disponible, pérdida de paquetes, latencia, y disponibilidad general.

Y, tal vez, la pregunta más importante de todas:

- ¿El patrón de tráfico observado cumple con nuestras expectativas?

Vamos a examinar de qué manera un sistema administrador típico puede hacer uso de buenas herramientas de monitoreo.

Un ejemplo efectivo de monitoreo de red

Para dar un ejemplo, vamos a suponer que estamos encargados de una red que ha estado funcionando por tres meses. Consiste de 50 computadoras y tres servidores: servidores de correo, web y proxy. Mientras que al comienzo las cosas van bien, los usuarios comienzan a quejarse de la lentitud de la red y del aumento de spam. A medida que pasa el tiempo, el desempeño se hace mucho más lento (incluso cuando no se usa la red), lo que causa gran frustración a los usuarios.

Debido a las quejas frecuentes y al poco uso de las computadoras, el Consejo de Administración se pregunta si hay necesidad de tanto hardware para la red. También quieren tener la seguridad de que el ancho de banda que están pagando se está usando efectivamente. En tanto administrador/a de la red, usted es quien recibe todas las quejas. ¿Cómo hace usted para diagnosticar la caída repentina de la red y el bajo desempeño de las computadoras, y a la vez, justificar los costos de hardware y ancho de banda?

Monitoreo de LAN (tráfico local)

Para tener una idea de qué es exactamente lo que está causando el enlentecimiento, usted debería comenzar por examinar el tráfico en la LAN local. Hay varias ventajas en hacer esto:

- La resolución de problemas se simplifica bastante.
- Los virus pueden ser localizados y eliminados.
- Los usuarios malintencionados pueden detectarse y solucionar el problema.
- Los recursos y el hardware de la red pueden justificarse con estadísticas reales.

Suponga que todos los conmutadores (switches) soportan ***SNMP*** (***Simple Network Management Protocol***) SNMP es un protocolo de la capa de aplicaciones diseñado para facilitar el intercambio de información de gestión entre los dispositivos de la red. AL asignarle una dirección IP a cada conmutador,

será capar de monitorizar todas las interfaces en ese conmutador y observar la red entera desde un sólo punto. Esto es mucho más fácil que habilitar SNMP en todas las computadoras de la red.

Usando una herramienta gratuita como MRTG (ver **página 189**), se puede monitorizar cada puerto en el conmutador y presentar los datos gráficamente, como un promedio acumulado en el tiempo. Las gráficas están disponibles en la web, de manera que puede verlas desde cualquier máquina en cualquier momento.

Mediante monitoreo MRTG, es obvio que la LAN interna está inundada con mucho más tráfico de lo que la conexión Internet puede manejar, incluso cuando el laboratorio no está ocupado. Esto es una indicación clara de que algunas computadoras están infestadas de virus. Luego de instalar un buen programa antivirus y detector de spyware en todas las máquinas, el tráfico de la LAN interna baja a los niveles esperados. Las máquinas funcionan más rápidamente, se reducen los correos spam, y el ánimo de los usuarios mejora también rápidamente.

Monitoreo de la WAN (tráfico externo)

Además de supervisar el tráfico de la LAN interna, usted necesita demostrar que el ancho de banda que la organización está pagando es el que de verdad están obteniendo de su ISP. Esto puede lograrlo al monitorizar el ***tráfico externo***.

El tráfico externo se clasifica generalmente como todo aquello que se envía por una ***Wide Area Network*** (***WAN***)—***Red de Área Extendida***. Todo lo que se reciba desde (ó se envíe a) una red diferente a su LAN interna, también califica de tráfico externo. Las ventajas de monitorizar el tráfico externo incluyen:

- Los costos de ancho de banda de Internet pueden justificarse mostrando su uso real y comparándolo con lo que su ISP le está cobrando por el ancho de banda.
- Las necesidades futuras de capacidad pueden calcularse examinado las tendencias de uso y prediciendo patrones de crecimiento probables.
- Los intrusos provenientes de Internet se detectan y se filtran antes de que causen problemas.

Monitorizar el tráfico es tarea fácil con el uso de MRTG en un dispositivo habilitado con SNMP, como un enrutador, por ejemplo. Si su enrutador no soporta SNMP, entonces puede añadir un conmutador entre el enrutador y la conexión de su ISP, y monitorizar el tráfico del puerto como lo haría con una LAN interna.

Cómo detectar fallas de red

Con las herramientas de monitoreo en su sitio, usted tiene ahora una medida precisa de cuánto ancho de banda está usando su organización. Esta medida debería concordar con lo que está cobrando su ISP. Puede también indicarle el caudal (throughput) real de su conexión si usted está cerca del límite de su capacidad disponible en horas pico. Una traza de tráfico constituida por una línea horizontal en la parte superior es una indicación clara de que usted

está operando a su máxima capacidad. La **Figura 6.7** muestra esta condición para el tráfico de salida pico al mediodía día, de cada día, excepto los domingos.

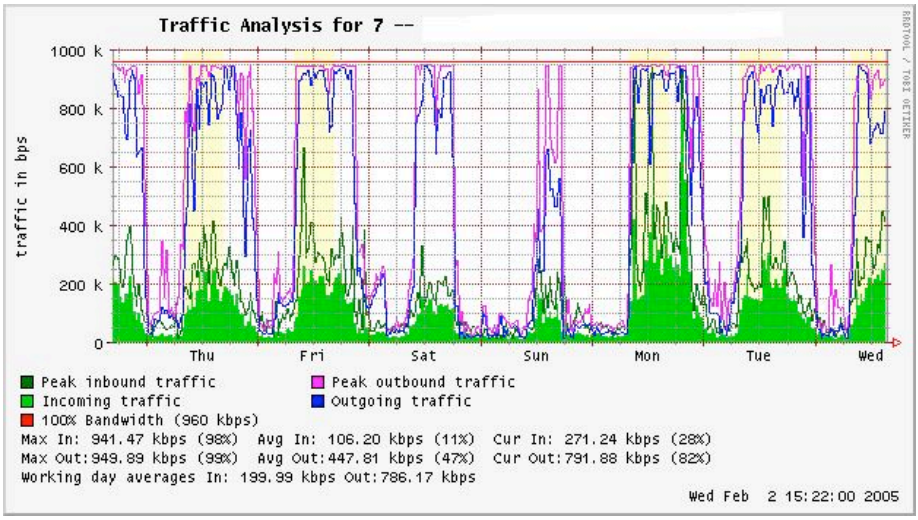


Figura 6.7: Una traza continua horizontal en el tope del gráfico indica claramente sobreutilización.

Es obvio que su conexión a Internet actual no tiene suficiente capacidad en las horas pico, lo que causa retardos en la red. Al presentar esta información al Consejo de Administración usted puede planificar otras optimizaciones tales como actualización del servidor proxy y otras técnicas explicadas en este libro, y estimar cuán pronto deberá actualizar su conexión para satisfacer la demanda. Esta es también una excelente oportunidad para revisar con el Consejo la política de operación y discutir maneras de hacer concordar el uso de la red con esa política.

Más tarde en la semana, usted recibe una llamada telefónica de emergencia en la tarde. Aparentemente, nadie en el laboratorio puede navegar en la web o mandar correos. Usted corre al laboratorio y rápidamente reinicia el servidor proxy, sin resultados. Ni la web ni los correos funcionan. Reinicia el enrutador, pero todavía sin éxito. Continúa eliminando una a una las posibles áreas problemáticas hasta que se da cuenta de que el conmutador de la red está apagado: un cable de energía suelto es el culpable. Después de conectar, la red vuelve a la vida.

¿Cómo se puede detectar este tipo de falla sin emplear este largo proceso de ensayo y error? ¿Es posible tener notificación de fallas en el momento en que se producen, en lugar de esperar las quejas de los usuarios? Una forma de lograrlo es usando un programa como ***Nagios*** que continuamente examina los dispositivos de la red y le notifica las fallas. Nagios le va a informar sobre la disponibilidad de las diferentes máquinas y sus servicios y le alertará sobre las máquinas que están fallando. Además de presentarle el estatus de la red

gráficamente en una página web, le enviará notificación por SMS o email para alertarle en el momento en que se produce el problema.

Con las herramientas de monitoreo en su lugar, usted debería ser capaz de justificar los costos de equipamiento y banda ancha demostrando efectivamente cómo es utilizada la red por la organización. Usted es notificado/a en el momento preciso en que surgen los problemas y tiene una historia estadística del rendimiento de los diferentes dispositivos. Puede comprobar los problemas presentes por comparación con el registro histórico para detectar comportamiento anómalo, y atacar los problemas antes de que se agraven. Si el problema se presenta de todas maneras, es más fácil determinar su fuente y naturaleza. Su trabajo es más fácil, el Consejo queda satisfecho y los usuarios están más contentos.

Monitorizar la red

Administrar una red sin monitorizar es equivalente a manejar un vehículo sin un velocímetro, o sin medidor de gasolina y con los ojos cerrados. ¿Cómo hace para saber a qué velocidad conduce? ¿El vehículo está consumiendo combustible de manera tan eficiente como le prometió el vendedor? Si usted le hace mantenimiento al vehículo unos meses después, ¿va a tener más velocidad o a ser más eficiente que antes?

De manera semejante, ¿cómo puede usted pagar el recibo del agua o de la electricidad sin ver en el medidor cuánto es su consumo mensual? Usted debe llevar cuenta de la utilización del ancho de banda de su red para poder justificar los costos de los servicios y de las compras de hardware y para dar cuenta de las tendencias de uso.

Hay varios beneficios al implementar un buen sistema para monitorizar su red:

1. **Los recursos y el presupuesto de red pueden justificarse.** Buenas herramientas de monitoreo pueden demostrar sin lugar a dudas que la infraestructura de red (ancho de banda, hardware y software) es adecuada y capaz de manejar las necesidades de los usuarios de la red.

2. **Los intrusos de la red pueden detectarse y filtrarse.** Al supervisar el tráfico de su red, puede detectar a los atacantes e impedirles el acceso a los servidores y servicios de la red.

3. **Los virus pueden detectarse con facilidad.** Puede ser alertado/a sobre la presencia de virus y tomar las medidas adecuadas antes de que consuman ancho de banda de Internet y desestabilicen la red.

4. **La detección de problemas en la red es mucho más fácil.** En lugar de intentar el ensayo y error para eliminar los problemas en la red, usted puede ser notificado/a de inmediato sobre problemas específicos. Algunos pueden incluso repararse automáticamente.

5. **El rendimiento de la red puede ser optimizado en gran medida**. Sin un monitoreo efectivo, es imposible afinar el funcionamiento de sus dispositivos y protocolos para lograr el mayor rendimiento posible.

6. **La planificación de capacidad es más fácil.** Con registros cronológicos sólidos sobre desempeño, usted no tendrá que "suponer" cuánto ancho de banda va a necesitar su red cuando ésta crezca.
7. **El uso apropiado de la red puede hacerse valer.** Cuando el ancho de banda es un recurso escaso, la única forma de ser justos con los usuarios es asegurarse de que la red se usa para lo que fue creada.

Afortunadamente, el monitoreo de la red no necesita ser una labor costosa. Hay numerosas herramientas de fuente abierta gratuitas que le enseña lo que está pasando exactamente en su red con bastantes detalles. Esta sección va a ayudarle a identificar muchas herramientas valiosas y a enseñarle la mejor manera de usarlas.

El servidor de monitoreo dedicado

Aunque hay herramientas de monitoreo que pueden adicionarse a un servidor de red ya existente, es deseable dedicar una máquina (o más, si fuera necesario) al monitoreo de la red. Algunas aplicaciones (como **ntop**) necesitan recursos considerables para ejecutarlas, especialmente en una red de mucho tráfico. Pero la mayor parte de los programas de registro (logging) y de monitoreo tienen exigencias modestas de RAM y almacenamiento, y de potencia del CPU. Puesto que los sistemas operativos de fuente abierta (como Linux o BSD) hacen un uso muy eficientes de los recursos de hardware, esto hace que sea posible construir un servidor de monitoreo muy capaz, a partir de piezas de PC recicladas. Comúnmente no hay necesidad de comprar un servidor nuevo para dedicarlo a las labores de monitoreo.

La excepción a esta regla son las instalaciones muy grandes. Si su red comprende más de unos cientos de nodos, o si usted consume más de 50 Mbps de ancho de banda de Internet, es probable que necesite dividir las labores de monitoreo entre varias máquinas dedicadas. Esto va a depender mucho de lo que quiera monitorizar exactamente. Si usted quiere dar cuenta de todos los servicios accedidos a través de direcciones MAC, esto consumirá bastantes más recursos que la simple medición del flujo de tráfico en un puerto del conmutador. Para la mayoría de las instalaciones, una sola máquina dedicada es suficiente.

Concentrar los servicios de monitoreo en una sola máquina no solo va a hacer más ágil la administración y la actualización del sistema, sino que también le va a asegurar un mejor monitoreo en tiempo real. Por ejemplo, si instala un servicio de monitoreo en un servidor web, y ese servidor presenta problemas, su red no puede ser monitorizada hasta tanto el problema haya sido resuelto.

Para un/a administrador/a de red, los datos recogidos acerca del desempeño de la red son casi tan importantes como la red misma. Su monitoreo debe ser robusto y tan bien protegido contra fallas de energía como sea posible. Sin estadísticas de red, usted está ciego/a ante los problemas de la red.

¿Dónde encaja el servidor en mi red?

Si usted está solamente interesado/a en recoger estadísticas del flujo de la red de un enrutador, lo puede hacer desde casi cualquier sitio de la LAN. Esto le da una retroalimentación básica sobre utilización, pero no puede darle detalles amplios sobre patrones de uso. La **Figura 6.8** muestra una gráfica típica MRTG generada desde el enrutador a Internet. Mientras que se distingue claramente el tráfico entrante y saliente, no hay detalles sobre cuáles computadoras, usuarios o protocolos están usando ancho de banda.

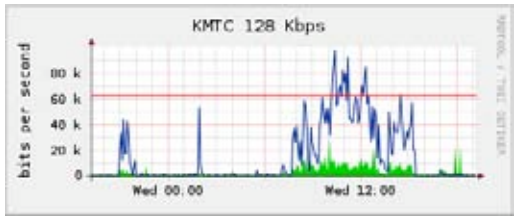


Figura 6.8: Sondear el enrutador perimétrico puede mostrarle la utilización general de la red, pero los datos no pueden analizarse en términos de máquinas, servicios y usuarios.

Para más detalles, el servidor dedicado al monitoreo debe tener acceso a todo lo que se necesite supervisar. Usualmente, esto significa que debe tener acceso a la red completa. Para monitorizar una conexión WAN, como el enlace Internet hacia su ISP, el servidor de monitoreo debe ser capaz de ver el tráfico que pasa por el enrutador perimetral. Para monitorizar una LAN, el servidor está comúnmente conectado con un ***puerto monitor*** en el conmutador. Si se están usando varios conmutadores en una instalación, el servidor monitor podría necesitar una conexión con todos ellos. Esta conexión puede ser un cable real, o si los conmutadores de su red lo permiten, una VLAN configurada específicamente para monitorizar tráfico.

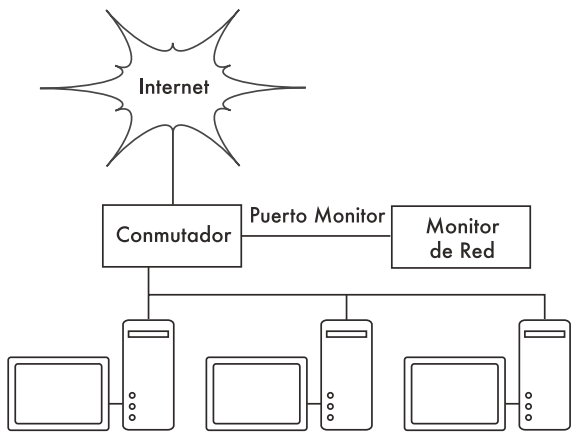


Figura 6.9: Use el puerto monitor en su conmutador para observar el tráfico que cruza todos los puertos de la red.

Si la función de puerto monitor no está disponible en su conmutador, el servidor monitor podría instalarse entre su LAN interna e Internet. A pesar de que esto funciona, introduce un punto crucial de falla en la red, ya que esta fallará si el servidor monitor presenta algún problema. También pudiera ser una fuente de embotellamiento si el servidor se ve incapacitado de cumplir las exigencias de la red.

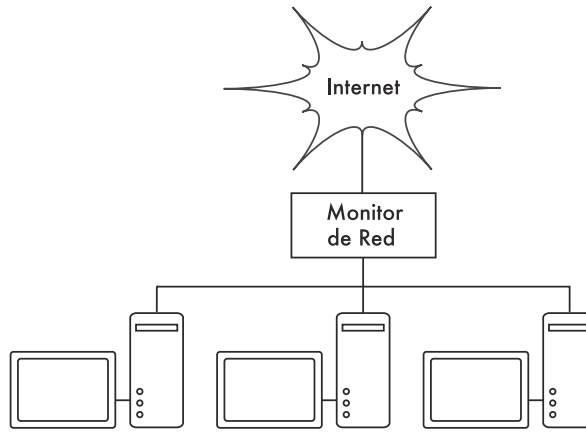


Figura 6.10: Al insertar un monitor de red entre la LAN y su conexión a Internet, se puede observar todo el tráfico de la red.

Una solución mejor es la de usar un simple concentrador (no un conmutador) que conecte la máquina monitora con la LAN interna, el enrutador externo y la máquina monitora. A pesar de que esto todavía introduce un punto crucial de falla en la red (puesto que la red completa será inaccesible si el concentrador se "muere"), los concentradores son considerados más confiables que los enrutadores. También son más fácilmente reemplazables si fallan.

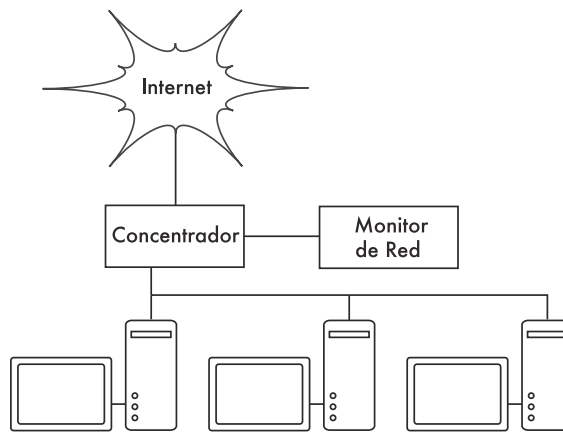


Figura 6.11: Si su conmutador no tiene la funcionalidad de puerto monitor, puede insertar un concentrador de red entre el enrutador de Internet y la LAN, y conectar el servidor monitor al concentrador.

¿Qué debemos monitorizar?

Es posible graficar casi cualquier evento de red y observar su valor en el tiempo. Ya que cada red es ligeramente diferente, usted tendrá que decidir cuál es la información importante con el fin de calibrar el rendimiento de su red.

Aquí les presentamos algunos indicadores importantes que un/una administrador/a de red comúnmente investiga:

Estadísticas de la red inalámbrica

- Señal y ruido recibidos desde todos los nodos del backbone
- Número de estaciones asociadas
- Redes y canales adyacentes detectados
- Retransmisiones excesivas
- Tasa de datos en los radios, si usa adaptación automática

Estadísticas del conmutador

- Uso de ancho de banda por puerto del conmutador
- Uso de ancho de banda discriminado por protocolo
- Uso de ancho de banda discriminado por direcciones MAC
- Porcentaje de paquetes de difusión respecto al total
- Pérdida de paquetes y tasa de error

Estadísticas de Internet

- Uso de ancho de banda por anfitrión y por protocolo
- Solicitudes a la caché del servidor proxy
- Los 100 sitios más visitados
- Solicitudes de DNS
- Número de correos entrantes, correos spam, correos rebotados
- Tamaño de la cola de correos entrantes
- Disponibilidad de servicios críticos (servidores web, servidores de correo, etc)
- Tiempos ping y tasa de pérdida de paquetes a su ISP
- Estatus de los respaldos

Estadísticas de salud del sistema

- Uso de memoria
- Uso del archivo Swap
- Conteo de procesos / Procesos zombie

- Carga del sistema
- Voltaje y carga del UPS
- Temperatura, velocidad del ventilador y voltajes del sistema
- Estatus del SMART del disco
- Estatus del arreglo RAID

Esta lista debería usarse como una sugerencia de dónde comenzar. A medida que su red madure, es probable que usted encuentre nuevos indicadores del rendimiento de su red, y por supuesto, debería analizarlos también. Hay muchas herramientas gratuitas disponibles que van a darle tantos detalles como desee sobre lo que pasa en su red. Usted debería considerar el monitoreo de la disponibilidad de cualquier recurso cuando la no-disponibilidad pueda afectar negativamente a los usuarios.

Por ejemplo, sus usuarios podrían discar hacia módems de su sitio para conseguir acceso remoto a su red. Si todos los módems están usados o son defectuosos, los usuarios no tendrán acceso y probablemente se quejen. Se puede predecir y evitar este problema monitorizando el número de módems disponibles y suministrar capacidad extra antes del colapso.

No olvide monitorizar la máquina monitora misma, por ejemplo el uso de la CPU y el espacio de disco para recibir advertencias por adelantado si se sobrecarga o falla. Una máquina monitora que tiene pocos recursos puede afectar su capacidad de monitorizar la red efectivamente.

Tipos de herramientas de monitoreo

Ahora veremos varios tipos de herramientas de monitoreo. Las herramientas de ***detección de red*** escuchan las balizas (beacons) enviadas por los puntos de acceso inalámbricos y presentan información como el nombre de la red, intensidad de la señal recibida, y canal. Las herramientas de monitoreo puntual están diseñadas para resolución de problemas y suelen funcionar interactivamente por períodos cortos. Un programa como ping puede considerarse como una herramienta de monitoreo puntual activa, puesto que genera tráfico sondeando a una máquina específica. Las herramientas de monitoreo puntual pasivas incluyen ***analizadores de protocolo***, que inspeccionan cada paquete de la red y proporcionan detalles completos sobre cualquier conversación de red (incluido direcciones de fuente y destino, información de protocolo, e incluso datos de aplicación). Las herramientas de ***predicción*** realizan monitoreo sin supervisión por períodos largos, y comúnmente presentan los resultados en una gráfica. Las herramientas de ***monitoreo en tiempo real*** hacen un monitoreo similar, pero le avisan al/la administrador/a cuando detectan un problema. Las herramientas de ***medida de caudal*** informan sobre el ancho de banda real disponible entre dos puntos en la red. Las herramientas de ***detección de intrusos*** supervisan el tráfico indeseable o inesperado y toman las medidas apropiadas (normalmente negando acceso y/o notificando al/la administrador/a). Finalmente, las herramientas de benchmarking, calculan el rendimiento máximo de un servicio o de una conexión de red.

Detección de redes

Las herramientas de monitoreo comunes, simplemente proveen una lista de redes disponibles con información básica (tal 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 intensidad de señal recibida desde el punto de acceso en uso.
- **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://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.

Herramientas de monitoreo puntual

¿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", se hace necesario aislar la ubicación exacta del problema. Estas herramientas lo van a ayudar a determinar exactamente dónde se encuentra el problema.

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 cuánto tiempo lleva obtener una respuesta.

Saber adónde dirigir el *ping* 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 con *ping*:

```
$ 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 los paquetes ping de retorno tienen un ***TTL*** (***Time to Live***) inusualmente bajo, puede que haya problemas de enrutamiento entre su computadora y el extremo remoto. ¿Pero, qué sucede si ping no obtiene respuesta? 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 defecto:

```
$ 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 defecto, 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 del rango de cobertura?

El diagnóstico de problemas de la red con ping es casi un arte, pero es muy útil. Ya que probablemente 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 descartan 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. Al ejecutar 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
 9. w2.rc.vip.dcn.yahoo.com           0.0%     3   91.2  93.1  90.8  99.2   4.1
```

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.

Analizadores de protocolos

Los analizadores de protocolos de redes proporcionan 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 populares (y gratuitos) de protocolos de redes:

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, información de identificación (*fingerprinting*) del AP, detección de Netstumbler, e integración de 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.

Figura 6.12: Kismet en un Internet Tablet Nokia 770.

Como utiliza el modo de monitoreo pasivo de la tarjeta de radio, hace todo esto sin transmitir ningún dato. Kismet es una herramienta valiosa para el diagnóstico de problemas de redes inalámbricas.

KisMAC

http://kismac.macpirate.ch/. 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 escáner pasivo que registra datos en el disco, en un formato PCAP compatible con Wireshark. Admite un rastreo pasivo con tarjetas AirportExtreme así como una variedad de tarjetas inalámbricas USB.

tcpdump

http://www.tcpdump.org/. **tcpdump** es una herramienta de línea de comando para el monitoreo de tráfico de red. No tiene los detalles cosméticos de *wireshark*, pero usa menos recursos. Tcpdump puede captar y presentar toda la información de protocolo de red hasta la capa de enlace. Puede mostrar todos los encabezados de los paquetes y datos recibidos o sólo los paquetes que cumplan con un criterio determinado. Los paquetes captados con tcpdump pueden ser cargados en wireshark para realizar análisis y diagnósticos posteriores. Esto es muy útil cuando se quiere monitorizar una interfaz o un sistema remoto y traerse un archivo hasta su máquina para analizarlo. Tcpdump se halla disponible como herramienta estándar en los sistemas derivados de Unix (Linux, BSD, y Mac OS X). Hay también una versión Windows llamado ***WinDump*** disponible en *http://www.winpcap.org/winpdump/*.

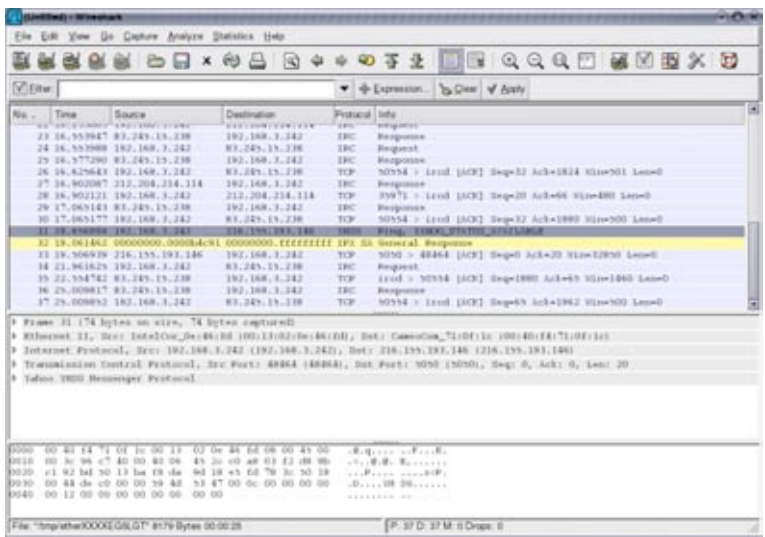


Figura 6.13: Wireshark (antes Ethereal) es un analizador de protocolo de red muy poderoso que puede mostrar todos los detalles que se deseen sobre los paquetes.

Wireshark

http://www.wireshark.org/. Antes conocido como **Ethereal**, **wireshark** es un analizador de protocolo de red gratuito para Unix y Windows. Ha sido calificado como “El Analizador de Protocolo de Red Más Popular del Mundo”.

Wireshark le permite examinar los datos de una red en vivo o de un archivo copiado desde un disco y examinar y clasificar los datos captados. Tanto el resumen como la información detallada de cada paquete están disponibles, incluidos los encabezados completos y fragmentos de los datos. Wireshark tiene algunas características muy poderosas, como un filtro de despliegue muy rico, y la capacidad de ver la cadena reconstruida de una sesión TCP.

Puede ser desalentador usarlo por primera vez o cuando las capas OSI no nos son familiares. Es comúnmente empleado para aislar y analizar tráfico específico desde o hacia una dirección IP, pero también puede usarse como una herramienta de uso general para detección de problemas. Por ejemplo, una máquina infestada con un gusano o un virus puede detectarse buscando la máquina que envía el mismo tipo de paquetes TCP/IP a un gran número de direcciones IP.

Herramientas de predicción

Las herramientas de predicción se usan para ver cómo se está usando su red en un determinado período. Funcionan monitorizando periódicamente la actividad de red y representándola de manera legible humanamente (gráficas, por ejemplo). Estas herramientas recolectan datos, los analizan y los presentan.

A continuación hay algunos ejemplos de herramientas de predicción. Algunas necesitan usarse en combinación con otras ya que no son programas independientes.

MRTG

http://oss.oetiker.ch./mrtg/. El ***Multi Router Traffic Grapher*** (***MRTG***) monitoriza la carga de tráfico en enlaces de red usando SNMP. MRTG genera gráficas que dan una representación visual del tráfico entrante y saliente. Estas gráficas se presentan normalmente en una página web.

MRTG puede ser un poco confuso de instalar, especialmente si no se está familiarizado con SNMP. Pero una vez instalado, MRTG virtualmente no requiere mantenimiento, a menos que usted cambie algo en el sistema que se está monitorizando (como su dirección IP).

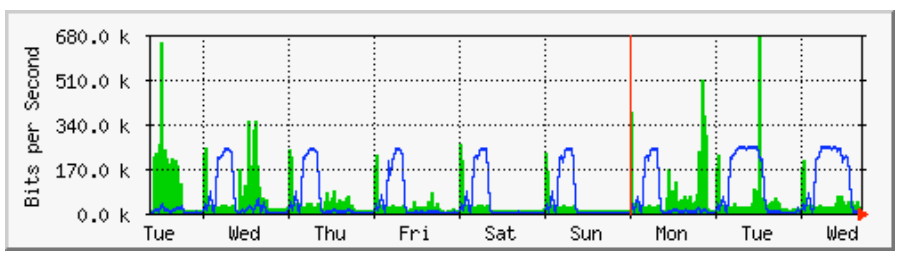


Figura 6.14: MRTG es probablemente el graficador de flujo instalado más a menudo.

RRDtool

http://oss.oetiker.ch/rrdtool/. ***RRD*** es la sigla de ***Round Robin Database***. RRD es una base de datos que almacena información de manera muy compacta que no se expande con el tiempo. ***RRDtool*** se refiere a un conjunto de herramientas que permiten crear y modificar bases de datos RRD, así como a generar gráficas útiles para representar los datos. Se usa para mantener el registro de datos en series de tiempo (como ancho de banda de la red, temperatura del cuarto de máquinas, o promedio de carga del servidor), y puede presentar estos datos como un promedio en el tiempo.

Note que RRDtool, en sí mismo, no hace contacto con los dispositivos de red para recuperar los datos. Es meramente una herramienta de manipulación de bases de datos. Se puede usar simplemente un guión (*shell o Perl*, normalmente) para que haga este trabajo por usted. RRDtool es también utilizado por muchos *front-ends* (interfaz de usuario) con todas las funcionalidades que presentan una interfaz amigable para configuración y despliegue. Las gráficas RRD le dan más control que MRTG sobre las opciones de presentación y número de elementos disponibles en la gráfica.

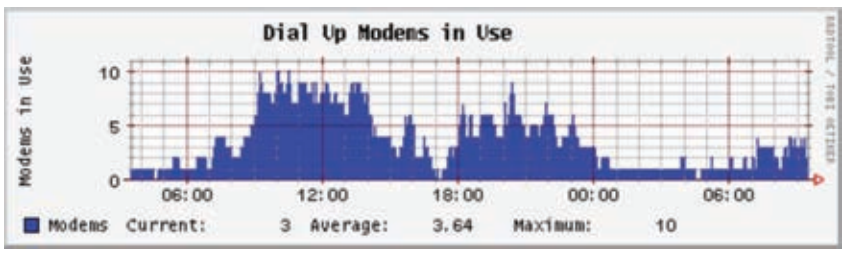


Figura 6.15: RRDtool le da mucha flexibilidad en cuanto a la forma de presentar los datos de red recolectados.

RRDtool ya forma parte de todas las distribuciones de Linux modernas y puede descargarse desde *http://oss.oetiker.ch/rrdtool/*.

ntop

http://www.ntop.org. Para el análisis histórico de tráfico y uso, considere **ntop**. Este programa elabora un informe detallado en tiempo real sobre el tráfico de red observado y presentado en su navegador de web. Se integra con rrdtool y elabora gráficas y diagramas que describen visualmente cómo se está usando la red. En redes de mucho tráfico ntop puede usar mucho CPU y espacio de disco, pero le ofrece una buena visión sobre el uso de su red. Funciona con Linux, BSD, Mac OS X, y Windows.

Algunas de sus ventajas más útiles son:

- La presentación del tráfico puede clasificarse de diversas maneras (fuente, destino, protocolo, direcciones MAC, etc.)
- Las estadísticas de tráfico están agrupadas por protocolo y número de puerto
- Una matriz de tráfico IP que muestra las conexiones entre máquinas

- Flujos de red para enrutadores y conmutadores que utilizan el protocolo NetFlow
- Identificación del sistema operativo del anfitrión
- Identificación del tráfico P2P
- Múltiples cuadros de gráficas
- API Perl, PHP, y Python

Ntop se puede descargar de *http://www.ntop.org/* y hay versiones para la mayoría de los sistemas operativos. A menudo se incluye en las distribuciones más populares como Red Hat, Debian, y Ubuntu. Aunque puede dejarse funcionando para colectar datos históricos, hace un uso bastante intensivo de la CPU, dependiendo del tráfico observado. Si lo va a utilizar por largos períodos debería estar pendiente del uso de CPU en la máquina de monitoreo.

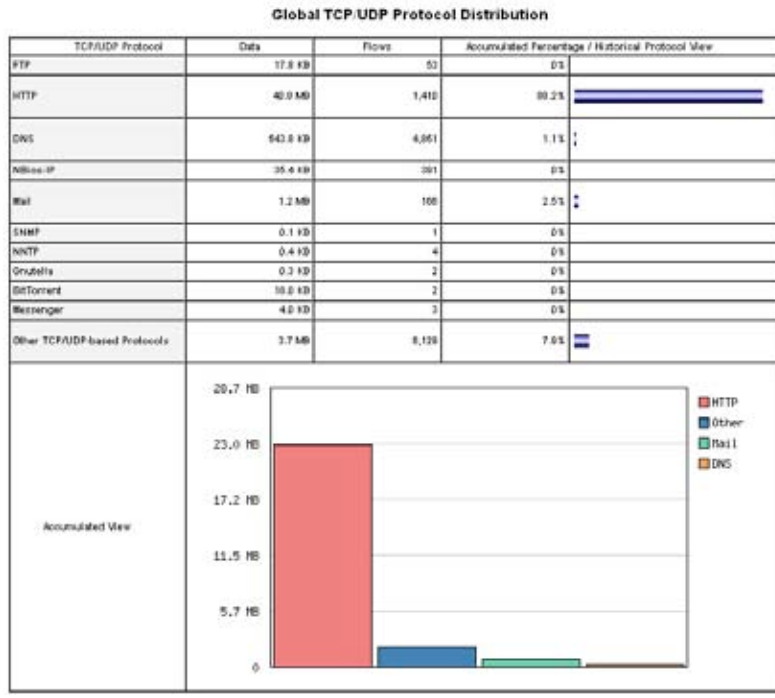


Figura 6.16: ntop presenta una información detallada sobre el uso de su red por varios clientes y servidores.

La principal desventaja de **ntop** es que no da información instantánea, sino promedios y totales a largo plazo. Esto puede hacer que se vuelva difícil diagnosticar un problema repentino.

Cacti

http://www.cacti.net/. ***Cacti*** es un front-end (interfaz de usuario) para RRDtool. Almacena toda la información necesaria para crear gráficas en una base de datos MySQL. El front-end está escrito en PHP. Cacti hace el trabajo de mantener las gráficas, fuentes de datos, y maneja la propia recolección de los datos. Hay soporte para los dispositivos SNMP, y se pueden escribir guiones específicos para sondear casi cualquier evento de la red.

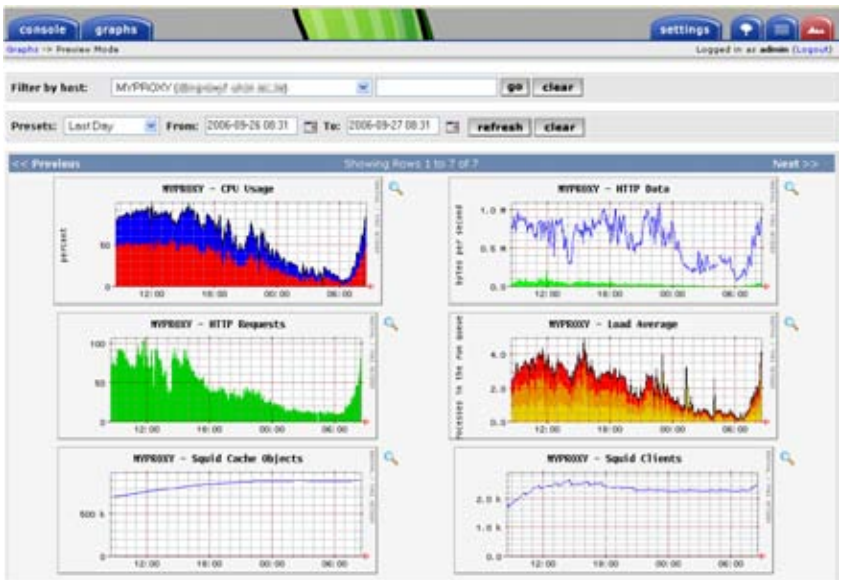


Figura 6.17: Cacti puede manejar el sondeo de sus dispositivos de red, y puede estructurar presentaciones visuales complejas y con mucha información sobre el comportamiento de la red

Cacti puede ser complicado de configurar, pero una vez que entendamos la documentación y los ejemplos puede proporcionar gráficos impresionantes. Hay cientos de plantillas para varios sistemas en el sitio web de cacti, y el código se está actualizando a gran velocidad.

NetFlow

NetFlow es un protocolo para colectar información sobe tráfico inventado por Cisco. En el sitio web de Cisco tenemos esta cita:

> *NetFlow IOS de Cisco proporciona de manera eficiente un conjunto de servicios clave para aplicaciones IP, incluidos examen de tráfico de la red, facturación basada en el uso, planeamiento de red, seguridad, capacidades de monitoreo de Denegación de Servicio y monitoreo de red. NetFlow ofrece información valiosa sobre los usuarios de la red y aplicaciones, tiempos de uso pico, y enrutamiento de tráfico.*

Los enrutadores Cisco pueden generar información NetFlow disponible desde el enrutador bajo la forma de paquetes UDP. NetFlow también hace menos uso de CPU en los enrutadores Cisco que cuando se usa SNMP. También presenta información más atomizada que SNMP, lo que permite tener una visión más detallada del uso de puerto y de protocolo.

Esta información se recoge a través de un colector NetFlow que almacena y presenta los datos como un acumulado en el tiempo. Al analizar los datos de flujo se puede armar un cuadro del flujo y el volumen del tráfico en una red o una conexión. Existen varios colectores NetFlow tanto comerciales como gratuitos. Ntop es una herramienta gratuita que puede funcionar como un colector y explorador NetFlow. Otra herramienta es Flowc (descrita a continuación).

También podría usarse NetFlow como herramienta de monitoreo puntual (spot check) al examinar una instantánea de los datos generados en una crisis de red. Considere NetFlow como una alternativa a SNMP para los dispositivos Cisco. Para más información sobre NetFlow: *http://en.wikipedia.org/wiki/Netflow*.

Flowc

http://netacad.kiev.ua/flowc/. **Flowc** es un colector NetFlow de fuente abierta (vea NetFlow arriba). Es liviano y de fácil configuración. Usa una base de datos MySQL para almacenar información acumulada de tráfico, por lo tanto, le permite generar su propio informe a partir de los datos usando SQL, o usar el generador de informes incluido. El generador de informes incluido produce los informes en HTML, sólo texto, o formato gráfico.

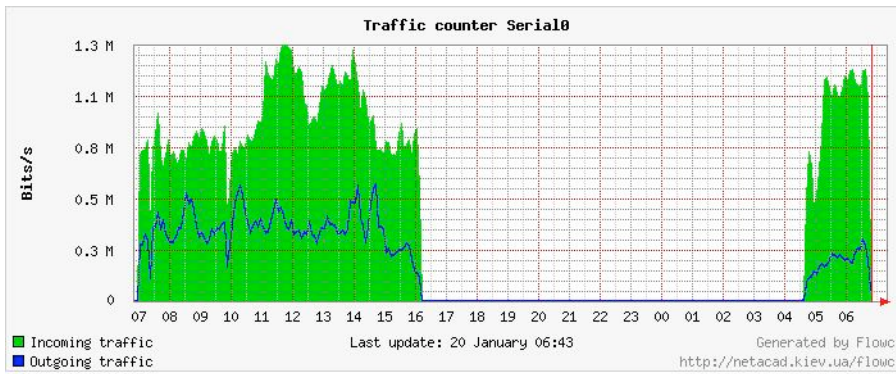


Figura 6.18: Gráfica típica de flujo generada por Flowc

La gran brecha entre los datos probablemente indica una falla en la red. Las herramientas de predicción normalmente no notifican sobre las fallas sino que únicamente registran su ocurrencia. Para tener notificación del momento en que ocurre un problema de red, debe usarse una herramienta de monitoreo en tiempo real, como Nagios (ver más adelante).

SmokePing

http://oss.oetiker.ch/smokeping/. **SmokePing** es una herramienta de lujo para medir latencia, escrita en Perl. Puede medir, almacenar, y presentar la latencia, su distribución y la pérdida de paquetes, todo en una sola gráfica. SmokePing usa RRDtool para almacenamiento de datos, y puede darnos gráficos muy completos que presenten información al minuto sobre el estado de su conexión de red.

Es muy útil ejecutar SmokePing en un anfitrión que tenga buena conectividad a toda su red. A medida que el tiempo pasa, se revelan las tendencias que pueden señalarnos cualquier tipo de problemas de red. En combinación con MRTG (**página 189**) o Cacti (**página 192**) se puede observar el efecto que tiene la congestión de la red sobre las pérdidas de paquetes y la latencia. SmokePing puede opcionalmente enviar alertas en presencia de ciertas condiciones, como cuando se observa una gran pérdida de paquetes durante un largo tiempo. Un ejemplo de cómo actúa SmokePing se presenta a continuación:

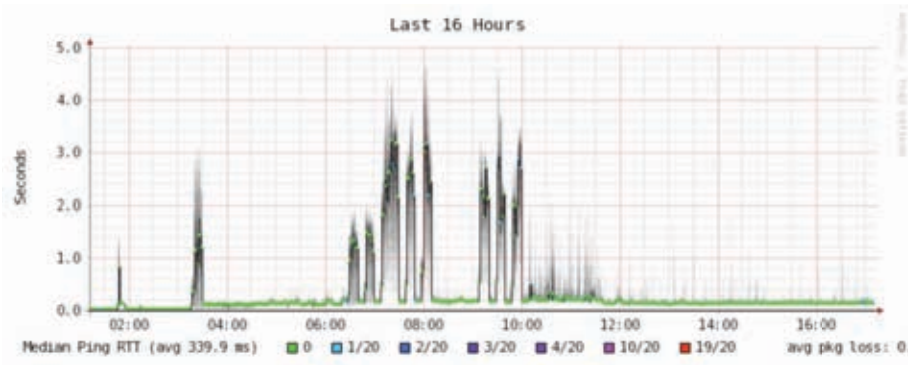


Figura 6.19: SmokePing puede presentar simultáneamente pérdida de paquetes y fluctuaciones de latencia en la misma gráfica.

EtherApe

http://etherape.sourceforge.net/. **EtherApe** proporciona una representación gráfica del tráfico de red. Los anfitriones y los enlaces cambian de tamaño dependiendo del tamaño del tráfico enviado y recibido. Los colores cambian para representar el protocolo más usado. Igual que con wireshark y tcpdump, los datos pueden ser captados "directamente desde el cable" a partir de una conexión de red en tiempo real, o leídos a partir de un archivo de captura tcpdump.

EtherApe no muestra tanto detalle como ntop, pero necesita muchos menos recursos.

iptraf

http://iptraf.seul.org/. **IPTraf** es un monitor de LAN liviano pero poderoso. Tiene una interfaz **ncurses** y se ejecuta desde un shell de comando. IPTraf se toma un tiempo para medir el tráfico observado, y luego presenta varias estadísticas, incluidas las conexiones TCP y UDP, información ICPM y OSPF,

flujo de tráfico, errores de la suma de comprobación IP, y otros. Es un programa de uso sencillo que usa muy pocos recursos de sistema.

Aunque no mantiene un histórico de los datos, es útil para ver un informe instantáneo de uso.

Figura 6.20: Despliegue de estadísticas de tráfico por puerto usando Iptraf

Argus

http://qosient.com/argus/. ***Argus*** es el acrónimo de ***Audit Record Generation an Utilization System***. También es el nombre del gigante de los cien ojos de la mitología griega.

Una cita de la página web de Argus:

> *Argus genera información de estadísticas de flujo, como conectividad, capacidad, demanda, pérdida, demora y fluctuación de tiempo (jitter) para cada transacción. Puede usarse para analizar e informar sobre el contenido de archivos de captación de paquetes, o puede funcionar como un monitor continuo examinando los datos de una interfaz en vivo; generando una bitácora (audit log) de toda la actividad de red observada en el flujo de paquetes. Argus puede desplegarse para monitorizar sistemas individuales, o la actividad de una empresa completa. Como monitor continuo, proporciona modelos de manejo "push" y "pull" que permiten estrategias flexibles para la recolección de datos de auditoría de la red. Los clientes de datos Argus permiten una gama de operaciones, tales como clasificación, acumulación, archivo e informe.*

Argus tiene dos partes: Un colector master que lee los paquetes desde un dispositivo de red, y un cliente que conecta con el master y presenta la estadística de uso. Argus funciona en BSD, Linux y la mayor parte de los otros sistemas UNIX.

NeTraMet

http://freshmeat.net/projects/netramet/. ***NeTraMet*** es otra herramienta popular de análisis de flujo. Igual que Argus, NeTraMet consta de dos partes: un colector que reúne información estadística por vía de SNMP, y un administrador que especifica cuál flujo debe observarse. Los flujos se especifican utilizando un lenguaje simple de programación que define las direcciones que se usan en cada extremo, y que pueden incluir Ethernet, IP, información de protocolo, u otros identificadores. NeTraMet funciona en DOS y la mayoría de sistemas UNIX, incluidos Linux y BSD.

Prueba del caudal (throughput)

¿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.

Figura 6.21: Herramientas como esta de SpeedTest.net son bonitas, pero no siempre le dan una idea precisa sobre el desempeño de su red.

Aunque existen páginas web que pueden hacer una "prueba de velocidad" en su navegador (como *http://www.speedtest.net/* y *http://dslreports.com/stest*), esas pruebas producen resultados de exactitud decreciente a medida que el usuario se aleja 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 rol 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 tamaño 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 al azar. 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 diferentes 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.

bing

http://fgouget.free.fr/bing/index-en.shtml. En lugar de inundar de datos una conexión y ver cuánto tiempo toma completar la transferencia, **Bing** trata de calcular el caudal disponible de una conexión punto a punto analizando los tiempos de ida y vuelta de paquetes ICMP de varios tamaños. Aunque no siempre es tan preciso como una verdadera prueba de flujo, puede proporcionar un buen cálculo sin transmitir un gran número de bytes.

Puesto que bing trabaja con solicitudes de eco ICMP estándares, también puede calcular el caudal disponible sin la necesidad de ejecutar un cliente especial en el otro extremo, puede incluso tratar de estimar el caudal de otros enlaces fuera de su red. Ya que usa poco ancho de banda, bing puede darle una idea aproximada del rendimiento de la red sin incurrir en los costos que ocasionaría una prueba de inundación.

Herramientas de tiempo real

Es deseable saber cuándo hay gente tratando de penetrar su red, o cuándo falla alguna de sus partes. Ya que ningún/a administador/a puede monitorizar la red todo el tiempo, hay programas que monitorizan la red y le envían alertas cuando hay eventos notables. A continuación presentamos algunas herramientas de fuente abierta que pueden ser de ayuda en este aspecto.

Snort

Snort (*http://www.snort.org/)* es un analizador y registrador de paquetes (packet sniffer and logger) que puede usarse como un sencillo sistema de detección de intrusos. Realiza registros basados en reglas y puede efectuar análisis de protocolos, búsqueda de contenido y correlación de paquetes. Puede usarse para detectar una variedad de ataques e intentos, como exploración de puertos disimulada, ataques CGI, sondeos SMB, intentos de identificación (fingerprinting) de sistema operativo y muchas otras clases de tráfico anómalo. Snort tiene una capacidad de alertar en tiempo real que le permite notificar al administrador sobre problemas en el momento en que ocurren, por medio de una variedad de métodos.

Instalar y ejecutar Snort no es tarea fácil y, dependiendo del tráfico de su red, va a necesitar una máquina monitora dedicada con considerables recursos. Afortunadamente, Snort está muy bien documentado, y tiene una comunidad de usuarios muy fuerte. Implementando un conjunto exhaustivo de reglas Snort, usted puede identificar comportamiento inesperado que, de otra manera, le consumirían misteriosamente el ancho de banda hacia Internet.

Vea *http://snort.org/docs/* para tener una lista extensa de recursos de instalación y configuración.

Apache: mod_security

ModSecurity (*http://modsecurity.org*) es un motor de fuente abierta para prevención y detección de intrusos para aplicaciones web. Este tipo de herramienta de seguridad también es conocido como ***cortafuego de aplicación web***. ModSecurity incrementa la seguridad de aplicaciones web contra ataques conocidos y desconocidos. Puede usarse solo, o como un módulo del servidor web Apache (*http://www.apache.org/*).

Hay una variedad de fuentes para reglas actualizadas mod_security que ayudan a protegerse contra los últimos ataques de seguridad. Un recurso excelente es GotRoot, que mantiene un gran almacén de reglas actualizadas con frecuencia:

http://gotroot.com/tiki-index.php?page=mod_security+rules

La seguridad de las aplicaciones web es importante en la defensa contra los ataques a su servidor web que podrían resultar en el robo de datos personales valiosos, o en el uso del servidor para lanzar ataques o enviar spam a otros usuarios. Además de ser perjudicial para la red en su totalidad, estas intrusiones pueden reducir considerablemente su ancho de banda.

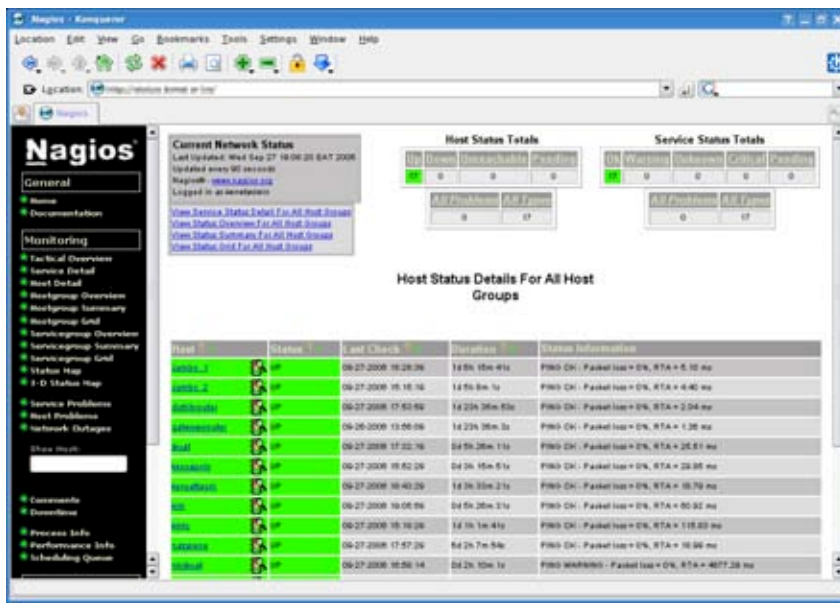


Figura 6.22: Nagios lo/la mantiene informado/a sobre el momento en que la red falla, o cuando hay una interrupción de servicio.

Nagios

Nagios (*http://nagios.org*) es un programa de monitoreo de anfitriones y servicios de su red, que le notifica inmediatamente los problemas en el momento en que ocurren. Estos avisos pueden ser por correo, por SMS, o ejecutando un

guión, y serán enviados a la persona relevante, o al grupo dependiendo de la naturaleza del problema. Nagios funciona en Linux o BSD, y proporciona una interfaz web para mostrar la situación de la red hasta el último minuto.

Nagios es extensible, y puede monitorizar el estatus de casi cualquier evento en la red. Realiza comprobaciones por medio de la ejecución de guiones pequeños a intervalos regulares y contrasta los resultados comparándolos con una respuesta esperada. Esto puede darnos revisiones más sofisticadas que un simple sondeo de red. Por ejemplo, ping (**página 185**) puede comprobar que una máquina está funcionando, y nmap, informa si un puerto TCP responde a pedidos, pero Nagios puede realmente recuperar una página web, o hacer un pedido de base de datos y verificar que la respuesta no es un error.

Nagios puede incluso dejarle saber cuándo el uso de ancho de banda, la pérdida de paquetes, la temperatura del cuarto de máquinas u otros indicadores de la salud de la red, traspasan un determinado umbral. Esto puede avisarle por adelantado sobre problemas potenciales y a menudo le permite resolverlos antes de que los usuarios se quejen.

Zabbix

Zabbix (*http://www.zabbix.org/*) es una herramienta de fuente abierta para monitoreo en tiempo real que funciona como un híbrido entre Cacti y Nagios. Usa una base de datos SQL para almacenamiento, tiene su propio paquete de presentación de gráficos, y realiza todas las funciones que usted esperaría de un monitor moderno en tiempo real (como sondeos SNMP y notificación instantánea de condiciones de error). Zabbix está cubierto por la GNU General Public License.

Otras herramientas útiles

Hay miles de herramientas de monitoreo de red gratuitas que satisfacen necesidades especiales. Les presentamos algunas de nuestras favoritas que no caen dentro de las categorías anteriores.

Drifnet 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/*.

ngrep

Ngrep proporciona la mayor parte de las características de identificación de patrones del grep de GNU, pero las aplica al tráfico de red. Normalmente reconoce IPv4 e IPv6, TCP, UDP, ICMP, IGMP, PPP, SLIP, FDDI, Token Ring y muchos más. Puesto que hace uso extenso de la concordancia de expresiones regulares (regular expression matches), es una herramienta apropiada para usuarios avanzados o los que tengan buen conocimiento de expresiones regulares.

Figura 6.23: Un collage de web generado por Etherpeg

Pero usted no tiene necesariamente que ser un experto en regex para hacer uso básico de ngrep. Por ejemplo, para ver todos los paquetes que contienen la cadena GET (presumiblemente solicitudes HTTP), pruebe lo siguiente:

```
# ngrep -q GET
```

La concordancia de patrones puede ser restringida aún más para combinarse con ciertos protocolos, puertos u otros criterios, usando filtros BPF. Este es el lenguaje de filtrado usado por las herramientas comunes de análisis de paquetes, como tcpdump y snoop. Para ver las cadenas de caracteres GET o POST enviadas al puerto de destino 80, use el siguiente comando:

```
# ngrep -q 'GET|POST' port 80
```

Usando ngrep de manera creativa usted puede detectar desde actividad de virus hasta correo spam. Puede descargarlo en *http://ngrepsourceforge.net/*.

¿Qué es lo normal?

Si usted está buscando la respuesta definitiva a la pregunta de cómo deberían verse sus patrones de tráfico, va a llevarse una desilusión. No hay respuesta cien por ciento correcta, pero con algún trabajo, podrá determinar lo que es normal en su red. Aunque cada entorno es diferente, algunos de los factores que pueden influir en el aspecto de su tráfico son:

- La capacidad de su conexión a Internet
- El número de usuarios que tienen acceso a la red

- Las políticas sociales (cobro por Bytes, cuotas, código de honor, etc.)
- La cantidad, tipos y nivel de los servicios ofrecidos
- La salud de la red (presencia de virus, tráfico de difusión excesivo, lazos de enrutamiento, relevadores de correo abiertos, ataques de denegación de servicios, etc.)
- La competencia de los usuarios de su red
- La ubicación y configuración de las estructuras de control (cortafuegos, servidores proxy, caches, etc.

Establecer una pauta de referencia (*baseline*)

Puesto que cada entorno es diferente, usted necesita determinar por sí mismo/a cuál es el aspecto normal de sus patrones de tráfico en condiciones normales. Esto es útil porque le permite identificar los cambios en el tiempo, bien sean repentinos o graduales. Estos cambios, a su vez, pueden ser indicadores de problemas actuales o potenciales en su red.

Por ejemplo, supongamos que su red se detiene y no está seguro/a de la causa. Afortunadamente, usted ha decidido mantener una gráfica de tráfico de difusión como porcentaje del tráfico global de la red. Si esta gráfica muestra un aumento repentino de tráfico de difusión, esto puede interpretarse como que la red ha sido infestada con un virus. Sin la idea apropiada de lo que es "normal" en su red (la pauta) podría no notar que el tráfico de difusión ha crecido, solo que éste es relativamente alto, lo cual no es necesariamente indicador de problemas.

Las gráficas y figuras de la pauta son también muy útiles cuando se quiere analizar los efectos de los cambios introducidos en la red. A menudo es conveniente experimentar con estos cambios probando diferentes valores. Saber cuál es el aspecto de su pauta le va a permitir apreciar si los cambios han mejorado o empeorado las cosas.

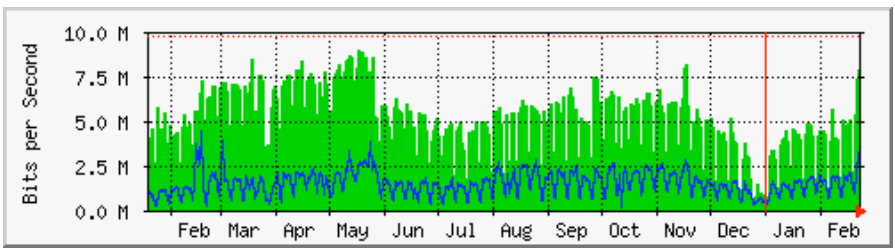


Figura 6.24: Al recoger datos por un período largo, usted podrá predecir el crecimiento de la red y resolver los problemas antes de que se presenten.

En la **Figura 6.24**, podemos observar el efecto que ha tenido sobre la red la implementación de "delay pools", alrededor del mes de mayo. Si no hubiéramos tenido una gráfica de la utilización de la línea, no hubiéramos sabido nunca cuál fue el efecto de este cambio en un período largo de tiempo. Cuando observe una gráfica de tráfico total después de haber hecho cambios, no debe suponer que

porque la gráfica no muestra cambios radicales, se ha perdido el tiempo. Usted podría haber sustituido uso frívolo de su línea por tráfico legítimo. Usted puede combinar esta pauta con otras, por ejemplo, los 100 sitios más contactados, o el uso promedio de los veinte usuarios más frecuentes para determinar si los hábitos de uso han cambiado. Como veremos, MRTG, RRDtool y Cacti, son herramientas excelentes que puede utilizar para mantener una pauta.

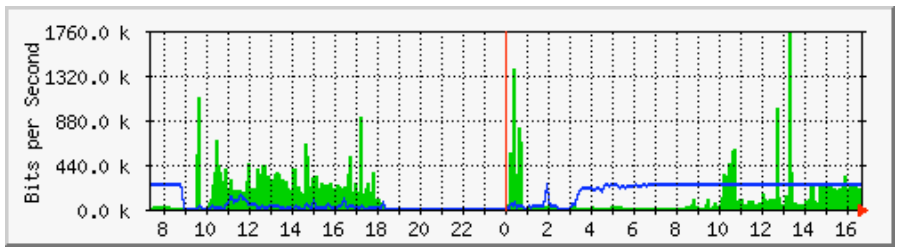


Figura 6.25: La tendencia del tráfico en Aidworld registrada en un solo día.

La **Figura 6.25** muestra el tráfico en un cortafuego durante un período de 24 horas. Aparentemente no hay nada raro en esta gráfica, pero los usuarios se quejaban de la lentitud de acceso a Internet.

La **Figura 6.26** muestra que el uso de ancho de banda de carga (área oscura) era más alto durante las horas laborales del último día que en los días previos. Un período de tráfico de carga fuerte comenzaba cada mañana a las 03:00, y terminaba hacia las 09:00. Pero el último día duró hasta las 16:40. La investigación posterior reveló la presencia de un problema con el software de respaldo que se ejecutaba a las 03:00 cada día.

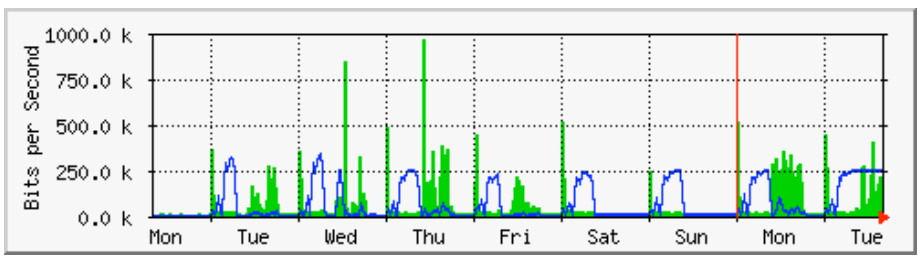


Figura 6.26: La misma red registrada durante una semana entera reveló un problema con los respaldos que les causaba a los usuarios una congestión inesperada.

La **Figura 6.27** muestra los valores de latencia en la misma conexión medidos por el programa SmokePing. La posición de los puntos muestra la latencia promedio mientras que el "humo" gris indica la distribución de la latencia (*jitter*). El color de los puntos indica la cantidad de paquetes perdidos. Esta gráfica de un período de cuatro horas no ayuda a identificar si hay o no problemas en la red.

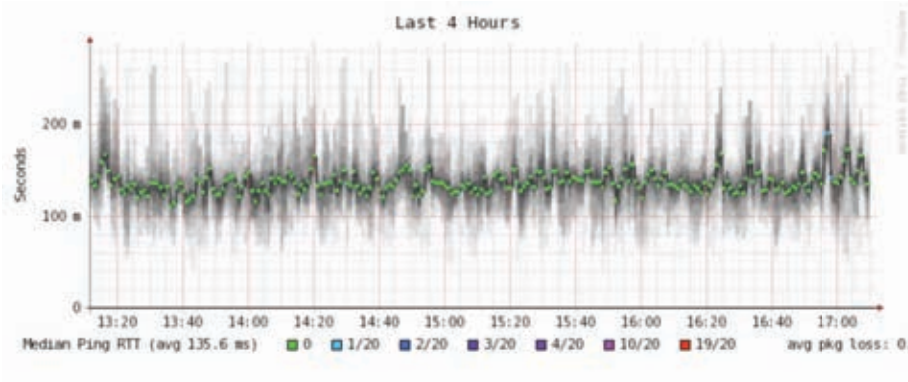


Figura 6.27: Cuatro horas de fluctuación de latencia (jitter) y pérdida de paquetes.

La próxima gráfica (**Figura 6.28**) muestra los mismos datos en un período de 16 horas. Eso indica que los valores de la gráfica superior están cerca de la pauta (*baseline*), pero que hay incrementos considerables de latencia a algunas horas temprano en la mañana, hasta 30 veces por encima de la pauta. Esto indica que debe haber un monitoreo extra de estas horas de la mañana para establecer las causas de la alta latencia, que van a ser probablemente algún tipo de tráfico pesado.

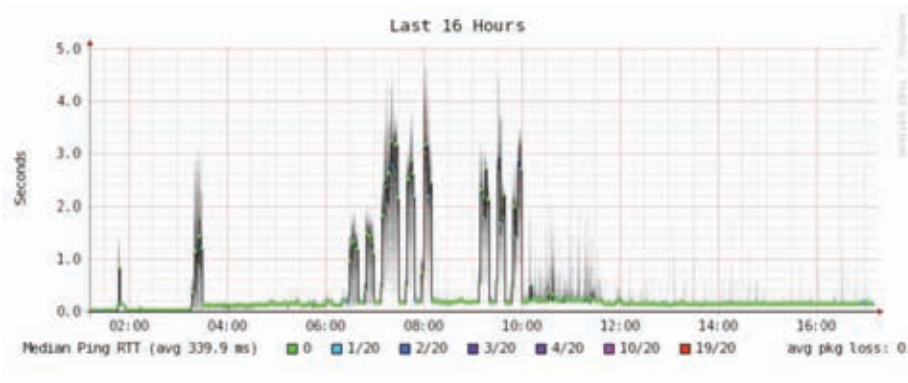


Figura 6.28: Un incremento de la variación de la latencia se muestra en un registro de 16 horas.

La **Figura 6.29** muestra que el martes fue significativamente peor que el domingo o el lunes respecto a la latencia, especialmente en el período de la mañana temprano. Esto podría indicar que algo ha cambiado en la red.

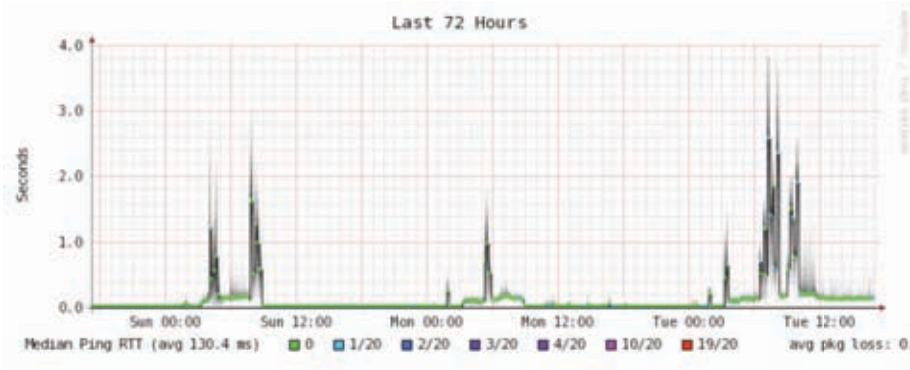


Figura 6.29: Cambiando la escala a una vista semanal revela una repetición definida del aumento de latencia y pérdida de paquetes a primeras horas de la mañana.

¿Cómo interpretar las gráficas de tráfico?

En una gráfica básica de flujo de red (como la generada por monitor de red MRTG) el área verde indica el tráfico entrante y la línea azul, el saliente. El tráfico entrante es tráfico que se origina en otra red (normalmente Internet), y va dirigido a un computador dentro de su red. El tráfico saliente se origina en su red y se dirige un computador en algún lugar de Internet. Dependiendo de qué clase de entorno de red se tenga, la gráfica le va a ayudar a entender cómo está siendo utilizada su red realmente. Por ejemplo, el monitoreo de servidores normalmente revela grandes cantidades de tráfico saliente cuando los servidores responden a las solicitudes (como enviar correos o abrir páginas web), mientras que las máquinas clientes de monitoreo pueden revelar grandes cantidades de tráfico entrante a las máquinas, cuando reciben datos desde los servidores.

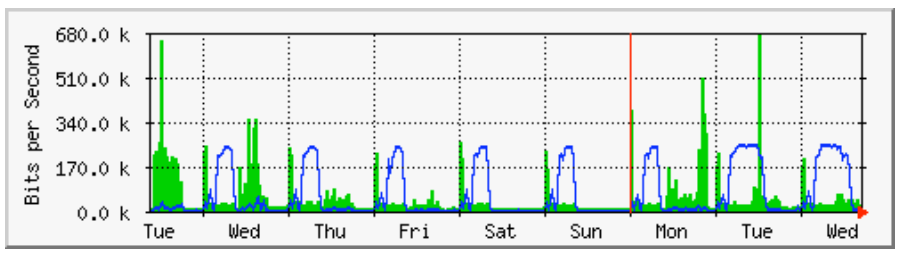


Figura 6.30: Gráfica clásica de flujo de red. El área oscura representa tráfico entrante, mientras que la línea representa el saliente. Los arcos repetidos de tráfico saliente muestran cuándo se ejecutan los respaldos nocturnos.

Los patrones de tráfico van a variar dependiendo de lo que use para el monitoreo. Un enrutador va normalmente a mostrar más tráfico entrante que saliente cuando los usuarios descargan datos desde Internet. Un exceso de ancho de banda saliente que no es transmitido por su servidor de red puede indicar un cliente par a par, un servidor no autorizado, o incluso un virus en uno o más clientes. No hay medidas establecidas que indiquen cómo debe aparecer

la relación entre tráfico saliente y entrante. Dependerá de usted establecer una pauta para entender cuáles son los patrones de tráfico normales en su red.

Detectando la sobrecarga de la red

La **Figura 6.31** muestra el tráfico de una conexión a Internet sobrecargada.

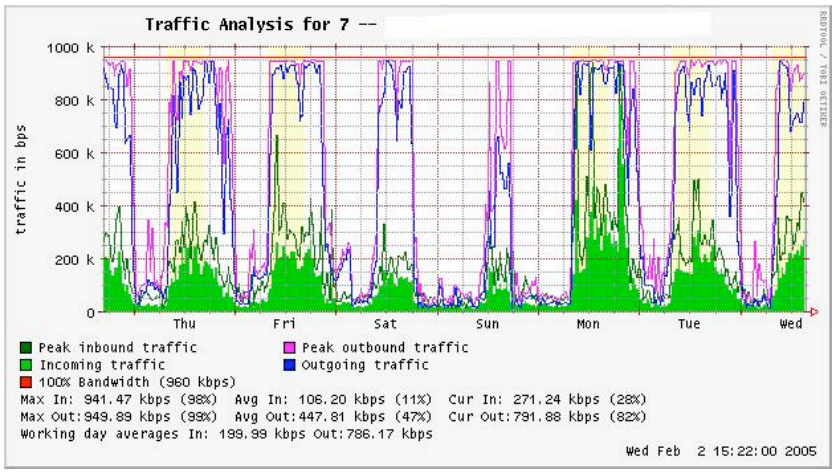


Figura 6.31: Las gráficas de traza plana en el tope indican que una línea está usando el ancho de banda máximo permitido, y que está sobreutilizada durante esos períodos.

La señal más obvia de sobrecarga va a ser la línea plana en el tope del tráfico saliente al mediodía cada día. Las líneas planas pueden indicar sobrecarga incluso si están muy por debajo de la capacidad teórica máxima del enlace. En este caso podría indicar que su proveedor no le está dando el ancho de banda que usted espera.

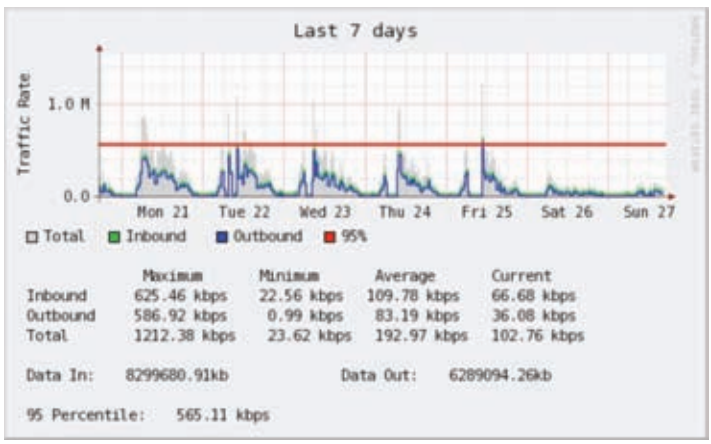


Figura 6.32: La línea horizontal muestra el valor del percentil 95.

Para medir el percentil 95

El percentil 95 es un cálculo muy usado en matemáticas para evaluar el uso sostenido y regular de una conexión de red. Su valor muestra el más alto consumo de tráfico en un período determinado. Calcular el percentil 95 significa que el 95% del tiempo el uso está por debajo de una cierta cantidad, y 5%, por encima de la misma. El percentil 95 es útil para mostrar el ancho de banda que se usa, al menos el 95% del tiempo.

MRTG y Cacti le van a hacer el cálculo del percentil 95. Esta es una gráfica de muestra de una conexión de 960 kbps. El percentil 95 es de 945 kbps después de descartar el 5% más alto del tráfico.

Monitoreo de RAM y uso del CPU

Por definición, los servidores dan servicios claves que deberían estar siempre disponibles. Los servidores reciben y responden las solicitudes de los clientes prestando servicios que constituyen la razón principal de tener una red. Por lo tanto, deben tener la capacidad de hardware suficiente para realizar la carga de trabajo. Esto significa que deben tener RAM adecuada, almacenamiento, y capacidad de procesamiento para atender todas las solicitudes de los clientes. De otra manera, el servidor se tardará en responder o, en el peor de los casos, va a ser incapaz de responder. Puesto que los recursos de hardware son finitos, es importante mantener un registro de cómo se usan sus recursos de red. Si un servidor central (como un servidor de correos o de proxy) se sobrecarga de solicitudes, los tiempos de acceso se enlentecen. Esto se percibe por parte de los usuarios como un problema de red.

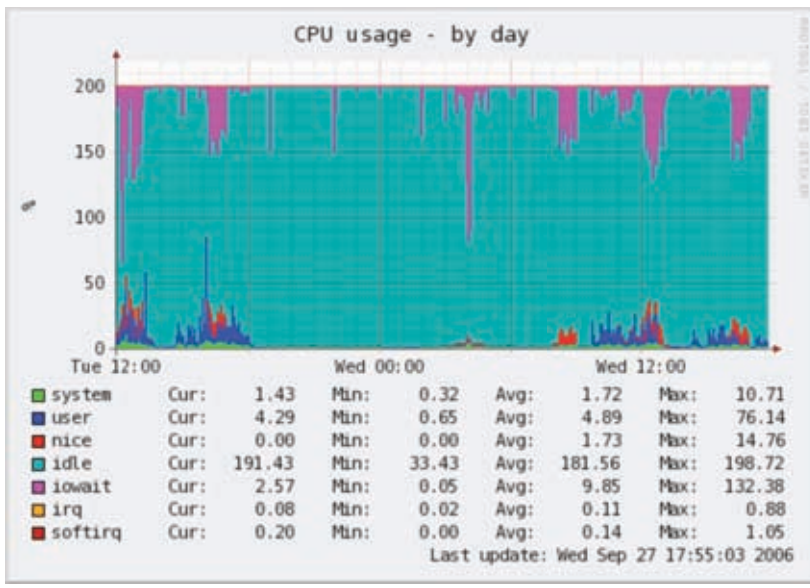


Figura 6.33: RRDtool puede mostrar datos arbitrarios como memoria y uso de CPU, expresados como promedio en el tiempo.

Hay varios programas que pueden usarse para el monitoreo de los recursos en un servidor. El método más simple en una máquina Windows es acceder el Task Manager usando las teclas **Ctrl Alt + Del** y luego hacer click en la Performance tab. En un sistema que ejecute Linux o BSD, puede escribir top en una ventana terminal. Para mantener registros históricos de este rendimiento, puede usarse MRTG o RRDtool (**página 190**).

Los servidores de correo requieren espacio adecuado, ya que algunas personas prefieren dejar sus mensajes en el servidor por largo tiempo. Los mensajes pueden acumularse y llenar el disco duro, especialmente si hay cuotas sin usar. Si el disco o la partición usada para almacenar correos se llenan, el servidor no puede recibir correos. Si ese disco es también usado por el sistema van a surgir todo tipo de problemas ya que el sistema operativo se queda sin espacio de intercambio (*swap space*) y de almacenamiento temporal.

El servidor de archivos necesita monitoreo, incluso si tiene discos grandes. Los usuarios van a encontrar la manera de llenar un disco de cualquier tamaño más rápido de lo esperado. El uso del disco puede ser reglamentado a través del uso de cuotas, o por simple monitoreo y advertencia al usuario de que está haciendo uso excesivo. Nagios puede avisarle cuándo el uso del disco, del CPU u otro recurso del sistema excede los niveles críticos.

Si una máquina deja de responder o se hace lenta, y las mediciones muestran que un recurso está sobre-usado, puede ser una indicación de que se necesita una actualización (*upgrade*). Si el uso del procesador excede constantemente el 60% del total, probablemente necesite actualizar el procesador. Las velocidades bajas pueden ser indicativas de RAM insuficiente. Asegúrese de comprobar el uso general de la CPU, RAM y espacio de disco antes de tomar la decisión de actualizar un componente en particular.

Una manera sencilla de comprobar si una máquina tiene suficiente RAM es observar la luz del disco duro. Cuando la luz permanece encendida, normalmente indica que la máquina está enviando grandes cantidades de datos hacia y desde el disco. Esto se conoce como ***thrashing*** y es muy malo para el rendimiento. Puede arreglarse averiguando cuál proceso está usando más RAM y abortarlo (*kill*) o reconfigurarlo. Si eso falla, el sistema necesita más RAM.

Debería determinar siempre si es más costo-efectiva la actualización de un componente individual, o comprar una máquina nueva. Algunas computadoras son difíciles o imposibles de actualizar y a menudo resulta más costoso reemplazar componentes individuales que el sistema completo. Como la disponibilidad de repuestos y de sistemas varía mucho en el mundo, asegúrese de ponderar el costo de los repuestos en comparación con el costo del sistema completo, incluidos el transporte y los impuestos, cuando determine el costo de la actualización.

7
Energía Solar

Este capítulo presenta una introducción a los componentes de un sistema fotovoltaico autónomo. La palabra autónomo (standalone) se refiere al hecho de que el sistema trabaja sin ninguna conexión a una red eléctrica establecida. En este capítulo se presentarán los conceptos básicos de la generación y almacenamiento de energía solar fotovoltaica. También presentaremos un método para diseñar un sistema solar funcional con acceso limitado a información y recursos. Este capítulo sólo discutirá el uso de la energía solar para la producción directa de electricidad (***energía solar fotovoltaica***). La energía solar también se puede utilizar para calentar fluidos (***energía solar térmica***) y puede ser usada como fuente de calor o para accionar una turbina para generar electricidad. Los sistemas de energía solar térmica están fuera de los objetivos de este capítulo.

Energía Solar

Un sistema fotovoltaico está basado en la capacidad que poseen ciertos materiales para convertir la energía luminosa en energía eléctrica.

A la energía luminosa incidente total por unidad de área se le denomina ***Irradianza Global*** (***G***) y se mide en ***vatios por metro cuadrado*** (**W/m²**). La ***insolación***, por otra parte, es la energía incidente por m² durante cierto tiempo, y así se habla, por ejemplo, de insolación horaria, diaria o mensual, como la energía incidente por unidad de superficie en una hora, un día, un mes respectivamente, y se suele expresar en **Wh/m²**.

Por supuesto, la cantidad exacta de radiación que llegará a la superficie terrestre en el lugar de la instalación no puede calcularse con gran precisión debido a las variaciones climáticas naturales. Por lo tanto, se hace necesario trabajar con datos estadísticos basados en la *"historia solar"* del lugar, datos normalmente recogidos en las estaciones meteorológicas, y recopilados en tablas y bases de datos. En la mayoría de los casos no encontraremos información detallada sobre un área específica y tendremos que trabajar con valores aproximados.

Existen varias organizaciones dedicadas a la producción de mapas que incluyen valores promedio de irradiación global diaria para una región. Estos valores también se conocen como ***horas de sol pico*** al día o ***HSP***. Se puede usar el HSP de la región para simplificar los cálculos. Una unidad de hora solar pico corresponde a una insolación de 1000 Vatios-hora por metro cuadrado. Si encontramos que un área determinada tiene 4 HSP en el peor mes, esto quiere decir que en ese mes no deberíamos esperar una irradiación diaria mayor de 4000 vatios/m2 por día. Encontramos mapas de HSP de baja resolución en numerosos recursos en línea, tales como *http://www.solar4power.com/solar-power-global-maps.html* o en *http://eosweb.larc.nasa.gov/cgi-bin/sse/sse.cgi?+s01+s03#s01.* Este último sitio contiene abundante información estadística de muchos lugares de la tierra obtenidos a través de satélites operados por la NASA y constituye una herramienta sumamente útil para el diseño de sistemas que utilizan energía solar[1]. También puede consultar alguna compañía local de energía solar o una estación meteorológica.

¿Qué hay sobre la energía eólica?

Es posible usar un generador eólico en lugar de paneles solares cuando se diseña un sistema autónomo para instalar en un cerro o montaña. Para que sea efectivo, la velocidad promedio del viento en el año debería ser de por lo menos 3 a 4 metros por segundo, y el generador eólico debería colocarse a 6 metros por encima de cualquier otro objeto en un radio de 100 metros. Las ubicaciones muy alejadas de las costas carecen en general de energía suficiente para operar un sistema de energía eólico. En términos generales, los sistemas fotovoltaicos son más confiables que los generadores eólicos ya que la luz del sol es más asequible que un viento constante en la mayoría de los sitios. Como contrapartida, los generadores eólicos pueden recargar sus baterías incluso en la noche, con la condición de que haya viento suficiente. También es posible usar el viento en conjunción con energía solar para ayudar a cubrir el tiempo en que haya nubosidades persistentes o cuando haya poco viento. En la mayor parte de los sitios, no se justifica el gasto de un buen generador eólico para añadir un poco de energía extra al sistema general. Este capítulo, por lo tanto, se enfocará en el uso de paneles solares para la generación de electricidad.

Componentes de un sistema fotovoltaico

Un sistema fotovoltaico básico consiste de cuatro componentes principales: el ***panel solar***, las ***baterías***, el regulador y la ***carga***. Los paneles son responsables por la recolección de la energía del sol y la generación de electricidad. La batería almacena la energía eléctrica para uso posterior. El regulador asegura que tanto el panel como la batería trabajen juntos de manera óptima. La carga se refiere a cualquier dispositivo que requiera de energía eléctrica, y es la suma del consumo de todo el equipo eléctrico conectado al sistema. Es importante recordar que tanto los paneles solares como las baterías

1. Comentario del revisor técnico de la edición en español.

usan corriente continua (DC). Si el rango de tensión de operación de su equipo no incluye la tensión de operación de la batería será necesario utilizar algún tipo de ***convertidor***. Si los equipos que se quieren alimentar utilizan una tensión continua diferente a la de la batería será necesario el uso de un ***convertidor DC/DC*** y si alguno de los equipos trabajan en corriente alterna necesitará un ***convertidor DC/AC***, también conocido como ***inversor***. Todo sistema eléctrico debería también incluir varios aditamentos de seguridad para el caso de fallas, tales como interruptores termo-magnéticos (breakers), dispositivos protectores contra picos de tensión, fusibles, cableado de tamaño apropiado, barras de tierra, pararrayos, etc.

El panel solar

El ***panel solar*** se compone de celdas solares que colectan la radiación solar y la transforman en energía eléctrica. A esta parte del sistema se la conoce generalmente como ***módulo solar*** o ***generador fotovoltaico***. Un ***banco de paneles*** se instala conectando un conjunto de paneles en serie y/o en paralelo a fin de proporcionar la energía necesaria para una carga específica. La corriente que da un banco de paneles varía proporcionalmente a la radiación solar. Esta variará en el tiempo debido a las condiciones climatológicas, la hora del día, la estación del año, etcétera.

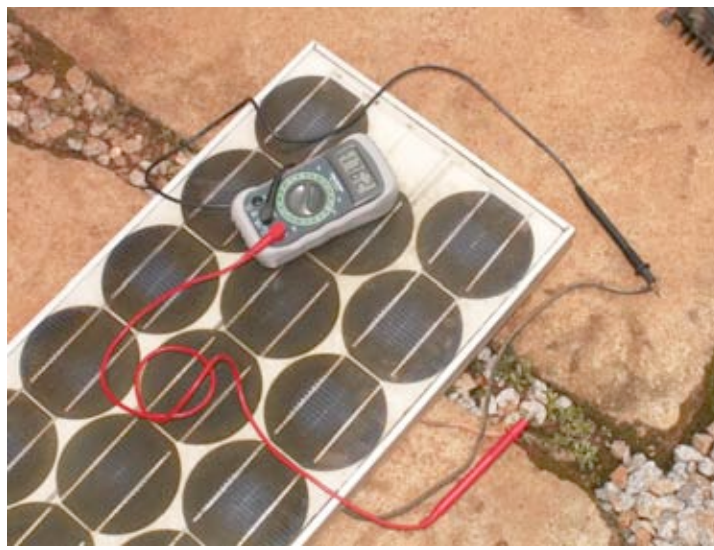


Figura 7.1: Un panel solar

Existen varias tecnologías en la manufactura de las células solares. La más común es la de silicio cristalino, que puede ser monocristalino o policristalino. El silicio amorfo puede ser más barato pero es menos eficiente en la conversión de energía solar en electricidad. Con una expectativa de vida reducida y de un 6 a 8% de eficiencia de conversión, el silicio amorfo es comúnmente utilizado para equipos de bajo consumo de energía, como las calculadoras portátiles. Nuevas

tecnologías solares como cintas de silicio y películas fotovoltaicas finas están en desarrollo en estos momentos y prometen una mayor eficiencia, pero no están muy difundidas todavía.

La batería

Almacena la energía producida por los paneles que no se consume inmediatamente para disponer de ella en periodos de baja o nula irradiación solar. Este componente es también llamado el ***acumulador***. Las baterías acumulan electricidad en forma de energía química. El tipo más común de batería empleado en aplicación solar es usualmente de plomo-ácido, también llamada recombinante o VRLA (plomo ácido, regulada por válvula, por sus siglas en inglés).

Figura 7.2: Batería de plomo-ácido de 200 Ah. El terminal negativo está roto por haberle aplicado todo el peso durante el transporte de la batería.

Además de almacenar energía, las baterías de plomo-ácido también cumplen dos funciones.

- Suministrar una potencia instantánea superior a la que el banco de paneles puede generar, necesaria para la puesta en marcha de algunos elementos (por ejemplo, el motor del frigorífico o una bomba).
- Determinar el margen de tensiones de trabajo de la instalación.

Para instalaciones de baja demanda de energía y donde haya restricciones de espacio se pueden usar otros tipos de baterías tales como NiCd, NiMh, o a iones de Li. Estas, sin embargo, necesitan un cargador/regulador especial y no pueden reemplazar directamente las de plomo-ácido.

El regulador

El ***regulador*** (o más formalmente, el r***egulador de carga de energía solar***) asegura que la batería funcione en condiciones apropiadas, evitando la ***sobrecarga*** y ***sobredescarga*** de la misma, fenómenos ambos muy perjudiciales para la vida de la batería. El procedimiento que utiliza para ello es determinar el ***estado de carga*** (***SoC***, por sus siglas en inglés) de la batería a partir de la tensión a la que ésta se encuentra. El regulador se programa en función de la tecnología de almacenamiento empleada por la batería, por lo que midiendo la tensión de la batería, determina con exactitud los umbrales precisos a los que desconecta la batería para evitar la sobrecarga o descarga excesiva.

Figura 7.3: Controlador de carga solar de 30 A

El regulador puede incluir otros elementos que añaden información valiosa y control de seguridad al equipo, tales como amperímetros, voltímetros, contadores de amperios-hora, temporizadores, alarmas, etcétera. Aunque convenientes, ninguno de estos elementos se requiere para el funcionamiento del sistema fotovoltaico.

El convertidor

La electricidad proporcionada por el módulo solar y la batería es continua (DC) a un voltaje fijo. Esta tensión podría no ser la requerida por la carga que se tiene. Un convertidor continua/alterna (DC/AC en inglés) también conocido como inversor, convierte la corriente continua de la batería en corriente alterna. El precio es que se pierde algo de energía en la conversión. Si fuera necesario, se puede usar el convertidor para obtener corriente continua a niveles de tensión diferentes a los proporcionados por las baterías. Los convertidores continua/continua también presentan pérdidas en la conversión. Para un funcionamiento

óptimo, a la hora de diseñar un sistema de comunicaciones que usa energía fotovoltaica es recomendable que todas las cargas trabajen a la tensión que suministran las baterías evitando el uso de convertidores.

Figura 7.4: Convertidor DC/AC.
Inversor con una potencia máxima de salida de 800 W

La carga

La ***carga*** está constituida por los equipos que se conectan al sistema y que consumen la energía del mismo (equipos de comunicaciones inalámbricas, enrutadores, estaciones de trabajo, iluminación, receptores de TV, módems VSAT, etc.).

Aunque no es posible saber con certeza absoluta cuál va a ser el consumo total de dichos equipos en operación, es vital hacer una buena estimación del mismo ya que de esto depende la funcionalidad del sistema. Asimismo, hay que tener cuidado en elegir equipos eficientes, para no derrochar energía. Por ejemplo, en escenarios donde sea necesario dimensionar equipos de comunicaciones por energía solar debemos utilizar equipos basados en arquitecturas de bajo consumo.

Ensamblando las partes

El sistema fotovoltaico incorpora todos estos componentes. Los paneles solares generan energía cuando se dispone de luz solar. El regulador garantiza la operación más eficiente de los paneles y previene posibles daños de las baterías. El banco de baterías almacena la energía recolectada para su uso posterior. Convertidores e inversores adaptan la energía almacenada para satisfacer las necesidades de la carga. Finalmente, la carga consume la energía

almacenada para efectuar el trabajo. Cuando todos los elementos están en equilibrio y reciben mantenimiento apropiado, el sistema se soportará a sí mismo durante años.

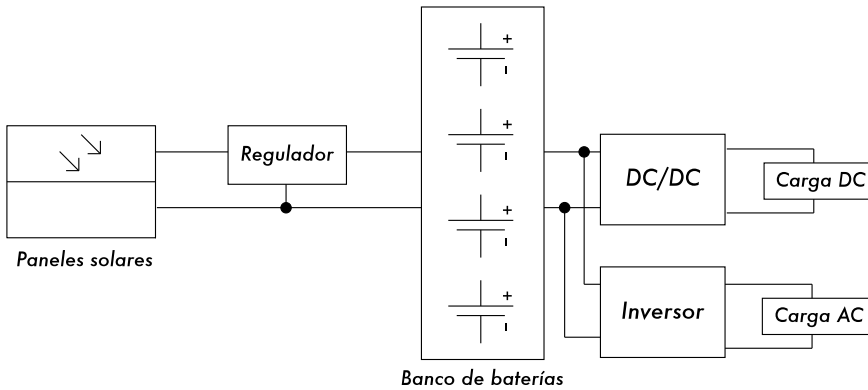


Figura 7.5: Una instalación solar con cargas DC (continuas) y AC (alternas)

Examinemos ahora cada uno de los componentes individuales del sistema fotovoltaico en más detalle.

El panel solar

Un panel solar individual está compuesto de muchas celdas solares. Las celdas están conectadas eléctricamente para proporcionar un valor específico de corriente y voltaje. Las celdas individuales están debidamente encapsuladas para asegurar aislamiento y protección de la humedad y la corrosión.

Figura 7.6: Efectos del agua y la corrosión en un panel solar

Hay diferentes tipos de módulos disponibles en el mercado dependiendo de las exigencias de potencia de su aplicación. Los módulos más comunes se componen de 32 ó 36 celdas solares de silicio cristalino. Estas celdas son todas de igual tamaño, asociadas en serie y encapsuladas entre vidrio y un material plástico, con una resina polimérica (EVA) como aislante térmico. El área del módulo varía comúnmente entre 0,1 y 0,5 m^2. Los paneles solares usualmente tienen dos contactos eléctricos, uno positivo y uno negativo.

Algunos paneles también incluyen contactos adicionales para permitir la instalación de ***diodos de paso*** a través de celdas individuales. Estos diodos protegen al panel contra un fenómeno conocido como "puntos calientes". Un "punto caliente" ocurre cuando algunas celdas están a la sombra mientras que el resto del panel está a pleno sol. En lugar de producir energía, las celdas a la sombra se comportan como una carga que disipa energía. En esta situación las celdas en la sombra pueden experimentar incrementos de temperatura (unos 85 a 100°C). Los diodos de paso previenen los puntos calientes de las celdas en sombra, pero reducen el voltaje máximo del panel. Estos diodos deberían usarse sólo cuando la sombra sea inevitable. Una mejor solución es exponer completamente el panel al sol, siempre que sea posible.

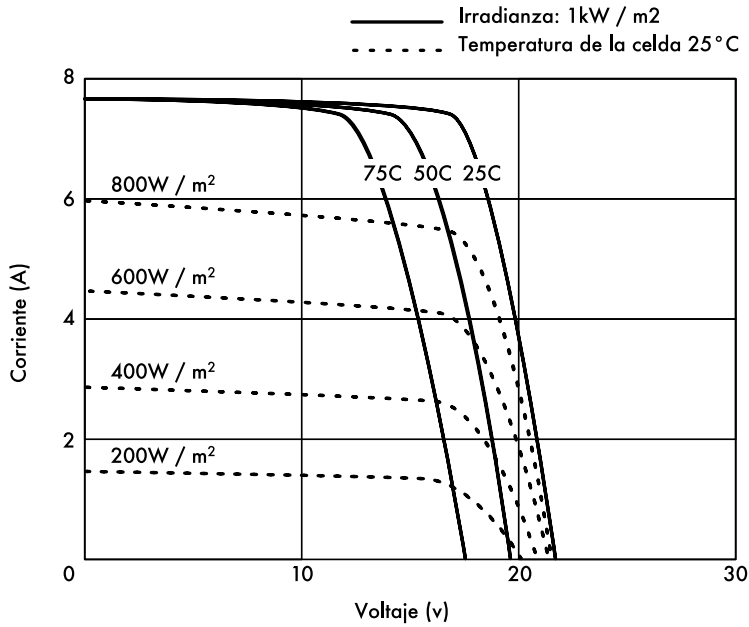


Figura 7.7: Diferentes curvas I-V. La corriente (A) cambia con la irradianza y el voltaje (V) cambia con la temperatura.

El rendimiento eléctrico de un módulo solar está representado por ***la curva característica I-V***, que representa la corriente generada en función del voltaje para una radiación específica.

La curva representa todos los valores posibles de voltaje-corriente. Las curvas dependen de dos factores principales: la temperatura y la radiación solar

recibida por las celdas. Para un área de una celda solar dada, la corriente generada es directamente proporcional a la irradianza solar (G), mientras que el voltaje se reduce ligeramente con un aumento de temperatura. Un buen regulador tratará de maximizar la potencia que proporciona un panel adaptándose al punto que proporciona el valor máximo del producto de la corriente y el voltaje (V x I). La potencia máxima se corresponde con el punto de quiebre de la curva I-V.

Parámetros del Panel Solar

Los principales parámetros que caracterizan un panel solar son:

1. **CORRIENTE DE CORTOCIRCUITO** (I_{SC}): Es la máxima intensidad de corriente que proporciona el panel, y corresponde a la corriente que entrega cuando se conectan directamente los dos bornes.
2. **TENSIÓN DE CIRCUITO ABIERTO** (V_{OC}): Es el máximo voltaje que proporciona el panel y ocurre cuando los bornes no están conectados a ninguna carga (circuito abierto). Voc suele ser de 22 V para paneles que vayan a trabajar a 12 V, y es directamente proporcional al número de celdas asociadas en serie.
3. **PUNTO DE MÁXIMA POTENCIA** (P_{max}): Es un punto de funcionamiento para el cual la potencia entregada es máxima, donde $P_{max} = I_{max} \times V_{max}$). El punto de máxima potencia del panel se mide en Vatios (W) o Vatios pico (W_P). Es importante no olvidar que en condiciones normales el panel no trabajará en condiciones pico ya que el voltaje de operación está determinado por la carga o la batería. Los valores típicos de V_{max} y de I_{max} son algo menores a los de I_{SC} y V_{OC}
4. **FACTOR DE FORMA** (El factor de forma es la relación entre la potencia máxima que el panel puede entregar y el producto de I_{SC} x V_{OC}. Da una idea de la calidad del panel porque es una medida de lo escarpada que es su curva característica, de forma que cuanto más se aproxima a la unidad, mayor potencia puede proporcionar. Los valores comunes suelen estar entre 0,7 y 0,8.
5. **EFICIENCIA O RENDIMIENTO** (η): Es el cociente entre la máxima potencia eléctrica que el panel puede entregar a la carga y la potencia de la radiación solar (P_L) que incide sobre el panel. Es habitualmente en torno al 10% dependiendo del tipo de celda (monocristalina, policristalina, amorfa o película delgada).

Considerando las definiciones de punto de máxima potencia y de factor de forma, tenemos que:

$$\eta = P_{max} / P_L = FF \cdot I_{SC} \cdot V_{OC} / P_L$$

Los valores de I_{SC}, V_{OC}, I_{Pmax} y V_{Pmax} son proporcionados por los fabricantes y hacen referencia a las condiciones estándar de medición con valores de

irradianza de G = 1.000 W/m^2, al nivel del mar, y para una temperatura de las celdas Tc = 25°C.

Los valores de los parámetros del panel cambian para otras condiciones de irradianza y temperatura. A menudo, los fabricantes incluyen gráficos o tablas con valores ajustados a condiciones diferentes del estándar. Es aconsejable revisar los valores de rendimiento para las temperaturas del panel que más se parezcan a su instalación particular.

Tenga presente que dos paneles pueden tener la misma Wp pero comportarse de manera distinta en condiciones de operación diferentes. Cuando adquiera un panel es importante verificar, en la medida de lo posible, que sus parámetros (por lo menos I_{SC}, y V_{OC}) coincidan con los valores prometidos por el fabricante.

Valores del panel necesarios para el dimensionado

Para calcular el número de paneles necesario para alimentar una determinada carga, es suficiente conocer los valores de intensidad y tensión para el punto de máxima potencia: I_{Pmax} and V_{Pmax}.

Usted debería recordar siempre que el panel no va a trabajar bajo condiciones ideales ya que ni la carga ni el sistema regulador van a trabajar siempre con el punto de máxima potencia del panel. Para compensar esto, se debe añadir en los cálculos una pérdida de eficiencia del 5%.

Interconexión de paneles

Un ***banco de paneles solares*** es un conjunto de paneles solares que están interconectados eléctricamente e instalados en algún tipo de estructura de soporte. El usar un banco de paneles le va a permitir generar una tensión o una corriente superiores a la que se genera con un solo panel. Los paneles están interconectados de manera que la tensión generada es próxima (pero mayor) que la tensión de las baterías, y la corriente producida es suficiente para alimentar el equipo y para cargar las baterías.

Conectar los paneles en serie aumenta la tensión generada mientras que conectarlos en paralelo incrementa la corriente. El número de paneles usados deberían incrementarse hasta que la cantidad de energía generada exceda ligeramente las demandas de su carga.

Es muy importante que todos los paneles de su banco sean lo más semejantes posible, de la misma marca y características, ya que cualquier diferencia en sus condiciones operativas afectarán en gran medida las condiciones y el desempeño de su sistema. Incluso paneles que tienen un desempeño idéntico van a presentar alguna variación en sus características debido a diferencias en el proceso de fabricación.

Cuando le sea posible, es buena idea probar el desempeño real de los paneles individuales para verificar sus características operativas antes de ensamblarlas en un banco de paneles.

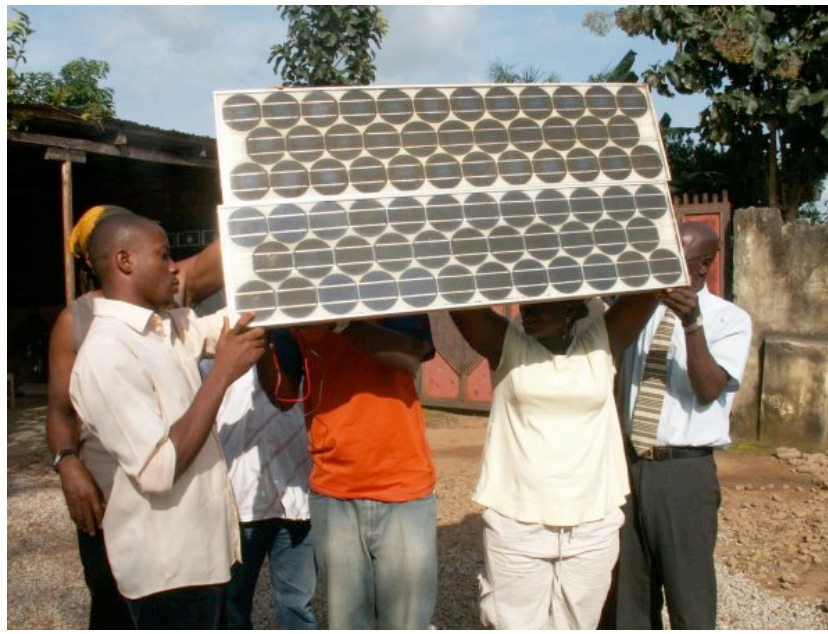


Figura 7.8: Interconexión de paneles en paralelo. La tensión permanece constante mientras que la corriente se duplica. (Foto: Fundación Fantsuam, Nigeria)

Cómo seleccionar un buen panel

Una medida obvia cuando se compran paneles es comparar la relación entre el punto de máxima potencia nominal (W_p) y el precio. Esto le dará una idea aproximada del costo por vatios de los diferentes paneles. Pero hay otras consideraciones que también deberían tomarse en cuenta.

Si usted va a instalar paneles solares en áreas geográficas donde la suciedad (causada por arena, polvo, cascajo) puede ser un problema, considere la compra de paneles que repelan el polvo. Estos paneles se fabrican con materiales que favorecen la limpieza automática con ayuda del viento o la lluvia.

Revise siempre la construcción mecánica de cada panel. Verifique que el vidrio sea resistente y el marco de aluminio robusto y bien construido. Las celdas solares dentro del panel pueden durar más de 20 años, pero son muy frágiles y se debe proteger al panel de accidentes mecánicos. Examine las garantías del fabricante respecto a la potencia que deben suministrar y a la construcción mecánica.

Finalmente, asegúrese de que el fabricante le proporcione no sólo el punto de máxima potencia nominal, sino también la variación de la tensión con la irrradiación y la temperatura. Esto es particularmente importante cuando los paneles se usan en bancos, ya que las variaciones en los parámetros operativos afectan grandemente la calidad de la energía generada y la vida útil de los paneles.

La batería

En una batería se producen ciertas reacciones químicas reversibles que hacen posible el almacenamiento de energía para ser entregada posteriormente cuando se necesite. La energía eléctrica se transforma en química cuando se carga una batería, y lo opuesto sucede cuando se descarga.

Una batería está conformada por una serie de elementos llamados celdas dispuestas en serie. Una batería de plomo-ácido consta de dos electrodos de plomo inmersos en una solución electrolítica de agua y ácido sulfúrico. Una diferencia de potencial de unos 2 voltios se establece entre los electrodos dependiendo del estado de carga de la batería. Las baterías más comunes en aplicaciones solares fotovoltaicas tienen un voltaje nominal de 6, 12 ó 24 voltios. Esto quiere decir que una batería de 12 V contiene 6 celdas en serie.

La batería tiene dos propósitos fundamentales en un sistema fotovoltaico: proporcionar energía eléctrica al sistema cuando el banco de paneles no la proporciona, y almacenar la energía proporcionada por los paneles cuando aquella excede las necesidades de la carga. La batería pasa por ciclos de carga y descarga dependiendo de la presencia o ausencia de luz solar. Durante las horas de sol, el banco de paneles produce energía eléctrica. La energía que no es consumida de inmediato se usa para cargar la batería. Durante las horas sin sol, cualquier necesidad de energía es provista por la batería, por lo tanto, se produce su descarga.

Estos ciclos de carga y descarga ocurren cada vez que la energía producida por los paneles no satisface la cantidad de energía necesaria para alimentar la carga. Cuando hay luz suficiente y la carga es ligera, las baterías se cargarán. Obviamente, en la noche se descargarán a la menor demanda de energía. También se descargarán cuando la radiación es insuficiente para satisfacer los requisitos de la carga (debido a variaciones climatológicas naturales tales como nubes, polvo, etc.).

Si la batería no almacena energía suficiente para satisfacer la demanda durante los períodos sin sol, el sistema no estará disponible para el consumo. Por otra parte, el sobre-dimensionamiento del sistema (por la adición de demasiados paneles o baterías) resulta caro e improductivo. Cuando se diseña un sistema autónomo tenemos que llegar a un compromiso entre el costo de los elementos y la disponibilidad de energía en el sistema. Una forma de hacerlo es calcular el número de días de autonomía requerido. En el caso de un sistema de telecomunicaciones, el número de días de autonomía dependerá de lo crítico de su función dentro de la red que se haya diseñado. Si el equipo va a funcionar de servidor y es parte de la troncal de su red, debe diseñar su sistema fotovoltaico con una autonomía de 5 a 7 días. Por otra parte, si el sistema solar va a encargarse de proporcionar energía a un equipo cliente, probablemente se puede reducir los días de autonomía a 2 ó 3. En áreas de baja irradiación, este valor debería incrementarse aún más. De cualquier manera, siempre tendrá que encontrar un equilibrio entre costo y disponibilidad.

Tipos de batería

Hay diferentes tipos de tecnología para baterías destinadas a diferentes usos. La más conveniente para aplicaciones fotovoltaicas es la llamada ***batería estacionaria***, diseñada para tener un emplazamiento fijo y para sitios donde el consumo de energía es más o menos irregular. Las "baterías estacionarias" pueden permitir ciclos de descarga profunda, pero no están diseñadas para producir corrientes altas en períodos cortos de tiempo.

Las baterías estacionarias pueden usar un electrolito alcalino (como las de Níquel-Cadmio), o ácido, (como las de Plomo-ácido). Las baterías estacionarias basadas en Níquel-Cadmio se recomiendan, cuando sea posible, por su alta confiabilidad y resistencia. Desafortunadamente suelen ser mucho más caras y difíciles de conseguir que las selladas de Plomo-ácido.

En muchos casos cuando se hace difícil conseguir localmente baterías estacionarias buenas y baratas (importarlas no es barato), se verá forzado a usar baterías diseñadas para automóviles.

Uso de baterías para automóvil

Las baterías de automóvil no son muy apropiadas para aplicaciones fotovoltaicas porque están diseñadas para proporcionar intensidades elevadas durante unos cuantos segundos (al encender el carro) en vez de mantener intensidades bajas por largos períodos. Este diseño característico de baterías de automóvil (también llamadas ***baterías de tracción***) se traduce en un acortamiento de su vida útil cuando se usa para sistemas fotovoltaicos. Estas baterías pueden usarse cuando el bajo costo sea la consideración más importante o cuando no se encuentre otro tipo de baterías.

Las baterías de tracción están diseñadas para vehículos y montacargas eléctricos. Son más baratas que las estacionarias y pueden usarse en sistemas fotovoltaicos si se toma en cuenta que requieren mantenimiento frecuente. Estas baterías no deben descargarse profundamente porque se reduce notablemente su capacidad de cargarse. Una batería de camión no debería descargarse más del 70% de su capacidad total. Esto significa que se puede usar un máximo de 30% de la capacidad nominal de una batería plomo-ácido antes de ser cargada de nuevo.

Se puede extender la vida de una batería plomo-ácido utilizando agua destilada. Al usar un densímetro o un hidrómetro se puede medir la densidad del electrolito de la batería. Una batería típica tiene una densidad específica de 1,28. Al añadir agua destilada, y bajarla a 1,2, se puede reducir la corrosión del ánodo a expensas de la capacidad total de la batería. Si usted ajusta la densidad del electrolito de la batería, debe usar agua destilada, porque el agua de grifo o de pozo la dañará permanentemente.

Estados de carga

Hay dos estados especiales de carga que pueden ocurrir durante los ciclos de carga y descarga de la batería que deben evitarse para preservar su vida útil.

Sobrecarga

La ***sobrecarga*** ocurre cuando la batería llega al límite de su capacidad. Si en este punto se sigue inyectando energía, el electrolito comienza a descomponerse. Esto produce burbujas de oxígeno e hidrógeno en un proceso que se llama ***gasificación***. Los resultados son pérdida de agua, oxidación en el electrodo positivo y, en casos extremos, hay riesgos de explosión.

Por otra parte, la presencia de gas evita la estratificación del ácido. Después de continuos ciclos de carga y descarga, el ácido tiende a concentrarse en el fondo de la batería con lo que se reduce su capacidad efectiva. El proceso de gasificación, entonces, revuelve el electrolito y evita la estratificación.

De nuevo, es necesario encontrar un compromiso entre las ventajas (evitar la estratificación electrolítica) y las desventajas (pérdida de agua y producción de hidrógeno). Una solución es la de permitir una ligera sobrecarga de vez en cuando. El método más común es permitir una tensión de 2,35 a 2,4 voltios por cada elemento de la batería a 25°C, cada pocos días. El regulador debería asegurar sobrecargas periódicas y controladas.

Sobredescarga

De la misma manera en que hay un límite superior, también hay un límite inferior respecto a la carga de una batería: descargarla por debajo de ese límite puede significar el deterioro de la batería. Cuando la energía efectiva de la batería se consume, es el regulador el que se encarga de que no se siga extrayendo energía de la batería. Cuando la tensión alcanza un límite mínimo de 1,85 voltios por celda a 25°C, el regulador desconecta la carga de la batería.

Si la descarga es muy profunda y la batería permanece mucho tiempo descargada, pueden ocurrir tres cosas: la formación de sulfato cristalizado en las placas de la batería, el aflojamiento del material activo de las placas de la batería, o la deformación de las placas. Al proceso de formación de cristales permanentes de sulfato se le conoce como sulfatación, lo que es particularmente perjudicial, ya que se generan grandes cristales que no forman parte de ninguna reacción química y que pueden dañar la batería de manera irreversible.

Parámetros de la Batería

Los principales parámetros que caracterizan a una batería son:

- ***Tensión Nominal***, V_{NBat}. Suele ser de 12 voltios
- ***Capacidad Nominal***, C_{NBat}: Cantidad máxima de energía que se puede extraer de una batería con carga completa. Se expresa en amperios-hora (Ah) o vatios-hora (Wh). La cantidad de energía que se puede extraer de una batería depende del tiempo en que se efectúe el proceso de extracción. Descargar una batería durante un periodo largo nos proporciona más energía que descargar la misma batería por corto tiempo. La capacidad de una batería es, por tanto, especificada en diferentes tiempos de descarga. Para aplicaciones fotovoltaicas este tiempo debe ser de 100 horas o más.
- ***Profundidad Máxima de Descarga***, PD_{max}: La profundidad de descarga es la cantidad de energía extraída de una batería en un ciclo único de descarga, expresada como porcentaje. La esperanza de vida de una batería depende de la profundidad de su descarga en cada ciclo. El fabricante debería proporcionar gráficos que muestren la relación entre el número de ciclos de carga-descarga y la vida de la batería. Como regla general, para baterías de ciclo profundo, deberían evitarse descargas mayores al 50%, y para las de uso automotriz, mayores al 30%.
- ***Capacidad Útil***, C_{UBat}: Es la capacidad real (disponible) de una batería. Es igual al producto de la capacidad nominal por la profundidad máxima de descarga, PD_{max}. Por ejemplo, una batería estacionaria de capacidad nominal con tiempo de descarga de 100 horas (c100), de 120 Ah y profundidad de descarga de 70%, tiene una capacidad útil de (120 x 0,7) 84 Ah.

Medida del estado de carga de la batería

Una batería de plomo-ácido de 12 V entrega diferente voltaje a los equipos dependiendo del estado de su carga. Cuando la batería está cargada al 100%, el voltaje de salida en circuito abierto es de 12,8 V y baja rápidamente a 12,6 V cuando se le conectan las cargas. Debido a que la batería tiene que entregar una corriente constante cuando está en operación, el voltaje de la batería baja linealmente entre 12,6 y 11,6 V dependiendo del estado de carga. Las baterías de plomo-ácido entregan el 95% de su energía dentro de este margen. Si estimamos que una batería está al 100% con 12,6 V y vacía (0%) con 11,6 V, podemos estimar que el voltaje, cuando la batería se ha descargado un 70%, es de 11,9 V. Estos valores son sólo una aproximación basta, ya que van a depender de la vida de la batería, la temperatura y calidad de la misma.

Estado de carga	Voltaje	Voltaje por celda
100%	12,70	2,12
90%	12,50	2,08
80%	12,42	2,07
70%	12,32	2,05
60%	12,20	2,03
50%	12,06	2,01
40%	11,90	1,98
30%	11,75	1,96
20%	11,58	1,93
10%	11,31	1,89
0%	10,50	1,75

Tabla 1: Relación entre el voltaje y estado de carga de una batería

De acuerdo con esta tabla, y considerando que una batería de camión no debería descargarse más del 20 ó 30%, podemos determinar que la capacidad útil de una batería de camión de 170 Ah es de 34 Ah (20%) a 51 Ah (30%). Usando la misma tabla, encontramos que deberíamos programar el regulador para que impida la descarga de la batería por debajo de 12, 3 V.

Protección de la batería y el regulador

Para proteger las baterías y las instalaciones de cortocircuitos y fallas, se usan corta-circuitos termomagnéticos y fusibles. Hay dos tipos de fusibles, de ***fusión lenta*** y de ***fusión rápida***. Deberían de usarse de fusión lenta con cargas inductivas y capacitivas donde pueden ocurrir corrientes muy altas en el momento de encender el aparato. Los fusibles de fusión lenta permiten que pasen corrientes más altas que las estipuladas por un corto tiempo. Los fusibles de difusión rápida, en estos casos, se fundirían rápidamente.

El regulador se conecta a la batería y a las cargas de manera que se deben considerar dos tipos diferentes de protección. Un fusible debería colocarse entre la batería y el regulador para proteger la batería de cortocircuitos, en caso de que el regulador falle. Un segundo fusible es necesario para proteger el

regulador de una excesiva corriente absorbida por la carga. Este segundo fusible está normalmente integrado al mismo regulador.

Figura 7.9: Un banco de baterías de 3.600 Ah. La corriente alcanza niveles de 45 A durante la carga

Cada fusible tiene estipulados una corriente máxima y un voltaje máximo de uso. La corriente máxima del fusible debería ser 20% más grande que la corriente máxima esperada. Aunque las baterías tienen un voltaje bajo, un cortocircuito puede ocasionar corrientes altas que pueden fácilmente alcanzar varios cientos de amperios. Las corrientes altas pueden ocasionar fuego, dañar los equipos y baterías e incluso causar quemaduras al cuerpo humano.

Si un fusible se funde, nunca lo reemplace con un alambre o un fusible estipulado para corrientes más altas sino que, en primer lugar, determine la causa del problema, y luego sustituya el fusible con otro que tenga las mismas características.

Efectos de la temperatura

La temperatura ambiente afecta de forma importante a las características de la batería:

- La capacidad nominal de una batería (que el fabricante suele dar para 25°C) aumenta con la temperatura a razón de un 1%/°C, aproximadamente. Pero en el caso de que la temperatura sea demasiado alta, la reacción química que tiene lugar en la batería se acelera, lo que puede provocar la oxidación mencionada al hablar de la sobrecarga. Esto, naturalmente, reducirá la vida de la batería. Para baterías automotrices, este problema se compensa en parte poniendo densidades de solución bajas (de 1,25 para baterías totalmente cargadas).

- A medida que la temperatura se reduce, la vida útil de la batería aumenta, pero si la temperatura es demasiado baja se corre el riesgo de congelar el electrolito. La temperatura de congelación depende de la densidad de la solución, a su vez directamente relacionada con el estado de carga de la batería. A menor densidad, mayor el riesgo de congelamiento. En zonas de temperatura baja debería evitarse las descargas profundas de la batería (es decir, PD_{max} efectivamente reducido).
- La temperatura también cambia la relación entre el voltaje y la carga. Es preferible usar un regulador que ajuste los valores de desconexión y reconexión por bajo voltaje de acuerdo con la temperatura. El sensor de temperatura del regulador debería estar fijado a la batería con cinta pegante o por otro medio sencillo.
- En zonas calientes es importante mantener las baterías tan frías como sea posible. Deben almacenarse en áreas sombreadas y nunca exponerse directamente al sol. También se aconseja colocarlas sobre un soporte pequeño para permitir que el aire fluya por debajo y, de esta manera, aumentar el enfriado.

Cómo escoger una buena batería

Escoger una buena batería puede demandar esfuerzos en países en desarrollo. Las de alta capacidad son pesadas, voluminosas y caras para importar. Una batería de 200 Ah pesa acerca de 50 kg (120 libras) y no puede transportarse como equipaje de mano. Si se quiere una batería duradera (> 5 años) que no requiera mantenimiento, hay que pagar el precio.

Una buena batería debe siempre venir con sus especificaciones técnicas, incluyendo su capacidad a diferentes tasas de descarga (C20, C100), temperatura de operación, valores críticos de voltaje y especificaciones para los cargadores.

Asimismo, las baterías no deben presentar rajaduras, derrame de líquido u otra señal de daño, y sus bornes deberían estar libres de corrosión. Puesto que son necesarias pruebas de laboratorio para obtener datos confiables sobre capacidad real y envejecimiento, esté alerta a la posibilidad de que le ofrezcan baterías de baja calidad (y hasta falsificaciones) en el mercado local. Un precio típico (sin incluir transporte o impuestos de importación) es de US $3-4 por Ah, para baterías de plomo-ácido.

Esperanza de vida versus número de ciclos

Las baterías son el único componente en un sistema fotovoltaico que se debería amortizar en un corto periodo y que debería reemplazarse a menudo. Se puede aumentar la vida útil de una batería reduciendo la profundidad de descarga por ciclo. Incluso las baterías de ciclo profundo obtendrán un aumento en su duración si el número de ciclos de descargas profundas (> 30%) se reduce.

Si descarga completamente la batería a diario, es probable que necesite cambiarla en un poco menos de un año. Si usa sólo 1/3 de la capacidad de la

batería, puede durarle más de tres años. Puede que sea más barato comprar una batería con el triple de capacidad que cambiarla cada año.

El regulador de carga

El regulador de carga se conoce también como controlador de carga, regulador de voltaje, controlador de carga-descarga, o controlador de carga-descarga y carga. El regulador se posiciona entre el banco de paneles, la batería y el equipo o carga.

Recuerde que el voltaje de una batería, a pesar de que es cercano a 2V por celda, varía de acuerdo con su estado de carga. El regulador impide las sobrecargas o sobredescargas monitoreando el voltaje de la batería.

Los reguladores que se usan en sistemas fotovoltaicos deben conectarse en serie: así desconectan el banco de paneles del banco de baterías para evitar la sobrecarga, y desconectan las baterías de la carga para evitar la sobredescarga. La conexión y desconexión se efectúa por medio de interruptores que pueden ser de dos tipos: electromecánicos (relés) o de estado sólido (transistor bipolar, MOSFET). Los reguladores no deben conectarse en paralelo.

Para proteger la batería de la gasificación, el interruptor se abre cuando la tensión en la batería alcanza su tensión de corte alta (***high voltage disconnect***, HVD). La tensión de corte baja (low voltage disconnect, LVD) impide que la batería se sobredescargue por medio de la desconexión de la carga. Para impedir las continuas conexiones y desconexiones, el regulador no se re-conectará hasta que la batería alcance su tensión de rearme por baja (***low reconnect voltage*** LRV).

Lo valores característicos de una batería plomo-ácido de 12 V son:

Umbrales de voltaje	Voltaje
LVD	11,5
LRV	12,6
Voltaje regulado constante	14,3
Ecualización	14,6
HVD	15,5

Tabla 2: Umbrales de voltaje de baterías

Los reguladores más modernos son también capaces de desconectar automáticamente los paneles durante la noche para evitar la descarga de la batería. Pueden también sobrecargarla cada cierto tiempo para incrementar su

vida, y usar un mecanismo conocido como modulación de duración de impulsos (***pulse width modulation***, PWM) para prevenir la gasificación excesiva.

Como el punto de operación de máxima potencia del banco de paneles va a variar con la temperatura y la iluminación solar, los reguladores modernos son capaces de rastrear el punto de potencia máxima del banco de paneles solares. Esta característica se conoce como rastreo del punto de máxima potencia (***maximum power point tracking***, MPPT).

Parámetros del regulador

Cuando seleccione un regulador para su sistema, debería conocer, al menos, la ***tensión de trabajo*** y la ***máxima corriente*** que aquel puede manejar. La tensión de trabajo será de 12, 24 ó 48 V. La máxima corriente debe ser 20% más grande que la proporcionada por los paneles conectados al regulador.

Otras características y datos de interés son:

- Valores específicos de tensión de corte por baja (LVD), tensión de rearme por baja (LRV) y tensión de corte por alta (HVD).
- Existencia de compensación por temperatura. Las tensiones que indican el estado de carga de la batería varían con la temperatura. Por esta razón, algunos reguladores pueden medir la temperatura de la batería y corregir las tensiones de sobrecarga.
- Instrumentación e indicadores. Los instrumentos más comunes miden la tensión de los paneles y las baterías, el estado de carga (SoC) o Profundidad de Descarga (DoD/PD). Algunos reguladores incluyen alarmas especiales que indican que el panel o la carga han sido desconectados, que se ha alcanzado la LVD o HVD, etc.

Convertidores

El regulador proporciona potencia a un voltaje continuo específico. Los convertidores e inversores se usan para ajustar el voltaje a las necesidades de la carga.

Convertidores de continua a continua (DC/DC)

Los convertidores DC/DC transforman un voltaje continuo en otro también continuo de valor diferente. Hay dos métodos de conversión que se usan para adaptar el voltaje al de las baterías: ***conversión lineal*** y ***conversión conmutada***.

La conversión lineal baja el voltaje de las baterías por conversión del exceso de energía en calor. Este método es muy simple, pero obviamente ineficiente. La conversión conmutada usa generalmente un componente magnético para almacenar temporalmente la energía y transformarla en otro voltaje que puede ser mayor, menor o el inverso (negativo) del voltaje de entrada.

La eficiencia de un regulador lineal disminuye a medida que se incrementa la diferencia entre el voltaje de entrada y el de salida. Por ejemplo, si queremos

convertir de 12 V a 6 V, el regulador lineal tendrá una eficiencia de sólo el 50%. Un regulador de conmutación tiene una eficiencia de, por lo menos, un 80%.

Convertidor o inversor de continua a alterna (DC/AC)

Los inversores se usan cuando su equipo requiere de corriente alterna. Los inversores cortan e invierten la corriente continua y generan una onda cuadrada que es luego filtrada para aproximarla a una onda sinusoidal y eliminar los armónicos indeseables. Muy pocos inversores proporcionan una sinusoidal pura como salida. La mayoría de los modelos disponibles en el mercado producen lo que se llama "onda sinusoidal modificada", ya que el voltaje de salida no es una sinusoidal pura. En términos de eficiencia, los inversores de onda modificada trabajan mejor que los de onda sinusoidal pura.

Tenga presente que no todos los equipos aceptarán una onda sinusoidal modificada como voltaje de entrada. Muy frecuentemente las impresoras láser no trabajan con inversores de onda modificada. Los motores sí trabajan, pero podrían consumir más energía que si trabajaran con sinusoidal pura. Además, las fuentes de alimentación de corriente continua (DC) tienden a calentarse más, y los amplificadores de audio a veces emiten un zumbido en presencia de inversores de onda sinusoidal modificada.

Aparte de la forma de onda, algunas características importantes que deben tener los inversores son:

- **Fiabilidad ante sobrecorrientes.** Los inversores tienen dos especificaciones de potencia: una para la potencia promedio y otra para la potencia máxima. Son capaces de proporcionar la potencia máxima en un tiempo corto, como cuando se enciende un motor. El inversor debería también ser capaz de auto-interrumpirse de manera segura (con un cortacircuito o un fusible) en la eventualidad de un cortocircuito, o si la potencia requerida fuera muy alta.
- **Eficiencia de conversión.** Los inversores presentan su máxima eficiencia cuando proporcionan del 50% al 90% de su especificación de potencia promedio. Usted debería seleccionar el inversor que satisfaga lo más posible las demandas de la carga. El fabricante normalmente proporciona el rendimiento del inversor al 70% de su potencia nominal.
- **Cargador de batería.** Muchos inversores también incorporan la función inversa: la posibilidad de cargar baterías en presencia de una fuente alternativa de energía (red eléctrica, generador, etc.) Este tipo de inversor se conoce como cargador/inversor.
- **Conmutación automática.** Algunos inversores pueden conmutar automáticamente entre diferentes fuentes de energía (red eléctrica, generador, solar) dependiendo de la disponibilidad.

Cuando se usan equipos de telecomunicaciones, es mejor evitar el uso de convertidores de continua a alterna (DC/AC) y en cambio alimentarlos directamente

con tensión continua. La mayoría de los equipos de telecomunicaciones aceptan un rango amplio de voltaje de entrada.

Equipo o carga

Obviamente, a medida que hay mayor demanda de consumo, el costo del sistema fotovoltaico también aumenta. Es, entonces, esencial que se dimensione el sistema adecuándolo lo más posible al consumo esperado. Cuando diseñe el sistema, debe hacer un estimado realista del consumo máximo, y una vez que el sistema esté instalado, el consumo máximo establecido debe respetarse para evitar fallas frecuentes de energía.

Equipos domésticos

No se recomienda el uso de energía solar fotovoltaica para aplicaciones de intercambio de calor (calentadores eléctricos, refrigeradores, tostadoras, etc.). Cuando le sea posible, la energía debe ser usada con moderación utilizando aparatos de bajo consumo.

A continuación enumeramos algunos puntos que se deben considerar cuando escoja equipos apropiados para usar con un sistema de energía solar:

- La energía solar fotovoltaica es adecuada para iluminación. En este caso, el uso de lámparas halógenas o fluorescentes es obligatorio ya que, aunque más caras, tienen más rendimiento que las bombillas incandescentes. Las lámparas a diodos emisores de luz (LED) también son una buena elección, ya que dan un buen rendimiento y se alimentan con corriente continua.
- También es posible usar energía fotovoltaica para aplicaciones que requieren consumo bajo y constante (el ejemplo más común es el televisor). Los televisores más pequeños consumen menos energía que los grandes. También debe considerarse que un televisor en blanco y negro consume cerca de la mitad de la energía de uno a color.
- La energía solar fotovoltaica tampoco se recomienda en el caso de aplicaciones que transforman la energía en calor (energía térmica). Se recomienda en su lugar el uso de calentadores solares o de butano.
- Las lavadoras de ropa automáticas convencionales pueden usarse, pero debe evitarse usar programas de centrifugado o calentamiento de agua.
- Si debe usar un refrigerador, debería ser de bajo consumo. Hay algunos especiales que trabajan con corriente continua, sin embargo su consumo es bastante alto (cerca de 1.000 Wh / día).

La estimación del consumo total es un paso fundamental en el cálculo de su sistema de energía solar. A continuación encontrará una tabla que le da una idea general del consumo de energía que se puede esperar con diferentes aplicaciones.

Equipo	Consumo (vatios)
Computadora portátil	30-50
Lámpara de baja potencia	6-10
Enrutador WRAP (un radio)	4-10
Punto de acceso WiFi (un radio)	4-10
Módem VSAT	20-30
PC Bajo consumo (sin LCD)	20-30
PC (con LCD)	200-300
Switch Ethernet (16 puertos)	6-8

Tabla 3: Orientación sobre los consumos de potencia (en vatios) de algunos equipo

Equipos de comunicaciones inalámbricas

Ahorrar energía al seleccionar el equipo adecuado le puede ahorrar bastante dinero y problemas. Por ejemplo, un enlace de larga distancia no necesita necesariamente un amplificador fuerte que consuma grandes cantidades de potencia. Una tarjeta WiFi con buena sensibilidad de receptor y con la zona de Fresnel despejada por lo menos en un 60%, trabajará mejor que un amplificador y también le ahorrará consumo. Un dicho popular entre los radioaficionados se puede aplicar aquí también: El mejor amplificador es una buena antena. Algunas medidas adicionales para el ahorro de energía incluyen limitar la velocidad del CPU, reduciendo la transmisión de energía al mínimo necesario para permitirle estabilidad al enlace, incrementando el intervalo entre balizas (***beacons***), y apagando el sistema cuando no se necesite.

La mayor parte de los sistemas solares autónomos trabajan a 12 ó 24 voltios. Es preferible usar un dispositivo inalámbrico que funcione con corriente continua trabajando a los 12 voltios que la mayoría de las baterías plomo-ácido proporciona. Cuando se transforma el voltaje proporcionado por la batería en corriente alterna, o cuando se usa un voltaje a la entrada del Punto de Acceso (***Access Point***, ***AP***) diferente al voltaje de la batería, se ocasionará una pérdida innecesaria de energía. Un enrutador, o un AP que acepte 8-20 voltios DC, sería perfecto.

La mayoría de los AP baratos traen incorporado un regulador de voltaje tipo conmutado y trabajarán en rangos amplios de voltaje, sin modificaciones y sin recalentarse (incluso si el dispositivo viene con una fuente de alimentación de 5 ó 12 voltios). Nótese que todos los dispositivos diseñados para trabajar con PoE (alimentación eléctrica mediante el cableado de datos) necesariamente aceptan una amplia gama de voltajes DC.

ADVERTENCIA: Cuando opere su AP con una fuente de alimentación diferente a la que provee el fabricante, cualquier garantía quedará anulada y puede dañar su equipo. Aunque la técnica siguiente va seguramente a funcionar como se describe, recuerde, que si la utiliza, lo hace a su propio riesgo.

Equipo	Consumo (vatios)
Linksys WRT54G (BCM2050 radio)	6
Linksys WAP54G (BCM2050 radio)	3
Orinoco WavePoint II ROR (30mW radio)	15
Soekris net4511 (sin radio)	1,8
PC Engines WRAP.1E-1 (sin radio)	2,04
Mikrotik Routerboard 532 (sin radio)	2,3
Inhand ELF3 (sin radio)	1,53
Senao 250mW radio	3
Ubiquiti 400mW radio	6

Tabla 4: Consumo de potencia de equipos inalámbricos

Abra su AP y busque cerca de la entrada DC dos capacitores (condensadores) relativamente grandes y un inductor (un toroide de ferrita con un alambre de cobre enrollado alrededor). Si los encuentra, es porque el dispositivo tiene una entrada tipo conmutada, y el voltaje máximo de entrada debería ser un poco menor que el voltaje especificado en los capacitores. Esta especificación es, normalmente, 16 ó 25 voltios. Tenga en cuenta que una fuente de alimentación no regulada tiene un rizado y podría aplicar un voltaje mucho más alto a su AP que el especificado. Por tanto, conectar una fuente de alimentación no regulada de 24 voltios a un dispositivo con un condensador de 25 voltios no es una buena idea. Y, naturalmente, cuando usted abre su dispositivo, pierde cualquier garantía. Así que no trate de operar un AP a un

voltaje más alto si no tiene un regulador tipo conmutado porque se calentará, presentará fallas o se quemará.

Los equipos basados en CPU Intel x86 tradicionales son grandes consumidores de energía comparados con arquitecturas basadas en RISC, tales como ARM o MIPS. Una de las tarjetas con menor consumo de energía es la plataforma Soekris que usa un procesador AMD Elan SC520. Otra alternativa a AMD (Elan SC ó Geode SC1100) es el uso de equipo con procesadores MIPS. Estos procesadores presentan mejor rendimiento que un AMD Geode al precio de consumir entre 20 y 30% más de energía.

El popular Linksys WRT54G funciona a cualquier voltaje entre 5 y 20 voltios DC y consume unos 6 vatios, pero tiene un conmutador (*switch*) Ethernet incorporado. Tener este conmutador es, por supuesto cómodo, pero consume energía extra. Linksys también ofrece un AP WiFi llamado WAP 54G que consume sólo 3 vatios y acepta los *firmware* OpenWRT o Freifunk. El Accesscube de 4G Systems consume unos 6 vatios cuando está equipado con una sola interfaz WiFi. Si 802.11b es suficiente, las tarjetas mini-PCI con el *chipset* Orinoco funcionan muy bien con un consumo mínimo de energía.

La cantidad de potencia que requiere un equipo inalámbrico depende no sólo de la arquitectura sino del número de interfaces de red, radios, tipo de memoria/almacenamiento y del tráfico. Por regla general, una tarjeta inalámbrica de bajo consumo, usa de 2 a 3 W, y un radio de 200mW disipa unos 3 W. Las tarjetas de alta potencia (como la Ubiquiti 400 mW) consumen alrededor de 6 W, y una estación repetidora con dos radios está en el rango de los 8 a 10 W.

A pesar de que el estándar IEEE 802.11 incorpora un mecanismo de ahorro de energía (PS), los beneficios no son tan buenos como se pudiera esperar. El principal mecanismo de ahorro de energía es permitirle a las estaciones que periódicamente "pongan a dormir" sus tarjetas por medio de un circuito temporizador. Cuando la tarjeta inalámbrica "despierta", verifica si hay tráfico pendiente para ella monitoreando las balizas (*beacons*), indicando así que hay tráfico pendiente. El ahorro de energía, entonces, sólo se efectúa en la parte del cliente, ya que el AP siempre necesita estar despierto para enviar balizas y almacenar el tráfico de los clientes. El modo de ahorro de energía podría ser incompatible entre las implementaciones de diferentes fabricantes, lo que podría ocasionar inestabilidad a las conexiones inalámbricas. Es casi preferible desactivar siempre el modo de ahorro de energía en todos los equipos ya que los problemas que ocasionan son más importantes que la energía que se ahorra.

Selección del voltaje de trabajo

La mayoría de los sistemas autónomos de bajo consumo usan 12 V que es el voltaje de trabajo más común en baterías de plomo-ácido. Cuando diseñe un sistema inalámbrico necesita tomar en cuenta el voltaje de trabajo más eficiente para su equipo. Aunque el equipo pueda aceptar un rango amplio de valores de voltaje, escoja el que le permita que el consumo total del sistema sea mínimo.

Cableado

Este es un aspecto importante de su instalación ya que un cableado adecuado le va a asegurar una transferencia eficiente de energía. Algunos buenos hábitos que debería recordar en esta sección son:

- Use un tornillo para asegurar el cable al borne de la batería. Las conexiones flojas ocasionan pérdidas de energía.
- Unte vaselina o jalea mineral a los bornes de la batería. La corrosión en las conexiones ocasionan aumento en la resistencia, por tanto, gasto de energía.
- Para corrientes bajas (< 10 A) considere usar conectores tipo Faston o Anderson. Para corrientes mayores, use terminales correspondientemente más robustos.

El tamaño de los cables usualmente se especifica en términos del *American Wire Gauge* (AWG). Para sus cálculos, se necesita convertir de AWG a mm2 para calcular la resistencia del cable. Por ejemplo, un cable AWG # 6 tiene un diámetro de 4,11 mm y puede manejar hasta 55 A. En el **Apéndice D** va a encontrar una tabla de conversión que incluye un estimado de resistencia y de capacidad de transporte de corriente. Tenga en cuenta que la capacidad de transporte de corriente también va a depender de la aplicación y del aislamiento. En caso de duda, consulte al fabricante para mayor información.

Orientación de los paneles

La mayor parte de la energía que proviene del sol llega en línea recta. El módulo solar captará más energía si está "de cara" al sol, perpendicular a la línea recta entre la posición de la instalación y el sol. Obviamente, la posición del sol está cambiando constantemente con relación a la tierra, así que necesitamos encontrar la posición óptima para nuestros paneles. La orientación de los mismos está determinada por dos ángulos, el ***azimut***, ***a*** y la ***inclinación*** o ***elevación***, **β**. El azimut es el ángulo que mide la desviación con respecto al sur en el hemisferio norte, y con respecto al norte, en el hemisferio sur. La inclinación es el ángulo formado por la superficie del módulo y el plano horizontal.

Azimut

El módulo debe orientarse hacia el ecuador terrestre (hacia el sur, en el hemisferio norte y hacia el norte en el hemisferio sur) de manera que durante el día el panel atrape la mayor cantidad de radiación (a = 0).

¡Es muy importante que ninguna parte del panel quede en la sombra! Examine los elementos que rodean el banco de paneles (árboles, edificios, paredes, otros paneles, etc.) para asegurarse de que no hagan sombra a sus paneles en ningún momento del día o del año. Es aceptable girar los paneles ± 20° hacia el este o hacia el oeste si se necesita (a = ± 20°).

Inclinación

Una vez que se fija el azimut, el parámetro clave para nuestro cálculo es la inclinación del panel, que expresaremos como el ángulo beta (β). La altura máxima que el sol alcanza cada día va a variar, con un máximo, el día de solsticio de verano y un mínimo, el día del solsticio de invierno. Idealmente, los paneles deberían rastrear esta variación, sin embargo, esto no siempre es posible por razones de costo.

En instalaciones con equipos de telecomunicaciones es usual instalar el panel con una inclinación fija. En la mayor parte de los casos de telecomunicaciones, las demandas de energía del sistema son constantes a lo largo del año. Calcular la energía suficiente para el "peor mes" es una medida que nos servirá para el resto del año.

El valor de β debería maximizar la razón entre la oferta y la demanda de energía.

- Para instalaciones con un consumo consistente (o casi consistente) durante el año es preferible optimizar la instalación para que capture la radiación máxima durante los meses de "invierno". Usted debería usar el valor absoluto de la latitud del lugar (ángulo F) con una adición de 10° (β = l F l + 10°).
- Para instalaciones con menor consumo durante el invierno, el valor de la latitud del lugar puede ser usado como la inclinación del panel solar. De esta manera, optimizamos el sistema para los meses de primavera y otoño (β = l F l).
- Para instalaciones que se usen solamente en verano, se debería usar el valor absoluto de la altitud del lugar (ángulo F) con una disminución de 10° (β = l F l - 10°).

La inclinación del panel nunca debería ser menor de 15° para evitar la acumulación del polvo o la humedad sobre el mismo. En áreas donde hay nieve o hielo es importante proteger los paneles e inclinarlos a un ángulo de 65° o mayor.

Si hay un incremento de consumo de energía considerable durante el verano, debería planificarse dos inclinaciones fijas: una posición para los meses de verano, y otra para los de invierno. Esto va a requerir de estructuras de soporte especiales y previsiones para cambiar la posición de los paneles.

Cómo dimensionar su sistema fotovoltaico

Cuando escoja el equipo para satisfacer sus necesidades de energía, va a necesitar la determinación de, al mínimo, la siguiente información:

- El número y tipo de paneles solares que se necesitan para la captación de la energía solar necesaria para su carga.
- La capacidad mínima de la batería. La batería necesita almacenar energía suficiente para proveer energía durante la noche y en días de poco sol, y determinará el número de días de autonomía.

- Las características de los otros componentes (el regulador, cableado, etc.) necesarios para mantener la cantidad de energía generada y almacenada.

Los cálculos de dimensionado del sistema son importantes porque, a menos que los componentes del mismo estén balanceados, derrochamos energía (y al final, dinero). Por ejemplo, si instalamos más paneles de los necesarios para obtener más energía, las baterías deberían tener capacidad suficiente para almacenar esa cantidad extra producida. Si el banco de baterías es muy pequeño y la carga no consume la energía a medida que se genera, la energía deberá desecharse. Un regulador con un amperaje menor del que se necesita, o un sólo cable que sea demasiado pequeño pueden causar fallas (incluso incendio) y dejar la instalación inservible.

Nunca olvide que la capacidad de un sistema fotovoltaico para producir y almacenar energía eléctrica es limitada. Dejar un bombillo encendido accidentalmente durante el día puede gastar las reservas de energía antes de que llegue la noche, cuando ya no tenemos disponibilidad de energía adicional. La disponibilidad de "combustible" para un sistema fotovoltaico (es decir, radiación solar) puede ser difícil de predecir. De hecho, nunca es posible tener la seguridad de que un sistema autónomo va a proporcionar la energía necesaria en un momento determinado. Los sistemas solares están diseñados para un cierto consumo y si el usuario excede los límites planeados, fallará la provisión de energía.

El método de diseñado que proponemos consiste en calcular las necesidades de energía, y con base en esto, calcular un sistema que trabaje durante el mayor tiempo posible, de manera que sea lo más confiable posible. Por supuesto, si se instalan más paneles y más baterías, seremos capaces de captar y almacenar más energía con un incremento de la confiabilidad, pero también de costos.

En algunas instalaciones fotovoltaicas (como en el suministro de energía para equipos de telecomunicaciones en la dorsal (*backbone*) de una red, el factor de disponibilidad es más importante que el costo, en cambio para una instalación de cliente, el bajo costo es más importante. Encontrar el balance entre costo y disponibilidad no es tarea fácil, pero cualquiera sea su situación, debería ser capaz de determinar lo que se espera de las opciones de su diseño y a qué precio.

El método que usaremos para dimensionar el sistema se conoce como el ***método del peor mes***. Simplemente calculamos las dimensiones del sistema autónomo para que trabaje durante el mes en que las demandas de energía van a ser mayores con respecto a la energía solar disponible. Es el peor mes del año porque presentará la mayor relación entre energía solicitada y energía disponible.

AL utilizar este método, la confiabilidad se considera estableciendo el máximo de días que el sistema puede trabajar sin recibir radiación solar (es decir, cuando el consumo se hace exclusivamente a expensas de la energía almacenada en la batería). Esto se conoce como ***máximo de días de autonomía*** (N), es decir, el número de días nublados consecutivos en los que los paneles no colectan ninguna cantidad significativa de energía.

Para determinar N, es necesario conocer la climatología del lugar, así como la relevancia económica y social de la instalación. ¿Va a usarse para iluminar casas, un hospital, una fábrica, para un radio enlace, u otra aplicación? Recuerde que a medida que N es mayor, también aumenta la inversión en equipos y mantenimiento. También es importante evaluar los costos logísticos de reemplazo de equipos. No es lo mismo cambiar una batería descargada de una instalación en medio de la ciudad, que una en la cima de una torre de telecomunicaciones que se encuentra a horas, o días de camino a pie.

Establecer el valor de N no es fácil porque hay muchos factores en juego y muchos no pueden ser evaluados con facilidad. Su experiencia va a jugar un importante papel en este punto del dimensionado. Un valor comúnmente usado para equipos críticos de telecomunicaciones es el de N = 5, mientras que para equipo cliente de bajo costo es posible reducir la autonomía a N = 3.

En el **Apéndice E**, presentamos varias tablas que le facilitarán la recolección de los datos necesarios para el dimensionado del sistema. En el resto del capítulo explicaremos en detalle la información que necesita para recolectar datos o hacer estimados para el uso del método del "peor mes".

¿Qué datos recolectar?

- **Latitud de la instalación.** Recuerde usar un signo positivo en el hemisferio norte y uno negativo en el hemisferio sur.
- **Datos de radiación solar**. Para el método del "peor mes" es suficiente conocer 12 valores, uno por cada mes. Los doce números son los valores promedio mensuales de la irradiación global diaria en plano horizontal. ($G_{dm}(0)$, in kWh/m² por día). El valor mensual es la suma de los valores de irradiación global para cada día del mes, dividida por el número de días del mes.

  Si usted tiene los datos en Joules (J), puede aplicar la siguiente conversión:

  $$1\ J = 2.78 \times 10^{-7}\ kWh$$

Los datos de irradiación $G_{dm}^{(0)}$ de muchos sitios del mundo están disponibles en tablas y bases de datos. Usted debería buscar esta información en alguna estación meteorológica cercana a su sitio de implementación, pero no se sorprenda si no los encuentra en formato electrónico. La NASA proporciona abundante información en el sitio *http://eosweb.larc.nasa.gov/cgi-bin/sse/sse.cgi?+s01+s03#s01*. Es una buena idea consultar compañías que instalen sistemas fotovoltaicos en el lugar ya que su experiencia puede ser muy valiosa.

No confunda "horas de sol" con el número de "horas de sol pico". El número de horas de sol pico no tiene que ver con las horas sin nubosidad, sino se refiere a la cantidad de irradiación diaria. Un día de 5 horas de sol sin nubes, no necesariamente tiene esas horas cuando el sol está en su cenit.

Una hora de sol pico es un valor estandarizado de radiación solar de 1.000 W/m² a 25°C. Así que cuando hablamos de 5 horas de sol pico (HSP), nos referimos a una radiación solar diaria de 5000 W/m².

Características eléctricas de los componentes del sistema

Las características eléctricas de los componentes de su sistema debe proporcionarlas el fabricante. Es recomendable que usted realice sus propias medidas para controlar posibles desviaciones de las especificaciones nominales. Desafortunadamente, la desviación de los valores prometidos puede ser grande y no debe sorprenderle.

A continuación le presentamos los valores mínimos que debería tener presente antes de comenzar el dimensionado:

Paneles

Necesita saber el voltaje V_{Pmax} y la corriente I_{Pmax} en el punto de máxima potencia en condiciones estándar.

Baterías

La capacidad nominal (para 100 horas de descarga) C_{NBat}, el voltaje operacional V_{NBat}, y, bien sea la profundidad máxima de descarga PD_{max}, o la capacidad útil C_{UBat}. También necesita conocer qué tipo de batería va a usar: plomo-ácido, gel, AGM, de tracción modificada, etc. El tipo de batería es importante cuando haya que decidir los puntos de corte del regulador.

Regulador

Necesita saber el voltaje nominal VNReg, y la coriente máxima a la que opera I_{maxReg}.

Convertidor/Inversor continua/alterna DC/AC

Si va a usar un convertidor, necesita saber el voltaje nominal VNConv, la energía instantánea PIConv y el rendimiento al 70% de la carga máxima H_{70}.

Equipo o carga

Es necesario saber el voltaje nominal VNC y la potencia nominal de operación PC para cada equipo alimentado por el sistema.

Para saber la energía total que nuestra instalación va a consumir es también importante tomar en cuenta el tiempo promedio que cada carga va a ser usada. ¿Es constante? ¿O va a usarse diariamente, semanalmente, mensualmente, anualmente? Considere cualquier cambio en el uso que pueda alterar la cantidad de energía que se necesitará (uso estacional, períodos escolares, etc.).

Otras variables

Aparte de las características eléctricas de los componentes de su carga es necesario considerar otros dos elementos antes de dimensionar el sistema: el número de días de autonomía y el voltaje de trabajo del sistema.

N: número de días de autonomía

Necesita decidir sobre el valor de N que establecerá un balance entre las condiciones meteorológicas, el tipo de instalación y el costo general. Es imposible asignarle un valor concreto a N válido para todo tipo de instalación, pero las tablas que se presentan a continuación le sugerirán algunos valores recomendados. Tome estos valores como una aproximación y consulte con un experto en el área para tomar su decisión definitiva.

Luz solar disponible	Instalación doméstica	Instalación crítica
Muy nublado	5	10
Variable	4	8
Soleado	3	6

Tabla 5: Días de autonomía

V_N, voltaje nominal de la instalación

Los componentes de su sistema se escogen para operar a un voltaje nominal V_N, que es normalmente de 12 ó 24 voltios para sistemas pequeños. Si la potencia de consumo sobrepasa los 3 kW, el voltaje será de 48 V. La selección de V_N no es arbitraria, y depende de la disponibilidad del equipo.

- Si el equipo lo permite, trate de fijar el voltaje nominal en 12 ó 24 V. Muchas tarjetas de comunicación inalámbrica aceptan un rango amplio de voltaje de entrada y pueden ser usadas sin un convertidor.
- Si necesita alimentar diferentes equipos que trabajen a diferentes voltajes nominales, calcule el voltaje que minimice el consumo global incluyendo la energía de los convertidores de continua/continua y continua/alterna.

Procedimientos de cálculo

Hay tres pasos principales que se deben seguir para calcular la dimensión adecuada de su sistema:

1. **Calcule la energía solar disponible (oferta).** Basándonos en estadísticas sobre radiación solar, la orientación y la inclinación óptima de los paneles, calculamos la energía solar disponible. Este estimado se hace en intervalos mensuales, reduciendo los datos a 12 valores. Este estimado es un buen compromiso entre precisión y simplicidad.

2. **Considere la energía eléctrica requerida (demanda).**Tome nota del consumo de energía característico del equipo escogido así como del uso estimado. Luego calcule la energía eléctrica requerida mensualmente. Debería tomar en cuenta las fluctuaciones de uso debido a variaciones entre invierno y verano; períodos de lluvia / sequía; período de clases/ vacaciones, etc. El resultado deben ser 12 valores de demanda de energía, una para cada mes del año.

3. **Calcule la dimensión ideal del sistema (resultado).** Con los datos procedentes del "peor mes", cuando la relación entre la energía solar requerida, y la energía disponible es la más grande, calculamos:

    - La corriente que el banco de paneles necesita proporcionar, lo que determinará la cantidad mínima de paneles necesitados.
    - La capacidad de almacenamiento de energía necesaria para cubrir el número mínimo de días de autonomía, lo que va a determinar el número de baterías requerido.
    - Las características eléctricas del regulador.
    - La longitud y las secciones necesarias de cables para la conexión eléctrica.

Corriente necesaria en el peor mes

Para cada mes se necesita calcular el valor I_m, que es la corriente máxima diaria que un banco de paneles operando al voltaje nominal V_N necesita proporcionar, en un día con una irradiación G_{dm} por mes "m", y paneles de una inclinación de β grados.

El I_m (PEOR MES) va a ser el valor más grande de I_m, y el dimensionado del sistema se basa en los datos de este mes. Los cálculos de $G_{dm}\beta$ para un cierto sitio pueden hacerse con base en $G_{dm}(0)$, usando un programa de computación tipo PVSYST (*http://www.pvsyst.com/*), o PVSOL (*http://www.solardesign.co.uk/*) y también a partir de *http://eosweb.larc.nasa.gov/cgi-bin/sse/sse.cgi?+s01+s03#s01*. Debido a pérdidas en el regulador y las baterías, y debido al hecho de que los paneles no siempre trabajan en su punto de máxima potencia, la corriente requerida I_{mMAX} se calcula así:

$$I_{mMAX} = 1.21\ I_m\ (\text{PEOR MES})$$

Una vez que se haya determinado el peor mes, el valor de I_{mMAX}, y la cantidad total de energía que necesite, E_{TOTAL}, (PEOR MES), puede proceder al cálculo final. E_{TOTAL} es la suma de todas las cargas de corriente continua (DC) y alterna (AC), en vatios. Para calcular E_{TOTAL}, vea el **Apéndice E**.

Número de paneles

Combinando los paneles solares en serie y en paralelo podemos obtener la corriente y el voltaje deseados. Cuando los paneles están conectados en serie, el voltaje total es igual a la suma de los voltajes individuales de cada módulo, mientras que la corriente permanece inalterada. Cuando se conectan los paneles en paralelo, las corrientes se suman, mientras que el voltaje permanece

inalterado. Es muy importante usar paneles que tengan aproximadamente las mismas características cuando construya su banco.

Debería tratar de conseguir paneles con un V_{Pmax} un poco mayor que el voltaje nominal del sistema (12, 24 ó 48 V). Recuerde que debe proporcionar una cantidad un poco mayor que el voltaje nominal de la batería para poder cargarla. Si no le es posible encontrar un panel único que satisfaga sus necesidades, va a necesitar conectar varios paneles en serie para obtener el voltaje deseado. El número de paneles en serie N_{ps} es igual al voltaje nominal del sistema dividido por el voltaje de un solo panel, con aproximación al entero superior.

$$N_{ps} = V_N / V_{Pmax}$$

Para calcular el número de paneles en paralelo (N_{pp}), necesita dividir el I_{mMAX} por la corriente de un solo panel en el punto de máxima potencia I_{Pmax}, aproximando al entero superior.

$$N_{pp} = I_{mMAX} / I_{Pmax}$$

El número total de paneles es el resultado de multiplicar el número de paneles en serie (para fijar el voltaje) por el número de paneles en paralelo (para fijar la corriente).

$$N_{TOTAL} = N_{ps} \times N_{pp}$$

Capacidad de la batería o acumulador

La batería determina el voltaje global del sistema y necesita tener la capacidad suficiente para proporcionar energía a la carga cuando no haya suficiente radiación solar.

Para estimar la capacidad de nuestra batería, calculamos primero la capacidad de energía requerida por nuestro sistema (capacidad necesaria, C_{NEC}). La capacidad necesaria depende de la energía disponible durante el "peor mes" y del número de días de autonomía deseados (N).

$$C_{NEC}\ (Ah) = E_{TOTAL}(WORST\ MONTH)(Wh) / V_N(V) \times N$$

La capacidad nominal de la batería C^{NOM} necesita ser mayor que la C_{NEC} porque no podemos descargar totalmente la batería. Para calcular el tamaño de la batería necesitamos considerar la profundidad máxima de descarga (PD) que permite la batería:

$$C_{NOM}(Ah) = C_{NEC}(Ah) / DoD_{MAX}$$

Para calcular el número de baterías en serie (N_{bs}), dividimos el voltaje nominal de nuestra instalación (V_N) entre el voltaje nominal de una sola batería (V_{NBat}):

$$N_{bs} = V_N / V_{NBat}$$

Regulador

Una precaución importante es usar siempre reguladores en serie, nunca en paralelo. Si su regulador no suministra la corriente requerida por el sistema, necesita comprar otro regulador con una corriente de trabajo más grande.

Por razones de seguridad, un regulador debe ser capaz de operar con una corriente I_{maxReg} por lo menos 20% más grande que la intensidad máxima proporcionada por el banco de paneles:

$$I_{maxReg} = 1.2\ N_{pp}\ I_{PMax}$$

Inversor continua / alterna (DC/AC)

La energía total que se necesita para el equipo de alterna (AC) se calcula incluyendo todas las pérdidas ocasionadas por el inversor/convertidor continua/alterna (DC/AC) Cuando escoja un inversor, recuerde que su rendimiento varía de acuerdo con la cantidad de energía demandada. Un inversor tiene un mayor rendimiento cuando trabaja con valores cercanos a los especificados. Usar un inversor de 1.500 vatios para alimentar una carga de 25 vatios es altamente ineficiente. Para evitar este gasto de energía se deben considerar no las potencias pico de todo el equipo, sino las potencias pico de las partes del equipo que vayan a trabajar simultáneamente.

Cables

Una vez que conozca el número de paneles y baterías, el tipo de reguladores e inversores que quiere usar, debe calcular la longitud y espesor de los cables que se necesitan para conectar todos los componentes juntos.

El **largo** va a depender del sitio de su instalación. Debería tratar de minimizar el largo de los cables entre el regulador, los paneles y las baterías. Usar cables cortos va a minimizar la pérdida de energía y el gasto en cableado.

El **espesor** se escoge en relación con el largo del cable y la corriente máxima que debe transportar. El objetivo es minimizar las caídas de voltaje. Para calcular el espesor S de un cable es necesario saber:

- La corriente máxima IMC que va a circular por el cable. En el caso del subsistema del panel-baterías, va a ser I_{mMAX} calculado por cada mes. En el subsistema baterías-cargas, va a depender de la manera en que las cargas estén conectadas.
- La caída de voltaje ($V_a - V_b$) que consideramos aceptable en el cable. La caída de voltaje que resulta de la suma de las caídas individuales posibles se expresa como un porcentaje del voltaje nominal de la instalación. A continuación se presentan algunos valores máximos típicos:

Componente	Caída de voltaje (% of V_N)
Banco de paneles –> Batería	1%
Batería –> Convertidor	1%
Línea principal	3%
Línea principal (Iluminación)	3%
Línea principal (Equipo)	5%

Tabla 6: Caídas de voltaje admisibles

Caídas de voltaje aceptable más comunes

La sección del cable se determina por la ley de Ohm:

$$S(mm^2) = r(\Omega mm^2/m)L(m)\ I_{mMAX}(A)/\ (V_a-V_b)(V)$$

donde S es la sección, r es resistividad (propiedad inherente del material: para el cobre es de 0,01286 Ωmm^2 / m), y L es el largo.

Vamos a escoger S de acuerdo con la disponibilidad de cables en el mercado. Se debería escoger la sección inmediatamente superior a la que se obtiene por la fórmula. Por razones de seguridad, hay valores mínimos para el cable que conecta los paneles con la batería. Este valor es de 4 mm^2.

Costo de una instalación solar

Aunque la energía solar es gratis, el equipo que se necesita para su aprovechamiento no lo es. Usted va a necesitar no sólo comprar equipo para transformar la energía solar en electricidad y almacenarla para su uso, sino que también debe gastar en mantenimiento y reemplazo de los varios componentes del sistema. El problema del reemplazo de equipo es a menudo pasado por alto, y un sistema de energía solar no se puede implementar sin un plan adecuado de mantenimiento.

Para calcular el costo real de su instalación vamos a proporcionarle un ejemplo ilustrativo. Lo primero que hay que hacer es calcular el costo de la inversión inicial.

Descripción	Número	Costo unitario	Subtotal
Panel solar de 60 W (unos $ 4 / W)	4	$300	$1.200
Regulador de 30 A	1	$100	$100
Cables (metros)	25	$1 / metro	$25
Batería de ciclo profundo de 50Ah	6	$150	$900
		Total:	$2.225

Tabla 7: Costo inicial de una instalación solar

El cálculo de nuestro costo de inversión se hace relativamente fácil una vez que el sistema ha sido dimensionado. Sólo se necesita ahora añadir el precio por cada pieza del equipo, y el costo de mano de obra de instalación y cableado de todo el equipo. Por razones de simplicidad no se incluye aquí los costos de transporte e instalación, pero no deberían dejarse de lado.

Para calcular cuánto cuesta en realidad operar un sistema debemos calcular la duración de cada pieza y la frecuencia de reemplazo. En el léxico de contaduría esto se llama ***amortización***. Nuestra nueva tabla, entonces, sería algo así:

Descripción	#	Costo unitario	Subtotal	Vida útil (años)	Costo anual
Panel solar 60 W (unos $ 4 / W)	4	$300	$1.200	20	$60
Regulador 30 A	1	$100	$100	5	$20
Cables (metros)	25	$1 / metro	$25	10	$2,50
Batería de ciclo profundo 50Ah	6	$150	$900	5	$180
		Total:	$2.225	Costo anual:	$262,50

Tabla 8: Costo anual de una instalación solar

Como puede observar, una vez que se ha hecho la primera inversión, se espera un costo anual de $262,50. El costo anual es el estimado del capital anual necesario para reemplazar los componentes del sistema una vez que estos agotan su vida útil.

8
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 inalámbrico. 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 entrar 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. Por su parte, la IEC (*International Electrotechnical Comission*) toma en cuenta no solamente la protección contra el agua sino también contra objetos que puedan penetrar en la caja. IEC asigna un índice de protección del ingreso (IP). El primer número se refiere al tamaño máximo del objeto que puede penetrar y el segundo número a la resistencia al agua. Un índice de protección de ingreso de ***IP66*** o ***IP67*** protege 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 o IEC. 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, todavía puede 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 conectan 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/a, 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 conozca 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.

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 reflectores parabólicos 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 reflector 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 la 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 para 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 8.1: 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 planificar una inspección anual del montaje y si es necesario repintado.

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 8.2: 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 8.3: 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 8.4: Una torre mucho más complicada.

Montajes sobre el techo

En los techos planos se pueden utilizar montajes para la antena que no penetren la platabanda. 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 8.5: 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 que va 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.

Cómo proteger los conectores de microondas

La humedad en los conectores es sin duda la causa de fallas más observada en los radioenlaces. Debe apretar los conectores firmemente, pero nunca utilice una llave ajustable 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.

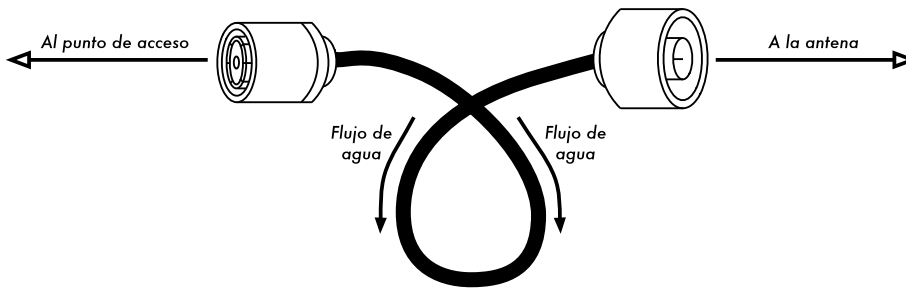


Figura 8.6: Un bucle en forma de gota fuerza al agua de lluvia a alejarse de sus conectores.

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

Para alinear antenas a larga distancia apropiadamente usted necesitará algún tipo de retroalimentación visual que le muestre la potencia instantánea recibida en el alimentador de la antena. Esto le permitirá hacer pequeños cambios en la alineación de la antena mientras observa la herramienta de registro empleada y detenerse cuando la máxima potencia recibida se haya logrado.

El equipo ideal de alineación de antenas consiste en un generador de señales y un analizador de espectro, preferiblemente uno de cada uno en cada extremo del enlace. En un extremo del enlace se conecta el generador de señales a la antena que está apuntada en la dirección del extremo remoto, en el cual conectaremos el analizador de espectro a la salida de la otra antena. Procedemos ahora a girar lentamente la antena en el extremo remoto, observando la intensidad de la señal hasta que alcanzamos el máximo. Fijamos la posición horizontal y movemos ahora la antena en elevación hasta alcanzar el máximo de señal recibida.

A continuación pasamos a alinear la antena en el otro extremo, para lo cual desconectamos el generador de señales y conectamos el analizador de espectro. En el extremo remoto, sustituimos el analizador de espectro por el generador de señales. Ahora movemos la antena conectada al analizador de espectro observando la intensidad recibida hasta obtener el máximo, en cuyo punto fijamos la antena. En enlaces críticos es conveniente reiterar el proceso en ambos extremos.

En el caso de que sólo dispongamos de un ***generador de señales*** y un ***analizador de espectro***, todavía se puede realizar el alineamiento en ambos extremos, aunque es un poco más engorroso. El equipo que utiliza el analizador de espectro le informa continuamente por teléfono u otro medio de comunicación al otro extremo los valores de señal recibida a medida que se mueve la antena, hasta alcanzar el posicionamiento óptimo en ambos extremos.

Aunque podríamos utilizar la salida de la tarjeta de radio como fuente de señal para la alineación de la antena, esto no funciona bien ya que una tarjeta WiFi transmite muchos paquetes discretos encendiendo y apagando el transmisor muy rápidamente, lo que ocasiona fluctuaciones en la intensidad de la señal recibida en el extremo remoto. Por ello conviene utilizar un generador de señales que produce un tono continuo y estable a la frecuencia de interés.

Obviamente, el costo de un generador de señal calibrado y de un analizador de espectro que trabaje a 2,4 GHz (o incluso 5 GHz, si se usa 802.11a) está fuera de los límites de la mayoría de los proyectos. Afortunadamente, hay una serie de herramientas baratas que pueden usarse en su lugar.

Generador de señales económico

Hay muchos transmisores económicos que usan la banda ISM de 2,4 GHz. Por ejemplo, los teléfonos inalámbricos, los monitores de bebés, y los transmisores de televisión en miniatura, generan todos una señal continua a 2,4 GHz. Los transmisores de televisión (llamados a veces ***transmisores de video*** –

video senders) son particularmente útiles, puesto que a menudo incluyen un conector externo SMA de antena y pueden ser operados con una batería pequeña.

Los transmisores de video normalmente transmiten en tres o cuatro canales y a pesar de que no se corresponden exactamente con canales WiFi, le permitirán probar los extremos bajo, medio o alto de la banda.

Para que 5 GHz funcione, usted puede usar un *video sender* en combinación con un conversor 2,4 GHz a 5 GHz. Estos dispositivos aceptan una señal de baja potencia de 2,4 GHz y emiten señales de alta potencia de 5 GHz. Son normalmente bastante caros (US$ 300-500 cada uno), pero van a ser todavía más baratos que un generador de señales de 5 GHz o un analizador de espectro.

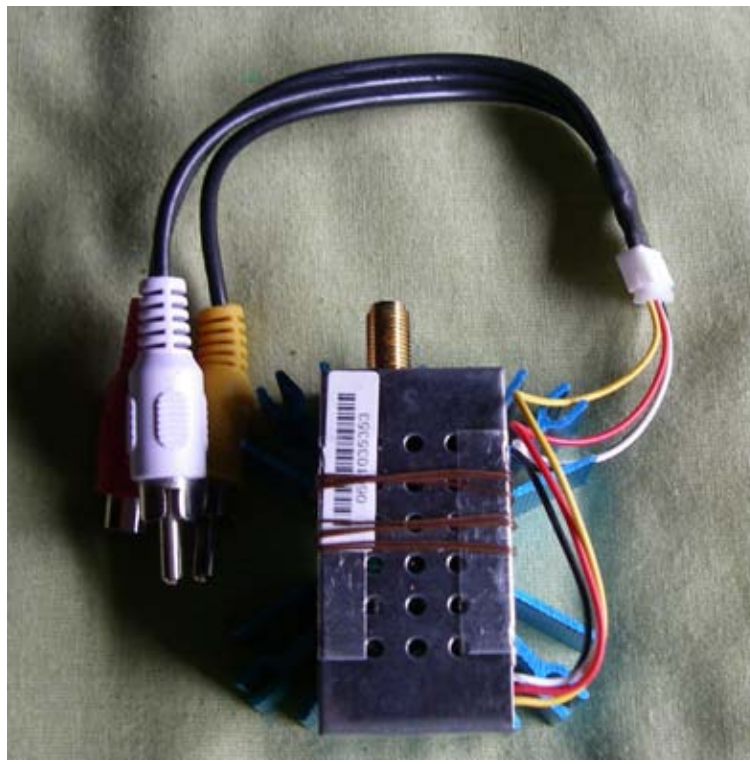


Figura 8.7: Un transmisor de video de 2,4 GHz con un conector de antena SMA.

Independientemente de lo que use como fuente de señal, va a necesitar una forma de mostrar los niveles de potencia recibidos en el otro extremo. Mientras que el costo de analizadores de espectro de 2,4 GHz está bajando progresivamente, lo normal es que cuesten algunos miles de dólares, aún los usados.

Wi-Spy

El Wi-Spy es una herramienta USB para análisis de espectro creada por MetaGeek (*http://www.metageek.net/*). Presenta un receptor muy sensible en un formato pequeño (del tamaño de una memoria USB).

Figura 8.8: El analizador de espectro USB Wi-Spy.

La última versión del Wi-Spy tiene un mejor rango dinámico y un conector de antena externo. También viene con un software muy bueno de análisis de espectro llamado ***Channalyzer***. Muestra valor instantáneo, promedio y máximo de la señal en función de la frecuencia y también ofrece una visión topográfica y un espectrograma que permite observar la evolución del espectro en el tiempo.

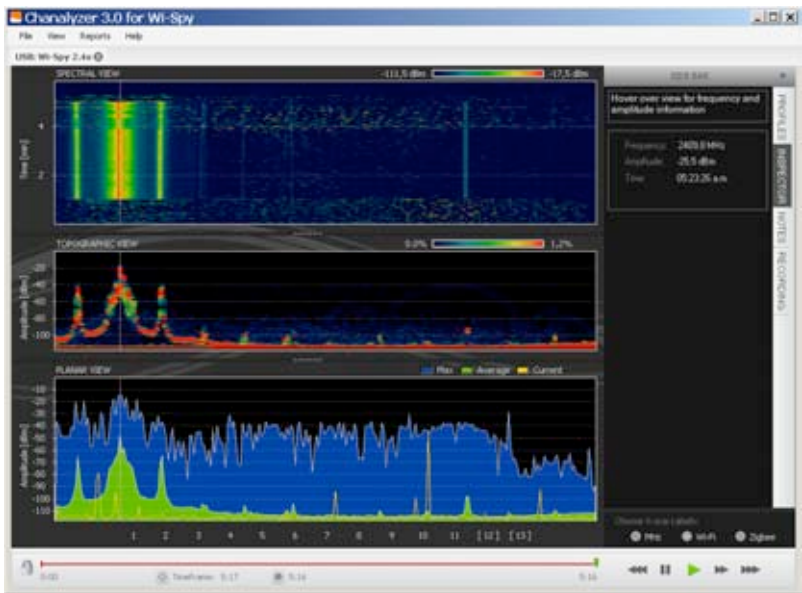


Figura 8.9: El patrón de picos que sobresale a la izquierda del gráfico es causado por un transmisor de televisión de alta potencia a 2,4 GHz.

Hay un excelente paquete de software gratuito para Mac OS X, llamado EaKiu *(http://www.cookwareinc.com/EaKiu/)*. Además de las presentaciones estándar, también tiene una presentación 3D animada, y añade soporte para múltiples dispositivos WiSpy.

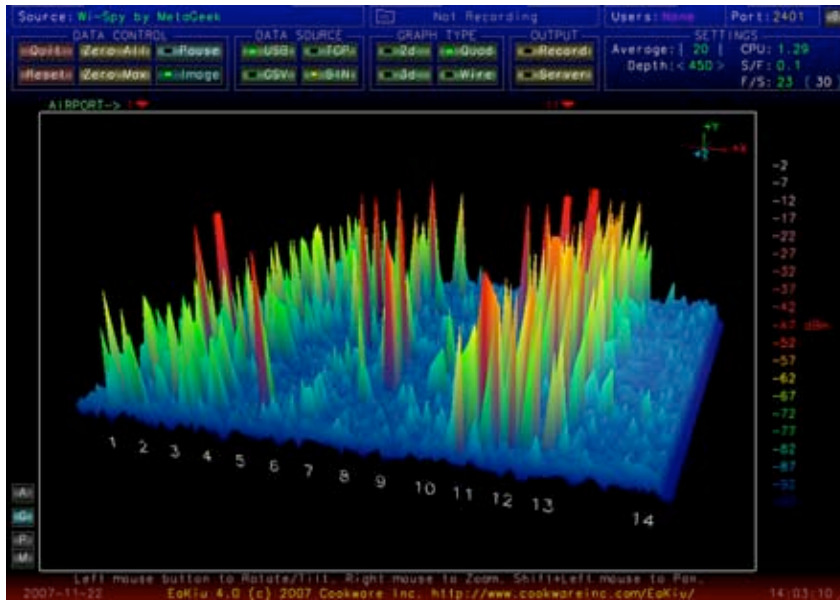


Figura 8.10: La presentación EaKiu en 3D le permite rotar y agrandar cualquier parte del gráfico en tiempo real. Hay probablemente una red WiFi en el canal 11, con otras fuentes de ruido más abajo en la banda.

Para usuarios de Linux, el proyecto Kismet Spectrum-Tools (*http://www.kismetwireless.net/spectools/*) maneja Wi-Spy. Este paquete incluye herramientas de línea de comando al igual que una GUI (Graphical User Interface) incorporado en GTK.

Otros métodos

Algunos enrutadores inalámbricos, (como el Mikrotik) proporcionan una "herramienta de alineación de antena" que le muestra una barra móvil que representa la potencia recibida. Cuando la barra está al máximo, la antena está alineada. Con algunos enrutadores, también se puede habilitar un modo de retroalimentación de audio. Esto hace que el enrutador emita un sonido alto y cambie de tono dependiendo de la potencia de la señal recibida.

Si usted no tiene un analizador de espectro, WiSPy, o un dispositivo que admita un modo de alineación de antena, va a necesitar usar el sistema operativo para obtener retroalimentación sobre la calidad del enlace inalámbrico. Un método simple de hacer esto con Linux es con un lazo (*loop*) que invoque continuamente **`iwconfig`**. Por ejemplo:

```
wildnet:~# while :; do clear; iwconfig; sleep 1; done
```

Esto le mostrará el estado de todas las tarjetas de radio del sistema, actualizado una vez cada segundo. Note que esto sólo va a funcionar en el extremo cliente del enlace. En el lado del punto de acceso (modo maestro), usted debe usar el comando **`iwspy`** para recoger estadísticas para la dirección MAC del cliente:

```
wildnet:~# iwspy ath0 00:15:6D:63:6C:3C
wildnet:~# iwspy
ath0 Statistics collected:
 00:15:6D:63:6C:3C : Quality=21/94  Signal=-74 dBm  Noise=-95 dBm
 Link/Cell/AP      : Quality=19/94  Signal=-76 dBm  Noise=-95 dBm
 Typical/Reference : Quality:0  Signal level:0  Noise level:0
```

Usted puede después usar un lazo **`while`** (como en el ejemplo anterior) para actualizar continuamente el estatus del enlace.

```
wildnet:~# while :; do clear; iwspy; sleep 1; done
```

Procedimiento de alineación de antena

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 para el transporte y asegúrese de que en el campo va a poder repetir bien lo que ha hecho ahora, sólo encendiendo su equipo, sin tener que modificar ningún parámetro. Este es un buen momento para acordar la polarización de las antenas (vea el **Capítulo 2** 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 tiene licencia para radio aficionado, 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 altura.

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 terreno 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. Después de encontrar la mejor elevación, fije la antena en su lugar y avísele 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 sospechosamente 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 al otro del eje visual de la antena. Los reflectores de alimentación excéntrica pueden parecer dirigidos demasiado hacia abajo, o incluso directamente al suelo. No se preocupe de dónde parece apuntar la antena; la posición óptima es aquella que produce la mejor señal.
10. **Revise la polarización.** Puede ser frustrante intentar alinear un reflector 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 está de más.
11. **Si nada funciona, pruebe todos los componentes uno a la vez.** ¿Están encendidos los dispositivos en ambos extremos? ¿Los latiguillos (*pigtails*) y los conectores están conectados correctamente, sin partes dañadas o poco confiables? Como subrayamos en el **capítulo nueve**, 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 (VSAT, por ejemplo). Establecer un cortocircuito a tierra es sencillo. El instalador simplemente debe proveer un camino lo más corto posible desde la estructura 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 tres 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*** y puede ser cualquier pieza de metal

que pese 50 kg o más, tal 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 conexión a 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 110 V ó 220 V). 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).

9
Resolución de Problemas

La manera de establecer 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 fallas en una red que llevaba tiempo funcionamiento satisfactoriamente. Este capítulo detalla una serie de estrategias para ayudarlo/la a formar un equipo de gente que pueda dar soporte a su red de forma efectiva.

Conformando su equipo

Cada pueblo, compañía o familia, tiene algunas personas que están intrigadas por la tecnología. Son aquellas a quienes encontramos empalmando el cable de televisión, reparando un televisor 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/as 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/las 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/as, 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/las más capacitados para darle soporte a la red a largo plazo. Si bien debe involucrar a los/las 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 determinado 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 tuviera 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/a administrador/a local, y trabajar con ellos/as para encontrar el equipo técnico adecuado. Los valores, la historia, las políticas locales y muchos otros factores pueden ser importantes para ellos/as, 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 comprende) 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 decirles que usted no puede contratar familiares, pero deben existir inspecciones y balances. Si tenemos un/a candidato/a 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 compromiso de la comunidad. Una vez que los/las participantes hayan sido seleccionados y se hayan comprometido con el proyecto, involúcrelos/as tanto como sea posible. Déjelos/as "manejar". Entrégueles la pinza crimpeadora (*crimper*), 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/as 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 crear 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 los/las aprendices 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 usted se va a encontrar cuando trabaja con redes inalámbricas, pero a menudo los problemas caen dentro de uno de los pocos errores comunes. A continuación se presentan algunos puntos que se deben recordar, y 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, con seguridad, que el mismo estaba funcionando 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 se pasa por alto hasta que se exploran muchas otras posibilidades. 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 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 estén 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 igual manera, 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 a la vez vez.** Cuando estamos bajo presión para poner un sistema de nuevo en línea, tendemos a actuar impulsivamente y a cambiar muchas variables al mismo tiempo. Si lo hace, y sus cambios solucionan 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 ponerle 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.

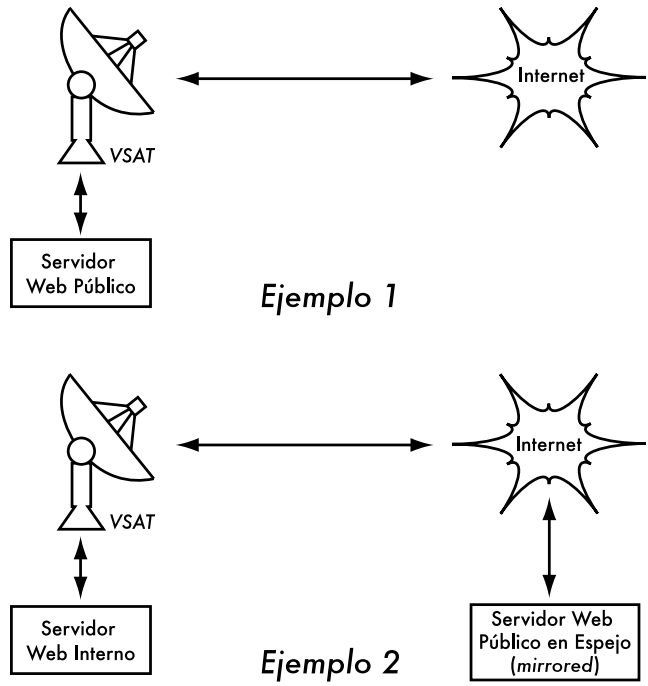


Figura 9.1: En el ejemplo 1, todo el tráfico del sitio web que viene desde Internet debe atravesar el VSAT. En el ejemplo 2, el sitio web público es alojado en un servicio europeo rápido, mientras que en el servidor interno se mantiene una copia para tener un acceso local muy rápido. Esto mejora la conexión del VSAT y reduce los tiempos de carga para los usuarios del sitio web.

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 utilizar un DNS dividido y un servidor espejo. La universidad establece una copia de sus sitios web en un servidor que puede ser una compañía de almacenamiento web (*hosting*)

europea, y utiliza el DNS dividido para direccionar a todos los usuarios de fuera de la universidad hacia el sitio espejo, 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.

Proxys abiertos

Un servidor proxy debe configurarse 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 va a conectarse y utilizar los proxys 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 de un cortafuego, puede configurar el cortafuego para que les 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 (*spam*). 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 ésta, 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 proteja 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). Este 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 para compartir archivos entre pares (*P2P*) tales como Kazaa, Morpheus, BitTorrent, 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/*) ó 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 ISP no lo bloquean, pero sí lo "limitan", utilizando un administrador de ancho de banda.

- **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 PC 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/*) y Ad-Aware (*http://www.lavasoft.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 para 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 es algo debatible que las necesiten las estaciones de trabajo de una red privada protegida, como la red de un campus.
- **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 PC cliente deben configurarse 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 (bitácora) 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 antivirus instalada en todas las PC. Más esencial aún es la educación de los usuarios en cuanto a no ejecutar archivos adjuntos, así como a no dar respuesta a correos no deseados. De hecho, debería haber una política de que ni las estaciones de trabajo, ni el servidor, puedan ejecutar servicios que no estén utilizándose. Una computadora no debería tener recursos compartidos, a menos que fuera un servidor de archivos; y un servidor no debería ejecutar servicios innecesarios. Por ejemplo, los servidores Windows y Unix generalmente ejecutan un servicio de servidor web por defecto. Éste debería deshabilitarse si dicho servidor tiene una función diferente; cuantos menos servicios se puedan ejecutar en 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 reenvían 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 defecto. Los administradores también deben tener cuidado de no apagarlas por error. Debe también evitarse instalar un sistema de reenvío 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, como por ejemplo, 650 MB de imágenes ISO, 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 de URL redireccionado. 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 esté completa. El sistema mantiene una memoria caché 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 soliciten 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 ingresen el URL del archivo que quieran descargar. El mismo se descarga durante la noche utilizando una tarea programada (o ***cron job***, 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 descargar 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 carga (*upload*) del archivo. En Windows, cargar archivos a un servidor FTP remoto puede hacerse 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 ejecutarse en la noche utilizando las Tareas Programadas (Inicio ➔ Configuración ➔ Panel de Control ➔ Tareas Programadas). En Unix, puede hacerse lo mismo utilizando las opciones ***at*** ó ***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, puede escribirse 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 correspondiente 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 puede implementarse fácilmente como un guión (*script*) CGI utilizando Python y Apache.

10
Sostenibilidad Económica

Lograr sostenibilidad a largo plazo es tal vez el objetivo más difícil al diseñar u operar redes inalámbricas y telecentros en los países en desarrollo. El costo prohibitivo de la conexión a Internet en muchos países en desarrollo impone un gasto operativo sustancial y hace que estos modelos sean sensibles a las fluctuaciones económicas, y que necesiten de cierta innovación para lograr factibilidad. Desde hace unos pocos años, ha habido un progreso considerable en el uso de redes inalámbricas para comunicaciones rurales debido, en gran parte, a avances tecnológicos. Se han construido enlaces de larga distancia, los diseños de gran ancho de banda son posibles, y hay disponibles medios seguros de acceso a las redes. En comparación, ha habido pocos éxitos en el desarrollo de modelos comerciales sostenibles para redes inalámbricas y telecentros, especialmente para áreas rurales. Basado en las experiencias y observaciones de los autores sobre redes existentes, así como en el conocimiento a partir de los mejores ejemplos empresariales, este capítulo enfocará la propuesta de métodos para implementar redes inalámbricas y telecentros sostenibles.

En la pasada década ha habido un enorme crecimiento de acceso a Internet en los países en desarrollo. La mayoría de las ciudades del mundo en desarrollo tienen redes inalámbricas o ADSL, y conexiones a Internet de fibra óptica, lo que es un cambio substancial. Sin embargo, fuera de las áreas urbanas, el acceso a Internet es todavía un reto formidable. Hay poca infraestructura cableada más allá de las ciudades importantes. Por lo tanto, la solución inalámbrica es una de las pocas opciones para proporcionar acceso a Internet asequible. Hay ahora modelos de viabilidad demostrada para acceso rural usando tecnología inalámbrica. En Macedonia, el proyecto “Macedonia Connects” ha conectado la mayoría de las escuelas del país a Internet. Este libro ha sido escrito para aquellos que deseen conectar sus comunidades. Los modelos aquí descritos son a escala menor y usan diseños asequibles. Nuestra meta es proporcionar ejemplos de cómo las redes inalámbricas pueden diseñarse para difundir acceso sostenible donde los grandes operadores de telecomunicaciones no han instalado todavía sus redes, en zonas donde usar modelos tradicionales no sería económicamente factible.

Hay dos errores de concepto muy comunes que deben ser aclarados. En primer lugar, muchos suponen que hay un modelo comercial que va a funcionar

para todas las comunidades del mundo en desarrollo, y que la clave del éxito es encontrar esa solución tipo "eureka". En la práctica no es así. Cada comunidad, pueblo o aldea son diferentes. No hay modelo prescrito que satisfaga las necesidades de todas las zonas de países en desarrollo. A pesar de que algunos lugares sean semejantes en términos económicos, las características de un modelo comercial sostenible varían de comunidad en comunidad. A pesar de que un modelo funcione en un poblado, otro poblado cercano puede no tener las características necesarias para que el mismo modelo sea sostenible. En estas circunstancias, otro modelo, novedoso, debe diseñarse para adaptarlo al contexto de esta comunidad en particular.

Otro error es suponer que sostenibilidad tiene una definición común para todo el mundo. A pesar de que este término generalmente significa que un sistema se construye para permanecer indefinidamente, este capítulo se concentrará más en la discusión sobre las condiciones económicas (financieras y gerenciales), que sobre otros aspectos de la sostenibilidad. También, en lugar de plantear horizontes indefinidos, nos centraremos en un período de 5 años—el período de duración útil esperado para las infraestructuras de TIC y tecnologías inalámbricas. De esta manera, el término sostenibilidad será usado para englobar un sistema diseñado para permanecer aproximadamente durante cinco o más años.

Cuando se escoge y se implementa el mejor modelo para una red inalámbrica o un telecentro, hay algunas claves que pueden ayudar a conseguir el éxito. Este capítulo no pretende ser una guía para la gerencia de redes inalámbricas sostenibles. Antes bien, esta guía de "cómo hacer" quiere presentar un enfoque que lo/la capacite para encontrar el modelo que mejor se adapte a su situación. Las herramientas y la información que contiene este capítulo ayudarán a la gente que implementa redes inalámbricas en los países en desarrollo a que se formulen las preguntas apropiadas, y a que recojan los datos necesarios para definir los componentes más apropiados a su modelo. Recuerde que determinar el mejor modelo no es un proceso secuencial donde cada paso se lleva hasta su culminación. De hecho, el proceso es continuado e iterativo. Todos sus pasos están conectados íntegramente unos con otros, y a menudo hay que volver sobre ellos varias veces a medida que se progresa.

Establezca una misión para el proyecto

¿Qué quiere usted lograr al crear su red? Parece una pregunta simple. Sin embargo, muchas redes inalámbricas se instalan sin tener una visión clara de lo que se quiere hacer o se espera lograr en el futuro. El primer paso incluye la conformación de esta visión con el estímulo proveniente de su equipo completo o de su personal. ¿Cuál es el propósito de la red inalámbrica? ¿A quién va a prestar servicio? ¿Qué va a hacer la red para satisfacer las necesidades de la comunidad y para crear beneficios tangibles? ¿Cuáles son los principios rectores de la red? Una buena definición de misión expresa el propósito de su red de una forma significativa y concisa a la vez que formula sus valores y servicios. Y, sobre todo, la misión que establezca proporciona una visión de las aspiraciones de su red inalámbrica.

Es importante que cada miembro del equipo involucrado en la creación de su red inalámbrica se incluya en el proceso de definir la misión, lo que ayuda a crear fortalezas futuras. Esto va a generar respaldo y compromiso, no sólo de parte de su personal, sino de sus clientes, socios, y patrocinadores, lo que va a incidir, a la postre, en el logro de sus objetivos principales. En el dinámico mundo de la tecnología, las necesidades de sus clientes y la mejor manera de satisfacerlas cambia rápidamente; por lo tanto, la definición de su misión es un proceso dinámico. Después de fijar la misión inicial con su equipo, debe investigar para determinar si esta concepción inicial se ajusta a las realidades de su entorno. Con base en un análisis del ambiente externo y de sus capacidades internas, usted debe modificar constantemente su concepto de misión a lo largo del ciclo vital de su red inalámbrica.

Evalúe la demanda de ofertas potenciales

El próximo paso en el establecimiento de su modelo de negocios es averiguar la demanda de la comunidad respecto a los productos de la red y sus servicios. En primer lugar, identifique en la comunidad los individuos, grupos y organizaciones que tienen necesidad de información y que se beneficiarían de las ofertas de una red inalámbrica. El grupo de usuarios potenciales comprende una amplia gama de individuos y organizaciones que incluyen, pero no exclusivamente, los siguientes:

- Asociaciones de agricultores y cooperativas
- Grupos de mujeres
- Escuelas y universidades
- Empresarios locales y comerciales
- Clínicas de salud y hospitales
- Grupos religiosos
- Organizaciones no gubernamentales (ONG) locales e internacionales
- Agencias gubernamentales locales y nacionales
- Estaciones de radio
- Organizaciones de la industria turística

Una vez que establezca una lista de todos los potenciales usuarios de la red, debe determinar sus necesidades de acceso a la información y a la comunicación. A menudo, la gente confunde servicios y necesidades. Un agricultor puede necesitar recabar información sobre precios de mercado y condiciones climatológicas para mejorar la producción de su cosecha y sus ventas. A lo mejor, una manera que tiene de obtener esta información es a través de Internet; sin embargo, también podría recibir esta información por SMS

(mensajes de texto) en un teléfono celular, o a través de Voz en Internet (VOIP, en inglés). Es importante diferenciar entre necesidades y servicios porque puede haber varias formas de satisfacer las necesidades del agricultor. Su red inalámbrica debe buscar la mejor manera de satisfacerlas, creando así beneficio al más bajo costo para el usuario.

Cuando se determinan las necesidades para la comunidad, es importante averiguar dónde puede la red proporcionar el mayor beneficio tangible para sus usuarios. Por ejemplo, en el pequeño pueblo de Douentza, Mali, el gerente de un telecentro consideró, a través de discusiones con algunas organizaciones locales, los beneficios potenciales de establecer una red inalámbrica. Él entrevistó una ONG local que planteó su necesidad de enviar informes mensuales a sus oficinas centrales en Bamako. En ese tiempo, no había acceso a Internet en Douentza, de manera que para enviar un correo electrónico con el informe mensual, la ONG enviaba mensualmente a uno de sus empleados a Mopti, lo que ocasionaba gastos de alojamiento y transporte, además de los adicionales generados por la ausencia al trabajo del empleado durante varios días al mes. Cuando el gerente del telecentro calculó el total de egresos mensuales de la ONG, pudo demostrar el beneficio de la conexión a Internet por el ahorro de gastos de la organización.

La colaboración de socios clave puede ser también necesaria para asegurar la sostenibilidad de su red inalámbrica. En esta etapa, usted debe establecer contacto con socios potenciales y explorar los beneficios mutuos de una cooperación.

Se puede evaluar las necesidades en su comunidad estableciendo contacto con sus clientes potenciales y preguntándoles directamente a través de encuestas, grupos de enfoque, entrevistas, o reuniones municipales. Hacer investigación a través de revisiones de estadísticas pertinentes, reportes industriales, censos, revistas, periódicos, y otras fuentes secundarias de información, también le dará una mejor perspectiva de su entorno local. El objetivo de esta recolección de datos es obtener una comprensión detallada de las necesidades de información y comunicación de su comunidad de manera que la red creada responda a esas necesidades. A menudo las redes inalámbricas que no tienen éxito en los países en desarrollo olvidan este paso clave. Su red entera debería basarse en las necesidades de la comunidad. Si usted inicia una red inalámbrica en la que la comunidad no encuentra ningún beneficio tangible o cuyos servicios sean muy costosos, va a fracasar a la postre.

Establezca incentivos apropiados

A menudo, hay pocos incentivos económicos para acceso a Internet por parte de aquellos participantes cuyos ingresos son de nivel básico. Además, el costo de comprar un computador, aprender a usarlo, y conseguir acceso a Internet, es más alto de lo que se obtiene en retribución. Recientemente, ha habido algunos desarrollos de aplicaciones que enfocan esta falta de incentivo, tales como sistemas de información de mercado, estándares de calidad impuestos por países importadores, e intercambio de bienes. El acceso a Internet se vuelve una ventaja obvia en situaciones donde conocer día a día los precios de los productos pueda hacer una diferencia importante en las ganancias.

Establecer los incentivos económicos apropiados es central para el éxito de la red. La red debe proporcionar beneficio económico a sus usuarios de manera tal que compense los costos, o ser lo suficientemente módica como para que los costos sean mínimos y asequibles para los usuarios. Es imprescindible que se diseñe una red con aplicaciones económicas viables y con costos que sean menores que el beneficio económico que proporciona. Además, al crear una estructura de incentivos adecuada, usted debe involucrar a la comunidad en la creación de la red desde los comienzos del proyecto, asegurando así que la iniciativa sea orgánica y no impuesta desde afuera. Para comenzar, usted debería tratar de responderse las preguntas siguientes:

1. ¿Qué valor económico puede generar la red en beneficio de la economía local e individuos?
2. ¿Qué tanto beneficio económico tangible puede generarse?
3. ¿Pueden solventarse los impedimentos actuales para que se produzcan estas compensaciones económicas?

Al responder estas preguntas, la red debe ser capaz de articular claramente las propuestas de beneficio que va a presentar a los usuarios. Por ejemplo: "Usando la red, usted será capaz de superar los márgenes en sus ventas en un 2 %", o, "Internet le va a permitir un ahorro mensual de X cantidad en costos de teléfono y de transporte". Usted debe calcular cómo su red va a mejorar la eficiencia, reducir los costos o incrementar las ganancias de sus clientes.

Por ejemplo, si la red va a proporcionar información de mercado para la industria local de maíz, debería instalarla cerca de donde los agricultores traen la cosecha para la venta a los comerciantes. Su red, además debería concentrarse en sistemas de información de mercadeo, proveer hojas de precios diarios ($1 cada una), o instalar terminales para vendedores y comerciantes ($2 por hora). Su red también podría proporcionar maneras para que los agricultores puedan leer información sobre nuevas técnicas y nuevos productos. También podría proporcionar conexión inalámbrica a los comerciantes y alquilarles terminales de bajas prestaciones (*thin-client*) para acceso a Internet. Si la clientela fuera pequeña, se podrían reducir los costos limitando el acceso a imágenes y otros servicios que requieran un considerable ancho de banda. De nuevo, conocer el beneficio tangible que su red va a generarles a los comerciantes, va a permitirle calibrar lo que ellos podrán gastar para pagar por sus servicios.

Investigue los marcos regulatorios para sistemas inalámbricos

Los marcos regulatorios para redes inalámbricas también inciden sobre el modelo de negocios que se quiera implementar. Primero, investigue si cualquier organización tiene el derecho de usar frecuencias de 2,4 GHz sin licencia. En la mayoría de las situaciones la banda de 2,4 GHz es de libre uso en todo el mundo; sin embargo, en algunos países el uso de esta banda está restringido, o la licencia para su uso es muy costosa. Por ejemplo, a pesar de que las redes

inalámbricas son legales en Ucrania, el gobierno exige una licencia muy cara para usar las frecuencias de 2,4 GHz, lo que hace que su utilización sea prohibitiva. Lo más frecuente es que sólo Proveedores de Servicio de Internet bien establecidos tengan el flujo de dinero suficiente para pagar estas licencias. Esta restricción hace que sea difícil para una comunidad pequeña compartir una red inalámbrica con otros socios u organizaciones interesados. Otros países, como la República de Mali, son más tolerantes: como no hay estas restricciones para el uso de redes inalámbricas, la posibilidad de compartir la conexión a Internet en pequeñas comunidades es una solución viable. La moraleja es que hay que hacer estas averiguaciones al comienzo para asegurarse de que su red cumpla con las leyes del país y de la comunidad local. Algunos gerentes de proyectos se han visto obligados a desconectar su red inalámbrica simplemente porque, sin saberlo, estaban violando la ley.

También debería indagar sobre la legalidad de los servicios de Voz sobre Protocolo de Internet (VoIP). La mayor parte de los países en desarrollo no han decidido si su uso está permitido. En estos países, nada le impide ofrecer los servicios de VoIP. Sin embargo, en otros países hay una reglamentación complicada sobre VoIP. En Syria, por ejemplo, está prohibido para todo tipo de redes, no sólo inalámbricas. En Ucrania, VoIP es legal sólo para llamadas internacionales.

Analice la competencia

La próxima fase en la evaluación de su comunidad se refiere al análisis de la competencia en redes inalámbricas. La competencia incluye a las organizaciones que proporcionen productos y servicios semejantes (por ejemplo, otro proveedor de Internet inalámbrica, o WISP (Wireless Internet Service Provider); organizaciones que son consideradas sustitutos o alternativas a los productos y servicios que usted proporciona (cibercafés, por ejemplo); y organizaciones que se definen como nuevos participantes en el mercado inalámbrico. Una vez que determine cuáles son sus competidores, debería estudiarlos cuidadosamente. Puede obtener información sobre ellos en Internet, por teléfono, en sus materiales de propaganda y mercadeo, en sondeos a sus clientes, o visitas a sus sitios Web. Genere un archivo para cada competidor. La información sobre la competencia que recolecte puede incluir una lista de servicios (con información sobre precios y calidad), sus clientes-objetivo, técnicas de servicio al cliente, reputación, mercadeo, etc. Asegúrese de recabar toda información que le ayude a determinar cómo posicionar su red en la comunidad.

Es importante evaluar a la competencia por muchas razones. En primer lugar, le ayuda a determinar el nivel de saturación del mercado. Ha habido algunos ejemplos donde un telecentro ha sido subsidiado y establecido por una organización donante en un poblado pequeño, con escasa demanda, y a pesar del hecho de que ya existiera un cibercafé en la localidad. En uno de los casos, el centro subsidiado mantuvo los precios bajos porque no tenía que cubrir sus costos. Este caso ocasionó que, a la postre, el cibercafé local quebrara, y después del cese del financiamiento, también quebró el telecentro subsidiado, debido a las pocas ganancias y altos costos. Conocer lo que ya existe le

permitirá determinar de qué manera su red puede proporcionar beneficio tangible a la comunidad. Además, el análisis de la competencia puede estimular ideas innovadoras para sus ofertas de servicio. ¿Hay algo que usted pueda hacer mejor que los competidores para hacer que sus servicios satisfagan mejor las necesidades de la comunidad? Finalmente, al analizar a la competencia desde el punto de vista de los clientes y al entender sus fortalezas y debilidades, puede determinar sus ventajas competitivas en la comunidad. Ventajas competitivas son aquellas que no pueden ser fácilmente copiadas por la competencia. Por ejemplo, si su red inalámbrica puede ofrecer exclusivamente una conexión a Internet más rápida que la competencia, esto constituye una ventaja competitiva que facilita la captación de clientes.

Determine costos y precios iniciales y recurrentes

Cuando esté planeando instalar y operar su red inalámbrica, debe determinar los recursos necesarios para arrancar el proyecto, y para su mantenimiento y operación. Los costos de instalación incluyen todo lo que debe comprar para arrancar su red inalámbrica. Estos gastos abarcan desde la inversión inicial que se hace en hardware, instalaciones, y equipamiento para *access points*, conmutadores (*switches*), cables, UPS, etc., hasta los costos para cubrir el registro legal de su organización. Los gastos recurrentes son aquellos en los que se incurre para continuar operando su red inalámbrica, incluidos costos de acceso a Internet, teléfono, préstamos, electricidad, salarios, alquiler de locales, mantenimiento y reparación de equipos, y la inversión normal para reemplazar desperfectos o equipos obsoletos.

Cada parte de su equipo va a dañarse en algún momento, o va a quedar obsoleta, y usted debería reservar algún fondo extra para estos propósitos. Un método muy común y aconsejable de enfrentar esto es el de tomar el precio del artefacto y dividirlo por un tiempo estimado de duración. A este proceso se le llama ***depreciación***. A continuación, un ejemplo. La duración de un computador promedio es de unos dos a cinco años. Si su costo inicial fue de USD 1.000, y usted considera que remplazará el computador a los cinco años, la depreciación anual va a ser de USD 200. En otras palabras, usted debe adjudicar USD 16,67 mensualmente para, finalmente, reemplazar ese computador. Para hacer que su proyecto sea sostenible, es de fundamental importancia que usted ahorre este dinero para compensar la depreciación del equipo cada mes. Guarde estos ahorros hasta que finalmente pueda utilizarlos para costear el reemplazo del computador. Algunos países tienen leyes de impuestos que determinan el período de depreciación para los diferentes tipos de artefactos. De cualquier manera, usted debería ser realista en cuanto a la vida útil de todo el equipo en uso y hacer planes cuidadosos para contrarrestar su depreciación.

Trate de establecer todos sus costos por anticipado, y haga estimaciones realistas sobre sus gastos. La siguiente tabla le muestra una forma de clasificar y detallar sus costos. La estructuración de los diferentes costos es un buen instrumento que le ayudará a distinguir entre los costos iniciales y los recurrentes.

Es importante investigar sus costos iniciales desde el comienzo y hacer estimaciones realistas de sus gastos recurrentes. Es siempre mejor presupuestar los gastos por encima que por debajo. Con cada proyecto inalámbrico hay siempre gastos imprevistos, especialmente durante el primer año de operaciones cuando se está aprendiendo a administrar mejor la red.

Categorías de costos

Para mejorar sus probabilidades de sostenibilidad, es generalmente mejor mantener la más baja estructura de costos para su red. En otras palabras, mantenga sus gastos lo más bajo posible. Tome tiempo en indagar sobre sus proveedores, en particular su proveedor de servicios de Internet (ISP, por sus siglas en inglés) y localice las mejores ofertas en servicio de calidad. Una vez más, asegúrese de que su compra se corresponda con las necesidades de la comunidad. Antes de instalar un VSAT caro, asegúrese de que en su comunidad haya un número suficiente de individuos y organizaciones que estén dispuestos a usarlo. Dependiendo de la demanda de acceso a la información y capacidad de pago, un método alternativo de conectividad podría ser más apropiado. No tenga miedo de innovar y sea creativo/a cuando establezca la mejor solución.

No se debe mantener los precios bajos a expensas de la calidad. Puesto que los equipos de baja calidad son más susceptibles a los daños, a la larga podría estar gastando más en mantenimiento. Es difícil prever la cantidad de dinero que gastará en mantener su infraestructura de TIC. A medida que ésta sea más grande y compleja, mayor es la cantidad de recursos laborales y financieros que se deben anticipar para su mantenimiento.

Muchas veces esta relación no es lineal sino exponencial. Si usted tiene algún problema de calidad con su equipo después de que esté instalado, puede costarle una cantidad considerable de dinero arreglarlo. Al mismo tiempo, sus ventas disminuirán porque el equipo no está funcionando como debería. Hay un ejemplo interesante de un gran proveedor de servicios inalámbricos de Internet (WISP, por sus siglas en inglés) que tenía más de 3.000 *access points* operando por un tiempo. Sin embargo, el proveedor nunca pudo alcanzar el punto de equilibrio porque tenía que gastar mucho en el mantenimiento de todos los *access points*.

	Costos iniciales	Costos recurrentes
Costos laborales	• Consultorías y revisiones • Definición de costos de programación, pruebas, integración, etc. • Costos de instalación • Costos de reclutamiento de personal • Costos de capacitación (inducción)	• Gestión, salarios para empleados/as y contratistas incluido/a usted • Mantenimiento y soporte de equipos (software, hardware y equipos auxiliares) • Seguridad del personal • Capacitación (mantenimiento)

	Costos iniciales	Costos recurrentes
Costos materiales	• Adquisición y producción (hardware: PC, equipos satelitales o de radio-enlaces, software) • Equipos auxiliares conmutadores (switches), cables y cableado, generadores, UPS, etc.) • Seguridad y protección de datos • Inventario inicial (sillas, mesas, iluminación, alfombras, cortinas, etc.) • Costos del local (nuevas construcciones, modificaciones, aire acondicionado, instalaciones eléctricas, rejas de seguridad) • Costos legales como el registro del negocio • Costos iniciales de licencias • Gastos iniciales de mercadeo (folletos, afiches, fiesta de apertura)	• Costos de operación de hardware y sistemas operativos (acceso a Internet, teléfono, etc.) • Rentas o alquileres • Depreciación de equipos y hardware • Gasto de licencias • Suministros e insumos de oficina (Ej.: dispositivos de almacenamiento de datos, papel, clips, carpetas, engrapadoras) • Mantenimiento de la seguridad y protección de datos • Primas de seguros • Pago de energía y mantenimiento de su suministro • Pagos de préstamos, costos de amortización • Costos de anuncios • Impuestos locales • Servicios legales y de contabilidad • Servicios legales y de contabilidad

Además, la compañía subestimó la corta duración de ese tipo de equipos. El hardware para TIC tiende a volverse más barato y mejor cada día. Tan pronto como la compañía había invertido tiempo y dinero en instalar la versión de los costosos access points 802.11b de primera generación, fue creado el nuevo estándar “g”. Nuevos competidores diseñaron access points mejores y más económicos y ofrecieron acceso más rápido y más barato a Internet. Finalmente, el primer proveedor de Internet inalámbrica se vio forzado a cerrar la compañía, a pesar de haber sido el líder del mercado al comienzo. Mire la tabla siguiente para tener una mejor visión del rápido desarrollo de los estándares y equipos inalámbricos:

Protocolo	Fecha de lanzamiento	Tasa de datos típica
802.11	1997	< 1 Mbps
802.11b	1999	5 Mbps
802.11g	2003	20 Mbps
802.11a	1999, raro antes de 2005	23 Mbps
802.11y	Junio 2008 (estimado)	23 Mbps
802.11n	Junio 2009 (estimado)	75 Mbps

Tenga presente el rápido avance y cambio de la tecnología y piense cuándo es el momento de reinvertir en equipos más nuevos y económicos (o mejores) y cómo hacerlo para mantener su infraestructura competitiva y actualizada. Como se mencionó antes, es muy importante que ahorre lo suficiente para hacerlo cuando sea necesario.

Una vez que haya identificado y delineado sus costos, debería determinar cuánto y cómo cobrar por sus servicios. Este es un proceso que es complicado y toma tiempo realizarlo correctamente. Las siguientes claves pueden orientarlo/la cuando tome decisiones respecto a precios.

- Calcule los precios que va a cobrar de manera que cubra todos los costos de proporcionar el servicio, incluidos los gastos recurrentes.
- Tome en cuenta los precios de la competencia.
- Evalúe la cantidad que los clientes están dispuestos a pagar por los servicios, y asegúrese de que sus precios sean concordantes.

Es completamente esencial diseñar un plan financiero antes de comenzar. Usted necesita registrar todos los costos tanto iniciales como recurrentes y hacer cálculos para determinar si el proyecto es sostenible.

Asegure el financiamiento

Una vez que determine sus costos iniciales y recurrentes, y cree su plan de financiamiento, usted va a saber cuánto es el financiamiento que necesita para administrar su red inalámbrica. El próximo paso es buscar y garantizar la cantidad de dinero apropiada para arrancar y gestionar su red inalámbrica.

EL método más tradicional de recibir financiamiento para redes inalámbricas en los países en desarrollo es a través de subvenciones provenientes de donantes.

Un donante es una organización que otorga dinero u otros tipos de donaciones a una organización o consorcio de organizaciones, con el fin de ayudarles a regentar proyectos o apoyar causas. Como este financiamiento se otorga en forma de donaciones u otros subsidios, no se espera que sean devueltos por las organizaciones que realizan el proyecto inalámbrico, ni por los beneficiarios del proyecto. Estos donantes incluyen grandes organizaciones

internacionales como la Organización de las Naciones Unidas (ONU) y algunas de sus agencias especializadas, como el Programa de Desarrollo de las Naciones Unidas (UNDP, por sus siglas en inglés) y la Organización Educativa, Científica y Cultural de las Naciones Unidas (UNESCO). También se consideran donantes las agencias gubernamentales especializadas en desarrollo internacional, como la Agencia Estadounidense para el Desarrollo Internacional (USAID, en inglés), el Departamento para Desarrollo Internacional del Reino Unido (DFID, en inglés), y la Agencia Canadiense para el Desarrollo Internacional (CIDA, en inglés). Organizaciones grandes como la Fundación Gates, la Red de la Fundación Soros y las compañías privadas son otro tipo de donantes.

Comúnmente, recibir fondos puede ser o no un proceso competitivo. El proceso no competitivo es más inusual, así que en este capítulo vamos a concentrarnos en el proceso competitivo de más alto nivel. La mayoría de los donantes tienen procedimientos complicados para la distribución de financiamiento. Los autores de este libro no estamos tratando de trivializar este sistema de reglas y regulaciones, sino que vamos a tratar de presentar una visión general de este proceso para aquellas comunidades que tratan de implementar redes inalámbricas en los países en desarrollo. Durante el proceso competitivo de convocatoria, el donante usualmente hace una ***convocatoria de propuestas*** (**RFP**, en inglés), o una ***convocatoria de solicitudes*** (**RFA**, en inglés), por medio de las cuales se invita a organizaciones no gubernamentales, compañías privadas y sus socios, a presentar propuestas donde se expongan los planes para llevar a cabo proyectos de acuerdo con los requisitos de los objetivos y lineamientos del donante. En respuesta a estas convocatorias, las ONG y otras organizaciones compiten presentando sus solicitudes, que luego son evaluadas por los donantes basándose en criterios específicos. Finalmente, la organización donante selecciona la propuesta más apropiada y que haya recibido la más alta evaluación para subvencionarla. A menudo, los donantes también otorgan fondos para financiar directamente las operaciones de una organización, pero lo más frecuente es que la asignación se haga en un proceso competitivo de convocatoria.

Otra forma de acceder a los fondos necesarios para comenzar y mantener una red inalámbrica es a través de micro-financiamiento o el otorgamiento de préstamos, ahorros u otros servicios financieros básicos para la gente más necesitada. En 1970, algunas organizaciones pioneras como ACCION Internacional y el Banco Grameen, otorgaron microcréditos, que es una forma de micro-financiamiento que les permite a personas necesitadas, o emprendedores, recibir préstamos de sumas módicas para fundar pequeñas empresas. A pesar de que estos individuos carezcan de los requisitos tradicionales para obtener préstamos, tales como bienes que puedan ofrecer como garantías, empleos secundarios o fijos, los programas de microcréditos han sido muy exitosos en muchos países en desarrollo. La situación más común en estos casos es la de una persona, o un grupo que realiza una solicitud de préstamo, y un ente financiador, persona u organización, que otorga el préstamo, proporcionando el dinero bajo la condición de que se devuelva con intereses.

El uso de microcréditos para financiar redes inalámbricas plantea una limitación. Comúnmente los microcréditos otorgan sumas muy pequeñas, y como se necesita un capital grande para adquirir el equipo inicial para implementar una red inalámbrica, a menudo el microcrédito no es suficiente. Sin embargo, ha habido otras aplicaciones exitosas del microcrédito que han proporcionado tecnología y sus beneficios al mundo en desarrollo. Un ejemplo de esto es la historia de los operadores de teléfono en pequeños poblados. Estos emprendedores usan los microcréditos para comprar teléfonos celulares y crédito telefónico. Luego alquilan el uso de estos celulares a las personas de la comunidad, cobrando por llamada, y obteniendo así suficiente dinero para pagar sus deudas y obtener ganancias para ellos y sus familias.

Otros mecanismos de financiamiento para instalar redes inalámbricas es conseguir inversores ángel (*angel investors*). Los inversores ángel son por lo general personas adineradas que proporcionan capital para iniciar negocios a cambio de una tasa alta de retorno de su inversión.

Ya que las empresas en las que invierten estos financistas son empresas nacientes (*start-ups*) y, por lo tanto, de alto riesgo, los inversores ángel suelen tener otras expectativas además de las tasas de retorno, tales como un puesto en las juntas directivas o algún rol en la organización. Algunos prefieren tener participaciones en la compañía, mientras que otros prefieren las acciones que puedan cambiar al valor nominal, garantizando una salida claramente definida para el financista. Para proteger sus inversiones, los inversores ángel a menudo piden al proyecto que no se tomen ciertas decisiones sin su aprobación. En vista del riesgo alto que se corre en el desarrollo de mercados, a menudo es difícil conseguir inversores ángel para lanzar una red inalámbrica, pero no es imposible. La mejor manera de encontrar financistas potenciales es a través de su red social y de búsquedas en línea.

Evalúe las fortalezas y debilidades de la situación interna

La calidad de una red se mide por la calidad de la gente que la opera. El equipo humano que usted ponga al frente puede hacer la diferencia entre el éxito y el fracaso. Esta es la razón por la cual debe analizar las calificaciones y destrezas de su equipo, incluyendo empleados y voluntarios, para evaluarlas en relación con las destrezas que se requieren para un proyecto inalámbrico. En primer lugar, haga una lista de las habilidades que se necesitan para desarrollar exitosamente un proyecto de red inalámbrica. Las capacidades deben incluir tecnología, recursos humanos, contabilidad, mercadeo, ventas, negociación, áreas legales, operaciones, entre otras. Después, identifique los recursos locales con los que cuenta para satisfacer estas necesidades. Compare las habilidades de su equipo humano con las destrezas que necesita, e identifique las carencias.

Una herramienta usada a menudo para ayudar en esta auto-evaluación es un método de análisis de fortalezas, oportunidades, debilidades, y amenazas, llamado FODA y en inglés SWOT (*Strengths, Weaknesses, Opportunities and Threats*). Para llevar a cabo el análisis, especifique sus fortalezas y debilidades

internas y detalle las oportunidades externas y amenazas en su comunidad. Es importante ser realista y honesto acerca de sus cualidades y de sus carencias. Asegúrese de distinguir entre la posición de su organización al comienzo de este esfuerzo, y la que podría ocupar en el futuro. Sus fortalezas y debilidades le permiten evaluar sus capacidades internas y entender mejor lo que su organización puede hacer, así como sus límites. Al entender sus fortalezas y debilidades y compararlas con las de la competencia, usted puede establecer ventajas competitivas en el mercado. También puede identificar las áreas donde se puede mejorar. Las oportunidades y riesgos son factores externos, lo que lo/la capacita para analizar las condiciones reales y cómo estas van a afectar su red.

El diagrama que presentamos a continuación le ayudará a crear el análisis FODA de su organización. Asegúrese de responder las preguntas planteadas y enumere sus fortalezas, oportunidades, debilidades y amenazas en los espacios apropiados.

Fortalezas	Debilidades
• ¿Qué hace usted bien? • ¿Qué recursos especiales puede usar? • ¿Qué perciben otros sobre sus fortalezas? • ¿?	• ¿Qué podría mejorar? • ¿Dónde tiene menos recursos? • ¿Qué podrían percibir los otros como sus debilidades? • ¿?
Oportunidades	**Riesgos**
• ¿Qué buenas oportunidades se le abren? • ¿Cuáles de sus tendencias puede aprovechar? • ¿Cómo puede transformar fortalezas en oportunidades? • ¿?	• ¿Qué tendencias podrían perjudicarle? • ¿Qué está haciendo la competencia? • ¿Cuáles riesgos se derivan de sus debilidades? • ¿?

Armando el conjunto

Una vez que usted haya reunido toda la información, ya está listo/a para armar las partes y decidir cuál es el mejor modelo de red inalámbrica para su comunidad. Con base en análisis internos y externos, debe refinar los términos de su misión y de sus ofertas de servicio. Todos los factores que ha investigado en los pasos anteriores entran en juego cuando determine su estrategia global. Es esencial utilizar un modelo que aproveche las oportunidades y las acciones dentro de los límites del entorno local. Para esto, usted debe, a menudo, encontrar soluciones novedosas para lograr sostenibilidad. Hay que explorar

diferentes ejemplos y discutir los componentes de los modelos implementados en ellos, para entender mejor cómo se llega al modelo adecuado.

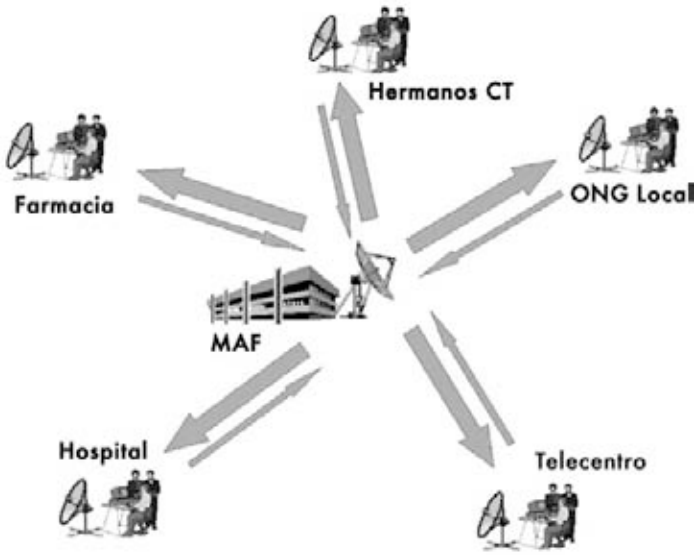


Figura 10.1: Compartiendo Internet con un sistema inalámbrico

En la distante jungla del la República Democrática del Congo, hay un hospital rural en un poblado llamado Vanga, en la provincia de Bandundu. Queda tan lejos que los pacientes viajan durante semanas para llegar, a veces en una combinación de viaje a pie y navegación fluvial. Este poblado, fundado por misioneros Baptistas en 1904, ha servido de hospital durante años. A pesar de su lejanía extrema, es renombrado por sus excelentes instalaciones y por tener el apoyo de misioneros de Alemania y Estados Unidos, quienes mantienen la instalación funcionando. En 2004, un proyecto financiado por USAID estableció un telecentro en este poblado para ayudar a mejorar la educación en esta comunidad tan aislada; esta instalación de Internet era muy usada por el grupo más educado de la comunidad: el personal del hospital. El centro había sido una bendición para la comunidad al ofrecer acceso al conocimiento mundial, e incluso acceso a consultas con colegas distantes en Suiza, Francia y Canadá. El centro requirió un financiamiento casi total para su operación y costos, y el subsidio debía finalizar en 2006. A pesar de que el centro proporcionó un gran beneficio tangible a la comunidad, tuvo algunos inconvenientes, principalmente factores técnicos, económicos, y políticos que limitaron su sostenibilidad. Se formó una comisión para estudiar sus opciones para el futuro. Después de revisar la estructura de costos del centro, se determinó que necesitaba rebajar sus costos y buscar nuevas formas de incrementar las ganancias. Los gastos más grandes eran los de electricidad y acceso a Internet; por lo tanto, se necesitaba un modelo creativo para reducir los gastos del telecentro y proporcionar acceso de manera sustentable.

En este ejemplo, se usó un VSAT tradicional para dar conectividad. Sin embargo, este modelo proporcionó una forma única de incluir la limitada

capacidad de pago de Internet de los grupos locales de la comunidad. Varias organizaciones en la comunidad compartieron el acceso a Internet por medio de una red inalámbrica; también compartieron los costos asociados con la conexión. Este modelo funcionó bien gracias a condiciones específicas—es decir, la conciencia y la concepción de Internet como un beneficio por parte de miembros clave de la comunidad, los recursos necesarios para proporcionar acceso a Internet, y un sistema regulatorio que permitió compartir el sistema inalámbrico. En Vanga, algunas organizaciones, incluidas el hospital, la farmacia, algunos grupos misioneros, un centro de recursos comunitarios y algunas organizaciones sin fines de lucro tienen la necesidad de acceso a Internet y los medios para pagarlo. Este arreglo hace que la red de organizaciones tenga una conexión de mejor calidad a bajo precio. Adicionalmente, una de las organizaciones del poblado tiene la capacidad y la voluntad de manejar algunos aspectos de la operación de la red, incluyendo emisión y cobro de recibos, mantenimiento técnico y manejo económico general de la red entera. De esta manera, este modelo funciona bien en Vanga porque ha sido diseñado para satisfacer las exigencias de la comunidad y para impulsar los recursos económicos locales.

Figura 10.2: Punto de acceso itinerante de DakNet

Otro ejemplo de un modelo adaptado para satisfacer el contexto local es el DakNet de First Mile Solutions. Este modelo ha sido empleado en poblados en India, Cambodia, Rwanda y Paraguay. Teniendo en cuenta la limitada capacidad adquisitiva de los habitantes, este modelo maneja sus necesidades comunicativas en una forma novedosa. En el modelo DakNet, hay una franquicia en el país, y se reclutan emprendedores locales para darles entrenamiento en la operación de los kioscos equipados con antenas WiFi. Por medio de tarjetas pre-pagadas, los habitantes pueden enviar y recibir,—asincrónicamente–, correos electrónicos, textos, y correos de voz, hacer

búsquedas en la Web y participar en el comercio electrónico. Estas comunicaciones se almacenan en el servidor local del kiosco. Cuando un autobús o una motocicleta con un punto de acceso itinerante pasa cerca del kiosco, el vehículo en cuestión recibe los datos almacenados y envía los datos recibidos. Una vez que el vehículo llega a un punto con conexión a Internet, procesa todas las solicitudes, transfiere correos electrónicos, mensajes y archivos compartidos.

DakNet integra acceso itinerante y modelos de franquicia para proporcionar beneficios tangibles a los habitantes de poblados remotos. Para que este modelo sea sostenible, algunas condiciones clave deben estar presentes. Primero, debe existir una organización de franquicia para proporcionar apoyo financiero e institucional, incluyendo la inversión inicial, capital operativo para ciertos gastos recurrentes, asesoramiento sobre actividades de inicio, entrenamiento de gerencia, procesos estandarizados, mecanismos de reporte y herramientas de mercadeo. Adicionalmente, este modelo necesita una persona del lugar, dinámica y muy motivada que tenga las destrezas apropiadas para manejar un negocio y voluntad de aceptar las sugerencias hechas por la franquicia. A estos emprendedores se les pide a menudo que empleen su propio capital en los gastos de inicio, de manera que necesitan tener acceso a suficientes recursos económicos. Finalmente, para asegurarse de que este modelo se auto-sostenga, debería haber suficiente demanda de información y comunicación y pocos competidores en la comunidad.

Conclusión

No hay un modelo único para que las redes inalámbricas sean sostenibles en los países en desarrollo; se deben usar y adaptar diferentes modelos de acuerdo con las circunstancias. Cada comunidad tiene características únicas y debe haber suficiente investigación al comienzo del proyecto para determinar el modelo más adecuado. El análisis debe considerar varios factores clave del entorno local, incluyendo demanda en la comunidad, competencia, costos, recursos económicos, etc. A pesar de que una planificación y puesta en marcha adecuadas van a maximizar las posibilidades de que su red sea sostenible, no hay garantías de éxito. Sin embargo, usando los métodos explicados en este capítulo, usted ayudará a garantizar que su red le proporcione a la comunidad beneficios tangibles que se correspondan con sus necesidades.

11
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/a veterano/a en esto, es reconfortante recordar que siempre hay algo por 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 90 mm 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, crean una cubierta muy robusta a prueba de agua. 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 entrada de insectos 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 30 mm 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 precaución. Este tipo de mástil puede ser alargado 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 compromiso de la comunidad es imperativo para asegurar el éxito y la sostenibilidad del proyecto. Involucrar a la comunidad en el proyecto puede ser

el desafío más grande, pero si no 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 estratégicos 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/a cuando elige sus aliados. Una reunión "del municipio" es útil para observar la política, alianzas y rencillas 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 desproporcionado. La honestidad, la franqueza y no hacer promesas que no se puedan cumplir son factores importantes.

En comunidades con altos índices de analfabetismo, enfóquese en servicios de transformación de digitales a analógicos, tales como Internet para estaciones de radio, impresión de 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 cuáles 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 ONG, donantes y socios no se informan entre sí sobre su compromiso con el beneficiario. Los beneficiarios astutos pueden ganar atractivas recompensas permitiendo que las ONG y los donantes derrochen equipos, capacitación y fondos. Es importante conocer qué otras organizaciones están involucradas de manera que pueda comprender cómo 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 equipadas con 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. Sin embargo, pueden consultarse en *www.wndw.net.*

Red Comunitaria Inalámbrica de la Fundación Fantsuam

Kafanchan es una comunidad de 83.000 personas situada a 200 km al noroeste de Abuja, en Nigeria central. Kafanchan era conocida como una ciudad animada y pujante ya que tenía uno de los principales nudos de la red nacional de ferrocarril.

Cuando la industria del ferrocarril estaba en su apogeo, casi el 80 % de la población de Kafanchan solía usarlo constantemente. Después de la quiebra del sistema de ferrocarriles de Nigeria, la población de Kafanchan se ha visto forzada a regresar a la fuente original de ingreso que es la agricultura.

Kafanchan es un área con conectividad limitada en lo que respecta a Internet y telefonía fija. Actualmente no hay telefonía fija (PSNT) en el área, y GSM llegó apenas en el 2005. Sin embargo, la cobertura GSM es tan deficiente como la calidad del servicio. Es estos momentos, los servicios de SMS son la fuente de comunicación más confiable porque la conversación de voz usualmente se corta y presenta mucho ruido.

El deficiente acceso a la electricidad les plantea retos adicionales a la gente de Kafanchan. La compañía de energía eléctrica nacional de Nigeria, NEPA (*National Electric Power Authority*), es comúnmente llamada por los nigerianos "*Never Expect Power Always*" (algo como "Nunca Esperes Energía Siempre"). En el 2005, NEPA cambió su nombre a *Power Holding Company of Nigeria* (PHCN).

Kafanchan recibe energía de NEPA durante un promedio de tres horas diarias. Las 21 horas restantes, la población depende de generadores a diesel o kerosén para alumbrarse y cocinar. Cuando se dispone de NEPA en el alumbrado público, proporciona un voltaje no regulado del rango de 100-120 V en un sistema diseñado para 240 V. Este voltaje debe regularse a 240 V antes de que la mayoría de las cargas puedan ser conectadas. Sólo los bombillos incandescentes pueden ser alimentados directamente de la red ya que pueden soportar voltajes bajos sin dañarse.

Participantes en el proyecto

Dadas las difíciles condiciones de Kafanchan, ¿cómo podría a alguien ocurrírsele la idea de establecer allí el primer ISP rural inalámbrico de Nigeria? La Fundación Fantsuam tuvo la idea y la llevó a cabo.

La Fundación Fantsuam es una organización local no gubernamental que ha venido trabajando con la comunidad de Kafanchan desde 1996 en la lucha contra la pobreza y la desigualdad a través de programas integrados de desarrollo. El enfoque de Fantsuam son los micro créditos, servicios ICT y el desarrollo social de las comunidades rurales de Nigeria. Transformarse en el primer ISP inalámbrico rural de Nigeria fue parte de su misión de constituirse en líderes reconocidos de la provisión de iniciativas de desarrollo rural, así como en importantes motores de la economía rural.

EL ISP inalámbrico de la Fundación Fantsuam, también conocido como ***Zittnet***, fue financiado por el IDCR (*International Development Research Centre of Canada*). IT +46, una compañia consultora de Suecia dedicada a ITC para el desarrollo, ha trabajado con el equipo Zittnet para proporcionarles soporte técnico para comunicaciones inalámbricas, manejo de banda ancha, energía solar, sistemas de respaldo de energía, y despliegue de VoIP.

Objetivos

El principal objetivo de Zittnet es mejorar el acceso a las comunicaciones en el área de Kafanchan a través de la implementación de una red inalámbrica comunitaria. La red proporciona acceso a intranet e Internet a socios locales de la comunidad. La red comunitaria está formada por organizaciones basadas en la comunidad, tales como instituciones educativas, instituciones religiosas, servicios de salud, pequeñas empresas e individuos.

Sistema de energía de respaldo

Con la finalidad de proporcionar un sistema confiable para la comunidad, Zittnet necesitaba proveerse de un sistema de energía de respaldo confiable que hiciera funcionar la red independientemente de NEPA. Se diseñó entonces un

sistema híbrido para Fantsuam que comprendía un banco de baterías de ciclo profundo y dos paneles solares de 2 kW (pico). Las baterías puede cargarse a partir de tres fuentes diferentes: un generador diesel, un arreglo solar, y desde NEPA, cuando se dispone de electricidad. El centro de operaciones de la red (**NOC**: *Network Operation Center*) funciona completamente con energía solar. El resto de las instalaciones de Fantsuam funciona a partir de NEPA o el generador a través del banco de baterías, lo que proporciona voltaje ininterrumpido estable. La carga del NOC se ha separado del resto de la carga de Fantsuam para garantizar una fuente confiable de energía a la crítica infraestructura del NOC incluso cuando el banco de baterías está parcialmente descargado.

Figura 11.1: Se montaron 24 paneles solares con una potencia nominal de 80 W en el techo del NOC para proporcionar energía 24/7 al sistema.

Las simulaciones con los mejores datos solares muestran que el estado de Kaduna, donde se encuentra Kafanchan, recibe por lo menos 4 horas solar pico durante sus peores meses que van de junio a agosto (estación de lluvias). Cada panel solar (Suntech 80 W pico) proporciona una corriente máxima de 5 A (cuando la radiación solar está al máximo durante el día). En los meses peores, se espera que el sistema produzca no menos de 6 KWh/día.

El sistema solar se diseñó para proporcionar salidas de 12 y 24 V DC con la finalidad de concordar con el voltaje de entrada de todos los servidores de bajo consumo y de las estaciones de trabajo de la infraestructura de NOC y de los salones de entrenamiento. Se usaron paneles solares ***Suntech STP080S-12/Bb-1*** con las especificaciones siguientes:

- Tensión de circuito abierto (V_{OC}): **21.6 V**
- Tensión de funcionamiento óptimo (V_{MP}): **17.2 V**
- Corriente de cortocircuito (I_{SC}): **5 A**

- Corriente de funcionamiento óptimo (I_{MP}): **4.65 A**
- Punto de máxima potencia (P_{MAX}): **80 W (Peak**)

El mínimo de 6 KWh/día que alimenta el NOC se usa para dar energía al equipo siguiente:

Dispositivo	Horas/día	Unidades	Potencia (W)	Wh
Puntos de acceso	24	3	15	1080
Servidores de bajo consumo	24	4	10	960
Pantallas LCD	2	4	20	160
Laptops	10	2	75	1500
Lámparas	8	4	15	480
Módem VSAT	24	1	60	1440
			Total:	**5620**

El consumo de energía para los servidores y las pantallas LCD está basado en Inveneo's Low Power Computing Station, *http://www.inveneo.org/?q=Computingstation*. El consumo de energía total estimado del NOC es de 5,6 kWh/día, que es menos que la energía diaria generada por los paneles solares en el mes peor.

Centro de Operaciones de Red (NOC, en inglés)

Un Centro de Operaciones de Red se estableció para albergar el sistema de energía de respaldo y las instalaciones del servidor. Se diseñó para proporcionar un lugar protegido del polvo, con buena capacidad de enfriamiento para las baterías y los inversores. El NOC utilizó métodos naturales y se construyó con materiales disponibles localmente. El edificio consta de cuatro habitaciones: un cuarto para las baterías, el cuarto del servidor, un lugar de trabajo y un cuarto para almacenamiento de equipo. El cuarto de las baterías alberga setenta baterías de ciclo profundo de 200 Ah, así como cinco inversores (uno de ellos de onda sinusoidal pura), dos reguladores solares, estabilizadores de energía y disyuntores para DC y AC. Las baterías están apiladas verticalmente en una estructura de repisas de metal para un mejor enfriamiento.

Figura 11.2: El NOC se construyó localmente con ladrillos de laterita producidos y colocados por jóvenes de Kafanchan.

El espacio del servidor tiene un estante para servidores y un ventilador. El cuarto no tiene ventanas regulares para evitar el polvo y el recalentamiento. Tanto el cuarto del servidor como el de las baterías están orientados hacia el sur para mejorar el enfriamiento natural y mantener así la temperatura adecuada.

El cuarto del servidor y el espacio de las baterías requieren enfriamiento efectivo de bajo costo/bajo consumo ya que necesitan operar 24 x 7. Para lograr este objetivo se introdujeron técnicas de enfriamiento natural en el diseño del NOC: pequeños ventiladores y extractores y paredes gruesas de ladrillos (doble ancho) hacia la dirección de poniente.

El lado sur del edificio alberga 24 paneles solares en un área sin sombras en su techo de metal. El techo fue diseñado con una inclinación de 20 grados para colocar los paneles y limitar la corrosión y el polvo. Se hicieron esfuerzos para mantener los paneles accesibles para su limpieza y mantenimiento. También se reforzó el techo para soportar el peso extra de 150-200 kg. El edificio del NOC se construyó con ladrillos de barro de laterita producidos localmente. El material es barato ya que es de uso común y proviene de la capa superficial del suelo. Los ladrillos se producen localmente a mano usando técnicas de compresión de baja tecnología. EL NOC es único en su especie en el Estado de Kaduna.

Figura 11.3: Omolayo Samuel, una de las empleadas de Zittnet, no muestra miedo a la altura en la torre de 45 m cuando alinea las antenas colocadas en el tope de la torre.

Estructura física. Un mástil de comunicación

La mayor parte de los clientes potenciales de Zittnet están ubicados entre 1 km y 10 km de las instalaciones de Fantsuam. Para servir a estos clientes, en octubre 2006 Fantsuam erigió un mástil auto-soportado de 45 m en sus instalaciones, equipado con conexión a tierra y pararrayos, así como con la obligatoria luz de señalización. Un anillo metálico se enterró en la base de la torre a una profundidad de 1,20 m. Las tres patas del mástil se conectaron al circuito de tierra y se colocó un pararrayos en lo más alto del mástil para su protección. El pararrayos se hizo de cobre puro y se conectó al anillo de tierra en la base del mástil usando cinta de cobre.

La luz de señalización en la punta del mástil es una exigencia de las Autoridades de Aeronáutica Civil. La luz se dotó de una fotocélula que le permite

un encendido automático basado en el nivel de luz ambiental. De esta manera la luz se enciende de noche y se apaga durante el día.

Infraestructura inalámbrica del backbone

La infraestructura inalámbrica del backbone se construyó usando puntos de acceso multi-banda SmartBridges y unidades cliente de la serie Nexus PRO™ TOTAL. Las unidades fueron diseñadas para que las empresas y los ISP establezcan enlaces punto-a-punto inalámbricos para exteriores, de alto rendimiento. Las unidades vienen con una antena sectorial multi-banda integrada que puede funcionar a las frecuencias de 2,4 GHz y 5,1 – 5,8 GHz. La serie Nexus PRO™ TOTAL ofrece QoS para priorización de tráfico y manejo de ancho de banda por cliente usando las extensiones WMM WiFi Multimedia del IEEE802.11e.

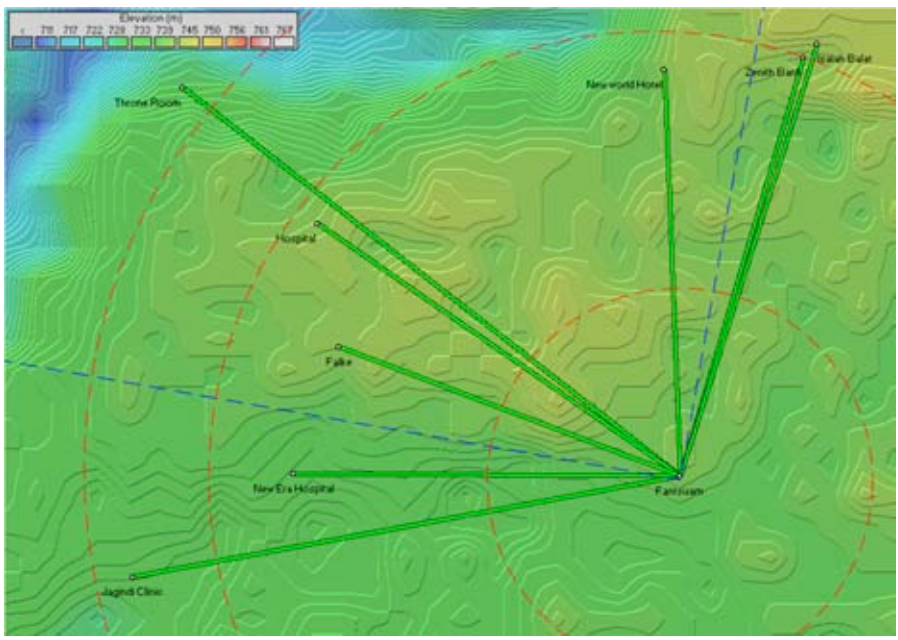


Figura 11.4: Topología de la red Zittnet en Octubre de 2007.

Actualmente, la topología de la red es una estrella con dos puntos de acceso en el mástil de comunicación en las instalaciones de Fantsuam. Un punto de acceso tiene una antena sectorial de 90 grados y el otro provee cobertura omnidireccional a los alrededores. Los clientes que están situados dentro del área de las líneas de punto están conectados a la antena sectorial, mientras que los clientes restantes están conectados a la antena omnidireccional.

Hay planes en proceso para expandir el backbone inalámbrico con la instalación de dos repetidores inalámbricos. Un repetidor se va a colocar en Kafanchan, usando una torre de NITEL existente para reforzar la cobertura inalámbrica en el centro de la ciudad. EL segundo repetidor va a estar en las

Kagoro Hills, un pequeño grupo de montañas, con una altura respecto a Kafanchan de unos 500 m, y situada a unos 7 km de ella. Este repetidor va a dar cobertura a muchas ciudades aledañas e incluso puede habilitar un enlace de larga distancia a Abuja.

Zittnet conectó su primer cliente a comienzos de Agosto, 2007. Dos meses después, no menos de ocho clientes están conectados a Zittnet. Estos clientes incluyen:

- El hospital general
- El Hospital Nueva Era
- La Clínica Jagindi Street (clínica de salud)
- El Banco Zenith (de uso privado)
- Isaiah Balat (cibercafé)
- Hotel New World
- Guest House Throne Room
- Fulke

Problemas encontrados

Algunas áreas problemáticas presentes a lo largo del proyecto fueron las siguientes:

Edificios bajos

La mayoría de las instalaciones de los clientes son edificios de un solo piso con una altura de no más de 3 metros. Muchas casas tienen estructuras de techo muy débiles, lo que hace imposible el montaje de equipo en el techo, ya que el acceso físico no es posible. Los edificios bajos nos obligan a montar el equipo a una altura bastante baja, porque los clientes no pueden darse el lujo de invertir en pequeños (10 m) mástiles para albergar el equipo. La mayoría de las instalaciones hacen uso de tanques de agua, o un simple tubo de metal de 3 metros fijado a la pared de la instalación.

Cuando el equipo está montado bajo, no se despeja la primera zona de Fresnel y el caudal de datos baja. Aunque el paisaje es muy plano en Kafanchan, la vegetación de espesos árboles de mango a menudo bloquea la línea de vista.

Rayos

Las tormentas eléctricas fuertes son frecuentes durante la estación lluviosa en Kafanchan. En septiembre de 2007, un rayo cercano dañó el equipo montado en un mástil, así como su fuente de alimentación. Por el momento, el punto de acceso y su Inyector PoE se conectan a tierra en la torre en sí. Hay que investigar otros medios para evitar daños a los equipos causados por rayos cercanos. El equipo de Zittnet está trabajando actualmente en la mejora de la protección antirrayos, añadiendo desviadores de rayos coaxiales extra. Por otra

parte, la pantalla del cable Ethernet que conecta el punto de acceso al NOC se va a conectar a tierra usando bloques y sujetadores de puesta a tierra.

Equipamiento de baja calidad

Desafortunadamente, la falta de equipamiento de calidad en el mercado es un problema muy extendido en todo el continente africano. Como la mayoría de los países subsaharianos carecen de políticas que aseguren la calidad de los productos de importación, el mercado está inundado de artículos "baratos" de muy baja calidad. Puesto que los de buena calidad son difíciles de encontrar, uno se encuentra a menudo en la situación de tener que comprar mercancía local que se daña aún antes de ponerla a funcionar. Como no existe garantía que cubra estos artículos, el proceso termina siendo muy caro. Este problema existe para la mayoría de los accesorios comunes como tomacorrientes, barras de conexión eléctrica, conectores RJ45, cables CAT5, y otro equipamiento de baja tecnología.

Modelo comercial

La única alternativa para acceso a Internet en Kafanchan es vía satélite. Durante el 2006, Fantsuam tenía una suscripción de 128/64 kbps para banda ancha dedicada por un costo de US$ 1.800 al mes. Este costo mensual para conectividad ha sido un gran peso para Fantsuam y una fuente constante de estrés de no ser capaz de pagar el recibo mensual.

Como alternativa a este modelo de "tarifa plana", Fantsuam implementó un sistema llamado ***HookMeUp*** (Conéctame) proporcionado por Koochi Communications. El sistema ofrece unos costos flexibles de *Pay-As-You-Go* para conexiones a Internet VSAT banda ancha, en países a lo largo del África subsahariana. Este tipo de modelo es el que se encuentra típicamente en los aeropuertos, hoteles o grandes centros comerciales de los países occidentales, donde el usuario final compra un cupón en línea y se autentifica usando un código de acceso.

El sistema ***HookMeUp*** ofrece una conexión VSAT dedicada a Fantsuam (desde su estación base en el reino unido). Fantsuam le compra cupones a Koochi Communications y los revende a los clientes locales de Kafanchan. De esta manera, Fantsuam no tiene el compromiso de pagar un costo mensual fijo, sino que le paga a Koochi solamente el ancho de banda consumido. El riesgo de comprar banda ancha internacional cara ha sido traspasado al proveedor de Internet en vez de al usuario, al precio de costos más elevados para este último.

La Fundación Fantsuam ahora actúa de revendedora de los cupones de Koochi y de proveedora de la infraestructura inalámbrica a los usuarios finales. La Red Comunitaria Inalámbrica ahora le da a la Fundación cinco fuentes de ingreso:

1. Instalación del equipamiento del cliente (una vez por cliente)
2. Alquiler de equipamiento inalámbrico (costo mensual por cliente)
3. Re-venta de equipamiento inalámbrico (una vez por cliente)
4. Instalación de hotspots inalámbricos en las instalaciones del cliente (una vez por cliente)
5. Reventa de cupones (continuamente)

El sistema de cupones se basa en tres parámetros: tiempo de acceso, límite de datos y tiempo de validez. Cualquiera de los parámetros que se agote primero va a consumir el cupón.

Tiempo de acceso	Límite de datos (MB)	Tiempo de validez	Precio (USD)	USD / h	USD / 700 MB
30 min	5	1 día	0,80	1,60	112,0
60 min	10	5 días	1,28	1,28	89,60
12 horas	60	14 días	10,40	0,87	121,33
24 horas	150	30 días	26,00	1,08	121,33
1 mes	500	1 mes	71,50	0,10	100,10
3 meses	1600	3 meses	208,00	0,10	91,00
6 meses	3500	6 meses	416,00	0,10	82,20
12 meses	7500	12 meses	728,00	0,08	67,95

La gran ventaja de este sistema es que la Fundación Fantsuam ya no va a tener el peso de pagar un gran recibo mensual por el ancho de banda internacional. El modelo de tarifa plana significa que usted se ve forzado a vender una cierta cantidad de ancho de banda mensualmente. Con el modelo *Pay-As-You-Go* (*PAYG*), la ganancia de Fantsuam al vender los cupones depende de cuánto ancho de banda consumen los clientes. El cliente paga por adelantado (modelo pre-pago) con el resultado de que Fantsuam no va a terminar debiéndole grandes cantidades al proveedor.

El modelo pre-pago funciona bien en África puesto que la gente ya lo conoce por la experiencia con los operadores de telefonía móvil. Incluso lo usan algunas compañías de electricidad en ciertas comarcas. Este modelo es además muy apreciado por la mayoría ya que les ayuda a llevar cuenta de sus gastos. Una de las principales limitaciones del modelo PAYG es la falta de flexibilidad y transparencia. EL modelo PAYG actual proporciona poca retroalimentación al usuario sobre el volumen o el tiempo consumidos. Sólo cuando el/la usuario/a cierra la sesión se le informa sobre cuántos minutos le quedan por consumir.

Sin embargo, el modelo comercial parece ajustarse bastante bien a la realidad local de Kafanchan y de muchas comunidades rurales en África. A pesar de que todavía puede haber mejoras, la ventaja de evitar las deudas es más grande que las desventajas. Con el tiempo, cuando crezca el número de clientes

y estos puedan apoyarse en una ganancia mensual sustanciosa por la red inalámbrica, podría ser ventajoso volver de nuevo al modelo de tarifa plana.

Clientes

Los clientes pueden usar el acceso a Internet con cualquier propósito. Por ejemplo, Isaiah Balat revende cupones (comprados a Fantsuam) a sus clientes. Su cibercafé tiene 10 computadoras conectadas a Zittnet. Los clientes del café le compran los cupones al dueño con un margen de 25% sobre el precio ofrecido por Fantsuam. En cambio, los clientes que no tienen acceso a un computador conectado a Zittnet, pueden tener acceso a la red a través de las computadoras del café Isaiah Balat.

El Hotel New World es otro cliente que busca crear un modelo comercial semejante pero a gran escala. Ellos proporcionan acceso a Internet a todas las habitaciones y ofrecen acceso al enlace de conexión de Zittnet por medio de la venta de cupones. Otros clientes, como el Hospital General, y la Jagindi Street Clinic hacen uso privado del acceso a Internet sin reventa de cupones a sus clientes.

–Louise Berthilson

Red mallada inalámbrica de la comunidad de Dharamsala

La Red mallada inalámbrica de la comunidad de Dharamsala vio la luz en febrero de 2005, después de la desregulación de WiFi para el uso en exteriores en la India. Para fines de febrero de 2005, la red había ya conectado 8 campus.

Varias jornadas de pruebas durante febrero de 2005 habían demostrado que para esta dura región montañosa, lo más apropiado era una red mallada, ya que las redes convencionales punto a multipunto no podían superar las limitaciones de línea de vista que presentaban las montañas. La topología en malla, además, ofrecía un área de cobertura mucho más amplia, y las características de "auto-reparación" del enrutamiento en malla demostraron ser esenciales en regiones donde el suministro de energía eléctrica es, cuando mucho, errática.

El backbone en malla incluye 30 nodos que comparten un único canal de radio. Los servicios de Internet de banda ancha se proporcionan a todos los miembros de la malla. El ancho de banda total de subida hacia Internet disponible es de 6 Mbps. Hay unas 2.000 computadoras conectados a la malla. La conexión a Internet de banda ancha carga fuertemente a la malla. En el presente, el sistema parece manejar la carga sin un incremento de la latencia o pérdida de paquetes. Queda claro que la escalabilidad va a ser un problema si se continúa usando un sólo canal de radio. Para resolver este problema, se están desarrollando y probando en Dharamsala nuevos enrutadores en malla que utilizan múltiples canales de radio, enfocándonos en productos que satisfagan nuestras exigencias técnicas y que sean económicamente viables.

La red mallada se basa en despliegues recurrentes de un dispositivo de hardware diseñado y fabricado localmente—conocido como el ***Himalayan-***

Mesh-Router (*http://drupal.airjaldi.com/node/9*). Los mismos enrutadores en malla se instalaron en cada sitio, sólo que con diferentes antenas, dependiendo de la ubicación y necesidades geográficas. Usamos una variedad de antenas, desde omnidireccionales de 8 – 11 dBi, hasta direccionales de 12 – 24 dBi, y ocasionalmente, algunas antenas sectoriales de alta ganancia (y costo).

La red mallada se usa principalmente para:

- Acceso interno
- Aplicaciones de archivos compartidos
- Respaldos remotos
- Reproducción de videos de alta calidad desde archivos remotos.

Se instaló una PBX central basada en Asterisk que proporciona servicios de telefonía avanzada a los miembros, conectada a la red telefónica pública. Sin embargo, debido a problemas legales, actualmente sólo se usa para llamadas entrantes a la malla.

Los subscriptores utilizan una gran variedad de *software-phones*, así como numerosos ATA (Adaptadores de Teléfonos Analógicos), y teléfonos IP independientes.

Figura 11.5: Instalador trabajando en una torre en Dharamsala

El backbone en malla encriptado no permite el acceso a dispositivos de móviles (notebooks y PDA), así que colocamos múltiples puntos de acceso 802.11b en muchas de las mismas ubicaciones donde se instalaron los enrutadores. La malla proporciona la infraestructura de backbone, mientras que los AP (*access points*) proporcionan acceso para los dispositivos de móviles cuando se necesite.

El acceso al backbone mallado es sólo posible a través de enrutadores en malla. Los clientes inalámbricos comunes carecen de la inteligencia que se necesita para “hablar” los protocolos de enrutamiento en malla y las estrictas políticas de acceso. El canal en malla, entonces, es encriptado (WPA) y “escondido” para impedir que los dispositivos móviles traten de encontrarlo o contactarlo. El conceder el acceso a la malla sólo a través de enrutadores en malla permite implementar políticas de control de acceso estrictas y limitaciones en el CPE (*Client Premises Equipment*), lo cual es un factor crucial para lograr

seguridad de extremo a extremo (*end-to-end*), conformación de tráfico (*traffic-shaping*) y calidad de servicio (*quality-of-service*).

El consumo de energía del enrutador en malla es de menos de 4 vatios. Esto los hace ideales para su uso con paneles solares. Muchos de los enrutadores en malla de Dharamsala funcionan solamente con pequeños paneles solares. El uso de energía solar, en combinación con pequeñas antenas y enrutadores de bajo consumo son ideales para áreas de desastre ya que tienen grandes probabilidades de sobrevivir cuando otras infraestructuras de comunicaciones se dañen.

–AirJaldi, http://airjaldi.com/

La red del estado Mérida

La ciudad de Mérida, que lleva el mismo nombre del estado, 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*)[1].

Figura 11.6: Mérida es uno de los tres estados montañosos de Venezuela, donde Los Andes llegan a 5.000 m.

No obstante, muchos lugares de la ciudad, sin mencionar los pueblos aledaños, quedan fuera del alcance del anillo de fibra óptica. La universidad

1. Para el año 2006, sobre el mismo cable de fibra óptica, se ha desplegado una red Gigabit Ethernet de 50 km y en la actualidad se utiliza MetroEthernet a 10 Gbps.

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 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.

Figura 11.7: En su ruta hacia el pico, el teleférico pasa por una estación intermedia llamada La Aguada, que está a 3.450 m de altura y ofrece una asombrosa vista a la ciudad de Mérida y otros poblados distantes unos 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 (T***erminal 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 pasarelas entre los radios VHF y HF conectando dos módems al mismo TNC y al mismo computador. Normalmente, una pasarela 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[2], 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, 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.

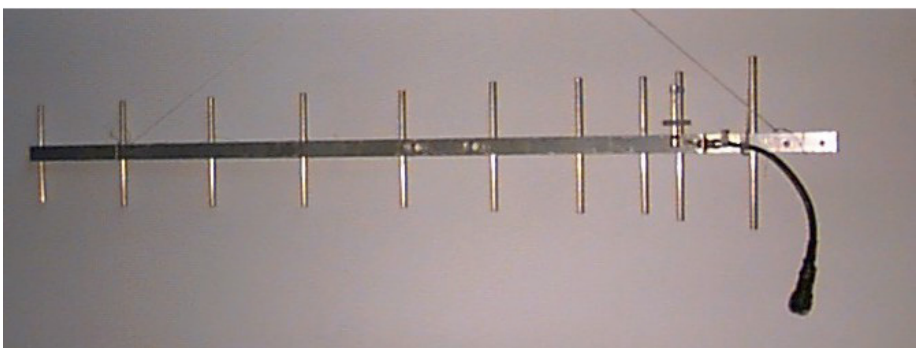


Figura 11.8: Antena UHF para packet radio desarrollada en el LabCom de la ULA.

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

2. Karn, Phil, "The KA9Q Internet (TCP/IP) Package: A Progress Report," Sixth ARRL Computer Networking Conference, Redondo Beach, CA, 29 August 1987.

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* inalámbrico para conectar poblaciones remotas.

Exploramos, entonces, el uso de los módems de 56 kbps desarrollados por Dale Heatherington[3] , 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

---

3. Heatherington, D., "A 56 kilobaud RF modem," Sixth ARRL Computer Networking Conference, Redondo Beach, CA, 29 August 1987.

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 algunas redes de prueba utilizando antenas externas construidas en el LabCom, lo que permitió una transmisión a varios kilómetros.

En 1993[4] 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 florecimiento 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

4. Conatel, Comision Nacional de Comunicaciones, Ministerio de Transporte y Comunicaciones, "Normas para la Operacion de Sistemas de Telecomunicaciones con Tecnología de Banda Esparcida (Spread Spectrum)," Caracas, 17 Noviembre1993.

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.[5]

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[6], 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:

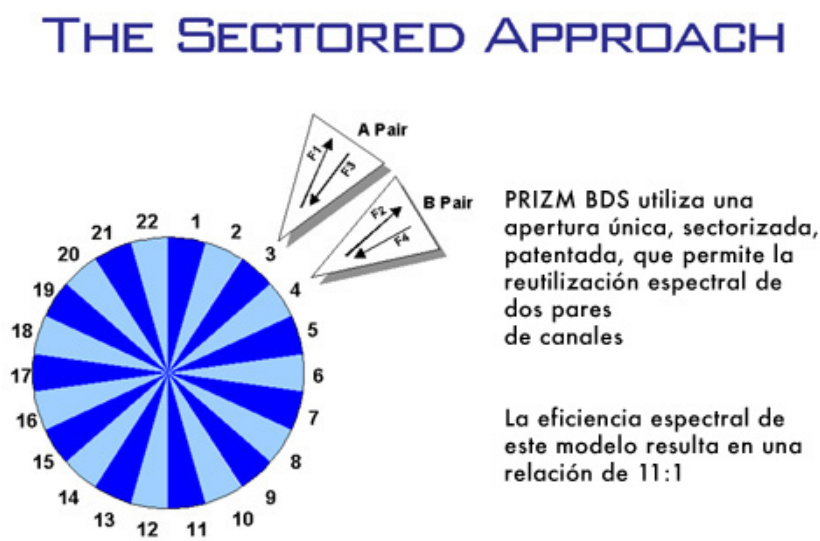


Figura 11.9: Sistema sectorial de alta densidad full duplex de Spike Technologies

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,

5. International Centre For Theoretical Physics, "Programme of Training and System Development on Networking and Radiocommunications," Trieste, Italy, 1996.

6. Spike Technologies, Inc. http://www.spike.com/

para un rendimiento agregado de 440 Mbps. El re-uso de frecuencias en los sectores no adyacentes permite una gran eficiencia espectral.

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.

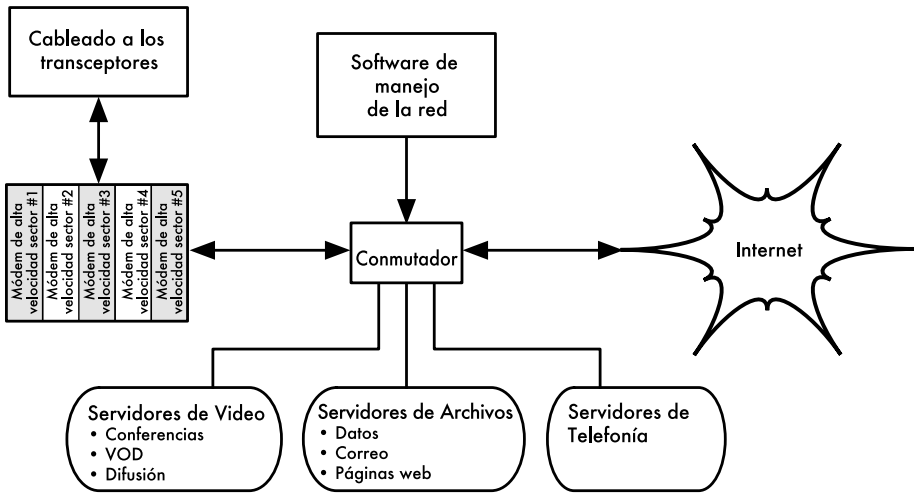


Figura 11.10: Interconexiones del sistema de Spike Technologies

En el sitio del suscriptor un radio similar y un módem proveen una conexión 10BaseT a la Ethernet local.

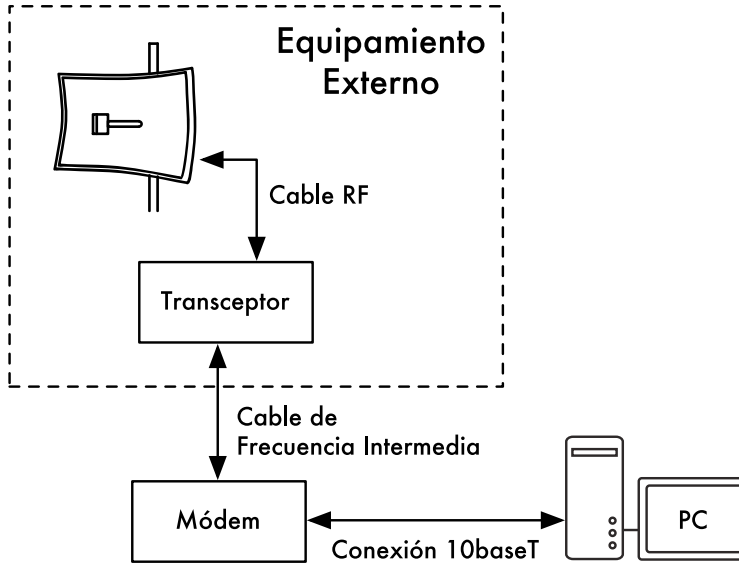


Figura 11.11: El lado del suscriptor en el enlace

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.

Figura 11.12 Instalación sobre Mérida, en La Aguada, a 3.600 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.

En enero de 1.998, una videoconferencia 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.

Figura 11.13. La red del estado Mérida

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.

La Figura 11.13 muestra un mapa del estado Mérida. Las líneas oscuras muestran el backbone inicial, y las líneas claras, la extensión.

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 Luís 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[7], 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. En el presente, EsLaRed continúa expandiendo sus esfuerzos de entrenamiento a lo largo de Latinoamérica.

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

7. Escuela Latinoamericana de Redes, http://www.eslared.org.ve/

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.

Referencias

- Karn, Phil, "*The KA9Q Internet (TCP/IP) Package: A Progress Report,*" Sixth ARRL Computer Networking Conference, Redondo Beach, CA, 29 August 1987.
- Heatherington, D., "*A 56 kilobaud RF modem,*" Sixth ARRL Computer Networking Conference, Redondo Beach, CA, 29 August 1987.
- Conatel, Comisión Nacional de Comunicaciones, Ministerio de Transporte y Comunicaciones, "*Normas para la Operación de Sistemas de Telecomunicaciones con Tecnología de Banda Esparcida (spread spectrum)*," Caracas, 17 November 1993.
- International Centre For Theoretical Physics, "*Programme of Training and System Development on Networking and Radiocommunications,*" Trieste, Italy, 1996, *http://www.ictp.trieste.it/*
- Escuela Latinoamericana de Redes, *http://www.eslared.org.ve/*

–Ermanno Pietrosemoli

Chilesincables.org

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 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.

Chilesincables.org busca promover y organizar redes inalámbricas libres en Chile de forma profesional; educar al respecto, tanto es sus aspectos técnicos como legales y apropiar nuevas tecnologías mediante la investigación, adaptándolas a las necesidades de la comunidad y la sociedad. 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*).

Descripción de la tecnología implementada

Actualmente se utiliza tecnología asociada con las especificaciones IEEE 802.11 en sus estándares a, b y g[8] 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 fabricantes 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 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:

- Transferencia de datos mediante servidores FTP o WEB.
- Servicios de VoIP.
- *Streaming* (flujo continuo) de audio y video.
- Mensajería instantánea.
- Investigar e implementar nuevos servicios como LDAP, resolución de nombres, seguridad, mejora de las prestaciones, etc.
- Adaptación de la red por parte de los clientes[9], esto significa que los usuarios pueden utilizar la infraestructura de la red para crear sus propios servicios.

---

8. Actualmente se está 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.

9. 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:

- Mantener un tiempo de operatividad adecuado (superior a un 90%)
- Mantener algunos servicios básicos (por lo general un servidor Web)
- 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:

- 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 radiocomunicaciones.
- Se debe utilizar materiales y métodos aprobados por la legislación vigente, de esa manera la actividad puede desarrollarse sin problemas.
- 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.
- 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:

- Talleres de antenas: donde se capacita en la construcción de antenas y se enseñan conceptos básicos de radio-comunicaciones.

- 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.
- 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.
- Se mantienen documentación actualizada y libremente accesible a quienes les interese la actividad.

Las siguientes fotografías son un resumen de algunas de las actividades que hemos realizado a lo largo de nuestra historia como comunidad:

Figura 11.14: Taller de antenas ranuradas omnidireccionales. En esta sesión se les enseñó a los asistentes cómo fabricar una antena y la teoría de su funcionamiento.

Figura 11.15: Uno de nuestros miembros dando una charla acerca de la implementación de un enrutador basado en m0n0wall en la administración de un nodo.

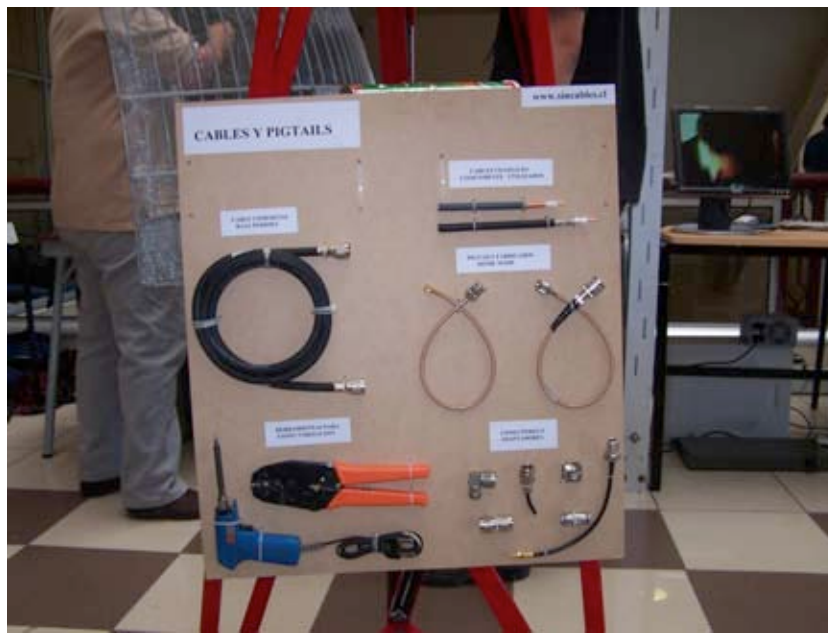


Figura 11.16: Detalle de mini torre con muestras de antenas, cables y pigtails.

Figura 11.17: Estación wireless con antena parabólica usada para la transmisión de la FLISOL de Santiago 2006 mediante flujo continuo de video (streaming) con software libre.

Figura 11.18: Ubicación del otro extremo del enlace.

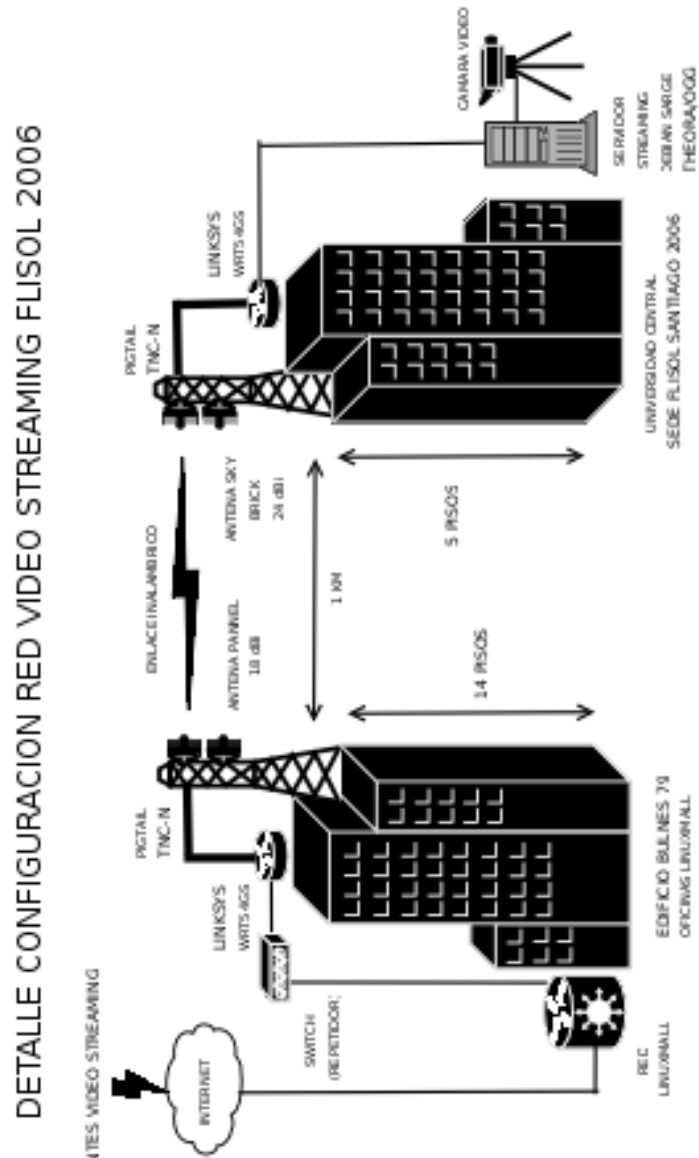


Figura 11.19: Esquema del proyecto de transmisión de la FLISOL de Santiago 2006 mediante flujo continuo de video (streaming) con software libre. La velocidad de transmisión inalámbrica obtenida fue de 36 Mbps a 1 km.

Figura 11.20: Nodo Quani. Este es uno de los nodos más altos del mundo. Ubicado a 4.000 m de altura, a unos 2.000 km al norte de la capital.

Figura 11.21: Nodo en el sur de Santiago. Consiste de una torre de 15 m, una antena Trevor Marshall 16 + 16 y 30 clientes. Está enlazado con un nodo en la zona centro a más de 12 km.

Figura 11.22: Vista panorámica de un nodo desde la cima de la torre.

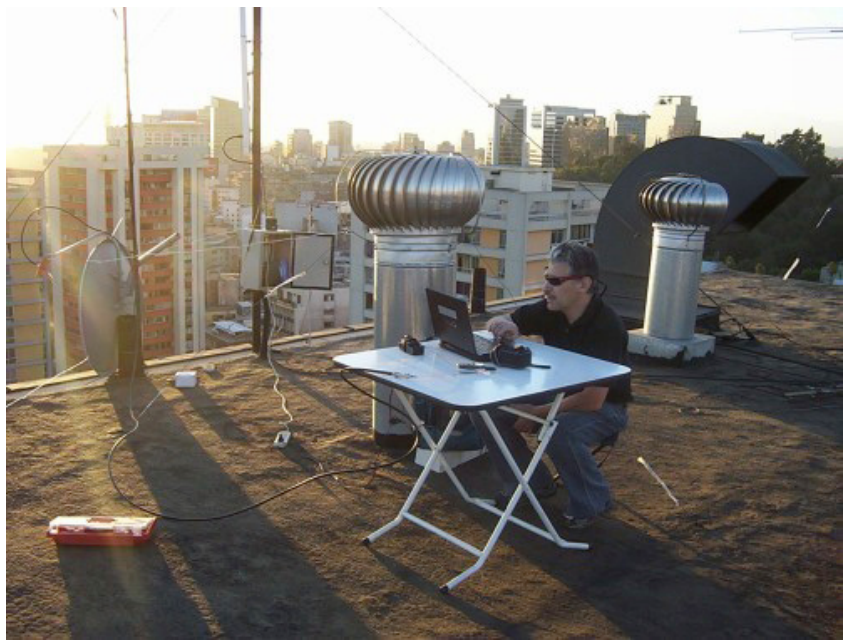


Figura 11.23: Nodo del centro conectado con el nodo del sur de Santiago. Se observa la antena parabólica que realiza el enlace y la antena ranurada para captar clientes.

Figura 11.24: Implementación de un nodo sobre una torre de agua en Batuco, Región Metropolitana que enlaza con el telecentro Cabrati.

Figura 11.25: Taller de antenas Yagi organizado por nuestra comunidad. Los participantes construyen sus propias 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), César Urquejo (Xeuron), Oscar Vásquez (Machine), José San Martín (Packet), Carlos Campano (Campano), Christian Vásquez (Crossfading), Andrés Peralta (Cantenario), Ariel Orellana (Ariel), Miguel Bizama (Picunche), Eric Azua (Mr. Floppy), David Paco (Dpaco), Marcelo Jara (Alaska).

–Chilesincables.org

Sistema de Información Agraria del Valle de Chancay-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 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 versus 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 versus 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.

Interconexión inalámbrica de 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:

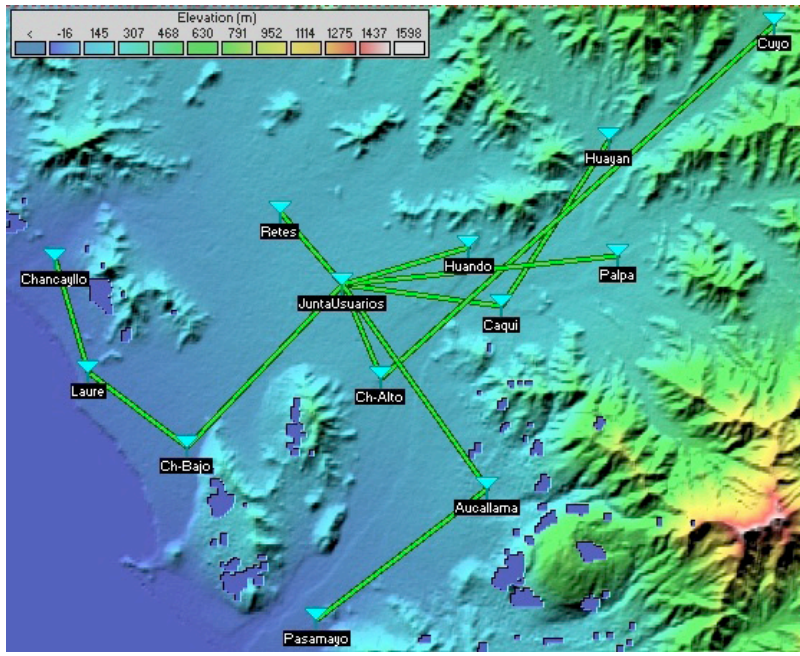


Figura 11.26: Mapa que indica los radioenlaces.

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 con el 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

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 ha 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 TIC y las utilizan dándoles 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 cibercafés en otras zonas rurales, con notable éxito y cubriendo un área más amplia del valle.

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

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 (6,5 Mbps 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 calificación 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 y 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 módems 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 rurales 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 de 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 con la mortalidad, así como la organización de los servicios de salud y su capacidad de respuesta en términos de resolución de problemas 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 sí 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 definen en gran medida 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 que operan en las bandas HF y VHF, ampliamente utilizadas para las comunicaciones de voz semidúplex, 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 manera 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.

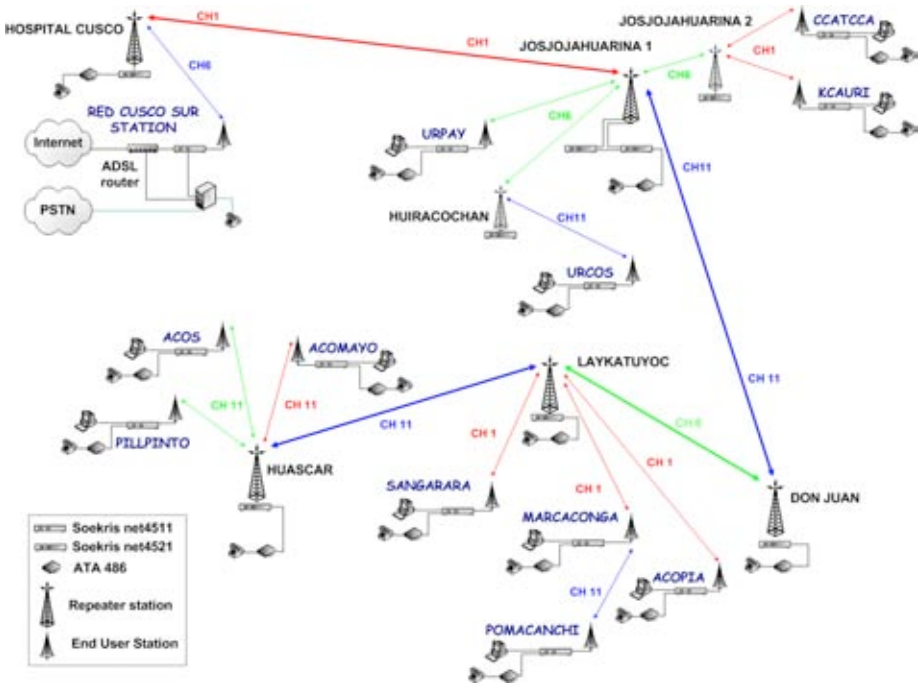


Figura 11.27: Esquema del diseño de la red Wi-Fi de Cusco

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 figura anterior 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, establecimiento de dispensarios en 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 contra-referidos 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: electrocardiógrafos 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 (desalineación 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. Estos cursos perseguían como objetivos específicos:

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 subsistemas 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 con el 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 de haber 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 computador 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 ha 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 computador 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 reflejan 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 diariamente, 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 como herramienta de trabajo y del acceso a Internet aún cuando la demanda de éste grupo es, de hecho, poco frecuente.

Repetidores

Figura 11.28: ***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.*

Figura 11.29: ***Josjojahuarina1****. De izquierda a derecha y arriba abajo: Antenas y paneles solares montados en torre ventada de 12 metros; equipos de telecomunicaciones y protección eléctrica en caja metálica; caja metálica de batería; paneles solares montados en la torre ventada.*

Estaciones cliente

Figura 11.30: ***Urcos****. De izquierda a derecha: Antena directiva de 24dBi montada en poste de 6 metros; estación de cómputo y equipo de telecomunicaciones en Urcos.*

Figura 11.31: ***Kcaury****. De izquierda a derecha: Antena directiva de 24dBi montada en brazo mecánico, estación de cómputo y caja de equipos de telecomunicaciones.*

*Figura 11.32: **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

Contacto: *info@ehas.org*
Sitio Web: *http://www.ehas.org*

WiFi para largas distancias

Gracias a una topografía favorable, Venezuela ya posee algunos enlaces WLAN de larga distancia, como el de 70 km operado por Fundacite Mérida entre Pico Espejo y Canaguá.

Para probar los límites de esta tecnología, es necesario encontrar un trayecto con línea de vista ininterrumpida y despeje de al menos el 60% de la primera zona de Fresnel.

Examinando el terreno en Venezuela en búsqueda de un recorrido con altas elevaciones en los extremos y tierras bajas en el ínterin, me enfoqué primero en la región de Guayana, en la que abundan las elevaciones, en particular los famosos “tepuys” (altas mesetas de paredes verticales), pero siempre había obstáculos en el terreno intermedio.

Mi atención se concentró entonces en los Andes, cuyas fuertes pendientes (que se alzan abruptamente desde los llanos) demostraron ser idóneas para el

propósito. Durante muchos años, he estado recorriendo las zonas escasamente pobladas gracias a mi pasión por la bicicleta de montaña, manteniéndome ojo avizor sobre la viabilidad de posibles enlaces de larga distancia.

El pico del Águila tiene condiciones muy favorables para establecer una estación. Tiene una altura de 4200 m y está a unas dos horas en automóvil de mi residencia en la ciudad de Mérida. Para el otro extremo, luego de examinar muchas posibilidades, finalmente escogí la población de El Baúl, en el estado Cojedes. Usando el software gratuito Radio Mobile (disponible en *www.cplus.org/rmw*) encontré que no había obstrucción de la primera zona de Fresnel en el tramo de 280 km entre Pico del Águila y el Baúl.

Plan de Acción

Una vez satisfechos con la existencia de una trayectoria adecuada, pasamos a escoger el equipo necesario para alcanzar nuestra meta. Hemos estado usando tarjetas Orinoco desde hace muchos años. Con una potencia de salida de 15 dBm y umbral de recepción de -84 dBm, son robustas y confiables. La pérdida en el espacio libre a 280 km es de 149 dB, por lo que necesitaríamos antenas de 30 dBi en ambos extremos y aún así el margen para compensar otras pérdidas sería muy reducido.

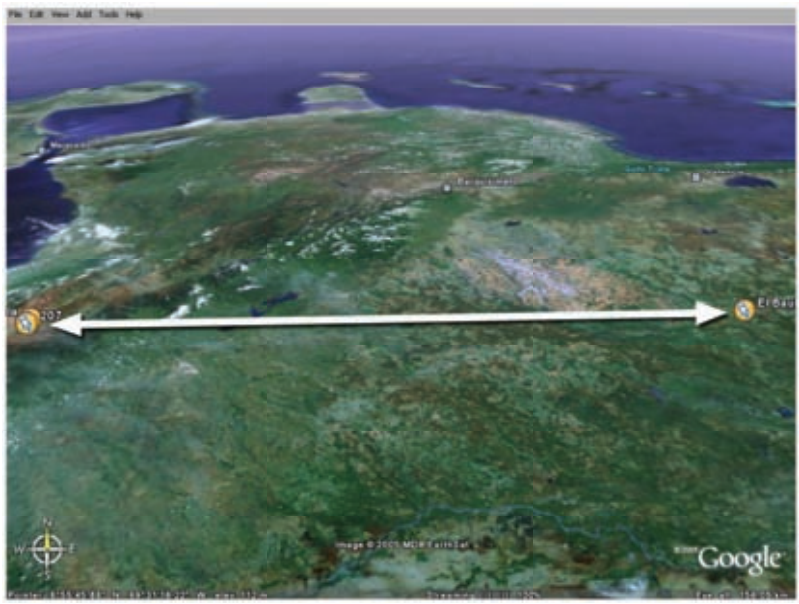


Figura 11.33: Vista del enlace de 280 km. El lago de Maracaibo al oeste y la península de Paraguaná al norte.

Por otra parte, el popular enrutador inalámbrico Linksys WRT54G está basado en Linux. La comunidad del software de fuente abierta ha producido varias versiones de *firmware* que permiten modificar todos los parámetros de transmisión de este dispositivo. En particular, el firmware OpenWRT permite

modificar el tiempo de espera de los reconocimientos (ACK) de la capa de acceso al medio, así como la potencia de transmisión. Otro *firmware*, DD-WRT, tiene una interfaz gráfica y ofrece facilidades para prospección de sitios. Además, el Linksys se puede colocar más cerca de la antena que un laptop, disminuyendo así las pérdidas en el cable de RF, así que decidimos usar una par de estos enrutadores, uno configurado como AP (*Access Point*) y el otro como cliente. El WRT54G puede ser operado a 100 mW con buena linealidad, e inclusive llevado a 200 mW, pero a este último valor se generan señales espurias que deben ser evitadas. Aunque este dispositivo es muy económico y no pretende ser un equipo profesional, lo hemos utilizado por varios años y confiamos que podía servir para nuestros propósitos. Por supuesto, teníamos un par de repuesto para cualquier eventualidad.

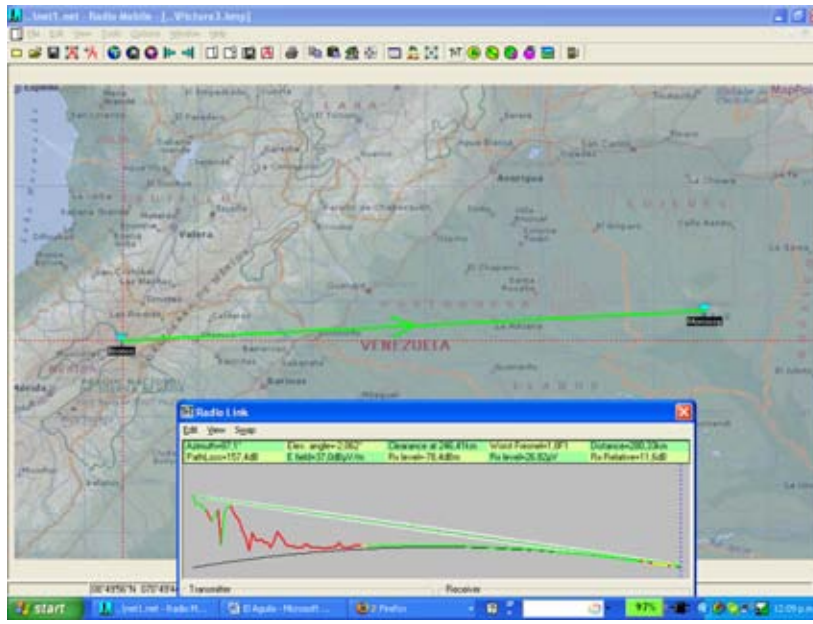


Figura 11.34: Mapa y perfil del trayecto entre Pico del Águila y el cerro Morrocoy, cerca de El Baúl.

Colocando la potencia de salida a100 mW (20dBm) podíamos obtener una ventaja de 5 dB comparado con las tarjetas Orinoco, por lo que nos decidimos por un par de WRT54G.

Prospección del sitio de Pico del Águila

El 15 de enero de 2006, visité el Pico del Águila para revisar el sitio que según el Radio Mobile era viable. El acimut hacia El Baúl es de 86°, pero puesto que la declinación magnética es de 8°16´, nuestra antena debería apuntarse a un rumbo magnético de 94°.

Desafortunadamente, cuando examiné esa dirección, me encontré con que la línea de vista estaba obstruida por un obstáculo que no había sido detectado

por el software, debido a la limitada resolución de los mapas digitales de elevación gratuitos que estaba utilizando.

Recorrí el área circundante durante varias horas en mi bicicleta de montaña, buscando una trayectoria sin obstrucción hacia el este. Logré identificar varios sitios prometedores y para cada uno de ellos tomé fotos y registré las coordenadas con el GPS para luego procesarlos con el software Radio Mobile. Esto me llevó a refinar mi selección de la trayectoria, resultando la que se muestra en la Figura 11.33 usando Google Earth.

Los detalles del enlace inalámbrico se muestran en la Figura 11.35.

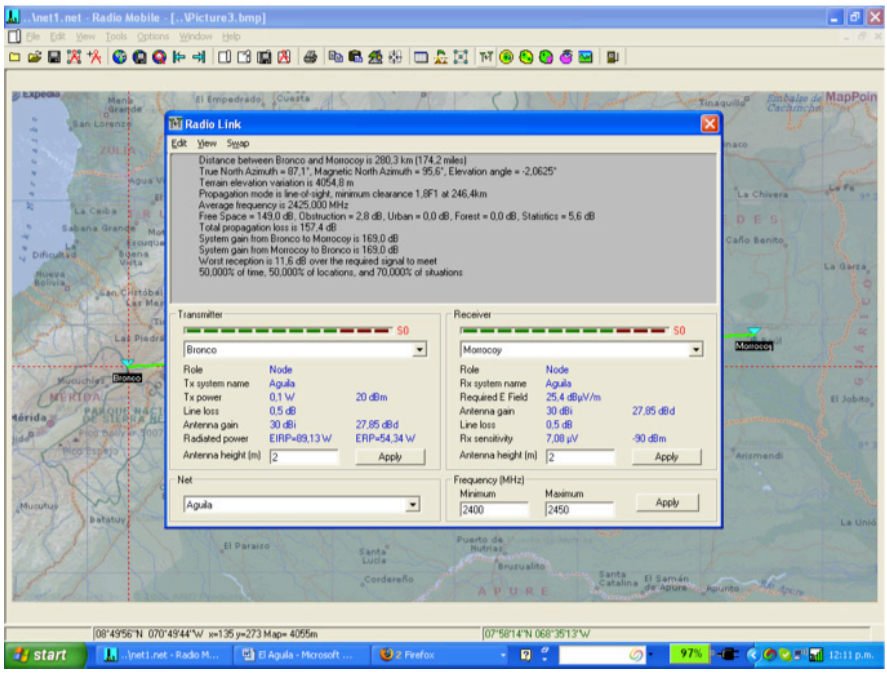


Figura 11.35: Detalles de propagación en el trayecto de 280 km.

A fin de obtener un margen razonable de unos 12 dB para el enlace, necesitamos antenas de al menos 30 dBi en cada extremo.

Antenas

En Venezuela no venden antenas de alta ganancia para la banda de 2,4 GHz. Los costos de importación son considerables, así que decidimos reciclar reflectores parabólicos (de los usados anteriormente para recepción satelital) reemplazándole el alimentador por uno de 2,4 GHz. Primeramente probamos la viabilidad con un reflector de 80 cm, la ganancia era demasiado baja, por lo que ensayamos con reflector de 2,4 m de diámetro con alimentación excéntrica. Este ofrecía amplia ganancia, a expensas de alguna dificultad en la alineación del haz de 3,5 °. La iluminación excéntrica desviada en 22,5° hacía que el reflector pareciera estar apuntando hacia abajo, cuando estaba alineado horizontalmente.

Se hicieron varias pruebas utilizando antenas de guía-onda (*cantenna*) y Yagi de 24 dBi como iluminadores del reflector parabólico. Apuntamos la antena a la estación base de la universidad, a una distancia de 11 km en una montaña de 3500 m de altura. El sitio de prueba está a 2000 m de altura por lo tanto el ángulo de elevación es de 8°. Debido a la iluminación excéntrica, apuntamos el reflector 14° hacia abajo, como se puede apreciar en la siguiente foto:

Figura 11.36: Reflector de 2,4 m con iluminación excéntrica y una antena de 12 dBi en su punto focal, mirando 14° hacia abajo. El ángulo real de elevación es de 8° hacia arriba.

Logramos conectar con la estación base de la universidad en La Aguada, pero los esfuerzos dirigidos a estimar la ganancia de la antena usando ***Netstumbler*** fueron vanos, ya que los niveles de potencia de la señal recibida correspondiente a tráfico normal fluctuaban considerablemente. Para poder realizar una medida razonable de la ganancia, se requiere un generador de señales y un analizador de espectros. Los mismos instrumentos son también necesarios en el trabajo de campo para alinear las antenas adecuadamente.

Mientras esperábamos la llegada de estos instrumentos, nos pusimos a buscar la antena a usar en el otro extremo, así como una mejor técnica para alinear las antenas de haz muy estrecho.

En febrero de 2006 viajé a Trieste para participar en el evento anual de entrenamiento en redes inalámbricas con el que he estado colaborando desde 1996. Allí le mencioné el proyecto a mi colega Carlo Fonda que enseguida se mostró entusiasta en participar.

La colaboración entre la **Escuela Latinoamericana de Redes (EsLaRed)** y el **Abdus Salam International Centre for Theorethical Physics (ICTP)** data

desde 1992 cuando la primera Escuela Latinoamericana de Redes se realizó en Mérida con el apoyo del ICTP. Desde entonces, los miembros de ambas instituciones han colaborado en numerosas actividades, incluyendo las Escuelas de Redes Inalámbricas organizadas anualmente por el ICTP y las de Redes de Computadoras organizadas por EsLaRed en diferentes países de Latinoamérica. En consecuencia, no fue difícil persuadir al Profesor Sandro Radiciella, jefe del *Aeronomy and Radio Propagation Laboratory* del ICTP que facilitara el viaje de Carlo Fonda en Abril a Venezuela para que participara en el experimento.

Figura 11.37: Carlo y Ermanno desarmando la antena satelital del Sr. Ismael Santos.

De vuelta a casa, conseguí un reflector parabólico de malla con iluminación central en casa de un vecino. Su dueño, el Señor Ismael Santos, amablemente nos prestó la antena para realizar los experimentos.

La **Figura 11.37** muestra el desmantelado del reflector de malla.

Cambiamos el iluminador por uno para 2,4 GHz y apuntamos la antena al generador de señales colocado a unos 30 m. Con el analizador de espectros buscamos el máximo de la señal para establecer la posición óptima para el iluminador. Asimismo establecimos la referencia de alineación tanto para la antena con iluminador excéntrico como para la de foco central, como se muestra en la Figura 11.31.

Figura 11.38: Hallando el foco de la antena con el iluminador de 2,4 GHz

También comparamos la potencia de la señal recibida con la de la salida de una antena comercial de 24 dBi apuntada a la misma fuente, mostrando una diferencia de 8 dB, lo que nos permite concluir que la ganancia total de nuestra antena es de unos 32 dBi. Por supuesto que este valor no es muy preciso, pues recibimos también señales reflejadas, pero el valor se corresponde a los cálculos realizados a partir de las dimensiones de la antena.

Prospección del sitio de El Baúl

Una vez satisfechos con el funcionamiento adecuado y la manera de apuntar ambas antenas, decidimos realizar una visita al otro extremo del enlace previsto. Carlo Fonda, Gaya Fior y Ermanno Pietrosemoli llegamos al sitio el 8 de abril. Al día siguiente encontramos una colina al sur del poblado de El Baúl con dos torres de telecomunicaciones pertenecientes a dos operadores de telefonía celular y una tercera perteneciente a la Alcaldía. Esta colina, llamada Morrocoy, está a 125 m sobre el nivel del mar y unos 75 m sobre el terreno circundante, ofreciendo una ruta sin obstrucción hacia el Pico del Águila. Hay una carretera de tierra, imprescindible para nuestros propósitos, dado el peso de la antena.

Realización del experimento

El 12 de abril Javier Triviño y Ermanno Pietrosemoli nos desplazamos hacia El Baúl con la antena de iluminación excéntrica cargada en el techo de nuestro vehículo. Temprano en la mañana del 13 instalamos la antena directamente sobre el borde del terreno en la colina de Morrocoy y la apuntamos al rumbo

magnético de 276° ya que la declinación magnética es de 8° y por lo tanto el acimut verdadero es de 268°.

Al mismo tiempo, el otro equipo compuesto por Carlo Fonda y Gaya Fior del ICTP, con la ayuda de Franco Bellarosa, Lourdes Pietrosemoli y José Triviño, trasladaron la antena mallada de 2,7 m al sitio del Pico del Águila previamente identificado.

Figura 11.39: Vista aérea de la zona del Pico del Águila con foto del vehículo.

El mal tiempo es común a 4100 m de altura, el equipo de el Águila pudo instalar y apuntar la antena justo antes de que cayera la neblina y el nevisco. La figura 11.40 muestra la antena con el cordel utilizado para apuntar el haz de radio de 3°.

Figura 11.40: Apuntando la antena en El Águila.

El generador de señales se alimentó desde el vehículo mediante un inversor de 12 V DC a 120 V AC. A las once de la mañana el analizador de espectros en el Baúl detectó un tono de -82 dBm a la frecuencia previamente acordada de 2450 MHz. Para asegurarnos de que se trataba realmente de la señal generada en el Águila, le pedí a Carlo que apagara el generador, y la traza del analizador de espectro mostró sólo ruido, confirmando que realmente la señal observada previamente se originaba a unos 280 km de distancia.

Figura 11.41: Instalación de la antena en El Baúl. La antena está apuntando 1° hacia arriba debido a la iluminación desviada en 22,5°.

Luego de volver a encender el generador de señales, realizamos un ajuste fino de elevación y de acimut en ambos extremos. Cuando nos convencimos de haber obtenido la mejor señal posible, Carlo sustituyó el generador de señales por un Linksys WRT54G configurado como un AP, mientras Javier sustituía el analizador de espectros en nuestro extremo por otro Linksys WRT54G configurado como cliente.

Enseguida empezamos a recibir "*beacons*" pero los paquetes ping no hallaban respuesta.

Esto era de esperarse, puesto que el tiempo de propagación de la onda de radio sobre un trayecto de 300 km es de 1 ms, por lo que el reconocimiento (ACK) a la transmisión de un paquete tarda al menos 2 ms para llegar al transmisor. Afortunadamente, el firmware OpenWRT permite que se ajuste el tiempo de espera por los ACK. Luego de que Carlo realizó el ajuste para compensar el aumento en tres órdenes de magnitud en el tiempo de propagación respecto a los valores estándar de una conexión WiFi, empezamos a recibir paquetes con retardos totales de unos 5 ms.

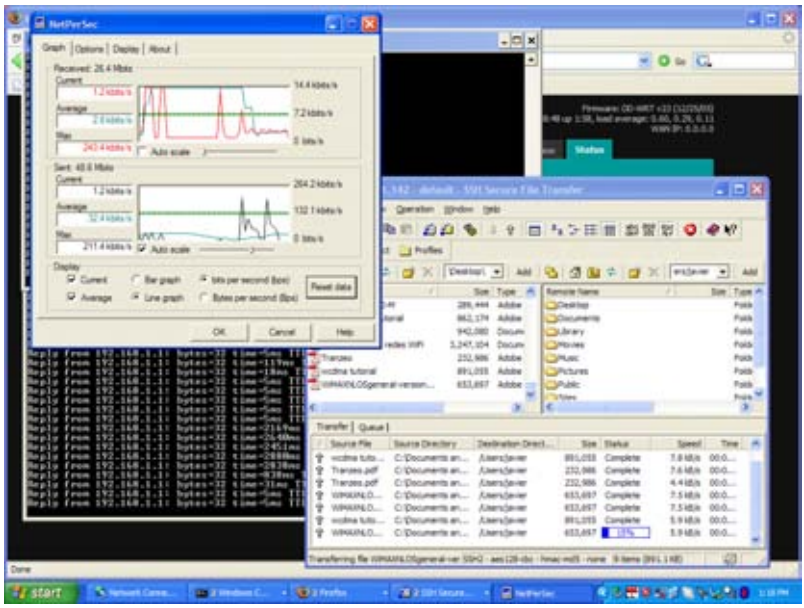


Figura 11.42: Pantalla del computador de Javier mostrando detalles de la transferencia de archivos desde el computador de Carlo a 280 km de distancia, usando dos enrutadores inalámbricos WRT54G, sin amplificadores.

Procedimos entonces a transferir varios archivos .PDF entre las computadoras de Carlo y de Javier. Los resultados se muestran en la Figura 11.42. Nótese que el tiempo de respuesta al ping es de unos pocos milisegundos.

Figura 11.43: Javier Triviño (derecha) y Ermanno Pietrosemoli con la antena en El Baúl.

Figura 11.44: Carlo Fonda en el Águila

Mérida, Venezuela, 17 de abril de 2006

Un año después de haber realizado el experimento descrito, encontramos el tiempo y los recursos para repetirlo, usando antenas comerciales de 30 dBi y un par de enrutadores inalámbricos modificados por el grupo TIER (*Telecommunication Infrastructure for Emerging Regions*) dirigido por el Dr. Eric Brewer de la universidad de Berkeley.

El propósito de la modificación de la capa de acceso al medio estándar de WiFi es hacerla más adecuada para la aplicaciones a grandes distancias reemplazando CSMA (*Carrier Sense Multiple Access*) por TDMA (*Time Division Multiple Access*). Este último es más adecuado para enlaces punto a punto de larga distancia puesto que no requiere el uso de reconocimiento de recepción (ACK). Esto elimina la necesidad de esperar los 2 ms de tiempo de propagación ida y vuelta en un trayecto de 300 km.

El 28 de Abril de 2007, un equipo formado por Javier Triviño, José Torres y Francisco Torres instaló una de las antenas en el sitio de El Águila. El otro equipo, compuesto por Leonardo González V., Leonardo González G., Alejandro González y Ermanno Pietrosemoli, instaló la otra antena en El Baúl.

Enseguida se logró establecer un enlace mediante los Linksys WRT54G que permitió transmitir video, con un caudal medido de 65 kbps. Cuando reemplazamos los Linksys por los enrutadores inalámbricos que implementan TDMA, el caudal medido subió a 3 Mbps en cada dirección de tráfico, para un total bidireccional de 6 Mbps, concordando con las simulaciones realizadas en Berkeley.

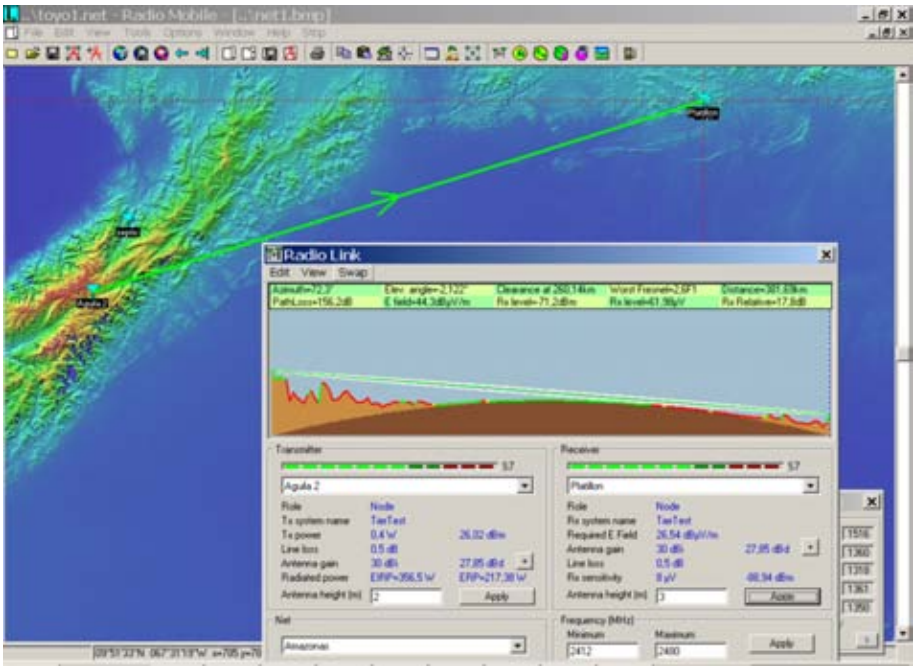


Figura 11.45: Mapa y perfil del trayecto de 380 km.

¿Podemos ir más lejos?

Entusiasmados por estos resultados, que permiten avizorar la factibilidad de enlaces de larga distancia a muy bajo costo, el segundo equipo se desplazó hacia otro sitio previamente identificado a 382 km de El Águila, un lugar llamado Platillón, a 1550 m sobre el nivel del mar, que según la simulación realizada con Radio Mobile, permite despejar la primera zona de Fresnel, tal como se puede apreciar en la **Figura 11.45**.

De nuevo, se logró rápidamente el enlace tanto con los Linksys como con los enrutadores suministrados por TIER. Los Linksys arrojaron alrededor de 1% de pérdida de paquetes, con un tiempo de propagación ida y vuelta de aproximadamente 12 ms. Los enrutadores TIER no registraron pérdidas de paquetes, con tiempos de propagación de 1 ms, lo que permitió transmisión de video, pero el enlace era inestable, notándose significativas variaciones en la intensidad de la señal recibida que a menudo interrumpían la comunicación.

Si embargo, cuando la señal recibida alcanzaba los -78 dBm, el caudal medido fue de 6 Mbps bidireccionales con los enrutadores de TIER que implementan TDMA.

Figura 11.46: El equipo de El Águila, José Torres (izquierda) Javier Triviño (centro) y Francisco Torres (derecha).

Aunque se requiere realizar otras pruebas para determinar los límites de una tasa de transmisión estable, estamos convencidos de que WiFi tiene un gran potencial para comunicaciones de banda ancha a grandes distancias. Es particularmente adecuado para zonas rurales, donde el espectro no está todavía congestionado y la interferencia no representa un problema, siempre que exista línea de vista despejada.

Reconocimientos

Deseamos expresar nuestra gratitud al Sr. Ismael Santos por prestarnos el reflector mallado utilizado en el Águila y al Ing. Andrés Pietrosemoli por suministrar las uniones para andamios utilizadas para el transporte e instalación de las antenas. También agradecemos al Abdus Salam International Centre of Theorethical Physics por facilitar el viaje de Carlo Fonda de Italia a Venezuela.

Figura 11.47 El equipo de El Platillón, de izquierda a derecha, Leonardo González V, Leonardo González G., Ermanno Pietrosemoli y Alejandro González.

El experimento de 2006 fue realizado por Ermanno Pietrosemoli y Javier Triviño de EsLaRed, Carlo Fonda y Gaya Fior de ICTP, con la ayuda de Franco Bellarosa, Lourdes Pietrosemoli y José Triviño.

Para el experimento de 2007, el Dr. Eric Brewer de la Universidad de Berkeley suministró los enrutadores inalámbricos con la MAC modificada para largas distancias, así como soporte a través de su colaborador Sonesh Surana. Se agradece también las colaboraciones de RedULa, CPTM (Corporación Parque Tecnológico de Mérida), Dirección de Servicios de la ULA (Universidad de los Andes) y Fundacite Mérida

Referencias

- Fundación Escuela Latinoamericana de Redes (EsLaRed) *http://www.EsLaRed.org.ve*
- Abdus Salam Interntional Centre for Theorethical Physics *http://wireless.ictp.it*
- Firmware libre Open WRT para Linksys *http://Open WRT.org*
- Fundacite Mérida *http://www.funmrd.gov.ve*

–Ermanno Pietrosemoli

Apéndices

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/* y el exhaustivo *http://wireless**U**.org*

Para materiales en español visite *http://www.eslared.org.ve*

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 Technologies, *http://hyperlinktech.com/*
- Pasadena Networks LLC,livepage.apple.com *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

- Bing throughput measurement tool, *http://fgouget.free.fr/bing/index-en.shtml*
- Cacti network monitoring package, *http://www.cacti.net/*
- DSL Reports bandwidth speed tests, *http://www.dslreports.com/stest*

- EaKiu spectrum analysis tool, *http://www.cookwareinc.com/EaKiu/*
- EtherApe network traffic monitor, *http://etherape.sourceforge.net/*
- Flowc open source NetFlow collector, *http://netacad.kiev.ua/flowc/*
- 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/*
- NetFlow, the Cisco protocol for collecting IP traffic information, *http://en.wikipedia.org/wiki/Netflow*
- ngrep network security utility for finding patterns in data flows, *http://ngrep.sourceforge.net/*
- Network monitoring implementation guides and tutorials, http://wiki.debian.org/Network_Monitoring
- 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://tldp.org/HOWTO/TransparentProxy.html*
- ttcp network performance testing tool, *http://ftp.arl.mil/ftp/pub/ttcp/*
- Wireshark network protocol analyzer, *http://www.wireshark.org/*

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/*
- Linux security and admin software, *http://www.linux.org/apps/all/Networking/Security_/_Admin.html*
- 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*
- 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/*
- Linux Advanced Routing and Traffic Control HOWTO, *http://lartc.org/*
- Microsoft Internet Security and Acceleration Server, *http://www.microsoft.com/isaserver/*
- Microsoft ISA Server Firewall and Cache, *http://www.isaserver.org/*
- Optimising Internet Bandwidth in Developing Country Higher Education, *http://www.inasp.info/pubs/bandwidth/index.html*
- Pittsburgh Supercomputing Center's guide to Enabling High Performance Data Transfers, *http://www.psc.edu/networking/perf_tune.html*

- Planet Malaysia blog on bandwidth management, *http://planetmy.com/blog/?p=148*
- 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 en malla (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*
- AirJaldi Mesh Router, *http://drupal.airjaldi.com/node/9*

Sistemas operativos y drivers

- 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 Pyramid wireless router OS, *http://pyramid.metrix.net/*
- OpenWRT wireless router OS for Linksys access points, h*ttp://openwrt.org/*
- Tomato wireless router OS for Linksys access points, *http://www.polarcloud.com/tomato*

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 con 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/*
- 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*

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/*
- WirelessU, *http://wirelessu.org/*
- World Summits on Free Information Infrastructures, *http://www.wsfii.org/*

Enlaces misceláneos

- 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/*
- ImageMagick image manipulation tools and libraries, *http://www.imagemagick.org/*
- 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*
- Rusty Russell's Linux Networking Concepts, *http://www.netfilter.org/documentation/HOWTO/networking-concepts-HOWTO.html*
- Ubuntu Linux, *http://www.ubuntu.com/*
- VoIP-4D Primer, *http://www.it46.se/voip4d/voip4d.php*
- wget web utility for Windows, *http://xoomer.virgilio.it/hherold/*
- WiFiMaps war driving map database, *http://www.wifimaps.com/*
- WiSpy spectrum analysis tool, *http://www.metageek.net/*

Libros

- *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

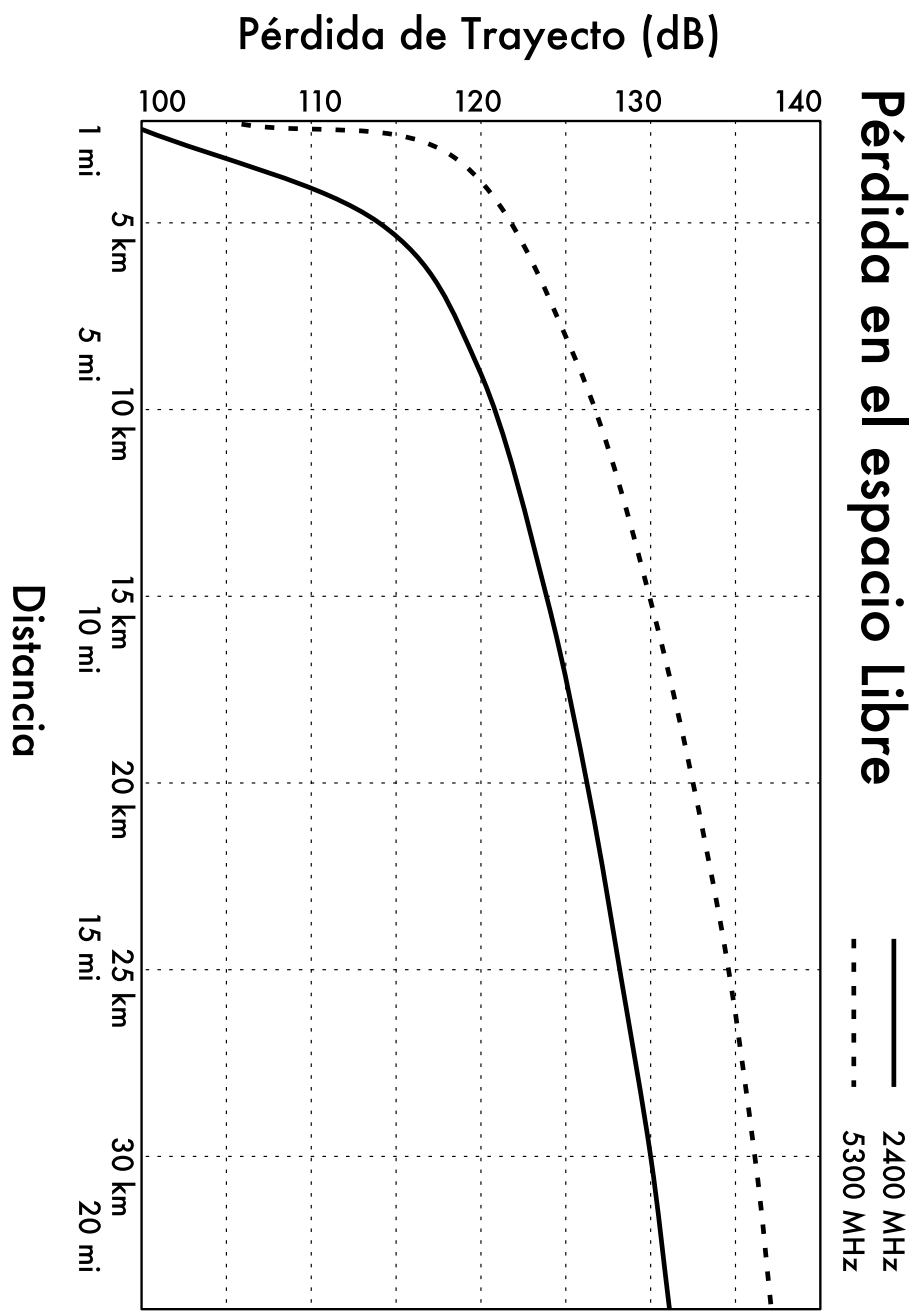
Las siguientes tablas listan los números de los canales y frecuencias centrales utilizadas para 802.11a y 802.11b/g. Si bien todas estas frecuencias están en las bandas sin licenciamiento ISM y U-NII, no todos los canales están disponibles en los diferentes países. Muchas regiones imponen restricciones 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 22 MHz en 802.11b/g, y de 20 MHz 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

Apéndice C: Pérdida de trayectoria



Apéndice D: Tamaño de los cables

Calibre, diámetro, capacidad máxima y resistencia a 200 C. Estos valores pueden variar de cable a cable. Cuando tenga duda, consulte las especificaciones del fabricante.

AWG: American Wire Gauge

Calibre AWG	Diámetro (mm)	Ohms / Metro	Amperios Max
0000	11,68	0,000161	302
000	10,40	0,000203	239
00	9,27	0,000256	190
0	8,25	0,000322	150
1	7,35	0,000406	119
2	6,54	0,000513	94
3	5,83	0,000646	75
4	5,19	0,000815	60
5	4,62	0,001028	47
6	4,11	0,001296	37
7	3,67	0,001634	30
8	3,26	0,002060	24
9	2,91	0,002598	19
10	2,59	0,003276	15

Apéndice E: Dimensionado de sistemas de energía solar

Use estas tablas para recolectar los datos necesarios para estimar el tamaño que va a necesitar su sistema de energía solar.

Datos Generales

Nombre del sitio	
Latitud del Sitio (0)	

Datos de Irradiación

$G_{dm}(0)$, en kWh / m^2 por día

Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Peor mes de irradiación											

Confiabilidad y Voltaje Operacional del Sistema

Días de Autonomía (N)	
Voltaje Nominal (V_{NEquip})	

Características de los Componentes

Paneles Solares	
Voltaje @ Potencia Máxima (V_{pmax})	
Corriente @ Potencia Máxima (I_{pmax})	
Tipo de Panel / Modelo y Potencia (W_p)	

Baterías	
Capacidad Nominal @ 100 H(C_{NBat})	
Voltaje Nominal (V_{NBat})	
Profundidad Máxima de Descarga(DoD_{MAX}) ó Capacidad Utilizable (C_{UBat})	

Regulador	
Voltaje Nominal (V_{NReg})	
Corriente Máxima (I_{maxReg})	

Inversor DC / AC (si se necesita)	
Voltaje Nominal (V_{NConv})	
Potencia Instantánea(P_{IConv})	
Desempeño @ 70 % de Carga	

Cargas

Energía Estimada Consumida por las Cargas (DC)				
			Mes del Mayor Consumo	
Descripción	# de Unidades	x Potencia Nominal	x Uso Horas / Día	= Energía (Wh / día)
			E_{TOTAL} DC	

Energía Estimada Consumida por las Cargas (AC)				
			Mes del Mayor Consumo	
Descripción	# de Unidades	x Potencia Nominal	x Uso Horas/Día	= Energía (Wh/día)
			E_{TOTAL} AC (antes del convertidor)	
			E_{TOTAL} AC (después del convertidor) = E_{TOTAL} AC / 70%	

Cómo Encontrar el Peor Mes

Nombre del Sitio												
Latitud del Sitio(°)												
Voltaje Nominal de la Instalación V_N												
(Mes)	J	F	M	A	M	J	J	A	S	O	N	D
Inclinación ß												
G_{dm} (ß) (kWh/m² × día)												
E_{TOTAL} (DC) (Wh/día)												
E_{TOTAL} (AC) (Wh/día)												
E_{TOTAL} (AC + DC)=												
I_m (A) = E_{TOTAL} (Wh/día) × 1kW/m²/ (G_{dm}(ß) x V_N)												

Resumen del Peor Mes	
Peor Mes	
I_m (A)	
I_{mMAX} (A) = 1.21 x I_m	
E_{TOTAL} (AC + DC)	

Cálculos Finales

Paneles		
Paneles en Serie (N_{PS})	$N_{PS} = V_N / V_{Pmax}$ =	
Paneles en Paralelo (N_{PP})	$N_{PP} = I_{mMAX} / I_{Pmax}$ =	
Número Total de Paneles	$N_{TOT} = N_{PS} \times N_{PP}$ =	

Baterías		
Capacidad Necesaria (C_{NEC})	E_{TOTAL}(PEOR MES) / V_N x N	
Capacidad Nominal (C_{NOM})	C_{NEC} / DoD_{MAX}	
Número de Baterías en Serie N_{BS})	V_N / V_{NBAT}	

Cables			
	Paneles > Baterías	Baterías > Convertidor	Línea Principal
Caída de Voltaje (V_a - V_b)			
Espesor (Sección) r x L x I_{mMAX} / (V_a - V_b)			

Para el cálculo del espesor, r = 0,01286 Ω mm2/m (para cobre) y L es la longitud en metros.

Glosario

0–9

802.11. Aunque 802.11 es un protocolo para redes inalámbricas hoy en día obsoleto, 802.11 se usa frecuentemente para referirse a una familia de protocolos utilizados principalmente para redes inalámbricas de área local que incluye 802.11b, 802.11g, y 802.11a. Ver también: ***Wi-Fi***.

A

AC: ver ***Corriente Alterna***.

access point (***AP***). ***Punto de Acceso***. Un dispositivo que crea una red inalámbrica que usualmente está conectado a una red Ethernet cableada. Ver también ***CPE***, ***master mode***

accumulator. ***Acumulador***. Otra denominación para la ***batería***.

ad-hoc mode. ***Modo ad hoc***. Modalidad de los dispositivos 802.11 que permite la creación de una red sin incluir Puntos de Acceso. Las redes en malla frecuentemente operan los radios en la modalidad ad hoc. Ver también: ***managed mode***, ***master mode***, ***monitor mode***

Address Resolution Protocol (***ARP***). Un protocolo muy usado en redes Ethernet para convertir las direcciones IP en direcciones MAC.

address space. ***Espacio de direcciones***. Grupo de direcciones IP que pertenecen a la misma subred lógica.

advertised window. ***Tamaño de ventana***. La porción del encabezamiento TCP que especifica cuántos bytes (octetos) adicionales de datos está dispuesto a aceptar el receptor.

Alternating Current (***AC***). C***orriente Alterna***. Corriente que varía en el tiempo, alternándose cíclicamente en valores positivos y negativos. Es la usada normalmente en hogares y oficinas. Ver también ***DC*** (***Direct Current*** –Corriente continua).

amortization. ***Amortización***. Técnica de contabilidad utilizada para tomar en cuenta el costo esperado de reemplazo de los equipos debido a obsolescencia o fin de la vida útil.

amplifier. ***Amplificador***. Dispositivo utilizado para incrementar la potencia de una señal.

amplitude. ***Amplitud***. La distancia desde el centro de una onda al extremo de uno de sus picos.

Analizador de espectros. Dispositivo que ofrece una representación visual de la potencia de las señales electromagnéticas en función de la frecuencia. Ver también: ***Wi-Spy***.

Ancho de banda. Gama de frecuencias ocupada por una señal. En comunicaciones digitales se usa comúnmente para indicar la ***capacidad*** o tasa de transmisión. Ver también: ***channel***, ***throughput***.

Ancho del haz. Distancia angular entre los puntos a ambos lados del lóbulo principal de una antena en donde la potencia es la mitad de la potencia máxima. Normalmente se expresa para los planos vertical y horizontal.

anchor clients. ***Clientes Ancla***. Clientes corporativos de un sistema de suscripción que son confiables y considerados de bajo riesgo.

AND logic. ***Lógica AND***. Operador lógico cuya salida es verdadera únicamente cuando todas las entradas son también verdaderas. Ver también: OR logic (Lógica Or).

Anfitrión: Término utilizado para designar cualquier nodo capaz de transmitir y recibir datos en una red.

anonymizing proxy. ***Proxy Anonimizador***. Servicio de red que oculta la fuente y el destino de las comunicaciones, para proteger la privacidad de las personas y para reducir los riesgos legales incurridos por una organización por las acciones de sus usuarios.

anonymity. ***Anonimato***. En redes de computadoras las comunicaciones que no pueden atribuirse a un individuo específico se llaman anónimas. El compromiso entre anonimato y la obligación de rendir cuentas en las comunicaciones en línea es un debate abierto, y las reglas correspondientes a las comunicaciones anónimas varían ampliamente en el mundo. Ver también: ***authenticated*** (***autenticado***)

antenna diversity. ***Diversidad de antenas***. Técnica utilizada para neutralizar la interferencia multitrayectoria mediante el empleo de dos o más antenas físicamente separadas.

antenna gain. ***Ganancia de Antena***. Cantidad en la que se concentra la potencia de una antena en la dirección de su radiación máxima, usualmente expresada en dBi. La ganancia de una antena es recíproca, lo que significa que el incremento de potencia se presenta tanto en transmisión como en recepción.

antenna pattern. ***Patrón de antena***. Gráfico que describe la intensidad relativa del campo radiado por una antena en varias direcciones. Ver también: ***rectangular plot***, ***polar plot***, ***linear polar coordinates***, ***logarithmic polar coordinates***.

AP: ver ***Access Point***.

application layer. ***Capa de aplicación***. La capa superior de los modelos de redes OSI y TCP/IP.

Argus: ver ***Audit Record Generation and Utilization System***.

ARP: ver ***Address Resolution Protocol***.

associated. ***asociado***. Un radio 802.11 se dice asociado a un punto de acceso cuando está listo para comunicarse con la red. Esto significa que está en el canal apropiado, dentro del rango del AP, usa el SSID correcto y otros parámetros de autenticación, etc.

at. Instrucción Unix que permite la ejecución de un programa en un tiempo específico y por una sola vez. Ver también: ***cron***.

attenuation. ***Atenuación***. La reducción de la potencia de una señal a medida que se propaga por su trayectoria, incluyendo la absorción por los árboles, paredes, edificios y otros objetos. Ver también: ***free space loss*** (***pérdida de espacio libre***), ***scattering*** (***dispersión***).

Audit Record Generation and Utilization System (***Argus***). Herramienta de monitoreo de fuente abierta usada para hacer seguimiento de los flujos entre anfitriones (hosts). Disponible en *http://www.qosient.com/argus.*

authenticated. ***Autenticado***. Usuario de la red que ha probado su identidad a un servicio o dispositivo (como un punto de acceso) más allá de toda duda, normalmente utilizando criptografía. Ver también: ***anonymity***.

Autoridad de Certificación. Entidad confiable que emite claves criptográficas firmadas. Ver también: ***Public Key Infrastructure***, ***SSL***.

azimuth. ***Azimut***, ***Acimut***. Ángulo que especifica la desviación con respecto al meridiano. Normalmente se mide en sentido de las agujas del reloj desde el norte, pero en astronomía a veces se mide desde el sur. Ver también: ***inclination***.

B

bandwidth. ***Ancho de banda***. Gama de frecuencias ocupada por una señal. En comunicaciones digitales se usa comúnmente para indicar la ***capacidad*** o tasa de transmisión. Ver también: ***channel***, ***throughput***.

battery. ***Batería***. Dispositivo usado para almacenar energía eléctrica, común en sistemas fotovoltaicos. Ver también: ***solar panel***, ***regulator***, ***load***, ***converter***, ***inverter***.

Baterías de plomo-ácido. Baterías constituidas por dos electrodos de plomo sumergidos en un electrolito de ácido sulfúrico diluido en agua. Ver también: ***stationary batteries***.

beamwidth. ***Ancho del haz***. Distancia angular entre los puntos a ambos lados del lóbulo principal de una antena en donde la potencia es la mitad de la potencia máxima. Normalmente se expresa para los planos vertical y horizontal.

benchmarking. Medida de las prestaciones de un servicio o dispositivo. Para medir la tasa de transmisión en una red se la inunda de tráfico y se observa el caudal (Throughput) medido tanto en transmisión como en recepción.

BGAN: ver ***Broadband Global Access Network***.

BNC connector. ***Conector BNC***. Conector para cable coaxial que utiliza un mecanismo de bayoneta, utilizado frecuentemente en Ethernet 10base2.

brick. ***Ladrillo***. Término utilizado para referise a un dispositivo que se ha vuelto inoperable por un error en el proceso de actualización del ***firmware***. También se usa como verbo para indicar la acción de arruinar el dispositivo, que puede ocurrir, por ejemplo, si se corta la energía durante el proceso de actualización.

bridge. ***Puente***. Dispositivo de red que conecta dos redes a nivel de la ***capa de enlace***. Los puentes no encaminan paquetes en la ***capa de red***. Simplemente repiten paquetes entre dos redes locales. Ver también: ***router*** y ***transparent bridging firewall***.

bridge-utils. Un paquete de Linux que se utiliza para crear puentes en redes Ethernet basados en 802.1d. *http://bridge.sourceforge.net/*

Broadband Global Access Network (***BGAN***). ***Red de Acceso Global de banda ancha***. Uno de los varios estándares utilizados para acceso a Internet por satélite. Ver también: ***Digital Video Broadcast*** (***DVB-S***) y ***Very Small Aperture Terminal*** (***VSAT***).

broadcast address. ***Dirección de difusión***. En redes IP, la dirección de difusión se usa para enviar datos a todos los anfitriones (***hosts***) en la subred local. En redes Ethernet, la dirección MAC de difusión se utiliza para enviar datos a todas las máquinas en el mismo dominio de colisión.

bypass diodes. ***Diodos de puenteo***. Dispositivos utilizados en algunos paneles solares que evita la formación de ***hot-spots*** (zonas calientes) en las celdas que estén a la sombra, a expensas de la disminución del voltaje total suministrado por el panel.

C

CA: ver ***Certificate Authority***.

Cacti (*http://www.cacti.net/*). Popular herramienta de monitoreo basada en la web y escrita en PHP.

capacity. ***Capacidad***. La cantidad de tráfico máximo que puede suministrar un sistema de comunicación digital. A menudo incorrectamente llamada ancho de banda.

captive portal. ***Portal cautivo***. Mecanismo utilizado para redireccionar automáticamente los navegadores web hacia un nuevo sitio. A menudo se utilizan para autenticación, o para interrumpir una sesión para, por ejemplo, informar sobre las políticas de usos aceptables.

Caudal. Cantidad real de información por segundo que fluye en una conexión de red, desechando la tara (overhead) de los protocolos. A veces se le llama también rendimiento de la transmisión. En inglés throughput.

Cell. ***Celda***. Los paneles solares se construyen conectando eléctricamente cierto número de celdas en serie y en

paralelo a fin de suministrar un valor especificado de voltaje y corriente. Las baterías también se construyen conectando en serie celdas individuales, cada una de las cuales aporta cerca de 2 voltios a la batería.

Certificate Authority. ***Autoridad de Certificación***. Entidad confiable que emite claves criptográficas firmadas. Ver también: ***Public Key Infrastructure***, ***SSL***.

channel capacity. ***Capacidad del canal***. Cantidad máxima de información que se puede enviar por segundo en un ancho de banda determinado y con una cierta relación señal/ruido. Ver también: ***bandwidth***, ***throughput***, ***data rate***.

channel. ***Canal***. Un rango de frecuencias bien definidas usadas para comunicaciones. En 802.11 cada canal tiene un ancho de banda de 22 MHz, pero la separación de canales es de 5 MHz. Ver también: ***Apéndice B***.

CIDR: ver ***Classless Inter-Domain Routing***.

CIDR notation. ***Notación CIDR***. Método de definir la máscara de red especificando el número de bits presentes. Por ejemplo la máscara 255.255.255.0 puede especificarse como /24 en la notación CIDR.

circular polarization. ***Polarización circular***. Disposición de los campos electromagnéticos, donde el vector de campo eléctrico efectúa una rotación circular perpendicular a la dirección de propagación, describiendo una rotación completa por cada ciclo de la onda. Ver también: ***horizontal polarization***, ***vertical polarization***.

Class A, ***B***, and ***C networks***. ***Redes Clase A***, ***B*** y ***C***. Originalmente el espacio de direcciones IP se adjudicaba en bloques de tres tamaños distintos: Clase A con unos 16 millones de direcciones, clase B con alrededor de 65 mil direcciones y clase C con 255 direcciones. Aunque CIDR ha reemplazado la adjudicación por clases, estas se siguen usando en el interior de organizaciones que usan direcciones privadas, y a menudo se hace referencia a las clases al hablar del espacio de direcciones IP. Ver también: ***CIDR notation***.

Classless Inter-Domain Routing. ***Enrutamiento entre dominios sin referencia a la clase***. CIDR se desarrolló para mejorar la eficiencia del enrutamiento en las dorsales Internet al permitir la agregación de rutas y máscaras de red de tamaño arbitrario. CIDR reemplaza el viejo sistema basado en clases. Ver también: ***Class A***, ***B***, and ***C networks***.

client. ***Cliente***. Un radio 802.11 en modo administrado (***managed mode***). Los clientes inalámbricos se conectan a una red creada por un AP y automáticamente cambiarán su canal para que coincida con el del AP. Ver también: ***access point***, ***mesh***.

closed network. ***Red cerrada***. Aquella en la que el AP no difunde su SSID, utilizado a menudo como una medida de seguridad.

coax. ***Coaxial***. Un cable de sección circular formado por un alambre central rodeado por un dieléctrico, un conductor cilíndrico externo y una cubierta protectora aislante. Los cables de antenas son de este tipo. Coaxial significa con el mismo eje.

collision. ***Colisión***. Las colisiones en una red Ethernet ocurren cuando dos dispositivos conectados al mismo segmento físico intentan transmitir al mismo tiempo. Cuando se detecta una colisión, los dispositivos se abstienen de transmitir por un tiempo breve determinado aleatoriamente.

conductor. Un material que permite el flujo de energía eléctrica o térmica con poca resistencia. Ver también: ***dieléctrico***, ***aislador***.

connectionless protocol. ***Protocolo sin conexión***. Protocolo de red, como por ejemplo UDP, que no requiere el establecimiento o mantenimiento de una conexión. Este tipo de protocolos requiere menos tara (overhead) que los protocolos orientados a conexión, pero no ofrecen protección a los datos o reensablaje de los paquetes. Ver también: ***session oriented protocol***.

consistent platform. ***Plataforma consistente***. Los costos de mantenimiento pueden reducirse al usar una plataforma común con el mismo hardware, software y firmware para muchos componentes de la red.

constructive interference. ***Interferencia constructiva***. Cuando dos ondas de la

misma frecuencia se combinan en fase, la amplitud de la onda resultante es la suma de las amplitudes de las dos ondas. A esto se le llama interferencia constructiva. Ver también: ***interferencia destructiva***.

controls. En ***NEC2***, controls define la fuente de RF (radiofrecuencia) en el modelo de la antena. Ver también: ***structure***.

converter. ***Conversor***. Dispositivo utilizado para convertir corriente continua a un voltaje diferente o a corriente alterna. Ver también: ***inverter*** (inversor).

corriente alterna. Corriente que varía en el tiempo, alternándose cíclicamente en valores positivos y negativos. Es la usada normalmente en hogares y oficinas. Ver también: ***DC*** (***Direct Current*** – ***Corriente continua***).

CPE: ver ***Customer Premises Equipment***.

cron. Instrucción de Unix que permite la ejecución de un programa a cierta hora incluyendo repeticiones. Ver también: ***at***.

Customer Premises Equipment. ***Equipo de usuario***. Equipo de red tal como un enrutador o un Puente instalado en la propiedad del usuario.

D

data link layer. ***Capa de enlace***. La segunda capa en los modelos de redes OSI o TCP/IP. La comunicación en esta capa ocurre directamente entre nodos. En redes Ethernet se le llama a menudo la capa MAC.

data rate.***Tasa de transmisión***. La velocidad a la cual los radios 802.11 intercambian símbolos, que es siempre mayor que el caudal (throughput) disponible. Por ejemplo, la tasa nominal de 802.11g es 54 Mbps, mientras que el caudal es de unos 20 Mbps. Ver también: ***throughput***.

dB: ver ***decibel***.

DC: ver ***Direct Current***.

DC/AC Converter. ***Conversor DC/AC***. Dispositivo que convierte corriente continua en corriente alterna, requerida por muchos artefactos. También conocido como inversor (***inverter***).

DC/DC Converter. ***Conversor DC/DC***. Dispositivo que cambia el voltaje de una fuente de alimentación continúa. Ver también: ***linear conversion***, ***switching conversion***

decibel (***dB***). Unidad de medida logarítmica que expresa la magnitud de potencia con respecto a un nivel de referencia. Sus derivadas más comunes son el dBi (decibeles relativos a un radiador isotrópico) y dBm (decibeles relativos a 1 mW).

default gateway. ***Pasarela por defecto***. Cuando un enrutador recibe un paquete destinado a una red para la cual no tiene una ruta específica, lo envía a la pasarela por defecto. La pasarela por defecto repite entonces el proceso, posiblemente enviando el paquete a su propia pasarela por defecto, hasta que el paquete alcanza su destino final.

default route. ***Ruta por defecto***. La ruta que apunta a la pasarela por defecto.

Denial of Service (***DoS***). ***Denegación de servicio***. Ataque a los recursos de red, usualmente cometido inundando la red de tráfico, o explotando algún error en una aplicación, o en el protocolo de red.

depreciation. ***Depreciación***. Método de contabilidad consistente en apartar dinero para cubrir el costo del eventual reemplazo del equipo.

destructive interference. ***Interferencia Destructiva***. Cuando se combinan dos ondas idénticas que están exactamente en contrafase, la amplitud de la onda resultante es cero. A esto se le llama interferencia destructiva. Ver también: ***constructive interference***.

DHCP: ver ***Dynamic Host Configuration Protocol***.

Dielectric. ***Dieléctrico***. Material no conductor que separa los conductores dentro de un cable.

Digital Elevation Map (***DEM***). ***Mapa digital con elevaciones***. Datos que representan la altura del terreno para una determinada área geográfica. Estos mapas son usados por programas como ***Radio Mobile*** para modelar la propagación de ondas electromagnéticas.

Digital Video Broadcast (***DVB-S***). Uno de los varios estándares usado para acceso

satelital a Internet. Ver también: ***Broadband Global Access Network*** (***BGAN***) y ***Very Small Aperture Terminal*** (***VSAT***).

Diodos de puenteo. Dispositivos utilizados en algunos paneles solares que evita la formación de ***hot-spots*** (zonas calientes) en las celdas que estén a la sombra, a expensas de la disminución del voltaje total suministrado por el panel.

dipole antenna. ***Antena dipolo***. La forma más simple de antena ***omnidireccional***.

Direct Current (***DC***). ***Corriente continua***. Corriente eléctrica que no cambia de dirección en el tiempo. Se usa normalmente para alimentar dispositivos como puntos de acceso y enrutadores. Ver también: ***Corriente Alterna***.

Direct Sequence Spread Spectrum (**DSSS**). ***Espectro Ensanchado por secuencia directa***. Método de modulación utilizado en los radios 802.11b

directional antenna. ***Antena direccional***. Antena que radia más energía en una dirección particular. Como ejemplos tenemos las Yagi, parabólicas y de guía-onda. Ver también: ***antena omnidireccional***, ***antena sectorial***.

directivity. ***Directividad***. Característica de una antena de enfocar la energía transmitida en una dirección particular en transmisión, o de recibir más energía de una cierta dirección en recepción

diversit: ver ***antenna diversity***.

DNS: ver ***Domain Name Service***.

DNS caching. Al instalar un servidor cache de DNS en su red local, las solicitudes de DNS de toda su red pueden ser almacenadas temporalmente en él, mejorando así los tiempos de respuesta. Esta técnica se llama DNS caching.

dnsmasq. Un servidor DNS caching y de DHCP de fuente abierta disponible en http://thekelleys.org.uk/

Domain Name Service (***DNS***). ***Servicio de nombres de dominio***. Protocolo de red ampliamente utilizado que convierte las direcciones IP numéricas en nombres.

dominant mode. ***Modo Dominante***. Disposición de los campos electromagnéticos a la frecuencia mínima que puede ser transmitida por una guía-onda de determinadas dimensiones.

DoS: ver ***Denial of Service***.

DSSS: ver ***Direct Sequence Spread Spectrum***.

DVB-S: ver ***Digital Video Broadcast***.

Dynamic Host Configuration Protocol (***DHCP***). Protocolo utilizado por los anfitriones (hosts) para determinar automáticamente su dirección IP.

E

eavesdropper. Persona que intercepta subrepticiamente datos como contraseñas, correos electrónicos o conversaciones en línea.

edge. ***Borde***. Lugar donde la red de una organización se encuentra con la de otra. Los bordes se definen por la ubicación de los enrutadores externos, que a menudo actúan como ***cortafuegos***.

electromagnetic spectrum. ***Espectro Electromagnético***. Rango de las diferentes frecuencias de la energía electromagnética, que incluye ondas de radio, microondas, luz visible y rayos X.

electromagnetic wave. ***Onda Electromagnética***. Onda que se propaga en el espacio sin necesidad de un medio de propagación, compuesta de un campo eléctrico y un campo magnético. Ver también: ***onda mecánica***.

elevation: ver ***inclination***.

end span injectors. ***Inyector de extremo***. Dispositivo para ***Power over Ethernet*** 802.3af que suministra energía eléctrica a través del cable Ethernet. Un switch o conmutador Ethernet que suministra energía en cada uno de sus puertos es un ejemplo de inyector de extremo. Ver también: ***mid span injectors***.

end-to-end encryption. ***Cifrado de extremo a extremo***. Una conexión cifrada negociada por ambos extremos de una sesión de comunicación, que provee protección más fuerte que el cifrado en la capa de enlace, recomendado en redes no confiables como la Internet.

EtherApe. Herramienta de visualización de redes de fuente abierta disponible en *http://etherape.sourceforge.net/*.

Ethereal: ver ***Wireshark***.

Extended Service Set Identifier (***ESSID***). Nombre utilizado para identificar una red 802.11. Ver también: ***closed network***.

external traffic. ***Tráfico externo***. Tráfico que se origina, o está destinado a una dirección IP por fuera de la red interna, como por ejemplo, el tráfico de Internet.

F

firestarter. Herramienta gráfica de configuración de cortafuegos Linux disponible en *http://www.fs-security.com/*.

filter. La tabla por defecto utilizada en el sistema de cortafuegos netfilter de Linux, utilizada para determinar el tráfico que debería ser aceptado o negado.

firewall. ***Cortafuego***. Enrutador que acepta o rechaza tráfico con base en algún criterio. Constituye una herramienta básica utilizada para proteger toda la red de tráfico no deseado.

firmware. pequeño programa residente en una memoria de sólo lectura reescribible de algún dispositivo que puede ser actualizado por el usurio.

flashing. acción de reprogramar el firmware de un dispositivo.

flush. Acción de eliminar todas las entradas de una tabla de enrutamiento o una cadena de netfilter.

forwarding. ***reenviar***. Cuando los enrutadores reciben paquetes destinados a otro anfitrión u otra red, envían el paquete hacia el enrutador próximo más cercano al destino final. Este proceso se denomina reenvío.

forwarding loops. ***Lazos de reenvío***. Error en la configuración de un enrutador que resulta en el reenvío cíclico de paquetes entre dos o más enrutadores. El colapso de la red se evita gracias al valor del TTL que lleva cada paquete, pero los lazos de reenvío deben ser resueltos para una adecuada operación de la red.

free space loss. ***Pérdida en el espacio libre***. Disminución de la potencia de la señal a consecuencia del esparcimiento sobre una superficie mayor a medida que el frente de onda se propaga en el espacio. Ver también: ***attenuation***, ***free space loss***, ***Appendix C***.

frequency. ***Frecuencia***. Número the ciclos por segundo de una onda. Ver también: ***wavelength***, ***Hertz***.

front-to-back ratio. ***Relación Adelante/Atrás***. El cociente entre la máxima directividad de una antena y su ***directividad*** en la dirección opuesta.

fuente conmutada. Fuente de alimentación de corriente continua (incorrectamente llamada fuente de poder) que usa un componenete magnético para almacenar temporalmente la energía y transformarla a otro voltaje. Es mucho más eficiente que las fuentes convencionales que usan un transformador y un rectificador y de menor tamaño.

full duplex. Equipo de comunicaciones capaz de transmitir y recibir simultáneamente (como un teléfono). Ver también: ***half duplex***.

fwbuilder. Herramienta gráfica que le permite la creación de guiones para ***iptables*** en una máquina diferente a su servidor y luego transferirlas al servidor. *http://www.fwbuilder.org/*.

G

Gain. ***Ganancia***. La capacidad de un dispositivo (tal como una antena o un amplificador) de aumentar la potencia de una señal. Ver también: ***decibel***.

gain transfer. ***Transferencia de ganancia***. Comparación de la ganancia de la antena a medir con la de una antena estándar cuya ganancia es conocida.

Ganancia de Antena. Cantidad en la que se concentra la potencia de una antena en la dirección de su radiación máxima, usualmente expresada en dBi. La ganancia de una antena es recíproca, lo que significa que el incremento de potencia se presenta tanto en transmisión como en recepción.

gasification. ***Gasificación***. Producción de burbujas de oxígeno e hidrógeno que ocurre cuando se le sigue suministrando corriente a una batería cargada.

Generador de señales. Un transmisor que emite continuamente a una frecuencia específica.

globally routable. ***Enrutable globalmente***. Direcciones suministradas por un ISP, o por el RIR (Regional Internet Registry) que son alcanzables desde cualquier punto de la Internet. En IPv4 hay unos cuatro mil millones de direcciones IP posibles, aunque no todas son enrutables globalmente.

H

half duplex. Equipo de comunicación capaz de transmitir o recibir, pero nunca simultáneamente (como los radios de dos vías). Ver también: ***full duplex***.

Heliax. Cable coaxial de alta calidad con un conductor central sólido o tubular y un conductor externo corrugado que le permite flexibilidad. Ver también: ***coax***.

Hertz (***Hz***). ***Hercio***. Unidad de medida de la frecuencia, correspondiente a ciclos por segundo.

HF (***High-Frequency***). ***Alta frecuencia***. Ondas de radio con frecuencias comprendidas entre 3 y 30 MHz. Se pueden utilizar para transmitir datos a gran distancia, pero con tasas de transmisión muy bajas.

hop. ***Salto***. Recorrido entre dos enrutadores adyacentes. Un servidor web puede estar a varios saltos de su computador local, y los paquetes pasarán de enrutador a enrutador hasta que alcancen su destino final.

Horas Solares Pico. Promedio de irradianza diaria en un área determinada. Equivale al número de horas que recibirían 1w/m2.

horizontal polarization. ***Polarización Horizontal***. Campo electromagnético en el que el campo eléctrico varía linealmente en el plano horizontal. Ver también: ***circular polarization***, ***vertical polarization***.

host. ***Anfitrión***. Cualquier nodo conectado a la red que puede recibir y enviar paquetes.

hot-spot. En una red inalámbrica, un hot-spot es un sitio que ofrece acceso a Internet mediante ***Wi-Fi***, usualmente a través de un ***portal cautivo***. En un sistema ***fotovoltaico*** ocurre un hot-spot cuando una celda del panel queda en sombra haciendo que funcione como una carga en lugar de generar potencia.

hub. ***Concentrador***. Dispositivo Ethernet que repite los datos recibidos en todos su puertos.

Huygens principle. ***Principio de Huygens***. Principio que establece que cada punto de un frente de onda se puede considerar que genera un infinito número de frentes de ondas que se propagan en todas direcciones. Este concepto se utiliza para modelar la propagación en presencia de obstáculos.

Hz: ver ***Hertz***.

I

IANA: ver ***Internet Assigned Numbers Authority***.

ICMP: ver ***Internet Control Message Protocol***.

ICP: ver ***Inter-Cache Protocol***.

impedance. ***Impedancia***. Cociente entre el voltaje y la corriente en una línea de transmisión, constituido por una resistencia y una reactancia. La impedancia de carga debe adaptarse a la impedancia de la fuente para máxima transferencia de potencia (normalmente 50 ohmios para sistemas de comunicaciones).

inbound traffic. ***Tráfico entrante***. Paquetes de red originados por fuera de la red local, y dirigidos a un destino dentro de ésta. Ver también: ***outbound traffic***.

inclination. ***Inclinación***. Ángulo con respecto al plano horizontal. Ver también: ***azimuth***.

infrastructure mode: ver ***master mode***.

insulator: ver ***dielectric***.

Inter-Cache Protocol (***ICP***). Protocolo de altas prestaciones usado para comunicar entre web caches.

Internet Assigned Numbers Authority (***IANA***). La organización que administra partes críticas de la infraestructura de Internet incluyendo la adjudicación de las direcciones IP, los servidores DNS raíz y los números de protocolos de servicio.

Internet Control Message Protocol (***ICMP***). Protocolo de la capa de red usado para informar a los nodos acerca del estado de la red, parte de la pila de protocolos de Internet. Ver ***Internet protocol suite***.

Internet layer: ver ***network layer***.

Internet Protocol (***IP***). ***Protocolo IP***. El protocolo de red de uso más común. IP define los anfitriones y las redes que constituyen la Internet global.

Internet protocol suite (***TCP/IP***). ***Grupo de protocolos Internet***. Familia de protocolos de comunicación que definen la Internet. Estos incluyen TCP, IP, ICMP, y UDP. También llamada ***TCP/IP protocol suite***, o simplemente ***TCP/IP***.

Intrusion Detection System (***IDS***). ***Sistema de detección de intrusos***. Un programa que examina el tráfico en la red buscando patrones o datos sospechosos. Un IDS puede realizar una anotación de bitácora (log entry), notificar un administrador de red, o tomar acciones directas en respuesta al tráfico indeseable.

inverter: ver ***DC/AC Converter***.

IP: ver ***Internet Protocol***.

iproute2. El paquete de herramientas de enrutamiento avanzado de Linux, usado para conformación de tráfico (traffic shaping) y otras técnicas avanzadas. Disponible en *http://linux-net.osdl.org/*.

iptables. Comando principal utilizado para manipular las reglas del cortafuego ***netfilter***.

Irradiance. ***Irradianza***. La potencia total de la radiación solar que incide sobre una determinada superficie en W/m2.

ISM band. ***Banda ICM***. La banda designada por la UIT (Unión Internacional de telecomunicaciones) para uso Industrial, Científico y Médico, utilizable sin necesidad de licencia previa en la mayoría de los países.

isotropic antenna. ***Antena Isotrópica***. Antena hipotética que distribuye su potencia en todas direcciones con la misma intensidad. No es físicamente realizable, pero se utiliza como referencia.

IV characteristic curve. ***Curva característica IV***. Gráfica que representa la corriente producida en función del voltaje generado en una celda o panel solar iluminado.

K

K. Símbolo del sistema internacional de medidas para indicar la unidad de temperatura, el kelvin. Informalmente se usa en computación para indicar la potencia de 2 más cercana a mil, es decir 1024.

k. Prefijo del sistema internacional de medidas que significa 1000. Debería escribirse siempre en minúscula.

knetfilter. Interfaz gráfica para configurar cortafuegos con Linux, disponible en http://venom.oltrelinux.com/.

known good. Componente cuya funcionalidad ha sido comprobada y que podemos utilizar para sustituir a otro que sospechamos pueda estar averiado en el proceso de identificación de fallas (troubleshooting).

L

lag. ***Demora***. Término utilizado para describir una red donde el tiempo de transmisión de los paquetes, también llamado latency sea considerable.

Lambda: (**λ**) ver ***wavelength*** (***longitud de onda***).

LAN: ver ***Local Area Network***.

latency. ***Latencia***. Tiempo que tarda un paquete en atravesar una conexión de red. A menudo se utiliza (incorrectamente) para designar el Round Trip Time (RTT), puesto que es mucho más fácil medir este último parámetro en una conexión de área extendida que la verdadera latencia. Ver también: ***Round Trip Time***.

lead-acid batteries. ***Baterías de plomo-ácido***. Baterías constituidas por dos electrodos de plomo sumergidos en un electrolito de ácido sulfúrico diluido en agua. Ver también: ***stationary batteries***.

lease time. Cuando se utiliza DHCP, las direcciones IP se asignan por un período limitado, conocido como lease time, una vez transcurrido éste, el cliente debe solicitar otra dirección IP del servidor DHCP.

Line of Sight (***LOS***). ***Línea de vista***. Si una persona desde un punto A logra ver un punto B, se dice que existe línea de vista entre ambos puntos.

linear polar coordinates. ***Coordenadas polares lineales***. Gráfica con círculos graduados concéntricos que representan el valor absoluto de una proyección polar. Estos gráficos se utilizan para representar patrones de radiación de las antenas. Ver también: ***logarithmic polar coordinates***

linear conversion. ***Conversión lineal***. Método de convertir voltajes continuos a un valor inferior disipando el exceso de potencia en forma de calor. Ver también: ***switching conversion***.

l***inear polarization***. ***Polarización Lineal***. Onda electromagnética en la que el campo eléctrico permanece siempre en el mismo plano. El campo eléctrico puede ser vertical, horizontal, o en un ángulo intermedio. Ver también: ***vertical polarization***, ***horizontal polarization***.

link budget. ***Presupuesto de potencia***. Análisis de los factores que determinan la potencia que alcanza el receptor en un enlace inalámbrico. Partiendo de la potencia de salida del transmisor, hay que considerar las pérdidas en los cables, ganancia de las antenas y pérdidas en el trayecto. El enlace será viable cuando la energía recibida exceda la energía umbral del receptor en un factor denominado margen del enlace.

link layer encryption. ***Cifrado en capa de enlace***. Conexión cifrada entre dispositivos en la misma red local, comúnmente un AP y un cliente. Ver también: ***end-to-end encryption*** (***cifrado de extremo a extremo***).

link-local. Los dispositivos de red que están conectados al mismo segmento físico se comunican entre sí directamente y se dicen que son link-local. Este tipo de conexiones no puede atravesar un enrutador a menos que utilicen algún tipo de encapsulación como un ***tunnel*** o una ***VPN***.

listen. ***Escuchar***. Los programas que aceptan una conexión en un puerto TCP se dice que escuchan en ese puerto.

load. ***Carga***. Equipo que consume energía. Ver también: ***battery***, ***solar panel***, ***regulator***, ***converter***, ***inverter***

Lóbulos laterales. Ninguna antena puede irradiar solamente en la dirección preferida. Inevitablemente irradia también en otras direcciones. Estos picos más reducidos se denominan lóbulos laterales.

Local Area Network (***LAN***). ***Red de area local***. Una red (típicamente Ethernet) usada dentro de una organización. La parte de la red detrás del enrutador del ISP es generalmente considerada parte de la LAN. Ver también: ***WAN***.

logarithmic polar coordinates. ***Coordenadas polares logarítmicas***. Gráfico formado por círculos graduados concéntricos, espaciados logarítmicamente, que representan el valor absoluto de una proyección polar. Comúnmente se usan para representar el patrón de radiación de una antena. Ver también: ***linear polar coordinates***.

long fat pipe network. Conexión de red (tal como una VSAT) que tiene gran capacidad y gran latencia. Para obtener buenas prestaciones, TCP debe entonarse para ajustarse a las características de estas redes.

LOS: ver ***Line of Sight***.

M

MAC layer: ver ***data link layer***.

MAC address. ***Dirección MAC***. Número de 48 bits asignado unívocamente a todo dispositivo de red cuando es fabricado. La dirección MAC se utiliza para comunicaciones ***link-local***.

MAC filtering. ***Filtrado por MAC***. Método de control de acceso basado en la dirección MAC de los dispositivos que se comunican.

MAC table. Un conmutador (switch) de red debe mantener una lista de las direcciones MAC usadas en cada uno de los puertos físicos, con el fin de distribuir eficazmente los paquetes. Esta información se mantiene en una tabla llamada MAC table.

maintenance-free lead-acid batteries: ver ***lead-acid batteries***.

Man-In-The-Middle (***MITM***). ***Hombre en el medio***. Tipo de ataque donde un usuario malicioso intercepta todas las comunicaciones entre el cliente y el

servidor, con lo que puede manipular la información.

managed hardware. ***Hardware administrado***. Hardware de red que provee una interfaz de administración, contadores de puertos, SNMP y otras características interactivas.

managed mode. ***Modo administrado***. Modalidad de los dispositivos 802.11 que permite que el radio de una estación cliente se una a una red creada por un AP (Access Point). Ver también: ***master mode***, ***ad-hoc mode***, ***monitor mode***.

master browser. En redes Windows el master browser es el computador que lleva una lista de todos los computadores, comparticiones e impresoras disponibles en **Network Neighborhood,** o **My Network Places**.

master mode. Modalidad de los dispositivos 802.1 que permite que un radio pueda crear una red tal como lo hace un AP. Ver también: ***managed mode***, ***ad-hoc mode***, ***monitor mode***.

match condition. ***Condición de selección***. En netfilter, la match condition especifica los criterios que determinan el blanco final de un determinado paquete. Los paquetes se pueden seleccionar en función de la dirección MAC, dirección IP de origen o de destino, número de puerto, contenido de los datos, o cualquier otra propiedad.

Maximum Depth of Discharge (***DoDmax***). ***Profundidad máxima de descarga***. La cantidad de energía extraída de una batería en un ciclo de descarga, expresada como porcentaje.

Maximum Power Point (***Pmax***). ***Punto de potencia máxima***. Punto en el que la potencia suministrada por un panel solar alcanza su máximo.

MC-Card. Diminuto conector de microondas utilizado en equipos Lucent / Orinoco/Avaya.

mechanical wave. ***Onda mecánica***. Onda causada cuando algún medio u objeto oscila de manera periódica. Ver también: ***electromagnetic wave***

Media Access Control layer: ver ***data link layer***.

mesh. ***Malla***. Red carente de organización jerárquica, donde cada nodo puede transportar el tráfico de otros nodos. Las buenas implementaciones de redes en malla detectan y resuelven automáticamente los problemas de enrutamiento en forma dinámica.

message types. ***Tipos de mensajes***. El tráfico ICMP utiliza tipos de mensajes en lugar de números de puerto para definir la información enviada. Ver también: ***ICMP***.

method of the worst month. ***Método del peor mes***. Método para dimensionar un sistema fotovoltaico de manera que satisfaga las necesidades de energía del mes en el que la demanda de energía eléctrica es mayor con relación a la oferta de energía solar. Al cumplir con el caso más desfavorable, los demás meses no tendrán problemas.

MHF: ver ***U.FL***.

microfinance. ***Microfinanzas***. Provisión de pequeños préstamos, ahorros y otros servicios financieros básicos a las personas más necesitadas del globo.

mid span injectors. ***Inyector de línea***. Dispositivo ***Power over Ethernet*** insertado entre un conmutador Ethernet y el dispositivo que va a ser alimentado. Ver también: ***end span injectors***.

milliwatts (***mW***). ***Milivatios***. Unidad de potencia correspondiente a una milésima de vatio.

MITM: ver ***Man-In-The-Middle***.

MMCX. Conector de microondas muy pequeño utilizado en equipos de Senao y Cisco.

monitor mode. ***Modo Monitor***. Modalidad de dispositivos 802.11 en la que el radio escucha pasivamente todo el tráfico en la red. Ver también: ***master mode***, ***managed mode***, ***ad-hoc mode***.

monitor port. ***Puerto de monitoreo***. En un conmutador administrado, se puede definir uno más puertos de monitoreo que recibirán el tráfico de todos los demás puertos. Esto permite conectar un servidor de monitoreo de tráfico para observar y analizar los patrones de tráfico.

Multi Router Traffic Grapher (***MRTG***). Herramienta de fuente abierta usada para

graficación y otras estadísticas, disponible en *http://oss.oetiker.ch/mrtg/*.

multipath. ***Multitrayectoria***. Característica de propagación en la que la presencia de obstáculos refleja las señales y hace que alcancen al receptor habiendo recorrido diferentes trayectos y por lo tanto con diferentes retardos de propagación.

multipoint-to-multipoint: ver ***mesh***.

mW: ver ***milliwatt***.

My TraceRoute (***mtr***). Herramienta de diagnóstico usada como alternativa al popular programa ***traceroute***, disponible en *http://www.bitwizard.nl/mtr/*. Ver también: ***traceroute*** / ***tracert***.

N

N connector. ***Conector N***. Robusto conector de microondas utilizado en componentes para exteriores, como antenas y puntos de acceso (AP).

Nagios (*http://nagios.org/*). Herramienta de monitoreo de tiempo real que registra en bitácora y notifica al administrador las fallas de servicios y de la red.

NAT: ver ***Network Address Translation***.

nat. La tabla usada en el cortafuego ***netfilter*** de Linux para configurar la conversión de direcciones.

NEC2: ver ***Numerical Electromagnetics Code***.

NetBIOS. Protocolo de la capa de sesión usado para compartir archivos e impresoras en Windows. Ver también: ***SMB***.

netfilter. Mecanismo de filtrado de paquetes utilizado en las versiones modernas de Linux. Utiliza el comando ***iptables*** para manipular las reglas de filtrado. *http://netfilter.org/*.

netmask (***network mask***). ***Máscara de red***. Número de 32 bits que divide los 16 millones de direcciones IP disponibles en porciones más pequeñas, denominadas subredes. Todas las redes IP usan las direcciones IP en combinación con las máscaras de red para agrupar lógicamente a los anfitriones y las redes.

NeTraMet. Herramienta de fuente abierta disponible en *freshmeat.net/projects/netramet/*.

network address. ***Dirección de la red***. El número IP inferior de una subred. La dirección de la red es utilizada en las tablas de enrutamiento para especificar el destinatario cuando se envían paquetes a un grupo lógico de direcciones IP.

Network Address Translation (***NAT***). NAT es una tecnología de red que permite que muchos computadores compartan una misma dirección de red válida (enrutable globalmente). Aunque esto es muy útil para resolver el problema del número limitado de direcciones IP disponibles, crea un desafío técnico para servicios bidireccionales, como Voz sobre IP.

network detection. Herramienta de diagnóstico que muestra información acerca de las rede inalámbricas, tales como el nombre de la red, canal, y método de cifrado utilizado.

network layer. ***Capa de red***. También llamada la capa Internet. Es la tercera capa tanto del modelo OSI como del modelo TCP/IP de redes. Es la que utiliza el protocolo IP, y donde se efectúa el enrutamiento.

network mask: ver ***netmask***.

ngrep. Programa de fuente abierta para seguridad de redes que permite encontrar patrones en flujos de datos. Disponible gratuitamente en *http://ngrep.sourceforge.net/*.

node. ***Nodo***. Cualquier dispositivo capaz de enviar y recibir datos en una red. Los AP, enrutadores, computadores y laptops son ejemplos de nodos.

Nominal Capacity (***CN***). ***Capacidad nominal***. Cantidad máxima de energía que puede ser extraída de una batería completamente cargada. Se expresa en Amperios-hora (Ah), o vatios-hora (Wh).

Nominal Voltage (***VN***). ***voltaje nominal***. Voltaje de operacion de un sistema fotovoltaico, comúnmente 12 ó 24 voltios.

ntop. Herramienta de monitoreo que suministra muchos detalles acerca de las conexiones y protocolos usados en una red de área local. *http://www.ntop.org/*.

null. ***Nulo***. En el patrón de radiación de una antena, un nulo es una zona en la cual la potencia irradiada efectiva es mínima.

nulling. ***Anulamiento***. Caso especial de la interferencia multitrayectoria donde las señales en la antena receptora se anula por la ***interferencia destructiva*** causada por las señales reflejadas.

number of days of autonomy (***N***). ***Número de días de autonomía***. Máximo número de días que puede operar un sistema fotovoltaico sin recibir energía significativa del sol.

Numerical Electromagnetics Code (***NEC2***). Paquete gratuito para modelar antenas que permite fabricar modelos tridimensionales, y luego analizar la respuesta electromagnética de la antena. *http://www.nec2.org/*.

O

OFDM: ver ***Orthogonal Frequency Division Multiplexing***.

omnidirectional antenna. ***Antena Omnidireccional***. Tipo de antena que irradia con igual intensidad en todas las direcciones del plano horizontal. Ver también: ***antena direccional***, ***antena sectorial***.

one-arm repeater. Repetidor inalámbrico que utiliza un solo radio, con lo que el caudal se reduce en la retransmisión. Ver también: ***repeater***.

onion routing. Herramienta de privacidad, (tal como Tor) que repetidamente rebota sus conexiones TCP sobre numerosos servidores esparcidos en la Internet, envolviendo la información de enrutamiento en varias capas cifradas.

OR logic. ***Logica OR***. Operación lógica cuyo resultado es verdadero si cualquiera de las entradas que se comparan es verdadera. Ver también: ***AND logic***.

Orthogonal Frequency Division Multiplexing (***OFDM***). Técnica de modulación que consiste en descomponer una señal de banda ancha en muchas componentes de banda angosta, cada una de las cuales es modulada en frecuencia por una subportadora. Gracias a la propiedad matemática de ortogonalidad de las subportadoras se minimiza la interferencia entre ellas, lo que resulta en una señal más robusta respecto a la multitrayectoria.

OSI network model. ***Modelo de red de la OSi***. Modelo muy popular de redes de comunicaciones definido por el estándar ISO/IEC 7498-1. El modelo OSI consiste de siete capas independientes, de la física, a la de aplicación. Ver también: ***TCP/IP network model***.

outbound traffic. ***Tráfico Saliente***. Paquetes originados en la red local y dirigidos a un destinatario exterior (usualmente algún lugar de Internet). Ver también: ***inbound traffic***.

overcharge. ***Sobrecarga***. Condición de una batería cuando se le sigue aplicando carga mas allá de la capacidad de la misma. En estas condiciones, el electrolito se descompone produciendo gases y se acorta la duración de la bateria. Los ***reguladores*** permiten una pequeña sobrecarga para que las burbujas así formadas ayuden a mezclar el electrolito, pero luego cortan la corriente para evitar daños en la batería.

overdischarge. ***Sobredescarga***. Descargar una batería mas allá de su ***Maximum Depth of Discharge*** (***Profundidad máxima de descarga***), lo que resulta en deterioro de la misma.

oversubscribe. ***Sobresuscripción***. Permitir un número de usuarios mayor de los que soporta el ancho de banda disponible.

P

packet. ***Paquete***. En redes IP, los mensajes enviados entre computadores se fraccionan en pequeños trozos llamados paquetes. Cada paquete contiene la información de procedencia, destinación y otros detalles de enrutamiento que permiten entregarlo a su destino. Los paquetes son reensamblados en el extremo remoto mediante TCP (u otro protocolo) antes de ser pasados a la aplicación.

packet filter. ***Filtro de paquetes***. Cortafuegos que funcionan en la capa de Internet inspeccionando las direcciones de procedencia y destino, número de puertos y protocolos. Los paquetes son admitidos o

rechazados dependiendo de las reglas de filtrado de paquetes.

partition. ***Apartado***.Técnica usada por concentradores de red para limitar el impacto de nodos que transmiten en exceso. El concentrador aísla temporalmente el nodo defectuoso (lo aparta) del resto de la red y lo reconecta despues de algún tiempo. Cuando esto ocurre excesivamente es señal de que hay un cliente que consume demasiado ancho de banda, tal como una aplicación ***peer-to-peer*** o un virus en la red.

Pasarela por defecto. Cuando un enrutador recibe un paquete destinado a una red para la cual no tiene una ruta específica, lo envía a la pasarela por defecto. La pasarela por defecto repite entonces el proceso, posiblemente enviando el paquete a su propia pasarela por defecto, hasta que el paquete alcanza su destino final.

passive POE injector: ver ***Power over Ethernet***.

path loss. ***Pérdida de trayectoria***. Disminución de la potencia de la señal debida a la distancia entre el transmisor y el receptor.

Peak Sun Hours (***PSH***). ***Horas Solares Pico***. Promedio de irradianza diaria en un área determinada. Equivale al número de horas que recibirían 1w/m2.

Pérdida de retorno. Medida logarítmica expresada en dB del cociente entre la potencia reflejada por la antena o la línea de transmisión y la potencia inyectada a la misma. Ver también: ***impedance***.

photovoltaic generator: ver ***solar panel***.

photovoltaic solar energy. ***Energía solar fotovoltaica***. Uso de paneles solares para producir electricidad. Ver también: ***thermal solar energy***.

photovoltaic system. ***Sistema fotovoltaico***. Sistema que convierte la energía de la radiación solar y la almacena para uso posterior. Un sistema fotovoltaico autónomo no necesita estar conectado a la red de energía eléctrica. Ver también: ***battery***, ***solar panel***, ***regulator***, ***load***, ***converter***, ***inverter***.

physical layer. ***Capa física***. La capa inferior de los modelos de red OSI y TCP/IP. La capa física especifica el medio utilizado para la comunicación, tal como cable de cobre, fibra óptica u ondas de radio.

pigtail. ***Latiguillo***. Cable corto y flexible usado en microondas para convertir un conector no estándar en algo más robusto y común. Sirve también para disminuir el esfuerzo mecánico aplicado al conector del radio.

ping. Herramienta de diagnóstico muy popular que utiliza paquetes ICMP de solicitud de eco y sus respuestas para determinar el tiempo de ida y vuelta a un anfitrión en la red. Cuando se transmite un ping entre dos máquinas podemos averiguar en qué parte de la trayectoria se interrumpe el flujo de comunicación.

PKI: ver ***Public Key Infrastructure***.

plomb. Una pieza de metal muy pesada que se entierra en el suelo para mejorar la conductividad de la puesta a tierra.

PoE: ver ***Power over Ethernet***.

point-to-multipoint. ***Punto a Punto*** (***Pt-Mpt***). Topología de red en la que varios nodos se conectan a la misma estación central, llamada estación base o AP (***Access Point***). El ejemplo clásico es el de varios laptops que se conectan a un AP para acceder a Internet. Ver también: ***point-to-point***, ***multipoint-to-multipoint***.

point-to-point. ***Punto a Punto*** (***Pt-Pt***). Red inalámbrica constituida únicamente por dos estaciones, usualmente separadas a una gran distancia.Ver también: ***point-to-multipoint***, ***multipoint-to-multipoint***.

Point-to-Point Protocol (***PPP***). Protocolo de red usado típicamente en líneas seriales (tales comoconexiones discadas) para proveer conectividad IP.

polar plot. ***Gráfico polar***. Gráfico construido proyectando los puntos sobre un eje que rota (radio) con la intersección de uno o varios círculos concéntricos. Ver también: ***rectangular plot***.

polarization. ***Polarización***. Trayectoria del campo eléctrico de una onda electromagnética en el espacio, o en una antena. Ver también: ***horizontal polarization***, ***vertical polarization***, ***circular polarization***.

polarization mismatch. ***Desacoplamiento de polarización***. Condición en la que la antena transmisora y receptora no usan la misma polarización, resultando en pérdida de señal.

policy. En ***netfilter***, policy es la acción tomada por defecto cuando ninguna de las reglas de filtrado son aplicables. Por ejemplo, la policy por defecto para cualquier cadena puede ser establecida como ACCEPT o DROP.

port counters. ***Contadores de puertos***. Los conmutadores (switches) y enrutadores administrados proveen estadísticas por cada puerto conectado llamadas port counters. Estas estadísticas pueden incluir número de paquetes y de bytes entrantes y salientes, así como errores y retransmisiones.

Portal cautivo. Mecanismo utilizado para redireccionar automáticamente los navegadores web hacia un nuevo sitio. A menudo se utilizan para autenticación, o para interrumpir una sesión para, por ejemplo, informar sobre las políticas de usos aceptables.

power. ***Potencia***. Cantidad de energía por unidad de tiempo.

Power over Ethernet (***PoE***). Técnica utilizada para suministrar corriente continua a un dispositivo utilizando el cableado Ethernet. Ver también: ***end span injectors***, ***mid span injectors***.

PPP: ver ***Point to Point Protocol***.

presentation layer. ***Capa de presentación***. La sexta capa del modelo de red OSI, que especifica la manera de representar los datos, tal como codificación MIME o compresión de los datos.

Presupuesto de potencia. Análisis de los factores que determinan la potencia que alcanza el receptor en un enlace inalámbrico. Partiendo de la potencia de salida del transmisor, hay que considerar las pérdidas en los cables, ganancia de las antenas y pérdidas en el trayecto. El enlace será viable cuando la energía recibida exceda la energía umbral del receptor en un factor denominado margen del enlace.

private address space. ***Espacio de direcciones privadas***. Conjunto de direcciones IP especificadas en RFC1918. Las direcciones privadas o no enrutables se usan a menudo en una organización en combinación con NAT (Conversión de direcciones). El espacio reservado para direcciones privadas incluye 10.0.0.0/8 , 172.16.0.0/12, y 192.168.0.0/16. Ver también: ***NAT***.

Privoxy (*http://www.privoxy.org/*). Un web proxy que ofrece anonimato mediante el uso de filtros. ***Privoxy*** se usa frecuentemente en conjunción con ***Tor***.

proactive routing. ***Enrutamiento proactivo***. Una implementación de ***mesh*** (***red en malla***) en la que cada nodo tiene conocimiento de todos los otros nodos en la nube de la malla y también de cuáles nodos pueden utilizarse como pasarelas de tráfico. Cada nodo mantiene una tabla de enrutamiento que abarca la totalidad de la nube de la malla. Ver también: ***reactive routing***.

protocol analyzer. ***Analizador de protocolos***. Programa de diagnóstico usado para observar y desensamblar los paquetes de red. Suministran la máxima cantidad de detalles acerca de paquetes individuales.

protocol stack. ***Pila de protocolos***. Conjunto de protocolos que proveen capas de funcionalidad independientes. Ver también: ***OSI network model*** y ***TCP/IP network model***.

Proxy. Programa o dispositivo que realiza una acción en representación de otro. Muy comunes los servidores proxy que almacenan localmente las páginas web mas frecuentadas para disminuir el tráfico del enlace a Internet.

PSH: ver ***Peak Sun Hours***.

Public key cryptography. ***Cifrado de clave pública***. Forma de cifrado utilizada por SSL, SSH y otros programas populares de seguridad. Permite que la información cifrada transite sobre una red no segura sin necesidad de distribuir la clave secreta de cifrado.

Public Key Infrastructure (***PKI***). ***Infraestructura de clave pública***. Mecanismo de seguridad usado en conjunción con ***public key cryptography*** para prevenir los ataques de tipo ***Man-In-The-Middle***. Ver tambien: ***certificate authority***.

Q

quick blow. Tipo de fusible que se funde inmediatamente cuando la corriente que lo atraviesa supera el valor establecido. Ver también: ***slow blow***.

R

radiation pattern: ver ***antenna pattern***.

radio. Porción del espectro electromagnético en la cual se pueden generar ondas al aplicar corriente alterna a una antena. Dispositivo capaz de emitir y recibir estas ondas.

reactive routing. ***Enrutamiento reactivo***. Tipo de malla (***mesh***) en la que las rutas se calculan únicamente en el momento en que se requiere enviar datos a un nodo específico. Ver también: ***proactive routing***.

realtime monitoring. ***Monitoreo en tiempo real***. Herramienta que permite el monitoreo por largos períodos de tiempo y notifica al administrador en el instante en que se produce algún problema.

reciprocity. ***Reciprocidad***. Propiedad de las antenas de presentar las mismas características en transmisión y en recepción.

recombinant batteries: ver ***lead-acid batteries***.

rectangular plot. ***Diagrama rectangular***. Gráfica donde los puntos se ubican en una grilla simple. Ver también: ***polar plot***.

Regional Internet Registrars (***RIR***). Los 4 mil millones de posibles direcciones IP son administrados por IANA. El espacio ha sido dividido entre grandes subredes, cuya administración ha sido delegada a alguna de las 5 entidades regionales llamadas ***Registrars***, cada una con autoridad sobre una gran área geográfica. Por ejemplo, en América Latina y el Caribe es LACNIC.

regulator. ***Regulador***. Componente de un sistema fotovoltaico que asegura que la batería trabaje en condiciones adecuadas, evitando la sobrecarga y sobredescarga que podrían disminuir la vida útil de la batería. Ver también: ***solar panel***, ***battery***, ***load***, ***converter***, ***inverter***.

repeater. ***Repetidor***. Nodo configurado para retransmitir el tráfico que no le está destinado, a menudo utilizado para extender el rango útil de una red.

Request for Comments (***RFC***). Los RFC son una serie de documentos numerados publicados por la Internet Socierty que describen las ideas y conceptos de las tecnologías de Internet. No todos los RFC son estándares, pero muchos son aprobados explícitamente por el IETF, o en algún momento se convierten en estándares de facto. Los RFC están disponibles en línea en *http://rfc.net/*.

return loss. ***Pérdida de retorno***. Medida logarítmica expresada en dB del cociente entre la potencia reflejada por la antena o la línea de transmisión y la potencia inyectada a la misma. Ver también: ***impedance***.

reverse polarity (***RP***). ***Polaridad Inversa***. Conectores de microondas especiales con el género invertido. Como ejemplo tenemos el popular RP-TNC que usan los Linksys, el RP-SMA y el RP-N.

RF transmission line. ***Línea de transmisión de radiofrecuencia***. El medio (usualmente un cable coaxial, heliax, o una guía de onda) que conecta el radio a la antena.

RIR: ver ***Regional Internet Registrars***.

Round Trip Time (***RTT***). ***Tiempo de ida y vuelta***. Cantidad de tiempo que le toma a un paquete para que la confirmación de su recepción llegue al transmisor. Frecuentemente confundido con la ***latencia***.

rogue access points. ***Punto de acceso pirata***. Un punto de acceso no autorizado instalado incorrectamente por un usuario autorizado o por una persona maliciosa que pretende recabar datos para dañar la red.

Round Robin Database (***RRD***). Base de datos que almacena información de manera muy compacta y que no se expande en el tiempo. Este es el formato de datos tanto por la herramienta RDD, como por otras herramientas de monitoreo de redes.

router. ***Enrutador***, ***ruteador***, ***encaminador***. Dispositivo que reenvía paquetes entre diferentes redes. El proceso de reenviar paquetes hacia el próximo salto

es llamado enrutamiento, ruteo o encaminamiento.

routing. ***enrutamiento***, ***ruteo o encaminamiento***. Proceso de reenviar paquetes entre diferentes redes. El dispositivo que lo realiza se llama enrutador o ruteador.

routing table.***Tabla de enrutamiento***. Una lista de redes y direcciones IP mantenida por un enrutador para determinar de qué manera deben reenviarse los paquetes. Si un enrutador recibe un paquete para una red que no aparezca en la tabla de enrutamiento, lo enviará a su pasarela por defecto (***default gateway***). Los enrutadores operan en la capa de red. Ver también: ***bridge y default gateway***.

RP: ver ***Reverse Polarity***.

RP-TNC. Versión modificada del popular conector de microondas TNC con el género invertido, utilizado por los equipos fabricados por Linksys.

RRD: ver ***Round Robin Database***.

RRDtool. Conjunto de herramientas que permiten crear y modificar bases de datos RDD así como generar gráficos útiles para presentar los datos. RRDtool se usa para hacerle el seguimiento de datos en el tiempo (tales como ancho de banda, temperatura del cuarto de máquinas o carga promedio del servidor) y pueden desplegar esos datos como un promedio en el tiempo. RRDtool se puede obtener en http://oss.oetiker.ch/rrdtool/.

Ruta por defecto. La ruta que apunta a la pasarela por defecto.

rsync (*http://rsync.samba.org/*). Herramienta de fuente abierta para transferencia incremental de archivos usada para mantener mirrors (servidores espejo).

RTT: ver ***Round Trip Time***.

S

SACK: ver ***Selective Acknowledgment***.

scattering. ***Dispersión***. Pérdida de señal debida a la presencia de objetos pequeños entre dos nodos. Ver también: f***ree space loss***, ***attenuation***.

sectorial antenna. ***Antena sectorial***. Antena que radia principalmente en un área específica. El haz puede ser tan amplio como de 180 grados, o tan estrecho como 60 grados. Ver también: ***directional antenna***, ***omnidirectional antenna***.

Secure Sockets Layer (***SSL***). Tecnología de cofrado de extremo a extremo incorporada prácticamente en todos los navegadores de red (***web browsers***). SSL usa ***public key cryptography*** y una ***public key infrastructure*** para permitir comunicaciones seguras en la web. Cuando usted ve una página cuyo URL comienza con https, está empleando SSL.

Selective Acknowledgment (***SACK***). ***Reconocimiento Selectivo***. Mecanismo utilizado para superar las ineficiencias del TCP en redes de alta latencia como las VSAT.

Server Message Block (***SMB***). Protocolo usado en redes Windows para proporcionar servicios de compartición de archivos. Ver también: ***NetBIOS***.

Service Set ID (***SSID***): ver ***Extended Service Set Identifier***.

session layer. ***Capa de sesión***. Quinta capa del modelo OSI que maneja las conexiones lógicas entre aplicaciones.

session oriented protocol. ***Protocolo orientado a sesión***. Protocolo orientado a sesión (tal como TCP) que requiere inicialización antes de que se pueda proceder al intercambio de datos, así como algunas tareas de limpieza una vez concluido el intercambio. Los protocolos orientados a sesión normalmente ofrecen corrección de errores y reensamblado de paquetes, a diferencia de los protocolos sin conexión. Ver también: ***connectionless protocol***.

shared medium. ***Medio Compartido***. Una red ***link-loca***l donde cada nodo puede ver el tráfico de todos los otros nodos.

Shorewall (*http://shorewall.net/*). Herramienta de configuración usada para establecer cortafuegos ***netfilter*** sin necesidad de aprender la sintaxis de ***iptables***.

sidelobes. ***Lóbulos laterales***. Ninguna antena puede irradiar solamente en la dirección preferida. Inevitablemente irradia también en otras direcciones. Estos picos

más reducidos se denominan lóbulos laterales.

signal generator. ***Generador de señales***. Un transmisor que emite continuamente a una frecuencia específica.

Simple Network Management Protocol (***SNMP***). Protocolo diseñado para facilitar el intercambio de información de gestión entre dispositivos de red. SNMP se usa típicamente para sondear conmutadores de red y enrutadores para recopilar estadísticas de operación.

site-wide web cache. Aunque todos los navegadores modernos proveen una memoria temporal local (cache), las organizaciones grandes pueden mejorar la eficiencia instalando un ***site-wide web cache*** tal como ***Squid***, que mantiene una copia de todas las solicitudes hechas desde dentro de la organización para agilizar el procesamiento de ulteriores solicitudes al mismo sitio. Ver también: ***Squid***.

slow blow. ***Fusible lento***. Tipo de fusible que permite el paso de una corriente superior a la nominal por un corto tiempo. Ver también: ***quick blow***.

SMA. Un conector de micronda pequeño de rosca.

SMB: ver ***Server Message Block***.

SmokePing. Herramienta que mide, almacena y despliega la latencia, la distribución de la latencia y las pérdidas de paqutes en el mismo gráfico. Disponible en *http://oss.oetiker.ch/smokeping/*.

SNMP: ver ***Simple Network Management Protocol***

Snort (***http://www.snort.org/***). Sistema muy popular de detección de intrusiones. Ver también: ***Intrusion Detection System***.

SoC: ver ***State of Charge***.

solar module: ver ***solar panel***.

solar panel. El componente de un sistema fotovoltaico que convierte la energía solar en electricidad. Ver también: ***battery***, ***regulator***, ***load***, ***converter***, ***inverter***.

solar panel array. ***Arreglo de paneles solares***. Conjunto de paneles solares conectados en serie o en paralelo para proporcionar la energía necesaria a una determinada carga.

solar power charge regulator: ver ***regulator***.

spectrum: ver ***electromagnetic spectrum***.

spectrum analyzer. ***Analizador de espectros***. Dispositivo que ofrece una representación visual de la potencia de las señales electromagnéticas en función de la frecuencia. Ver también: ***Wi-Spy***.

Speed. ***Velocidad***. Término genérico usado para referirse a la rapidez de una conexión de red. Una red de “alta velocidad” debería tener baja latencia y capacidad más que suficiente para transportar el tráfico de sus usuarios. Ver también: ***bandwidth*** (***ancho de banda***), ***capacity***, y ***latency***.

split horizon DNS. ***DNS de horizonte dividido***. Técnica que consiste en ofrecer diferentes respuestas a las solicitudes de DNS en función de la fuente de la solicitud. Se utiliza para dirigir a los usuarios internos a otro grupo de servidores DNS diferente de los que sirven a los usuarios de Internet.

spoof. Sustituir falsamente un dispositivo, usuario o servicio.

spot check tools. ***Herramientas de comprobación ocasional***. Herramientas de monitoreo que se ejecutan únicamente cuando se necesita diagnosticar un problema. Ejemplos: ***ping*** y ***traceroute***.

Squid. Un ***web proxy cache*** muy popular. Es flexible, robusto, con muchas funcionalidades y puede adaptarse a redes de cualquier tamaño. *http://www.squid-cache.org/*.

SSID: ver ***Extended Service Set Identifier***.

SSL: ver ***Secure Sockets Layer***.

standalone photovoltaic system: ver ***photovoltaic system***.

State of Charge (***SoC***). ***Estado de carga***. Cantidad de carga presente en una batería, determinada por el voltaje medido y el tipo de batería.

stateful inspection. Reglas de cortafuego que toman en cuenta el estado asociado con un paquete dado. El estado no es parte del paquete y se transmite sobre la Internet, pero es determinado por el propio cortafuego.Las conexiones nuevas, establecidas y relacionadas pueden ser tomadas en cuenta para filtrar los paquetes. La inspección tomando en cuenta el estado

es también llamada a veces connection tracking (rastreo de conexiones).

stationary batteries. ***Baterías estacionarias***. Baterías diseñadas para estar en una ubicación fija y en un escenario donde el consumo de potencia es más o menos irregular. Las baterías estacionarias pueden soportar ciclos de descarga muy fuerte, pero no están diseñadas para producir grandes corrientes por breves periodos de tiempo como las baterías automotrices. Ver también: ***lead-acid batteries***.

structure. En ***NEC2***, una descripción numérica de la ubicación de las diferentes partes de una antena y de cómo están interconectados los alambres. Ver también: ***controls***.

subnet mask: ver ***netmask***.

subnets. ***Subredes***. Un subconjunto de redes IP definido por la máscara de red.

switch. ***Conmutador***. Dispositivo de red que provee una conexión temporal dedicada entre nodos que se comunican. Ver también: hub.

switching conversion. ***Conversión por conmutación***. Método de conversion de voltajes continuos que usa un componenete magnético para almacenar temporalmente la energía y transformarla a otro voltaje. Es mucho más eficiente que la conversión lineal.

T

target. En ***netfilter***, la acción que se debe tomar cuando un paquete cumple con las condiciones de una regla. Algunos targets posibles son: ***ACCEPT***, ***DROP***, ***LOG***, y ***REJECT***.

TCP: ver ***Transmission Control Protocol***.

TCP acknowledgment spoofing. Técnica utilizada en comunicaciones vía satélite para mejorar el caudal de la transmisión. En lugar de esperar la respuesta del extremo satelital remoto, el enrutador en el extremo cercano envía un ACK cuando el paquete está aún en tránsito.

TCP window size. ***Tamaño de la ventana TCP***. El parámetro de TCP que define cuántos datos pueden ser transmitidos antes de que un paquete ACK sea enviado por el receptor. Por ejemplo, una ventana de 3000 implica que se transmitirán dos paquetes de 1500 bytes cada uno, depués de lo cual el extremo receptor enviará un ACK o pedirá una retransmisión.

TCP/IP: ver ***Internet protocol suite***.

TCP/IP network model. Modelo de redes TCP/IP. Simplificación del modelo de redes OSI que se usa con las redes Internet. El modelo TCP/IP consiste de 5 capas independientes, desde la física hasta la de aplicación. Ver también: ***OSI network model***.

tcpdump. Herramienta popular para capturar y analizar paquetes disponible en *http://www.tcpdump.org/*. Ver también: WinDump and Wireshark.

Temporal Key Integrity Protocol (***TKIP***). Protocolo de cifrado utilizado en conjunto con ***WPA*** para mejorar la seguridad de una sesión de comunicaciones.

thermal solar energy. ***Energía solar térmica***. Energia del sol recolectada en forma de calor. Ver también: ***photovoltaic solar energy***.

thrashing. Estado de un computador que ha utilizado toda la memoria RAM disponible y debe usar el disco duro para almacenamiento temporal, disminuyendo significativamente las prestaciones del sistema.

throughput. ***Caudal***. Cantidad real de información por segundo que fluye en una conexión de red, desechando la tara (overhead) de los protocolos.

throughput testing tools. ***Herramientas para medir caudal***. Herramientas que miden el ancho de banda neto real entre dos puntos de la red.

Time To Live (***TTL***). ***Tiempo de vida***. El TTL funciona como un freno de emergencia para señalar el tiempo después del cual los datos deberían ser descartados. En redes TCP/IP el TTL es un contador que empieza con cierto valor (tal como 64), y se decrementa en cada salto (travesía por un enrutador). Si el TTL llega a 0, el paquete se descarta. Este mecanismo ayuda a reducir los daños causados por los lazos de enrutamiento. En DNS, el TTL define la cantidad de tiempo que un determinado registro de zona debe ser mantenido antes

de actualizarlo. En Squid, el TTL define cuánto tiempo se debe almacenar un objeto antes de volver a buscarlo en el website original.

TKIP: ver ***Temporal Key Integrity Protocol***.

TNC connector. Un popular conector de rosca utilizado en microondas.

Tor (*http://www.torproject.org/*). Una herramienta ***onion routing*** que ofrece buena protección contra el análisis de tráfico.

traceroute / ***tracert***. Herramienta de diagnóstico ubicua usada a menudo en conjunción con ping para determinar la ubicación de un problema en la red. La versión Unix se llama traceroute, mientras que la versión Windows es tracert. Ambas usan paquetes ICMP de solicitud de eco que van incrementando el valor del TTL para deteminar cuáles enrutadores se están usando para conectar al anfitrión remoto y también muestra las estadísticas de latencia. Otra variante es tracepath que usa una técnica similar con paquetes UDP. Ver también: ***mtr***.

traction batteries: ver ***lead-acid batteries***.

Transmission Control Protocol (***TCP***). Protocolo orientado a sesión que opera en la capa de transporte, suministrando reensablado de paquetes, manejo de la congestión y entrega confiable. TCP es un protocolo integral usado por muchas aplicaciones de Internet incluyendo HTTP y SMTP. Ver también: ***UDP***.

transmission power. ***Potencia de transmisión***. Potencia eléctrica a la salida del transmisor de radio, antes de la ganancia de antena, o de las pérdidas de la línea de transmisión.

transparent bridging firewall. Cortafauego puente-transparente.Técnica de cortafuego que introduce un puente y reenvía selectivamente los paquetes basada en las reglas del cortafuego. Una ventaja del cortafuego puente-transparente es que no requiere una direccion IP. Ver también: ***bridge***.

transparent cache. ***Caché transparente***. Método de implementar una caché que sirva a toda una organización y que no requiere configuración en las máquinas clientes. Las solicitudes al web se redireccionan automáticamente a la caché, la cual se encarga de procesarlas. Las cache transparentes no pueden utilizar autenticación, lo que hace imposible implementar contabilidad de tráfico en el nivel del usuario. Ver también: ***site-wide web cache***, ***Squid***.

transparent proxy. ***Proxy transparente***. Un proxy instalado de manera que las solicitudes al web sean redireccionadas automáticamente al servidor proxy, sin necesidad de configurar los navegadores de las máquinas de los usuarios.

transport layer. ***Capa de transporte***. Tercera capa de los modelos de redes ISO y TCP/IP, que provee un método para utilizar un servicio específico en un nodo de la red dado. Los ejemplos más comunes de protocolos de esta capa son ***TCP*** y ***UDP***.

trending. Tipo de herramienta que realiza monitoreo sobre largos periodos, y registra los resultados en una gráfica. Las herramientas trending le permiten predecir el comportamienmto futuro de su red, lo que ayuda en la planificación de actualizaciones y cambios.

TTL: ver ***Time To Live***.

tunnel. ***Tunel***. Una forma de encapsulacion que envuelve una pila de protocolos dentro de otra, usada a menudo en conjunción con cifrado para proteger la comunicacion contra usuarios no autorizados, eliminando así el requerimiento de que la propia aplicación soporte el cifrado. Los túneles se usan frecuentemente en combinacion con ***VPN***.

U

U.FL. Diminuto conector de microndas utilizado por muchas tarjetas de radio mini-PCI.

UDP: ver ***User Datagram Protocol***.

unintentional users. ***Usuarios no intencionales***. Usuarios de Laptops que accidentalmente se asocian a una red inalámbrica equivocada.

Unshielded Twisted Pair (***UTP***). ***Par trenzado no apantallado***. Cable usado para Ethernet 10baseT y 100baseT, que consiste de cuatro pares de hilos trenzados.

Useful Capacity (***Cu***). ***Capacidad usable***. Capacidad utilizable de una batería, correspondiente al producto de la ***Capacidad nominal*** y la ***Profundidad máxima de descarga***.

User Datagram Protocol (***UDP***). Protocolo de la capa de transporte que no utiliza conexión usado comúnmente para audio y video de flujo continuo.

UTP: ver ***Unshielded Twisted Pair***.

V

valve regulated lead acid battery (***VRLA***): ***ver lead-acid batteries***.

vertical polarization. ***Polarizacion Vertical***. Campo electromagnético en el que el campo eléctrico se mueve en una dirección lineal vertical. La mayoría de los dispositivos inalámbricos para consumidores utilizan polarización vertical. Ver también: circular polarization, horizontal polarization.

Very Small Aperture Terminal (***VSAT***). Una de las muchas tecnologías utilizadas para acceso a Internet satelital. VSAT es la tecnología de acceso satelital mas difundida en África y en Latinoamérica. Ver también: ***Broadband Global Access Network*** (***BGAN***) y ***Digital Video Broadcast*** (***DVB-S***).

video sender. Transmisor de video a 2,4 GHz; puede ser utilizado como ***generador de señales*** de bajo costo.

Virtual Private Network (***VPN***). Herramienta utilizada par unir dos redes a través de una tercera no confiable (tal como la Internet). Las VPN se usan a menudo para que los usuarios remotos puedan tener acceso a la red de la organización cuando están viajando, o desde sus hogares. Las VPN utilizan una combinacion de túneles y cifrado para asegurar todo el tráfico de red, independientemente de la aplicacion que se esté usando. Ver también: ***tunnel***.

VoIP (***Voice over IP***). Tecnología que ofrece servicios similares a los telefónicos sobre una conexión Internet. Ejemplos de clientes populares de VoIP son Skype, Gizmo Project, MSN Messenger, e iChat.

VPN: ver ***Virtual Private Network***.

VRLA: ver ***valve regulated lead acid battery***.

VSAT: ver ***Very Small Aperture Terminal***.

W

WAN: ver ***Wide Area Network***.

War drivers. Entusiastas de la tecnología inalámbrica que se interesan por encontrar la ubicación física de las redes WiFi.

wavelength. ***Longitud de onda***. La distancia desde un punto en una onda hasta su parte equivalente en la siguiente, por ejemplo desde un pico positivo hasta el siguiente. Se suele representar por la letra griega ***lambda*** (**λ**).

WEP: ver ***Wired Equivalent Privacy***.

wget. Herramienta de fuente abierta para descargar páginas web: *http://www.gnu.org/software/wget/*.

Wi-Fi. Marca comercial de propiedad de la WiFi Alliance usada para referirse a las tecnologías 802.11a, 802.11b, y 802.11g. Wi-Fi es la abreviación de ***Wireless Fidelity***.

Wi-Fi Protected Access (***WPA***). Protocolo de cifrado bastante robusto que opera en la capa de enlace soportado por la mayor parte de los dispositivos Wi-Fi modernos.

Wi-Spy. Dispositivo para análisis de espectro de bajo costo para la banda de 2,4 GHz. Ver *http://www.metageek.net/*.

Wide Area Network (***WAN***). ***Red de área extensa***. Cualquier tecnología de redes de larga distancia, tales como líneas dedicadas, frame relay, DSL, inalámbrico fijo y servicios vía satélite. Ver también: ***LAN***.

wiki. Sitio web que permite que cualquier usuario edite el contenido de cualquier página. Uno de los mas populares wiki públicos es *http://www.wikipedia.org/*.

window scale. Extensión de TCP definido en RFC1323 que permite tamaños de ventana superiores a 64 kB.

WinDump. Version Windows de tcpdump disponible en *http://www.winpcap.org/windump/*.

Wired Equivalent Privacy (***WEP***). Protocolo de cifrado en la capa de enlace que ofrece cierto grado de seguridad

soportado por prácticamente todos los equipos 802.11a/b/g.

Wireless Fidelity: ver ***Wi-Fi***.

wireshark. Analizador de protocolos open source para Linux, Unix , Mac y Windows. *http://www.wireshark.org/*.

WPA: ver ***Wi-Fi Protected Access***

Z

Zabbix (*http://www.zabbix.org/*). Herramienta de monitoreo en tiempo real que registra y notifica al administrador del sistema las fallas de red y de los servicios.