Redes sem fio no Mundo em Desenvolvimento

Um guia prático para o planejamento e a construção de uma infra-estrutura de telecomunicações

Redes sem fio no Mundo em Desenvolvimento

Para mais informações sobre este projeto, visite-nos na web em *http://wndw.net/*

Primeira edição, janeiro de 2006
Segunda edição, dezembro de 2007
Primeira tradução para o português, outubro de 2008

Muitas designações usadas por fabricantes e fornecedores na distinção de seus produtos são consideradas marcas proprietárias. Quando essas designações aparecerem neste livro e os autores estiverem cientes de que tais são marcas proprietárias, as mesmas serão impressas totalmente em letras maiúsculas, ou com as iniciais em letras maiúsculas. Todas as demais marcas pertencem a seus respectivos proprietários.

Os autores e o editor tomaram o devido cuidado no preparo deste livro, mas não fornecem nenhuma garantia explícita ou implícita de qualquer tipo ou assumem qualquer responsabilidade por erros ou omissões. Nenhuma responsabilidade é assumida por danos acidentais ou conseqüentes de conexões feitas através do uso da informação aqui contida.

© 2008 Hacker Friendly LLC, *http://hackerfriendly.com/*

ISBN: 978-0-9778093-8-7

SOME RIGHTS RESERVED

Esta obra é disponibilizada sob a licença Creative Commons **Attribution-ShareAlike 3.0**. Para mais detalhes sobre seus direitos de uso e redistribuição desta obra, visite *http://creativecommons.org/licenses/by-sa/3.0/*

Índice

Capítulo 1
Por onde começar 1

Propósito deste livro....2
Adequando a comunicação sem fio à sua rede atual.... 3
Protocolos de redes wireless....3
Perguntas e Respostas.... 5

Capítulo 2
Uma introdução prática à rádio-física 9

O que é uma onda?....9
Polarização....12
O espectro eletromagnético.... 13
Largura de banda....14
Freqüências e canais.... 15
Comportamento das ondas de rádio.... 15
Linha de visão....22
Potência....24
A física no mundo real....25

Capítulo 3
Projeto de rede 27

Entendendo redes....27
Projetando a rede física....51
Rede Mesh com OLSR....56
Mais informações....93

Capítulo 4
Antenas e linhas de transmissão 95

Cabos....95
Guias de onda....97
Conectores e adaptadores....100
Antenas e padrões de radiação....102
Teoria de refletores....115
Amplificadores....115
Projetos práticos de antenas....117

Capítulo 5
Hardware de rede 137

Escolhendo componentes wireless....139
Soluções comerciais versus “faça você mesmo”....141
Proteção profissional contra raios....143
Construindo um ponto de acesso a partir de um PC....145

Capítulo 6
Segurança e monitoramento 157

Segurança física....158
Ameaças à rede....160
Autenticação....162
Privacidade....167
O que é normal?....202

Capítulo 7
Energia solar 211

Energia solar....211
Componentes de sistemas fotovoltaicos....212
O painel solar....217
A bateria....221
O regulador de potência de carga....228
Conversores....230
Equipamento ou carga....231
Como dimensionar seu sistema fotovoltaico....236
Custo de uma instalação de energia solar....244

Capítulo 8
Construindo um nó externo 247

Gabinetes à prova d'água....247
Fornecendo energia elétrica....248
Considerações de montagem....249
Segurança....255
Alinhando antenas em um link de longa distância....256
Proteção contra surtos elétricos e raios....262

Capítulo 9
Diagnósticos 265

Montando seu time....265
Técnicas apropriadas para o diagnóstico....268
Problemas comuns de rede....269

Capítulo 10
Sustentabilidade Econômica 279

Crie uma declaração de Missão....280
Avalie a demanda para as potenciais ofertas....281
Estabelecendo incentivos apropriados....282

Pesquise a regulamentação local para o uso de comunicações wireless. 283
Analise os competidores..... 284
Determine custos iniciais, recorrentes e seus preços..... 285
Garantindo o investimento..... 288
Avalie forças e fraquezas da situação interna..... 290
Colocando tudo junto..... 291
Conclusão..... 294

Capítulo 11
Estudos de Caso 295

Recomendações gerais..... 295
Quebrando barreiras com uma bridge simples em Timbuktu..... 298
Encontrando um terreno sólido em Gao..... 301
Rede wireless comunitária da Fundação Fantsuam..... 304
A cruzada pela Internet de baixo custo na zona rural de Mali..... 313
Ofertas comerciais no Leste da África..... 320
Rede Mesh sem fio na Comunidade Dharamsala..... 326
Rede no estado de Mérida..... 328
Chilesincables.org..... 338
Longa Distância com 802.11..... 348

Apêndices 363

Apêndice A: Recursos..... 363
Apêndice B: Alocações de Canal..... 370
Apêndice C: Perdas no Caminho..... 372
Apêndice D: Tamanhos de Cabo..... 373
Apêndice E: Dimensionamento Solar..... 374

Glossário 379

Prefácio da tradução para o português

O caminho que levou-me à tradução deste livro para o português foi longo. Começou com o Timothy Ney, da Linux GreenHouse, que apresentou-me ao Marco Figueiredo, da ONG Gemas da Terra e que, por fim, sugeriu ao Rob Flickenger, da Hacker Friendly, que a Brod Tecnologia assumisse a tradução.

Sou um daqueles vários que, em meados dos anos 90, aventuraram-se a implantar provedores de acesso à Internet usando uma infra-estrutura que envolvia softwares de código aberto. Esse livro trouxe lembranças de muitas madrugadas intensas, passando cabos Ethernet (coaxiais ou 10BaseT) de um lado a outro e editando arquivos de configuração do servidor de email. Quisera eu ter um livro destes naquela época, onde a pouca e esparsa literatura só existia em inglês.

Justamente pela linguagem da tecnologia ser o inglês, e por termos lido o material disponível nessa língua quando criávamos a "nossa" Internet, acabamos por tomar palavras de uma ou outra língua e hoje nos são comuns termos que podem doer nos ouvidos dos mais puristas. Linkamos as coisas, deletamos arquivos, clicamos em links e, quando vemos alguém navegando na Internet em seu computador, perguntamos: "tu tens wireless?"

Usamos a palavra wireless com a mesma naturalidade que usamos "sem fio", browser ao invés de navegador e, ao mesmo tempo, usamos roteador ao invés de router e sequer traduzimos os termos mouse ou switch—ou alguém chama um switch de chaveador?

Claro, em outros países de língua portuguesa, que não o Brasil, estas questões podem ser ligeiramente diferentes, mas a gente se entende.

Por causa desta idiossincrasia idiomática lutei muito, durante o processo de tradução, para ficar no limite entre manter-me o mais literal possível próximo do fantástico texto original e, ao mesmo tempo, torná-lo agradável ao leitor de língua portuguesa. Procurei, de maneira básica, conceituar (de forma adicional ao texto original) textos que no dia-a-dia usamos em inglês—como o próprio termo wireless. De forma similar, mesmo quando usamos um termo em português (por exemplo, provedor de acesso ao invés de ISP), mantive a

referência ao termo em inglês, buscando sempre auxiliar o leitor em sua posterior busca por mais informação.

Agradeço muito à minha sócia Joice Käfer, que fez a revisão técnica desta tradução e, além disso, contribuiu com críticas que multiplicaram o seu próprio trabalho. Ela criticava, eu reescrevia, ela tinha que revisar de novo, e assim sucessivamente. Agradeço também a paciência da Lara Sobel, editora deste livro, que profetizou: "um dia, no futuro, escritores, desenhistas, revisores e editores serão capazes de colaborar conjuntamente nos mesmos documentos, em um espaço web livre e aberto!". Mais agradecimentos ao Rob Flickenger, Marco Figueiredo, Timothy Ney, a todos os autores deste livro, com quem aprendi muito, e à minha família, que não cheguei a ver muito durante os meses em que executei este trabalho.

Boa leitura!

Cesar Brod
cesar@brod.com.br
http://brodtec.com/

Sobre este livro

Este livro é parte de um conjunto de materiais relativos ao mesmo tópico: Redes sem fio (wireless) no Mundo em Desenvolvimento, para o qual utilizamos o acrônimo WNDW (*Wireless Networking in the Developing World*). O projeto WNDW inclui:

- Livros impressos, disponíveis sob demanda;
- Várias traduções, incluindo francês, espanhol, português, italiano, árabe e outras;
- Uma versão em PDF e HTML, isentas de DRM (*Digital Rights Management*), deste livro;
- Uma lista de discussões arquivada sobre conceitos e técnicas descritas neste livro;
- Casos de estudo adicionais, material de treinamento e demais informações relacionadas ao tema.

Para acesso a este e outros materiais, visite o endereço web: *http://wndw.net/*

O livro e o arquivo PDF estão publicados sob a licença **Attribution-ShareAlike 3.0** da Creative Commons. Essa licença permite a qualquer um fazer cópias e mesmo vendê-las com lucro, desde que o devido reconhecimento seja feito aos autores e que cada trabalho derivado seja disponibilizado sob os mesmos termos. Toda e qualquer cópia ou trabalho derivado **deve** incluir o link para o nosso website, em destaque, *http://wndw.net/*.

Visite *http://creativecommons.org/licenses/by-sa/3.0/* para mais informações sobre estes termos. Cópias impressas podem ser encomendadas de Lulu.com, um serviço de impressão sob demanda. Consulte o website (*http://wndw.net/*) para detalhes sobre como pedir uma cópia impressa. O PDF será atualizado periodicamente e, a encomenda do livro através do serviço de impressão sob demanda, garante que você receberá a versão mais recente.

O website conta com casos de estudo adicionais, equipamento atualmente disponível e mais referências para websites externos. Voluntários e idéias são bem-vindos. Por favor, assine nossa lista de discussão e envie-nos suas idéias.

O material de treinamento foi escrito para os cursos ministrados pela *Association for Progressive Communications* e o *Abdus Salam International Center for Theoretical Physics*. Visite *http://www.apc.org/wireless/* e *http://wireless.ictp.trieste.it/* para mais detalhes sobre esses cursos e seu material. Informação adicional foi fornecida pela *International Network for the Availability of Scientific Publications*, *http://www.inasp.info/*. Parte deste material foi incorporado diretamente neste livro. Textos adicionais foram adaptados de *How To Accelerate Your Internet*, *http://bwmo.net/*.

Créditos

Este livro começou como o projeto BookSprint na sessão de 2005 da WSFII, em Londres, na Inglaterra (*http://www.wsfii.org/*). Um núcleo de sete pessoas construiu as linhas iniciais do livro durante o evento, apresentando os resultados na conferência e escrevendo o livro durante alguns meses. No decorrer do projeto, o grupo solicitou, ativamente, contribuições e críticas da comunidade de redes sem fio (*wireless*). Contribua com suas próprias críticas e atualizações no wiki de WNDW em *http://www.wndw.net/*

Grupo Central

- **Rob Flickenger** foi o autor líder e editor deste livro. Rob escreveu e editou vários livros sobre redes sem fio e Linux, incluindo *Wireless Hacks* (O'Reilly Media) e *How To Accelerate Your Internet* (*http://bwmo.net/*). Ele é, orgulhosamente, um hacker, cientista maluco amador e proponente de redes livres em todos os lugares.
- **Corinna "Elektra" Aichele.** Entre os principais interesses de Elektra estão sistemas autônomos de geração de energia e comunicação sem fio (antenas, redes sem fio de longa distância, redes *mesh*). Ela criou uma pequena distribuição Linux (baseada na distribuição Slackware) preparada para redes mesh, sem fio. Esta informação, claro, é redundante para aqueles que lerem, o livro... *http://www.scii.nl/~elektra*
- **Sebastián Büttrich** *(http://wire.less.dk)* é um generalista em tecnologia, com um histórico de programação científica e física. Nascido em Berlim, na Alemanha, ele trabalhou no IconMedialab em Copenhagen de 1997 até 2002. Tem Ph.D. em física quântica pela Technical University de Berlim. Sua formação em física inclui os campos de rádio-freqüência e espectroscopia com microondas, sistemas fotovoltaicos e matemática avançada. Também é músico em apresentações e de estúdio.
- **Cesar Brod,** (*http://www.brod.com.br*) formou-se técnico em eletrônica em 1982 e, antes disto, já trabalhava com computadores. Usuário de Linux desde 1993, teve papel importante na expansão da Internet no Vale do Taquari, interior do Rio Grande do Sul, Brasil. Trabalhou em várias empresas multinacionais e, graças a elas, pôde conhecer boa parte do mundo. Em 2003 participou de um projeto do governo Finlandês que analisou o uso de softwares de código livre e aberto na geração de emprego e renda. Desde 1999 presta serviços de

consultoria através da Brod Tecnologia. É gestor de projetos dos Innovation Centers de Código Aberto e Interoperabilidade mantidos pela Microsoft junto a universidades brasileiras.

- **Laura M. Drewett** é co-fundadora da Adapted Consulting Inc., um empreendimento social especializado na adaptação de tecnologia e modelos de negócios para o mundo em desenvolvimento. Desde que viveu em Mali, nos anos 90, e escreveu sua tese em programas educativos para meninas, Laura tem lutado pela busca de soluções sustentáveis para o desenvolvimento. Especialista em sustentabilidade para projetos de informática e tecnologia em ambientes do mundo em desenvolvimento, ela desenvolveu e gerenciou projetos para uma diversidade de clientes na África, Oriente Médio e Europa Oriental. Laura tem bacharelado em Artes, com distinção em Negócios Internacionais e Francês da University of Virginia e mestrado em Gestão de Projetos pela George Washington University School of Business.

- **Alberto Escudero-Pascual** e **Louise Berthilson** são fundadores da IT +46, uma empresa sueca de consultoria com foco em tecnologia da informação para regiões em desenvolvimento. IT +46 é internacionalmente conhecida por promover e implementar infra-estrutura para a Internet e redes sem fio nas áreas rurais da África e da América Latina. Desde 2004, a empresa treinou mais de 350 pessoas em 14 países e publicou mais de 600 páginas de documentação sob licença Creative Commons. Mais informações podem ser encontradas em *http://www.it46.se/*

- **Carlo Fonda** é membro da Unidade de Rádio Comunicações no Abdus Salam International Center for Theoretical Physics em Trieste, Itália.

- **Jim Forster** ocupou sua carreira com desenvolvimento de software, trabalhando especialmente com sistemas operacionais e redes em empresas fornecedoras de produtos. Ele tem experiência com várias empresas embrionárias que não tiveram sucesso no Silicon Valley, e com uma de sucesso: Cisco Systems. Depois de trabalhar bastante com desenvolvimento de produtos nessa empresa, suas atividades mais recentes envolvem projetos e políticas para a melhoria do acesso à Internet em países em desenvolvimento. Ele pode ser contatado através do email *jrforster@mac.com.*

- **Ian Howard.** Depois de voar pelo mundo inteiro como um paraquedista do exército canadense, Ian Howard decidiu trocar sua arma por um computador. Depois de concluir sua graduação em ciências ambientais na University of Waterloo, ele escreveu em uma proposta: "a tecnologia de redes sem fio traz a oportunidade de quebrar as barreiras digitais. Nações pobres, que não têm a mesma infra-estrutura para a conectividade que nós temos, agora têm a capacidade de criar uma infra-estrutura de rede sem fio." Como recompensa, o Geekcorps o enviou a Mali como gestor de programa, onde ele liderou uma equipe que aparelhou estações de rádio com interconexões de rede sem fio e

projetou sistemas de compartilhamento de conteúdo. Hoje ele é consultor de vários programas do Geekcorps.

- **Kyle Johnston,** *http://www.schoolnet.na/*

- **Tomas Krag** passa seus dias trabalhando com *wire.less.dk*, uma organização sem fins lucrativos baseada em Copenhagen, que ele fundou com seu amigo e colega Sebastian Büttrich no início de 2002. A *wire.less.dk* é especializada em soluções para redes sem fio comunitárias, focando-se especialmente em redes wireless de baixo custo para o mundo em desenvolvimento.

  Tomas é também um associado do *Tactical Technology Collective* (*http://www.tacticaltech.org/*), uma organização sem fins lucrativos baseada em Amsterdã, que tem por meta "fortalecer movimentos sócio-tecnológicos e redes em países em desenvolvimento e transição, assim como promover o uso consciente e criativo de novas tecnologias por parte da sociedade civil." Atualmente, Tomas direciona a maior parte de sua energia ao Wireless Roadshow (*http://www.thewirelessroadshow.org/*), um projeto que dá suporte a parceiros da sociedade civil no mundo em desenvolvimento para o planejamento, construção e implementação de soluções sustentáveis de conectividade baseadas em um espectro de isenção de licenças, tecnologia e conhecimento abertos.

- **Gina Kupfermann** faz sua graduação de engenharia em gestão de energia e é graduada em engenharia e negócios. Além de seu trabalho com controladoria financeira, ela tem trabalhado com vários projetos comunitários auto-organizados e organizações sem fins lucrativos. Desde 2005, ela é membro da diretoria executiva da associação de desenvolvimento de redes livres, a entidade legal de *freifunk.net*.

- **Adam Messer.** Originalmente treinado como um entomologista (cientista de insetos), Adam Messer metamorfoseou-se em um profissional de telecomunicações, depois de uma conversa ao acaso que, em 1995, levou-o a criar o primeiro provedor de acesso à Internet na África. Pioneiro em serviços de redes de dados sem fio na Tanzânia, Messer trabalhou por 11 anos nas regiões leste e sul da África, com comunicação de voz e dados para novas empresas e operadoras multinacionais de celulares. Atualmente, reside em Amã, na Jordânia.

- **Juergen Neumann** *(http://www.ergomedia.de/)* começou a trabalhar com tecnologia da informação em 1984 e, desde então, tem buscado maneiras de implantar essa tecnologia de forma útil para organizações e a sociedade. Como consultor estratégico e de implantação de tecnologias de informação, ele tem trabalhado para as principais empresas alemãs e internacionais e muitos projetos sem fins lucrativos. Em 2002, foi co-fundador de *www.freifunk.net*, uma campanha para disseminar conhecimento e uma rede social sobre redes livres e abertas. Freifunk é reconhecida mundialmente como um dos projetos comunitários de maior sucesso nesta área.

- **Ermano Pietrosemolli** tem mestrado em telecomunicações pela Universidade de Stanford. Tem se envolvido com o planejamento e construção de redes de computadores nos últimos 20 anos, primeiro na Universidad de los Andes, onde é professor de telecomunicações desde 1970, e a seguir na função de presidente da Fundação Escuela Latinoamericana de Redes ("EsLaRed" *www.eslared.org.ve*). Como consultor, também expandiu suas atividades para o plano, projeto e implantação de redes de transmissão de dados na Argentina, Colômbia, Equador, Itália, Nicarágua, Peru, Uruguai, Trinidad e Venezuela onde mantém sua base na cidade de Mérica. Lecionou em cursos sobre redes sem fio também no Brasil, Índia, Quênia, México e República Dominicana. Desde 1996, colabora com o ICTP de Trieste nas atividades de formação e desenvolvimento em redes sem fio realizadas pela instituição com apoio da UIT. Esta colaboração frutífera levou a demonstrações da viabilidade de conexões Wi-Fi para distâncias de 279 km em 2006 e de 382 km em 2007.
- **Frédéric Renet** é um co-fundador da Technical Solutions at Adapted Consulting, Inc. Frédéric está envolvido com tecnologia da informação por mais de dez anos e trabalha com computadores desde sua infância. Ele começou sua carreira em TI no início dos anos 90, com um BBS (*bulletin board system*) em um modem analógico e, desde então, continuou a criar sistemas para aprimorar a comunicação entre as pessoas. Mais recentemente, Frédéric passou mais de um ano no IESC/ Geekcorps em Mali, como consultor. Nesse trabalho, ele projetou muitas soluções inovadoras para a transmissão de rádio em FM, laboratórios de computadores para escolas e sistemas de iluminação para comunidades rurais.
- **Marco Zennaro,** também conhecido por marcusgennaroz, é um engenheiro eletrônico que trabalha no ICTP em Trieste, na Itália. Ele é usuário de BBSs e rádio-amadores desde a adolescência e é muito feliz por ter unido estas duas tecnologias no campo de redes sem fio. Ele ainda usa seu *Apple Newton.*

Apoio

- **Lisa Chan** (*http://www.cowinanorange.com/*) foi a editora chefe.
- **Casey Halverson** (*http://seattlewireless.net/~casey/*) fez a revisão técnica e apresentou sugestões.
- **Jessie Heaven Lotz** *(http://jessieheavenlotz.com/)* proveu uma série de ilustrações atualizadas para esta edição.
- **Richard Lotz** *(http://greenbits.net/~rlotz/)* contribuiu com a revisão técnica e sugestões. Ele trabalha nos projetos *SeattleWireless* e gostaria de tirar seu nó (e sua casa) fora da grade (grid).
- **Joice Käfer** (*http://www.brodtec.com*) fez a revisão técnica da tradução para o português, além de contribuir com críticas e sugestões.

- **Catherine Sharp** *(http://odessablue.com/)* auxiliou na edição.
- **Lara Sobel** (*lara@hackerfriendly.com*) Projeto da capa e leiaute do livro.
- **Matt Westervelt** (*http://seattlewireless.net/~mattw/)* contribuiu com a revisão técnica e a edição. Matt é o fundador de *SeattleWireless* (*http://seattlewireless.net/*) e um evangelista para FreeNetworks em todo o mundo.

Sobre o guia de energia solar

O material para o capítulo sobre Energia Solar foi traduzido e desenvolvido por Alberto Escudero-Pascual. Em 1998, a organização Engineering without Borders (Federação Espanhola) publicou a primeira versão de um livro chamado "*Manual de Energía Solar Fotovoltaica y Cooperación al Desarrollo*". Este manual foi escrito e publicado pelos membros da ONG e especialistas do Institute of Energy Solar da Universidade Politécnica de Madri. Por um desses fatos curiosos da vida, nenhum membro da equipe editorial manteve uma cópia do documento em formato eletrônico e assim, novas edições jamais foram feitas. Passados quase dez anos daquela primeira edição, este documento é um esforço para resgatar e estender o manual.

Como parte desta operação de resgate, Alberto agradece aos coordenadores da primeira edição original e seus mentores durante os anos em que estava na Universidade: Miguel Ángel Eguido Aguilera, Mercedes Montero Bartolomé e Julio Amador. Este novo trabalho está sob a licença Creative Commons **Attribution-ShareAlike 3.0**. Esperamos que este material torne-se um ponto de partida para novas edições, incluindo novas contribuições da comunidade.

Esta segunda edição estendida do guia de energia solar recebeu contribuições valorosas de Frédéric Renet e Louise Berthilson.

Agradecimentos especiais

O núcleo da equipe agradece aos organizadores do WSFII por garantir o espaço, apoio e a ocasional largura de banda que serviu como incubadora para este projeto. Queremos agradecer especialmente a comunidade de "networkers" que, de todos os lugares, devotam tanto de seu tempo e energia na busca de concretizar a promessa de uma Internet global. Sem vocês, redes comunitárias não poderiam existir.

A publicação deste trabalho tem o apoio do International Development Research Centre do Canadá, *http://www.idrc.ca/*. Apoio adicional foi fornecido por *NetworktheWorld.org.*

Este livro é apoiado pelas seguintes organizações: Rede Gemas da Terra de Telecentros Rurais (*www.gemasdaterra.org.br*) e Center for Community Informatics of the Loyola University Maryland (*http://cci.cs.loyola.edu*).

IDRC CRDI

The Abdus Salam International Centre for Theoretical Physics

1
Por onde começar

Este livro foi criado por uma equipe de pessoas que, cada qual em seu campo, participam ativamente na constante expansão da Internet, forçando seus limites mais do que nunca havia sido feito. A popularidade massiva das redes sem fio tem feito com que o custo dos equipamentos caia contínua e rapidamente, enquanto a capacidade dos mesmos aumente de forma acelerada. Nós acreditamos que, tomando proveito desses acontecimentos, as pessoas podem finalmente começar a tomar partido na construção de sua própria infra-estrutura de comunicações. Esperamos não apenas convencê-lo de que isso é possível, mas também mostrar como nós o fizemos e dar a você a informação e as ferramentas necessárias para a criação de um projeto de rede em sua comunidade local.

Uma infra-estrutura de rede sem fio pode ser implantada com custo muito baixo, comparada a estruturas cabeadas. Mas a construção de redes sem fio é apenas parcialmente uma questão de economia financeira. Permitir às pessoas em sua comunidade local o acesso fácil e barato à informação é beneficiá-las diretamente do que a Internet pode oferecer. O acesso a uma rede global de informação traduz-se em riqueza em uma escala local, já que mais trabalho poderá ser feito em menos tempo, com menos esforço.

Desta maneira, a rede passa a ter cada vez mais valor na medida em que mais pessoas conectam-se a ela. Comunidades conectadas à Internet, com alta velocidade, têm voz no mercado global, onde transações acontecem ao redor do mundo na velocidade da luz. Pessoas conectadas em todo o mundo estão descobrindo que o acesso à Internet dá-lhes voz para a discussão de seus problemas, política e qualquer coisa importante para as suas vidas, de uma forma com a qual o telefone e a televisão simplesmente não podem competir. O que até há pouco parecia ficção científica, está tornando-se agora realidade, e esta realidade está sendo construída em redes sem fio.

Mas, mesmo sem o acesso à Internet, redes comunitárias sem fio têm um tremendo valor. Elas permitem que as pessoas colaborem em projetos através de longa distância. A comunicação através de voz, correio eletrônico e outras formas de dados pode ser feita com um custo muito baixo. Envolvendo as pessoas do local na construção da rede permite a disseminação de conhecimento e confiança na comunidade e as pessoas começam a entender a

importância de ter uma participação em sua infra-estrutura de comunicação. Acima de tudo, elas dão-se conta de que redes de comunicação são feitas de forma a permitir que as pessoas conectem-se umas com as outras.

Neste livro, nos concentraremos em tecnologias de redes sem fio de transmissão de dados na família 802.11. Uma rede desse tipo permite o tráfego de dados, voz e vídeo (assim como o tradicional tráfego de informações Internet e web), mas aqui nosso foco serão as redes de dados. Especialmente, não iremos cobrir GSM, CDMA, ou outras tecnologias de transmissão de voz sem fio, uma vez que o custo dessas tecnologias está além do alcance da maioria dos projetos comunitários.

Propósito deste livro

O principal propósito deste livro é ajudá-lo a construir tecnologia de comunicação com um custo aceitável em sua comunidade local, através do melhor uso dos recursos disponíveis. Com a utilização de equipamentos baratos, comuns, você pode construir redes de dados de alta velocidade que conectam áreas remotas, provendo acesso a redes de banda larga em áreas onde sequer a telefonia comum alcança e, no limite, permitir a sua conexão e a de seus vizinhos à Internet global. Com o uso de fornecimento local de materiais e a construção de peças por você, é possível construir redes confiáveis com um orçamento muito pequeno. E trabalhando com sua comunidade local, você poderá construir uma infra-estrutura de telecomunicações da qual todos os que participam dela podem se beneficiar.

Este livro não é um guia para configurar um cartão de rádio em seu laptop ou para escolher equipamentos para a sua rede doméstica. A ênfase aqui é a construção de uma infra-estrutura de conexões que será utilizada como a espinha-dorsal de uma ampla rede sem fio. Com este objetivo em mente, a informação aqui é apresentada a partir de diferentes perspectivas, incluindo fatores técnicos, sociais e financeiros. A extensa coleção de estudos de caso apresentam tentativas de vários grupos na construção destas redes, os recursos que estavam disponíveis a eles e os resultados finais destas tentativas.

Desde as primeiras experiências com fagulhas elétricas na virada do século passado, a comunicação sem fio é uma área de rápida evolução dentro da tecnologia de comunicação. Ainda que forneçamos exemplos específicos sobre a construção de conexões de dados de alta velocidade, as técnicas aqui descritas não têm a intenção de substituir redes cabeadas já existentes (como sistemas telefônicos ou estruturas de fibra ótica). Antes disto, estas técnicas têm a intenção de ampliar o alcance desses sistemas existentes, provendo conectividade em áreas onde a instalação de fibra ótica ou algum outro tipo físico de cabeamento seria impraticável.

Esperamos que você ache este livro útil na solução de seus desafios de comunicação.

Adequando a comunicação sem fio à sua rede atual

Caso você seja um administrador de redes, você pode estar imaginando de que forma uma comunicação sem fio pode agregar-se a sua infra-estrutura atual. Wireless pode ser utilizado de muitas maneiras, como uma simples extensão (como um cabo Ethernet de vários quilômetros) até um ponto de distribuição (como um grande hub). Aqui estão apenas alguns exemplos de como a sua rede pode beneficiar-se da tecnologia wireless.

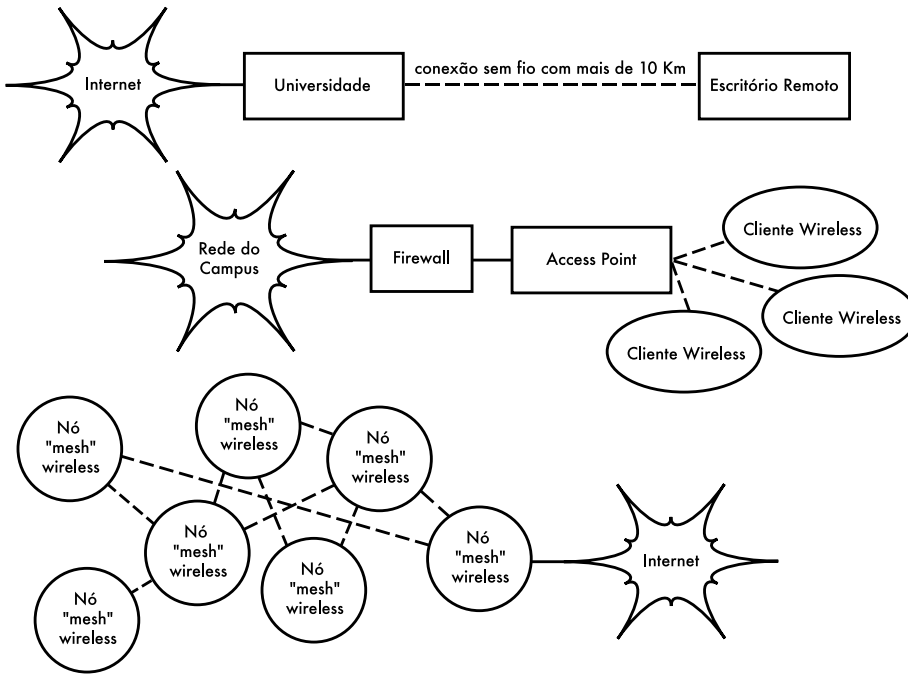


Figura 1.1: Alguns exemplos de redes wireless.

Protocolos de redes wireless

A principal tecnologia utilizada na construção de redes sem fio de baixo custo é, atualmente, a família de protocolos 802.11, também conhecida entre muitos como ***Wi-Fi***. A família 802.11 de protocolos de transmissão por rádio (802.11a, 802.11b e 802.11g) tem incrível popularidade nos Estados Unidos e Europa. Através da implementação de um conjunto comum de protocolos, os fabricantes de todo o mundo conseguiram construir equipamentos altamente interoperáveis. Esta decisão provou ser significativa para a rápida expansão da indústria e consumidores da tecnologia, que podem utilizar um equipamento que implemente o protocolo 802.11 sem temer a prisão a um determinado fornecedor. Como resultado, os consumidores são capazes de comprar

equipamentos de baixo custo em um volume que tem beneficiado os fabricantes. Caso os fabricantes tivessem optado por implementar, cada um, protocolos proprietários, as redes sem fio não seriam tão baratas e ubíquas (onipresentes) como nos dias de hoje.

Mesmo que novos protocolos, tais como o 802.16 (também conhecido como WiMax), venham a resolver alguns problemas difíceis atualmente observados com o 802.11, eles ainda têm um longo caminho a percorrer até que alcancem os pontos de popularidade de preço dos equipamentos 802.11. Como os equipamentos que suportam WiMax estão apenas começando a tornar-se disponíveis enquanto este livro é escrito, nosso foco principal se manterá na família 802.11.

São muitos os protocolos da família 802.11, nem todos diretamente relacionados ao próprio protocolo de rádio. Os três padrões wireless atualmente implementados nos equipamentos fáceis de serem encontrados são:

- **802.11b.** Aprovado pelo IEEE (Institute of Electrical and Electronics Engineers, Inc.) no dia 16 de setembro de 1999, o 802.11b é provavelmente o protocolo de rede sem fio mais utilizado atualmente. Milhões de dispositivos com suporte a ele foram vendidos desde 1999. Ele utiliza um tipo de modulação chamado ***Direct Sequence Spread Spectrum*** (DSSS - seqüência direta de espalhamento do espectro), ocupando uma porção da banda ISM (*industrial, scientific and medical*), entre 2,400 e 2,495 GHz. Possui uma capacidade máxima de transmissão de dados de 11 Mbps, com uma real utilização de cerca de 5 Mbps.

- **802.11g.** Como o protocolo ainda não havia sido totalmente finalizado até junho de 2003, o 802.11g é relativamente tardio no mercado wireless. Apesar de sua chegada atrasada, tornou-se o padrão de fato entre os protocolos de rede sem fio, uma vez que o mesmo é atualmente incluído como funcionalidade padrão em praticamente todos os computadores laptop e handheld (palmtops, por exemplo). O 802.11g utiliza o mesmo espaço de freqüência ISM que o 802.11b, mas o esquema de modulação utilizado é o ***Orthogonal Frequency Division Multiplexing*** (OFDM - multiplexação da divisão ortogonal de freqüência). Tem a capacidade de transmissão máxima de 54 Mbps (com uma utilização real aproximada de 22 Mbps) e pode diminuir para 11 Mbps DSSS ou ainda menos para a garantia da compatibilidade com o altamente popular 802.11b.

- **802.11a.** Também ratificado pelo IEEE em 16 de setembro de 1999, o 802.11a utiliza OFDM. Tem uma capacidade máxima de transmissão de 54 Mbps, com utilização real de até 27 Mbps. O 802.11a opera na banda ISM entre 5,745 e 5,805 GHz e em uma porção da banda UNII entre 5,150 e 5,320 GHz. Isto o torna incompatível com o 802.11b ou o 802.11g, e uma freqüência mais alta implica em um alcance menor, comparado com o 802.11b/g, utilizando a mesma potência. Mesmo que essa porção do espectro seja de pouco uso, comparada com a de 2,4 GHz, ela pode ser utilizada legalmente apenas em poucos lugares do mundo. Verifique a legislação vigente em seu local antes de usar equipamentos 802.11a, especialmente em aplicações externas. Os

equipamentos 802.11a ainda são baratos, mas não chegam perto da popularidade dos 802.11b/g

Adicionalmente aos padrões acima, há algumas extensões que são específicas dos fabricantes e que buscam atingir velocidades mais altas, criptografia mais forte e um maior alcance. Infelizmente, tais extensões não funcionarão entre equipamentos de diferentes fabricantes e a aquisição dos mesmos irá obrigá-lo a comprar de apenas um fornecedor específico para cada porção de sua rede. Novos equipamentos e padrões (como o 802.11y, 802.11n, 802.16, MIMO e WiMax) prometem aumentos significativos de velocidade e confiabilidade, mas estes estão apenas começando a ser fornecidos no momento da escrita deste livro e sua disponibilidade e interoperabilidade entre os diversos fabricantes ainda são uma incógnita.

Devido à ubiqüidade do equipamento e a natureza da inexistência de licenças da banda ISM 2,4 GHz, este livro irá concentrar-se na construção de redes utilizando os protocolos 802.11b e 802.11g.

Perguntas e Respostas

Caso você esteja começando a aprender sobre redes sem fio, você certamente tem uma série de perguntas sobre o que a tecnologia pode fazer e o quanto isso irá custar. Aqui estão algumas perguntas comumente feitas, com respostas e sugestões nas páginas listadas.

Energia

Como posso fornecer energia a meu equipamento de rádio, se não há uma rede de distribuição disponível? ***Página 211***

Preciso ter um cabo de energia que vá até a torre? ***Página 248***

Como posso usar um painel solar para alimentar meu nó wireless mantendo-o ativo durante a noite? ***Página 217***

Por quanto tempo meu access point (AP) funcionará com uma bateria? ***Página 236***

Posso usar um gerador eólico (movido pelo vento) para energizar meu equipamento durante a noite? ***Página 212***

Gerenciamento

Qual a largura de banda que preciso adquirir para meus usuários? ***Página 65***

Como posso monitorar e gerenciar os access points que estão localizados remotamente? ***Página 174***

O que eu faço quando há uma falha em minha rede? ***Páginas 174, 265***

Quais são os problemas mais comuns em redes sem fio e como os conserto? ***Página 265***

Distância

Qual é o alcance de meu access point? ***Página 68***

Há alguma fórmula que eu possa usar para saber a distância máxima que eu possa estar de um dado access point? ***Página 68***

Como posso saber se uma localidade remota pode ser conectada à Internet através de uma rede sem fio? ***Página 68***

Há algum software que possa ajudar-me a estimar a possibilidade de ter uma conexão wireless de longa distância? ***Página 73***

O fabricante diz que meu access point tem um alcance de 300 metros. Isto é verdade? ***Página 68***

Como posso prover conectividade wireless para muitos clientes remotos, espalhados por toda a cidade? ***Página 53***

É verdade que eu posso cobrir distâncias muito maiores adicionando uma lata ou folha de alumínio à antena de meu access point? ***Página 117***

Posso usar wireless para a conexão a um local remoto e compartilhar um único ponto de acesso à Internet? ***Página 51***

Minha conexão wireless parece muito distante para que possa funcionar bem. Posso usar um repetidor no meio do caminho para melhorá-la? ***Página 76***

Ao invés disso, devo usar um amplificador? ***Página 115***

Instalação

Como posso instalar meu access point interno em um mastro no topo de meu telhado? ***Página 247***

Devo realmente instalar um pára-raios e um aterramento apropriado para o suporte de minha antena, ou isto não é necessário? ***Página 262***

Posso construir, eu mesmo, um suporte de antena? Qual a altura que posso conseguir? ***Página 247***

Por que minha antena funciona muito melhor quando eu a monto "de lado"? ***Página 12***

Que canal devo usar? ***Página 15***

As ondas de rádio atravessam prédios e árvores? E as pessoas? ***Página 16***

As ondas de rádio atravessarão uma colina que se encontra no caminho? ***Página 20***

Como construo uma rede mesh? ***Página 56***

Que tipo de antena é a melhor para a minha rede? ***Página 102***

Posso construir um access point utilizando um PC reciclado? ***Página 145***

Como eu posso instalar Linux no meu AP? Por que eu deveria fazer isto? ***Página 153***

Dinheiro

Como posso saber se uma conexão wireless é factível dentro de um determinado orçamento? ***Página 279***

Qual o melhor AP com o menor preço? ***Página 139***

Como posso rastrear e cobrar clientes que estão utilizando minha rede wireless? ***Página 165***

Parceiros e Clientes

Uma vez que eu estou fornecendo conectividade, ainda preciso dos serviços de um provedor de acesso à Internet (ISP)? Por quê? ***Página 27***

Quantos clientes eu preciso ter para cobrir meus custos? ***Página 285***

Quantos clientes posso suportar com minha rede wireless? ***Página 65***

Como fazer com que minha rede wireless seja mais rápida? ***Página 80***

Minha conexão com a Internet é a mais rápida que pode ser? ***Página 89***

Segurança

Como posso proteger minha rede wireless de acessos não autorizados? ***Página 157***

É mesmo verdade que redes wireless são sempre inseguras e abertas a ataques por hackers? ***Página 160***

É verdade que o uso de softwares de código aberto tornam minha rede menos segura? ***Página 167***

Como posso ver o que está acontecendo em minha rede? ***Página 174***

Informação e licença

Que outros livros devo ler para aprimorar minha formação em redes sem fio? ***Página 369***

Onde posso encontrar mais informações online? ***http://wndw.net***

Posso usar partes deste livro para ministrar minhas aulas? Posso imprimir e vender cópias deste livro? Sim. Veja **Sobre este livro** para mais detalhes.

2
Uma introdução prática à rádio-física

Comunicações sem fio utilizam-se de ondas eletromagnéticas para o envio de sinais através de longas distâncias. Na perspectiva de um usuário, conexões sem fio não são particularmente diferentes de qualquer outro tipo de conexão de rede: seu navegador web, email e outras aplicações funcionarão de acordo com o esperado. Mas ondas de rádio têm algumas propriedades inesperadas se comparadas com o cabo de Ethernet. Por exemplo, é muito fácil ver o caminho que o cabo Ethernet faz: localize o conector que sai de seu computador, siga o cabo até a outra ponta e você descobriu! Você também pode ter a confiança de que ter vários cabos Ethernet lado-a-lado não causarão problemas, uma vez que os sinais são mantidos dentro dos fios.

Mas como você sabe para onde as ondas que emanam de seu cartão wireless estão indo? O que acontece quando estas ondas chocam-se com os objetos da sua sala ou com os prédios de sua conexão externa? Como vários cartões wireless podem ser usados na mesma área, sem que um interfira com o outro?

Para construir redes wireless estáveis e de alta velocidade, é importante entender como as ondas de rádio comportam-se no mundo real.

O que é uma onda?

Todos temos alguma familiaridade com vibrações e oscilações em suas várias formas: um pêndulo, uma árvore balançando ao vento, a corda de um violão - estes são exemplos de oscilações.

O que elas têm em comum é que alguma coisa, algum meio ou objeto, está "balançando" de uma maneira periódica, com um certo número de ciclos por unidade de tempo. Este tipo de oscilação é, algumas vezes, chamada de onda mecânica, uma vez que é definida pelo movimento de um objeto ou por seu meio de propagação.

Quando tais oscilações viajam (isto é, quando o "balanço" não fica preso a um único lugar) dizemos que as ondas propagam-se no espaço. Por exemplo, um cantor cria oscilações periódicas em suas cordas vocais. Estas oscilações, periodicamente,

comprimem e descomprimem o ar, e esta mudança periódica de pressão do ar deixa a boca do cantor e viaja na velocidade do som. Uma pedra atirada em um lago causa uma perturbação, que então viaja através do lago como uma **onda**.

Uma onda possui uma certa ***velocidade***, ***freqüência*** e ***comprimento de onda***. Estas propriedades estão conectadas por uma relação simples:

```
Velocidade = Freqüência * Comprimento de Onda
```

O comprimento de onda (algumas vezes chamado de lambda, **λ**) é a distância medida de um ponto em uma onda até a parte equivalente da onda seguinte. Por exemplo, do topo de um pico até o seguinte. A freqüência é o número de ondas completas que passam por um ponto fixo dentro de um período de tempo. A velocidade é medida em metros por segundo, a freqüência é medida em ciclos por segundo (ou Hertz, abreviado como ***Hz***) e o comprimento de onda é medido em metros.

Por exemplo, se uma onda na água viaja a um metro por segundo e oscila cinco vezes por segundo, então cada onda terá o comprimento de 20 centímetros (0,2 metros.):

Onde W, abaixo, é o comprimento de onda (de *wavelength*, em inglês)

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

As ondas também têm uma propriedade chamada ***amplitude***. Ela é a distância do centro da onda para o extremo de um de seus picos e pode ser visualizada como a "altura" da onda na água. A relação entre freqüência, comprimento de onda e amplitude são mostradas na **Figura 2.1**.

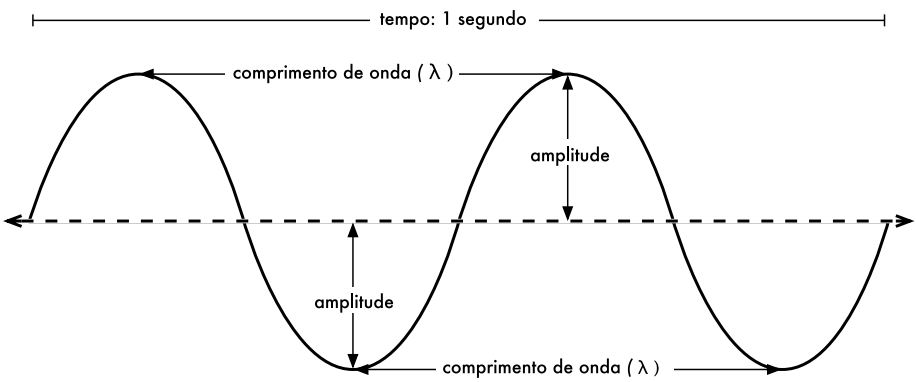


Figura 2.1: Comprimento de onda, amplitude e freqüência,
Para esta onda, a freqüência é de dois ciclos por segundo, ou 2 Hz.

Ondas na água são de fácil visualização. Simplesmente deixe cair uma pedra em um lago e você verá as ondas moverem-se através da água com o passar do tempo. No caso de ondas eletromagnéticas, a parte que provavelmente será a mais difícil de entender é: "O que está oscilando?"

Para entender isto, você precisa entender as forças eletromagnéticas.

Forças eletromagnéticas

Forças eletromagnéticas são as forças que existem entre partículas e correntes elétricas. Nosso acesso mais direto a elas é quando nossa mão toca a maçaneta de uma porta depois que caminhamos em um tapete sintético, quando levamos um choque ao tocar a porta de um carro em um dia seco ou quando nos encostamos em uma cerca eletrificada. Um exemplo mais poderoso de forças eletromagnéticas são os raios que vemos durante tempestades. A ***força elétrica*** é a força que existe entre cargas elétricas. A ***força magnética*** é a que existe entre correntes elétricas.

Elétrons são partículas que carregam uma carga elétrica negativa. Existem outras partículas, mas os elétrons são os responsáveis pela maior parte do que precisamos saber sobre como rádios comportam-se.

Vamos observar o que acontece em um pedaço de fio metálico reto, no qual forçamos os elétrons a irem e voltarem, de uma ponta a outra, periodicamente. Em um determinado momento, o topo do fio está carregado negativamente -- todos os elétrons, com sua carga negativa, estão reunidos lá. Isto cria um campo elétrico, do positivo ao negativo, ao longo do fio. No momento seguinte, todos os elétrons são forçados ao extremo oposto e o campo elétrico muda de direção. Com isto acontecendo constantemente, os vetores do campo elétrico (flechas imaginárias que apontam do positivo para o negativo) estão afastando-se do fio, por assim dizer, e estão irradiando pelo espaço ao redor do fio.

O que acabamos de descrever é conhecido como um dipolo (por causa dos dois polos, positivo e negativo) ou, mais comumente, como uma ***antena dipolo***. Esta é a forma mais simples de uma antena omnidirecional. A movimentação do campo elétrico é chamada comumente de uma ***onda eletromagnética***.

Voltemos à nossa relação:

```
Velocidade = Freqüência * Comprimento de Onda
```

No caso de ondas eletromagnéticas, a velocidade é c (velocidade da luz).

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

Ondas eletromagnéticas diferem de ondas mecânicas por não precisarem de nenhum meio de propagação. As ondas eletromagnéticas propagam-se mesmo no vácuo do espaço.

Potências de dez

Na física, matemática e engenharia, freqüentemente expressamos números como potências de dez. Nós veremos estes termos novamente, como em Giga-Hertz (GHz), Centi-metros (cm), Micro-segundos (μs), entre outros.

Potências de 10			
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	k
Mega-	10^{6}	1.000.000	M
Giga-	10^{9}	1.000.000.000	G

Conhecendo a velocidade da luz, calculamos, então, o comprimento de onda para uma dada freqüência. Tomemos como exemplo a freqüência utilizada por uma rede sem fio do tipo 802.11b, que é:

$$f = 2{,}4 \text{ GHz}$$
$$= 2.400.000.000 \text{ ciclos/segundo}$$

$$\text{comprimento de onda lambda } (\lambda) = c / f$$
$$= 3*10^{8} / 2{,}4*10^{9}$$
$$= 1{,}25*10^{-1} \text{ m}$$
$$= 12{,}5 \text{ cm}$$

A freqüência e o comprimento de onda determinam a maior parte do comportamento da onda, desde as antenas que construímos até os objetos que se encontram no caminho das redes que pretendemos implantar. Eles são responsáveis por muitas das diferenças entre os vários padrões pelos quais possamos nos decidir. Desta forma, uma compreensão das idéias básicas sobre freqüência e comprimento de onda auxiliam bastante nos trabalhos práticos que envolvem redes sem fio.

Polarização

Outra qualidade importante de ondas eletromagnéticas é a ***polarização***. A polarização descreve a direção do vetor do campo elétrico.

Se você imaginar uma antena dipolo (o pedaço reto de um fio metálico) alinhada verticalmente, os elétrons apenas movimentam-se para cima e para baixo, não horizontalmente (simplesmente porque não há espaço para que eles façam isto) e, dessa forma, os campos elétricos apenas apontam para cima ou para baixo, verticalmente. O campo deixando o fio e propagando-se como uma onda tem uma polarização estritamente linear (e, nesse caso, vertical). Caso a antena seja colocada, de forma horizontal, no chão, verificamos uma polarização linear horizontal.

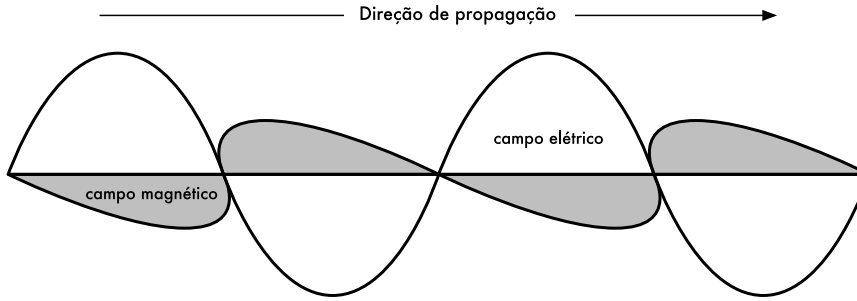


Figura 2.2: Campo elétrico e campo magnético complementar que compõem uma onda eletromagnética. A polarização descreve a orientação do campo magnético.

A polarização linear é apenas um caso especial e nunca é exatamente perfeita: geralmente, sempre teremos algum componente no campo que apontará também para outras direções. O caso mais genérico é o da polarização elíptica, com os extremos da polarização linear (apenas uma direção) e da polarização circular (em todas as direções com igual potência).

Como é possível imaginar, a polarização torna-se importante quando necessitamos alinhar antenas. Se você ignorar a polarização é possível que tenha um sinal muito fraco, mesmo usando as antenas mais potentes. Chamamos isto de ***descasamento de polarização***.

O espectro eletromagnético

Ondas eletromagnéticas existem em uma ampla variação de freqüências (e, da mesma maneira, de comprimentos de onda). Esta variação de freqüências e comprimentos de onda é chamada de ***espectro eletromagnético***. A parte deste espectro que é a mais familiar para os humanos é, provavelmente, a luz, a porção visível do espectro eletromagnético. A luz está aproximadamente entre as freqüências de $7{,}5*10^{14}$ Hz e $3{,}8*10^{14}$ Hz, correspondendo a comprimentos de onda de cerca de 400 nm (violeta/azul) até 800 nm (vermelho).

Regularmente, também estamos expostos a outras regiões do espectro eletromagnético, incluindo a ***corrente alternada*** (AC, *alternating current*, do inglês), que é a distribuição elétrica doméstica, na faixa de 50/60 Hz; Ultravioleta (ao lado das mais altas freqüências da luz visível); Raios X ou radiação Roentgen, e muitas outras. ***Rádio*** é o termo utilizado para a porção do espectro eletromagnético onde ondas podem ser geradas através da aplicação de corrente alternada em uma antena. Isto acontece dentro da variação de 3 Hz até 300 GHz, mas, em um sentido mais estrito do termo, o limite mais alto da freqüência será de 1 GHz.

Sempre que falamos de rádio, muitas pessoas pensam em rádio FM, que utiliza uma freqüência nas proximidades de 100 MHz. Entre rádio e infravermelho encontramos a região das microondas - com freqüências que variam entre 1 GHz e 300 GHz e comprimentos de onda de 30 cm a 1 mm.

O uso mais popular das microondas é em fornos de microondas que, de fato, trabalham exatamente na mesma região na qual estão os padrões wireless com os quais estamos lidando. Estas regiões estão dentro das bandas que são mantidas

abertas para o uso genérico, sem a necessidade de licenças. Esta região é chamada de banda ***ISM***, que representa *Industrial, Scientific and Medical* (em português, Industrial, Científica e Médica). A maior parte do restante do espectro eletromagnético é mantida sob rígido controle da legislação, onde as licenças de uso representam um enorme fator econômico. Isto aplica-se especialmente àquelas regiões do espectro destinadas à transmissão ampla (*broadcast*[1]) de TV e rádio, assim como às comunicações de voz e dados. Na maioria dos países, a banda ISM está reservada para o uso independente de licença.

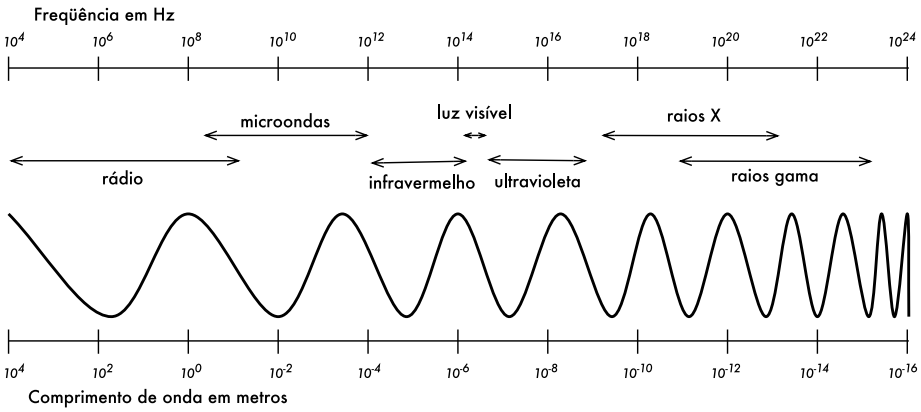


Figura 2.3: O espectro eletromagnético.

As freqüencias que mais nos interessam estão entre 2,400 e 2,495 GHz, que são utilizadas pelos padrões de rádio 802.11b e 802.11g (com o comprimento de onda correspondente de cerca de 12,5 cm). Outros equipamentos comumente disponíveis utilizam o padrão 802.11a, que opera na faixa de 5,150 a 5,850 GHz (com comprimento de onda entre 5 e 6 cm).

Largura de banda

Um termo que você encontrará com freqüência em rádio-física é ***largura de banda*** (*bandwidth*). A largura de banda é simplesmente a medida da variação de freqüência. Se uma variação entre 2,40 GHz e 2,48 GHz é usada por um dispositivo, então a largura de banda será de 0,08 GHz (ou mais comumente descrita como 80 MHz).

É fácil notar que a largura de banda que definimos aqui está intimamente relacionada com a quantidade de dados que podemos transmitir dentro dela - quanto mais espaço possível na variação da freqüência, mais dados conseguimos colocar neste espaço em um dado momento. O termo largura de banda é freqüentemente usado para algo que, preferencialmente, deveríamos chamar de capacidade de dados, como em "minha conexão com a Internet tem

1. N. do T. - O termo broadcast será amplamente usado neste texto. Ele significa a transmissão em uma única direção, de um para muitos, e tem como principal exemplo a transmissão de TV ou rádio, onde uma estação transmite para vários receptores (clientes), sem que estes tenham a capacidade de usar o mesmo meio para transmitir dados em retorno.

1 Mbps de largura de banda", significando que podemos transmitir dados a um megabit por segundo.

Freqüências e canais

Vamos olhar com mais detalhe a forma como a banda de 2,4 GHz é utilizada no 802.11b. O espectro é dividido em pedaços uniformemente distribuídos dentro da banda como ***canais*** individuais. Repare que cada canal tem a largura de 22 MHz, mas estão apenas separados por 5 MHz. Isto significa que existe intersecção entre canais adjacentes eles podem interferir um com o outro. Isto está representado visualmente na **Figura 2.4**.

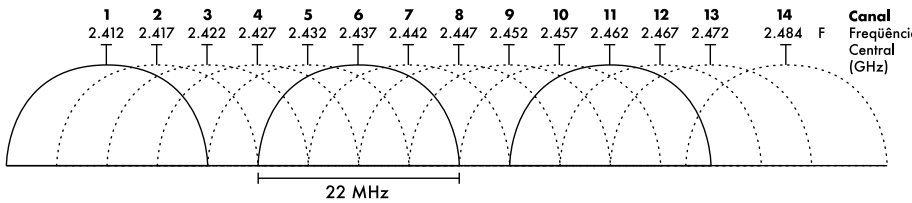


Figura 2.4: Canais e freqüências centrais para o 802.11b. Note que não há intersecções entre os canais 1, 6 e 11.

Para uma lista completa dos canais e suas freqüências centrais para o 802.11b/g e 802.11a, veja o **Apêndice B**.

Comportamento das ondas de rádio

Há uma série de regras básicas e simples que têm se provado extremamente úteis no planejamento inicial de uma rede sem fio:

- Quanto maior o comprimento de onda, maior é o alcance;
- Quanto maior o comprimento de onda, maior a facilidade com que ela atravessa e contorna as coisas;
- Quanto menor o comprimento de onda, mais dados ela pode transportar.

Todas estas regras, mesmo simplificadas desta forma, tornam-se mais fáceis de entender através de exemplos.

Ondas mais longas viajam mais longe

Assumindo níveis iguais de potência, ondas com comprimentos de onda maiores tendem a viajar mais longe do que ondas com comprimentos de ondas menores. Este efeito é freqüentemente observado em rádio FM, quando comparada a distância atingida por um transmissor nas freqüências de 88 MHz até 108 MHz. Transmissores de freqüência mais baixa tendem a cobrir distâncias muito maiores que os transmissores de freqüência mais alta, com a mesma potência.

Ondas maiores passam ao redor de obstáculos

Uma onda na água que tenha a largura de cinco metros não será impedida por um pedaço de madeira de cinco milímetros na superfície do lago. Por outro lado, se o pedaço de madeira tiver 50 metros, ou for um navio, ele certamente se interporia no caminho da onda. A distância que uma onda pode viajar depende da relação entre o comprimento de onda e o tamanho dos obstáculos no caminho de sua propagação.

É mais difícil visualizar ondas movendo-se "através" de objetos sólidos, mas isto é o que acontece com ondas eletromagnéticas. Ondas com maiores comprimentos de onda (e conseqüentemente, menor freqüência) tendem a penetrar objetos com mais facilidade que ondas com menor comprimento de onda (e, assim, maior freqüência). Por exemplo, transmissões de FM (entre 88 e 108 MHz) podem atravessar prédios e outros obstáculos facilmente, enquanto ondas mais curtas (como telefones GSM operando na freqüência de 900 MHz ou 1800 MHz) têm dificuldade de penetrar prédios. Este efeito é parcialmente devido à diferença de potência utilizada para rádios FM e GSM, mas também é devido ao menor comprimento de onda dos sinais GSM.

Ondas mais curtas carregam mais dados

Quanto mais rápido uma onda "balança", ou "bate", maior é a quantidade de informação que pode carregar - cada batida, ou ciclo, pode ser usado, por exemplo, para transportar um bit digital ('0' ou '1') ou um 'sim' ou 'não'.

Há ainda outro princípio que pode ser aplicado a todos os tipos de ondas e que é extremamente útil no entendimento da propagação das ondas de rádio. Este princípio é conhecido como o ***Princípio de Huygens***, que recebeu este nome por causa de Christiaan Huygens, um matemático, físico e astrônomo holandês que viveu entre 1629 e 1695.

Imagine que você pega uma pequena vareta e a mergulha verticalmente na superfície calma da água de um lago, fazendo com que a mesma balance e dance. As ondas vão deixar o centro da vareta - no local onde você a mergulha - em círculos. Agora, seja onde for que a água oscile e dance, as partículas vizinhas farão o mesmo: a partir de cada ponto de perturbação, uma nova onda circular terá início. Isto é, de uma forma simplificada, o princípio Huygens. Nas palavras da Wikipedia (*http://pt.wikipedia.org*):

> *O Princípio de Huygens é um método de análise aplicada aos problemas de propagação de ondas.*
>
> *Através dos escritos deixados por Huygens, pode-se perceber que cada ponto localizado na frente de onda se comporta como uma nova fonte pontual de emissão de novas ondas esféricas, que ao se somarem formarão uma nova frente de onda e assim consecutivamente.*
>
> *Segundo o próprio Huygens, "no estudo da propagação destas ondas deve-se considerar que cada partícula do meio através do qual a onda evolui não só transmite o seu movimento à partícula seguinte, ao longo da reta que parte do ponto luminoso, mas também a todas as partículas que a rodeiam e que se opõem ao movimento. O resultado é uma onda em torno de cada partícula e que a tem como centro.*

Este princípio mantém-se verdadeiro para ondas de rádio, da mesma forma que para ondas na água, assim como para o som e a luz - só que, no caso da luz, o comprimento de onda é curto demais para que seres humanos possam observar diretamente este efeito.

Este princípio nos ajudará a entender a difração, as zonas Fresnel, a necessidade de se ter uma linha visual de contato e o fato de que, algumas vezes, parece que conseguimos a capacidade de ultrapassar cantos, sem a necessidade desta linha visual.

Vamos agora observar o que acontece com as ondas eletromagnéticas na medida em que elas viajam.

Absorção

Quando ondas eletromagnéticas penetram alguma coisa, elas geralmente enfraquecem ou deixam de existir. O quanto elas perdem de potência irá depender de sua freqüência e, claro, do material que penetram. Janelas de vidro são, obviamente, transparentes para a luz, enquanto o vidro usado em óculos de sol filtram um bom bocado da intensidade da luz e também da radiação ultravioleta.

Freqüentemente, o coeficiente de absorção é usado para descrever o impacto do material na radiação. Para microondas, os dois principais materias absorventes são:

- **Metal**. Elétrons podem mover-se livremente em metais, sendo prontamente capazes de oscilar e absorver a energia de uma onda que passe por eles.
- **Água**. Microondas fazem com que as moléculas de água agitem-se, tomando parte da energia da onda[2].

Em termos práticos de redes sem fio, podemos considerar metais e água como absorventes perfeitos: as ondas de rádio não serão capazes de atravessá-los (ainda que camadas finas de água permitam que alguma energia passe por elas). Eles são, para as microondas, a mesma coisa que um muro é para a luz. Quando falamos de água, devemos lembrar que ela existe em diversas formas. Chuva, vapor, neblina, nuvens baixas, entre outras, estarão no caminho das conexões de rádio. Elas têm forte influência e, em várias circunstâncias, podem causar a perda de conexões.

Há outros materiais que têm um efeito mais complexo na absorção de ondas de rádio. Para **árvores** e **madeira**, a capacidade de absorção irá depender do quanto de água elas contêm. Madeiras velhas, mortas e secas são relativamente transparentes, uma madeira jovem e úmida será bastante absorvente.

Plásticos e similares não costumam ser absorventes, mas isto irá depender da freqüência e do tipo de material. Antes de construir algum componente com plástico (por exemplo, alguma cobertura de proteção para um equipamento de

---

2. Um mito popular é o de que a água "ressoa" na freqüência de 2,4 GHz, que é a freqüência utilizada em fornos de microondas. Na verdade, a água não tem nenhuma freqüencia de ressonância especial. As moléculas de água agitam-se na presença de ondas de rádio, aquecendo-se se esta onda tiver potência suficiente, independente de sua freqüência. Como a freqüência de 2,4 GHz não requer licença especial, ela foi simplesmente a escolha politicamente correta para o uso em fornos de microondas.

rádio e suas antenas), é conveniente medir e verificar se o material não absorve energia na freqüência de 2,4 GHz. Uma maneira simples de fazer este teste é colocar uma amostra do material em um forno de microondas por alguns minutos. Caso o material esquente, isto significa que ele absorve energia de rádio e, por isto, não poderá ser utilizado.

Finalmente, falemos sobre nós: humanos (assim como qualquer outro animal) são especialmente compostos de água. Para redes de rádio, podemos ser considerados grandes barris de água com grande capacidade de absorção. Orientar os pontos de acesso sem fio de um escritório de maneira que o sinal tenha que atravessar muitas pessoas é um grande erro. Isto também deve ser levado em conta na instalação de redes comunitárias em cafeterias, bibliotecas e outras redes externas.

Reflexão

Da mesma forma que a luz visível, as rádio-freqüências são refletidas quando entram em contato com materiais apropriados para isto: para ondas de rádio, as principais fontes de material refletor são metais e superfícies de água. As regras de reflexão são bastante simples: o ângulo em que uma onda atinge a superfície é o mesmo ângulo em que ela é refletida. Note que, do ponto de vista de uma onda de rádio, uma densa grade de barras funciona da mesma forma que uma superfície densa, desde que a distância entre as barras da grade seja pequena, comparada com o comprimento de onda. Assim, em uma freqüência de 2,4 GHz, uma grade de metal com um centímetro de espaçamento entre as barras funcionará da mesma forma que um prato metálico sólido.

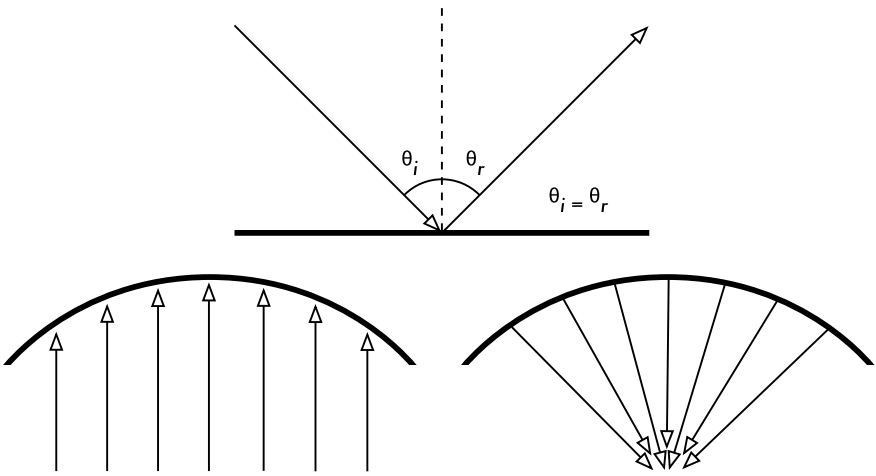


Figura 2.5: Reflexão de ondas de rádio. O ângulo de incidência é sempre igual ao ângulo de reflexão. Uma antena parabólica usa este efeito para concentrar as ondas de rádio que chocam-se em sua superfície em uma direção comum.

Ainda que as regras de reflexão sejam simples, as coisas podem se complicar quando você imagina o interior de um escritório com múltiplas e pequenas peças de metais das mais variadas formas e tamanhos. O mesmo se

aplica a situações urbanas: observe o ambiente de uma cidade e procure destacar seus componentes metálicos. Isto explica o porque de ***efeitos multicaminhos*** (isto é, o sinal chegando até o seu alvo através de caminhos diferentes e, conseqüentemente, em tempos diferentes) terem um papel tão importante em redes sem fio. Superfícies aquáticas, com ondas e oscilações mudando-as a todo o tempo, compõem superfícies refletivas que são, praticamente, impossíveis de se calcular com precisão.

Devemos ainda considerar o impacto da polarização: ondas com polarização diferente serão, geralmente, refletidas de forma diversa.

Usamos a reflexão a nosso favor quando construímos uma antena: posicionamos parábolas atrás de nosso transmissor ou receptor de rádio para coletar os sinais em um ponto ideal.

Difração

A difração é a aparente dobra das ondas quando atingem um objeto. É o efeito das "ondas que dobram esquinas".

Imagine uma onda na água que viaja diretamente para a frente, de forma similar às ondas que vemos quebrarem-se em uma praia. Agora, coloquemos uma barreira sólida, como uma cerca de madeira, de forma a bloquear esta onda. Cortamos, nesta barreira, uma passagem, como se fosse uma pequena porta. A partir desta passagem, uma onda circular terá início e atingirá, obviamente, pontos que não estão localizados em uma linha direta a partir dela. Se você olhar para esta frente de onda - que poderia ser uma onda eletromagnética - como um raio (uma linha reta), seria difícil explicar como ela atingiu pontos que deveriam estar protegidos pela barreira. Mas neste exemplo da frente de onda, e sua barreira na água, este fenômeno faz sentido.

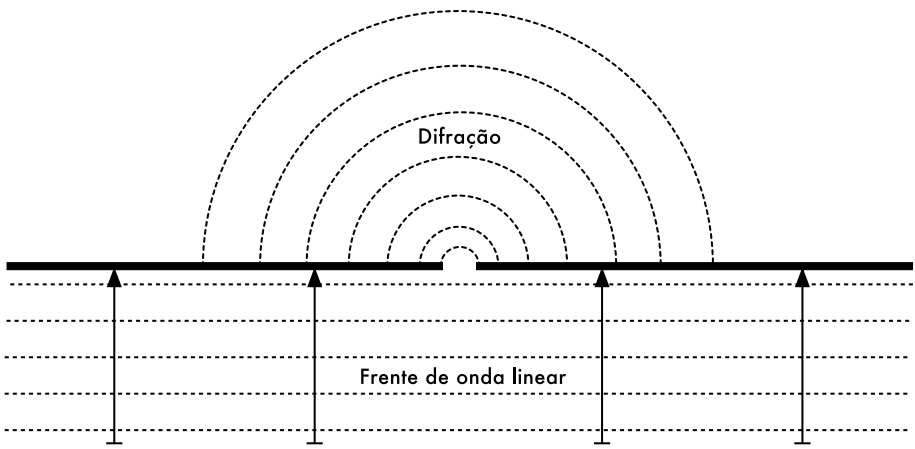


Figura 2.6: Difração através de uma abertura estreita.

O princípio de Huygens fornece um modelo para a compreensão deste comportamento. Imagine que, em qualquer dado instante, cada ponto da frente de onda seja o ponto de partida para uma "ondinha" esférica. Esta idéia foi, posteriormente, estendida por Fresnel e ainda há uma discussão se ela

descreve, adequadamente, o fenômeno. Para nosso propósito, o modelo de Huygens aplica-se relativamente bem ao efeito.

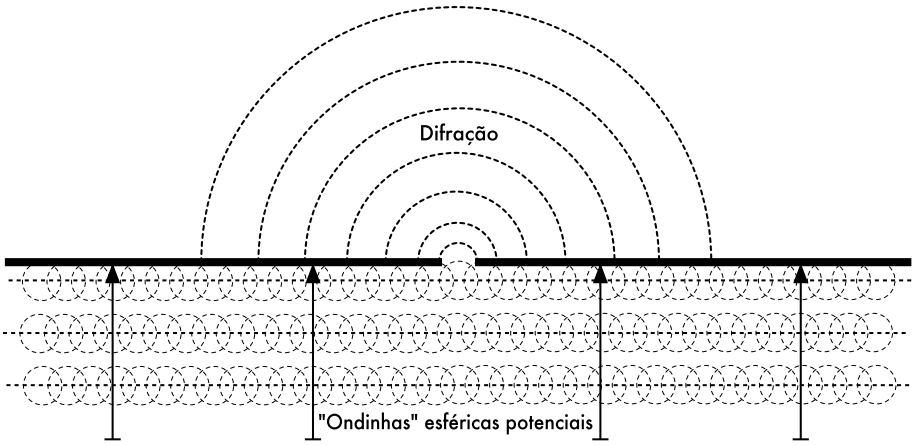


Figura 2.7: Princípio Huygens.

Por causa da difração, ondas dobram esquinas e atravessam aberturas em barreiras. O comprimento de onda da luz visível é muito pequeno para que os humanos possam observar este efeito diretamente. Microondas, com o comprimento de alguns centímetros, mostram o efeito da difração quando atingem paredes, picos de montanhas e outros obstáculos, dando a impressão de que a onda muda de direção e dobra em cantos e esquinas.

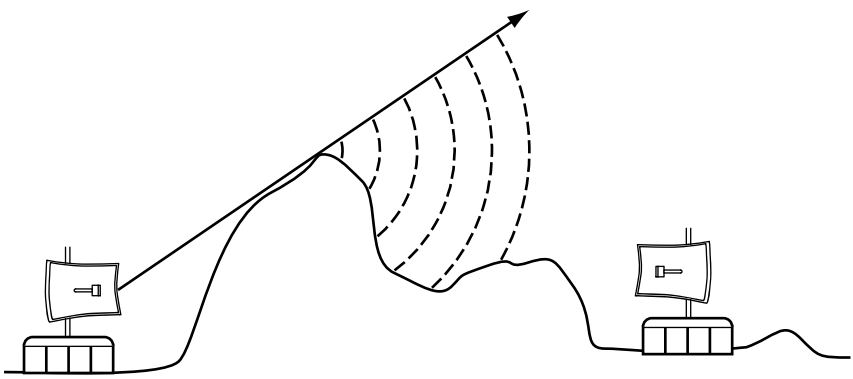


Figura 2.8: Difração sobre o topo de uma montanha.

Note que a difração ocorre ao custo de perda de potência: a energia da onda difratada é significativamente menor que a da frente de onda que a originou. Mas em algumas situações específicas você pode tomar vantagem da difração para contornar obstáculos.

Interferência

Quando trabalhamos com ondas, um mais um não é necessariamente igual a dois. O resultado pode até ser nulo.

Isto é fácil de entender quando você desenha duas ondas senoidais e soma as amplitudes. Quando os picos acontecem simultaneamente, você tem o resultado máximo (1 + 1 = 2). Isto é chamado de ***interferência construtiva***. Quando um pico acontece em conjunto com um vale, você tem a completa aniquilação (1 + (-1) =0), ou a ***interferência destrutiva***.

Você pode tentar isto na prática na superfície da água, usando duas varetas para criar ondas circulares - você verá que onde as ondas se encontram existirá áreas de picos maiores, enquanto outras ficarão praticamente calmas.

Para que trens de ondas possam ser combinados, cancelando perfeitamente um ao outro, eles necessitam ter exatamente o mesmo comprimento de onda e uma relação fixa de fase, ou seja, posições fixas entre os picos de uma onda e a outra.

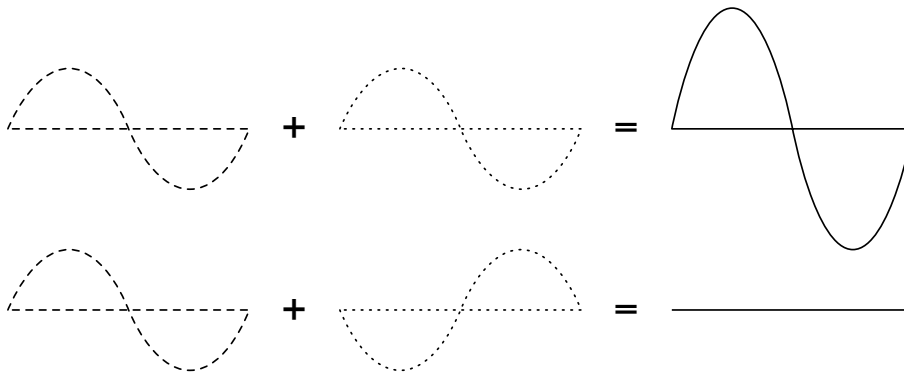


Figura 2.9: Interferência construtiva e destrutiva.

Em tecnologia wireless, a palavra interferência é, tipicamente, usada em um sentido mais amplo e diz respeito à perturbações causadas através de outras fontes de rádio-freqüência, como canais vizinhos, por exemplo. Assim, quando técnicos de redes falam sobre interferência, eles podem estar referindo-se a todo o tipo de perturbação causado por outras redes e outras fontes de microondas. A interferência é uma das principais fontes de problemas na construção de conexões sem fio, especialmente em ambientes urbanos e espaços fechados (como uma sala de conferências) onde muitas redes podem competir pelo uso do espectro.

Em qualquer lugar em que ondas de amplitudes iguais e fases opostas cruzem seus caminhos, a onda é aniquilada e nenhum sinal poderá ser recebido. O caso mais comum é o de ondas que combinam-se em uma forma de onda completamente embaralhada que não poderá ser efetivamente usada para a comunicação. As técnicas de modulação e o uso de múltiplos canais ajudam a lidar com problemas de interferência, mas não os eliminam completamente.

Linha de visão

O termo ***linha de visão***, freqüentemente abreviado por ***LOS*** (do inglês, *line of sight*), é bastante fácil de se entender quando falamos de luz visível: se conseguimos ver o ponto B a partir do ponto A, onde estamos, temos uma linha de visão. Simplesmente trace uma linha de A até B e, caso não exista nada no caminho, temos linha de visão.

As coisas complicam-se um pouco mais quando lidamos com microondas. Lembre-se que a maioria das características de propagação de ondas eletromagnéticas estão relacionadas com seu comprimento de onda. Este também é o caso para ondas que se alargam na medida em que viajam. A luz tem um comprimento de onda de cerca de 0,5 micrômetros. Microondas, como as usadas em redes wireless, tem um comprimento de onda de alguns poucos centímetros. Conseqüentemente, seus raios são bem mais largos - precisam de mais espaço, por assim dizer.

Note que raios visíveis de luz também alargam-se da mesma forma e, se você deixá-los viajar por longas distâncias, você verá os resultados independente de seu comprimento de onda. Ao apontar um laser bem focado para a lua, ele irá alargar mais de 100 metros em seu raio quando atingir a superfície. Você mesmo pode comprovar esse efeito com um apontador laser comum e binóculos em uma noite clara. Ao invés de apontar para a lua, aponte para uma montanha distante ou alguma estrutura desocupada (como uma caixa d'água). O tamanho do ponto projetado será maior quanto maior for a distância.

A linha de visão que necessitamos a fim de ter a melhor conexão sem fio entre os pontos A e B é mais do que simplesmente uma linha fina - sua forma deve ser mais parecida com a de um charuto, uma elipse. Sua largura pode ser descrita pelo conceito das zonas Fresnel.

Entendendo a zona Fresnel

A teoria exata de Fresnel é bastante complicada. O conceito, entretanto, é fácil de entender: sabemos, do princípio de Hyugens que, a cada ponto de uma frente de onda, inicia-se uma nova onda circular. Sabemos que os feixes de microondas alargam-se na medida em que se afastam da antena. Sabemos que as ondas de determinadas freqüências interferem umas com as outras. A teoria da zona Fresnel simplesmente considera a linha entre os pontos A e B em conjunto com todo o espaço no entorno dessa linha, que pode contribuir para o que chega no ponto B. Algumas ondas viajam diretamente do ponto A até o B, enquanto outras viajam em um caminho ao redor do eixo. Conseqüentemente, passa a existir um deslocamento de fase entre as ondas que trafegam em linha direta e as que se desviam do caminho. Toda a vez que o deslocamento de fase corresponde a um comprimento inteiro de onda, obtem-se uma interferência construtiva: o sinal é otimizado. Com o cálculo apropriado, você descobrirá que existem zonas ao redor da linha direta entre A e B que contribuem para o sinal chegando até o ponto B.

Note que são muitas as zonas Fresnel possíveis, mas nossa preocupação principal é com a zona 1. Caso esta área esteja particularmente bloqueada por uma obstrução, como uma árvore ou um prédio, o sinal que chega na outra

extremidade será reduzido. Quando construímos conexões sem fio, precisamos ter certeza de que estas zonas se manterão livres de obstruções. Claro, nada é sempre perfeito, então, normalmente, em redes wireless buscamos que cerca de 60% do raio da primeira zona Fresnel esteja desobstruído.

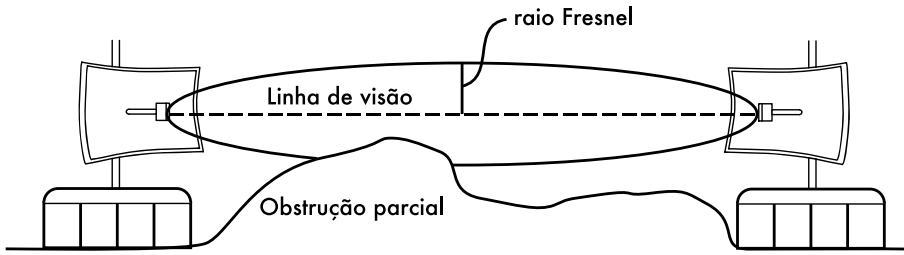


Figura 2.10: A zona Fresnel está parcialmente bloqueada nesta conexão, ainda que a linha de visão esteja clara.

Abaixo está a fórmula para o cálculo da primeira zona Fresnel:

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

onde r é o raio da zona, em metros, d1 e d2 são as distâncias, em metros, do obstáculo para cada uma das pontas da conexão, d é a distância total do link, em metros e f é a freqüência, em MHz. O resultado desta fórmula será o raio da zona, não a altura acima do chão. Para calcular a altura acima do chão você deve subtrair o resultado de uma linha traçada diretamente entre os topos das duas torres.

Como exemplo, vamos calcular o tamanho da primeira zona Fresnel no meio de um link wireless de 2 Km, transmitindo a uma freqüência de 2,437 GHz (802.11b, canal 6):

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

Assumindo que ambas as torres tenham 10 metros de altura, a primeira zona Fresnel passaria a apenas 2,16 metros sobre o chão na posição central do link. Mas qual deveria ser a altura desta estrutura para que este ponto central ainda garanta 60% de desobstrução da primeira zona?

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

Subtraindo este resultado de 10 metros, podemos ver que uma estrutura de 5,3 metros de altura a partir do centro do link iria bloquear até 40% da primeira zona Fresnel. Isto é normalmente aceitável, mas para melhorar a situação nós precisaríamos posicionar nossas antenas em uma altura ainda maior, ou mudar a direção do link para evitar o obstáculo.

Potência

Qualquer onda eletromagnética transporta energia - nós podemos sentir isto quando aproveitamos (ou sofremos com) o calor do sol. A quantidade de energia recebida em uma determinada quantidade de tempo é chamada de ***potência***. A potência **P** é de fundamental importância para que links sem fio funcionem: você precisa de uma quantidade mínima de potência para que o receptor reconheça o sinal.

Nós trataremos dos detalhes sobre potência de transmissão, perdas, ganhos e sensibilidade de rádio no **Capítulo 3**. Aqui discutiremos brevemente como a potência P é definida e medida.

O campo elétrico é medido em V/m (diferença de potencial por metro). A potência contida nele é proporcional ao quadrado da intensidade do campo elétrico:

$$P \sim E^2$$

Na prática, nós medimos a potência com o auxílio de alguma forma de receptor, por exemplo, uma antena e um voltímetro, medidor de potência, osciloscópio ou mesmo um cartão wireless e um laptop. Ao olhar diretamente para a potência do sinal, estamos olhando para o quadrado deste sinal, em Volts.

Calculando com dB

De longe, a técnica mais importante para o cálculo de potência é com o uso de ***decibéis*** (***dB***). Não há nenhuma nova física escondida aqui - é apenas um conveniente método que torna os cálculos muito mais simples.

O decibel é uma unidade sem dimensão[3], ou seja, é definida pela relação de duas medidas de potência. É definido como:

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

onde **P1** e **P0** podem ser quaisquer dois valores que você deseja comparar. Tipicamente, em nosso caso, serão duas quantidades de potência.

Porque os decibéis são tão práticos de usar? Muitos fenômenos na natureza comportam-se de uma forma que chamamos exponencial. Por exemplo, o ouvido humano percebe um som como duas vezes mais alto que outro apenas quando este é dez vezes, fisicamente, mais forte que o primeiro sinal.

Outro exemplo, bastante próximo ao nosso campo de interesse, é a absorção. Suponha que uma parede esteja no caminho de nossa conexão wireless, e que a cada metro de parede percamos metade do sinal disponível.

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

Este é o comportamento exponencial.

---

3. Outro exemplo de uma unidade sem dimensão é o percentual (%), também usado em todos os tipos de quantidades ou números. Enquanto unidades como metros e gramas são fixos, unidades sem dimensão representam uma comparação, uma relação entre valores.

Uma vez que utilizemos o truque da aplicação de logaritmos (log), as coisas tornam-se muito mais fáceis. Ao invés de pegar um valor na "enésima" potência, nós multiplicamos por "n". Ao invés de multiplicar valores, os adicionamos.

Aqui estão alguns valores comumente usados, que são importantes de se manter em mente:

```
 +3 dB = o dobro da potência
 -3 dB = metade da potência
+10 dB = ordem de magnitude (10 vezes a potência)
-10 dB = um décimo da potência
```

Em adição ao dB sem dimensão, há algumas definições relativas que estão baseadas em um valor base para P0 (potência de referência). Os mais importantes, para nós, são:

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

Uma ***antena isotrópica*** é uma antena hipotética que distribui potência de forma uniforme em todas as direções. Ela pode ser comparada a um dipolo, mas uma antena isotrópica perfeita não pode ser construída na realidade. O modelo isotrópico é útil para descrever o ganho relativo de potência em uma antena real.

Outra convenção comum (ainda que seja menos conveniente) para expressar a potência é em miliwatts. Aqui está a equivalência de níveis de potência expressos em miliwatts e dBm:

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

A física no mundo real

Não se preocupe se os conceitos neste capítulo pareceram muito desafiadores. O entendimento da forma como as ondas se propagam e interagem com o ambiente é um campo de estudo realmente complexo. A maior parte das pessoas acha difícil compreender fenômenos que não podem testemunhar com seus próprios olhos. Por enquanto, você deve entender que as ondas de rádio não viajam em um caminho reto e previsível. Para construir redes de comunicação confiáveis, você precisará ser capaz de calcular quanta potência será necessária para cobrir uma determinada distância e prever como as ondas viajarão por este caminho.

Há muito mais para aprender sobre a física de rádio do que teríamos espaço para colocar aqui. Para mais informações sobre esse campo em constante evolução, leia os recursos que listamos no **Apêndice A**.

3
Projeto de rede

Antes de adquirir algum equipamento ou decidir qual plataforma de hardware utilizar, você deve ter uma idéia clara da natureza de seu problema de comunicação. Provavelmente você está lendo este livro porque necessita conectar redes de computadores de forma a compartilhar recursos e, afinal, conectar-se à Internet global. O projeto de rede que você decidir implementar deve estar adequado ao problema de comunicação que você deseja resolver. Você precisa conectar um local remoto à uma ligação com a Internet no centro de seu campus? Sua rede tem a possibilidade de crescer para incorporar vários locais remotos? A maior parte dos componentes de sua rede será instalada em locais fixos, ou sua rede irá expandir para incluir centenas de laptops e outros dispositivos móveis?

Neste capítulo vamos revisar os conceitos de rede que definem o TCP/IP, a família principal de protocolos de rede utilizada na Internet. Veremos exemplos de como outras pessoas construíram suas redes wireless para resolver seus problemas de comunicação, incluindo os diagramas da estrutura essencial da rede. Finalmente, apresentaremos vários métodos comuns para garantir o fluxo eficiente da informação dentro de sua rede e também para o restante do mundo.

Entendendo redes

O nome TPC/IP refere-se a um conjunto de protocolos que permite a troca de informações na Internet global. Com o conhecimento do TCP/IP, você poderá construir redes que poderão crescer para, virtualmente, qualquer tamanho e, objetivamente, permitir que sua rede faça parte da Internet.

Caso você sinta-se confortável com os fundamentos de redes com TCP/IP (incluindo endereçamento, roteamento, switches, firewalls e roteadores), você pode ir direto para **Projetando a rede física**, na **Página 51**. Agora iremos rever os conceitos básicos de rede Internet.

Introdução

Veneza, na Itália, é uma cidade fantástica para nos perdermos. As estradas são meros caminhos que cruzam a água em centenas de lugares, nunca em

uma linha reta. Os funcionários de correio em Veneza estão entre os mais altamente treinados do mundo, cada um especializado na entrega de correspondência para apenas um ou dois dos seis *sestieri* (distritos) da cidade. Isto acontece em função do intrincado projeto dessa cidade ancestral. Muitas pessoas descobrem que saber a localização da água e do sol é muito mais útil do que tentar encontrar o nome de uma rua em um mapa.

Figura 3.1: Outro tipo de máscara de rede.

Imagine um turista que acaba de encontrar, como um suvenir, uma máscara de papel-machê, e quer enviá-la do estúdio em S. Polo, Veneza, para um escritório em Seattle, nos Estados Unidos. Isto pode parecer uma tarefa ordinária, mesmo trivial, mas vamos observar o que realmente acontece.

O artista, primeiramente, coloca a máscara em um pacote apropriado para a remessa e a endereça para o escritório em Seattle, nos Estados Unidos. Depois, a entrega a um empregado do correio, que anexa alguns formulários oficiais ao pacote e o envia para um departamento central de processamento, que lida com a remessa para localidades internacionais. Depois de vários dias, o pacote é liberado pela alfândega italiana e segue seu destino em um vôo transatlântico, chegando a uma central de processamento de importações nos Estados Unidos. Uma vez que é liberado pela alfândega americana, o pacote é enviado pra um ponto de distribuição no noroeste dos Estados Unidos e, daí, para a central de processamento dos correios de Seattle. Então, o pacote segue seu caminho em um carro de entregas que cumpre uma rota que o leva para um determinado endereço, em uma determinada rua, dentro de um determinado bairro. Um recepcionista, no escritório, aceita o pacote e o coloca na caixa de correio apropriada. Finalmente, o pacote é retirado pelo destinatário e a máscara chega a seu destino.

O recepcionista no escritório de Seattle não sabe ou sequer se importa em como se faz para chegar no sestiere de S. Polo, em Veneza. Seu trabalho é simplesmente receber os pacotes que chegam e colocá-los na caixa de correio da pessoa que irá recebê-los. De forma similar, o carteiro em Veneza não precisa preocupar-se em como chegar ao bairro correto em Seattle. Seu trabalho é pegar os pacotes de sua vizinhança local e encaminhá-los ao posto de correio mais próximo na cadeia de remessas.

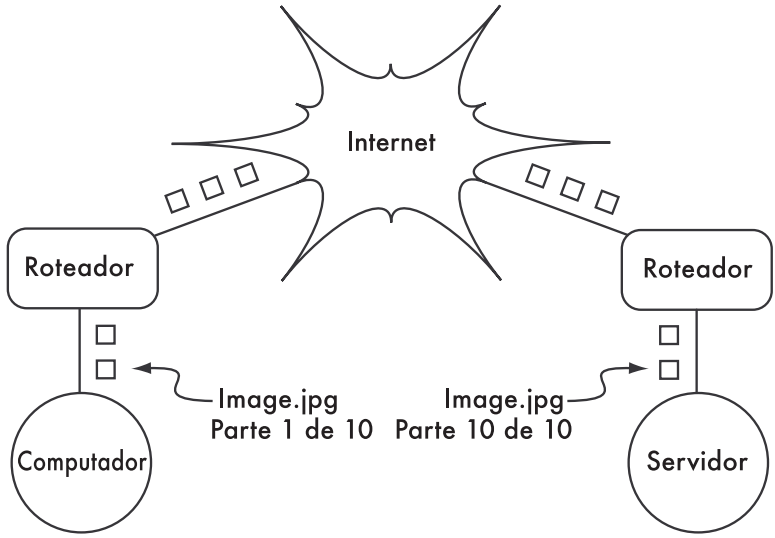


Figura 3.2: Transmissão de rede internet. Pacotes são encaminhados entre os roteadores até que atinjam seu destino final.

Isto é bastante similar à forma pela qual o roteamento na Internet funciona. Uma mensagem é dividida em uma série de ***pacotes*** individuais, que são etiquetados com seu remetente (fonte) e destinatário (ou destino). O computador envia, então, estes pacotes para um ***roteador***, que decide para onde enviá-los a seguir. O roteador apenas precisa conhecer um punhado de rotas (por exemplo, como chegar à rede local, a melhor rota para algumas outras redes locais e uma rota para o caminho de acesso—*gateway*—que conecta ao resto da Internet). Esta lista de possíveis rotas é chamada de ***tabela de roteamento*** (em inglês, *routing table*). Na medida em que os pacotes chegam ao roteador, o endereço de destino é examinado e comparado com a sua tabela de roteamento interna. Caso o roteador não tenha nenhuma rota explícita para o destino em questão, ele envia o pacote para o destino mais parecido que consiga encontrar, que é, tipicamente, o próprio gateway para a Internet (através da ***rota padrão***, ou *default route*). O próximo roteador executa o mesmo processo, e assim sucessivamente, até que o pacote chegue a seu destino.

Pacotes apenas podem seguir seu caminho pelo sistema postal internacional porque estabelecemos um esquema de endereçamento padrão para eles. Por exemplo, o endereço destino deve estar escrito de forma legível na frente do pacote e incluir toda a informação crítica (como o nome do destinatário, rua e número, cidade, estado, país e código de endereçamento postal). Sem esta informação, os pacotes são devolvidos para o remetente ou perdem-se pelo caminho.

Pacotes apenas podem trafegar pela Internet global porque foi possível chegar a um acordo sobre um esquema de endereçamento e protocolo para o encaminhamento dos mesmos. Estes protocolos de comunicação padrão permitem a troca de informação em uma escala global.

Comunicações cooperativas

A comunicação só é possível quando os participantes falam em um idioma comum. Mas quando a comunicação torna-se mais complexa que uma simples conversa entre duas pessoas, o protocolo torna-se tão importante quanto o idioma. Todas as pessoas em um auditório podem falar inglês, mas sem um conjunto de regras que estabeleçam quem tem o direito de uso do microfone, a comunicação das idéias de um indivíduo para todos os demais será praticamente impossível. Agora, imagine um auditório tão grande quanto o mundo, cheio de todos os computadores existentes. Sem um conjunto comum de protocolos de comunicação que regule quando e como cada computador pode falar, a Internet seria uma bagunça caótica onde todas as máquinas tentam falar ao mesmo tempo.

Uma série de modelos de comunicação foi desenvolvida para resolver este problema. O mais conhecido é o ***modelo OSI***.

O modelo OSI

O padrão internacional para a interconexão de sistemas abertos (OSI—Open Systems Interconection) está definido no documento ISO/IEC 7498-1, referendado pela International Standards Organization e pela International Electrotechnical Commission. O padrão completo está disponível na publicação "ISO/IEC 7498-1:1994," que pode ser encontrada em *http://standards.iso.org/ittf/PubliclyAvailableStandards/*.

O modelo OSI divide o tráfego de rede em um número de ***camadas***. Cada camada é independente das demais camadas ao redor dela e cada uma constrói, a partir dos serviços entregues pela camada inferior, novos serviços que provê para a camada superior. A abstração entre as camadas torna fácil o projeto de elaboradas e altamente confiáveis ***pilhas de protocolos*** (*protocol stacks*), como a onipresente pilha ***TCP/IP***. Uma pilha de protocolo é uma real implementação de um ambiente de rede em camadas. O modelo OSI não define qual o protocolo a ser utilizado em uma determinada rede, mas simplesmente delega quais trabalhos de comunicação são executados por cada camada, dentro de uma hierarquia bem definida.

Enquanto a especificação ISO/IEC 7498-1 detalha como as camadas devem interagir uma com as outras, ela deixa os detalhes desta implementação para os fabricantes. Cada camada pode ser implementada em hardware (comumente, as mais baixas) ou em software. Desde que a interface entre as camadas esteja de acordo com o padrão, os fabricantes estão à vontade para usar qualquer recurso disponível para construir sua pilha de protocolo. Isto significa que qualquer camada de um fabricante A pode interoperar com a mesma camada do fabricante B (desde que as especificações relevantes tenham sido interpretadas e implementadas corretamente).

Aqui está uma breve descrição das sete camadas do modelo de rede OSI:

Camada	Nome	Descrição
7	Aplicação	A ***Camada de Aplicação*** é a camada à qual a maior parte dos usuários da rede estão expostos e é o nível no qual a comunicação humana acontece. HTTP, FTP e SMTP são todos protocolos da camada de aplicação. O humano fica acima desta camada, interagindo com a aplicação.
6	Apresentação	A ***Camada de Apresentação*** é responsável por lidar com a representação dos dados, antes que eles cheguem à aplicação. Isto pode incluir a codificação MIME, compressão de dados, verificação de formatos, ordenação de bytes, etc.
5	Sessão	A ***Camada de Sessão*** gerencia as sessões de comunicação lógica entre aplicações. NetBIOS e RPC são dois exemplos de protocolo da camada cinco.
4	Transporte	A ***Camada de Transporte*** fornece um método para o acesso a um serviço específico em um dado nó da rede. Exemplos de protocolos que operam nesta camada são o TCP e o UDP. Alguns protocolos na camada de transporte (como o TCP) garantem que todos os dados cheguem ao destino, sejam rearranjados e entregues à próxima camada na ordem correta. UDP é um protocolo "*connectionless*" (sem conexão) comumente usado para a transmissão (*streaming*) de áudio e vídeo.
3	Rede	IP (o Protocolo de Internet, *Internet Protocol*) é o mais comum protocolo de ***Camada de Rede***. Esta é a camada onde o roteamento ocorre. Pacotes podem deixar a conexão de rede local e ser retransmitidos para outras redes. Roteadores executam esta função na rede tendo ao menos duas interfaces de rede, uma para cada rede que interconectam. Nós na Internet são alcançados pelo seu único, globalmente individual, endereço IP. Outro protocolo de rede crítico é o ICMP, um protocolo especial que fornece várias mensagens de gerenciamento necessárias para a correta operação do IP. Esta camada é chamada também, algumas vezes, de ***Camada de Internet***.

Camada	Nome	Descrição
2	Conexão de Dados	Sempre que dois ou mais nós compartilham o mesmo meio físico (por exemplo, vários computadores conectados em um hub, ou uma sala cheia de dispositivos wireless, todos usando o mesmo canal de rádio), eles utilizam a ***Camada de Conexão de Dados*** para comunicarem-se. Exemplos de protocolos de conexão de dados são Ethernet, Token Ring, ATM e os vários protocolos wireless (802.11 a/b/g). A comunicação nesta camada é dita link-local, uma vez que todos os nós conectados nesta camada comunicam-se, um com o outro, diretamente. Esta camada também é conhecida como ***Media Access Contro***l (***MAC***— Controle de Acesso ao Meio). Em redes modeladas com base na Ethernet, os nós são referenciados por seu ***endereço MAC***. Ele é composto de um número de 48 bits designado de forma única e individual para cada dispositivo de rede quando o mesmo é fabricado.
1	Física	A ***Camada Física*** é a mais baixa camada no modelo OSI e refere-se ao próprio meio físico no qual a comunicação ocorre. Ela pode ser um cabo de cobre de categoria 5 (***CAT 5***), um feixe de fibra ótica, ondas de rádio ou qualquer outro meio capaz de transmitir sinais. Cabos cortados, fibras quebradas e interferência de RF são exemplos de problemas da camada física.

As camadas neste modelo são numeradas de um a sete, com o sete no topo. Isto é feito para reforçar a idéia de que cada camada constrói-se acima, e depende da camada abaixo. Imagine o modelo OSI como um prédio, onde a fundação é a primeira camada, as camadas seguintes são os sucessivos andares e o telhado é a camada sete. Caso você remova qualquer uma das camadas, o prédio não se sustenta. De maneira similar, se o quarto andar está em chamas, ninguém consegue passar acima, ou abaixo dele.

As primeiras três camadas (Física, Conexão de Dados e Rede) acontecem todas "na rede". Isto quer dizer que a atividade nestas três camadas é determinada pela configuração de cabos, switches, roteadores e dispositivos similares. Um switch de rede somente pode distribuir pacotes utilizando endereços MAC, assim, ele necessita implementar apenas as camadas um e dois. Um roteador simples pode rotear pacotes utilizando apenas seus endereços IP, então ele necessita implementar as camadas um a três. Um servidor web ou um computador laptop executam aplicações, então eles devem implementar todas as sete camadas. Alguns roteadores avançados podem implementar a camada quatro e acima, permitindo que eles tomem decisões baseadas no conteúdo de alto nível de um pacote, como o nome de um website ou os anexos de um email.

O modelo OSI é reconhecido internacionalmente e é amplamente considerado como o completo e definitivo modelo de rede. Ele fornece aos fabricantes e implementadores de protocolos um ambiente para a construção de dispositivos de rede que interoperam em qualquer parte do mundo.

Pela perspectiva de um engenheiro ou analista de redes, o modelo OSI pode parecer desnecessariamente complexo. Em particular, pessoas que fazem a implementação e a análise de redes TCP/IP raramente necessitam lidar com problemas das camadas de Sessão ou Apresentação. Para a maioria das implementações de conexões de rede Internet, o modelo OSI pode ser simplificado em uma coleção menor, de cinco camadas.

O modelo TCP/IP

De maneira diversa do modelo OSI, o modelo TCP/IP não é um padrão internacional e suas definições variam. Mesmo assim, ele é freqüentemente utilizado como um modelo prático para o entendimento e diagnóstico de redes Internet. A absoluta maioria da Internet usa TCP/IP e, assim, podemos fazer algumas suposições sobre redes que as tornarão mais fáceis de entender. O modelo TCP/IP para redes descreve as quatro camadas a seguir:

Camada	Nome
5	Aplicação
4	Transporte
3	Internet
2	Conexão (link) de Dados
1	Física

Nos termos do modelo OSI, as camadas cinco a sete ficam reunidas, aqui, na camada superior (a Camada de Aplicação). As primeiras quatro camadas, em ambos os modelos, são idênticas. Muitos engenheiros de rede pensam nas camadas acima da quatro como "apenas dados" que variam de aplicação para aplicação. Uma vez que as primeiras três camadas são interoperáveis entre os equipamentos de praticamente qualquer fornecedor, a camada quatro funciona entre quaisquer computadores rodando TCP/IP e o que está acima desta camada tende a relacionar-se a aplicações específicas. Este modelo simplificado funciona bem para a construção e diagnóstico de redes TCP/IP. Usaremos o modelo TCP/IP sempre que discutirmos redes neste livro.

O modelo TCP/IP pode ser comparado com uma pessoa entregando uma carta em um edifício de escritórios no centro da cidade. Esta pessoa primeiro precisa interagir com as próprias ruas (a camada Física), prestar atenção ao tráfego nessas ruas (a camada de Conexão de Dados), virar em uma ou outra rua para chegar ao endereço correto (a camada de Internet), dirigir-se ao prédio, ao andar e ao escritório correto (a camada de Transporte) e, finalmente, entregar

a carta ao recepcionista do escritório que se encarregará dela daí em diante (a camada de Aplicação). Uma vez que a carta foi entregue ao recepcionista, a pessoa que a entregou está livre para seguir seu caminho.

As cinco camadas podem ser facilmente lembradas usando o mnemônico, em inglês, "**P**lease **D**on't **L**ook **I**n **T**he **A**ttic," que corresponde a "**P**hysical / **D**ata **L**ink / **I**nternet / **T**ransport / **A**pplication."

Uma sugestão de um mnemônico em português é: "**F**aça **C**omo **D**efinido, **I**gnorando **T**rabalhos **A**lternativos", correspondendo às camadas "**F**ísica / **C**onexão de **D**ados / **I**nternet / **T**ransporte e **A**plicação".

Os protocolos Internet

TCP/IP é a pilha de protocolos mais comumente utilizada na Internet global. A sigla significa ***Transmission Control Protocol*** (***TCP***—Protocolo de Controle de Transmissão) e ***Internet Protocol*** (***IP***—Protocolo de Internet), mas de fato refere-se a toda uma família de protocolos de comunicação relacionados. O TCP/IP é também conhecido como a ***suíte de protocolo Internet*** (*Internet Protocol suite*), e opera nas camadas três e quatro do modelo TCP/IP.

Nesta discussão, manteremos o foco na versão quatro do protocolo IP (IPv4), uma vez que este é o protocolo mais utilizado na Internet.

Endereçamento IP

Em uma rede IPv4, o endereço é um número de 32 bits, normalmente escrito como quatro números de oito bits expressos no formato decimal e separados por pontos. Exemplos de endereços IP são 10.0.17.1, 192.168.1.1 ou 172.16.5.23.

Se você escrever todos os endereços IP possíveis, eles irão variar de 0.0.0.0 a 255.255.255.255. Isto leva a um total de mais de quatro bilhões de possíveis endereços IP (255 x 255 x 255 x 255 = 4.228.250.625), ainda que alguns deles estejam reservados para funções especiais e não sejam designados a servidores. Cada um dos endereços IP utilizáveis é um identificador único, que distingue um nó da rede de outro.

Redes interconectadas devem chegar a um acordo em um plano de endereçamento IP. Cada endereço IP deve ser único e, geralmente, não poderá ser usado em diferentes lugares na Internet ao mesmo tempo, de outra forma, os roteadores não saberiam a qual deveriam rotear seus pacotes.

Endereços IP são alocados por uma autoridade central de endereçamento, que fornece um método consistente e coerente de numeração. Isto garante que endereços duplicados não serão usados por diferentes redes. Esta autoridade designa grandes blocos de endereços consecutivos a autoridades menores, que por sua vez designam blocos menores destes endereços consecutivos para outras autoridades ou para seus clientes. Estes grupos de endereços são chamados de sub-redes, ou ***subnets***. Grandes sub redes podem ser posteriormente divididas em sub-redes menores. Um grupo de endereços relativos é chamado de um espaço de endereçamento, ou ***address space***.

Subredes

Aplicando uma máscara de sub-rede (***subnet mask***, também chamada de ***network mask*** ou simplesmente ***netmask***) a um endereço IP, você consegue definir logicamente tanto o servidor (host) quanto a rede a qual ele pertence. Tradicionalmente, máscaras de sub-rede são expressas utilizando-se o formato decimal, de forma similar a um endereço IP. Por exemplo, 255.255.255.0 é uma máscara de rede comum. Você irá se deparar com este tipo de notação quando estiver configurando interfaces de rede, criando rotas, etc. Entretanto, máscaras de sub redes são expressas de forma mais sucinta utilizando a ***notação CIDR***, que simplesmente enumera o número de bits em uma máscara após uma barra (/). Assim, 255.255.255.0 pode ser simplificada como /24. CIDR é a abreviatura de ***Classless Inter-Domain Routing*** (roteamento inter-domínios sem classe), e está definido no RFC1518[1].

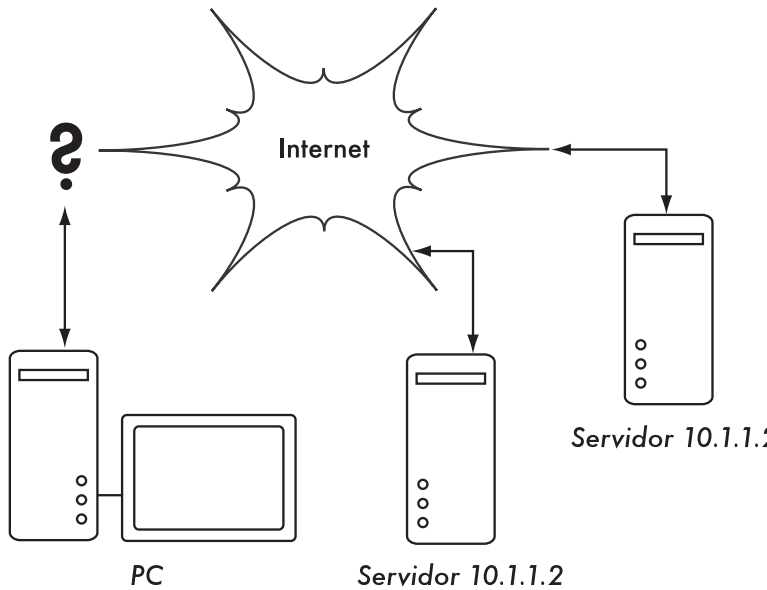


Figura 3.3: Sem que exista um único endereço IP, a não ambigüidade global de roteamento é impossível. Se um PC solicita uma página web do servidor 10.1.1.2, em qual servidor chegará?

Uma máscara de sub-rede define o tamanho de uma determinada rede. Por exemplo, em uma máscara do tipo /24, 8 bits são reservados para servidores (32 bits no total—24 bits da máscara de rede = 8 bits para hosts). Isto permite um total de 256 endereços de servidores (2^8=256). Por convenção, o primeiro valor é reservado para o ***endereço da rede*** (*network address*, .0 ou 00000000), e o

1. RFC é a abreviatura de *Request For Comments* (Solicitação de Comentários). Os RFCs são uma série numerada de documentos publicados pela Internet Society, que registram idéias e conceitos relacionados a tecnologias de Internet. Nem todos os RFCs são, de fato, padrões. Os RFCs estão disponíveis online em *http://rfc.net/*

último valor é definido como o ***endereço de broadcast*** (.255 ou 11111111). Isto deixa 254 endereços disponíveis para os servidores desta rede.

Máscaras de sub-rede trabalham com a aplicação da operação lógica AND (E) a um número IP de 32 bits. Em notação binária, os bits "1" na máscara indicam a porção do endereço de rede, e os bits "0" indicam a porção de endereço do servidor. Uma operação lógica AND é feita comparando dois bits. O resultado é "1" se os dois bits comparados são, ambos, "1". Caso contrário, o resultado é "0". Aqui estão todos os possíveis resultados de uma comparação com a operação AND entre dois bits.

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

Para entender como uma máscara de sub-rede é aplicada a um endereço IP, primeiro converta todos os números para seu equivalente em base binária. A máscara 255.255.255.0 em binário contém 24 bits "1".

```
     255.     255.     255.       0
11111111.11111111.11111111.00000000
```

Quando esta máscara é combinada com um endereço IP 10.10.10.10, podemos aplicar uma operação lógica AND para cada um dos bits, a fim de determinar o endereço da rede.

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

Isto resulta na rede 10.10.10.0/24. Esta rede consiste de servidores cujo endereço IP varia de 10.10.10.1 até 10.10.10.254, com 10.10.10.0 como o endereço da rede e 10.10.10.255 como o endereço de broadcast.

Máscaras de sub-rede não estão limitadas a octetos inteiros. É possível especificar máscaras como 255.254.0.0 (ou /15 CIDR). Este é um grande bloco, contendo 131.072 endereços, de 10.0.0.0 até 10.1.255.255. Ele pode ser posteriormente subdividido, por exemplo, em 512 sub-redes de 256 endereços cada. A primeira teria os endereços entre 10.0.0.0 e 10.0.0.255, a seguinte entre 10.0.1.0 e 10.0.1.255, e assim sucessivamente até chegar a 10.1.255.0 e 10.1.255.255. Alternativamente, ela poderia ser dividida em dois blocos de 65.536 endereços, ou 8192 blocos de 16 endereços, ou ainda de muitas outras maneiras. Ela poderia até ser dividida em uma mescla de blocos de endereços

de diferentes tamanhos, desde que eles não tenham intersecções entre si e cada um tenha uma sub-rede válida, com o número de endereços representado por uma potência de dois.

Mesmo que muitas máscaras de rede sejam possíveis, os tipos comuns incluem:

CIDR	Decimal	Número de Hosts
/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

A cada redução do valor CIDR, o espaço de endereço IP é dobrado. Lembre-se que dois endereços IP dentro de cada rede sempre estão reservados para o endereço da rede e o de broadcast.

Três máscaras comuns têm nomenclatura especial. Uma rede /8 (com uma máscara de rede de 255.0.0.0) define uma rede ***Classe A***. Uma /16 (255.255.0.0) é uma ***Classe B*** e uma /24 (255.255.255.0) é chamada de ***Classe C***. Estes nomes já eram usados muito antes da notação CIDR, mas seguem em uso por questões históricas.

Endereçamento IP global

Você já se perguntou quem controla a distribuição de endereços IP? ***Endereços IP roteáveis globalmente*** (*Globally routable IP addresses*) são atribuídos e distribuídos por ***Registradores Regionais de Internet*** (*Regional Internet Registrars—**RIR**s*) para provedores de acesso à Internet (*Internet Services Providers—**ISP**s*). Um ISP irá alocar blocos menores de endereços IP para seus clientes quando solicitados. Praticamente todos os usuários da Internet obtêm seus endereços IP de um ISP.

Os quatro bilhões de endereços IP disponíveis são administrados pela ***Internet Assigned Numbers Authority*** (***IANA***, *http://www.iana.org/*). A IANA dividiu este espaço em grandes subnets, usualmente do tipo /8, com 16 milhões de endereços cada. Estas subnets são delegadas para uma das cinco registradoras regionais de Internet (RIRs), para as quais é dada a autoridade sobre grandes áreas geográficas.

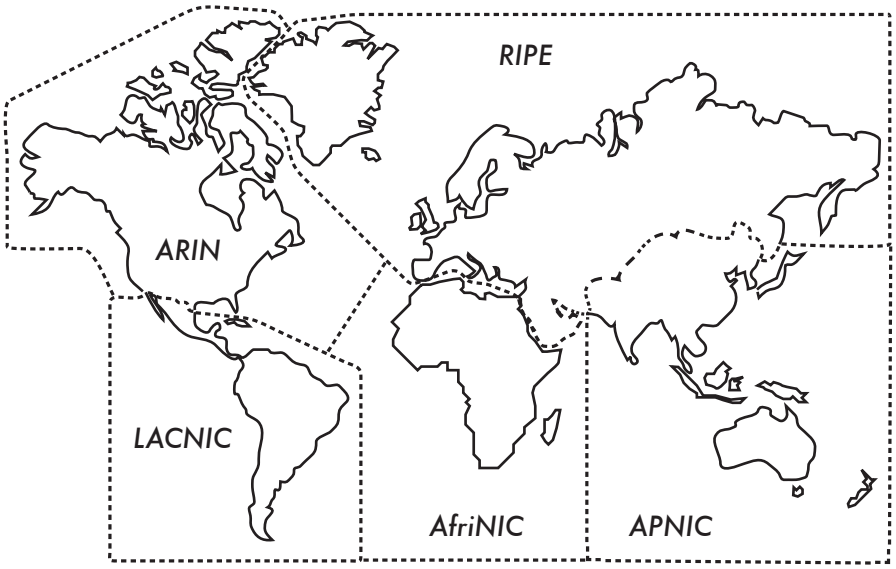


Figura 3.4: Autoridade para a designação de endereços IP é delegada aos cinco Regional Internet Registrars.

Os cinco RIRs são:

- African Network Information Centre (AfriNIC, *http://www.afrinic.net/*)
- Asia Pacific Network Information Centre (APNIC*, http://www.apnic.net/*)
- American Registry for Internet Numbers (ARIN, *http://www.arin.net/*)
- Regional Latin-American and Caribbean IP Address Registry (LACNIC, *http://www.lacnic.net/*)
- Réseaux IP Européens (RIPE NCC, *http://www.ripe.net/*)

Seu provedor de acesso irá fornecer-lhe um espaço de endereços IP roteáveis globalmente, que vem do conjunto de endereços alocado a ele pelo RIR correspondente. O sistema de registro garante que os endereços IP não serão reutilizados em nenhum local da rede, em todo o mundo.

Uma vez que há uma concordância na destinação de endereços IP, é possível transportar pacotes entre as redes e participar da Internet global. Este processo de mover pacotes entre redes é chamado de ***roteamento***.

Endereços IP estáticos

Um endereço IP estático é uma alocação de endereço que nunca muda. Endereços IP estáticos são importantes pois os servidores que usam estes endereços podem ter mapeamentos de DNS apontados para eles e, tipicamente,

eles fornecem informações para outras máquinas (como serviços de email, servidores web, etc.).

Blocos de endereços IP estáticos podem ser disponibilizados por seu provedor de acesso, tanto mediante uma requisição ou automaticamente, dependendo da maneira pela qual você conecta-se à Internet.

Endereços IP Dinâmicos

Endereços IP dinâmicos são atribuídos por um provedor de acesso à Internet para conexões que não são nós permanentes para a Internet, como um computador doméstico que utiliza uma conexão discada.

Endereços IP dinâmicos podem ser atribuídos automaticamente através do protocolo de configuração dinâmica do servidor, o ***Dynamic Host Configuration Protocol*** (***DHCP***) ou do protocolo ponto-a-ponto, ***Point-to-Point Protocol*** (***PPP***), dependendo do tipo de conexão à Internet. Um nó que utiliza DHCP primeiramente solicita um endereço IP da rede e, automaticamente, configura sua interface para o acesso. Endereços IP podem ser atribuídos de forma aleatória, a partir de um conjunto de endereços possíveis, pelo provedor de acesso, ou podem ser atribuídos de acordo com determinada política. Endereços IP atribuídos por DHCP são válidos por um período de tempo (chamado de ***lease time***, tempo de "empréstimo"). O nó deve renovar seu "empréstimo" de DHCP antes que o lease time expire. No momento da renovação, o nó pode receber o mesmo endereço IP ou outro diferente, vindo do conjunto de endereços disponíveis.

Endereços dinâmicos são populares entre os provedores de acesso à Internet, pois esta técnica permite que eles usem endereços IP em menor quantidade do que o número de seus clientes. Eles precisam de um endereço para cada ***cliente ativo em um dado momento***. Endereços IP globalmente roteáveis custam dinheiro, e algumas autoridades que são especializadas na atribuição de endereços (como a RIPE, a RIR da Europa) são bastante estritos na entrega de endereços de IP para provedores de acesso. A atribuição dinâmica de endereços permite economia aos provedores de acesso, e eles tipicamente irão cobrar um valor adicional para oferecer um endereço IP estático a seus clientes.

Endereço IP privado

Muitas redes privadas, em empresas, não necessitam alocar, para todos os seus computadores, endereços IP que possam ser globalmente roteados ou que estejam públicos para a Internet. Particularmente, computadores que não são servidores públicos não precisam estar visíveis na Internet. As empresas normalmente utilizam endereços IP do espaço de endereços privados (***private address space***) para máquinas de sua rede interna.

Existem, atualmente, três blocos de espaços de endereços privados reservados pela IANA: 10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16. Eles estão definidos no RFC1918. Estes endereços não são destinados ao roteamento na Internet e são, tipicamente, únicos apenas dentro de uma organização ou agrupamento de organizações que escolherem utilizar um mesmo esquema de endereçamento.

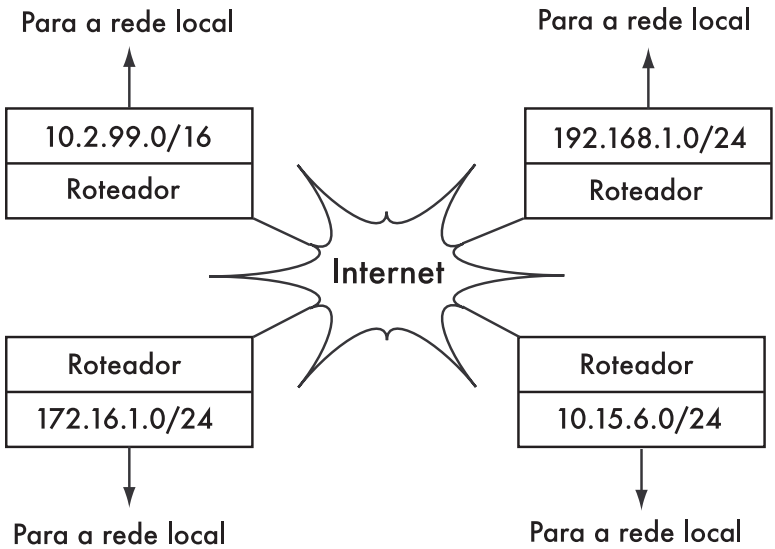


Figura 3.5: Conforme o RFC1918, endereços privados podem ser usados dentro de uma organização e não serão roteados na Internet global.

Caso você pretenda conectar redes privadas que usam o espaço de endereços do RFC1918, certifique-se de que estará usando endereços únicos em todas as redes em questão. Por exemplo, você pode dividir o espaço de endereços 10.0.0.0/8 em múltiplas redes Classe B (10.1.0.0/16, 10.2.0.0/16, etc.). Um bloco pode ser designado para cada rede, de acordo com sua localização física (a sede do campus da Universidade, o primeiro escritório remoto, o segundo escritório remoto, casa do estudante e assim por diante). Os administradores de rede em cada localização podem ainda subdividir a rede em múltiplas sub-redes Classe C (10.1.1.0/24, 10.1.2.0/24, etc.) ou em blocos de qualquer outro tamanho lógico. Assim, caso todas estas redes venham a ser conectadas no futuro (seja por uma conexão cabeada, wireless ou VPN), todas as máquinas poderão ser acessadas de qualquer ponto da rede sem a necessidade de rearranjo de endereços.

Alguns provedores de acesso podem alocar endereços privados como os descritos, ao invés de endereços públicos, a seus clientes, ainda que isto traga sérias desvantagens. Uma vez que estes endereços não podem ser roteados na Internet, os computadores que os usam não são realmente "parte" da Internet, não podendo ser acessados através dela. Para que eles possam comunicar-se com a Internet, seus endereços privados devem ser traduzidos para endereços públicos. Este processo de tradução é conhecido por Tradução de Endereço de Rede (Network Address Translation—NAT), e é normalmente feito pelo gateway entre a rede privada e a Internet. Estudaremos o NAT com mais detalhe na **Página 44**.

Roteamento

Imagine uma rede com três servidores: A, B e C. Eles usam os respectivos endereços IP: 192.168.1.1, 192.168.1.2 e 192.168.1.3. Estes servidores são parte de uma rede /24 (sua máscara é 255.255.255.0).

Para que dois servidores comuniquem-se em uma rede local, eles devem conhecer o endereço MAC um do outro. É possível configurar manualmente cada servidor com uma tabela de mapeamento entre endereços IP e MAC, mas o protocolo de resolução de endereço (***Address Resolution Protocol—ARP***) é normalmente usado para fazer automaticamente esta tarefa.

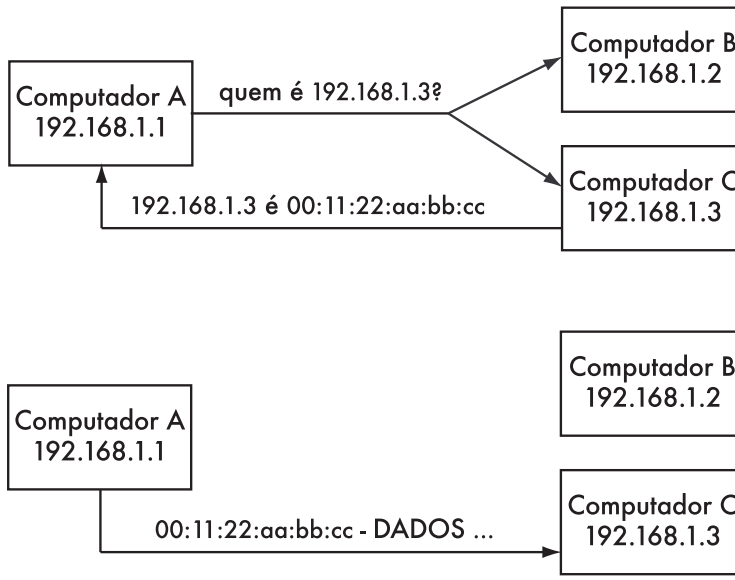


Figura 3.6: O computador A necessita enviar dados para o endereço 192.168.1.3. Mas antes disto, ele deve primeiro perguntar a toda a rede qual é o MAC address que responde pelo endereço 192.168.1.3.

Através da utilização do ARP, o computador A envia uma mensagem geral (broadcast) para todos os demais computadores: "Quem possui o endereço MAC para o IP 192.168.1.3?". Quando o computador C vê a solicitação ARP para o seu próprio endereço IP, ele responde com o seu endereço MAC.

Considere agora outra rede com três hosts: D, E e F, com os respectivos endereços IP 192.168.2.1, 192.168.2.2 e 192.168.2.3. Esta é mais uma rede /24, mas em um espaço de endereços diferente da rede acima. Todos os três hosts conseguem comunicar-se diretamente (primeiro utilizando o ARP para traduzir os endereços IP em endereços MAC, e depois enviando pacotes para o endereço MAC).

Agora vamos adicionar o host G. Este computador tem dois cartões de rede, cada um conectado a uma rede. O primeiro cartão de rede usa o endereço 192.168.1.4 e o outro o 192.168.2.4. O host G é agora um link local para ambas as redes, e pode rotear pacotes entre elas.

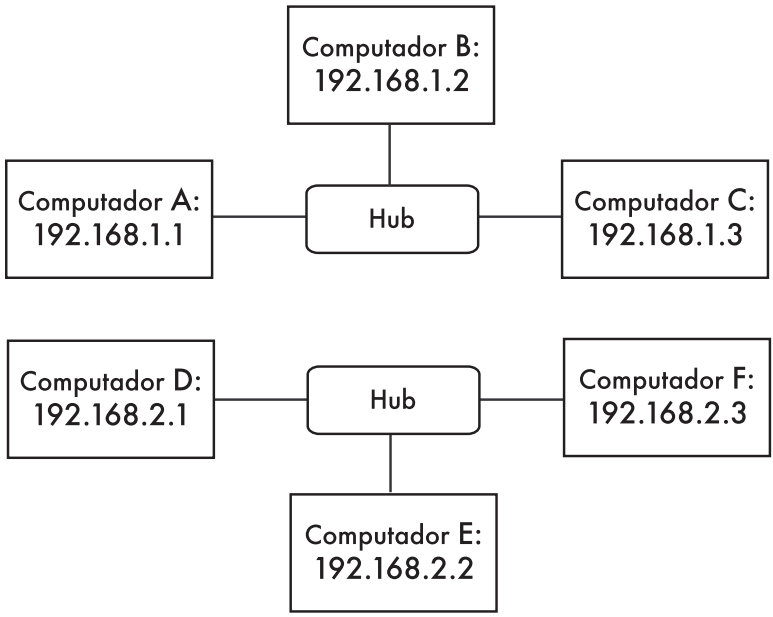


Figura 3.7: Duas redes IP separadas.

Mas como os hosts A, B e C podem comunicar-se com os hosts D, E e F? Eles necessitarão adicionar uma rota para a outra rede através do host G. Por exemplo, os hosts A-C adicionariam uma rota via 192.168.1.4. No Linux, isso é feito com o seguinte comando:

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

... e os hosts D-F adicionariam o seguinte:

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

O resultado é mostrado na **Figura 3.8**. Note que a rota é adicionada através do endereço IP no host G, que é o link local para a respectiva rede. O host A não poderia adicionar a rota via 192.168.2.4, mesmo que seja, fisicamente, a mesma máquina que 192.168.1.4 (host G), uma vez que este IP não é um link local.

Uma rota diz ao sistema operacional que a rede desejada não reside no link local imediato e deve ***encaminhar*** o tráfego através do roteador especificado. Se o host A quiser enviar um pacote ao host F, ele precisará, primeiro, enviá-lo ao host G. O host G irá, então, procurar pelo host F em sua tabela de roteamento, verificando que ele tem uma conexão direta para a rede do host F. Finalmente, o host G irá descobrir o endereço de hardware (MAC) do host F e encaminhar a ele o pacote.

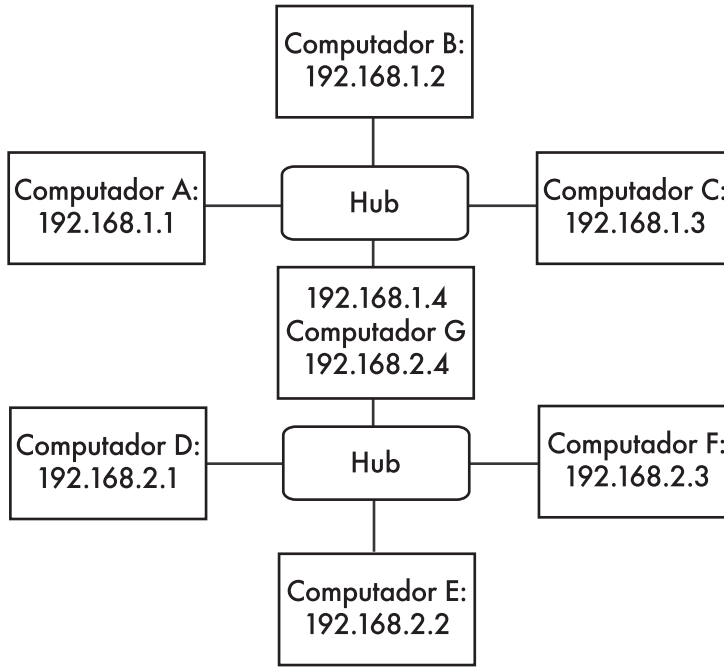
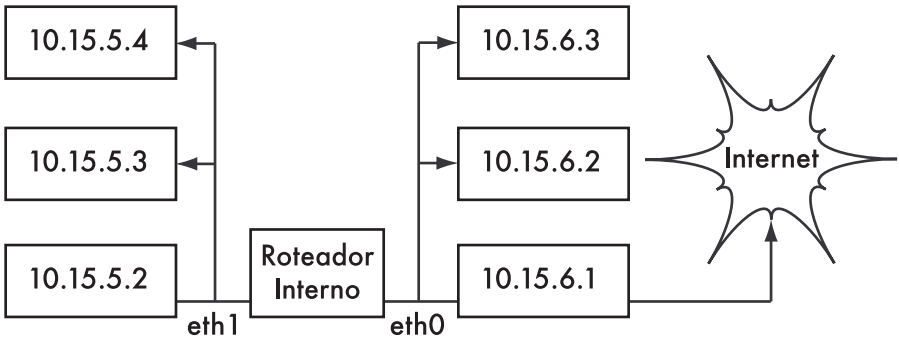


Figura 3.8: O host G atua como um roteador entre as duas redes.

Este é um exemplo muito simples de roteamento, onde o destino está apenas um intermediário (***hop***) distante da fonte. Conforme as redes tornam-se mais complexas, muitos hops precisam ser atravessados para que o destino final seja alcançado. Uma vez que não é prático, para cada máquina na Internet, conhecer a rota para cada uma das demais, fazemos uso de uma diretiva de roteamento conhecida por ***rota padrão*** (***default route***, ou ***default gateway***). Quando um roteador recebe um pacote destinado a uma rede para a qual não há uma rota específica, o pacote é encaminhado para a sua rota padrão.

A rota padrão é, tipicamente, a melhor rota de saída em sua rede, normalmente em direção a seu provedor de acesso à Internet. Um exemplo de roteador que usa uma rota padrão é mostrado na **Figura 3.9**.

Rotas podem ser atualizadas manualmente ou podem reagir automaticamente a quedas de rede e outros eventos. Alguns exemplos de protocolos de roteamento dinâmico são RIP, OSPF, BGP e OLSR. A configuração de rotas dinâmicas não faz parte do escopo deste livro mas, para leituras adicionais sobre o assunto, consulte os recursos do **Apêndice A**.




```
Tabela de roteamento para o roteador interno:

Destino         Roteador    MáscaraGen.    Opções Ref    Iface
10.15.5.0       *           255.255.255.0  U      0       eth1
10.15.6.0       *           255.255.255.0  U      0       eth0
default         10.15.6.1   0.0.0.0        UG     0       eth0
```

Figura 3.9: Quando não há rota explícita para um destino em particular, um computador deve usar a rota padrão definida em sua tabela de roteamento.

Network Address Translation (NAT)

Para que se possa acessar servidores na Internet, os endereços IP do tipo RFC1918 devem ser convertidos para endereços IP globais, publicamente roteáveis na Internet. Isto é possível através de uma técnica conhecida como ***Network Address Translation***, ou ***NAT*** (Tradução de Endereços de Rede). Um dispositivo NAT é um roteador que modifica os endereços dos pacotes ao invés de simplesmente encaminhá-los. Em um roteador NAT, a conexão com a Internet usa um (ou mais) endereço IP globalmente roteável, enquanto a rede privada usa um endereço IP do espaço de endereços privados do RFC1918. O roteador NAT permite que endereços globais possam ser compartilhados com os usuários internos que utilizam endereços privados. Ele converte os pacotes de uma forma de endereçamento para a outra quando os pacotes passam por ele. Do ponto de vista dos usuários da rede, eles estão diretamente conectados à Internet, não necessitando de nenhum software ou driver específico. Eles simplesmente usam o roteador NAT como sua rota padrão e endereçam os pacotes como fariam normalmente. O roteador NAT traduz os pacotes que estão deixando a rede privada para que usem um endereço IP global, e os traduzem novamente para um endereço interno quando retornam.

A principal conseqüência da utilização do NAT é que as máquinas que estão na Internet não têm acesso fácil aos servidores internos à organização, a não ser que sejam configuradas regras explícitas de ***encaminhamento*** (*forwarding*) no roteador. As conexões que partem de dentro do espaço de endereços privados, porém, não têm dificuldade em acessar a Internet, ainda que algumas aplicações (como voz sobre IP e alguns softwares de VPN) tenham alguns problemas ao lidar com o NAT.

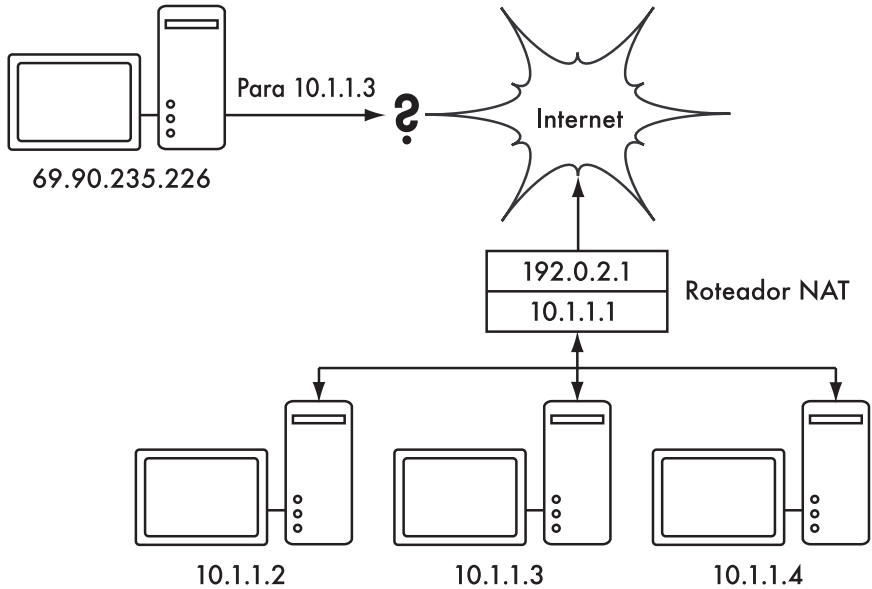


Figura 3.10: A tradução de endereços de rede (NAT) permite que você compartilhe um único endereço IP público com muitos servidores internos, mas pode dificultar o funcionamento de alguns serviços.

Dependendo de seu ponto de vista, isto pode ser considerado um defeito, um *bug* (uma vez que isto torna mais difícil a configuração de uma comunicação de mão dupla) ou um benefício, um *feature* (uma vez que, efetivamente, esta técnica implementa, sem custo adicional, um *firewall* para a sua organização inteira). Os endereços RFC1918 devem ser filtrados no limite de sua rede a fim de prevenir a entrada ou saída de tráfego RFC1918, tanto de forma acidental quanto maliciosa. Mesmo que o NAT execute algumas funções ao estilo de um firewall, ele não substitui um firewall de verdade.

A suíte de protocolos Internet

Máquinas na Internet utilizam o Internet Protocol (IP) para alcançarem umas às outras, mesmo quando estiverem separadas por máquinas intermediárias. Há mais protocolos que são usados em conjunto com o IP, provendo funções tão críticas às operações normais quanto o próprio IP. Cada pacote especifica um número de protocolo que o irá qualificar. Os protocolos mais comumente usados são o ***Transmission Control Protocol*** (***TCP***, número 6), o ***User Datagram Protocol*** (***UDP*** , número 17) e o ***Internet Control Message Protocol*** (***ICMP***, número 1). Em grupo, estes protocolos (e outros) são conhecidos como a suíte de protocolos Internet (***Internet Protocol Suite***) ou, simplesmente, ***TCP/IP***.

Os protocolos TCP e UDP introduzem o conceito de numeração de portas. Os números de portas (port numbers) permitem que vários serviços possam ser executados em um único endereço IP e, ainda assim, de forma distinta um do outro. Cada pacote tem um número de porta para a sua fonte e seu destino. Alguns números de portas são padrões bem definidos, usados para alcançar serviços bem conhecidos, como servidores de email e web. Por exemplo, um

servidor web normalmente escuta (***listen***) a porta 80, e servidores de email SMTP escutam a porta 25. Quando dizemos que um serviço "escuta" em uma porta (como a porta 80), queremos dizer que ele irá aceitar pacotes que usem seu IP como o endereço de destino, e a porta 80 como a porta de destino. Os servidores normalmente não se importam com a origem do pacote (seja seu IP ou porta), ainda que algumas vezes utilizem esta informação para estabelecer a identidade do servidor que os enviou. Ao enviar uma resposta para tais pacotes, o servidor irá usar seu próprio IP e porta como a nova origem (no caso, a porta 80).

Quando um cliente conecta-se a um serviço, ele pode utilizar como porta de origem qualquer uma, de seu lado, que não esteja sendo usada, mas deve conectar-se à porta apropriada no servidor que está provendo tal serviço (isto é, 80 para web, 25 para email). O TCP é um protocolo ***orientado à sessão*** (***session oriented***) com funções que garantem a entrega e a transmissão de pacotes (como a detecção e atenuação de congestionamento de rede, repetição de tentativas de envio, reordenação e montagem de pacotes, etc). O UDP é projetado para o fluxo de informação sem controle de conexão (***connectionless***), e não dá nenhuma garantia de entrega, ou nenhuma ordenação em particular.

O protocolo ICMP é projetado para o diagnóstico de problemas e manutenção na Internet. Ao invés de usar números de portas, ele possui tipos de mensagens (***message types***), que também são números. Diferentes tipos de mensagens são usados para solicitar uma simples resposta de um outro computador (*echo request*), notificar o remetente de uma mensagem de um possível "loop" na rota (*time exceeded*) ou informar ao remetente que um pacote não pôde ser entregue em função de regras de firewall ou outro problema (*destination unreachable*).

Até aqui você já deve ter um bom entendimento da forma como os computadores são endereçados na rede e como a informação flui entre eles. Agora, vamos dar uma rápida olhada no hardware que implementa estes protocolos de rede.

Ethernet

Ethernet é o nome do mais conhecido padrão para a conexão de computadores em uma rede local (***LAN—Local Area Network***). Ele é, algumas vezes, usado para conectar computadores individuais à Internet, através de um roteador, modem ADSL ou dispositivo wireless. Entretanto, ao conectar um único computador à Internet, pode ser que você sequer use Ethernet. O nome vem do conceito físico do éter (*ether*), o meio que foi, certa vez, considerado o responsável por carregar ondas de luz pelo espaço. O padrão oficial é chamado IEEE 802.3.

O padrão mais comum Ethernet é o 100baseT. Isto define uma taxa de transmissão de dados de 100 megabits por segundo, em um par trançado de fios, com conectores modulares RJ-45 na ponta. A topologia da rede é uma estrela, com switches ou hubs no centro da estrela e nós finais (dispositivos e switches adicionais) nas extremidades.

Endereço MAC

Cada dispositivo conectado a uma rede Ethernet tem um endereço MAC único, atribuído pelo fabricante do cartão de rede. Sua função é similar a de um endereço IP, uma vez que serve como o identificador individual que permite a um dispositivo conversar com outro. Entretanto, o escopo de um endereço MAC está limitado a um domínio de *broadcast*, definido como todos os computadores conectados fisicamente por cabos, hubs, switches e bridges, sem cruzar roteadores ou gateways de Internet. Os endereços MAC nunca são usados diretamente na Internet e não são transmitidos além dos roteadores.

Hubs

Os ***hubs*** Ethernet conectam múltiplos dispositivos Ethernet de par trançado entre si. Eles trabalham na camada física (a camada mais baixa, primeira). Eles repetem os sinais recebidos em cada porta[2] para todas as demais. Assim, os hubs podem ser considerados como simples repetidores. Em função deste projeto, apenas uma porta pode transmitir por vez. Caso dois dispositivos transmitam ao mesmo tempo, eles corrompem a transmissão um do outro, devendo ambos cancelar sua transmissão e retransmitir, posteriormente, os pacotes. Isto é conhecido como uma ***colisão*** (***collision***), e cada servidor fica responsável por detectar as colisões durante uma transmissão e pela retransmissão de seus próprios pacotes, quando necessário.

Quando um excesso de colisões é detectado em uma porta, alguns hubs podem desconectar (***partition***) tal porta por algum tempo, limitando o impacto do problema no resto da rede. Quando uma porta é desconectada, os dispositivos ligados a ela não mais podem comunicar-se com o restante da rede. Redes baseadas em hubs são, geralmente, mais robustas que as que utilizam conexões Ethernet coaxiais (também conhecidas como 10base2 ou ThinNet), onde dispositivos com problemas podem indisponibilizar todo um segmento de rede. Mas os hubs têm limitações em sua utilidade, uma vez que podem tornar-se, facilmente, pontos de congestionamento em redes de alto tráfego.

Switches

Um ***switch*** é um dispositivo que opera de forma parecida a um hub, mas que fornece uma conexão dedicada (chaveada, ***switched***) entre as suas portas. Ao invés de repetir todo o tráfego em todas as portas, o switch determina quais portas estão se comunicando diretamente e, temporariamente, as conecta. Em geral, os switches oferecem um desempenho muito melhor que os hubs, especialmente em redes de alto tráfego, com muitos computadores. Eles não são muito mais caros que os hubs e os estão substituindo em muitas situações.

Os switches trabalham na camada de comunicação de dados (a segunda camada), uma vez que eles interpretam e atuam no endereço MAC dos pacotes que recebem. Quando um pacote chega à porta de um switch, o mesmo anota a fonte do endereço MAC, que fica associado àquela porta. A informação é

---

2. N. do T. - Quando falamos em portas aqui, o leitor deve observar que elas não são do mesmo tipo daquelas a que nos referimos no protocolo TCP/IP. Aqui estamos falando de portas que correspondem ao conector físico de um hub. O mesmo ocorrerá quando falarmos em portas de um switch. Normalmente será fácil de distinguir, neste texto, a qual tipo de porta estamos nos referindo.

armazenada em uma ***MAC table*** (tabela de endereços MAC), internamente. Para cada pacote que recebe, o switch verifica qual o endereço MAC destino em sua MAC table e transmite o pacote para a porta correspondente. Caso o endereço MAC não seja encontrado na MAC table, o pacote é transmitido para todas as interfaces. Caso o endereço de destino corresponda à mesma porta pela qual ele foi enviado, o pacote é filtrado e não é encaminhado para essa porta.

Hubs versus Switches

Hubs são considerados dispositivos pouco sofisticados, uma vez que eles retransmitem, de forma ineficiente, todo o tráfego em todas as portas. Esta simplicidade leva tanto a um desempenho fraco quanto a um problema de segurança. O desempenho é fraco porque a largura de banda deve ser dividida entre todas as suas portas. Uma vez que o tráfego é visto por todas as portas, qualquer servidor na rede pode monitorá-lo integralmente.

Os switches criam conexões virtuais entre as portas que estão transmitindo e recebendo. Isto leva a um melhor desempenho porque muitas conexões virtuais podem ser estabelecidas simultaneamente. Switches mais sofisticados (e caros) podem direcionar melhor o tráfego através da inspeção dos pacotes em níveis mais altos (como as camadas de transporte e aplicação), permitindo a criação de VLANs e implementando outras funcionalidades avançadas.

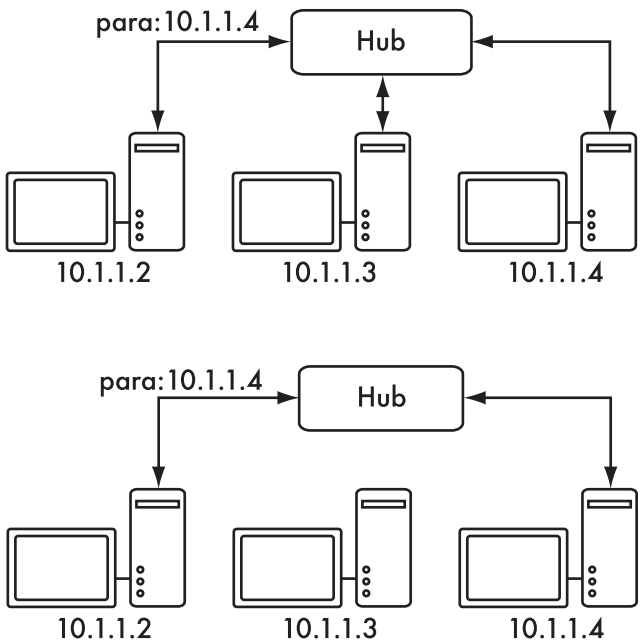


Figura 3.11: Um hub simplesmente repete todo o tráfego para todas as portas, enquanto um switch estabelece uma conexão temporária dedicada entre as portas que necessitam comunicar-se.

Um hub pode ser usado onde a repetição do tráfego em todas as portas for desejável. Por exemplo, quando, explicitamente, você permite que uma máquina

de monitoramento inspecione o tráfego de toda a rede. Muitos switches fornecem uma porta de monitoração (***monitor port***) que permite a repetição do tráfego nela, especificamente para esta função.

Os hubs são mais baratos que os switches. Entretanto, o preço dos switches caiu dramaticamente com o passar do tempo. Desta forma, os hubs de redes antigas devem ser substituídos, sempre que possível, por novos switches.

Tanto hubs como switches podem oferecer serviços gerenciados (***managed***). Alguns destes serviços incluem a habilidade de configurar a velocidade do link (10baseT, 100baseT, 1000baseT, *full* ou *half duplex*) por porta, habilitar gatilhos (*triggers*) para inspecionar eventos de rede (como mudanças de endereço MAC ou pacotes com má formação) e, usualmente, incluem bilhetagem de portas (*port counters*) para facilitar as estatísticas de utilização de banda. Um switch gerenciado que forneça informações sobre a quantidade de dados que entram ou saem de cada porta física pode simplificar bastante a gestão da rede. Estes serviços são, tipicamente, disponibilizados via SNMP, ou podem ser acessados via telnet, ssh, inteface web ou alguma ferramenta customizada de configuração.

Roteadores e firewalls

Enquanto hubs e switches fornecem conectividade para um segmento local de rede, a função de um roteador é a de encaminhar pacotes entre diferentes segmentos de rede. Um roteador, tipicamente, tem duas ou mais interfaces físicas de rede. Ele pode incluir o suporte a diferentes tipos de rede, como Ethernet, ATM, DSL ou conexão discada. Os roteadores podem ser dispositivos de hardware dedicados (como os roteadores Cisco ou Juniper) ou podem ser feitos a partir de um PC padrão, com múltiplos cartões de rede e o software apropriado.

Roteadores localizam-se no limite (***edge***) entre duas ou mais redes. Por definição, eles têm uma conexão para cada rede e, como são máquinas de fronteira, podem ter outras responsabilidades além do roteamento. Muitos roteadores executam funções de ***firewall***, provendo um mecanismo para a filtragem ou redirecionamento de pacotes que não se enquadram na política de acesso ou segurança da rede. Eles também podem fornecer serviços de tradução de endereços (NAT).

Os roteadores possuem uma variação muito grande de custo e funcionalidades. Os mais baratos e menos flexíveis são dispositivos de hardware simples e dedicados, freqüentemente com funcionalidade NAT, utilizados para compartilhar uma conexão Internet com alguns poucos computadores. O próximo passo é um roteador por software, que consiste em um sistema operacional rodando em um PC com múltiplas interfaces de rede. Sistemas operacionais padrão como o Microsoft Windows, Linux ou BSD realizam funções de roteamento e são muito mais flexíveis que os dispositivos de hardware de baixo custo. Entretanto, eles têm os mesmos problemas que os PCs convencionais: alto consumo de energia, grande e complexo número de componentes não confiáveis e maior necessidade de configuração.

Os mais caros são roteadores de hardware de alto nível, feitos por empresas como a Cisco ou a Juniper. Eles tendem a ter um desempenho muito superior, mais funcionalidade e confiabilidade muito maior que roteadores por

software implementados com PCs. Também é possível adquirir suporte técnico e ter contratos de manutenção para eles.

A maioria dos roteadores modernos oferecem mecanismos para monitorar e registrar seu desempenho remotamente, normalmente através do ***Simple Network Management Protocol*** (***SNMP***—Protocolo Simples de Gerenciamento de Rede), ainda que os dispositivos mais baratos freqüentemente omitam esta funcionalidade.

Outros equipamentos

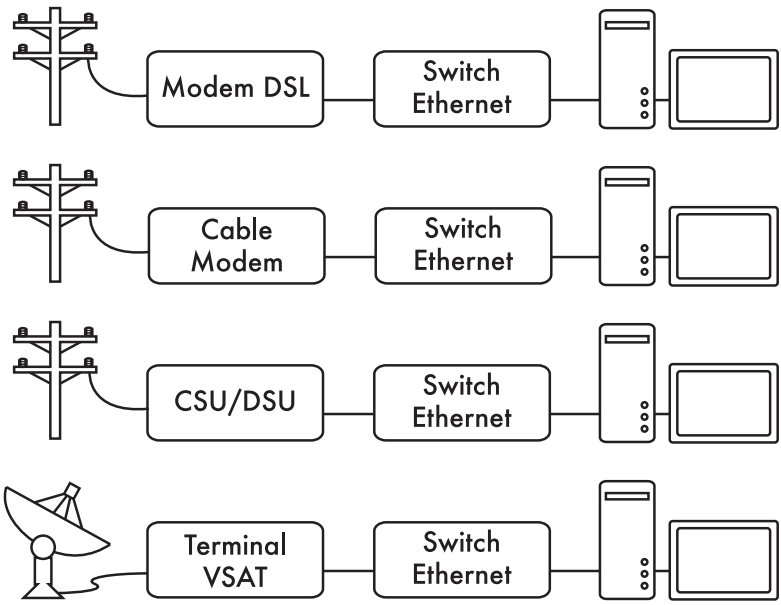


Figura 3.12: Muitos modems DSL, cable modems, CSU/DSUs, pontos de acesso wireless e terminais VSAT fornecem conexão para um cabo Ethernet.

Cada rede física possui um equipamento terminal associado. Por exemplo, conexões VSAT são compostas de um prato de satélite conectado a um terminal que, ou liga-se a uma placa dentro de um PC, ou fornece uma conexão Ethernet padrão. Linhas DSL usam um ***modem DSL*** que conecta uma linha telefônica a um dispositivo local, seja uma rede Ethernet ou um único computador via USB. ***Cable modems*** ligam um cabo de televisão à Ethernet, ou a algum tipo de cartão no PC. Alguns tipos de circuitos de telecomunicação (como T1 ou T3) usam uma CSU/DSU para a conexão com uma porta serial ou Ethernet. Linhas da rede de telefonia pública usam modems para conectar um computador ao telefone, normalmente através de um cartão interno ou uma porta serial. Existem ainda muitos tipos diferentes de equipamentos de rede sem fio que conectam-se a uma variedade de rádios e antenas, mas praticamente todos eles fornecem uma conexão para um cabo Ethernet.

Conectando todas as coisas

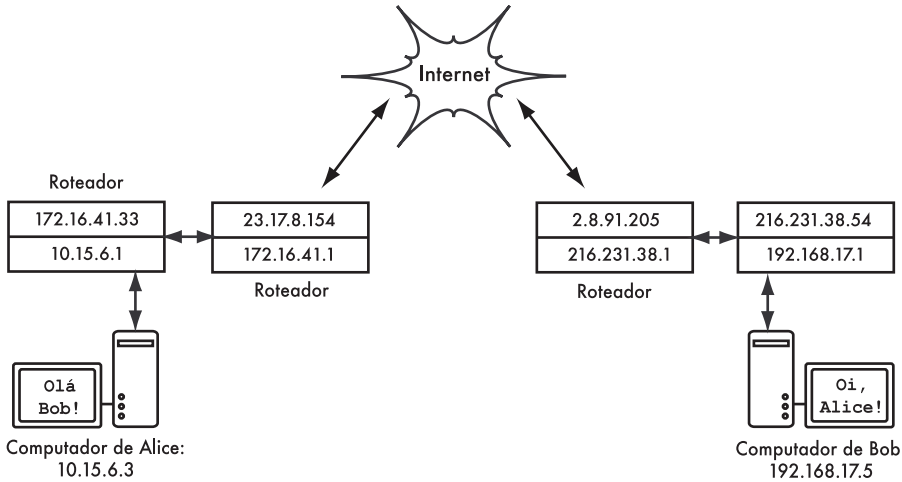


Figure 3.13: Rede Internet: Cada segmento de rede tem seu próprio roteador com dois endereços IP, fazendo seu "link local" para duas redes diferentes. Os pacotes são encaminhados entre os roteadores até que atinjam seu destino final.

Uma vez que todos os nós de rede tenham endereços IP, eles podem enviar e receber pacotes pelos endereços uns dos outros. Através de roteamento e encaminhamento, estes pacotes podem atingir redes que não estejam fisicamente conectadas ao nó que os originou. Este processo descreve muito do que acontece na Internet.

Neste exemplo, você pode ver o caminho que os pacotes percorrem quando Alice conversa com Bob através de um serviço de mensagens instantâneas. Cada linha representa um cabo Ethernet, uma conexão wireless, ou algum outro tipo de rede física. O símbolo da nuvem é comumente usado para representar "A Internet", significando qualquer rede IP que está no caminho da comunicação. Alice ou Bob não precisam preocupar-se com a forma como a rede funciona, desde que os roteadores encaminhem o tráfego a seus destinos. Não fosse por causa dos protocolos de Internet e da colaboração entre todos os elementos da rede, este tipo de comunicação seria impossível.

Projetando a rede física

Pode parecer estranho falar de uma rede "física" quando estamos construindo redes sem fio. Afinal, qual é a parte física de uma rede? Em redes wireless, o meio físico que usamos para a comunicação é, obviamente, a energia eletromagnética. Mas, no contexto deste capítulo, a rede física refere-se ao tópico mundano de "onde colocamos as coisas". Como organizamos o equipamento de maneira que possamos alcançar nossos clientes wireless? Seja em um prédio de escritórios ou espalhadas por muitos quilômetros, redes sem

fio estão naturalmente implementadas nestas três configurações lógicas: ***links ponto-a-ponto***, ***links ponto-para-multiponto*** e ***nuvens multiponto-para-multiponto***. Enquanto porções diferentes de sua rede possam tomar vantagem de todas estas três configurações, qualquer link individual estará em uma destas três topologias.

Ponto-a-ponto

Links ***ponto-a-ponto*** tipicamente fornecem uma conexão à Internet onde é impossível o acesso de outra forma. Um lado da conexão ponto-a-ponto já tem uma conexão com a Internet, enquanto o outro usará este link para alcançá-la. Por exemplo, uma Universidade pode ter uma conexão de alta velocidade com a Internet, utilizando *frame relay* ou VSAT no campus central, mas o custo seria alto demais para ter o mesmo tipo de conexão em um prédio localizado fora de seus limites. Caso o prédio principal tenha uma visão desobstruída para a localidade remota, uma conexão ponto-a-ponto pode ser utilizada. Isto pode aumentar, ou mesmo substituir, conexões discadas existentes. Com antenas apropriadas e uma linha de visão clara, links ponto-a-ponto podem ser estabelecidos para distâncias superiores a 30 quilômetros.

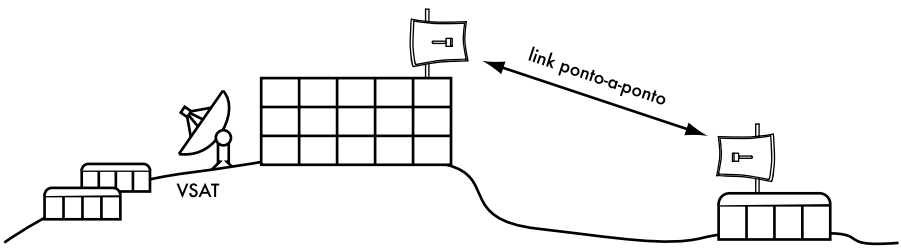


Figura 3.14: Um link ponto-a-ponto permite a uma localidade remota compartilhar uma conexão à Internet no prédio principal.

É claro que, uma vez que uma conexão ponto-a-ponto é estabelecida, outras podem ser usadas para estender a rede para distâncias maiores. Caso o prédio remoto de nosso exemplo esteja no topo de uma colina, ele pode ter visibilidade para outras localizações importantes que não poderiam ser acessadas diretamente do campus central. Com a instalação de outro link ponto-a-ponto na localidade remota, mais um nó poderia juntar-se à rede, usando a mesma conexão à Internet do campus central.

Links ponto-a-ponto não necessariamente precisam envolver o acesso à Internet. Imagine que você tenha que, fisicamente, dirigir até uma estação de monitoramento meteorológico no topo de uma montanha para coletar os dados registrados nela ao longo do tempo. Você pode conectar esta estação com um link ponto-a-ponto, permitindo que a coleta e monitoração de dados ocorram em tempo real, sem que seja necessário o deslocamento até ela. Redes wireless fornecem largura de banda suficiente para o transporte de grande quantidade de dados (incluindo áudio e vídeo) entre quaisquer dois pontos conectados entre si, mesmo que não exista uma conexão direta com a Internet.

Ponto-para-multiponto

O segundo tipo de rede mais encontrado é o ***ponto-para-multiponto***. Sempre que vários nós[3] estão em comunicação com um ponto de acesso central temos uma aplicação de ponto-para-multiponto. O típico exemplo de um leiaute ponto-para-multiponto é o uso de um access point que provê a conexão para vários laptops. Os laptops não se comunicam entre si diretamente, mas devem estar nas proximidades do access point para que possam utilizar a rede.

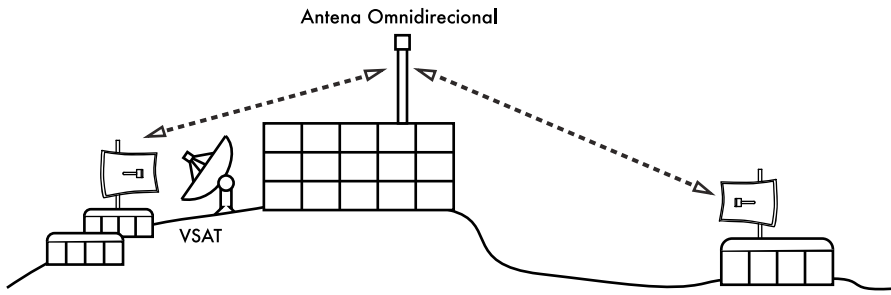


Figura 3.15: A conexão VSAT central é, agora, compartilhada por múltiplas localidades remotas. Todas as três localidades podem também comunicar-se entre si a velocidades muito maiores que o VSAT.

A rede ponto-para-multiponto pode também ser aplicada ao nosso exemplo anterior, na Universidade. Suponha que o edifício remoto, ao topo de uma colina, está conectado ao campus central por um link ponto-a-ponto. Ao invés de configurar vários links ponto-a-ponto para distribuir a conexão com a Internet, uma simples antena, visível a partir dos vários prédios, pode ser utilizada. Este é um clássico exemplo de uma conexão de um ***ponto*** de rede ampla (a localidade remota no topo da montanha) ***para multiponto*** (muitas localidades no vale sob a montanha).

Note que há uma série de considerações de desempenho que devem ser consideradas quando se utiliza a conexão ponto-para-multiponto com distâncias muito longas, que serão tratadas posteriormente neste capítulo. Tais links são possíveis e úteis em muitas circunstâncias, mas não cometa o clássico erro de instalar uma única torre de rádio no meio da cidade esperando atender a milhares de clientes, como você poderia fazer com uma estação de rádio FM. Como veremos adiante, redes de dados bidirecionais comportam-se de maneira bem diferente da transmissão *broadcast* de uma rádio.

Multiponto-para-multiponto

O terceiro tipo de leiaute de rede é o ***multiponto-para-multiponto***, também chamado de rede ***ad-hoc*** ou ***mesh***. Em uma rede multiponto-para-multiponto, não existe uma autoridade central. Todos os nós da rede encarregam-se do tráfego um do outro, conforme o necessário, e cada nó comunica-se com o outro diretamente.

---

3. Um **nó** é qualquer dispositivo capaz de enviar e receber dados em uma rede. Access points, roteadores, computadores e laptops são exemplos de nós.

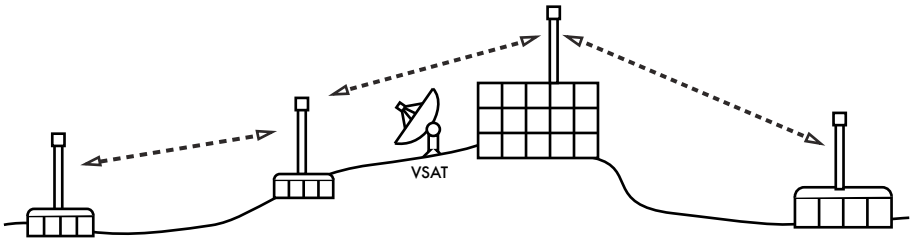


Figura 3.16: Uma rede mesh, multiponto-para-multiponto. Cada ponto pode atingir o outro a uma velocidade altíssima, ou usar o VSAT central para a conexão com a Internet.

O benefício do leiaute desta rede é que, mesmo que nenhum dos nós esteja ao alcance de um ponto de acesso central, ainda assim eles podem comunicar-se um com o outro. Boas implementações de redes mesh são "auto-curáveis", o que significa que elas detectam automaticamente problemas de roteamento e os consertam quando necessário. A extensão de uma rede mesh é simplesmente feita com a adição de mais nós. Caso um dos nós na "nuvem" seja um gateway para a Internet, esta conexão pode ser compartilhada por todos os clientes da rede.

Duas grandes desvantagens desta topologia são a complexidade aumentada e o desempenho diminuído. A segurança neste tipo de rede também é uma preocupação, uma vez que todos os participantes carregam o tráfego, um do outro. Redes multiponto-para-multiponto tendem a ser difíceis de diagnosticar devido ao grande número de variáveis, como os nós que entram e deixam a rede. Nuvens multiponto-para-multiponto têm, tipicamente, uma capacidade reduzida se comparadas com redes ponto-a-ponto ou ponto-para-multiponto, em função da sobrecarga adicional da gestão do roteamento de rede e contenção no espectro de rádio.

De qualquer forma, as redes mesh são úteis em muitas circunstâncias. Mais adiante, nesse capítulo, veremos um exemplo de construção de uma rede mesh multiponto-para-multiponto utilizando um protocolo de roteamento chamado OLSR.

Use a tecnologia adequada

Todos estes esquemas de rede podem ser usados de forma complementar em uma grande rede e, obviamente, pode-se usar também técnicas tradicionais de redes cabeadas sempre que possível. É prática comum, por exemplo, usar um link wireless de longa distância para prover acesso à Internet para uma localidade remota e, a partir daí, distribuir pontos de acesso sem fio locais para distribuir a conexão. Um dos clientes deste ponto de acesso pode também atuar como um nó mesh, permitindo que a rede espalhe-se organicamente entre usuários de laptops. Todos, em última instância, estão usando o link ponto-a-ponto original para o acesso à Internet.

Agora que temos uma clara idéia de como as redes wireless estão tipicamente organizadas, podemos começar a entender como a comunicação é possível nestas redes.

Redes wireless 802.11

Antes que os pacotes possam ser encaminhados e roteados para a Internet, as camadas um (física) e dois (o link de dados) precisam estar conectadas. Sem conexão ao link local, os nós da rede não podem comunicar-se entre si e rotear pacotes.

Para prover conectividade física, os dispositivos de rede wireless devem operar na mesma porção do espectro de rádio. Como vimos no **Capítulo 2**, isto significa que rádios 802.11a irão se comunicar com rádios 802.11a numa freqüência próxima a 5 GHz, e rádios 802.11b/g irão se comunicar com outros rádios 802.11b/g na faixa de 2.4 GHz. Mas um dispositivo 802.11a não irá interoperar com um dispositivo 802.11b/g, uma vez que eles utilizam porções completamente diferentes do espectro eletromagnético.

Mais especificamente, cartões wireless devem estar de acordo sobre o canal comum que utilizarão. Se um cartão de rádio 802.11b está configurado para usar o canal 2, enquanto outro está configurado para o canal 11, eles não falarão entre si.

Quando dois cartões wireless estão configurados para usar o mesmo protocolo, no mesmo canal de rádio, então eles estão prontos para negociar a conectividade da camada de comunicação de dados. Cada dispositivo 802.11a/b/g pode operar em um destes quatro possíveis modos:

1. ***Modo master*** (também chamado de ***AP*** ou ***modo de infra-estrutura***) é usado para criar um serviço que se parece com um ponto de acesso tradicional. O cartão wireless cria uma rede com um nome específico (chamado SSID) e canal, oferecendo serviços de rede nele. No modo master, os cartões wireless gerenciam toda a comunicação relativa à rede (autenticando clientes wireless, tratando da contenção do canal, repetindo pacotes, etc). Cartões wireless em modo master podem apenas comunicar-se com cartões associados a ele em modo gerenciado.

2. ***Modo gerenciado*** é chamado também, algumas vezes, de modo ***cliente***. Cartões wireless no modo gerenciado irão unir-se a uma rede criada pelo master, automaticamente trocando seu canal para corresponder a ele. Eles então apresentam qualquer credencial que é necessária para o master e, se estas credenciais são aceitas, diz-se que eles estão ***associados*** ao master. Cartões no modo gerenciado não se comunicam diretamente um com o outro e se comunicarão apenas com o master associado.

3. ***Modo ad-hoc*** cria uma rede multiponto-para-multiponto, onde não existe um único nó master ou AP. Em modo ad-hoc, cada cartão wireless comunica-se diretamente com os vizinhos. Os nós devem estar ao alcance para que se comuniquem e devem estar de acordo quanto ao nome da rede e o canal utilizado.

4. ***Modo monitor*** é usado por algumas ferramentas (tais como **Kismet**, veja no **Capítulo 6**) para passivamente inspecionar todo o tráfego de rádio em um dado canal. Quando estão no modo monitor, os cartões

wireless não transmitem nenhum dado. Isto é útil para a análise de problemas em um link wireless ou para observar a utilização do espectro na área monitorada. O modo monitor não é usado para a comunicação normal.

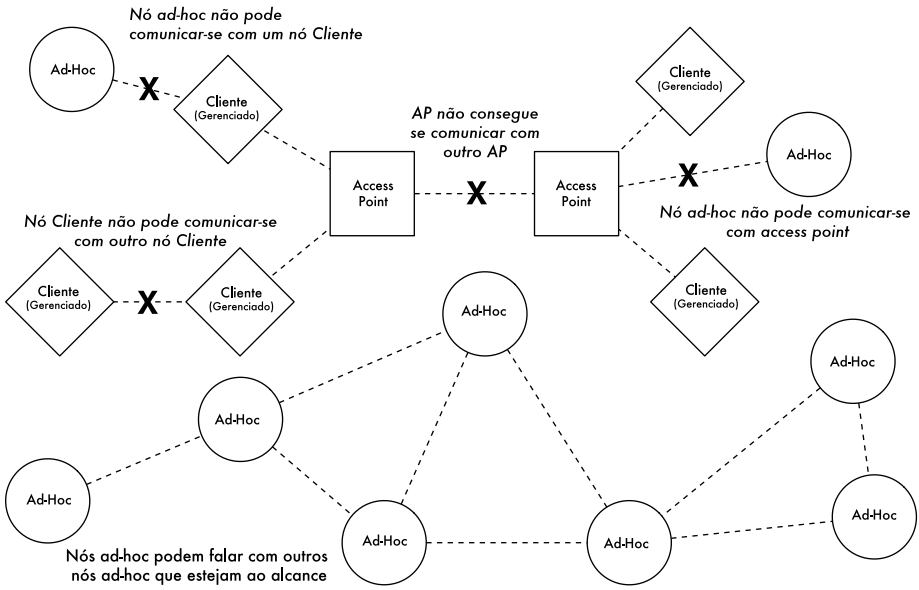


Figura 3.17: Nós APs, Clientes e Ad-Hoc

Quando se implementa um link ponto-a-ponto ou ponto-para-multiponto, um rádio irá operar, tipicamente, em modo master, enquanto os demais irão operar em modo gerenciado. Em um mesh multiponto-para-multiponto, todos os rádios operam em modo ad-hoc e, assim, podem comunicar-se diretamente uns com os outros.

É importante manter estes modos em mente quando estiver projetando sua rede. Lembre-se que clientes em modo gerenciado não podem comunicar-se entre si diretamente, assim, é provável que você queira implementar um site de repetidores no modo master ou ad-hoc. Como veremos adiante neste capítulo, o modo ad-hoc é mais flexível, mas tem uma série de problemas de desempenho quando comparado ao uso dos modos master ou gerenciado.

Rede Mesh com OLSR

A maioria das redes Wi-Fi opera em modo de infra-estrutura, ou seja, consiste de um access point em algum lugar (com um rádio operando em modo master), conectado a uma linha DSL ou algum outro tipo de rede cabeada de larga escala. Em um ***hotspot*** deste tipo, o access point usualmente atua como uma estação master, distribuindo o acesso Internet a seus clientes, que operam em modo gerenciado. Esta topologia é similar a um serviço celular GSM. Os telefones celulares conectam-se a uma estação base—sem a presença desta

estação, os celulares não podem comunicar-se entre si. Se você quiser passar um trote para o seu amigo sentado à sua frente em uma mesa, seu celular envia os dados para uma estação base de sua operadora, que pode estar a três quilômetros de distância, e esta, então, envia os dados para o telefone de seu amigo.

Da mesma forma, cartões Wi-Fi em modo gerenciado não podem comunicar-se diretamente. Clientes—por exemplo, dois laptops em uma mesma mesa—precisam usar um access point como um ponto de passagem (relay). Qualquer tráfego entre os clientes conectados a um access point tem que ser enviado duas vezes. Se o cliente A e o C comunicam-se, o cliente A envia os dados para o access point B, e então o access point retransmitirá os dados para o cliente C. Uma simples transmissão pode ter a velocidade de 600 kByte/s (isto é aproximadamente a máxima velocidade que você alcança com um 802.11b) em nosso exemplo—então, como os dados tem que ser repetidos pelo access point para alcançar seu alvo, a velocidade efetiva entre dois clientes será de apenas 300 kByte/s.

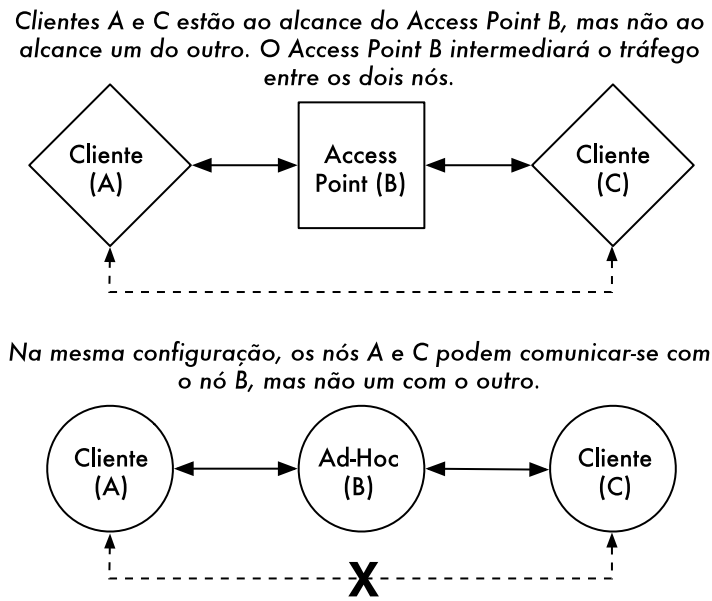


Figura 3.18: O Access Point B irá intermediar o tráfego entre os clientes A e C. Em modo Ad-Hoc, o nó B, por padrão, não irá intermediar o tráfego entre A e C.

No modo ad-hoc não existe uma relação hierárquica master-cliente. Os nós podem comunicar-se diretamente, desde que estejam ao alcance de suas interfaces wireless. Assim, em nosso exemplo, ambos os computadores poderiam atingir a velocidade plena de transmissão de dados trabalhando em modo ad-hoc, em circunstâncias ideais.

A desvantagem do modo ad-hoc é que os clientes não repetem o tráfego destinado a outros clientes. No exemplo do access point, os dois clientes A e C podem não estar ao alcance um do outro, mas podem comunicar-se desde que ambos estejam ao alcance do access point.

Como padrão, nós ad-hoc não repetem dados, mas eles podem fazê-lo se aplicarmos ***roteamento***. As redes mesh são baseadas na estratégia de que cada nó em modo mesh atua como um repetidor para estender a cobertura da rede wireless. Quanto mais nós, melhor a cobertura de rádio e maior o alcance da nuvem mesh.

Há um considerável ponto negativo que mencionaremos agora. Caso o dispositivo utilize apenas uma interface de rádio, a capacidade de banda é significativamente reduzida a cada vez que o tráfego é repetido por nós intermediários no caminho entre A e B. Haverá também interferências na transmissão, uma vez que os nós compartilham o mesmo canal. Assim, redes ad-hoc de baixo custo podem prover boa cobertura de rádio nos últimos quilômetros de uma rede wireless comunitária, ao custo de velocidade—especialmente se a densidade dos nós e a potência de transmissão for alta.

Se uma rede ad-hoc consiste de apenas alguns poucos nós que estão constantemente ligados, não se deslocam e tem sempre links estáveis de rádio —ou seja, uma longa lista de "se"—então é possível configurar tabelas de roteamento para cada nó, manualmente.

Infelizmente, essas condições raramente existem no mundo real. Nós podem falhar, dispositivos com Wi-Fi circulam por todos os lados e a interferência pode derrubar links de rádio a qualquer momento. E ninguém quer ficar atualizando manualmente tabelas de roteamento a cada vez que um novo nó integra a rede. Através do uso de protocolos de roteamento que, automaticamente, mantém tabelas de roteamento individuais em cada nó envolvido, podemos evitar estes problemas. Protocolos populares de roteamento do mundo cabeado (como o OSPF) não funcionam bem neste ambiente porque não são projetados para lidar com conexões intermitentes ou topologias que mudam rapidamente.

Roteamento mesh com olsrd

O ***Optimized Link State Routing Daemon*** (***olsrd***—*http://www.olsr.org*)—traduz-se por serviço de roteamento otimizado para estado de conexão—é uma aplicação de roteamento desenvolvida para funcionar em redes wireless. Nos concentraremos neste software de roteamento por várias razões. Ele é um projeto de código aberto com suporte a Mac OS X, Windows 98, 20000, XP, Vista, Linux, FreeBSD, OpenBSD e NetBSD. Olsrd está disponível para access points que usam (ou podem usar) o Linux, como a família Linksys WRT54G, Asus WI500g, AccessCube ou Pocket PCs rodando o Familiar Linux e ele também é o padrão para os kits Metrix rodando o Pyramid. O olsrd pode trabalhar com múltiplas interfaces e ser estendido através de plugins. Suporta o protocolo IPv6 e é ativamente desenvolvido e usado em redes comunitárias em todo o mundo.

Note que há muitas implementações do *Optimized Link State Routing*, que começou como uma proposta para o IETF escrita no INRIA da França. A implementação do olsrd começou como uma tese de mestrado de Andreas Toennesen na UniK University. Com base na experiência prática de redes comunitárias livres, o serviço de roteamento foi modificado. O olsrd difere, hoje, significativamente de seu projeto original, pois passou a incluir um mecanismo chamado *Link Quality Extension* (extensão de qualidade de linha) que mede a perda de pacotes entre os nós e calcula as rotas levando em conta esta

informação. Esta extensão quebra a compatibilidade com os serviços de roteamento que seguem a especificação original do INRIA. O olsrd disponível em *www.olsr.org* pode ser configurado para que se comporte de acordo com a especificação do IETF que não possui esta funcionalidade—mas não há razão para desabilitar a *Link Quality Extension*, a não ser que a compatibilidade com outras implementações seja necessária.

Teoria

Depois que o olsrd está em execução por algum tempo, um nó sabe da existência de todos os outros nós da nuvem mesh e quais podem ser usados para rotear tráfego para eles. Cada nó mantém uma tabela de roteamento cobrindo toda a rede mesh. Este tratamento dado ao roteamento mesh é chamado de ***roteamento proativo*** (***proactive routing***). Por outro lado, algoritmos de ***roteamento reativo*** (***reactive routing***) procuram rotas apenas quando é necessário o envio de dados para um nó específico.

Há prós e contras para o roteamento proativo e existem muitas outras idéias sobre a forma de se implementar roteamento mesh que valeriam a pena mencionar. A maior vantagem do roteamento proativo é que você sabe quais são os nós que compõem a rede, não precisando esperar que rotas sejam encontradas. Uma maior sobrecarga do protocolo e maior utilização de processamento são algumas das desvantagens. Em Berlim, a comunidade Freifunk opera uma nuvem mesh onde o olsrd tem que gerenciar mais de 100 interfaces. A média de carga de CPU, causada pelo olsrd em um Linksys WRT54G, rodando a 200 MHz, é de 30% na rede mesh de Berlim. Há claramente um limite na capacidade de escala de um protocolo proativo—dependendo de quantas interfaces são utilizadas e da freqüência de atualização das tabelas de roteamento. A manutenção de rotas em uma nuvem mesh estática dá menos trabalho do que em uma onde os nós mudam constantemente de lugar, uma vez que, no primeiro caso, as tabelas de roteamento necessitam ser atualizadas com menor freqüência.

Mecanismo

Um nó rodando olsrd está, constantemente, enviando mensagem de broadcast 'Hello' (Olá) em intervalos de tempo determinados, de forma que os vizinhos possam detectar sua presença. Cada nó faz a estatística de quantos 'Hellos' foram perdidos ou recebidos de cada vizinho—obtendo, desta maneira, informações sobre a topologia e qualidade do link para os nós da vizinhança. A informação obtida sobre a topologia é transmitida como mensagens de controle de topologia (Topology Control, ou TC messages) e encaminhada pelos vizinhos que o olsrd escolheu para serem retransmissores multiponto.

O conceito de retransmissores multiponto (multipoint relays) é uma idéia nova em roteamento proativo que surgiu com o projeto do OLSR. Se cada nó retransmite a informação de topologia que recebeu, uma sobrecarga desnecessária é gerada. Tais transmissões são redundantes se um nó tem muitos vizinhos. Assim, um nó olsrd decide quais vizinhos, que são retransmissores multiponto favoráveis, irão encaminhar as mensagens de controle de topologia. Note que os retransmissores multiponto são escolhidos

para o propósito de encaminhamento de mensagens TC. A carga de trabalho é roteada considerando todos os nós disponíveis.

Há outros dois tipos de mensagens no OLSR que anunciam informação: quando um nó oferece um gateway para outras redes (mensagens HNA) ou quando o mesmo possui múltiplas interfaces (mensagens MID). Não há muito a dizer sobre estas mensagens, a não ser que elas existem. Mensagens HNA tornam o olsrd bastante conveniente quando é feita a conexão com a Internet através de um dispositivo móvel. Quando um nó mesh é movido de um lado a outro, ele irá detectar gateways para outras redes, escolhendo aquele para o qual existe a melhor rota. Entretanto, o olsrd não é infalível. Se um nó anuncia que é um gateway para a Internet—o que ele não é, seja porque nunca foi ou porque está desconectado no momento—os demais nós acreditarão nesta informação. Este pseudo-gateway é um buraco negro. Para contornar este problema, um plugin para gateway dinâmico foi escrito. Este plugin irá automaticamente detectar, no gateway, se ele está realmente conectado e se o link ainda está ativo. Caso contrário, o olsrd suspende o envio de falsas mensagens HNA. É altamente recomendável instalar e utilizar este plugin, ao invés de habilitar estaticamente mensagens HNA.

Prática

O olsrd implementa roteamento baseado em IP em uma aplicação no espaço do usuário—a instalação é relativamente fácil. Pacotes de instalação estão disponíveis para OpenWRT, AccessCube, Mac OS X, Debian GNU/Linux e Windows. O OLSR é componente padrão do Metrix Pyramid. Caso você tenha que compilar a partir do código-fonte, primeiro leia a documentação que está presente na distribuição do programa. Caso tudo esteja configurado corretamente, o que você tem a fazer é executar o olsr.

Antes de mais nada, certifique-se de que cada nó tem um endereço IP único, designado de forma estática, para cada interface utilizada na rede mesh. Não é recomendado (e também não é prático) usar DHCP em uma rede mesh baseada em IP. Um pedido de DHCP não será respondido por um servidor DHCP se o solicitante precisar passar por vários hops para chegar até ele, e aplicar a retransmissão de DHCP através de uma rede mesh é virtualmente impraticável. Esta questão poderia ser resolvida com o uso de IPv6, uma vez que ele permite espaço suficiente para a geração de endreços IP únicos a partir do endereço MAC de cada interface envolvida (como sugerido em "IPv6 Stateless Address Autoconfiguration in large mobile ad hoc networks" de K. Weniger e M. Zitterbart, 2002).

Uma página wiki, onde cada pessoa interessada possa escolher um endereço IPv4 para cada interface onde o serviço olsr esteja rodando, pode servir muito bem a esse propósito. Não há maneira fácil de automatizar o processo se o IPv4 for utilizado.

O endereço de broadcast deve ser 255.255.255.255 para as interfaces mesh em geral, como uma convenção. Não há razão para configurar o endereço de broadcast explicitamente, uma vez que o olsrd pode ser configurado para sobrescrever o endereço de broadcast por este convencionado. Deve-se certificar, apenas, que as configurações são as mesmas em todos os lugares. O oslrd pode encarregar-se disto. Quando um arquivo de configuração oslrd é

preparado e distribuído, esta funcionalidade deve estar habilitada para evitar confusões do tipo "por que os outros nós não conseguem ver a minha máquina?!?".

Agora vamos configurar a interface wireless. Aqui está um exemplo de comando de configuração de um cartão Wi-Fi com o nome wlan0 usando o Linux:

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

Verifique que a porção wireless do cartão Wi-Fi foi configurada de modo a permitir uma conexão ad-hoc para outros nós mesh dentro do alcance direto (*single hop*). Certifique-se de que a interface junta-se ao mesmo canal wireless, use o mesmo nome de rede ***ESSID*** (***Extended Service Set IDentifier***) e tenha o mesmo Cell-ID que todos os outros cartões Wi-Fi usados na construção da rede mesh. Muitos cartões Wi-Fi, ou seus respectivos drivers, não são compatíveis com o padrão 802.11 para redes ad-hoc e podem falhar miseravelmente na conexão com uma célula. Eles podem ser incapazes de conectar com outros dispositivos na mesma tabela, mesmo que estejam configurados com o canal e nome de rede corretos. Eles podem até confundir outros cartões que comportam-se de acordo com o padrão ao criar seu próprio Cell-ID no mesmo canal, como o mesmo nome de rede. Cartões Wi-Fi feitos pela Intel que são embarcados com os notebooks Centrino são notórios por este tipo de comportamento.

Você pode verificar isto com o comando **`iwconfig`**, quando usar o GNU/Linux. Aqui está o resultado em minha máquina:

```
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
```

É importante configurar o limite (*threshold*) do parâmetro ***Request to Send*** (***RTS***—solicitação para envio) para uma rede mesh. Existirão colisões no canal de rádio entre as transmissões de nós no mesmo canal wireless e o RTS atenuará isto. RTS/CTS adicionam um handshake[4] antes da transmissão de cada pacote, garantindo que o canal está livre. Isto adiciona uma sobrecarga, mas aumenta o desempenho no caso de nós escondidos—e nós escondidos são o padrão em uma rede mesh. Este parâmetro configura o limite do menor pacote (em bytes) para o qual o nó envia um RTS. O limite (*threshold*) RTS deve ser menor que o tamanho do pacote IP (*IP Packet*) e que o limite de fragmentação (*fragmentation threshold*)—aqui configurado para 256—de outra

---

4. N. do. T - *Handshake* traduz-se, literalmente, por "sacudida de mãos". É o tradicional cumprimento de apertar as mãos de alguém. Neste caso, é um "comportamento" do protocolo na transmissão de dados. Antes de enviar qualquer coisa, que deve ter o tamanho mínimo definido pelo threshold (no caso, 256 bytes), o lado que vai transmitir envia um sinal RTS, Request to Send, ou seja, pede permissão para enviar dados. Caso o canal esteja liberado, ele receberá como resposta um sinal CTS, Clear to Send, ou "liberado para enviar". Atendidas estas condições, a transmissão de dados se inicia.

forma, será desabilitado. O TCP é muito sensível a colisões, então é importante manter o RTS ligado.

A fragmentação permite a divisão de um pacote IP em fragmentos menores, transmitidos no meio de comunicação. Isto adiciona sobrecarga mas, em um ambiente com muito ruído, acaba por diminuir a incidência de erros e permite que os pacotes atravessem picos de interferência. Redes mesh possuem bastante ruído pois todos os seus nós usam o mesmo canal e, por causa disto, as transmissões interferem umas com as outras. Este parâmetro (*Fragment thr*) configura o tamanho máximo que um pacote deve ter, antes de ser dividido e enviado em uma rajada (*burst*). Um valor igual ao tamanho máximo do pacote IP (*IP packet size*) desabilita o mecanismo de fragmentação, desta forma, Fragment thr deve ser menor que o *IP packet size*. A configuração do limite de fragmentação é recomendada.

Uma vez que um endereço IP válido e uma máscara de rede são atribuídos, e a interface wireless está ligada, o arquivo de configuração do olsrd deve ser alterado de maneira que o olsrd encontre e use a interface na qual deve trabalhar.

Para o MAC OS X e Windows há uma boa interface gráfica para a configuração e monitoração do serviço. Infelizmente, isto é uma tentação para usuários que não têm conhecimento suficiente façam coisas estúpidas—como anunciar buracos negros. No BSD e no Linux, o arquivo de configuração /etc/olsrd.conf precisa ser manipulado com um editor de textos.

Um simples olsrd.conf

Não seria muito prático fornecer, aqui, um arquivo de configuração completo. Abaixo estão alguns itens essenciais que devem ser verificados.

```
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
       }
```

Há muito mais opções disponíveis no olsrd.conf, mas estas opções básicas servem como ponto de partida. Uma vez que estes passos estão completos, o olsrd pode ser iniciado com um simples comando no terminal:

```
olsrd -d 2
```

Recomendo que você execute o comando com a opção de debug -d 2, especialmente na primeira vez que o fizer. Desta forma, você pode ver o que o olsrd faz e monitorar de que maneira estão os links para seus vizinhos. Em

dispositivos embarcados, o nível de debug deve ser 0 (desligado), porque o debug aumenta bastante a carga da CPU.

A saída do comando anterior deve ser parecida com o seguinte:

```
--- 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
```

Usando OLSR em Ethernet e múltiplas interfaces

Não é necessário ter uma interface wireless para testar ou usar o olsrd—ainda que seja para isto que o olsrd tenha sido projetado. Ele pode ser usado em qualquer cartão de rede. Interfaces Wi-Fi não têm que operar sempre no modo ad-hoc para formar uma rede mesh quando um nó mesh tem mais do que uma interface. Para links dedicados, pode ser uma boa opção tê-los rodando em modo infra-estrutura. Muitos cartões Wi-Fi e seus drivers apresentam problemas em modo ad-hoc, mas funcionam bem no modo de infra-estrutura—porque todos esperam que ao menos isto funcione bem. O modo ad-hoc ainda não tem muitos usuários, assim, a implementação do mesmo foi feita de forma descuidada por muitos fabricantes. Com o aumento da popularidade de redes mesh, a situação dos drivers está melhorando hoje.

Plugins

Uma boa quantidade de plugins está disponível para o olsrd. Visite o site *www.olsr.org* para uma lista completa deles. Aqui apresentamos apenas um pequeno tutorial para o plugin de visualização de topologia de rede **`olsrd_dot_draw`**.

Com freqüência, é muito bom para o entendimento de uma rede mesh ter a capacidade de exibir a topologia da rede de forma gráfica. O plugin **`olsrd_dot_draw`** gera a topologia da rede em formato de pontos na porta TCP 2004. As ferramentas graphviz podem então ser usadas para desenhar os gráficos.

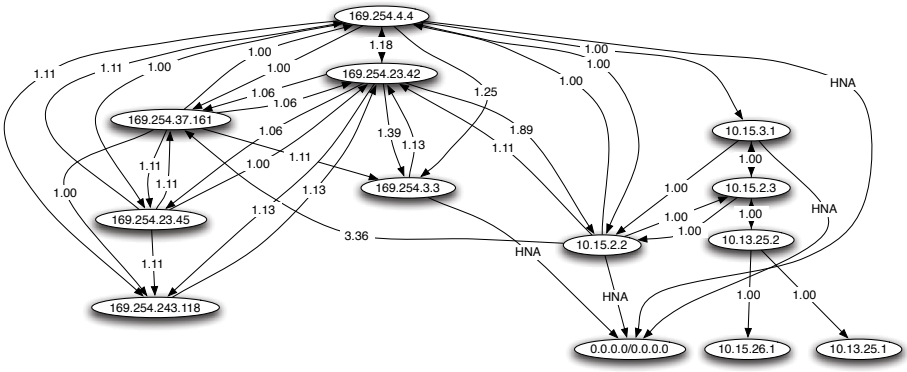


Figura 3.19: Uma topologia de rede OLSR gerada automaticamente.

Instalando o plugin dot_draw

Compile os plugins olsr separadamente e instale-os. Para carregar o plugin adicione as seguintes linhas ao **`/etc/olsrd.conf`**. O parâmetro "accept" especifica qual host é aceito para ver a informação de topologia (atualmente, apenas um) e, por padrão, é "localhost" (o computador local). O parâmetro "port" especifica a porta TCP.

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

Feito isto, reinicie o olsr e verifique se você obtém uma saída na porta TCP 2004.

```
telnet localhost 2004
```

Após algum tempo, você deve começar a ver alguma saída de texto.

Agora, você pode salvar a saída das descrições gráficas e rodar as ferramentas **`dot`** ou **`neato`** do pacote graphviz para obter as imagens.

Bruno Randolf escreveu um pequeno script em perl, que obtém continuamente a informação de topologia do olsrd e a exibe graficamente, utilizando as ferramentas graphviz e ImageMagick.

Comece instalando os seguintes pacotes em seu computador:

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

Faça o download do script em *http://meshcube.org/nylon/utils/olsr-topology-view.pl*

Você pode, agora, executar o script com **`./olsr-topology-view.pl`** e verificar a atualização da topologia praticamente em tempo real.

Diagnóstico de problemas

Desde que os cartões Wi-Fi possam "ver" diretamente um ao outro com seus rádios, executar um "ping" irá funcionar, quer o olsrd esteja sendo executado ou não. Isto funciona porque a grande máscara de rede (255.255.255.255) faz de cada nó um link local, colocando de lado questões de roteamento no nível do primeiro "hop" (local). Esta é a primeira coisa a ser verificada se algo parece não estar de acordo com o esperado. A maior parte das dores de cabeça que as pessoas têm com o Wi-Fi em modo ad-hoc são causadas pelo fato de que o modo ad-hoc em cartões e drivers é implementado de forma descuidada. Se não for possível "pingar" os nós diretamente quando eles estão ao alcance um do outro, é mais provável que exista um problema no cartão ou driver, ou as configurações da sua rede estão erradas.

Se as máquinas conseguem "pingar" uma a outra, mas o olsrd não encontra as rotas, então os endereços IP, máscaras de rede e endereço de broadcast devem ser verificados.

Finalmente, você está rodando um firewall? Verifique se você não está bloqueando a porta UDP 698.

Estimando a capacidade

Links wireless podem proporcionar capacidades de transmissão de dados para seus usuários que são maiores que as conseguidas em conexões Internet tradicionais, como VSAT, linha discada, ou DSL. Esta capacidade de transmissão é também chamada de ***throughput***, ***capacidade de canal*** (***channel capacity***), ou simplesmente ***largura de banda*** (***bandwidth***)—ainda que este termo não esteja relacionado com a largura de banda de um rádio. É importante entender que a velocidade listada para um dispositivo, a taxa de transmissão de dados (***data rate***) refere-se à velocidade pela qual os rádios podem trocar símbolos, e não a capacidade utilizável que você irá observar. Como mencionado anteriormente, um simples link 802.11g pode usar rádios de 54 Mbps, mas fornecerá apenas um máximo de 22 Mbps de transmissão efetiva de dados. O restante é a sobrecarga que os rádios utilizam para coordenar seus sinais usando o protocolo 802.11g.

Note que o throughput é uma medida de bits em um determinado tempo. 22 Mbps significa que, em um segundo, até 22 megabits podem ser enviados de uma ponta de um link para a outra. Se os usuários tentarem enviar mais do que 22 megabits pelo link, isto tomará mais do que um segundo. Uma vez que os dados não possam ser enviados imediatamente, eles são colocados em uma fila (***queue***) e transmitidos tão rapidamente quanto seja possível. Este atraso no envio de dados aumenta o tempo necessário para que aqueles bits colocados mais recentemente na fila atravessem o link. Este tempo que leva para os dados atravessarem o link é chamado ***latência*** (***latency***), e uma latência alta é comumente chamada de ***lag***. Seu link irá, eventualmente, enviar todo o tráfego que está na fila, mas seus usuários provavelmente reclamarão se o *lag* for muito grande.

Quanto throughput seus usuários realmente precisam? Isto irá depender de quantos usuários você têm e como eles utilizam o link wireless. Várias aplicações Internet requerem diferentes quantidades de throughput.

Aplicação	Consumo de banda por usuário	Observações
Mensagens em texto, comunicadores instantâneos	< 1 kbps	Como o tráfego é pouco freqüente e assíncrono, programas de mensagens instantâneas toleram latências altas.
Correio eletrônico	1 a 100 kbps	Da mesma forma que programas de mensagens instantâneas, a comunicação através de email é assíncrona e, assim, tolerará latência. Grandes anexos, vírus e spam aumentam significativamente a utilização de banda. Note que serviços de webmail (como o Yahoo, Hotmail e gMail) devem ser considerados como navegação, não como email.
Navegação web	50 a mais de 100 kbps	Navegadores web apenas utilizam a rede quando dados são requisitados. A comunicação é assíncrona, assim, uma quantidade considerável de *lag* pode ser tolerada. Quando os navegadores requisitam mais dados (imagens grandes, longos downloads, etc) o uso da banda aumentará significativamente.
Streaming de áudio	96 - 160 kbps	Cada usuário de um serviço de streaming de áudio (ouvintes de rádios online, podcasts e outros) usa uma quantidade relativamente grande da largura de banda durante todo o tempo em que está ouvindo. Alguma latência pode ser tolerada com o uso de *buffers* (memória local) de bom tamanho no computador do cliente. Períodos extensos de *lag*, porém, farão com que o sinal de áudio “salte” ou que ocorram outros problemas com a sessão.
Voz sobre IP (VoIP)	24 - 100+ kbps	Assim como o streaming de áudio, o uso do VoIP compromete uma quantidade de banda de cada usuário enquanto durar a chamada. Mas com VoIP, o consumo de banda é praticamente igual em ambas as direções. A latência em uma conexão VoIP é imediata e irritante para os usuários. Uma interrupção maior que alguns milissegundos é inaceitável para VoIP.

Aplicação	Consumo de banda por usuário	Observações
Streaming de vídeo	64 - 200+ kbps	Como no streaming de áudio, alguma latência intermitente é evitada com o uso de buffers no cliente. A transmissão de vídeo requer um throughput alto e uma latência baixa para que funcione apropriadamente.
Aplicações peer-to-peer para o compartilhamento de arquivos (BitTorrent, KaZaA, Gnutella, eDonkey, etc.)	0 - infinitos Mbps	Enquanto aplicações peer-to-peer toleram qualquer quantidade de latência, elas tendem a utilizar o throughput máximo disponível para transmitir dados para quantos clientes forem possíveis. O uso destas aplicações irá causar latência e problemas de consumo de banda para todos os outros usuários da rede, a não ser que você use alguma forma cuidadosa de limitação de banda (*bandwidth shaping*)

Para estimar a largura de banda necessária para a sua rede, multiplique o número esperado de usuários pelo tipo de aplicação que eles irão, provavelmente, utilizar. Por exemplo, 50 usuários que irão, primariamente, navegar pela web consumirão entre 2,5 e 5 Mbps. Por outro lado, 50 usuários simultâneos de VoIP necessitarão de 5 Mbps ou mais de largura de banda em ***ambas as direções*** sem, absolutamente, nenhuma latência. Uma vez que os equipamentos wireless 802.1g são ***half duplex*** (ou seja, apenas transmitem ou recebem, nunca simultaneamente), você deve, apropriadamente, dobrar a largura de banda requerida para um total de 10 Mbps. Seus links wireless devem prover esta capacidade em todos os momentos, ou haverá falhas nas conversações.

Dificilmente todos os seus usuários usarão a conexão precisamente ao mesmo tempo, então, é uma prática comum superestimar (***oversubscribe***) o uso da largura de banda disponível em algum fator (isto é, permitir mais usuários que a largura de banda máxima pode suportar). Superestimar em um fator de 2 a 5 vezes o número de usuários é bastante comum. Na prática, você irá superestimar em algum fator quando estiver montando sua infra-estrutura de rede. Através do monitoramento cuidadoso do consumo de banda, você será capaz de planejar quando deve atualizar as várias partes de sua rede e quantos recursos adicionais serão necessários.

Você pode ter certeza de que, independente da capacidade que você irá fornecer, seus usuários encontrarão aplicações que irão usá-la integralmente. Conforme veremos ao final deste capítulo, o uso de técnicas de limitação de banda (*bandwidth shaping*) auxiliará na minimização de alguns problemas de latência. Com o uso de limitação de banda, armazenamento local de páginas web (*web caching*) e outras técnicas, você poderá diminuir a latência significativamente e melhorar, de maneira geral, a utilização da banda de sua rede.

Para ter uma idéia do lag percebido em conexões muito lentas, o ICTP construiu um simulador de largura de banda. Ele irá, simultaneamente, fazer a carga de uma página web em velocidade total ou a uma taxa reduzida de sua escolha. Esta demonstração dá a você um entendimento imediato de como uma taxa de transferência baixa e uma alta latência reduzem a utilidade da Internet como ferramenta de comunicação. O simulador está disponível em *http://wireless.ictp.trieste.it/simulator/*

Planejamento do link

Um sistema básico de comunicação consiste em dois rádios e suas respectivas antenas, separados por um caminho a ser coberto. Para que seja estabelecida a comunicação entre os dois rádios é necessário que as antenas captem uma certa quantidade mínima de sinal, apresentando-o ao conector de entrada do rádio. A determinação da viabilidade do link é um processo chamado "cálculo do orçamento do link" (***link budget***). A passagem, ou não, do sinal entre os rádios dependerá da qualidade do equipamento utilizado e da diminuição do sinal devido à distância (***path loss***).

Cálculo do orçamento do link

A potência disponível em um sistema 802.11 pode ser caracterizada pelos seguintes fatores:

- **Potência de transmissão** (*TX power*). É expressa em miliwatts ou dBm. Varia entre 30 mW a mais de 200 mW. A potência de transmissão freqüentemente depende da taxa de transmissão. A TX Power de um determinado dispositivo deve estar especificada na literatura fornecida pelo fabricante, mas pode ser difícil de ser encontrada às vezes. Bases de dados online, como a fornecida pela SeattleWireless (*http://www.seattlewireless.net/HardwareComparison*) podem ajudar.

- **Ganho da antena**. Antenas são componentes passivos que criam o efeito de amplificação em função de sua forma física. Elas têm as mesmas características, tanto na transmissão quanto na recepção. Assim, uma antena de 12 dBi é simplesmente uma antena de 12 dBi, sem importar se está em modo de transmissão ou recepção. Antenas parabólicas têm um ganho de 19 a 24 dBi, antenas omnidirecionais têm de 5 a 12 dBi e antenas setoriais têm um ganho aproximado de 12 a 15 dBi.

- **Nível mínimo de sinal para recepção** (*Minimum Received Signal Level*, ou RSL mínimo) expressa simplesmente a sensitividade do receptor. O mínimo RSL é sempre expresso como um dBm negativo (- dBm) e é o sinal de menor potência que o receptor consegue distinguir. O mínimo RSL depende da taxa de transmissão mas, como regra geral, a menor taxa (1 Mbps) implica na maior sensitividade. O mínimo ficará tipicamente entre -75 a -95 dBm. Como a TX Power, as especificações do RSL devem ser fornecidas pelo fabricante do equipamento.

- **Perdas em cabos**. Parte da energia do sinal é perdida nos cabos, conectores e outros dispositivos que estão entre os rádios e as antenas.

A perda depende do tipo de cabo usado e de seu comprimento. A perda de sinal em cabos coaxiais curtos, incluindo seus conectores, é bem pequena, na faixa de 2 a 3 dB. É melhor manter cada cabo sempre o mais curto possível.

Quando se calcula a perda de energia em um caminho de transmissão, vários efeitos devem ser considerados. É necessário levar em conta a ***perda em espaço aberto*** (***free space loss***), ***atenuação*** (***attenuation***) e ***espalhamento*** do sinal (***scattering***). A potência do sinal diminui com o espalhamento geométrico da frente de onda (*free space loss*). Ignorando todo o resto, quanto maior a distância entre os rádios, menor é o sinal recebido em função da perda de sinal em espaço aberto. Isto não depende do ambiente, mas apenas da distância. Esta perda acontece porque o sinal irradiado se expande em função da distância do transmissor.

Usando decibéis para expressar a perda, e usando 2,45 GHz como a freqüência do sinal, a equação que define a perda em espaço aberto é a seguinte:

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

Onde L_{fsl} é expresso em dB e r é a distância entre o transmissor e o receptor, em metros.

A segunda contribuição para as perdas é dada pela atenuação. Ela acontece porque a potência do sinal é absorvida quando o mesmo atravessa objetos sólidos como árvores, paredes, janelas e separações entre andares em um prédio. A atenuação pode variar bastante, dependendo da estrutura do objeto que o sinal está atravessando e é muito difícil de ser quantificada. A maneira mais conveniente de expressar a sua contribuição para o total de perdas é adicionando uma "perda permitida" (allowed loss) para o espaço aberto. Por exemplo, a experiência mostra que árvores adicionam entre 10 a 20 dB de perda para cada uma que esteja no caminho direto do sinal, enquanto paredes contribuem de 10 a 15 dB, dependendo do tipo de material com que foram construídas.

Ao longo do caminho do link, a energia de rádio-freqüência deixa a antena de transmissão e se espalha. Uma parte da energia de RF atinge diretamente a antena de recepção, enquanto outra choca-se com o chão. Parte desta energia que chocou-se com o chão também atinge a antena de recepção. Uma vez que o sinal refletido percorre um caminho maior, ele atinge a antena depois que o sinal direto. Este efeito é chamado ***multipath*** (caminho múltiplo) ou dispersão de sinal. Em alguns casos, os sinais refletidos somam-se, sem causar problemas. Quando eles combinam-se em fases diferentes, o sinal recebido é praticamente sem valor. Em alguns casos, o sinal recebido pela antena pode ser totalmente anulado pelos sinais refletidos. Isto é conhecido como anulação (***nulling***). Há uma técnica simples que é usada para lidar com o efeito multipath, chamada de diversidade de antena (***antenna diversity***). Ela consiste na adição de uma segunda antena ao rádio. O multipath é, de fato, um fenômeno essencialmente dependente da localização. Se dois sinais adicionam-se fora de fase em um local, eles não irão adicionar-se de forma igualmente destrutiva em outro local próximo. Com duas antenas, ao menos uma dela deve ser capaz de receber um sinal utilizável, mesmo que a outra receba um distorcido. Em

dispositivos comerciais, a diversidade de troca de antenas é utilizada: há múltiplas antenas em múltiplas entradas para um único receptor. O sinal é, portanto, recebido por apenas uma antena de cada vez. Na transmissão, o rádio usa a última antena usada para a recepção. A distorção vinda do efeito multipath degrada a habilidade do receptor recuperar o sinal, de uma forma bastante similar à perda de sinal. Uma simples forma de aplicar o efeito do espalhamento no cálculo de perdas no caminho consiste na mudança do expoente do fator da distância na fórmula de perda no espaço aberto. O expoente tende a aumentar se o ambiente é propício a muito espalhamento de sinal. Um expoente 3 pode ser usado em um ambiente externo, enquanto um expoente 4 pode ser usado em um ambiente interno.

Quando as perdas no espaço aberto, a atenuação e o espalhamento são combinados, a perda total no caminho fica:

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

Para uma estimativa rápida da viabilidade de um link, pode-se avaliar apenas a perda no espaço aberto. O ambiente pode adicionar perdas posteriores de sinal e deve ser considerado para uma avaliação exata do link. O ambiente é, de fato, um fator muito importante, que jamais deve ser negligenciado.

Para avaliar se um link é viável, as características do equipamento usado devem ser conhecidas e as perdas no caminho devem ser avaliadas. Note que, ao fazer estes cálculos, você deve considerar apenas a potência de transmissão de um lado do link. Se você usar rádios diferentes em cada lado do link, deve calcular a perda no caminho duas vezes, uma para cada direção (usando a potência de TX apropriada em cada cálculo). Adicionando todos os ganhos e subtraindo todas as perdas, temos:

```
  TX Power Rádio 1
+ Ganho de Antena Rádio 1
- Perdas no Cabo Rádio 1
+ Ganho de Antena Rádio 2
- Perdas de Cabo Rádio 2
  ___________________________
=       Ganho Total
```

Subtraindo a perda que ocorre no caminho do ganho total:

```
  Ganho Total
- Perda no Caminho
  ____________________________________
= Nível de sinal de um lado do link
```

Se o sinal resultante for maior do que o nível mínimo de sinal de recepção, então o link é viável. O sinal recebido é potente o suficiente para que os rádios o utilizem. Lembre-se que o mínimo RSL é sempre expresso com um dBm negativo, assim -56 dBm é maior que -70 dBm. Em um determinado caminho, a variação de perdas de sinal em um período de tempo pode ser grande, desta forma uma certa margem (a diferença entre o nível de sinal e o mínimo DSL) deve ser considerada. Esta margem é a quantidade de sinal acima da sensitividade do rádio que irá garantir um link de rádio estável e de alta qualidade durante uma tempestade ou outras perturbações atmosféricas. Uma margem de 10 a 15 dB já é boa. Para dar algum espaço para a atenuação pelo

efeito multipath no sinal recebido, uma margem de 20 dB deve ser suficientemente segura.

Agora que você calculou o orçamento do link em uma direção, repita o cálculo para outra. Substitua a potência de transmissão do segundo rádio e compare o resultado com o nível de sinal mínimo de recepção do primeiro.

Exemplo de cálculo de orçamento do link

Como exemplo, vamos estimar a viabilidade de um link de 5 km, com um access point e um rádio para o cliente. O access point está conectado a uma antena omnidirecional com um ganho de 10 dBi, enquanto o cliente está conectado a uma antena setorial com um ganho de 14 dBi. A potência de transmissão do AP é 100 mW (ou 20 dBm) e sua sensitividade é de -89 dBm. A potência de transmissão do cliente é de 30 mW (ou 15 dBm) e sua sensitividade é de -82 dBm. Os cabos são curtos, com uma perda de 2 dB em cada lado.

Adicionando todos os ganhos e subtraindo todas as perdas do AP ao cliente temos:

```
  20 dBm (TX Power Rádio 1)
+ 10 dBi (Ganho de antena Rádio 1)
-  2 dB  (Perdas no cabo Rádio 1)
+ 14 dBi (Ganho de antena Rádio 2)
-  2 dB  (Perdas no cabo Rádio 2)
_____________________________________
= 40 dB Ganho Total
```

A perda no caminho, para um link de 5 km, considerando apenas a perda no espaço aberto é:

```
Perda no caminho = 40 + 20 log (5000) = 113 dB
```

Subtraindo a perda no caminho do ganho total:

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

Uma vez que -73 dB é maior que a sensitividade mínima do rádio cliente (-82 dBm), o nível do sinal está justo o suficiente para que o cliente “ouça” o access point. Há apenas uma margem de 9 dB (82 dB – 73 dB), o que significa que o link provavelmente funcionará bem com tempo bom, mas que pode não ser o bastante em más condições do tempo.

A seguir, vamos calcular o link do cliente de volta ao access point:

```
  15 dBm (TX Power Rádio 2)
+ 14 dBi (Ganho de antena Rádio 2)
-  2 dB  (Perdas no cabo Rádio 2)
+ 10 dBi (Ganho de antena Rádio 1)
-  2 dB  (Perdas no cabo Rádio 1)
_____________________________________
  35 dB = Ganho Total
```

Obviamente, a perda no caminho é a mesma na volta. Então, o sinal que recebemos do lado do access point é:

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

Como a sensitividade do AP é -89 dBm, isto nos deixa uma pequena margem de 11 dB (89dB – 78dB). De maneira geral, este link provavelmente funcionará, mas poderia ter um pouco mais de ganho. O uso de um receptor do tipo prato no cliente, ao invés de uma antena setorial de 14 dBi, proporcionará um ganho adicional de 10 dBi em ambas as direções do link (lembre-se, o ganho da antena é recíproco). Uma opção mais cara seria usar rádios mais potentes em ambos os lados do link, mas note que a adição de um amplificador ou um cartão que proporcione maior potência apenas de um lado não ajudará, normalmente, a qualidade global do link.

Ferramentas online podem ser usadas para o orçamento do link. Por exemplo, a *Green Bay Professional Packet Radio's Wireless Network Link Analysis* (*http://my.athenet.net/~multiplx/cgi-bin/wireless.main.cgi*) é uma excelente ferramenta. A Super Edition gera um arquivo PDF contendo a zona Fresnel e os gráficos de caminhos do rádio. Os scripts para os cálculos podem até ser baixados do site e instalados localmente.

O site Terabeam também dispõe de calculadoras excelentes (*http://www.terabeam.com/support/calculations/index.php*).

Tabelas para o orçamento do link

Para calcular o orçamento do link, simplesmente use a distância aproximada de seu link e a preencha nas tabelas a seguir:

Perda no espaço livre a 2,4 GHz

Distância (m)	100	500	1.000	3.000	5.000	10.000
Perda (dB)	80	94	100	110	113	120

Para mais distâncias em perdas no caminho, consulte o **Apêndice C**.

Ganho de Antena:

Antena do Rádio 1 (dBi)	+ Antena do Rádio 2 (dBi)	= Ganho total de antena

Perdas:

Perda no cabo para o Rádio 1 (dB)	+ Perda no cabo para o Rádio 2 (dB)	+ Perda no espaço aberto (dB)	= Perda total (dB)

Orçamento do link do Rádio 1 para o Rádio 2:

TX Power do Rádio 1	+ Ganho de antena	- Perda total	= Sinal	> Sensitivitade do Rádio 2

Orçamento do link do Rádio 2 para o Rádio 1:

TX Power do Rádio 2	+ Ganho de antena	- Perda total	= Sinal	> Sensitivitade do Rádio 1

Caso o sinal recebido seja maior que o mínimo nível de sinal aceitável em ambas as direções do link, considerando os ruídos recebidos ao longo do caminho, então o link é possível.

Softwares para planejamento do link

Mesmo que o cálculo manual do orçamento do link seja simples, há uma série de ferramentas que podem ajudar na automação deste processo. Adicionalmente ao cálculo da perda no espaço aberto, estas ferramentas levam em conta muitos outros fatores relevantes (como a absorção por árvores, efeitos do terreno, clima e mesmo a estimativa de perda de sinal em áreas urbanas). Nesta sessão, discutiremos duas ferramentas livres que são úteis para o planejamento de links wireless: os utilitários online para projeto de rede do *Green Bay Professional Packet Radio* e o *Radio Mobile*.

CGIs para projeto interativo

O grupo *Green Bay Professional Packet Radio* (GBPRR) disponibiliza, online e gratuitamente, uma variedade de ferramentas úteis para o planejamento de links. Você pode acessá-las em http://www.qsl.net/n9zia/wireless/page09.html. Elas funcionarão em qualquer dispositivo que tenha um navegador web e uma conexão com a Internet.

Vamos olhar com detalhe a primeira ferramenta: ***Wireless Network Link Analysis*** (Análise de link de rede wireless), que pode ser encontrada em *http://my.athenet.net/~multiplx/cgi-bin/wireless.main.cgi*.

Para começar, digite o canal a ser usado no link. Ele pode ser especificado em MHz ou GHz. Caso você não saiba a freqüência, consulte a tabela no **Apêndice B**. Note que a tabela lista a freqüência central do canal, enquanto a ferramenta pede que seja digitada a maior freqüência transmitida. A diferença no resultado final é mínima, assim, sinta-se a vontade para usar a freqüência central. Mas, para usar a freqüência maior do canal, basta adicionar 11 MHz à freqüência central.

A seguir, digite os detalhes para o transmissor do outro lado do link, incluindo o tipo de linha de transmissão, ganho de antena e outros detalhes. Procure preencher todos os dados que conhecer ou puder estimar. Você pode até colocar a altura da antena e a elevação do local onde ela está montada. Estes dados serão usados para o cálculo do ângulo de balanço (*tilt angle*) da antena. Para o cálculo de passagem da zona Fresnel, você precisará da ferramenta *Fresnel Zone Calculator* do GBPRR.

A próxima sessão é bastante similar, mas inclui informação sobre a outra extremidade do link. Preencha os dados disponíveis nos campos apropriados.

Finalmente, a última sessão descreve o clima, o terreno e a distância do link. Preencha com tantos dados que souber ou puder estimar. A distância do link pode ser calculada fornecendo a latitude e longitude de ambas as extremidades do link, ou digitada manualmente.

Feito isto, clique no botão Submit para obter um relatório detalhado acerca do link proposto. Ele irá incluir todos os dados digitados, assim como a estimativa de perdas no caminho, taxas de erro e disponibilidade do link. Todos estes números são teóricos, mas podem dar uma idéia básica da viabilidade do link. Através do ajuste de valores no formulário, você pode fazer um exercício do tipo "e se...", verificando como a mudança de determinados parâmetros irão afetar a conexão.

Adicionalmente a ferramenta de análise básica do link, o GBPRR fornece uma "*super edition*", que produz um relatório no formato PDF, assim como uma série de outras ferramentas úteis (incluindo uma para o cálculo da zona Fresnel, um conversor de decibéis e uma calculadora para distância e direção, para ficar apenas em algumas delas). O código-fonte para a maioria das ferramentas também é fornecido.

Radio Mobile

Radio Mobile é uma ferramenta para o projeto e simulação de sistemas wireless. Ele prevê o desempenho de um link de rádio através do uso de informações sobre o equipamento e um mapa digital da área a ser coberta. O software é de domínio público, para o Windows, que pode também ser usado no Linux com o uso do emulador Wine.

O Radio Mobile usa um modelo digital de elevação de terreno (***digital terrain elevation model***) para o cálculo de cobertura, indicando a potência do sinal recebido em vários pontos ao longo do caminho. Ele automaticamente constrói um perfil entre dois pontos no mapa digital, mostrando a área de cobertura e a primeira zona Fresnel. Durante a simulação, ele verifica a linha de visão e calcula a perda no caminho, incluindo a que é devido a obstáculos. É possível criar redes de diferentes topologias, incluindo *master/slave*, ponto-a-ponto e multiponto. Ele funciona para sistemas que utilizam freqüências entre 100 kHz e 200 GHz. Mapas digitais de elevação (***Digital elevation maps – DEM***) estão livremente disponíveis a partir de várias fontes, cobrindo a maior parte do mundo. Os DEMs não mostram linhas costeiras ou outros acidentes geográficos facilmente identificáveis, mas podem ser facilmente combinados com outras fontes de dados (como fotografias aéreas ou mapas topográficos) em múltiplas camadas, para que seja possível a obtenção de representações geográficas de maior utilidade e representação mais fácil. Você também pode

digitalizar seus próprios mapas e combiná-los com DEMs. Mapas de elevação digital podem ser combinados com mapas digitalizados, fotos de satélite e serviços de mapas disponíveis na Internet (como o Google Maps) para a produção de projetos com bastante precisão.

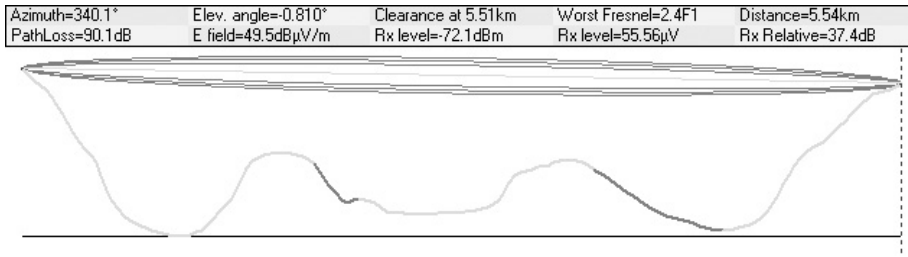


Figura 3.20: Viabilidade de link, incluindo estimativas de zona Fresnel e linha de visão, utilizando o Radio Mobile.

A página principal do Radio Mobile, com exemplos e tutoriais, está disponível em *http://www.cplus.org/rmw/english1.htm*

Radio Mobile com Linux

É possível utilizar o Radio Mobile com o Ubuntu Linux mas, enquanto a aplicação é executada, algumas legendas de botões podem ficar escondidas sobre a moldura dos mesmos e serem de difícil leitura.

Conseguimos executar o Radio Mobile em uma máquina Linux com o seguinte ambiente[5]:

- IBM Thinkpad x 31
- Ubuntu Breezy (v5.10), *http://www.ubuntu.com/*
- Wine versão 20050725, do repositório Ubuntu Universe

Há instruções detalhadas para a instalação do Radio Mobile no Linux em *http://www.cplus.org/rmw/english1.htm*l. Você deve seguir todos os passos listados, exceto o primeiro (uma vez que é difícil extrair uma DLL do arquivo VBRUN60SP6.EXE[6] no Linux). Você precisará de uma cópia do MSVBVM60.DLL de uma máquina Windows onde o run-time do Visual Basic 6 esteja instalado, ou simplesmente busque no Google o arquivo MSVBVM60.DLL e baixe-o para a sua máquina.

Agora, continue com o segundo passo do site acima, certificando-se de que a descompactação dos arquivos seja feita no mesmo diretório em que você colocou o DLL. Note que você não precisará preocupar-se com os passos

5. N. do T. - O tradutor conseguiu executar o Radio Mobile em uma distribuição Linux Mint Elyssa (baseada no Ubuntu Hardy), usando o Wine versão 0.9.59. Provavelmente, qualquer distribuição que aceite esta, ou qualquer outra versão mais recente do Wine, deve servir ao propósito. Os problemas com as legendas dos botões, descritos no texto, não foram sentidos.

6. N. do T. - Apenas usando o Wine, o tradutor pôde instalar apropriadamente o arquivo DLL, usando as instruções do site original do Radio Mobile.

seguintes ao quarto, uma vez que estes são necessários apenas para os usuários do Windows.

Para executar o programa, basta clicar duas vezes sobre ele, usando seu gerenciador de arquivos, ou através de um terminal com o seguinte comando:

```
# wine RMWDLX.exe
```

Isto deve apresentar a janela inicial do Radio Mobile em sua interface gráfica.

Evitando ruídos

As bandas irrestritas ISM e U-NII representam uma peça muito pequena do espectro eletromagnético conhecido. Como esta região pode ser usada sem o pagamento de licenças, muitos dispositivos a utilizam para um amplo número de aplicações. Telefones sem fio, transmissores analógicos de vídeo, Bluetooth, monitores para bebês e mesmo fornos de microondas competem com redes wireless no uso da bastante limitada banda de 2,4 GHz. Os sinais destes dispositivos, em conjunto com o sinal de outras redes wireless, podem causar problemas significativos para redes sem fio de longo alcance. Aqui apresentamos alguns passos que você pode seguir para reduzir a recepção de sinais indesejados.

- **Aumente o ganho da antena em ambos os lados de um link ponto-a-ponto**. Antenas não apenas adicionam ganho a um link, mas também aumentam sua direcionalidade e tendem a rejeitar ruídos vindos de áreas nos arredores do mesmo. Duas antenas parabólicas (em forma de prato) que apontam uma para a outra irão rejeitar sinais que estão fora do caminho do link. Antenas omnidirecionais receberão ruído de todas as direções.
- **Use antenas setoriais ao invés de usar uma antena omnidirecional**. Com o uso de múltiplas antenas setoriais, você pode reduzir a quantidade de ruído recebida em um ponto de distribuição. Com a divisão dos canais usados em cada setor, você pode também aumentar a largura de banda disponibilizada para seus clientes.
- **Não use um amplificador**. Como você verá no **Capítulo 4**, estes dispositivos podem piorar a recepção por amplificar indiscriminadamente todos os sinais recebidos, incluindo os de fontes de interferência. Os amplificadores também podem ser a causa de problemas de interferência para os outros usuários nas vizinhanças da banda utilizada.
- **Use o melhor canal disponível**. Lembre-se que os canais 802.11b/g têm a largura de 22 MHz, mas são separados por apenas 5 MHz. Faça uma pesquisa nos locais onde instalará seus equipamentos e escolha um canal que esteja o mais longe possível de fontes de interferência existentes. Lembre-se que o cenário wireless pode mudar a qualquer momento, uma vez que as pessoas podem passar a usar novos dispositivos (telefones sem fio, outras redes, etc). Se o seu link começar, repentinamente, a ter problema de transmissão de pacotes, você talvez precise fazer uma nova pesquisa de seu ambiente e selecionar um canal diferente.

- **Use pequenos saltos (hops) e repetidores, ao invés de cobrir uma longa distância com um link único**. Mantenha seus links ponto-a-ponto tão curtos quanto possível. Mesmo que seja possível criar um link de 12 kms que passe pelo meio de uma cidade, é bem provável que você tenha muitos problemas com interferências. Se você puder dividir este link em dois ou mais saltos (*hops*) curtos, ele ganhará mais estabilidade. Obviamente, isto não é viável em links de longa distância em áreas rurais, onde não há estruturas de rede elétrica ou suportes para antenas. Mas neste caso, problemas com ruídos também são improváveis.

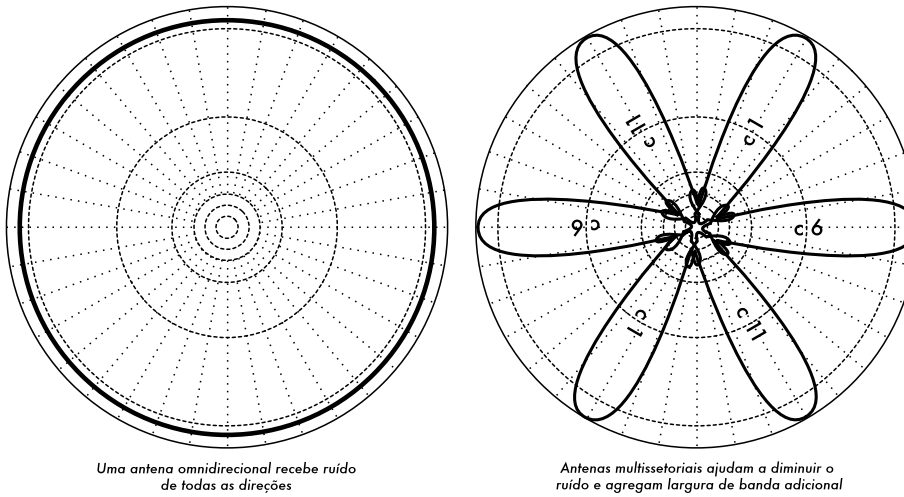


Figura 3.21: Uma antena omnidirecional em comparação com antenas multissetoriais.

- **Se possível, use bandas livres de 5,8 GHz, 900 MHz ou outras**. Mesmo sendo uma solução de curto prazo, hoje há muito mais equipamentos instalados que usam a freqüência de 2,4 GHz. Usando 802.11a ou um dispositivo que eleva a freqüência de 2,4 GHz para 5,8 GHz permitirá que o congestionamento seja evitado. Caso você consiga encontrá-los, alguns equipamentos antigos 802.11 usam o espectro livre de 900 MHz (infelizmente, com taxas de transmissão bem menores). Outras tecnologias, como Ronja (*http://ronja.twibright.com/*) usam a transmissão ótica para a implantação de links de curta distância, livres de ruído.

- **Se tudo isso falhar, use o espectro sob licença**. Existem lugares onde todo o espectro livre disponível já é, efetivamente, utilizado. Nestes casos, pode fazer sentido gastar mais dinheiro para a aquisição de equipamentos proprietários que usam bandas menos congestionadas. Para links ponto-a-ponto de longa distância que requerem uma alta taxa de transmissão esta é, certamente, uma opção. Claro que estas funcionalidades estão disponíveis em uma faixa de preço bem mais alta, comparada com a de equipamentos que operam nas bandas livres.

Para identificar as fontes de ruído, você precisará de ferramentas que mostrem o que está acontecendo no ar, em 2,4 GHz. Veremos alguns exemplos destas ferramentas no **Capítulo 6**.

Repetidores

O componente mais crítico na construção de links de longa distância é a linha de visão (***line of sight***, ou ***LOS***). Sistemas terrestres de microondas simplesmente não toleram altas colinas, árvores ou outros obstáculos no caminho de uma conexão de longa distância. Você deve ter uma boa idéia da topografia do espaço entre os dois pontos que deseja conectar, antes de determinar se o link é mesmo possível.

Mas mesmo que exista uma montanha entre dois pontos, lembre-se que os obstáculos podem, às vezes, serem usados em nosso benefício. Montanhas podem bloquear seu sinal, mas, assumindo que uma rede elétrica esteja disponível, elas podem ser locais muito bons para a instalação de repetidores.

Repetidores (***repeaters***) são nós que estão configurados para retransmitir o tráfego que não tem por destino o próprio nó. Em uma rede mesh, todo nó é um repetidor. Em uma infra-estrutura de rede tradicional, nós podem ser configurados para passar adiante o tráfego para outros nós.

Um repetidor pode usar um ou mais dispositivos wireless. Quando apenas um rádio é utilizado (repetidor de um braço só, *one-arm repeater*), a eficiência é, de maneira geral, um pouco menor que a metade da banda disponível, uma vez que o rádio pode apenas transmitir ou receber dados, nunca os dois ao mesmo tempo. Estes dispositivos são mais baratos, mais simples e possuem requerimentos menores de energia elétrica. Um repetidor com dois ou mais rádios pode operá-los em sua capacidade total, desde que eles estejam configurados para que não usem canais que interfiram um com o outro. Claro que repetidores podem também prover uma conexão Ethernet para equipamentos locais.

Repetidores podem ser adquiridos como uma solução completa de hardware ou implementados de forma simples através da conexão de um ou mais nós wireless por meio de um cabo Ethernet. Quando planejar o uso de um repetidor construído com a tecnologia 802.11, lembre-se que os nós devem ser configurados para o modo master, gerenciado ou ad-hoc. Tipicamente, ambos os rádios em um repetidor são configurados em modo master, permitindo que múltiplos clientes conectem-se com qualquer lado do repetidor. Mas dependendo do projeto de sua rede, um ou mais dispositivos podem necessitar o uso do modo ad-hoc ou mesmo do modo cliente.

Tipicamente, repetidores são usados para superar obstáculos no caminho de um link de longa distância. Por exemplo, podem existir prédios em seu caminho, mas nestes prédios moram pessoas. Com freqüência, podem ser feitos acordos com o proprietário do prédio para que a oferta de serviços de conectividade a eles seja trocada pelos direitos de uso do telhado e da eletricidade. Mesmo que o proprietário do prédio não esteja interessado, os moradores dos andares mais altos podem ser persuadidos a instalar o equipamento em uma janela.

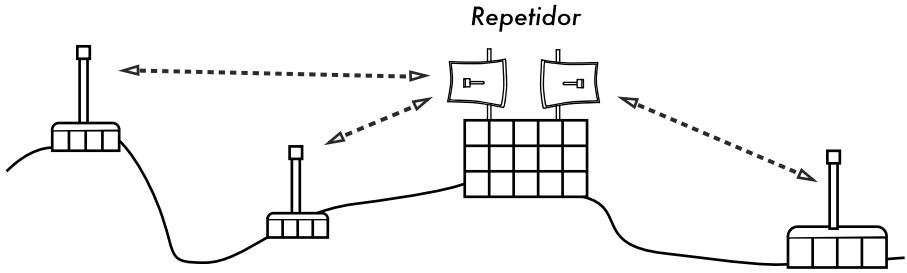


Figura 3.22: O repetidor encaminha pacotes entre os nós que não possuem uma linha de visão direta entre eles.

Caso você não possa atravessar um obstáculo, você pode contorná-lo. Ao invés de usar um link direto, tente um projeto com múltiplos hops para evitá-lo.

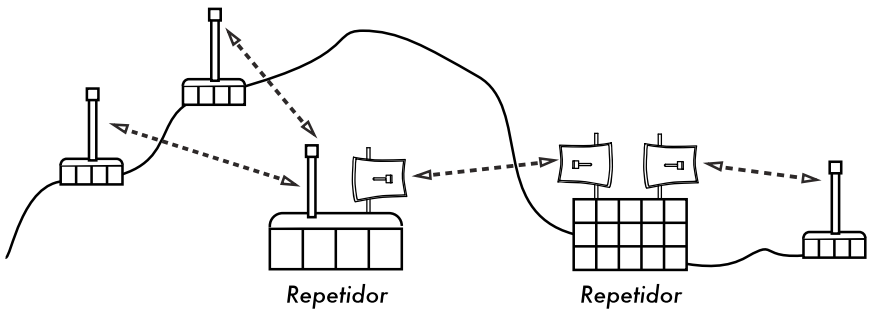


Figura 3.23: Não havia energia elétrica no topo da colina, mas a mesma foi contornada com o uso de múltiplos repetidores ao redor da base.

Finalmente, você deve considerar ir para trás, ao invés de ir adiante. Caso exista um local alto disponível em uma direção diferente, mas que possa ser visto além do obstáculo, uma conexão estável poderá ser possível com o uso de uma rota indireta.

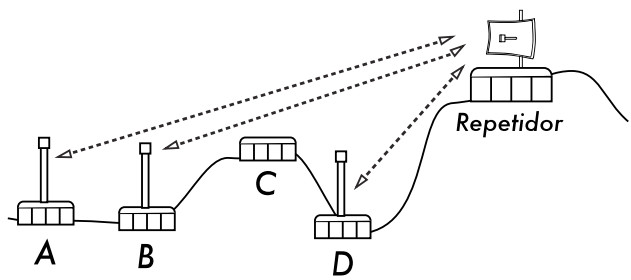


Figura 3.24: A localidade D não consegue estabelecer uma conexão direta para a localidade A ou B, pois C está no caminho e não há nenhum nó disponível ali. Com a instalação de um repetidor alto, os nós A, B e D podem comunicar-se. Note que o tráfego do nó D primeiro afasta-se da rede, antes que o repetidor encaminhe-o adequadamente.

Os repetidores em redes fazem-me lembrar do princípio de "seis graus de separação". A idéia é a de que não importa quem você está procurando, você precisará apenas contatar cinco intermediários antes de encontrar tal pessoa. Repetidores em localidades altas podem "ver" um grande número de intermediários, e desde que seu nó esteja ao alcance do repetidor, você pode comunicar-se com qualquer outro nó que o repetidor possa alcançar.

Otimização de tráfego

A largura de banda é a medida da quantidade de bits que podem ser transmitidos em um intervalo de tempo. Isto quer dizer que, na medida que o tempo passa, a largura de banda disponível em um link aproxima-se do infinito. Infelizmente, para qualquer período definido de tempo, a largura de banda fornecida por qualquer rede não é infinita. Você sempre pode fazer o download (ou upload) da quantidade de informação que quiser; apenas terá que esperar o tempo suficiente para isso. Claro que usuários humanos não são tão pacientes quanto os computadores e não desejam esperar um tempo infinito para que seus dados atravessem a rede. Por esta razão, a largura de banda deve ser gerenciada e priorizada da mesma forma que qualquer outro recurso limitado.

Você aumentará significativamente o tempo de resposta e maximizará a taxa de transferência disponível através da eliminação do tráfego não desejado e redundante em sua rede. Esta sessão descreve algumas técnicas comuns que garantem que sua rede apenas carregue o tráfego que deve atravessá-la. Para uma discussão mais aprofundada do complexo assunto de otimização de ocupação de banda, leia o livro *How to Accelerate Your Internet* (*http://bwmo.net/*), que está disponível livremente.

Web caching

Um web proxy é um servidor em sua rede local que mantém cópias de páginas recentemente vistas, ou as mais freqüentemente visitadas, ou partes de páginas na web. Quando a próxima pessoa buscar estas páginas, elas serão servidas pelo servidor proxy local ao invés de virem da Internet. Isto resulta, na maioria dos casos, em um acesso web mais rápido, ao mesmo tempo em que reduz, de forma geral, o uso da largura de banda na Internet. Quando um servidor proxy é implementado, o administrador deve também saber que algumas páginas não podem ser armazenadas localmente – por exemplo, aquelas geradas por scripts no servidor, ou outros conteúdos gerados dinamicamente.

A aparente carga das páginas web também é afetada. Com uma conexão de baixa velocidade com a Internet, uma página estática começa a ser carregada lentamente, primeiro mostrando algum texto e depois as figuras, uma a uma. Em uma rede com um servidor proxy, pode haver a percepção de um pequeno atraso, dentro do qual nada parece acontecer, e então a página é carregada quase imediatamente. Isto acontece porque a informação é enviada tão rapidamente ao computador que ele necessita de uma quantidade perceptível de tempo para renderizar (montar e exibir) a página. O tempo total que uma página inteira leva para ser carregada pode ser de apenas dez segundos (enquanto, sem um servidor proxy, poderia demorar 30 segundos para carregar gradualmente a página). Mas, a não ser que isto seja explicado para alguns

usuários impacientes, eles podem achar que o servidor proxy tornou as coisas mais lentas. Usualmente, é tarefa do administrador de rede lidar com questões de percepção como esta.

Produtos para servidores proxy

Há uma série de servidores web proxy disponíveis. Estes são os pacotes de software mais comumente usados:

- **Squid**. O Squid, de código aberto, é o padrão de fato em universidades. Ele é gratuito, confiável, fácil de usar e pode ser melhorado (por exemplo, com a adição de filtragem de conteúdo e bloqueio de propagandas). O Squid gera registros que podem ser analisados por programas como o Awstats ou Webalizer, ambos de código aberto, capazes de produzir bons relatórios gráficos. Na maioria dos casos, é mais fácil instalá-lo como parte de sua distribuição do que fazer o download diretamente de *http://www.squid-cache.org/* (a maioria das distribuições Linux, como o Debian, assim como outras versões de Unix como o NetBSD e o FreeBSD já têm o Squid). Um bom guia de configuração do Squid pode ser encontrado no *Squid Users Guide Wiki* em *http://www.deckle.co.za/squid-users-guide/*.

- **Microsoft Proxy server 2.0**. Não está disponível para novas instalações, pois foi sucedido pelo servidor Microsoft ISA, e não é mais suportado. Mesmo assim, ele é utilizado por algumas instituições, mas não deve ser considerado para novas instalações.

- **Microsoft ISA server**. O ISA server é um servidor proxy muito bom, mas talvez muito caro para o que faz. Entretanto, com descontos acadêmicos ele pode ser acessível para algumas instituições. Ele produz seus próprios relatórios gráficos, mas seus registros podem também ser analisados por ferramentas populares como Sawmill (*http://www.sawmill.net/*). Os administradores em localidades que usam o MS ISA Server devem dispender tempo suficiente para configurá-lo corretamente, pois, de outra forma, o próprio servidor pode tornar-se um considerável usuário de largura de banda. Por exemplo, uma instalação padrão pode facilmente consumir mais banda que a usada anteriormente, pois páginas populares com datas de expiração curtas (tais como sites de notícias) serão continuamente atualizadas. Por isso, é importante ter os parâmetros de pre-fetching (busca antecipada) definidos corretamente, e que o processo de pre-fetching ocorra, preferencialmente, na madrugada. O ISA Server pode também ser usado com produtos de filtragem de conteúdo, como o WebSense. Para mais informações, visite *http://www.microsoft.com/isaserver/* e *http://www.isaserver.org/* .

Evitando que os usuários contornem o servidor proxy

Mesmo que o contorno a censuras impostas à Internet e a política de acesso à informações restritas possam ser um louvável esforço político, proxies e firewalls são ferramentas necessárias em áreas com largura de banda

extremamente limitada. Sem tais ferramentas, a estabilidade e usabilidade da rede podem ser ameaçadas pelos próprios usuários legítimos da rede. Técnicas para contornar (*bypass*) um servidor proxy podem ser encontradas em *http://www.antiproxy.com/*. Este site é útil para administradores de rede, para que eles vejam como seus sistemas resistem a estas técnicas.

Para forçar o uso do proxy que armazena o conteúdo localmente (*caching proxy*), você deve considerar a simples elaboração de uma política de acesso à rede e confiar que seus usuários a respeitarão. Na configuração abaixo, o administrador tem que confiar que seus usuários não contornarão o servidor proxy.

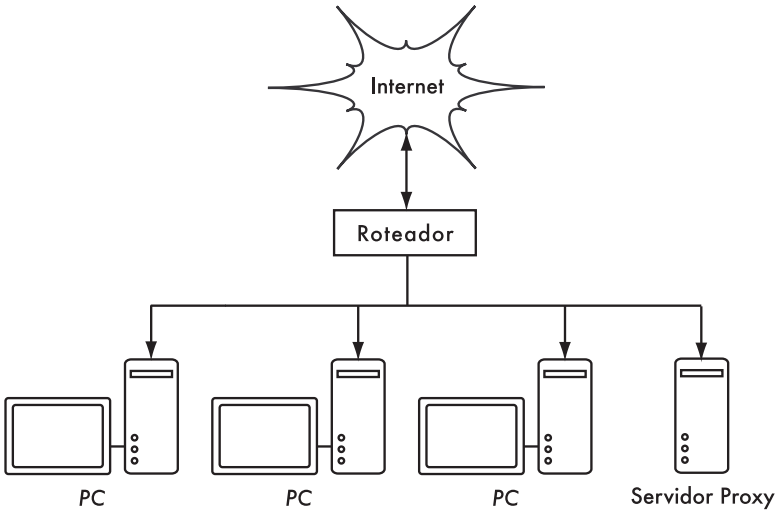


Figura 3.25: Esta rede parte do princípio de que usuários confiáveis configurem propriamente seus Pcs para que usem o servidor proxy.

Neste caso, o administrador utilizará, tipicamente, uma das seguintes técnicas:

- **Não disponibilizar o endereço do gateway padrão através de DHCP**. Isto pode funcionar por um tempo, mas alguns usuários conhecedores de redes que querem contornar o proxy podem descobrir, ou tentar adivinhar, o endereço do gateway padrão. Uma vez que tal endereço é descoberto, a tendência é que a informação sobre como contornar o proxy seja espalhada.
- **Uso de políticas de domínios ou grupos**. Isto é bastante útil para a configuração dos parâmetros de servidor proxy para o Internet Explorer em todos os computadores em um domínio, mas não garante que o proxy não seja contornado porque depende da autenticação do usuário no domínio NT. Um usuário com o Windows 95/98/ME pode cancelar sua autenticação (logon) e então contornar o proxy, e alguém que conheça a senha local em um Windows NT/2000/XP pode autenticar-se localmente e fazer o mesmo.
- **Implorar e brigar com os usuários**. Esta técnica, mesmo comum, nunca é a melhor situação para um administrador de rede.

Firewall

Uma forma mais confiável de garantir que os PCs não evitem o proxy pode ser implementada usando o firewall. O firewall pode ser configurado para permitir que apenas o servidor proxy faça solicitações HTTP para a Internet. Todos os demais PCs serão bloqueados, como mostra a **Figura 3.26**.

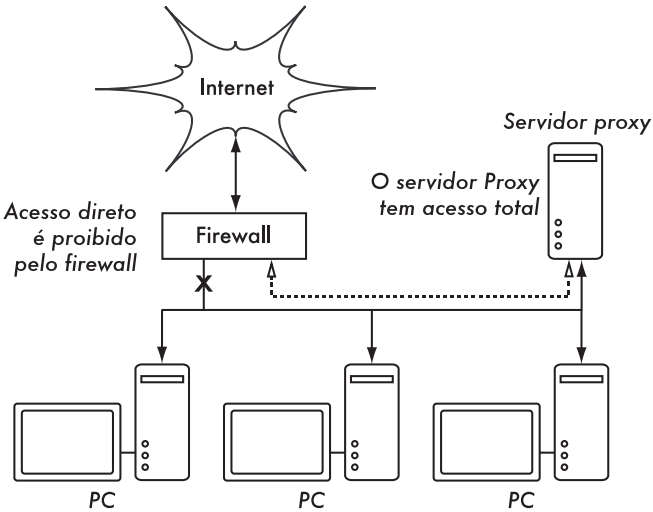


Figura 3.26: O firewall evita que os PCs acessem diretamente a Internet, mas permite este acesso através do servidor proxy.

Confiar em um firewall pode, ou não, ser suficiente, dependendo da forma como ele está configurado. Se ele apenas bloquear o acesso da rede local do campus para a porta 80 dos servidores web, usuários inteligentes ainda encontrarão meios de contornar este bloqueio. Eles também poderão usar outros serviços famintos por banda, como o BitTorrent ou Kazaa.

Dois cartões de rede

Talvez o mais confiável método seja a instalação de dois cartões de rede no servidor proxy, conectando a rede do campus à Internet como mostrado abaixo. Desta forma, a configuração da rede torna fisicamente impossível o acesso à Internet sem que se passe pelo servidor proxy.

O servidor proxy neste diagrama não deve ter o encaminhamento de IP (*IP forwarding*) habilitado, a não ser que os administradores de rede saibam exatamente o que eles querem deixar passar.

Uma grande vantagem desta configuração é que uma técnica conhecida como ***proxy transparente*** (***transparent proxying***) pode ser usada. Isto significa que os pedidos de acesso à web pelos usuários são automaticamente passados para o servidor proxy, sem nenhuma necessidade de configuração dos navegadores. A técnica faz com que, efetivamente, todo o tráfego seja armazenado localmente pelo proxy, eliminando muitas chances de erros de usuários, permitindo mesmo que se trabalhe com dispositivos que não suportem

a configuração manual para o acesso através de um proxy. Para mais detalhes sobre a configuração de um proxy transparente com o Squid, veja:

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

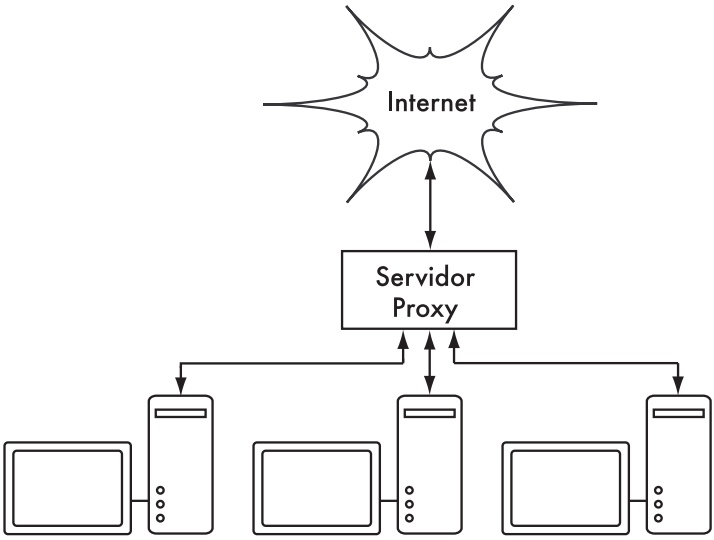


Figura 3.27: A única rota para a Internet é através do proxy.

Políticas de roteamento

Uma forma de prevenir o contorno do proxy, usando equipamento Cisco, é o uso de políticas de roteamento. O roteador Cisco direciona, de forma transparente, todo o tráfego web para o servidor proxy. Esta técnica é usada na Makerere University. A vantagem deste método é que, caso o servidor proxy não esteja funcionando, a política de roteamento pode ser temporariamente removida, permitindo que os clientes conectem-se diretamente à Internet.

Espelhando um website

Com a permissão do proprietário ou web master de um site, ele pode ser completamente espelhado para o servidor local durante a madrugada, caso não seja muito grande. Isto é algo que deve ser considerado para websites que são de particular interesse para a organização, ou aqueles que são muito populares entre os usuários. Assim como pode ser de grande utilidade, esta técnica também tem suas falhas. Por exemplo, caso o site a ser espelhado tenha scripts CGI ou outro conteúdo dinâmico que necessite de interação com o usuário, isto irá causar problemas. Uma pessoa que entra com seus dados em um site para o registro em uma conferência, onde os scripts de registro também foram espelhados localmente, pode não ter o seu registro efetivado no site real.

O espelhamento de um site pode infringir direitos autorais. Por isso, esta técnica deve apenas ser usada com a permissão formal para o site a ser

espelhado. Caso o site use ***rsync***, ele pode ser espelhado com o mesmo. Este é, provavelmente, o meio mais rápido e eficiente de manter conteúdos sincronizados. Caso o site remoto não utilize o rsync, o software recomendado é o ***wget***. Ele é parte da maioria das versões de Unix/Linux. Uma versão para Windows pode ser encontrada em *http://xoomer.virgilio.it/hherold/*, ou no pacote livre de ferramentas Cygwin Unix (*http://www.cygwin.com/*).

Um script pode ser configurado no servidor web local para que, todas as noites, faça o seguinte:

Vá para o diretório raiz de documentos do servidor web: por exemplo **`/var/www/`** no Unix, ou **`C:\Inetpub\wwwroot`** no Windows;

Faça o espelhamento do website com o seguinte comando:

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

O website espelhado ficará no diretório *www.python.org*. O servidor web deve agora ser configurado para servir o conteúdo deste diretório em um host virtual. Configure o servidor DNS local para "imitar" uma entrada para este site. Para que isto funcione, os PCs clientes devem ser configurados para usar o servidor DNS local como seu DNS primário (isto é recomendável em todos os casos, já que um DNS local acelera o tempo de resposta da web).

Popule antecipadamente o cache usando wget

Ao invés de configurar o espelhamento de um website, como descrito na sessão anterior, uma técnica melhor é a de popular o proxy cache usando um processo automatizado. Este método foi descrito por J. J. Eksteen e J. P. L. Cloete do CSIR em Pretória, África do Sul, no artigo *Enhancing International World Wide Web Access in Mozambique Through the Use of Mirroring and Caching Proxies* (Melhorando o acesso internacional para a web em Moçambique através do uso de espelhamento e proxies de armazenamento local). Neste artigo (disponível em *http://www.isoc.org/inet97/ans97/cloet.htm*) eles descrevem como este processo funciona:

> *"Um processo automático busca a página principal do site e um número especificado de páginas adicionais (recursivamente seguindo os links HTML nas páginas buscadas) através do uso de um proxy. Ao invés de gravar as páginas buscadas no disco local, o processo de espelhamento as descarta. Isto é feito para conservar recursos do sistema e também para evitar possíveis conflitos de direitos autorais. Através do uso do proxy como um intermediário, as páginas buscadas ficam, com certeza, no cache do proxy, como se um usuário tivesse acessado tais páginas. Quando um cliente acessa uma página já armazenada, ela é servida do cache e não do congestionado link internacional. Este processo pode ser executado fora dos horários de pico a fim de maximizar o uso da banda e não competir com outras atividades que requeiram acesso à web."*

O comando a seguir (programado para ser executado todas as noites, ou uma vez por semana) é tudo o que é necessário (repetido para cada site que deva ser populado antecipadamente).

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

Estas opções habilitam o seguinte:

- **-m**: Espelha o site inteiro. O wget inicia em *www.python.org* e segue os links, baixando, então, todas as páginas;
- **--proxy-on**: Espelha o site inteiro. O wget inicia em www.python.org e segue os links, baixando, então, todas as páginas;
- **--c cache-off**: Garante que o conteúdo recente seja buscado da Internet e não do servidor proxy local;
- **--delete after**: Apaga a cópia espelhada. O conteúdo espelhado é mantido no cache do proxy, desde que exista espaço suficiente em disco e os parâmetros de configuração estejam corretamente ajustados.

Adicionalmente, o wget tem muitas outras opções, por exemplo, fornecendo uma senha para sites que necessitem de uma. Quando esta ferramente é usada, o Squid deve ser configurado com o espaço em disco suficiente para conter todos os sites pré-populados e mais (para o uso normal do Squid, incluindo as demais páginas que não são pré-populadas). Felizmente, espaço em disco está se tornando cada vez mais barato e em quantidades cada vez maiores. Ainda assim, esta técnica deve ser usada apenas para alguns poucos sites selecionados. Eles não podem ser grandes a ponto de fazer com que o processo demore além da madrugada e a utilização do espaço em disco deve ser monitorada.

Hierarquias de cache

Quando uma organização tem mais de um servidor proxy, eles podem compartilhar a informação armazenada entre eles. Por exemplo, se uma página existir no cache do servidor A, mas não no cache do servidor B, um usuário conectado através do servidor B pode obter o conteúdo armazenado no servidor A através do servidor B. Os protocolos ***ICP*** (***Inter-Cache Protocol*** – protocolo inter-cache) e ***CARP*** (***Cache Array Routing Protocol*** – protocolo de roteamento para matriz de caches) podem ser usados para o compartilhamento da informação entre caches. O CARP é considerado o melhor protocolo. O Squid tem suporte a ambos os protocolos e o servidor MS ISA suporta o CARP. Para mais informações consulte *http://squid-docs.sourceforge.net/latest/html/c2075.html*. Este compartilhamento de informações reduz o consumo de banda em organizações onde mais de um proxy é utilizado.

Especificações do proxy

Na rede de um campus de uma universidade deve existir mais de um servidor proxy, tanto por questões de desempenho quanto por redundância. Com os discos baratos, de grande capacidade, disponíveis hoje, servidores proxy poderosos podem ser construídos, com 50 GB ou mais de espaço em disco alocado para o cache. O desempenho do disco é importante, por isso os discos com interface SCSI terão a melhor performance (mas um cache baseado em discos IDE ainda é melhor do que não ter um cache). O espelhamento RAID ou de outro tipo não é recomendado.

Também é recomendável ter um disco dedicado exclusivamente ao cache. Por exemplo, um disco poderia ser usado para o cache e um outro para o

sistema operacional e para os registros (logs) do cache. O Squid foi projetado para usar o máximo de memória RAM que puder, uma vez que os dados, quando estão na RAM, são obtidos com velocidade muito maior do que quando estão no disco rígido. Para a rede de um campus, a memória RAM deve ser de 1 GB ou mais:

- Além da memória requerida pelo sistema operacional e outras aplicações, o Squid necessita de 10 MB de RAM para cada 1 GB de cache em disco. Assim, se há 50 GB alocados em espaço no disco para o cache, o Squid precisará de 500 MB de memória adicional;
- A máquina também precisará de 128 MB para o Linux e 128 MB para o Xwindows;
- Mais 256 MB devem ser adicionados para outras aplicações e a fim de que tudo seja executado devidamente. Nada melhora mais o desempenho de uma máquina do que a adição de uma grande capacidade de memória, já que isto reduz a necessidade de uso do disco rígido. A memória é milhares de vezes mais rápida do que o disco rígido. Sistemas operacionais modernos mantêm os dados freqüentemente acessados na memória, desde que haja RAM disponível o suficiente, mas usam páginas de arquivo como memória extra, caso a RAM não seja suficiente.

Cache de DNS e otimização

DNSs apenas de cache (caching-only DNS) são servidores sem autoridade para nenhum domínio, apenas armazenando os resultados das buscas solicitadas pelos clientes. Assim como um servidor proxy que armazena as páginas web populares por algum tempo, os endereços DNS são armazenados até que seu tempo de vida (***TTL*** – ***time to live***) expire. Isto reduz a quantidade de tráfego DNS em uma conexão com a Internet, uma vez que o DNS cache pode satisfazer muitas das resoluções de endereço localmente. Obviamente, os computadores clientes devem ser configurados de forma a usar o servidor de nomes em cache como seu servidor DNS. Quando todos os clientes usam este servidor como seu DNS primário, ele rapidamente terá seu cache populado com a relação entre endereços IP e nomes e, desta forma, a resolução para endereços já armazenados pode ser feita rapidamente. Servidores DNS que têm autoridade sob um domínio podem também atuar como cache para mapas de endereços de hosts resolvidos por eles.

Bind (named)

O Bind é o programa padrão de fato para o serviço de nomes na Internet. Quando o Bind está instalado e em execução, ele irá atuar como um servidor caching-only, sem a necessidade de configuração adicional. O Bind pode ser instalado a partir de um pacote, como um pacote Debian ou um RPM. A instalação a partir de um pacote é, usualmente, o método mais simples. No Debian, digite:

```
apt-get install bind9
```

Além de rodar um cache, o Bind pode também rodar na forma de servidor com autoridade para zonas de nomes, servir como escravo para zonas de nomes, implementar horizonte dividido (*split horizon*) e qualquer outra configuração possível com DNS.

dnsmasq

Um servidor caching-only alternativo é o ***dnsmasq***. Existem pacotes disponíveis para o BSD e para a maioria das distribuições Linux, ou diretamente em *http://www.thekelleys.org.uk/dnsmasq/*. A grande vantagem do dnsmasq é sua flexibilidade: ele atua tanto como um caching DNS como fonte de autoridade para servidores e domínios, sem a complexidade de um arquivo de configuração de zonas. As zonas podem ser atualizadas sem a necessidade de reinicializar o serviço. Ele também pode servir como um servidor DHCP e integrar o serviço de DNS com as solicitações de DHCP dos servidores. Ele é bastante leve, estável e extremamente flexível. O Bind é, provavelmente, a melhor escolha para redes muito grandes (mais de algumas centenas de nós), mas a simplicidade do dnsmasq o torna atrativo para redes de tamanho pequeno ou médio.

Windows NT

Para instalar o serviço de DNS em um Windows NT4: selecione *Control Panel* ➔ *Network* ➔ *Services* ➔ *Add* ➔ *Microsoft DNS server*. Coloque o CD do Windows NT4 quando solicitado. A configuração de um servidor caching-only no NT é descrita no artigo 167234 do Knowledge Base. Do artigo:

> *"Simplesmente instale o DNS e execute o Domain Name System Manager. Clique em DNS no menu, selecione New Server e digite o endereço IP do computador onde você tem o DNS instalado. Você agora tem um servidor DNS caching- only."*

Windows 2000

Instalação do serviço DNS: *Start* ➔ *Settings* ➔ *Control Panel* ➔ *Add/Remove Software*. Em *Add/Remove Windows Components*, selecione *Components* ➔ *Networking Services* ➔ *Details* ➔ *Domain Name System (DNS)*. Agora execute o DNS MMC (*Start* ➔ *Programs* ➔ *Administrative Tools* ➔ *DNS*). No menu Action selecione "*Connect To Computer*...". Na janela *Select Target Computer*, habilite "*The following computer*:" e coloque o nome do servidor DNS do qual você quer fazer cache. Se houver um . [ponto] no DNS manager (isto aparece como padrão), significa que o servidor DNS pensa que ele é o servidor DNS raiz da Internet, o que ele, certamente, não é. Apaque o . [ponto] para que qualquer coisa possa funcionar.

DNS dividido (Split DNS) e servidor espelhado

O propósito do DNS dividido (split DNS, também conhecido como horizonte dividido–***split horizon***) é apresentar uma visão diferente de seu domínio para os mundos interno e externo. Há mais de uma maneira de fazer um DNS dividido, mas, por razões de segurança, é recomendável que você tenha separados os conteúdos de seus servidores DNS interno e externo (cada um com base de dados distinta).

O split DNS pode permitir que clientes na rede de um campus resolvam endereços do domínio local do campus para os IPs do tipo RFC1918, enquanto o resto da Internet resolve os mesmos nomes para endereços IPs diferentes. Isto é conseguido tendo duas zonas em dois servidores DNS diferentes para o mesmo domínio.

Uma das zonas é usada pelos clientes da rede interna e a outra por usuários na Internet. Por exemplo, na rede abaixo, o usuário no campus de Makerere tem o endereço *http://www.makerere.ac.ug/* resolvido para 172.16.16.21, enquanto outro usuário qualquer na Internet tem o mesmo resolvido para 195.171.16.13.

O servidor DNS do campus, no caso acima, tem um arquivo de zona para makerere.ac.ug e está configurado como autoridade para este domínio. Em adição, ele serve como caching DNS para o campus de Makerere e todos os computadores no campus estão configurados para usá-lo como seu servidor DNS.

Os registros de DNS para o servidor do campus serão parecidos com estes:

```
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
```

Mas há outro servidor DNS na Internet que é realmente autoridade para o domínio *makerere.ac.ug*. Os registros DNS para a zona externa se parecerão com estes:

```
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
```

O DNS dividido não é dependente do uso de endereçamento RFC 1918. Um provedor de acesso à Internet africano poderia, por exemplo, hospedar os websites da universidade, mas também espelhar estes mesmos websites na Europa. Sempre que um cliente daquele provedor acessar o website, ele terá um endereço IP do provedor africano, mantendo o tráfego dentro do mesmo país. Quando visitantes de outros países acessarem o website, eles obtêm o endereço IP do site espelhado na Europa. Desta forma, visitantes internacionais não irão congestionar a conexão VSAT do provedor quando visitarem o site da universidade. Isto está se tornando uma solução atrativa, na medida em que a hospedagem de sites próximos ao backbone (links centrais, de alta velocidade) da Internet tornaram-se muito baratos.

Otimização do link de Internet

Como já foi mencionado, uma taxa de transmissão de 22 Mbps na rede pode ser atingida com o uso de equipamentos wireless no padrão 802.11g, sem necessidade de licenças. Esta largura de banda será ao menos uma ordem de magnitude acima daquela fornecida pela sua conexão com a Internet, e deve ser

suficientemente confortável para o suporte a muitos usuários simultâneos da Internet.

Mas se a sua conexão primária com a Internet for através de um link VSAT, você enfrentará alguns problemas de desempenho caso utilize apenas os parâmetros padrão do TCP/IP. Com a otimização do link VSAT você poderá melhorar significativamente os tempos de resposta no acesso a servidores na Internet.

Fatores TCP/IP em uma conexão via satélite

Freqüentemente, referimo-nos a um VSAT como uma rede de cano longo e grosso (***long fat pipe network***). Este termo tem a ver com os fatores que afetam o desempenho do TCP/IP em qualquer rede que tenha uma largura de banda relativamente grande, mas alta latência. A maioria das conexões à Internet na África e em outras partes do mundo em desenvolvimento são feitas com VSAT. Desta forma, mesmo que uma universidade tenha sua conexão à Internet fornecida por um provedor de acesso, a instruções fornecidas aqui também se aplicam, caso a conexão deste provedor à Internet for através de VSAT. A alta latência de redes via satélite é devida à longa distância até o satélite e à velocidade constante da luz. A distância adiciona cerca de 520 ms para o tempo de viagem de um pacote (***RTT*** – ***round-trip time***), comparado com um RTT típico entre a Europa e os Estados Unidos, de cerca de 140 ms.

Os fatores que mais significativamente impactam o desempenho do TCP/IP são ***RTT longo***, ***atrasos de entrega em largura de banda alta*** e ***erros de transmissão***.

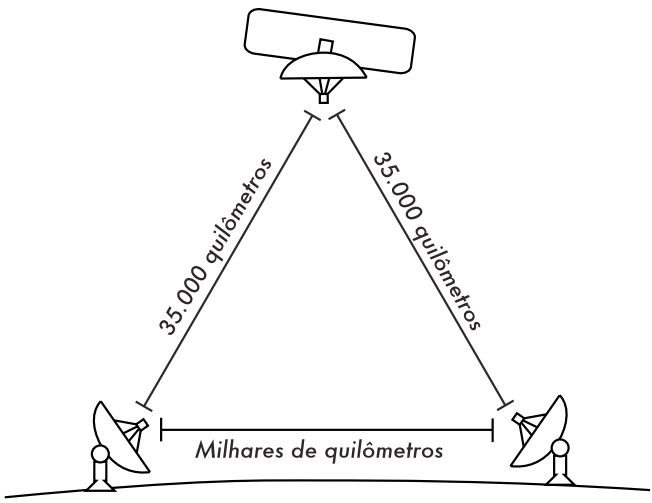


Figura 3.28: Devido à velocidade da luz e das longas distâncias envolvidas, um simples pacote de ping pode demorar mais de 520 ms para ser recebido em um link VSAT.

De maneira geral, sistemas operacionais que suportam implementações modernas de TCP/IP devem ser usados em redes via satélite. Estas implementações fornecem o suporte às extensões RFC 1323:

- A opção ***window scale*** para o suporte à largas janelas TCP (maiores que 64 KB);
- ***Selective acknowledgement*** (***SACK*** – reconhecimento seletivo) para permitir a rápida recuperação de erros de transmissão;
- ***Timestamps*** (registros de tempo) para o cálculo apropriado de RTT e valores de retransmissão por expiração de tempo (*timeout*) para o link em uso.

RTT Longo

Links via satélite tem um RTT médio de 520 ms para o primeiro enlace. O TCP usa um mecanismo de inicialização lenta (*slow start*) no estabelecimento da conexão a fim de descobrir os parâmetros apropriados para a mesma. O tempo gasto no estágio de inicialização lenta é proporcional ao RTT, o que significa que, em um link via satélite, este estágio dura mais tempo do que duraria em outros casos. Isto diminui drasticamente a taxa de transferência em conexões TCP de curta duração. Observa-se isto quando um website pequeno demora um tempo surpreendentemente longo para ser carregado, mas um arquivo grande é transferido a taxas de transferência aceitáveis.

Além disto, quando pacotes são perdidos o TCP entra em fase de controle de congestionamento (*congestion-control*) e, devido ao longo RTT, permanece nesta fase por um longo tempo, assim reduzindo a taxa de transferência tanto para conexões TCP de curta como de longa duração.

Produto do atraso de entrega em largura de banda alta (Large bandwidth-delay product)

A quantidade de dados em trânsito num link, em qualquer período de tempo, é produto da largura de banda e do RTT. Devido à alta latência do link via satélite, o atraso de produto em largura de banda é grande. O TCP/IP permite que o servidor remoto envie uma certa quantidade de dados sem a necessidade de confirmação de recebimento. Uma confirmação é necessária para qualquer dado recebido em uma conexão TCP/IP. Entretanto, o servidor remoto sempre pode enviar uma certa quantidade de dados sem que uma confirmação seja recebida, o que é importante para que se consiga uma boa taxa de transmissão em redes com conexões que apresentam grandes atrasos de entrega. Esta quantidade de dados é chamada de tamanho de janela TCP (***TCP window size***). Em implementações modernas de TCP/IP, o tamanho de janela é, usualmente, 64 KB.

Em redes via satélite, o valor do produto do atraso de entrega é importante. Para utilizar o link integralmente, o tamanho da janela de conexão deve ser igual ao do produto do atraso de entrega. Se o tamanho máximo de janela permitido é de 64 KB, a máxima taxa de transferência, teoricamente, atingível via satélite é (tamanho da janela) / RTT, ou 64 KB / 520 ms. Isto resulta em uma taxa de transferência máxima de 123 KB/s, ou seja, 984 kbps, independente do fato da capacidade do link ser muito maior.

Cada cabeçalho de segmento TCP contém um campo chamado ***advertised window*** (janela publicada), que especifica quantos bytes adicionais de dados o

receptor está preparado para aceitar. A *advertised window* é o tamanho disponível do *buffer* do receptor.

O remetente não tem a permissão de enviar mais bytes do que a advertised window. Para maximizar o desempenho, o remetente deve configurar o tamanho de seu buffer de envio e o receptor o tamanho de seu buffer de recepção para um número que não seja menor que o produto do atraso de entrega. Este tamanho de buffer tem o valor máximo de 64 KB na maioria das implementações TCP/IP modernas.

Para contornar este problema em pilhas TCP/IP em sistemas operacionais que não aumentam a janela além dos 64 KB, uma técnica conhecida como ***TCP acknowledgment spoofing*** ("trapaça" no reconhecimento de recepção) pode ser usada (veja Melhora de desempenho com PEP, abaixo).

Erros de transmissão

Em implementações mais antigas de TCP/IP, a perda de pacotes era sempre considerada como resultado de congestionamentos (ao invés de erros de conexão). Quando isto acontece, o TCP realiza manobras para evitar congestionamentos, passando a requerer três ACKs (reconhecimento de recepção) duplicados ou uma reinicialização lenta em caso de um timeout. Em função do longo RTT, uma vez que esta fase de controle de congestionamento é iniciada, links TCP/IP via satélite irão levar um longo tempo até que voltem ao nível de taxa de transmissão anterior ao problema. Desta forma, erros em um link via satélite têm um efeito muito mais sério na performance do que o TCP em links de latência baixa. Para contornar esta situação, mecanismos como o ***SACK*** (***Selective Acknowledgement***) foram desenvolvidos. O SACK especifica exatamente aqueles pacotes que foram recebidos, permitindo ao remetente retransmitir apenas os segmentos que foram perdidos por causa de erros de conexão.

O artigo sobre os detalhes de implementação do TCP/IP no Microsoft Windows 2000 declara:

> *"O Windows 2000 introduz o suporte para uma funcionalidade importante de desempenho, conhecida como SACK (Selective Acknowledgement), especialmente para conexões que usam grandes janelas TCP."*

O SACK vem sendo uma funcionalidade padrão nos kernels Linux e BSD por um longo tempo. Certifique-se de que seu roteador Internet e seu provedor tenham, ambos, suporte ao SACK.

Implicações para universidades

Se uma localidade tem uma conexão de 512 kbps para a Internet, a configuração padrão do TCP/IP provavelmente será suficiente, uma vez que uma janela de 64 KB é o bastante para uma velocidade de 984 kbps. Mas se a universidade tiver uma conexão com velocidade acima de 984 kbps, em alguns casos não será possível utilizar toda a largura de banda disponível em função das características de uma rede de cano longo e grosso (***long fat pipe network***) que discutimos acima. Estes fatores realmente evitam que uma única máquina ocupe integralmente a banda, o que não é ruim durante o dia, pois

muitas pessoas estão usando a rede. Mas se, por exemplo, há uma grande programação de downloads para a madrugada, o administrador da rede possivelmente irá querer que estes ocupem toda a largura de banda e, neste caso, as características da rede de cano longo e grosso podem ser um obstáculo. Isto também pode ser crítico se uma significativa parte de seu tráfego de rede é roteada por um único túnel, ou uma conexão VPN para a outra ponta do link VSAT.

Os administradores devem tomar as devidas precauções para que o uso de toda a banda possa ser conseguido através do ajuste fino do TCP/IP. Caso uma universidade tenha implementado uma rede onde todo o tráfego passe por um proxy (assegurado pela configuração da rede), então as únicas máquinas que farão a conexão com a Internet serão este proxy e os servidores de email.

Para mais informações, veja *http://www.psc.edu/networking/perf_tune.html*.

Melhora de desempenho com PEP (Performance-enhancing proxy)

A idéia de um proxy que melhore o desempenho da rede, ou ***PEP*** (***Performance-enhancing proxy***), é descrita no RFC 3135 (*http://www.ietf.org/rfc/rfc3135*) e consiste em um servidor proxy com um grande espaço em disco para o cache, usando as extensões RFC 1323 dentre outras funcionalidades. Um laptop tem uma sessão TCP com o PEP de um provedor de acesso. Este PEP comunica-se com o que está na outra extremidade da conexão via satélite, usando uma outra sessão TCP ou mesmo um protocolo proprietário. O PEP do provedor da conexão via satélite obtém os arquivos do servidor web. Desta forma, a sessão TCP é dividida e as características do link que afetam o desempenho do protocolo (os fatores da rede de cano grosso e longo) são contornados, usando ***TCP acknowledgment spoofing*** ("trapaça" no reconhecimento de recepção), por exemplo. Adicionalmente, o PEP faz uso de técnicas de busca antecipada de conteúdos (pre-fetching) para acelerar ainda mais o acesso à web.

Sistemas assim podem ser construídos do zero com o uso do Squid, por exemplo, ou adquiridos de uma variedade de fornecedores.

Mais informações

Enquanto a otimização de banda é um tema complexo e freqüentemente difícil, as técnicas descritas neste capítulo devem ajudar a reduzir as fontes mais claras de desperdício no uso da rede. Para utilizar da melhor forma possível a largura de banda disponível, você precisará definir uma boa política de acesso, configurar boas ferramentas para o monitoramento e análise, e implementar uma arquitetura que reforce os limites de utilização da rede.

Para mais informações sobre a otimização da largura de banda, consulte o livro *How to Accelerate Your Internet* (*http://bwmo.net/*), que está disponível livremente.

4
Antenas e linhas de transmissão

O transmissor que gera energia de RF[1] para alimentar a antena está normalmente localizado a alguma distância dos conectores da mesma. A conexão entre os dois é a linha de transmissão de rádio freqüência. Sua finalidade é levar a energia de RF de um local a outro, fazendo isto da forma mais eficiente possível. Do lado do receptor, a antena é responsável por coletar qualquer sinal de rádio no ar, passando-o ao receptor com o mínimo de distorções, de forma que o rádio tenha a melhor chance de decodificar o sinal. Por isto, o cabo de RF tem um papel muito importante em sistemas de rádio: ele deve manter a integridade dos sinais em ambas as direções.

Há duas categorias principais de linhas de transmissão: cabos e guias de onda. Ambos funcionam bem no transporte de energia de RF na freqüência de 2,4 GHz.

Cabos

Cabos de RF são, para freqüências mais altas do que HF (*High frequency* – alta freqüência), quase exclusivamente do tipo coaxial (ou, abreviando-se, ***coax***, derivado das palavras "*of common axis*" -- de eixo comum). Cabos coaxiais possuem um fio ***condutor*** em seu núcleo, revestido por material não condutivo, chamado ***dielétrico*** ou ***isolamento***. O dielétrico é então revestido por uma blindagem, freqüentemente composta de fios elétricos trançados. O dielétrico evita a conexão elétrica entre a blindagem e o condutor central. Finalmente, o cabo coaxial é protegido por uma capa externa, geralmente feita com um material do tipo PVC. O condutor interno transporta o sinal de RF e a blindagem ao redor dele evita que este sinal irradie-se para a atmosfera, assim como previne que outros sinais interfiram com o que está sendo carregado. Outro fato interessante é que sinais elétricos de alta freqüência sempre viajam na camada

1. Rádio-freqüência. Veja o **Capítulo 2** para a discussão sobre ondas eletromagnéticas.

mais externa de um condutor: quanto maior o condutor central, melhor o sinal irá fluir. Isto é chamado de "efeito pelicular" (*skin effect*).

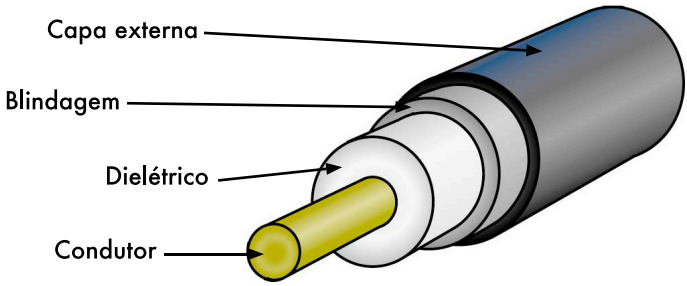


Figura 4.1: Cabo coaxial com capa externa, blindagem, dielétrico e condutor central.

Mesmo que a construção do cabo coaxial seja boa para conter o sinal dentro do condutor central, há alguma resistência ao fluxo elétrico: na medida em que o sinal viaja dentro do condutor, ele irá diminuir em intensidade. Esta diminuição é conhecida como ***atenuação***, que é medida, em linhas de transmissão, em decibéis por metro (***dB/m***). A taxa de atenuação é função da freqüência do sinal e da própria construção física do cabo. Quanto maior a freqüência do sinal, maior a atenuação. Obviamente, precisamos minimizar a atenuação no cabo o máximo possível, mantendo-o bem curto e usando material de boa qualidade.

Aqui estão alguns pontos que devem ser considerados na escolha de um cabo para o uso com equipamentos de microondas:

1. "Quanto menor, melhor!" A primeira regra para a instalação de um cabo é tentar mantê-lo o mais curto possível. A perda de potência não é linear, assim, dobrando o comprimento do cabo significa que você irá perder muito mais do que duas vezes a potência. Da mesma forma, reduzindo o cabo pela metade permite que se tenha mais de duas vezes a potência entregue à antena. A melhor solução é colocar o transmissor o mais perto possível da antena, mesmo quando isto significa instalá-lo em uma torre.

2. "Quanto mais barato, pior!" A segunda regra de ouro é a de que o dinheiro investido em um cabo de boa qualidade vale a pena. Cabos baratos são feitos para serem usados em baixas freqüências, como VHF (*Very High Frequency* – Freqüências Muito Altas, mas baixas se comparadas às microondas). Equipamentos de microondas necessitam dos cabos de maior qualidade disponível. Todas as outras opções são nada mais que cargas inúteis (*dummy load*[2])

3. Evite sempre o RG-58. Ele é projetado para o uso com redes Ethernet, rádios CB ou VHF, não para microondas.

---

2. Uma carga inútil (*dummy load*) é um dispositivo que dissipa energia de RF sem irradiá-la, apenas disperdiçando-a.

4. Evite sempre o RG-213. Ele é projetado para o uso com rádios CB ou HF. Neste caso, o diâmetro do cabo não implica em alta qualidade ou pouca atenuação.

5. Sempre que possível, use cabos ***Heliax*** (também chamados de cabos de "espuma") para conectar o transmissor à antena. Cabos Heliax possuem um condutor central sólido ou tubular, revestido por um outro condutor sólido, na forma de tiras longitudinais, que faz com que o conjunto todo seja flexível. Estes cabos podem ser construídos de duas maneiras, usando ar ou espuma como dielétrico. Os que possuem o ar como dielétrico são os mais caros, garantem menores perdas, mas são de difícil manuseio. Os de espuma causam uma perda maior de sinal, mas são mais baratos e fáceis de instalar. Um procedimento especial deve ser seguido quando os conectores são soldados, a fim de que o dielétrico de espuma mantenha-se seco e sem estragos. Quando cabos Heliax não estiverem disponíveis, use o melhor cabo LMR que puder encontrar. O LMR é um tipo de cabo coaxial disponível em vários diâmetros, que funciona bem em freqüências de microondas. LMR-400 e LMR-600 são as mais comuns alternativas ao Heliax.

6. Sempre que possível, use cabos que já tenham seus conectores e que foram testados em um laboratório apropriado. Instalar conectores em um cabo pode ser complicado, mesmo quando ferramentas apropriadas são utilizadas. A não ser que você tenha acesso a equipamento que pode verificar um cabo que você mesmo construiu (como um analisador de espectro e um gerador de sinal, ou um reflectômetro), a detecção de problemas em uma rede que usa cabos "feitos em casa" pode ser difícil.

7. Não abuse de sua linha de transmissão. Nunca pise em um cabo, dobre-o muito ou desconecte-o puxando diretamente pelo cabo. Todas estas ações podem mudar as características mecânicas do cabo, alterar sua impedância, colocar em curto o condutor e a blindagem ou mesmo provocar sua quebra. Estes problemas são difíceis de detectar e reconhecer e podem levar a comportamentos imprevistos do link de rádio.

Guias de onda

Acima de 2 GHz, o comprimento de onda é curto o suficiente para permitir a prática e eficiente transferência de energia com o uso de meios diferentes. Uma guia de onda é um tubo condutor através do qual a energia é transmitida na forma de ondas eletromagnéticas. O tubo serve como um limite de confinamento para as ondas, em um espaço fechado. A gaiola de Faraday previne que os efeitos eletromagnéticos apareçam fora da guia. Os campos eletromagnéticos são propagados através da guia de onda por meio de reflexão em suas paredes internas, que são consideradas condutores perfeitos. A intensidade dos campos é maior no centro, ao longo da dimensão X, e deve diminuir para zero nas

paredes laterais, em função de que a existência de qualquer campo, paralelo às paredes na superfície, poderia causar o fluxo de uma corrente infinita em um condutor perfeito. Guias de onda, claro, não podem transportar RF desta maneira.

As dimensões X, Y e Z de uma guia de onda retangular podem ser vistas na figura abaixo:

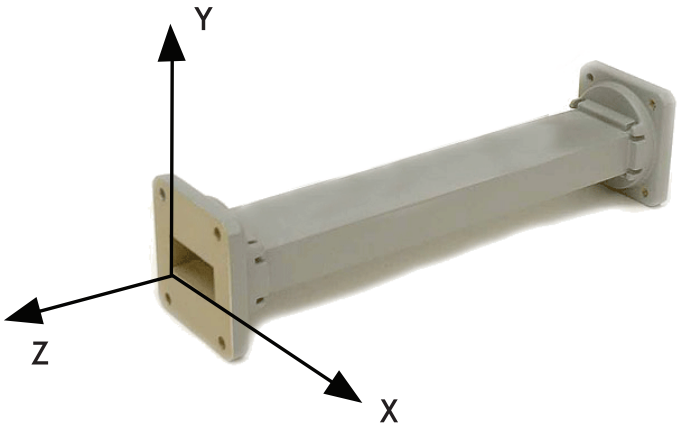


Figura 4.2: As dimensões X, Y e Z de uma guia de onda retangular.

Há um infinito número de formas nas quais os campos elétricos e magnéticos podem arranjar-se em uma freqüência acima da freqüência de corte baixa. Cada uma destas configurações de campo é chamada de modo. Os modos podem ser separados em dois grupos gerais. Um grupo, designado como ***TM*** (***Transverse Magnetic***–Magnético Transversal), tem o campo magnético inteiramente transverso à direção de propagação, mas tem o componente do campo elétrico na mesma direção da propagação. O outro tipo, designado ***TE*** (***Transverse Electric***–Elétrico Tansversal) tem o campo elétrico inteiramente transverso em direção a propagação, mas o componente magnético na mesma direção.

O modo de propagação é identificado pelo grupo de letras seguido por dois numerais subscritos. Por exemplo, TE 10, TM 11, etc. O número de modos possíveis aumenta com a freqüência para um dado tamanho de guia, e há sempre um único modo possível, chamado ***modo dominante***, para a menor freqüência que pode ser transmitida. Em uma guia retangular, a dimensão crítica é X. Esta dimensão deve ser maior que 0,5 λ na menor freqüência a ser transmitida. Na prática, a dimensão Y é feita igual a 0,5 X, para evitar a possibilidade de operação em modo diferente do dominante. Outros formatos seccionais podem ser usados, além do retângulo, sendo que o mais importante é o cano circular. Muitas das mesmas considerações do caso retangular são aplicáveis. As dimensões de comprimentos de onda para guias circulares e retangulares são dadas na tabela a seguir, onde X é a largura de uma guia retangular e r é o raio de uma guia circular. Todos os números aplicam-se ao modo dominante.

Tipo de Guia	Retangular	Circular
Comprimento de onda de corte	**2X**	**3,41r**
Maior comprimento de onda transmitido com pequena atenuação	**1,6X**	**3,2r**
Menor comprimento de onda antes que o próximo modo torne-se possível	**1,1X**	**2,8r**

Energia pode ser introduzida ou extraída de uma guia de onda através do uso do campo elétrico ou magnético. A transferência de energia tipicamente acontece através de uma linha coaxial. Duas formas possíveis de acoplar uma guia de onda a uma linha coaxial são através do uso do condutor central do cabo coaxial ou através de um *loop*. Um pedaço pequeno (*probe*) da extensão do condutor interno do coaxial pode ser orientado de forma a ficar paralelo às linhas de força elétrica. Um loop (algumas voltas do fio condutor) pode ser orientado de forma a envolver algumas linhas de força do campo magnético. O ponto no qual o máximo acoplamento é obtido depende do modo de propagação da guia ou cavidade. O acoplamento é máximo quando o dispositivo de acoplamento está no campo mais intenso.

Se uma guia de onda é deixada aberta em uma de suas extremidades, ela irradiará energia (isto é, pode ser usada com uma antena ao invés de uma linha de transmissão). Esta radiação pode ser melhorada ajustando a guia de onda para formar uma antena do tipo “corneta piramidal” (pyramidal horn). Veremos um exemplo de uma antena feita com guia de onda para Wi-Fi mais adiante neste capítulo.

Tipo de cabo	Núcleo	Dielétrico	Blindagem	Capa
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

Esta tabela apresenta os tamanhos dos vários tipos de linhas de transmissão. Escolha o melhor cabo que você pode adquirir, com a menor atenuação possível, na freqüência que você pretende usar em seu link wireless.

Conectores e adaptadores

Conectores permitem que um cabo seja conectado a outro cabo ou a um componente na cadeia de transmissão de RF. Há uma grande variedade de encaixes e conectores projetados para funcionar em conjunto com os vários tamanhos e tipos de linhas coaxiais. Vamos descrever alguns dos mais populares.

Conectores BNC foram desenvolvidos no final dos anos 40. As iniciais BNC vem de Bayonet Neill Concelman, nomes dos inventores deste conector: Paul Neill e Carl Concelman. A linha de produtos BNC é composta de um pequeno conector para a rápida conexão e desconexão. O conector apresenta duas travas do tipo "baioneta" no conector fêmea, e a conexão é feita com um quarto de volta no conector de acoplamento. Eles prestam-se, idealmente, para a terminação de cabos coaxiais do tipo miniatura e subminiatura (RG- 58 a RG-179, RG-316, etc.) Eles têm desempenho aceitável até alguns poucos GHz. São mais comumente encontrados em equipamentos de teste e em cabos coaxiais Ethernet 10base2.

Conectores TNC também foram inventados por Neill e Concelman, e são um aprimoramento do BNC. Devido à melhor interconexão rosqueada fornecida por esses conectores, eles trabalham bem até freqüências de 12 GHz. TNC é a abreviatura de *Threaded* (rosqueado) Neill Concelman.

Conectores Tipo N (novamente por Neil, ainda que algumas vezes são atribuídos a "*Navy*"—Marinha) foram originalmente desenvolvidos durante a Segunda Guerra Mundial. São utilizáveis até freqüências de 18 GHz e muito comumente usados para aplicações de microondas. Estão disponíveis para praticamente todos os tipos de cabos. Todas as juntas (conector e cabo, conector e soquete) são à prova d'água, garantindo uma efetiva junção no cabo.

SMA é o acrônimo para *Sub-Miniature* (subminiatura) versão A, e foi desenvolvido nos anos 60. Os conectores SMA são unidades de precisão, subminiaturizadas, que fornecem excelente desempenho elétrico até uma freqüência de 18 GHz. Estes conectores de alta performance são compactos no tamanho e têm uma excelente durabilidade mecânica.

O nome ***SMB*** deriva de *Sub-Miniature* B e é o segundo projeto de conector subminiaturizado, menor ainda que o SMA e com um acoplamento de encaixe (*snap-on*). A capacidade de banda vai até 4 GHz.

Conectores ***MCX*** foram introduzidos nos anos 80. Enquanto o MCX usa dimensões de contato interno e isolamento idênticos ao SMB, o diâmetro externo do plug é 30% menor que o seu antecessor. Esta série de conectores fornecem opções aos projetistas nos casos onde o peso e o espaço são limitados. A capacidade de banda atinge 6 GHz com um acoplamento de encaixe (*snap-on*).

Além destes conectores padrão, a maioria dos dispositivos Wi-Fi usam uma variedade de conectores proprietários. Freqüentemente, eles são conectores padrão para microondas com as partes centrais invertidas, ou a rosca na direção contrária. Estas partes são, com freqüência, integradas a um sistema de microondas com o uso de um conector curto (*jumper*), chamado de ***pigtail*** (rabo de porco) que converte o conector proprietário em algo mais robusto e comumente disponível. Alguns destes conectores incluem:

RP-TNC. É um conector TNC com os gêneros invertidos. São mais comumente encontrados em equipamentos Linksys, como o WRT54G.

U.FL (também conhecido como ***MHF***). O conector U.FL é patenteado pela Hirose, sendo que o MHF é um conector mecanicamente equivalente. É talvez o menor conector para microondas em uso de forma ampla, atualmente. Ele é bastante utilizado para conectar um cartão de rádio mini-PCI a uma antena ou a um conector maior (como um N ou TNC).

A série de conectores ***MMCX***, também chamada de MicroMate, é composta dos menores conectores de RF, desenvolvida nos anos 90. MMCX é um conector micro-miniaturizado, com um mecanismo de encaixe e trava que permite uma rotação de 360 graus, permitindo flexibilidade. Estes conectores são comumente usados em cartões de rádio PCMCIA, como os fabricados pela Senao e a Cisco.

Conectores ***MC-Card*** são ainda menores e mais frágeis que os MMCX. Eles possuem uma parte externa dividida que quebra-se facilmente após algumas poucas interconexões, e são comumente encontrados em equipamentos Lucent/Orinoco/Avaya.

Adaptadores coaxiais são conectores pequenos, de dois lados, usados para a união de dois cabos ou componentes que não podem ser conectados diretamente. Por exemplo, um adaptador pode ser usado para unir um conector SMA a um BNC. Eles também podem ser usados para a adequação de conectores do mesmo tipo, que não podem ser conectados por serem do mesmo gênero (adaptadores do tipo macho-macho, ou fêmea-fêmea).

Um adaptador muito útil é aquele que permite a conexão de dois conectores tipo N, através de soquetes fêmea em ambos os seus lados.

Figura 4.3: Um adaptador fêmea do tipo N.

Escolhendo o conector apropriado

1. "A questão do gênero." Virtualmente todos os conectores têm um gênero bem definido, consistindo de um pino (o lado "macho") ou um soquete (o lado "fêmea"). Usualmente, os cabos possuem conectores macho em ambos os lados, enquanto equipamentos de RF (transmissores e antenas) possuem conectores fêmea. Dispositivos como acopladores direcionais e dispositivos de monitoramento de linha possuem os dois tipos de conectores. Certifique-se de que todo conector macho em seu sistema está associado a um conector fêmea.

2. “Menos é mais!” Tente minimizar o número de conectores e adaptadores da cadeia de RF. Cada conector introduz alguma perda adicional (até alguns dBs para cada conexão, dependendo do conector).
3. “Compre, não construa!” Como mencionamos anteriormente, compre cabos que já possuem conectores em suas terminações sempre que possível. A solda de conectores não é uma tarefa fácil e realizar esta tarefa é quase impossível em pequenos conectores como U.FL e MMCX. Mesmo a montagem de conectores em cabos de “espuma” não é fácil.
4. Não use BNC para freqüências de 2,4 GHz ou maiores. Use conectores tipo N (ou SMA, SMB, TNC, etc.)
5. Conectores para microondas são componentes de precisão, podendo ser facilmente danificados por maus tratos. Como regra geral, você deve apenas girar a camada mais externa para fixar o conector, deixando fixo todo o restante do conector (e do cabo). Caso outras partes sejam giradas enquanto estiver prendendo ou soltando o conector, danos podem ser causados facilmente.
6. Nunca pise em conectores ou os derrube ao chão quando estiver desconectando cabos (isto acontece com mais freqüência do que você imagina, especialmente quando se trabalha em um suporte para antena em um telhado).
7. Nunca use ferramentas como alicates para apertar conectores. Sempre use suas mãos. Quando trabalhar externamente, lembre-se que metais expandem em temperaturas altas e contraem-se em baixas temperaturas: um conector muito apertado no verão pode entortar ou mesmo quebrar no inverno.

Antenas e padrões de radiação

Antenas são um componente muito importante em sistemas de comunicação. Por definição, uma antena é um dispositivo usado para transformar um sinal de RF atravessando um condutor em uma onda eletromagnética que viajará no espaço aberto. As antenas demonstram uma propriedade conhecida como ***reciprocidade***, o que significa que uma antena manterá as mesmas características, quer estejam transmitindo ou recebendo um sinal. A maioria das antenas são dispositivos ressonantes, que operam eficientemente dentro de uma banda de freqüência relativamente estreita. Uma antena deve ser sintonizada para a mesma banda de freqüência da estação de rádio à qual está conectada. Caso contrário, tanto a transmissão quanto a recepção serão prejudicadas. Quando um sinal é enviado para a antena, ela emitirá radiação que será distribuída no espaço de uma certa maneira. Uma representação gráfica da distribuição relativa da potência irradiada no espaço é chamada de ***padrão de radiação***.

Glossário de termos de antenas

Antes de falarmos sobre antenas específicas, aqui estão alguns termos comuns que devem ser definidos e explicados:

Impedância de entrada

Para uma transferência eficiente de energia, as impedâncias do rádio, da antena e do cabo de transmissão devem ser idênticas. Transceptores e suas linhas de transmissão são tipicamente projetadas para impedâncias de 50Ω. Se a antena tiver uma impedância diferente de 50Ω, haverá um descasamento, e um circuito de casamento de impedâncias será necessário. Quando houver o descasamento de impedância entre quaisquer componentes, a eficiência da transmissão será prejudicada.

Relação de onda estacionária

A relação de onda estacionária (***ROE***), ou em inglês, ***Standing Wave Ratio*** (***SWR***), é a que existe entre a potência enviada para uma linha de transmissão e a potência refletida, de volta, ao transmissor. A ROE é expressa como uma razão, tipo 1,5:1 (um e meio para 1). Uma ROE de 2:1 ou mais indica, usualmente, um descasamento de impedância.

Perda pelo retorno

A ***perda pelo retorno*** (***return loss***) é outra maneira de expressar um descasamento. É uma taxa logarítmica, medida em dB que compara a potência refletida pela antena à potência que é entregue à antena pela linha de transmissão. A relação entre SWR e a perda de retorno é a seguinte:

$$\text{Perda pelo retorno o (em dB)} = 20\log_{10} \frac{SWR}{SWR-1}$$

Enquanto alguma energia sempre será refletida de volta ao sistema, uma alta perda pelo retorno poderá levar a um desempenho inaceitável da antena.

Largura de banda

A ***largura de banda*** de uma antena refere-se ao intervalo de freqüências no qual a antena pode operar corretamente. A largura de banda de uma antena é o número de Hz para os quais a antena irá exibir um SWR menor que 2:1.

A largura de banda também pode ser descrita em termos percentuais a partir da freqüência central da banda.

$$\text{Largura de banda} = 100 \times \frac{F_H - F_L}{F_C}$$

onde F_H é a mais alta freqüência da banda, F_L é a mais baixa e F_C é a freqüência central.

Desta forma, a largura de banda é constante em relação à freqüência. Se a largura de banda fosse expressa em unidades absolutas de freqüência, ela seria

diferente dependendo da freqüência central. Diferentes tipos de antenas têm limitações diferentes de largura de banda.

Diretividade e ganho

Diretividade é a habilidade de uma antena de focar energia em uma direção em particular durante a transmissão, ou de receber energia de uma direção particular durante a recepção. Se um link wireless utiliza localizações fixas em ambos os lados da conexão, é possível usar a diretividade da antena para concentrar o feixe de radiação na direção pretendida. Em uma aplicação móvel, onde o transceptor não é fixo, pode ser impossível de se prever onde ele estará e, assim, a antena deve, idealmente, irradiar o melhor possível em todas as direções. Neste caso, uma antena omnidirecional é utilizada.

Ganho não é uma quantidade que possa ser definida nos termos de uma quantidade física, como Watts ou Ohms, mas uma relação sem dimensões. O ganho é dado em referência a uma antena padrão. As duas antenas de referência mais comuns são a ***antena isotrópica*** e a ***antena dipolo ressonante de meia-onda*** (*resonant half-wave dipole antenna*). A antena isotrópica irradia igualmente bem em todas as direções. Antenas isotrópicas reais não existem, mas elas fornecem padrões teóricos simples e úteis com os quais as antenas reais podem ser comparadas. Qualquer antena real irá irradiar mais energia em algumas direções do que em outras. Uma vez que antenas não criam energia, a energia total irradiada é a mesma de uma antena isotrópica. Qualquer energia adicional irradiada em uma direção favorecida é conseqüência da perda de energia irradiada em outras direções.

O ganho de antena em uma dada direção é a quantidade de energia irradiada naquela direção, comparada com a energia que uma antena isotrópica iria irradiar na mesma direção quando alimentada com a mesma potência. Usualmente, estamos apenas interessados no ganho máximo, que é o ganho na direção para a qual a antena está irradiando a maior parte da potência. Um ganho de antena de 3 dB, comparado a uma antena isotrópica, é representado por **3 dBi**. O dipolo de meia-onda pode ser um padrão útil na comparação com antenas em uma única freqüência ou em uma faixa estreita de freqüências. Comparar o dipolo com uma antena em um conjunto de freqüências requer um número de dipolos de tamanhos diversos. Um ganho de antena de 3 dB, comparado a uma antena dipolo, é representado por **3 dBd**.

O método de medida de ganho através da comparação da antena testada contra uma antena padrão conhecida, que tem um ganho calibrado, é conhecida como técnica de ***transferência de ganho*** (***gain transfer***). Outro método para a medida de ganho é o método das três antenas, onde a potência de transmissão e recepção nos terminais da antena é medida entre três antenas arbitrárias, a distâncias fixas e conhecidas.

Padrões de radiação

O padrão de radiação, ou padrão de antena, descreve a força relativa do campo irradiado em várias direções da antena, em uma distância constante. O padrão de radiação é também o padrão de recepção, uma vez que serve também para descrever as propriedades de recepção da antena. O padrão de

radiação é tridimensional, mas usualmente os padrões de radiação medidos são uma fatia bidimensional deste padrão tridimensional, no plano horizontal ou vertical. As medidas são apresentadas em um formato ***retangular*** ou ***polar***. As seguintes figuras mostram a representação retangular de uma antena Yagi típica, de dez elementos. O detalhamento é bom, mas é difícil visualizar o comportamento da antena em diferentes direções.

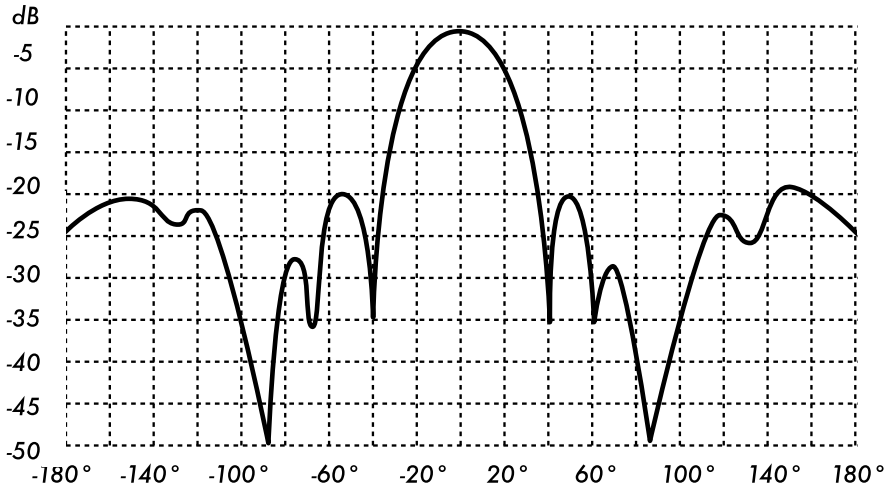


Figura 4.4: Representação retangular do padrão de radiação de uma antena Yagi.

Sistemas de coordenadas polares são usados quase universalmente. No gráfico de coordenadas polares, os pontos estão localizados pela projeção ao longo de um eixo rotacional (raio) para uma intersecção com um entre vários círculos concêntricos. O gráfico polar representando a mesma antena Yagi de dez elementos é mostrado a seguir.

Sistemas de coordenadas polares podem ser divididos, geralmente, em duas classes: linear e logarítmico. No sistema de coordenadas linear, os círculos concêntricos estão espaçados igualmente e são graduados. Tal grade pode ser usada para preparar o gráfico linear da potência contida no sinal. Para facilidade de comparação, os círculos concêntricos igualmente espaçados podem ser substituídos por círculos, apropriadamente localizados, representando a resposta em decibéis, referenciando 0 dB na beirada externa do gráfico. Neste tipo de gráfico, os lóbulos menores são suprimidos. Lóbulos com picos maiores que 15 dB abaixo do lóbulo principal desaparecem em função de seu tamanho pequeno. Esta grade destaca os resultados nos quais a antena tem uma alta diretividade e pequenos lóbulos menores. A voltagem do sinal, ao invés da potência, também pode ser grafada em um sistema de coordenadas lineares. Neste caso, também, a diretividade é destacada e os lóbulos menores suprimidos, mas não no mesmo grau que na grade linear de potência.

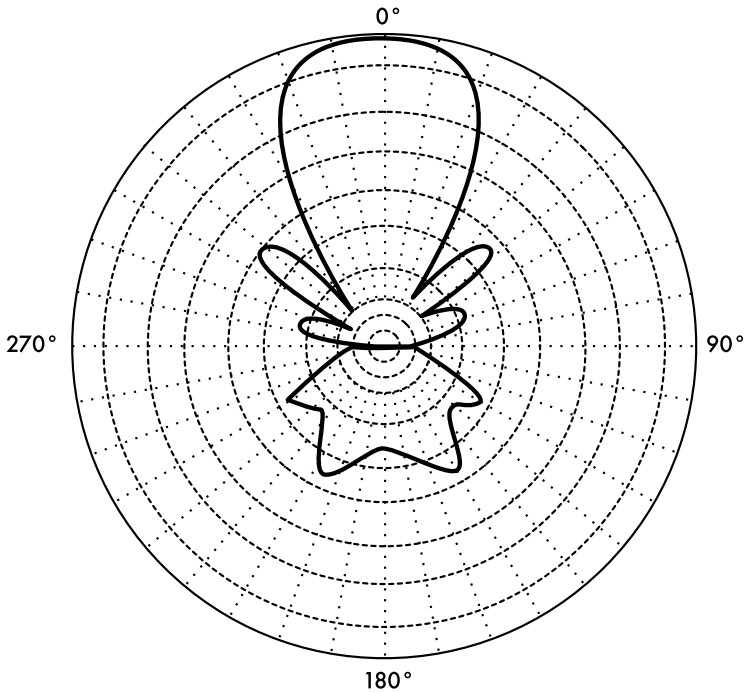


Figura 4.5: Uma representação polar linear da mesma Yagi.

No sistema logarítmico de coordenadas polares, as linhas concêntricas da grade estão espaçadas periodicamente, de acordo com o logaritmo da voltagem no sinal. Valores diferentes podem ser usados para a constante de periodicidade do logaritmo e esta escolha terá um efeito na aparência dos padrões plotados no gráfico. Geralmente, a referência de 0 dB para o limite externo do gráfico é usada. Com este tipo de grade, lóbulos que estão 30 ou 40 dB abaixo do lóbulo principal ainda podem der distingüidos. O espaçamento entre os pontos em 0 dB e -3 dB é maior que o espaçamento entre -20 dB e -23 dB, que é maior que o espaçamento entre -50 dB e -53 dB. O espaçamento, desta forma, corresponde ao significado relativo de tais mudanças no desempenho da antena.

Uma escala logarítmica modificada enfatiza a forma do feixe principal, enquanto comprime os lóbulos laterais de nível muito baixo (>30 dB) em direção ao centro do padrão. Isto é mostrado na **Figura 4.6**.

Há dois tipos de padrão de radiação: ***absoluto*** e ***relativo***. Padrões absolutos de radiação são apresentados em unidades absolutas de força do campo ou potência. Padrões relativos de radiação são referenciados em unidades relativas de força do campo ou potência. A maioria das medidas de padrões de radiação são relativas à antena isotrópica, e o método de transferência de ganho é usado para estabelecer o ganho absoluto da antena.

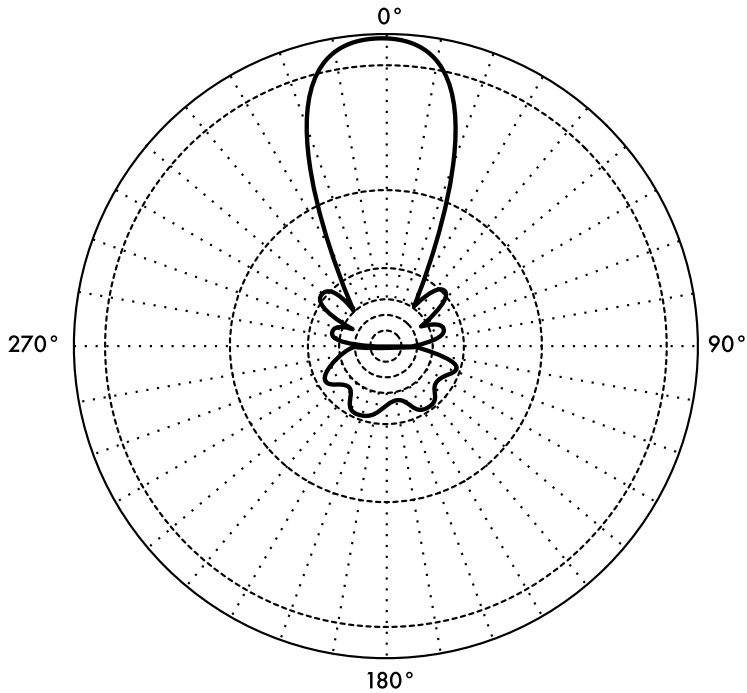


Figura 4.6: O gráfico polar logarítmico.

O padrão de radiação na região próxima à antena não é o mesmo padrão para distâncias longas. O termo "campo próximo" (*near-field*) refere-se ao padrão de campo que existe nas proximidades da antena, enquanto o termo "campo distante" (*far-field*) refere-se ao padrão em grandes distâncias. O campo distante também é chamado de campo de radiação, e é o que mais será de interesse comum. O que, ordinariamente, irá interessar é justamente a potência irradiada, assim, os padrões de antena são tipicamente medidos na região do campo distante. Para a medida do padrão, é importante a escolha de distâncias suficientemente grandes, de forma que estejam efetivamente no campo distante e não no campo próximo. A mínima distância permissível depende das dimensões da antena em relação ao comprimento de onda. A fórmula aceita para a distância é a seguinte:

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

onde r_{min} é a distância mínima da antena, d é a maior dimensão da antena e λ é o comprimento de onda.

Largura do feixe

A ***largura do feixe*** (*beamwidth*) de uma antena é usualmente entendida como a largura do feixe em meia potência. A intensidade de pico da radiação é encontrada, e então os pontos de cada lado do pico que representam a metade

da intensidade do mesmo são localizados. A distância angular entre os pontos com metade da potência é definida como a largura do feixe. A metade da potência expressa em decibéis é -3 dB. Então, a largura de feixe em meia potência é algumas vezes chamada de largura de feixe de 3 dB. Tanto a largura de feixe horizontal como vertical são, usualmente, consideradas.

Assumindo que a maior parte da potência irradiada não será dividida em lóbulos laterais, então o ganho direcional é inversamente proporcional à largura do feixe: quanto menor a largura do feixe, maior o ganho direcional.

Lóbulos laterais

Nenhuma antena é capaz de irradiar toda a energia em uma única direção preferida. Alguma energia é, inevitavelmente, irradiada em outras direções. Estes picos menores são chamados de ***lóbulos laterais*** (*sidelobes*), comumente especificados em dB abaixo do lóbulo principal.

Nulos

Em um padrão de radiação de antena, um ***nulo*** (*null*) é uma zona onde a radiação efetiva está em um mínimo. Um nulo freqüentemente tem um ângulo de direção estreito, comparado com o do feixe principal. Assim, o nulo é útil para vários propósitos, como a eliminação de interferências em uma determinada direção.

Polarização

A ***polarização*** é definida como a orientação do campo elétrico de uma onda eletromagnética. A polarização é tipicamente descrita por uma elipse. Dois casos especiais de polarização elíptica são a ***polarização linear*** e a ***polarização circular***. A polarização inicial de uma onda de rádio é determinada pela antena.

Com a polarização linear o vetor do campo elétrico fica no mesmo plano o tempo inteiro. O campo elétrico pode deixar a antena em uma orientação vertical, horizontal, ou em algum ângulo entre estas duas. A radiação da ***polarização vertical*** é, de alguma forma, menos afetada por reflexões no caminho da transmissão. Antenas omnidirecionais sempre têm polarização vertical. Com a ***polarização horizontal*** tais reflexões causam variação na força do sinal recebido. Antenas horizontais tendem a captar menos interferências produzidas pelos humanos, uma vez que estas normalmente têm polarização vertical.

Na polarização circular o vetor do campo elétrico aparenta estar em movimento circular na direção da propagação, fazendo um giro completo para cada ciclo de RF. A rotação pode ser no sentido horário ou anti-horário. A escolha da polarização é uma das escolhas disponíveis para o projetista de sistemas de RF.

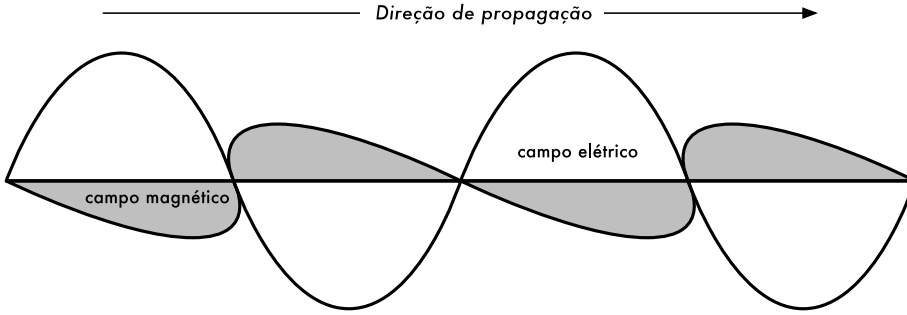


Figura 4.7: A onda elétrica é perpendicular à onda magnética e ambas são perpendiculares à direção de propagação.

Descasamento de polarização

A fim de transferir a potência máxima entre as antenas de transmissão e recepção, ambas devem ter a mesma orientação espacial, a mesma polarização e a mesma proporção axial.

Quando as antenas não estão alinhadas ou não têm a mesma polarização, haverá redução de potência na transferência entre as duas antenas. Esta redução irá reduzir o desempenho e a eficiência do sistema.

Quando as antenas de transmissão e recepção estão, ambas, linearmente polarizadas, o desalinhamento da antena irá resultar em uma perda por descasamento de polarização, que pode ser determinada usando a seguinte fórmula:

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

Onde Θ é a diferença no ângulo de alinhamento entre as duas antenas. Para 15°, a perda é de aproximadamente 0,3 dB, para 30° perdemos 1,25 dB, para 45°, 3 dB e para 90° temos uma perda infinita.

Em resumo, quanto maior for o descasamento da polarização entre a antena transmissora e a receptora, maior será a perda percebida. No mundo real, 90° de diferença na polarização entre as antenas ocasiona uma perda muito grande, mas não infinita. Algumas antenas, como as Yagis ou antenas de latas (*can antennas*) podem ser rotacionadas até 90° para equalizar com a polarização do outro lado do link. Você pode usar o efeito da polarização para sua vantagem em um link ponto-a-ponto. Use uma ferramenta de monitoração para observar a interferência de redes adjacentes e rotacione uma antena até conseguir o menor nível de sinal na recepção. Em seguida, ligue o outro lado de seu link e o oriente para casar a polarização com o primeiro. Esta técnica pode ser usada, às vezes, para criar links estáveis, mesmo em ambientes com muito ruído.

Relação frente-costas (front-to-back ratio)

Freqüentemente é útil comparar a ***relação frente-costas*** (*front-to-back ratio*) de antenas direcionais. Esta é a relação entre a máxima diretividade de uma antena e a sua diretividade na direção oposta. Por exemplo, quando o padrão de radiação é plotado em uma escala dB relativa, a relação frente-costas

é a diferença em dB entre o nível máximo de radiação à frente e o nível de radiação a 180 graus.

Este número não significa nada para uma antena omnidirecional, mas dá uma idéia da quantidade de potência direcionada à frente em uma antena bastante direcional.

Tipos de antenas

Uma classificação de antenas pode ser baseada em:

- **Freqüência e tamanho**. Antenas usadas para HF são diferentes de antenas usadas para VHF que, por sua vez, são diferentes das antenas usadas para microondas. O comprimento de onda é diferente para diferentes freqüências e, desta forma, as antenas devem ter tamanhos diferentes para irradiar o sinal no comprimento de onda correto. Estamos particularmente interessados em antenas que trabalham na faixa de microondas, especialmente nas freqüências de 2,4 GHz e 5 GHz. Em 2,4 GHz o comprimento de onda é de 12,5 cm, enquanto em 5 GHz é de 6 cm.

- **Diretividade**. Antenas podem ser omnidirecionais, setoriais ou diretivas. ***Antenas omnidirecionais*** irradiam praticamente a mesma energia ao redor de toda a antena, em um padrão completo de 360°. Os tipos mais populares de antenas omnidirecionais são as ***dipolo*** e ***plano-terra***. Antenas setoriais irradiam primariamente em uma área específica. O feixe pode ser largo como 180°, ou estreito como 60°. ***Antenas direcionais*** ou ***diretivas*** são aquelas onde o feixe é muito mais estreito que o possível em antenas setoriais. Elas têm o maior ganho e, por isso, são usadas em links de longa distância. Tipos de antenas direcionais são a Yagi, a *biquad*, a *horn* (corneta), a helicoidal, a *patch*, a parabólica e muitas outras.

- **Construção física**. Antenas podem ser construídas de muitas formas diferentes, desde simples fios a pratos parabólicos, passando por latas de óleo ou café.

Considerando antenas apropriadas para redes sem fio em 2,4 GHz, uma classificação adicional é usada:

- **Aplicação**. Pontos de acesso tendem a ser usados em redes ponto-a-multiponto, enquanto links remotos são ponto-a-ponto. Cada um destes usos sugere diferentes tipos de antena. Nós usados em acessos multiponto irão, provavelmente, usar antenas omnidirecionais que irradiam igualmente em todas as direções, ou antenas setoriais que focam-se em uma pequena área. No caso ponto-a-ponto, as antenas são usadas para unir duas localidades únicas, assim, antenas direcionais serão a escolha primária neste caso.

Uma pequena lista com as antenas mais comuns para a freqüência de 2,4 GHz é apresentada agora, com uma breve descrição e informações básicas sobre suas características.

Plano-terra de ¼ de comprimento de onda

A antena plano-terra de ¼ de comprimento de onda é de construção muito simples e é útil nos casos onde tamanho, preço e facilidade de montagem são importantes. Esta antena é projetada para transmitir um sinal polarizado verticalmente. Ela consiste em ¼ de elemento de onda como um meio dipolo e três ou quatro ¼ de comprimento de onda de elementos de terra, dobrados 30 a 45 graus para baixo. Este conjunto de elementos, chamados radiais, é conhecido como plano-terra.

Esta é uma antena simples e efetiva que pode captar sinais igualmente de todas as direções. Para aumentar o seu ganho, o sinal pode ser "achatado", reduzindo o foco nas direções acima e abaixo e aumentando o foco horizontal. A largura do feixe vertical representa o grau de achatamento do foco. Isto é útil na situação ponto-a-multiponto, caso todas as antenas estejam na mesma altura. O ganho desta antena é da ordem de 2 a 4 dBi.

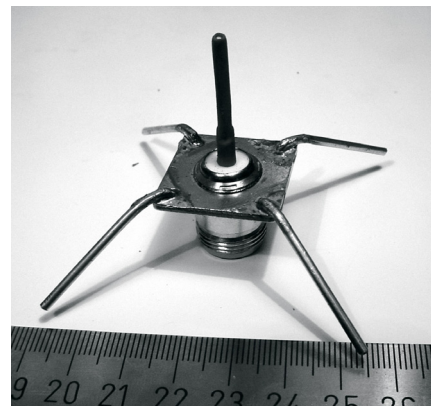


Figura 4.8: Antena plano-terra de ¼ de comprimento de onda.

Antena Yagi

Uma Yagi básica consiste de um certo número de elementos retos, cada um medindo aproximadamente meio comprimento de onda. O elemento motor, ou ativo, de uma Yagi é o equivalente de uma antena dipolo de meia onda, com alimentação central. Em paralelo ao elemento ativo e aproximadamente 0,2 a 0,5 comprimento de onda em cada um de seus lados, localizam-se fios ou arames chamados refletores e diretores, os elementos passivos. Um refletor é colocado atrás do elemento ativo e é ligeiramente maior que meio comprimento de onda; um diretor é colocado à frente do elemento ativo e é ligeiramente menor que meio comprimento de onda. Uma Yagi típica tem um refletor e um ou mais diretores. A antena propaga a energia do campo eletromagnético na direção do elemento ativo para os diretores, e é bastante sensitiva à energia de campos eletromagnéticos vindos da mesma direção. Quanto mais diretores tiver uma Yagi, maior o ganho, e também maior o tamanho da antena. A seguir, a foto de uma antena Yagi com seis diretores e um refletor..

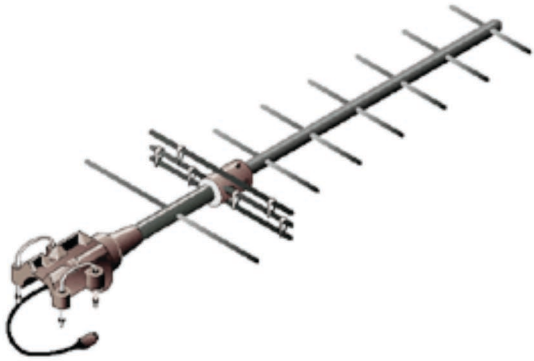


Figura 4.9: Uma antena Yagi

Antenas Yagi são usadas primariamente para links ponto-a-ponto, tendo um ganho de 10 a 20 dBi e uma largura de feixe horizontal entre 10 e 20 graus.

Corneta

A antena corneta (*horn*) tem seu nome em função de sua clássica aparência. A porção de recepção (corneta) da antena pode ser quadrada, retangular, cilíndrica ou cônica. A direção da radiação máxima corresponde ao eixo da corneta. Ela é facilmente alimentada com uma guia de onda, mas pode ser também alimentada através de um cabo coaxial e um elemento de transição apropriado.

Antenas corneta são comumente usadas como o elemento ativo de uma antena parabólica. A corneta é apontada para o centro do prato refletor. O uso de uma corneta, ao invés de um dipolo ou qualquer outro tipo de antena como ponto focal do prato, minimiza a perda de energia ao redor das bordas do prato refletor. Em 2,4 GHz, uma simples antena corneta feita com uma lata tem um ganho da ordem de 10 a 15 dBi.

Prato parabólico

Antenas baseadas em refletores parabólicos são o tipo mais comum de antenas direcionais quando há a necessidade de um alto ganho. A principal vantagem é que elas podem ser feitas para ter ganho e diretividade tão grandes quanto necessários. A principal desvantagem é que pratos grandes são difíceis de montar e provavelmente terão um grande bloqueio ao vento (o que pode implicar em dificuldades de manter a montagem firme em situações de muito vento).

Pratos de até um metro são, normalmente, feitos de material sólido. O alumínio é freqüentemente usado em função de seu pouco peso, sua durabilidade e boas características elétricas. A resistência ao vento (*windage*) aumenta rapidamente com o tamanho do disco e logo torna-se um problema sério. Discos que têm uma superfície reflexiva usando uma grade aberta são bastante usados. Estes têm uma relação frente-costas mais pobre, mas são mais seguros para usar e mais fáceis de construir. Cobre, alumínio, aço galvanizado e ferro são materiais apropriados para a construção da grade.

Figura 4.10: Corneta de alimentação feita com uma lata de comida.

Figura 4.11: Um prato parabólico sólido.

BiQuad

A antena BiQuad é fácil de construir e oferece boa diretividade e ganho para comunicações ponto-a-ponto. Ela consiste de dois quadrados idênticos, medindo ¼ do comprimento de onda como elementos de irradiação e de um prato ou grade metálica como refletor. Esta antena tem uma largura de feixe da ordem de 70 graus e um ganho entre 10 a 12 dBi. Ela pode ser usada como uma antena isolada ou como alimentadora de um prato parabólico. A polarização é vertical, no caso de você olhar para a antena de frente, com os quadrados colocados lado a lado.

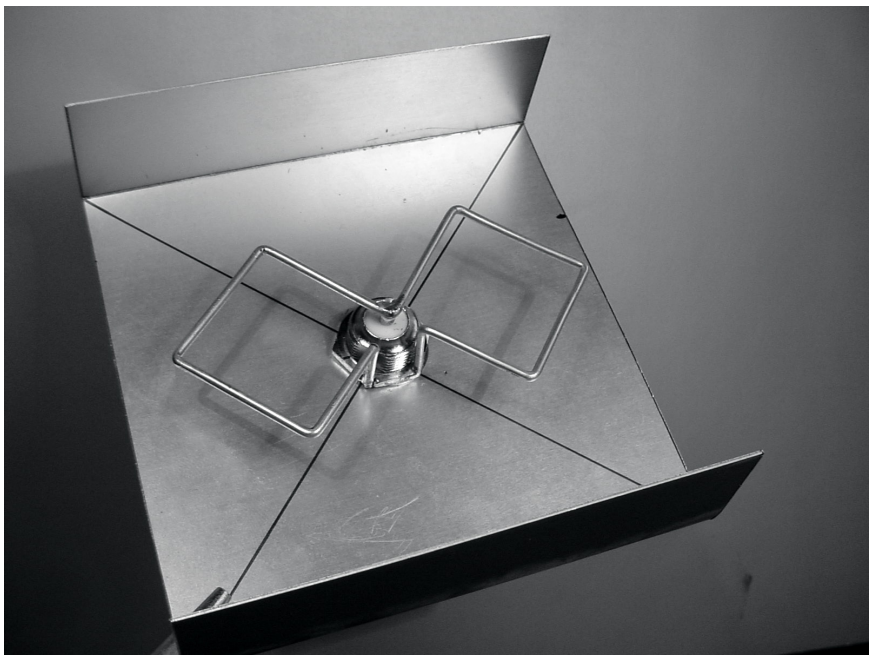


Figura 4.12: Antena BiQuad.

Outras antenas

Existem muitos outros tipos de antena e novas são criadas seguindo os avanços da tecnologia.

- Antenas setoriais: amplamente utilizadas na infra-estrutura de redes de telefonia celular, são normalmente construídas com a adição de um prato refletivo para um ou mais dipolos em fase. Sua largura de feixe horizontal pode ser tão larga quanto 180 graus ou tão estreita quanto 60 graus, enquanto a horizontal é, usualmente, muito mais estreita. Antenas compostas podem ser feitas com muitos setores para cobrir uma área horizontal mais ampla (antenas multisetoriais).
- Antenas de Painel ou “Patch”: são painéis planos sólidos, usados para cobertura interna de rede, com ganho de até 20 dB.

Teoria de refletores

A propriedade básica de um perfeito refletor parabólico é que ele converte uma onda esférica, irradiando de uma fonte colocada em seu foco, em uma onda plana. De forma recíproca, toda a energia de uma fonte distante, recebida pelo prato, é refletida para um ponto único em seu foco. A posição do foco, ou distância focal, é dada pela fórmula:

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

onde D é o diâmetro do prato e c é a profundidade da parábola, em seu centro.

O tamanho do prato é o fator mais importante, uma vez que ele determina o máximo ganho que pode ser conseguido para uma dada freqüência, assim como a largura do feixe resultante. O ganho e a largura de banda são dados por:

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

$$\text{Largura do Feixe} = \frac{70\ \lambda}{D}$$

onde D é o diâmetro do prato e n sua eficiência. A eficiência é determinada primariamente pela efetividade da iluminação do prato por sua alimentação, mas também por outros fatores. A cada vez que o diâmetro do prato duplica, seu ganho é quatro vezes, ou 6 dB, maior. Caso ambas as estações dupliquem o tamanho de seus pratos, a intensidade do sinal pode ser aumentada em 12 dB, um ganho bastante substancial. Uma eficiência de 50% pode ser assumida quando a mesma é construída manualmente.

A razão f / D (distância focal / diâmetro do prato) é o fator dominante para o projeto da alimentação para o prato. Esta razão é diretamente relacionada com a largura do feixe de alimentação necessário para iluminar efetivamente o disco. Dois discos do mesmo diâmetro, mas com distâncias focais diferentes, requerem um projeto diferente da alimentação para que ambos sejam eficientemente iluminados. O valor de 0,25 corresponde ao plano-foco comum, no qual o foco está no mesmo plano que a borda do disco.

Amplificadores

Como mencionamos anteriormente, antenas não criam energia. Elas simplesmente direcionam toda a energia disponível dentro de um padrão particular. Usando um ***amplificador de potência***, você pode usar uma fonte de corrente contínua para aumentar o sinal disponível. Um amplificador conecta-se entre um transmissor de rádio e a antena, e um cabo adicional o conecta a uma fonte de energia. Existem amplificadores que trabalham na faixa de 2,4 GHz e

podem adicionar vários Watts de potência em sua transmissão. Estes dispositivos detectam quando um rádio está transmitindo, ligando-se rapidamente e amplificando o sinal. Depois, desligam-se novamente ao final da transmissão. Na recepção, o mesmo acontece quando recebem o sinal da antena e o amplificam antes de enviá-lo ao rádio.

Infelizmente, adicionar amplificadores não irá, magicamente, resolver todos os seus problemas de rede. Não discutimos profundamente amplificadores neste livro porque há um número significativo de pontos negativos em seu uso:

- **Eles são caros**. Os amplificadores devem trabalhar com larguras de banda relativamente amplas em 2,4 GHz e devem ser capazes de comutar rápido o suficiente para trabalhar com aplicações Wi-Fi. Amplificadores assim existem, mas tendem a custar várias centenas de dólares por unidade.
- **Você precisará no mínimo de dois**. Enquanto antenas podem proporcionar um ganho recíproco, que beneficia ambos os lados de uma conexão, amplificadores funcionam melhor ao amplificar um sinal transmitido. Se você colocar um amplificador apenas do lado da conexão com ganho insuficiente de antena, ele provavelmente poderá ser ouvido, mas não poderá ouvir o outro lado da conexão.
- **Eles não fornecem direcionamento adicional**. A adição de ganho de antena beneficia tanto o ganho quanto o direcionamento do sinal em ambos os lados do link. Isto não aumenta apenas a quantidade de sinal, mas também a rejeição de ruído vindo de outras direções. Os amplificadores aumentam cegamente a intensidade dos sinais desejados e dos ruídos, podendo até piorar problemas de interferência.
- **Amplificadores geram ruído para outros usuários da banda**. Ao aumentar sua potência de transmissão, você cria uma fonte maior de ruído para outros usuários da banda livre. Isto pode não ser um problema muito grande hoje nas áreas rurais, mas pode causar grandes problemas em áreas populadas. Ao contrário, a adição de ganho de antena irá melhorar seu link e pode, de fato, reduzir o nível de ruído para seus vizinhos.
- **Usar amplificadores pode ser ilegal**. Cada país impõe limites de potência para o uso do espectro livre. A adição de uma antena para um sinal altamente amplificado pode fazer com que o link exceda os limites legais.

O uso de amplificadores é freqüentemente comparado com aquele vizinho sem consideração pelos demais, que quer ouvir seu rádio do lado de fora de sua residência e, para isto, coloca o volume no máximo. Eles podem até “melhorar” sua recepção apontando seus alto-falantes para o lado de fora de suas janelas. Enquanto ele pode, agora, ouvir seu rádio, toda a vizinhança é obrigada a fazer o mesmo. O que aconteceria se todos os vizinhos decidissem fazer o mesmo com os seus próprios rádios? Usar amplificadores em uma conexão sem fio pode causar problemas parecidos na banda de 2,4 GHz. Sua conexão pode até funcionar melhor no momento, mas você começará a perceber os problemas quando todos os outros usuários da banda decidirem fazer o mesmo.

Com o uso de antenas de maior ganho, ao invés de amplificadores, você evita todos esses problemas. Antenas custam bem mais barato que amplificadores e podem melhorar um link simplesmente com a troca da antena de uma das pontas. O uso de rádios de maior sensitividade e cabos de boa qualidade também ajuda significativamente em links de longa distância. Estas técnicas dificilmente causam problemas para outros usuários da banda e, assim, recomendamos seu uso antes da adição de amplificadores.

Projetos práticos de antenas

O custo de antenas de 2,4 GHz vem caindo drasticamente desde a introdução do padrão 802.11b. Projetos inovadores usam componentes mais simples e pouco material para atingir ganhos impressionantes com montagens mecânicas modestas. Infelizmente, a disponibilidade de boas antenas ainda é limitada em muitos lugares do mundo e sua importação pode ter um custo proibitivo. Enquanto o projeto de uma antena possa ser complexo e sujeito a erros, a construção de antenas a partir de componentes localmente disponíveis é bastante simples e pode ser muito divertido. Vamos apresentar quatro projetos práticos de antenas que podem ser feitas com muito pouco dinheiro.

USB dongle[3] como alimentador de um prato

Possivelmente, o projeto mais simples de antena é o uso de uma parábola para direcionar a saída de sinal de um dispositivo wireless USB (conhecido também como ***USB dongle***). Ao colocar o dipolo interno presente nos dispositivos USB no foco de um prato parabólico, você pode fornecer um ganho significativo, sem a necessidade de soldas ou mesmo de abrir o dispositivo. Muitos tipos de pratos parabólicos funcionarão, incluindo os usados para recepção de satélites, antenas de televisão ou mesmo utensílios metálicos de cozinha (como uma tigela ou peneira). Como um bônus, cabos USB baratos ou não utilizados podem ser usados para alimentar a antena, sem a necessidade de cabos coaxiais ou Heliax mais caros.

Para construir uma antena parabólica com um USB dongle, você precisará encontrar a orientação e localização do dipolo dentro do dongle. A maioria dos dispositivos orientam o dipolo para que esteja paralelo com a beirada estreita do dongle, mas outros podem montá-lo de forma perpendicular. Você pode abrir o dispositivo e verificar como o dipolo está montado ou simplesmente tentar posicionar o dongle em ambas as posições, vendo qual resulta em um maior ganho.

Para testar a antena, aponte-a para um ponto de acesso colocado a vários metros de distância e conecte o dongle ao laptop. Usando o driver cliente do laptop ou alguma ferramenta como o Netstubler (veja o Capítulo 6), observe a força do sinal recebido. Agora, lentamente mova o dongle em relação à parabólica, enquanto observa o medidor de sinal. Você perceberá um aumento significativo de ganho (20 dB ou mais) quando encontrar a posição apropriada

---

3. N. do. T. - Em português, já ouvi chamar este dispositivo USB wireless de pendurico, penduricalho, palito, entre outros nomes. Como "*dongle*" também é utilizado, optei por mantê-lo em inglês.

(que irá depender do formato da parábola e da construção do USB dongle). Tente várias posições enquanto observa a força do sinal, até encontrar a melhor localização.

Quando a melhor localização for encontrada, fixe o dongle em seu local. Você precisará tornar sua montagem à prova d'água caso a antena seja usada externamente. Use um composto de silicone ou uma peça de tubo de PVC para proteger os componentes eletrônicos das condições do tempo. Muitas idéias e projetos de parabólicas alimentadas por USB estão documentadas online em *http://www.usbwifi.orcon.net.nz/*

Colinear Omni

Esta antena é muito simples de construir, necessitando apenas de um pedaço de fio, um soquete N e uma placa metálica quadrada. Ela pode ser usada em ambientes externos ou internos para a cobertura de curtas distância em links ponto-para-multiponto. A placa tem um buraco perfurado no meio para acomodar um soquete de chassis tipo N, que será rosqueado neste local. O fio é soldado no pino central do soquete N e tem espiras que separam os elementos ativos em fase. Duas versões desta antena são possíveis: uma com os dois elementos em fase e duas espiras e outra com quatro elementos em fase e quatro espiras. Para a antena pequena, o ganho será de cerca de 5 dBi, enquanto para a antena mais longa (com quatro elementos) o ganho será de 7 a 9 dBi. Descreveremos apenas como construir a antena maior.

Lista de componentes e ferramentas necessárias

- Um conector tipo N, fêmea, de parafusar
- 50 cm de fio (arame) de cobre ou bronze, com 2 mm de diâmetro
- Placa metálica quadrada, de 10 x 10 cm ou maior

Figura 4.13: Placa metálica de alumínio de 10 cm x 10 cm e demais componentes.

Lista de ferramentas

- Régua
- Alicate
- Lima
- Ferro de solda
- Solda
- Furadeira com um conjunto de brocas para metal (incluindo uma broca de 1,5 cm de diâmetro)
- Um pedaço de cano ou uma broca de furadeira com 1 cm de diâmetro
- Torninho ou outro tipo de suporte
- Martelo
- Chave inglesa ou grifo

Construção

1. Estique e endireite o fio usando o torninho.

Figura 4.14: Endireite o fio, tornando-o o mais reto que conseguir.

2. Com um marcador, desenhe uma linha a 2,5 cm de uma das pontas do fio. Nesta linha, dobre o fio em um ângulo de 90 graus, com a ajuda do torninho e do martelo.

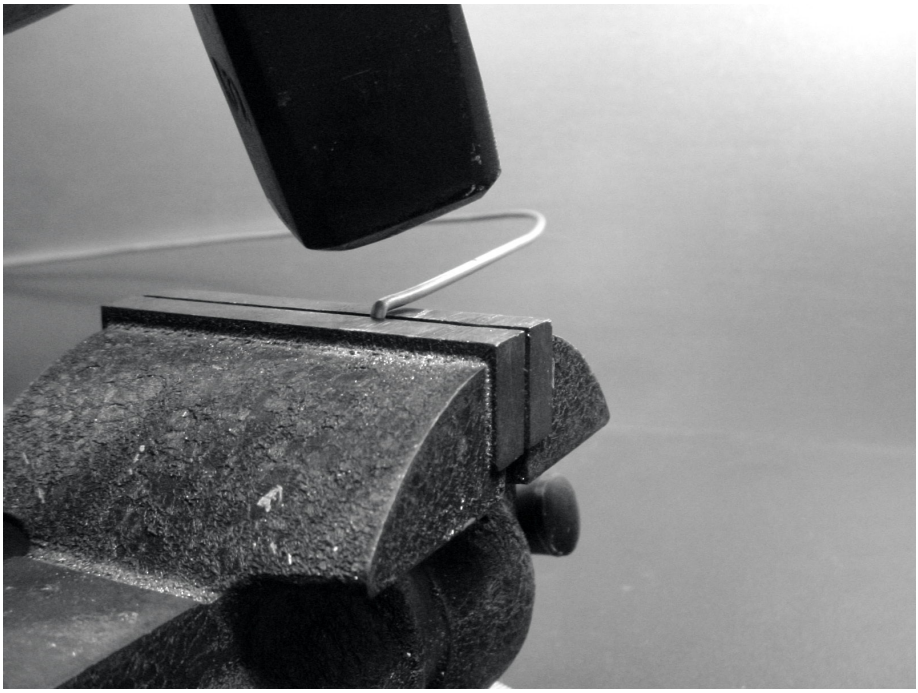


Figura 4.15: Com cuidado, martele o fio para fazer um ângulo reto.

3. Trace uma outra linha na distância de 3,6 cm da dobra. Usando o torninho e o martelo, dobre novamente o fio nesta segunda linha, a 90 graus, na direção oposta à primeira dobra, no mesmo plano. O fio deve ficar parecido com um 'Z'.

Figura 4.16: Dobre o fio na forma de um 'Z'.

4. Agora, iremos curvar a perna central do 'Z' no fio para fazer uma espira com o diâmetro de 1 cm. Para isto, usaremos como guia a broca ou o cano, curvando o fio ao seu redor, com a ajuda do torninho e do alicate.

Figura 4.17: Curve o fio ao redor da broca para fazer uma espira.

A espira deve parecer-se com a figura abaixo:

Figura 4.18: A espira completa.

5. Você deve fazer uma segunda espira na distância de 7,8 cm da primeira. Ambas as espiras devem ser curvadas na mesma direção e devem estar do mesmo lado do fio. Faça a terceira e a quarta espira seguindo o mesmo procedimento, mantendo a distância de 7,8 cm entre elas. Corte o último elemento de fase a uma distância de 8,0 cm da quarta espira.

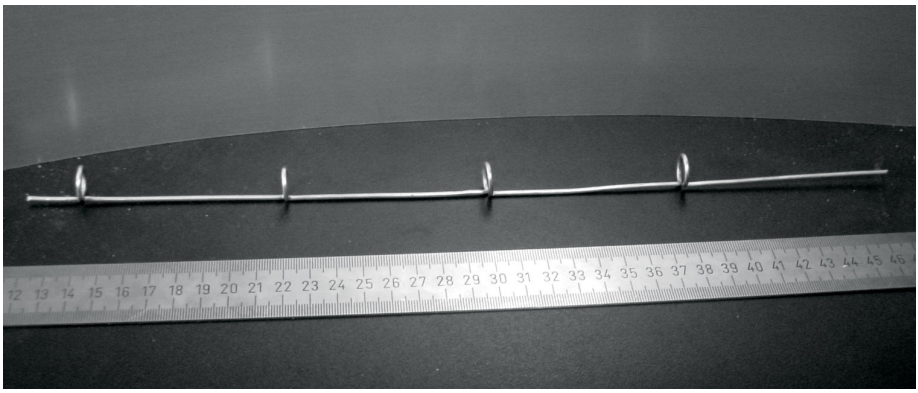


Figure 4.19: Tente manter sua montagem tão reta quanto possível.

Se as espiras foram feitas de forma correta, deve ser possível inserir um cano entre elas, como mostrado abaixo:

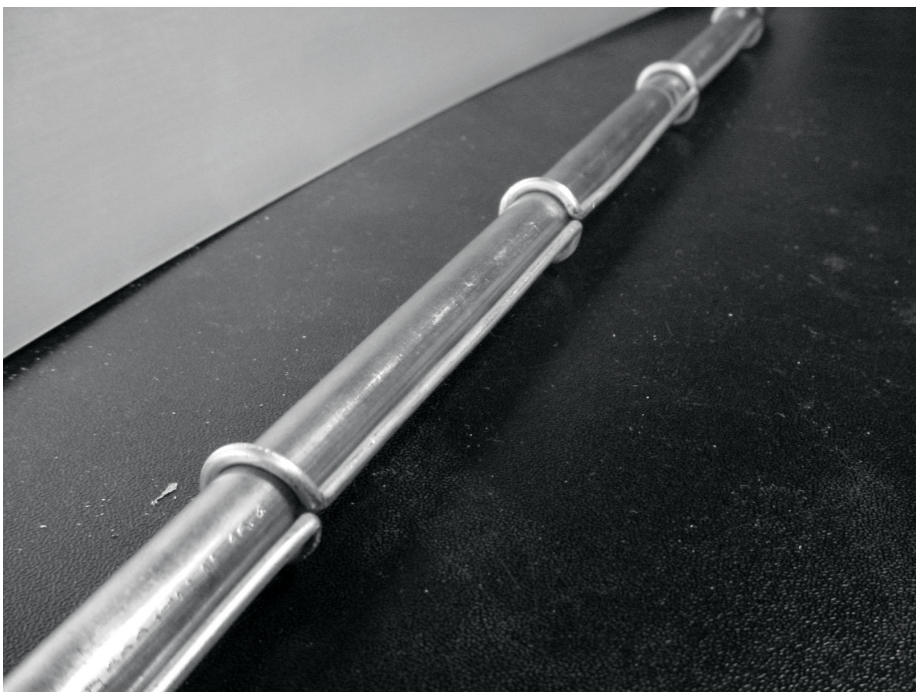


Figura 4.20: Inserir um cano entre as espiras pode ajudar a endireitar o fio.

6. Com o marcador e uma régua, desenhe as diagonais na placa metálica, de forma a encontrar seu centro. Com uma broca de diâmetro pequeno, faça um furo guia no centro da placa. Aumente o diâmetro do furo com brocas de diâmetro crescente.

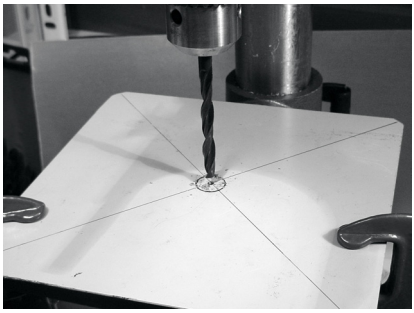


Figura 4.21: Furando a placa metálica.

O furo deve servir para o encaixe perfeito do conector N. Use uma lima se necessário.

Figura 4.22: O furo deve servir para o encaixe perfeito do conector N.

7. Para que a antena tenha uma impedância de 50 Ohms, é importante que a superfície visível do isolante interno do conector (a área branca ao redor do pino central) esteja no mesmo nível da superfície da placa. Por isto, corte 0,5 cm do cano de cobre com o diâmetro externo de 2 cm, e coloque-o entre o conector e a placa.

Figura 4.23: A adição de um espaçador feito a partir do cano de c obre ajuda a casar a impedância da antena em 50 Ohms.

8. Rosqueie a porca ao conector, fixando-o firmemente à placa com a ajuda da chave inglesa ou outra ferramenta apropriada.

Figura 4.24: Firme bem o conector N à placa.

9. Lime o lado do fio que tem 2,5 cm de distância da primeira espira. Use o torninho como auxiliar e estanhe cerca de 0,5 cm da área suavizada.

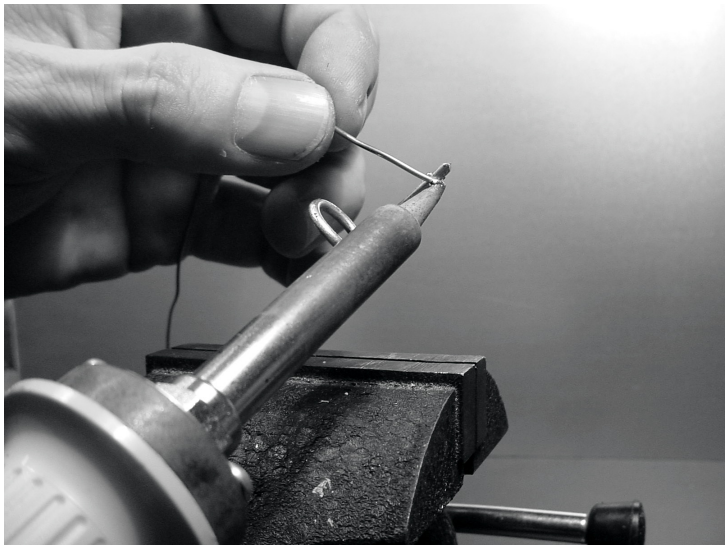


Figura 4.25: Adicione um pouco de solda ao final do fio, estanhando-o antes de soldá-lo.

10. Com o ferro de solda, estanhe o pino central do conector. Mantendo o fio na posição vertical, com o auxílio do alicate, solde seu lado estanhado no furo do pino central. A primeira espira deve ficar a 3,0 cm da placa.

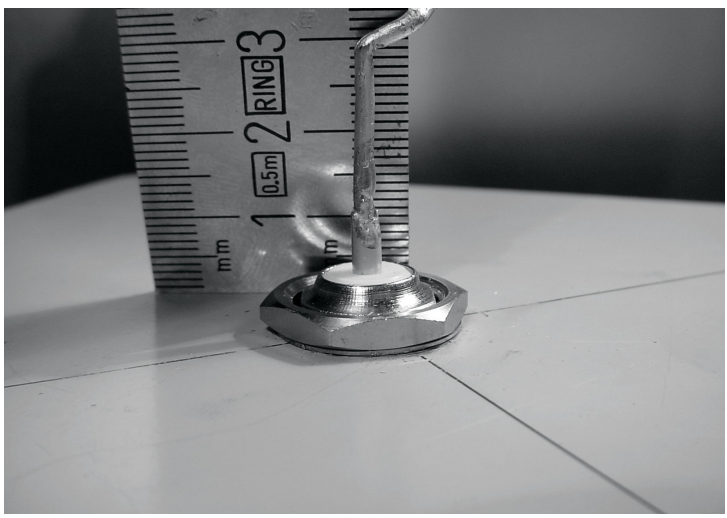


Figura 4.26: A primeira espira deve começar a 3,0 cm da superfície da placa.

11. Agora vamos esticar as espiras, aumentando o comprimento vertical do fio. Usando o torninho e o alicate, você deve puxar o cabo de

forma que o comprimento total da espira seja de 2,0 cm.

Figura 4.27: Esticando as espiras. Seja cuidadoso e tente não arranhar a superfície do fio com o alicate.

12. Repita o mesmo procedimento para as outras três espiras, esticando-as para o comprimento de 2,0 cm.

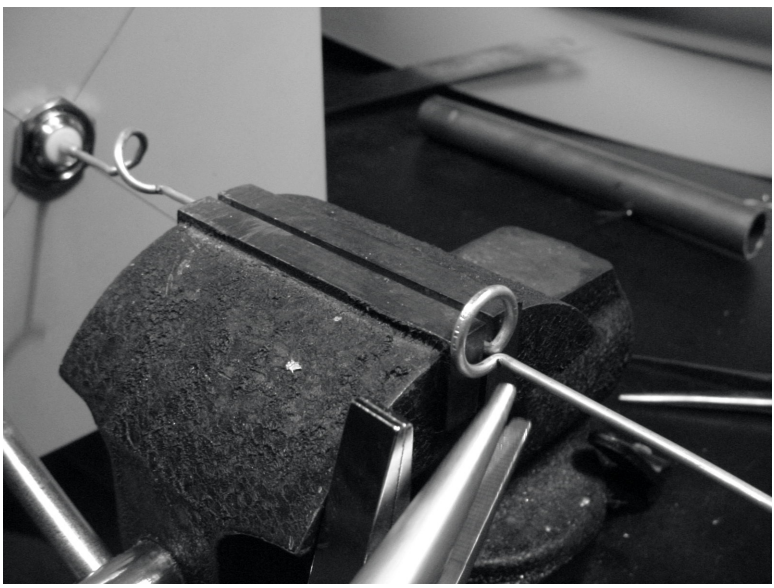


Figura 4.28: Repita o procedimento, esticando todas as demais espiras.

13. No final, a antena deve medir 42,5 cm da placa ao topo.

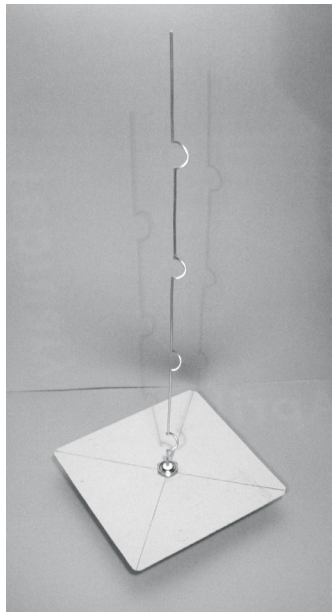


Figura 4.29: A antena finalizada deve ter 42,5 cm da placa ao final do fio.

14. Se você tiver um analisador de espectro com um gerador de sinal e um acoplador direcional, você poderá verificar a curva da potência refletida da antena. A figura abaixo mostra o visor do analisador de espectro.

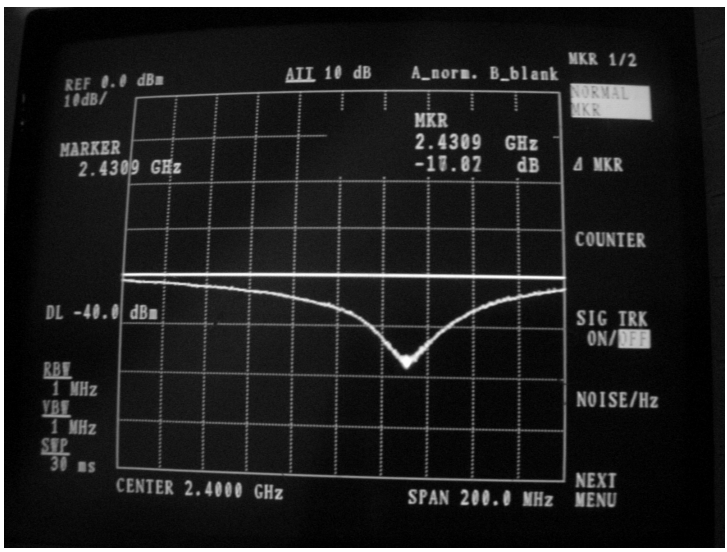


Figura 4.30: Plotagem do espectro da potência refletida da antena colinear omni.

Caso você for usá-la como uma antena externa, precisará protegê-la do tempo. O método mais simples de fazer isto é colocar todo o conjunto em um pedaço de cano grosso de PVC, encapando suas aberturas. Corte um furo no fundo para a linha de transmissão e sele o conjunto com silicone ou cola de PVC.

Cantenna

A antena de guia de onda, algumas vezes chamada Cantenna (do inglês "*can*", lata), usa uma lata metálica como guia de onda e um pequeno fio soldado em um conector N como sonda (*probe*) para a transição entre o cabo coaxial e a guia de onda. Ela pode ser construída apenas com o investimento no conector e reciclando uma lata de comida, suco, ou qualquer outra. É uma antena direcional, útil para links ponto-a-ponto de curta ou média distância. Pode também ser usada como alimentação para um prato ou grade parabólica.

Nem todas as latas são boas para a construção da antena em função da dimensão de seus limites.

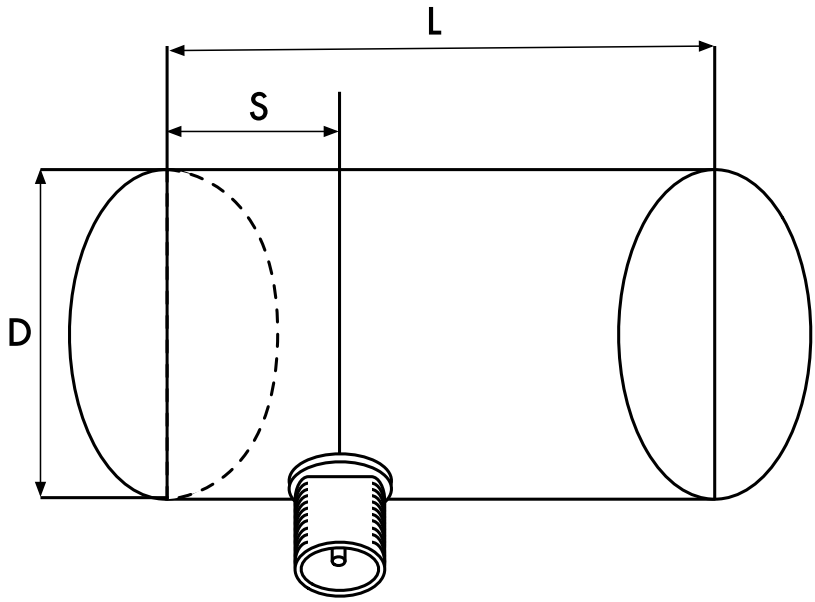


Figura 4.31: Os limites dimensionais para uma cantenna.

1. Os valores aceitáveis do diâmetro D para o alimentador estão entre 0,60 e 0,75 do comprimento de onda no ar da freqüência desejada. Com 2,44 GHz o comprimento de onda λ é 12,2 cm. Então, o diâmetro da lata deve estar entre 7,3 e 9,2 cm.

2. O comprimento L da lata deve ter, preferencialmente, um mínimo de 0,75 λ_G, onde λ_G é a guia do comprimento de onda, que e dada por:

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

Para D = 7,3 cm, precisamos de uma lata com ao menos 56,4 cm, enquanto para D = 9,2 cm, ela terá que ter ao menos 14,8 cm. Na prática, quanto menor o diâmetro, mais longa deve ser a lata. Em nosso exemplo, usaremos latas de óleo com um diâmetro de 8,3 cm e altura de cerca de 21 cm.

3. A sonda (probe) para a transição entre o cabo coaxial e a guia de onda deve ser posicionada à distância S do fundo da lata, dada por:

$$S = 0.25\ \lambda_G$$

Seu comprimento deve ser 0,25 λ, correspondendo, para uma freqüência de 2,44 GHz, a 3,05 cm.

O ganho desta antena será da ordem de 10 a 14 dBi, com a largura do feixe de cerca de 60 graus.

Figura 4.32: A cantenna finalizada.

Lista de componentes

- Um conector tipo N, fêmea, de parafusar
- 4 cm de fio (arame) de cobre ou bronze, com 2 mm de diâmetro
- Uma lata de óleo com 8,3 cm de diâmetro e 21 cm de altura

Figura 4.33: Componentes necessários para a antena de lata.

Lista de ferramentas

- Abridor de latas
- Régua
- Alicate
- Lima
- Ferro de solda
- Solda
- Furadeira com um conjunto de brocas para metal (incluindo uma broca de 1,5 cm de diâmetro)
- Um pedaço de cano ou uma broca de furadeira com 1 cm de diâmetro
- Torninho ou outro tipo de suporte
- Martelo
- Furador

Construção

1. Com o abridor de latas, remova cuidadosamente a parte de cima da lata.

Figura 4.34: Tenha cuidado com as beiradas afiadas ao abrir a lata.

O disco circular tem a beirada muito afiada. Tenha cuidado ao manuseá-lo! Esvazie a lata e lave-a com sabão. Caso a lata contenha abacaxi, bolachas ou alguma outra guloseima, compartilhe com um amigo.

2. Com a régua, meça 6,2 cm a partir do fundo da lata e marque um ponto. Tenha cuidado em medir a partir da parte de dentro do fundo da lata. Use um furador (ou uma pequena broca, ou uma chave Phillips) e um martelo para marcar o ponto. Isto facilita na hora de usar a broca para fazer o furo. Certifique-se de não mudar a forma da lata ao fazer isto usando um pequeno bloco de madeira ou outro objeto dentro da lata antes de marcá-la.

Figura 4.35: Marque o furo antes de usar a broca.

3. Com uma broca de diâmetro pequeno, faça um furo na posição marcada. Aumente o diâmetro do furo gradualmente, usando brocas de tamanho crescente. O furo deve comportar, exatamente, o conector N. Use a lima para suavizar a borda do furo e remover a tinta ao redor dele, garantindo um melhor contato elétrico com o conector.

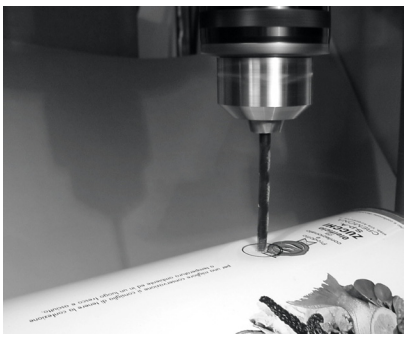


Figura 4.36: Com cuidado, faça primeiro um furo guia, depois use brocas maiores para terminar o trabalho.

4. Lime uma das extremidades do fio, estanhando-a em cerca de 0,5 cm, com o auxílio do torninho ou alicate.

Figura 4.37: Estanhe a extremidade do fio antes de soldá-lo.

5. Com o ferro de solda, estanhe o pino central do conector. Mantendo o fio na vertical com o alicate, solde o lado estanhado ao furo do pino central.

Figura 4.38: Solde o fio ao copo dourado no conector N.

6. Insira a arruela e gentilmente rosqueie a porca no conector. Corte o fio em 3,05 cm, medido a partir da base do conector.

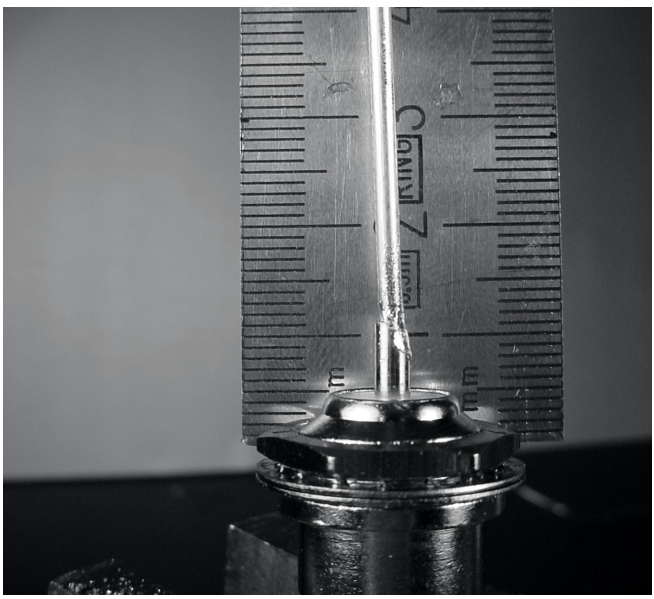


Figura 4.39: O tamanho do fio é crítico.

7. Desenrosque a base do conector, deixando a arruela em seu lugar. Insira o conector no buraco da lata e rosqueie novamente o conector por dentro da lata.

Figura 4.40: Montagem da antena.

8. Use o alicate ou a chave inglesa para rosquear firmemente a porca no conector. Pronto!

Figura 4.41: Sua antena concluída.

Assim como outros projetos de antena, você deve protegê-la contra o tempo para o uso externo. Tubos de PVC funcionam bem para a antena de lata. Insira toda a lata em um tubo largo de PVC, vedando as extremidades com tampas e cola. Você precisará fazer um furo lateral no tubo para acomodar o conector N no lado da lata.

Cantenna como alimentador de parabólica

Da mesma forma que o USB dongle e a parabólica, você pode usar o projeto da cantenna como um alimentador, com um ganho significativamente mais alto. Monte a lata na parabólica com a abertura da mesma apontando para o centro do prato. Use a técnica descrita no exemplo da antena com o USB dongle (observando a mudança da intensidade do sinal) para encontrar a melhor posição da lata para a parabólica que você está usando.

Usando uma cantena bem construída em conjunto com uma parabólica devidamente sintonizada, você pode ter um ganho total de 30 dBi ou mais. Aumentando o tamanho da parabólica, aumenta também o ganho e a diretividade da antena. Com parabólicas bem maiores, você pode conseguir ganhos significativamente maiores.

Por exemplo, em 2005, uma equipe de estudantes universitários estabeleceu um link de Nevada para Utah nos Estados Unidos. Este link atravessou uma distância acima de 200 Km. Os entusiastas de comunicações sem fio usaram um prato de satélite de 3,5 metros para estabelecer uma conexão 802.11b de 11 Mbps, sem o uso de um amplificador. Os detalhes desta conquista podem ser encontrados em *http://www.wifi-shootout.com/*

NEC2

NEC2 significa ***Numerical Electromagnetics Code*** versão 2, e é um software livre para o projeto de antenas, que permite a você construir um modelo tridimensional de antena e então analisar a sua resposta eletromagnética. O programa foi desenvolvido há mais de dez anos e foi compilado para a execução em muitos sistemas operacionais distintos. O NEC2 é particularmente eficaz para a análise de modelos de grades de fios, mas também tem alguma capacidade para modelos de superfícies sólidas (patch).

O projeto da antena é descrito em um arquivo texto e então o modelo é feito a partir desta descrição. Uma antena descrita em NEC2 é dividida em duas partes: sua ***estrutura*** e a seqüência de ***controles***. A estrutura é simplesmente a descrição numérica mostrando onde as diferentes partes da antena estão localizadas e como os fios estão conectados. Os controles dizem ao NEC onde a fonte de RF está conectada. Uma vez definidos estes valores, a antena é modelada. Em função do teorema da reciprocidade, o padrão de transmissão é igual ao de recepção, de forma que as características do modelo de transmissão são suficientes para a compreensão completa do comportamento da antena.

Uma freqüência, ou uma variação de freqüências, para o sinal RF deve ser especificada. Outro elemento importante é a característica do aterramento. A condutividade da terra varia de um lugar para outro, mas em muitos casos ela tem um papel vital na determinação do padrão de ganho da antena.

Para rodar o NEC2 no Linux, instale o pacote NEC2 da URL *http://www.nec2.org/*[4]. Ele pode ser executado digitando **`nec2`** e fornecendo os nomes dos arquivos de entrada e saída (também é interessante instalar o pacote **`xnecview`** para a verificação da estrutura e exibição gráfica do padrão de radiação). Se tudo correr bem, você deve ter como resultado o arquivo de saída populado de informações. Ele pode ser dividido em várias sessões, mas para uma idéia rápida do que ele representa, pode-se usar o xnecview para que o padrão de ganho seja exibido graficamente. Você deve ver o padrão esperado, horizontalmente omnidirecional, com um pico de melhor ângulo. Versões para Windows e Mac também estão disponíveis.

A vantagem do NEC2 é que ele nos dá uma boa idéia de como a antena funcionará, mesmo antes de sua construção, permitindo-nos modificar o projeto a fim de obter o máximo ganho. A ferramenta é complexa e requer algum estudo para que se aprenda a usá-la efetivamente, mas é uma ferramenta inestimável para projetistas de antenas.

A documentação online pode ser obtida da "Unofficial NEC Home Page" em *http://www.nittany-scientific.com/nec/*

4. N. do T. - Nas versões mais recentes do Ubuntu e seus derivados, estes softwares estão disponíveis para a instalação através do gerenciador de programas.

5
Hardware de rede

Nos últimos anos, o interesse sem precedentes em equipamentos para redes sem fio fez com que uma variedade de equipamentos de baixo custo aparecessem no mercado. Tal variedade é tamanha que, de fato, é impossível catalogar todos os equipamentos existentes. Neste capítulo, abordaremos quais funcionalidades e atributos são desejáveis em componentes wireless, e veremos vários exemplos de equipamentos comerciais e outros no estilo "faça você mesmo" que provaram funcionar bem até o momento.

Wireless com fio

Quando falamos em redes "sem fio" é difícil imaginar a quantidade de fios envolvida no estabelecimento de uma simples conexão ponto-a-ponto. Um nó wireless consiste em muitos componentes que devem ser conectados uns aos outros com cabos apropriados. Obviamente, você precisa ao menos de um computador conectado a uma rede Ethernet, assim como um roteador wireless conectado à mesma rede. Componentes de rádio precisam estar conectados a antenas, mas ao longo do caminho eles podem estar conectados também a um amplificador, um supressor de raios ou outros dispositivos. Muitos equipamentos necessitam de energia, seja diretamente da rede elétrica ou através de fontes de alimentação. Todos eles usam vários tipos de conectores, além de cabos de vários tipos e tamanhos.

Agora, multiplique estes cabos e conectores pelo número de nós que estarão online e você pode se perguntar o porquê disto tudo ser chamado de "sem fio". O diagrama na página a seguir dá uma idéia da quantidade de cabeamento necessária para uma simples rede ponto-a-ponto. Note que o diagrama não está em escala e sequer representa a melhor escolha para um projeto de rede, mas ele mostra as várias interconexões e componentes que você encontrará no mundo real.

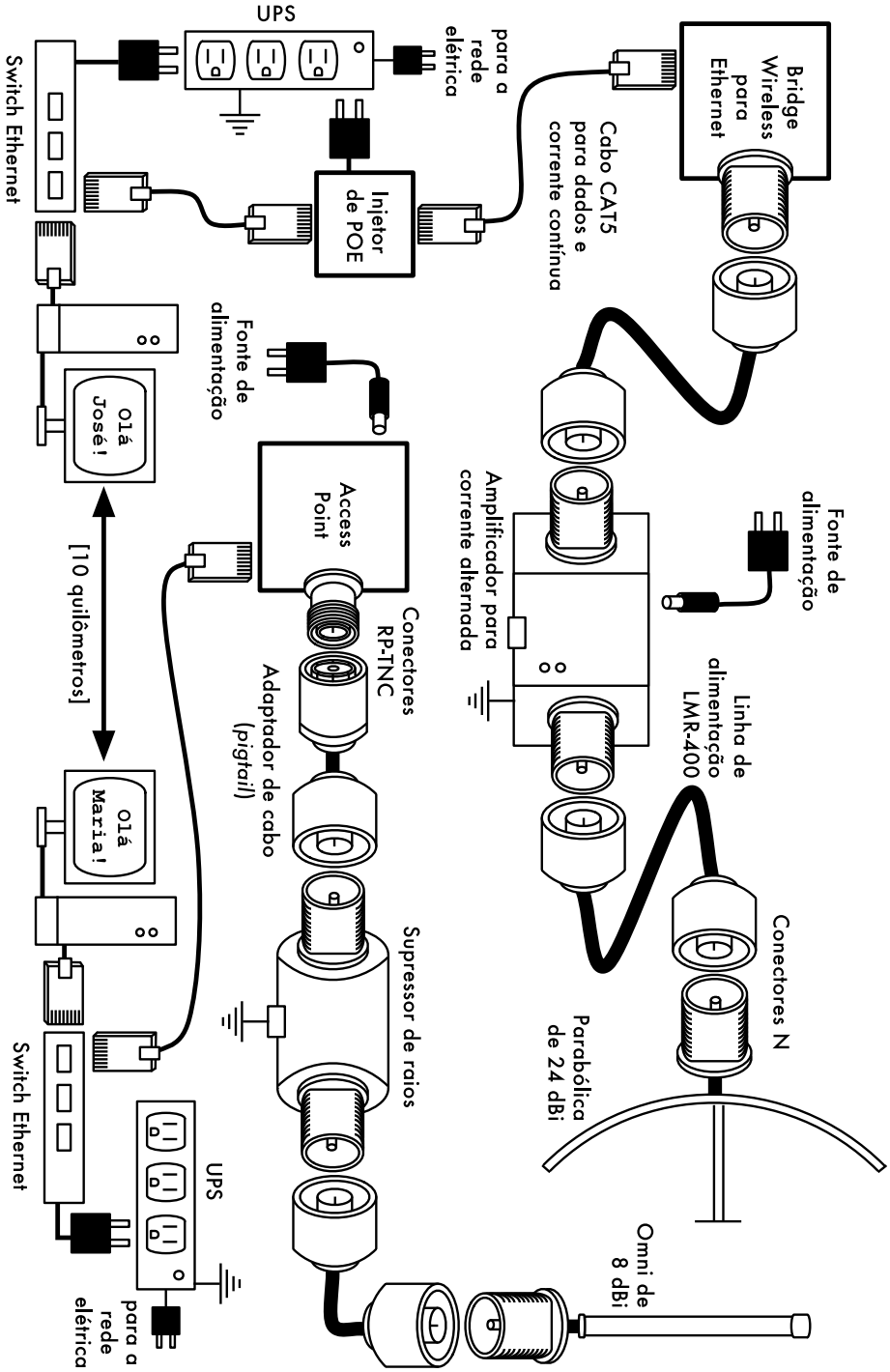


Figura 5.1: Interconexão de componentes.

Mesmo que os componentes possam variar a cada nó, toda instalação terá ao menos os seguintes:

1. Um computador ou rede conectada a um switch Ethernet;
2. Um dispositivo que conecte a rede a um dispositivo wireless (um roteador wireless, bridge ou repetidor);
3. Uma antena que estará conectada através de uma linha de transmissão ou integrada ao dispositivo wireless;
4. Componentes elétricos compostos de fontes de alimentação, filtros de linha e supressores de raios.

A real seleção do hardware será determinada pelos requisitos do projeto, orçamento possível e a sua viabilidade considerando os recursos disponíveis (considerando previsão de peças sobressalentes e custos de manutenção). Como discutido no **Capítulo 1**, a fase de estabelecimento do escopo do projeto é crítica e acontece antes que decisões sobre compras sejam feitas.

Escolhendo componentes wireless

Infelizmente, em um mundo de competição entre fabricantes de hardware e orçamentos limitados, a etiqueta de preço é o fator que acaba recebendo a maior atenção. O velho ditado "o barato sai caro" é freqüentemente real quando adquirimos equipamentos de alta tecnologia, mas isto não deve ser considerado como verdade absoluta. Ainda que o preço seja parte importante na decisão de qualquer compra, é de importância fundamental o entendimento do que está se obtendo pelo valor pago para que se possa escolher algo que realmente corresponda às necessidades.

Na comparação de equipamentos wireless para o uso em sua rede, considere as seguintes variáveis:

- **Interoperabilidade**. O equipamento considerado funcionará com equipamentos de outros fabricantes? Caso contrário, isto é um fator importante para este segmento de sua rede? Caso o dispositivo em questão suporte um protocolo aberto (como o 802.11b/g), então ele provavelmente irá interoperar com equipamentos de outros fabricantes.
- **Alcance**. Como vimos no **Capítulo 4**, o alcance não é algo inerente a uma peça particular de equipamento. O alcance de um dispositivo depende da antena conectada a ele, das características da área coberta pelo link, do equipamento na outra ponta e vários outros fatores. Ao invés de confiar em uma taxa de alcance quase fictícia fornecida pelo fabricante, é melhor conhecer a ***potência de transmissão*** e o ***ganho de antena*** (caso seja parte do equipamento). Com esta informação, você pode calcular o alcance teórico, conforme descrito no **Capítulo 3**.
- **Sensitividade do rádio**. Qual é a sensitividade do rádio em uma determinada taxa de comunicação? O fabricante deveria fornecer esta informação, ao menos os limites de sensitividade para as velocidades mais altas e mais baixas de comunicação. Isto pode ser usado como

uma medida da qualidade do hardware, assim como ajudar no cálculo do orçamento do link. Como abordamos no **Capítulo 3**, um número baixo para a sensitividade é o melhor.

- **Throughput** (taxa de transmissão). Os fabricantes apresentam, consistentemente, a maior taxa de transmissão como a "velocidade" do equipamento. Tenha em mente que esta taxa simbólica (por exemplo, 54 Mbps) nunca é a real velocidade do dispositivo (por exemplo, 22 Mbps para o padrão 802.11g). Caso a informação sobre a real taxa de transmissão do dispositivo que você está avaliando não esteja disponível, uma boa estimativa é dividir a informação sobre a velocidade do mesmo por dois e diminuir cerca de 20%. Em caso de dúvida, faça testes para descobrir a taxa de transmissão no equipamento que está sendo avaliado, antes de comprometer o orçamento em algum dispositivo que não forneça oficialmente esta informação.
- **Acessórios requeridos**. Para manter o preço inicial baixo, os fornecedores freqüentemente deixam de fora acessórios que são necessários para o uso normal do equipamento. O preço inclui todas as fontes de alimentação? (Conversores de rede elétrica para corrente contínua estão, tipicamente, incluídos; conversores para a alimentação a partir da Ethernet não estão. Verifique a tensão de rede elétrica de entrada – 110V, 220V, etc – já que muitos equipamentos levam em conta apenas a realidade dos Estados Unidos). E conversores de cabos, adaptadores, cabos, antenas e cartões de rádio? Caso você venha a usar o equipamento externamente, ele tem proteção contra o mau-tempo?
- **Disponibilidade**. Você conseguirá, com facilidade, substituir componentes com problemas? Você poderá encomendar peças sobressalentes em altas quantidades, caso seu projeto necessite? Qual o tempo de vida projetado para um determinado produto, tanto em termos de vida útil quanto de disponibilidade do fabricante?
- **Outros fatores**. Certifique-se de que outras funcionalidades estão contempladas para sua necessidade em particular. Por exemplo, o dispositivo possui um conector para antena externa? De que tipo é este conector? Há limitações de taxas de transmissão impostas pelo software do equipamento? Qual o custo para a ampliação destes limites? Qual o tamanho e forma do equipamento? Qual o consumo de energia? Ele pode ser alimentado via Ethernet (*POE – Power Over Ethernet*)? O dispositivo fornece criptografia? NAT? Ferramentas de gestão? Alguma outra funcionalidade considerada crítica para seu projeto de rede?

Ao responder estas questões, você será capaz de, inteligentemente, tomar decisões sobre a aquisição de equipamentos de rede. Dificilmente você conseguirá responder todas as questões possíveis antes de efetuar uma compra, mas você pode priorizar estas questões de acordo com as necessidades de seu projeto e, usando-as para pressionar o fornecedor antes de efetuar a compra, você fará o melhor uso do orçamento disponível e construirá uma rede com componentes adequados à sua necessidade.

Soluções comerciais versus "faça você mesmo"

Seu projeto de rede irá, quase com certeza, ser composto de componentes comprados de fornecedores clássicos e de outros comprados ou mesmo fabricados localmente. Isto é o que acontece em todas as partes do mundo. No estágio atual da tecnologia, a distribuição global de informação é trivial quando comparada à distribuição de bens. Em muitas regiões, a importação dos componentes necessários à construção de uma rede tem um custo proibitivo para a maioria dos orçamentos disponíveis. Você pode economizar bastante, em curto prazo, buscando fornecedores de equipamentos e mão-de-obra locais, apenas importando o que é absolutamente necessário.

Claro, há limite na quantidade de trabalho fornecida por um indivíduo ou grupo dentro de uma certa quantidade de tempo. Colocando isto de outra maneira, ao importar tecnologia, você pode resolver um problema ao trocar dinheiro gasto em um equipamento pela quantidade de tempo na qual resolveria o mesmo problema com recursos locais. A arte da construção de uma infra-estrutura local de comunicação está baseada no equilíbrio ao encontrar a melhor solução, seja com a importação de equipamentos ou com investimentos em produtos e serviços localmente disponíveis.

Alguns componentes, como cartões de rádio e linhas de alimentação de antena, são complexos demais para a fabricação local, manual. Outros componentes, como antenas e torres, são relativamente simples e podem ser fabricados localmente por uma fração do custo de sua importação. Entre estes extremos estão os próprios dispositivos de comunicação.

Ao usar equipamentos de prateleira, como cartões de rádio, placas-mãe e outros, você pode construir dispositivos que fornecem funcionalidades comparáveis (ou até superiores) a ofertas comercialmente disponíveis. Combinando plataformas de hardware aberto com softwares de código aberto é possível a construção de soluções robustas, personalizadas e com custo muito baixo.

Não queremos dizer com isto que equipamentos comerciais são inferiores a soluções do tipo "faça você mesmo". Ao fornecer soluções com tecnologia de ponta, prontas para o uso, os fabricantes não apenas economizam nosso tempo de desenvolvimento como também permitem que indivíduos, sem a necessidade de especialização técnica, instalem e mantenham equipamentos de rede. A grande força das soluções comerciais está no fato de que elas incluem ***suporte*** técnico e a oferta de ***garantia do equipamento***, mesmo que limitada. Estas soluções comerciais também fornecem uma plataforma de rede consistente, que tende a ser bastante estável e intercambiável.

Caso um equipamento não funcione, ou seja difícil de configurar, um bom fornecedor fornecerá o auxílio necessário. Se o mesmo falhar em seu uso normal (salvo algum dano extremo, como o causado por um raio), o fabricante o substituirá. A maioria dos fabricantes fornecerá este serviço por um tempo limitado, incluído no preço de compra, ou pode fornecer uma garantia estendida ou suporte mensal por uma taxa mensal. Justamente por fornecer uma plataforma consistente, é viável para o fornecedor manter peças de substituição

e equipamentos reserva para a substituição em caso de falhas, sem a necessidade de enviar um técnico para o conserto e configuração do equipamento. Claro, todos estes serviços podem ter um custo adicional, comparado ao "preço de prateleira" do equipamento.

Do ponto de vista de um arquiteto de rede, os três principais riscos ocultos na escolha de soluções comerciais estão na ***dependência de um fabricante único***, ***descontinuidade de uma linha de produtos*** e ***custos contínuos de licenças***.

O custo da utilização de "novas funcionalidades", definidas de maneira muito prematura pelos fornecedores, em sua rede, pode ser muito alto. Os fabricantes oferecem, com freqüência, funcionalidades que são incompatíveis, de propósito, com seus competidores, fazendo um marketing que tenta convencê-lo de que é impossível viver sem tais funcionalidades (independente delas contribuírem para a solução de seus problemas de comunicação). Na medida em que você começa a usar estas funcionalidades, você pode ser forçado a decidir pela continuidade de compra de equipamentos do mesmo fornecedor, criando uma dependência. Se uma grande instituição utiliza uma grande quantidade de equipamento proprietário, é improvável que ela irá abandonar tal equipamento para adotar outros fornecedores. Equipes de venda sabem disso muito bem e irão usar este fator como uma estratégia para garantir a dependência do cliente em negociações de preço.

Garantida a dependência, um fornecedor pode decidir descontinuar uma linha de produtos, independente de sua popularidade. Isto garante que os consumidores, dependentes das funcionalidades proprietárias do fornecedor, irão adquirir novos (e mais caros) modelos do mesmo. Os efeitos de longo prazo da dependência de um fornecedor e de produtos que podem ser descontinuados são difíceis de estimar em um projeto de rede mas, mesmo assim, eles devem ser levados em conta.

Por fim, se um determinado equipamento usa código de programa proprietário, você poderá ter que adquirir uma licença de uso para o mesmo. O custo desta licença pode variar de acordo com funções e volumes utilizados, como número de usuários, velocidade de conexão, entre outros. Alguns equipamentos são projetados para, simplesmente, deixarem de funcionar caso a licença não seja paga. Certifique-se de entender os termos de uso de qualquer equipamento que você adquirir, incluindo as taxas de licença.

Ao usar equipamentos genéricos que suportem padrões abertos e softwares de código livre, você evita algumas destas armadilhas. Por exemplo, é muito difícil criar a dependência de um fornecedor que use protocolos abertos (como o TCP/IP sobre 802.11a/b/g). Caso você encontre algum problema com o equipamento ou o fornecedor, você pode adquirir equipamentos de um fornecedor diferente, que irá interoperar com os que você adquiriu anteriormente. É por esta razão que recomendamos que você **apenas** use protocolos proprietários e o espectro regulamentado apenas em casos onde equipamentos de padrão aberto (como o 802.11a/b/g) não sejam tecnicamente viáveis.

De qualquer forma, produtos individuais podem ser descontinuados a qualquer momento. Para limitar o impacto disto você deverá usar em sua rede apenas componentes genéricos. Por exemplo, uma determinada placa-mãe pode tornar-se indisponível, mas você deverá ter à mão outras placas-mães de

PCs que desempenhem, efetivamente, as mesmas tarefas. Veremos alguns exemplos de como usar componentes genéricos na construção de um nó wireless mais adiante neste capítulo.

Obviamente, não existem custos permanentes de licenças quando se utiliza software de código aberto (com a exceção de um fornecedor que ofereça suporte estendido ou outros serviços, sem cobrar pelo uso deste software). Há fornecedores que, ocasionalmente, capitalizam em cima da dádiva que os programadores de código aberto ofereceram ao mundo, oferecendo seu código sob a venda de licenças, violando os termos de distribuição definidos pelos autores deste código. A atitude sábia é evitar tais fornecedores e suspeitar qualquer oferta de "software livre" atrelada ao pagamento de alguma licença.

A desvantagem do uso de software de código aberto e hardware genérico é, claramente, a questão do suporte. Caso surjam problemas com a rede, você deverá solucioná-los de forma independente. Freqüentemente, isto é conseguido através da consulta da documentação online livre, de mecanismos de busca e da aplicação das correções por você, sua equipe ou recursos terceirizados. Se não tiver, em sua equipe, pessoas que tenham a competência para desenvolver soluções para seu problema de comunicação, então pode ser necessária uma quantidade enorme de tempo para que seu projeto de rede se concretize. Claro, não existe garantia alguma de que gastando o dinheiro suficiente o problema será resolvido. Enquanto fornecemos muitos exemplos de como o trabalho pode ser feito por você, é possível que você o ache muito desafiador e complicado. É preciso descobrir o equilíbrio entre as soluções comerciais e as do tipo "faça você mesmo" para o funcionamento do projeto.

Em resumo, sempre defina, primeiramente, o escopo de seu projeto. Identifique os recursos que devem estar disponíveis para a solução de seu problema e permita que a seleção do equipamento surja, de forma natural, dos resultados. Considere soluções comerciais e componentes abertos tendo em mente o custo a longo prazo de ambos.

Ao considerar qual equipamento usar, lembre-se sempre de levar em conta a distância a ser coberta, a confiabilidade e taxa de transmissão, em conjunto com o preço. Certifique-se de incluir taxas de licenças ao totalizar o custo do equipamento. Por fim, verifique se os rádios que você está adquirindo operam dentro do espectro livre onde você os está instalando ou se você possui o orçamento e a autorização para pagar as devidas licenças.

Proteção profissional contra raios

Raios são predadores naturais de equipamentos wireless. Há duas maneiras pelas quais eles podem prejudicar os equipamentos: atingindo-os diretamente ou por indução. Raios podem atingir diretamente as torres ou antenas. A indução ocorre quando o raio atinge locais próximos ao equipamento. Imagine um raio carregado negativamente. Uma vez que cargas iguais repelem uma a outra, este raio irá causar com que os elétrons nos cabos fujam deles, criando uma corrente elétrica nas linhas de transmissão. Esta corrente pode estar acima da capacidade com a qual os sensíveis rádios possam lidar. Qualquer tipo de raio irá, usualmente, destruir equipamentos desprotegidos.

Figura 5.2: Uma torre com aterramento pesado de fios de cobre.

A proteção de redes sem fio contra raios não é uma ciência exata e não existe garantia de que um raio não causará danos, mesmo que todas as precauções sejam tomadas. Muitos dos métodos usados ajudam a prevenir tanto raios diretos quanto a indução. Mesmo que não seja necessário usar cada método de proteção, quantos mais forem usados, mais protegido estará o equipamento. A quantidade de raios observada historicamente dentro de uma determinada área será o melhor guia para determinar o tipo de proteção a ser tomada.

Comece na base da torre. Lembre-se que a base da torre está debaixo da terra. Depois que a base da torre for instalada, mas antes que o buraco onde ela foi colocada seja concretada, um anel com muitas voltas de fio de aterramento deve ter sido instalado, com um terminal disponível sobre a superfície, próximo à base metálica da torre. O fio de aterramento deve ser do tipo AWG #4 (*American Wire Gauge*) ou maior. Adicionalmente, uma barra de aterramento deve ser enterrada e um fio de aterramento ainda deve unir esta barra ao anel enterrado sob a base da torre.

É importante notar que nem todo aço conduz eletricidade da mesma maneira. Alguns tipos de aço funcionam melhor como condutores de eletricidade que outros, e diferentes tipos de cobertura ou pintura também afetam a forma como uma torre de aço lida com correntes elétricas. O aço inoxidável é um dos piores condutores, e coberturas à prova de ferrugem, como as galvanizadas ou pintadas, diminuem a condutividade do aço. Por esta razão, um fio trançado de aterramento é instalado da base da antena até o seu topo. A base deve estar conectada tanto ao anel de aterramento quanto à haste adicional. O topo da torre deve ter um pára-raios, e este deve ser pontiagudo. Quanto mais fina e

afiada for a ponta do pára-raios, melhor ele será. O fio trançado de aterramento deve estar conectado ao pára-raios. É muito importante que o fio de aterramento esteja realmente conectado às partes metálicas. Qualquer tipo de cobertura ou capa, como pintura, deve ser removida antes que o fio seja conectado. Uma vez que a conexão for feita, a área exposta pode ser novamente pintada, cobrindo o fio e os conectores, se necessário, para evitar a ferrugem e outros tipos de corrosão.

A solução acima detalha a instalação de um sistema básico de aterramento. Ela fornece a proteção da torre contra raios diretos e garante a base para qualquer outra proteção adicional.

A proteção ideal contra a indução indireta de raios são supressores de surtos (centelhadores) a ar, colocados em ambas as extremidades do cabo. Estes centelhadores devem estar aterrados diretamente ao cabo de aterramento instalado na torre, caso estejam ligados à ponta do cabo que está no topo. Para a outra extremidade dos cabos, o aterramento deve ser feito em algo que seja eletricamente seguro, como uma placa de aterramento ou um encanamento de cobre que esteja consistentemente cheio de água. É importante que o centelhador instalado externamente seja protegido contra o tempo. Muitos supressores para cabos coaxiais já têm esta proteção, enquanto supressores para cabos CAT5 não a tem.

Caso centelhadores não sejam usados, e o cabeamento usado for do tipo coaxial, aterrar a blindagem do cabo, em um lado ao aterramento da antena e do outro ao aterramento local, irá fornecer alguma proteção. Isto irá fornecer um caminho de passagem para as correntes de indução e, se a carga for fraca o suficiente, não afetará o fio condutor do cabo. Mesmo que este método não consista, de maneira alguma, uma proteção tão eficiente quanto o uso de centelhadores, ele é melhor do que não ter proteção alguma.

Construindo um ponto de acesso a partir de um PC

Ao contrário de sistemas operacionais para o consumo (como o Microsoft Windows), o sistema operacional GNU/Linux permite ao administrador de redes o acesso completo à pilha de rede. É possível manipular os pacotes de rede em qualquer nível, desde o de conexão de dados até o de aplicação. Decisões de roteamento podem ser feitas baseadas na informação contida em um pacote, desde o endereço de roteamento e portas até o conteúdo do segmento de dados. Um ponto de acesso baseado em Linux pode servir como roteador, bridge, firewall, concentrador de VPN, servidor de aplicação, monitor de rede ou virtualmente qualquer outro papel na rede que você puder imaginar. O software é disponível livremente e não requer o pagamento de licenças. O GNU/Linux é uma ferramenta muito poderosa, que pode preencher uma ampla variedade de tarefas em uma infra-estrutura de rede.

A adição de um cartão wireless e de um dispositivo Ethernet a um PC rodando o Linux irá proporcionar uma ferramenta flexível que auxiliará na oferta de largura de banda e na gestão da rede por um custo muito baixo. O hardware pode ser qualquer um, desde um laptop ou desktop reciclados ou um

computador embarcado (*embedded*), como o Linksys WRT54G ou um kit de rede Metrix.

Nesta sessão, veremos como configurar o Linux nas seguintes situações:

- Um ponto de acesso wireless com NAT e uma conexão cabeada à Internet (também chamado de *gateway wireless*);
- Um ponto de acesso wireless que atua como uma bridge transparente. A bridge pode ser usada tanto como um ponto de acesso como um repetidor com dois rádios.

Considere estas receitas como um ponto de partida. Construindo a partir destes exemplos, você poderá criar um servidor que estará precisamente adequado à sua infra-estrutura de rede.

Pré-requisitos

Antes de seguir adiante, você deve ter alguma familiaridade com o Linux, do ponto de vista de um usuário, e ser capaz de instalar uma distribuição Linux de sua escolha. O conhecimento básico do uso da linha de comando (terminal) também é necessário.

Você precisará de um computador com uma ou mais interfaces wireless instaladas, assim como uma interface Ethernet padrão. Estes exemplos usam um cartão e um driver específicos, mas há uma série de outros que também funcionarão bem. Cartões wireless baseados na arquiteturas (chipsets) Atheros ou Prism funcionam particularmente bem. Estes exemplos são baseados no Ubuntu Linux versão 5.10 (Breezy Badger), com um cartão wireless que é suportado pelos drivers HostAP ou MADWiFi. Para mais informações sobre estes drivers, visite *http://hostap.epitest.fi/* e *http://madwifi.org/* .

Os softwares a seguir são necessários para completar estas instalações. Eles devem ser fornecidos por sua distribuição Linux:

- Wireless Tools (iwconfig, comandos iwlist)
- iptables firewall
- dnsmasq (servidor caching DNS e DHCP)

A potência requerida para a CPU irá depender de quanto trabalho ela deverá executar além do simples roteamento e tradução de endereços (NAT). Para muitas aplicações, um processador 486 com 133MHz é perfeitamente capaz de rotear pacotes nas velocidades requeridas pelo link wireless. Caso você pretenda usar muita criptografia (como WEP ou um servidor VPN), você precisará de uma máquina mais rápida. Se você também quiser executar um servidor de cache (como o Squid), então você precisará de uma máquina com um bom espaço em um disco rápido e também memória RAM o suficiente. Um roteador típico que apenas faça o NAT irá funcionar com apenas 64MB de RAM.

Ao construir uma máquina que deverá fazer parte de uma infra-estrutura de rede, tenha em mente que discos rígidos têm um tempo de vida útil limitado quando comparados à maioria dos demais componentes. Você pode, freqüentemente, usar dispositivos de estado sólido para o armazenamento, como um disco flash no lugar do HD. Ele pode ser um disco flash USB

(assumindo que o PC seja capaz de inicializar o sistema a partir da USB) ou um "*Compact Flash*", usando um adaptador CF para IDE. Este tipo de adaptador é barato e faz com que o cartão CF comporte-se como um HD IDE padrão. Eles podem ser usados em qualquer PC que possua interfaces IDE. Uma vez que não existem partes móveis, estes PCs operarão por muitos anos, suportando variações de temperatura muito maiores que um disco rígido toleraria.

Cenário 1: Ponto de Acesso com NAT

Este é o cenário mais simples e é especialmente útil em situações onde você quer um único access point para um ambiente de escritório. É o mais fácil de implementar em situações onde:

1. Já existe um firewall dedicado e um gateway rodando Linux e você só quer adicionar uma interface wireless;
2. Você possui um computador (desktop ou laptop) velho disponível e prefere usá-lo como um access point;
3. Você precisa de mais capacidade em termos de monitoramento, registro de acessos e segurança que a maioria dos access points comerciais fornecem, mas não quer estourar seu orçamento com a compra de um access point empresarial;
4. Você quer que uma única máquina atue como dois access points (e firewall) de forma a oferecer tanto um acesso seguro à sua intranet quanto um acesso aberto para seus convidados.

Configuração inicial

Comece com um computador que já está configurado e rodando o GNU/Linux, que pode ser Ubuntu Server, ou Fedora Core. O computador deve ter ao menos duas interfaces para que isto funcione, sendo que ao menos uma delas será wireless. O resto da descrição assume que sua interface Ethernet (eth0) está conectada com a Internet e que há uma interface wireless (wlan0) que proverá a funcionalidade de access point.

Para verificar se o seu dispositivo wireless suporta o modo master, tente o seguinte comando, como usuário root:

```
# iwconfig wlan0 mode Master
```

Substitua wlan0 pelo nome que corresponda à sua interface wireless.

Se você tiver como resposta uma mensagem de erro, seu cartão wireless não suporta o modo de access point. Você ainda pode tentar a mesma configuração no modo Ad-hoc, que é suportado pela maioria dos chipsets. Isto requer que você configure todos os laptops que estarão conectados a este access point também em modo Ad-hoc, e isto pode não funcionar da forma como você espera. O melhor é encontrar um cartão que suporte o modo AP. Veja os sites HostAP e MADWiFi mencionados anteriormente para uma lista de cartões suportados.

Antes de continuar, certifique-se de que o dnsmasq está instalado em sua máquina. Você pode usar o gerenciador de pacotes em modo gráfico de sua

distribuição para instalá-lo. No Ubuntu, você pode simplesmente executar o seguinte comando, como root:

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

Configurando as interfaces

Configure seu servidor de forma que a eth0 esteja conectada à Internet. Use a ferramenta gráfica de configuração disponível em sua distribuição.

Caso sua rede Ethernet use DHCP, você pode tentar o seguinte comando, como root:

```
# dhclient eth0
```

Você deve receber um endereço IP e um gateway padrão. A seguir, configure sua interface wireless para o modo master, dando a ela o nome de sua escolha:

```
# iwconfig wlan0 essid "minha rede" mode Master enc off
```

O parâmetro **`enc off`** desliga a criptografia WEP. Para habilitar o WEP, adicione um conjunto de caracteres hexadecimais, com o tamanho apropriado:

```
# iwconfig wlan0 essid "minha rede" mode Master enc 1A2B3C4D5E
```

Alternativamente, você pode usar uma palavra legível, da seguinte forma:

```
# iwconfig wlan0 essid "minha rede" mode Master enc "s:gremio"
```

Agora, dê um endereço IP de sua sub-rede privada a sua interface wireless, certificando-se de que ele não é o mesmo usado para o seu adaptador Ethernet:

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

Configurando o NAT no kernel

A fim de que tenhamos a capacidade de traduzir endereços entre as duas interfaces no computador, precisamos habilitar o NAT (Network Address Translation) no kernel Linux. Primeiro, carregamos o módulo relevante no kernel:

```
# modprobe ipt_MASQUERADE
```

Agora, removeremos todas as regras de firewall existentes para garantir que o firewall não esteja bloqueando o envio de pacotes entre as duas interfaces. Caso você tenha um firewall rodando, certifique-se de restaurar as regras existentes depois deste teste:

```
# iptables –F
```

Habilite a funcionalidade NAT entre as duas interfaces:

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

Finalmente, precisamos habilitar o kernel para que ele encaminhe pacotes entre as interfaces:

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

Em distribuições Linux baseadas no Debian, como o Ubuntu, esta modificação também pode ser feita através da edição do arquivo **/etc/network/options**, configurando a opção **ip_forward** para yes:

```
ip_forward=yes
```

Agora, reinicie as interfaces da seguinte forma:

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

ou

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

Configurando o servidor DHCP

Neste ponto, já devemos ter um access point funcional. Ele pode ser testado conectando uma outra máquina com uma interface wireless à rede "minha rede" e dando a ela um endereço que esteja no mesmo intervalo da interface wireless do servidor (10.0.0.0/24, conforme nosso exemplo). Caso você tenha habilitado o WEP, use a mesma chave que você especificou no AP.

Para facilitar às pessoas a conexão ao servidor sem que tenham que conhecer o intervalo de endereços IP, iremos configurar um servidor DHCP que automaticamente forneça endereços aos clientes wireless.

Usaremos, para este propósito, o programa dnsmasq. Como o nome indica, ele fornece um caching DNS e um servidor DHCP. Este programa foi desenvolvido especialmente para o uso com firewalls que realizam a tradução de endereços (NAT). Ter um caching DNS é especialmente útil se a sua rede possui uma alta latência ou uma conexão de baixa largura de banda, como VSAT ou conexões discadas. Isto permite que muitas consultas de DNS sejam resolvidas localmente, economizando o tráfego para a Internet e tornando a conexão sensivelmente mais rápida para os usuários.

Instale o dnsmasq com o gerenciador de pacotes de sua distribuição. Caso ele não esteja disponível como um pacote, baixe o código fonte e instale-o manualmente. Ele está disponível em *http://www.thekelleys.org.uk/dnsmasq/doc.html*.

Tudo o que é necessário para rodar o dnsmasq é a edição de umas poucas linhas de seu arquivo de configuração, **/etc/dnsmasq.conf**.

Este arquivo é bem comentado, possuindo muitas opções para os vários tipos de configuração.

Procure a linha que começa com:

```
interface=
```

E certifique-se que ela está como:

```
interface=wlan0
```

Caso a sua interface wireless não seja a wlan0, mude para a correspondente. A seguir, encontre a linha que começa com:

```
#dhcp-range=
```

Descomente-a e edite-a de forma que corresponda ao endereço que está sendo usado, por exemplo:

```
dhcp-range=10.0.0.10,10.0.0.110,255.255.255.0,6h
```

Agora salve o arquivo e inicie o dnsmasq:

```
# /etc/init.d/dnsmasq start
```

Agora você deve poder conectar-se ao servidor como um access point e obter um endereço IP usando DHCP. Isto deve permitir que você conecte-se à Internet através do servidor.

Segurança adicional: configurando um firewall

Assim que tudo estiver configurado e testado, você pode adicionar novas regras para o firewall, usando qualquer ferramenta para firewall incluída em sua distribuição. Algumas delas são as seguintes:

- **firestarter** – um cliente gráfico para o Gnome, o que requer que seu servidor rode o ambiente Gnome;
- **knetfilter** – um cliente gráfico para o KDE, o que requer que seu servidor rode o ambiente KDE;
- **Shorewall** – um conjunto de scripts e arquivos de configuração que facilitam a configuração de um firewall iptables. Há também interfaces para o shorewall, como o webmin-shorewall;
- **fwbuilder** – uma ferramenta gráfica poderosa, mas um tanto complexa, que permite que você crie scripts iptables um uma máquina diferente do servidor e depois os transfira para ele. Não é necessário que o servidor rode um desktop gráfico, e a ferramenta é uma opção robusta para uma segurança eficiente.

Uma vez que tudo esteja devidamente configurado, certifique-se de que todas as configurações estão refletidas nos scripts de inicialização do sistema. Desta forma, elas continuarão válidas mesmo que a máquina tenha que ser reinicializada.

Cenário 2: Access point como bridge transparente

Este cenário pode ser usado tanto para um repetidor com dois rádios como para um ponto de acesso conectado a uma Ethernet. Usamos uma bridge (ponte) ao invés de roteamento quando queremos que ambas as interfaces do access point compartilhem a mesma sub-rede. Isto pode ser particularmente útil em redes com múltiplos pontos de acesso onde preferimos ter um firewall único, central, e talvez também um servidor de autenticação. Como todos os clientes compartilham a mesma sub-rede eles podem ser facilmente gerenciados com um único servidor de DHCP e firewall.

Por exemplo, você pode configurar um servidor como no primeiro cenário, mas usar duas interfaces Ethernet cabeadas ao invés de uma interface com fio e outra sem. Uma interface será a sua conexão com a Internet e a outra será conectada a um switch. Depois conecte quantos access points você precisar no mesmo switch, configurando-os como bridges transparentes. Assim, todos passarão pelo mesmo firewall e usarão o mesmo servidor DHCP.

A simplicidade de montagem de uma bridge tem, como contrapartida, o prejuízo na eficiência. Uma vez que todos os clientes usam a mesma sub-rede, o tráfego de broadcast será repetido através da rede. Isto não causa problemas em redes pequenas mas, com o aumento do número de clientes, a largura de banda passa a ser desperdiçada neste tráfego de broadcast.

Configuração inicial

A configuração inicial para o access point como bridge é similar ao do cenário anterior, sem a necessidade do dnsmasq. Siga as instruções iniciais do primeiro exemplo.

Adicionalmente, o pacote **bridge-utils** será necessário para montar a bridge. Ele está disponível para o Ubuntu e outras distribuições baseadas no Debian, assim como para o Fedora Core. Certifique-se de que ele está instalado e que o comando **brctl** está disponível antes de seguir adiante.

Configurando as interfaces

No Ubuntu ou Debian, as interfaces de rede são configuradas através da edição do arquivo **/etc/network/interfaces**.

Adicione uma seção como a que está abaixo, trocando os nomes das interfaces e os endereços IP para que reflitam sua instalação. Este exemplo assume que você está construindo um repetidor wireless com duas interfaces, wlan0 e wlan1. A interface wlan0 será a cliente para a rede “escritorio” e a wlan1 criará uma rede chamada “repetidora”.

Adicione o seguinte em **/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 “escritorio” mode Managed
pre-up iwconfig wlan1 essid “repetidora” mode Master
bridge_ports wlan0 wlan1
post-down ifconfig wlan1 down
post-down ifconfig wlan0 down
```

Comente outras seções do arquivo que correspondam a wlan0 ou wlan1 para certificar-se de que elas não interfiram em nossa configuração.

A sintaxe para a configuração de bridges através do arquivo **interfaces** é específica para distribuições baseadas no Debian, e os detalhes para a

configuração real das bridges são tratados por um par de scripts: **/etc/network/if-pre-up.d/bridge** e **/etc/network/if-post-down.d/bridge**. A documentação para estes scripts está disponível em **/usr/share/doc/bridge-utils/**.

Caso estes arquivos não existam em sua distribuição (como a Fedora Core), abaixo está uma configuração alternativa para o **/etc/network/interfaces** que fará a mesma coisa, apenas com um pouco mais de trabalho:

```
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 “escritorio” mode Managed
pre-up iwconfig wlan1 essid “repetidora” 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
```

Iniciando a bridge

Uma vez que a bridge está definida como uma interface, para iniciá-la basta executar o seguinte comando:

```
# ifup -v br0
```

O “-v” indica ao comando a utilização do modo “verboso”, que dará a você informação detalhada de sua execução.

Em Fedora Core (e outras distribuições não baseadas no Debian), você precisará ainda dar um endereço IP e uma rota padrão para o resto da rede:

```
# ifconfig br0 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
# route add default gw 192.168.1.1
```

Você deve ser capaz, agora, de conectar um laptop wireless ao novo access point e acessar a Internet (ou, ao menos, o resto de sua rede) através deste PC. Use o comando **brctl** para saber o que sua bridge está fazendo.

```
# brctl show br0
```

Cenário 1 e 2, o jeito fácil

Ao invés de configurar seu computador como um access point a partir do zero, você pode preferir usar uma distribuição Linux feita especialmente para este propósito. Distribuições deste tipo tornam o trabalho tão simples quanto inicializar um PC com uma interface wireless a partir de um CD. Veja a seção “Sistemas operacionais wireless-friendly” para mais informações.

Como você pode ver, é tarefa simples fornecer serviços de ponto de acesso a partir de um roteador Linux padrão. Usar o Linux dá a você maior controle sobre os pacotes que você está roteando através de sua rede, permitindo funcionalidades que simplesmente não são possíveis em hardware de consumo.

Por exemplo, você pode começar com qualquer um dos cenários acima para implementar uma rede wireless privada na qual os usuários são autenticados utilizando um navegador web padrão. Com o uso de um portal como o Chillispot, usuários wireless podem ser autenticados a partir de uma base de dados existente (como um domínio Windows acessível através do RADIUS, por exemplo). Este arranjo poderia permitir acesso preferencial aos usuários que estão na base, ao mesmo tempo em que permite acesso bastante limitado ao público em geral.

Outra aplicação popular é o modelo comercial pré-pago. Neste modelo os usuários adquirem um cartão antes de acessarem a rede. O cartão contém uma senha que permitirá o acesso por um período limitado de tempo. Quando este tempo expirar, o usuário deve adquirir outro cartão. Este sistema de cobrança está disponível apenas em equipamentos de rede comerciais, relativamente caros, mas pode ser implementado a partir de softwares livres como o ***Chillispot*** e o ***phpMyPrePaid***. Veremos mais sobre tecnologias de portais cativos e sistemas de cobrança (bilhetagem) na seção **Autenticação** do **Capítulo 6**.

Sistemas operacionais wireless-friendly

Há uma variedade de sistemas operacionais de código aberto que fornecem ferramentas úteis para o trabalho com redes sem fio. Estes são projetados para o uso com PCs reutilizados ou outros dispositivos de rede (ao invés de um laptop ou servidor) e são refinados para a construção de redes sem fio. Alguns destes projetos incluem:

- **Freifunk**. Baseado no projeto OpenWRT (*http://openwrt.org/*), o firmware Freifunk fornece o fácil suporte ao OLSR para access points de consumo baseados em MIPS, como os Linksys WRT54G / WRT54GS / WAP54G, Siemens SE505, e outros. Através da simples instalação do firmware Freifunk em um destes APs você pode construir rapidamente um mesh OLSR que se forma automaticamente com os demais que tenham o mesmo firmware instalado. O Freifunk não está disponível para a arquitetura x86. Ele é mantido por Sven Ola do grupo "Freifunk wireless em Berlin". Você pode fazer o download do firmware em *http://www.freifunk.net/wiki/FreifunkFirmware*

- **Pyramid Linux**. Pyramid é uma distribuição Linux para o uso em plataformas embarcadas que evoluiu da venerável plataforma Pebble Linux. Ela suporta diversos cartões wireless e tem uma interface web simples para a configuração das interfaces de rede, encaminhamento de portas, WifiDog e OLSR. A Pyramid é distribuída e mantida pela Metrix Communication LLC e está disponível em *http://pyramid.metrix.net/*.

- **m0n0wall**. Baseado em FreeBSD, o m0n0wall é um pacote para firewall bastante pequeno, mas completo, que provê serviços de access point. Ele é configurado a partir de uma interface web e toda a configuração do sistema é armazenada em um único arquivo XML. Seu minúsculo tamanho (menos de 6MB) torna-o atrativo para o uso em sistemas embarcados muito pequenos. Seu objetivo é prover um firewall seguro, que não inclui ferramentas no espaço de usuário (não é sequer possível

fazer o login remoto). Apesar desta limitação, ele é uma escolha popular em redes sem fio, especialmente para aqueles que conhecem bem o FreeBSD. Você pode fazer o download do m0n0wall de *http://www.m0n0.ch/*.

Todas estas distribuições são projetadas para o uso em máquinas com memória limitada. Se você está usando um disco flash ou um HD de bom tamanho, você poderá instalar um sistema operacional mais completo (como o Ubuntu ou o Debian) e usar a máquina como um roteador ou access point. Possivelmente isto tomará mais tempo para que você certifique-se de que todas as ferramentas necessárias estão instaladas sem que pacotes desnecessários estejam presentes. O uso de um dos projetos acima como um ponto de partida na construção de seu nó wireless irá proporcionar a considerável economia de tempo e esforço.

O Linksys WRT54G

Um dos mais populares access points de consumo atualmente no mercado é o Linksys WRT54G. Este access point apresenta duas conexões para antenas externas RP-TNC, um switch Ethernet de quatro portas e um rádio 802.11b/g. Ele é configurado através de uma simples interface web. Mesmo não sendo projetado para o uso externo, ele pode ser instalado em uma caixa ou tubo plástico de custo relativamente baixo. No momento da escrita deste livro, o WRT54G custava cerca de 60 dólares (no Brasil, o preço é de aproximadamente R$ 160,00).

Em 2003, hackers de rede descobriram que o firmware embarcado no WRT54G era, de fato, uma versão do Linux. Isto criou um tremendo interesse na construção de um firmware customizado que estendesse significativamente as capacidades do roteador. Algumas destas novas capacidades incluem o suporte ao modo cliente, portais cativos[1] e rede mesh. Algumas alternativas populares para o WRT54G são o DD-Wrt (*http://www.dd-wrt.com/*), OpenWRT (*http://openwrt.org/*), Tomato (*http://www.polarcloud.com/tomato*) e Freifunk (*http://www.freifunk.net/*).

Infelizmente, no outono de 2005, a Linksys lançou a versão 5 do WRT54G. Esta versão de hardware eliminou alguma memória RAM e flash na placa mãe, tornando muito difícil a execução do Linux (ele vem com o VxWorks, um sistema operacional menor que não permite a fácil customização). A Linksys também lançou o WRT54GL, que é essencialmente a versão 4 do WRT54G (que roda Linux) por um preço maior.

Outros access points da Linksys também rodam Linux, incluindo o WRT54GS e o WAP54G. Mesmo que eles também tenham um preço relativamente baixo, as especificações do hardware podem mudar a qualquer momento. É difícil saber qual a versão do hardware que está sendo usada sem

---

1. N. do T. - Portais cativos são aqueles por onde são obrigados a passar os usuários de uma rede, tipicamente em sua primeira conexão e em todas as vezes em que uma nova autenticação é necessária. São muito usados em redes que fornecem acesso público. O usuário, ao conectar-se na rede, apenas consegue acessar ao portal cativo, onde terá instruções de acesso e um formulário para o login. Veja mais sobre este assunto na sessão **Portais cativos** do **Capítulo 6**.

abrir a caixa, o que torna arriscada a compra em uma loja e praticamente impossível a encomenda online. Enquanto o WRT54GL é garantido para usar o Linux, a Linksys tornou público que não espera vender este modelo em larga escala, e é incerta a sua continuidade no mercado.

Felizmente, os hackers de rede já conseguiram instalar firmware customizado nas versões 5 e 6, notoriamente difíceis, do WRT54G, assim como nas versões mais recentes (7 e 8). Para informações detalhadas de como instalar este firmware visite *http://www.scorpiontek.org/portal/content/view/27/36/*

Para mais informações sobre o estado atual dos hacks para o roteador wireless Linksys, veja *http://linksysinfo.org/*

6
Segurança e monitoramento

Em uma rede cabeada tradicional, o controle de acesso é bastante direto: se uma pessoa tem acesso físico a um computador ou a um hub de rede, ela pode usar (ou abusar) dos recursos da rede. Enquanto mecanismos de software sejam componentes importantes para a segurança da rede, o limite ao acesso físico à rede é o controle de acesso primordial. De forma simples, se todos os terminais e componentes de rede estiverem apenas ao acesso de indivíduos confiáveis, então a rede pode ser considerada segura.

As regras mudam significativamente em redes sem fio. Embora o alcance aparente de seu access point seja de umas poucas centenas de metros, um usuário com uma antena de alto ganho pode utilizar a rede, mesmo à distância de alguns quarteirões. Caso um usuário não autorizado seja detectado, é impossível "seguir o cabo" até a localidade deste usuário. Sem transmitir um único sinal, um usuário malicioso pode copiar todo o tráfego da rede para um disco. Estes dados podem, mais tarde, ser usados em um ataque mais sofisticado à rede. Nunca assuma que as ondas de rádio simplesmente "param" nos limites de sua propriedade.

Normalmente, não é razoável confiar cegamente em todos os usuários da rede, mesmo em redes cabeadas. Empregados insatisfeitos, usuários de rede mal educados ou simples erros da parte de usuários honestos podem ferir as operações de rede. Como arquiteto de rede, seu objetivo é facilitar a comunicação privada entre usuários legítimos da mesma. Mesmo que uma certa quantidade de controle de acesso e autenticação sejam necessários, você terá falhado em seu trabalho se os usuários tiverem dificuldades no uso da rede para a sua comunicação.

Há um velho ditado que diz que a única maneira de tornar um computador completamente seguro é desligá-lo, colocá-lo em um cofre, destruir a chave do cofre e enterrar tudo isto em concreto. Mesmo que um sistema destes seja completamente "seguro", ele é inútil para a comunicação. Quando você tomar decisões sobre a segurança de sua rede lembre-se que, acima de tudo, ela existe para que os usuários possam se comunicar uns com os outros.

Considerações de segurança são importantes, mas não devem se interpor no caminho dos usuários da rede.

Segurança física

Ao instalar sua rede, você constrói uma infra-estrutura da qual as pessoas passam a depender. Medidas de segurança existem para garantir que a rede é confiável. Na maioria das instalações, indisponibilidades acontecem com freqüência devido à ação humana, acidental ou não. As redes possuem componentes físicos, como fios e computadores, que são facilmente prejudicados. Em muitas instalações, as pessoas não entendem o propósito dos componentes instalados ou a curiosidade pode levá-los à experimentação. Eles podem não entender a importância de um cabo conectado a uma porta. Alguém pode desconectar um cabo de rede para usá-lo em seu laptop por cinco minutos, ou mover um switch porque ele está atrapalhando o caminho. Uma tomada pode ser retirada de uma extensão porque alguém precisa ligar alguma outra coisa. Garantir a segurança física da rede é prioridade. Sinais e etiquetas são apenas úteis para aqueles que conheçam o idioma. Colocar as coisas fora do caminho e limitar o acesso físico é o melhor meio para garantir que acidentes e o uso inadequado não irão ocorrer.

Em economias menos desenvolvidas, dispositivos físicos para a proteção apropriada podem não ser facilmente encontrados. Você pode encontrar material elétrico que poderá suprir esta necessidade. Caixas de proteção personalizadas também são de fácil manufatura e devem ser consideradas essenciais em qualquer instalação. Freqüentemente, é possível economizar contratando-se um marceneiro para fazer todos os furos e instalar passagens (conduítes) para os cabos. Enquanto esta é uma opção cara no mundo desenvolvido, o custo de mão-de-obra para atividades pesadas pode ser razoável nos países do Sul. Tubos de PVC podem ser previamente embutidos, em paredes de cimento ou gesso, para a passagem de cabos entre as salas. Isto evita a necessidade de se fazer novos furos a cada vez em que um cabo deve ser passado de um lado a outro. Sacos plásticos podem ser colocados nos conduítes, ao redor dos cabos, para isolamento.

Equipamentos pequenos devem ser montados nas paredes e equipamentos maiores devem ser colocados em um armário ou gabinete.

Switches

Switches, hubs ou access points internos podem ser montados diretamente em uma parede, próximos a tomadas elétricas. O melhor é colocar estes equipamentos o mais alto possível, evitando que alguém toque os dispositivos ou seus cabos.

Cabos

No mínimo, cabos devem ser escondidos e amarrados. É possível encontrar conduítes plásticos para cabos que podem ser usados em construções. Se você não conseguir encontrá-los, simples amarras para cabos podem ser parafusadas

à parede para manter os cabos presos. Isto irá garantir que o cabo não ficará pendurado onde ele possa ser pisado, torcido, perfurado ou cortado.

É preferível enterrar cabos do que deixá-los soltos ao longo de um terreno. Cabos pendurados podem ser usados para secar roupas, ou podem ser danificados por uma escada, etc. Para evitar vermes e insetos, use um conduíte plástico. A pequena despesa extra irá compensar os problemas. O conduíte deve ser enterrado a 30 cm de profundidade, ou abaixo do nível de congelamento em locais frios. Vale a pena investir a mais em um conduíte que seja maior do que o necessário, assim futuros cabos podem passar pelo mesmo tubo. Etiquete e sinalize o caminho do cabo com mensagens "ligue para o número (...) antes de cavar" para evitar acidentes futuros.

Energia elétrica

A melhor opção é ter as tomadas de energia dentro de um gabinete que possa ser trancado. Se isto não for possível, monte a barra de tomadas debaixo de uma mesa, ou em uma parede, utilizando fita isolante de boa qualidade para prender as flechas (*plugs*) às tomadas. Na barra de alimentação e nos no-breaks não deixe nenhuma tomada vazia. Isole-as com fita isolante se for necessário. As pessoas têm a tendência de sempre usar as tomadas que estão facilmente a seu alcance, então torne difícil o acesso às tomadas destinadas aos equipamentos de rede. Se você não fizer isto, poderá encontrar um ventilador ou abajur ligados a seu no-break. Ainda que seja bom ter iluminação, melhor ainda é manter o servidor rodando.

Água

Proteja seu equipamento contra água e umidade. Em todos os casos, certifique-se de que seu equipamento, incluindo os no-breaks, estejam ao menos em uma altura de 30 cm do chão, para evitar danos por alagamento. Sempre tente ter um telhado sobre o seu equipamento, de forma que água e umidade não caiam sobre ele. Em climas úmidos, é importante que o equipamento tenha a ventilação apropriada, assegurando a exaustão da umidade. Pequenos armários e caixas fechadas precisam de ventilação, caso contrário a umidade e o calor irão degradar ou destruir seus equipamentos.

Mastros e suportes

Equipamentos instalados em mastros estão, na maioria das vezes, à salvo de ladrões. Mesmo assim, para evitar roubos e proteger seu equipamento do vento é bom caprichar na montagem. Pintar o equipamento de branco ou tons de cinza fará com que ele reflita a luz do sol e pareça desinteressante. Painéis de antenas são freqüentemente preferidos porque são mais sutis e desinteressantes que pratos parabólicos. Qualquer instalação em paredes deve ser alta o suficiente, de forma a requerer uma escada para seu acesso. Tente escolher locais bem iluminados, mas não muito proeminentes, para colocar os equipamentos. Evite também antenas que se pareçam com antenas de televisão, uma vez que estas atraem o interesse de ladrões, enquanto uma antena Wi-Fi é de pouca utilidade para um ladrão médio.

Ameaças à rede

Uma diferença crítica entre redes Ethernet e wireless é que as redes wireless são construídas em um ***meio compartilhado***. Elas têm mais semelhança com os antigos hubs de rede que com os switches modernos, no sentido de que qualquer computador conectado à rede pode "ver" o tráfego de dados de outros usuários. Para monitorar todo o tráfego de rede em um access point, basta selecionar o canal utilizado, colocar o cartão de rede em modo monitor e registrar cada quadro de dados. Esta informação pode ser valiosa para um espião (incluindo dados como email, registros digitais de voz e logs de conversas em chats). Ela também pode fornecer outros dados sensíveis, como senhas, que podem comprometer ainda mais a segurança da rede. Como veremos adiante neste capítulo, este problema pode ser minimizado com o uso de criptografia.

Outro problema sério com redes sem fio é que os usuários são relativamente ***anônimos***. Mesmo sendo verdade que cada dispositivo wireless inclua um único endereço MAC fornecido pelo seu fabricante, este endereço pode ser, freqüentemente, modificado por software. Mesmo que o endereço MAC seja conhecido, pode ser muito difícil definir onde o usuário wireless está, fisicamente. Efeitos multipath (multicaminhos), antenas de alto ganho e amplas variações nas características de transmissores tornam impossível determinar se um usuário malicioso está na sala ao lado ou em um prédio de apartamentos a dois quilômetros de distância.

O espectro livre permite uma grande economia para o usuário, mas tem o ruim efeito colateral de tornar os ataques de negação de serviço (***denial of service – DoS***) trivialmente simples. Uma pessoa mal-intencionada pode causar problemas significativos na rede simplesmente ligando um access point de alta potência, um telefone sem fio, um transmissor de vídeo ou outro dispositivo que opere na freqüência de 2,4 GHz. Muitos dispositivos de rede estão sujeitos a outras formas de ataque de negação de serviços, como "disassociation flooding" (tipo de ataque que destrói a conexão entre os clientes e o access point) e sobrecarga de tabelas ARP.

Aqui estão várias categorias de indivíduos que podem causar problemas em uma rede sem fio:

- ***Usuários incautos***. Na medida em que mais redes sem fio são instaladas em áreas densamente populadas, é comum que usuários de laptops conectem-se, acidentalmente, a redes erradas. Muitos clientes wireless simplesmente escolhem qualquer rede sem fio disponível quando a sua rede padrão está indisponível. O usuário pode fazer uso desta rede normalmente, desconhecendo totalmente o fato de que pode estar transmitindo dados sensíveis através da rede de outras pessoas. Pessoas maliciosas podem até tomar proveito disto, criando access points em locais estratégicos, tentando atrair usuários incautos e capturar seus dados.

  O primeiro passo para evitar este problema é educar os usuários, ressaltando a importância da conexão apenas em redes conhecidas e confiáveis. Muitos clientes wireless podem ser configurados para que se

conectem apenas em redes confiáveis, ou para que permitam explicitamente a conexão antes do acesso a uma nova rede. Como veremos mais tarde neste capítulo, usuários podem conectar-se com segurança em redes públicas através do uso de criptografia forte.

- ***War drivers***. O fenômeno "*war driving*" ganhou seu nome do popular filme hacker de 1983 "*War Games*"[1]. *War drivers* estão interessados na localização física de redes wireless. Eles costumam dirigir com um laptop, GPS e uma antena omnidirecional, registrando o nome e a localização das redes que encontram. Estes registros são combinados com outros, feitos por outros *war drivers*, e transformam-se em mapas mostrando a planta de redes wireless de uma determinada cidade.

  A vasta maioria dos *war drivers* não oferece ameaça direta às redes, mas os dados coletados por eles podem ser de interesse de um *cracker* de rede (pessoa interessada em causar danos ou roubar informações). Por exemplo, pode-se verificar que um access point desprotegido está localizado em um local com informações sensíveis, como um prédio de governo ou o escritório de uma empresa. Uma pessoa maliciosa poderia usar esta informação para conseguir um acesso ilegal à rede neste ponto. Obviamente, este ponto de acesso jamais deveria ter sido configurado assim, mas o *war driving* torna este problema ainda mais evidente, requerendo uma solução urgente. Como veremos adiante neste capítulo, *war drivers* que utilizam o programa NetStumbler podem ser detectados com programas como o Kismet. Para mais informações sobre *war driving*, visite os sites *http://www.nodedb.com/*, *http://www.wifimaps.com/*, ou *http://www.netstumbler.com/*

- ***Pontos de acesso desonestos***. Há duas classes genéricas de pontos de acesso desonestos: aqueles incorretamente instalados por usuários legítimos e aqueles instalados por pessoas mal-intencionadas que pretendem coletar dados ou causar danos à rede. No caso mais simples, um usuário legítimo da rede pode querer uma melhor cobertura de rede para o escritório, ou achar que as restrições de segurança da rede da empresa são difíceis de serem seguidas. Com a instalação de um access point barato, sem permissão da empresa, o usuário abre toda a rede interna para um potencial ataque. Mesmo que seja possível buscar por access points não autorizados em sua rede cabeada, o estabelecimento de uma política clara que os proíba é extremamente importante.

  A segunda classe de pontos de acesso desonestos pode ser muito difícil de se lidar. Com a instalação de um ponto de acesso de alta potência que utilize o mesmo ESSID de uma rede existente, uma pessoa mal-intencionada pode enganar os usuários, fazendo com que use seu equipamento e, com isso registrar ou mesmo manipular os

---

1 N. do T. - No Brasil, o filme foi exibido com o nome "Jogos de Guerra". Não há um termo ou tradução que tenha sido empregada, ao menos no conhecimento do tradutor, em substituição à *war driving*.

dados que passam por ele. Novamente, se os usuários estão treinados no uso de criptografia forte, este problema é significativamente reduzido.

- ***Espiões*** (***eavesdroppers***). Como anteriormente mencionado, a espionagem é um problema muito difícil de se lidar em redes wireless. Com o uso de uma ferramenta passiva de monitoramento (como o Kismet), um espião pode registrar todos os dados de uma rede a partir de uma grande distância, sem que sua presença seja notada. Dados com criptografia fraca podem ser armazenados para serem decodificados mais tarde, enquanto dados sem criptografia podem ser facilmente lidos em tempo real.

Se você tiver dificuldades de convencer outros deste problema, você pode fazer a demonstração de ferramentas como Etherpeg (*http://www.etherpeg.org/*) ou Driftnet (*http://www.ex-parrot.com/~chris/driftnet/*). Estas ferramentas monitoram a rede à procura de gráficos, como arquivos GIF e JPEG. Enquanto os usuários estão navegando na Internet, estas ferramentas simplesmente mostram todas as imagens encontradas em uma montagem. Quando ministro aulas sobre segurança de redes, eu freqüentemente uso estas ferramentas como uma demonstração. Ainda que você explique a um usuário que seu email é vulnerável sem criptografia, nada funciona melhor do que mostrar as imagens que eles estão olhando em seu navegador.

Mais uma vez, mesmo que a espionagem não possa ser totalmente evitada, a devida aplicação de criptografia forte irá desencorajá-la.

Esta introdução pretende apenas dar-lhe uma idéia dos problemas que você enfrenta ao projetar uma rede sem fios. Mais tarde, neste capítulo, vamos discutir ferramentas e técnicas que o ajudarão a minimizar estes problemas.

Autenticação

Antes que lhes seja concedido o acesso aos recursos de rede, os usuários devem ser, primeiramente, ***autenticados***. Em um mundo ideal, cada usuário de uma rede sem fio deveria ter uma identificação única, pessoal e intransferível, de forma que um usuário jamais pudesse passar-se por outro. Isto constitui um problema que é muito difícil de solucionar no mundo real.

O que você tem mais perto deste identificador único é o endereço MAC. Ele é o número de 48 bits atribuído pelo fabricante para cada dispositivo Ethernet e wireless. Através do emprego de ***filtragem MAC*** em nossos access points, podemos autenticar usuários com base em seus endereços MAC. Através desta funcionalidade, o access point mantém uma tabela interna dos endereços MAC aprovados. Quando um usuário wireless tenta conectar-se ao access point, seu endereço MAC deve estar cadastrado na tabela, ou sua conexão será negada. Alternativamente, o AP pode manter uma lista de endereços MAC já identificados como “maus”, permitindo o acesso de todos os outros que não estão nesta lista.

Infelizmente, este não é um mecanismo ideal de segurança. A manutenção de tabelas MAC em cada dispositivo pode ser trabalhosa, requerendo que todos os dispositivos clientes tenham seu endereço MAC registrado e carregado para

o AP. Pior ainda, endereços MAC podem ser modificados por software. Observando os endereços MAC em uso em uma rede sem fios, um atacante insistente pode passar-se por um endereço MAC aprovado, conectando-se com sucesso ao AP (esta técnica é chamada de ***spoofing***). A filtragem MAC irá prevenir o acesso à rede de usuários não intencionais e curiosos, mas usada individualmente, ela não irá prevenir atacantes especializados.

Filtros MAC são úteis para limitar temporariamente o acesso de clientes "mal-comportados". Por exemplo, um laptop infectado por vírus que envie uma grande quantidade de emails indesejados, ou outro tipo qualquer de tráfego, pode ter seu endereço MAC adicionado à tabela de filtragem, impedindo imediatamente todo o tráfego gerado por ele. Isto pode nos dar tempo para identificar o usuário e solucionar o problema.

Outra funcionalidade popular de autenticação em redes wireless é a chamada ***rede fechada*** (***closed network***). Em uma rede típica, os APs irão publicar seu ESSID muitas vezes por segundo, permitindo a clientes wireless (e a ferramentas como o NetStumbler) encontrar a rede e mostrar sua presença ao usuário. Em uma rede fechada, o AP não publica seu ESSID, fazendo com que os usuários sejam obrigados a conhecer o nome completo da rede antes que o AP permita a conexão. Isto previne que usuários casuais descubram o nome da rede e a selecionem para o uso em seu cliente wireless.

Há uma série de contrapontos para esta funcionalidade. Forçar os usuários a digitar o ESSID completo antes da conexão pode induzir a erros e freqüentemente gera chamadas e reclamações para a equipe de suporte. Como a rede não está obviamente presente em ferramentas de pesquisas de localidades de acesso wireless, como o NetStumbler, isto pode evitar que sua rede apareça em mapas de *war driving*. Mas isto também significa que outros construtores de rede não terão como conhecer a sua rede e, especialmente, não saberão qual o canal que você pode estar ocupando. Um projetista consciente de uma rede vizinha irá fazer uma pesquisa da localidade, verificar quais as redes próximas e, ao desconhecer a sua, irá instalar uma nova rede no mesmo canal que você está utilizando. Isto causará problemas de interferência tanto para a sua rede como à nova que está sendo instalada.

Finalmente, o uso de redes fechadas adiciona muito pouco, de forma geral, para a segurança de sua rede. Com o uso de ferramentas passivas de monitoramento (como o Kismet), um usuário hábil pode detectar informações enviadas de seus clientes legítimos para o AP. Estas informações contêm, necessariamente, o nome da rede. Um usuário malicioso poderá, então, usar este nome para conectar-se ao access point, como qualquer usuário normal faria.

A criptografia é provavelmente a melhor ferramenta que temos para a autenticação de usuários wireless. Com criptografia forte, podemos identificar individualmente um usuário em uma maneira que será muito difícil de ser descoberta, usando esta identificação para determinar o tipo de acesso à rede que será permitido. A criptografia também tem o benefício da adição de uma camada de privacidade, impedindo que espiões observem facilmente o tráfego de rede.

O método mais usado de criptografia em redes sem fio é o ***WEP***. WEP significa ***wired equivalent privacy*** (privacidade equivalente a redes cabeadas), e é suportado por por praticamente todos os equipamentos 802.11a/b/g. WEP usa uma chave compartilhada de 40 bits para criptografar os dados entre o

access point e o cliente. A chave deve ser configurada tanto no AP como em cada um dos clientes. Com o WEP habilitado, os clientes não podem acessar o AP até que usem a chave correta. Um espião observando uma rede utilizando WEP ainda poderá ver o tráfego e os endereços MAC, mas os dados em cada pacote estarão criptografados. Isto fornece um mecanismo de autenticação razoavelmente bom, além de adicionar um pouco de privacidade à rede.

WEP não é, definitivamente, a melhor solução de criptografia disponível. Uma boa razão para isto é que a chave WEP é compartilhada entre todos os usuários. Caso a chave seja comprometida (digamos que um usuário a entregue a um amigo, ou um funcionário é demitido) sua troca poderá ser quase impraticável, uma vez que todos os APs e dispositivos clientes necessitam de reconfiguração. Cada usuário da rede ainda poderá espionar o tráfego de outros, uma vez que todos compartilham a mesma chave.

A chave é, com freqüência, escolhida de maneira pobre, fazendo com que tentativas de quebra da mesma possam ser feitas. Pior do que tudo isso, a implementação do próprio WEP tem problemas em muitos pontos de acesso, tornando ainda mais fácil a invasão de algumas redes. Mesmo que os fabricantes tenham implementado uma série de extensões para o WEP (como chaves maiores e esquemas rápidos de rotação de chaves), estas extensões não são parte do padrão e geralmente não irão interoperar com equipamentos de outros fabricantes. A atualização para o firmware mais recente em todos os seus equipamentos wireless pode prevenir contra alguns dos ataques mais antigos e conhecidos para o WEP.

O WEP ainda pode ser uma ferramenta útil de autenticação. Assumindo que todos os seus usuários são de confiança e não passarão adiante a chave de acesso, você pode estar razoavelmente certo de que seus clientes wireless são legítimos. Mesmo que a quebra do WEP seja possível, ela está além das habilidades da maioria dos usuários. O WEP é bastante útil na segurança de links ponto-a-ponto de longa distância, mesmo em redes geralmente abertas. Com o uso do WEP em um link deste tipo, você desencoraja que outros conectem-se a ele, fazendo com que procurem outros APs disponíveis. Pense no WEP como uma placa de "Mantenha Distância" para a sua rede. Qualquer um que detecte sua rede, verá que uma chave de acesso é necessária, ficando claro que nem todos são bem-vindos à entrar nela.

A maior força do WEP é sua interoperabilidade. A fim de seguir os padrões 802.11, todos os dispositivos wireless fornecem suporte WEP básico. Mesmo não sendo o mais robusto disponível, ele é certamente o método de criptografia mais largamente utilizado. Veremos outras técnicas de criptografia avançada mais adiante neste capítulo.

Para mais detalhes sobre o estado atual da criptografia WEP, veja estes artigos:

- *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*

Outro protocolo de autenticação na camada de link de dados é o ***Wi-Fi Protected Access*** (Acesso Protegido Wi-Fi), ou ***WPA***. O WPA foi criado para lidar especificamente com os problemas do WEP descritos anteriormente. Ele

provê um esquema de criptografia significativamente mais forte e pode usar uma chave privada compartilhada, chaves únicas designadas para cada usuário ou mesmo certificados SSL para autenticar tanto o cliente como o access point. As credenciais de autenticação são verificadas com o uso do protocolo 802.1X, que consulta uma terceira base de dados, como o RADIUS. Através do uso de um protocolo de integridade temporal de chave (***Temporal Key Integrity Protocol – TKIP***), as mesmas podem ser rotacionadas rapidamente com o passar do tempo, reduzindo a possibilidade de uma sessão ser quebrada. De forma geral, o WPA fornece uma autenticação e privacidade bem melhores que o padrão WEP.

O WPA requer access points com hardware relativamente recente e o firmware atualizado em todos os clientes wireless, assim como uma boa dose de configuração. Se você está instalando a rede em um ambiente onde tem o total controle da plataforma de hardware, o WPA pode ser o ideal. Com a autenticação de todos os clientes e APs, o problema dos access points desonestos está resolvido, além de outras vantagens sobre o WEP. Mas em ambientes de rede onde ainda existem equipamentos antigos e o conhecimento dos equipamentos utilizados pelos usuários é limitado, a instalação do WPA pode ser um pesadelo. É por esta razão que a maioria dos ambientes continua utilizando WEP, quando alguma forma de criptografia é utilizada.

Portais cativos

Uma forma comum de autenticação em redes wireless é o uso de ***portais cativos***. Um portal cativo usa um navegador web padrão para fornecer ao usuário uma maneira de apresentar suas credenciais de login. Ele também pode ser usado para apresentar informações ao usuário (como uma Política de Uso) antes de permitir a continuidade do acesso. O uso de um navegador web, ao invés de um programa específico para a autenticação, permite que o portal cativo funcione com praticamente todos os laptops e sistemas operacionais. Portais cativos são tipicamente utilizados em redes abertas que não tenham outros métodos de autenticação (como WEP ou filtros MAC).

Para começar, um usuário wireless seleciona a rede em seu laptop. O computador irá solicitar e receber um endereço DHCP. O usuário, então, abre seu navegador para acessar algum site na Internet.

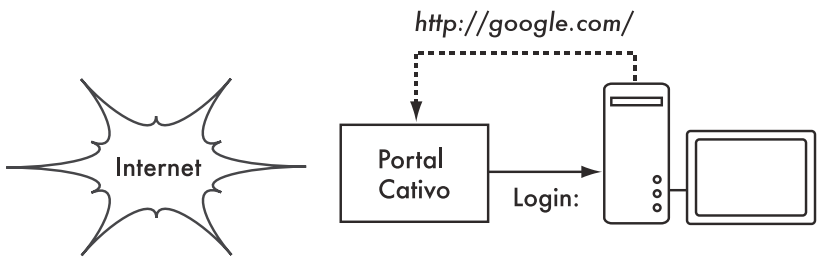


Figura 6.1: O usuário solicita uma página web e é redirecionado.

Ao invés de receber a página solicitada, o usuário é apresentado a uma tela de login. Esta página solicita que o usuário digite seu nome de acesso e senha,

simplesmente clique em um botão de “login” após ler a política de uso, digite os números de um cartão pré-pago ou forneça qualquer outra credencial requerida pelo administrador de rede. Tais credenciais são verificadas pelo access point ou outro servidor da rede. Qualquer outro tipo de acesso à rede é bloqueado até que as credenciais sejam verificadas.

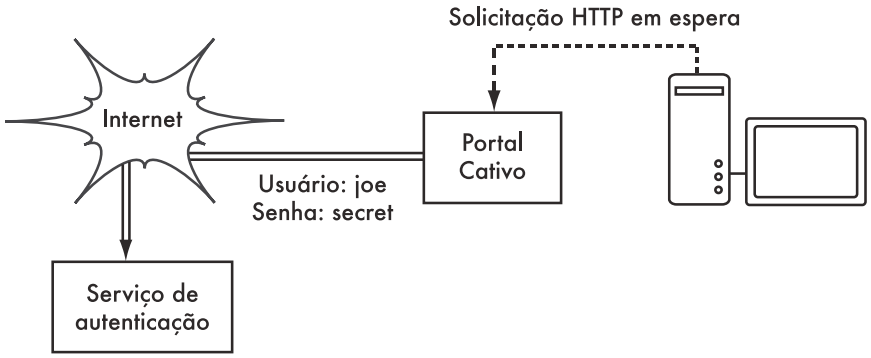


Figura 6.2: As credenciais do usuário são verificadas antes que o acesso posterior à rede seja permitido. O servidor de autenticação pode ser o próprio access point, outra máquina da rede local ou um servidor em qualquer lugar, via Internet.

Uma vez autenticado, o usuário tem acesso aos recursos da rede e é, normalmente, direcionado ao site originalmente solicitado.

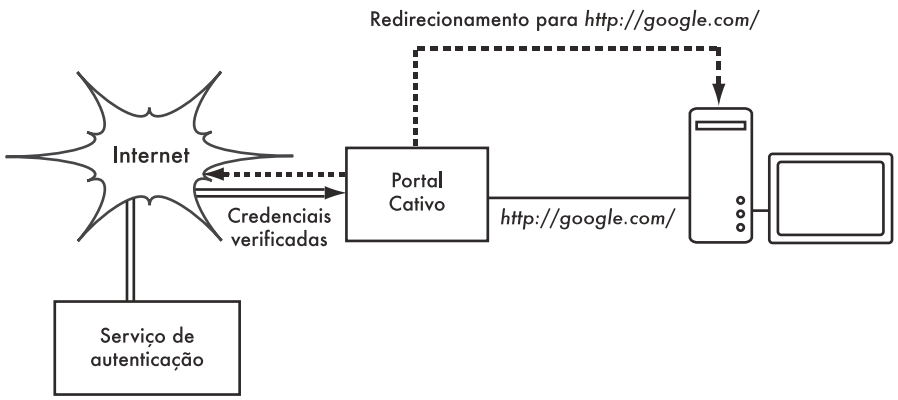


Figura 6.3: Após a autenticação, o usuário pode acessar o resto da rede.

Os portais cativos não fornecem criptografia ao usuário wireless, apenas confiando no endereço MAC e IP do cliente como identificadores únicos. Uma vez que isto não é, necessariamente, muito seguro, muitas implementações irão requerer novas autenticações periódicas. Freqüentemente, isto é feito, de forma automática, em uma pequena janela de popup que é minimizada assim que o usuário é autenticado pela primeira vez.

Já que não fornecem criptografia forte, os portais cativos não são uma boa escolha para redes que precisam ser travadas de forma a permitir acesso

apenas a usuários confiáveis. Eles prestam-se mais a cafés, hotéis e outros locais de acesso público, onde usuários casuais de rede são esperados.

Na configuração de uma rede pública, ou semi-pública, técnicas de criptografia como WEP e WPA são, efetivamente, inúteis. Simplesmente, não há uma maneira de distribuir chaves públicas ou compartilhadas para um grande número de pessoas sem comprometer a segurança de tais chaves. Nestas configurações, uma simples aplicação, como um portal cativo, fornece um nível de serviço que fica entre algo completamente aberto ou completamente fechado.

Projetos populares de hotspots

- **Chillispot** (*http://www.chillispot.info/*). O Chillispot é um portal cativo designado à autenticação de usuários a partir de uma base de dados de credenciais, como o RADIUS. Combinado a uma aplicação como a phpMyPrePaid, a autenticação baseada em cartões pré-pagos pode ser implementada facilmente. Você pode baixar o phpMyPrePaid de http://sourceforge.net/projects/phpmyprepaid/.
- **WiFi Dog** (*http://www.wifidog.org/*). O WiFi Dog fornece um pacote completo de portal cativo e autenticação que ocupa muito pouco espaço (tipicamente, abaixo de 30kb). Da perspectiva do usuário, ele não requer nenhum popup ou suporte a javascript, o que permite que seja usado em uma grande variedade de dispositivos wireless.
- **m0n0wall** (*http://m0n0.ch/wall/*). O m0n0wall é um sistema operacional completo, embarcado, baseado no FreeBSD. Ele inclui um portal cativo com suporte a RADIUS, assim como um servidor web PHP.
- **NoCatSplash** (*http://nocat.net/downloas/NoCatSplash/)* O NoCatSplash fornece uma página de apresentação (splash page) personalizada para seus usuários, requerendo que eles cliquem em um botão de "login" antes de acessarem a rede. Isto é útil para fornecer a identificação e os contatos das pessoas de suporte à rede e exibir regras para o seu acesso. Ele consiste em uma solução muito simples em situações onde você necessita prover informações e enfatizar a política de uso para usuários de uma rede aberta.

Privacidade

A maioria dos usuários está inocentemente ignorante do fato que seu email privado, conversas em salas de bate-papo e mesmo senhas, com freqüência, circulam abertamente por dezenas de redes desconhecidas antes de chegarem a seu destino final na Internet. Independente do quão enganados possam estar, os usuários ainda têm alguma expectativa de privacidade quando usam computadores em rede.

A privacidade pode ser conseguida mesmo em redes não confiáveis, como em pontos de acesso público à Internet. O único método comprovado para a proteção da privacidade é o uso de criptografia forte fim-a-fim (***end-to-end encryption***).

Técnicas de criptografia como WEP e WPA tentam endereçar questões de privacidade no nível dois, a camada de comunicação de dados. Isto realmente protege contra espiões observando uma conexão sem fio, mas tal proteção acaba no ponto de acesso. Caso o cliente wireless use protocolos inseguros (como o POP ou SMTP para o envio e recebimento de email), então os usuários que estejam na rede do access point podem ainda registrar sessões e ter acesso a dados sensíveis. Como mencionado anteriormente, os usuários WEP também sofrem com o fato de compartilharem uma chave privada. Isto significa que usuários legítimos podem espionar uns aos outros, uma vez que todos conhecem a chave privada.

Com o uso de criptografia até o ponto final da conexão remota, os usuários podem, de forma elegante, contornar inteiramente o problema. Estas técnicas funcionam bem mesmo em redes públicas não confiáveis, onde espiões estão observando e possivelmente manipulando dados vindos do access point.

Para assegurar a privacidade dos dados, uma boa criptografia fim-a-fim deve fornecer as seguintes funcionalidades:

- ***Verificação de autenticidade da extremidade remota***. O usuário deve ser capaz de saber, sem dúvida alguma, que a extremidade remota é aquela que diz ser. Sem esta autenticação, um usuário pode entregar dados sensíveis a qualquer um que se passe por um receptor ou serviço legítimo.
- ***Métodos de criptografia forte***. O algoritmo de criptografia deve ser submetido a escrutínio público e os dados não devem ser facilmente descriptografados por um terceiro. Não há segurança na obscuridade, e a criptografia forte é ainda mais forte quando o algoritmo é amplamente conhecido e está sujeito a revisão. Um bom algoritmo, com uma chave de proteção grande e apropriada, dificilmente será quebrado por qualquer esforço durante nosso tempo de vida, usando a tecnologia atual.
- ***Criptografia de chave pública***. Mesmo não sendo um requerimento absoluto para a criptografia fim-a-fim, o uso de uma chave pública de criptografia, ao invés de uma chave compartilhada, pode garantir que os dados de um indivíduo permaneçam privados, mesmo que a chave de outro usuário do serviço esteja comprometida. Isto também resolve alguns problemas com a distribuição de chaves para usuários em redes não confiáveis.
- ***Encapsulamento de dados***. Um bom mecanismo de criptografia fim-a-fim protege os dados o máximo possível. Isto pode variar da proteção de uma simples transação de email até o encapsulamento de todo o tráfego IP, incluindo buscas ao DNS e outros protocolos de suporte. Algumas ferramentas de criptografia simplesmente fornecem um canal seguro que outras aplicações possam utilizar. Isto permite que os usuários executem qualquer programa que desejem e, ainda assim, fiquem protegidos por uma criptografia forte, mesmo que os próprios programas não ofereçam este suporte.

Esteja ciente de que as leis relativas ao uso de criptografia variam bastante em cada local. Alguns países tratam a criptografia como se fosse munição, e

podem exigir uma permissão formal, a inspeção e guarda de chaves privadas, ou mesmo proibir seu uso. Antes de implementar qualquer solução que envolva criptografia, certifique-se de que o uso desta tecnologia é autorizado em sua localidade.

Nas sessões seguintes, vamos tratar de algumas ferramentas específicas que podem fornecer boa proteção para os dados de seus usuários.

SSL

A tecnologia de criptografia fim-a-fim mais amplamente disponível é a ***Secure Sockets Layer*** (Camada de Conexão Segura), conhecida simplesmente como ***SSL***. Implementada em praticamente todos os navegadores web, a SSL utiliza criptografia de chave pública e uma infra-estrutura confiável de chaves públicas (***public key infrastructure—PKI***) para proteger a comunicação de dados na web. Sempre que você visita um site cujo endereço inicia-se com https (ao invés de http), você está usando SSL.

A implementação SSL em muitos navegadores inclui uma coleção de certificados de fontes confiáveis, chamadas de ***autoridades certificadoras*** (***AC***, ou *CA* para o termo em inglês, *certificate authorities*)[2]. Estes certificados são chaves criptográficas usadas para verificar a autenticidade de websites. Quando você acessa um site que usa SSL, o navegador e o servidor trocam certificados entre si, antes de qualquer coisa. O browser verifica que o certificado fornecido pelo servidor está de acordo com o nome do mesmo no DNS, que o mesmo ainda não expirou e que está assinado por uma autoridade certificadora confiável. O servidor, opcionalmente, verifica a identidade do certificado do navegador. Se os certificados estão aprovados, o navegador e o servidor negociam uma chave principal de sessão (*master session key*) usando os certificados que foram trocados para protegê-la. Esta chave é, por sua vez, usada para criptografar toda a comunicação até que o navegador desconecte-se do site. Este tipo de encapsulamento de dados é conhecido como um ***túnel***.

O uso de certificados com uma PKI não apenas protege a comunicação do acesso de espiões, mas também previne contra os chamados ataques de "homem do meio" (***man-in-the-middle*** – ***MITM***). Em um ataque deste tipo, um usuário malicioso intercepta a comunicação entre o navegador e o servidor. Ao apresentar certificados falsificados tanto para o navegador quanto para o servidor, o usuário malicioso consegue manter estabelecidas duas conexões criptografadas simultaneamente. Conhecendo o segredo de ambas as conexões, o usuário malicioso pode observar e manipular os dados que passam entre o servidor e o navegador.

O uso de uma boa PKI previne este tipo de ataque. Para ter sucesso, o usuário malicioso teria que apresentar um certificado ao cliente, assinado por uma autoridade certificadora confiável. A não ser que a AC tenha sido comprometida (uma possibilidade muito remota) ou o usuário seja enganado de forma a aceitar um certificado forjado, o ataque não será possível. Por isto, é vital que os usuários entendam que ignorar avisos de certificados impróprios ou

---

2. N. do T. - Para saber mais sobre Autoridades Certificadoras e a Infra-estrutura de chaves públicas no Brasil, visite o site *https://www.icpbrasil.gov.br/*

expirados é muito perigoso, especialmente quando usam redes sem fio. Ao clicar o botão "ignorar" quando avisado pelo navegador, os usuários ficam abertos a muitos ataques potenciais.

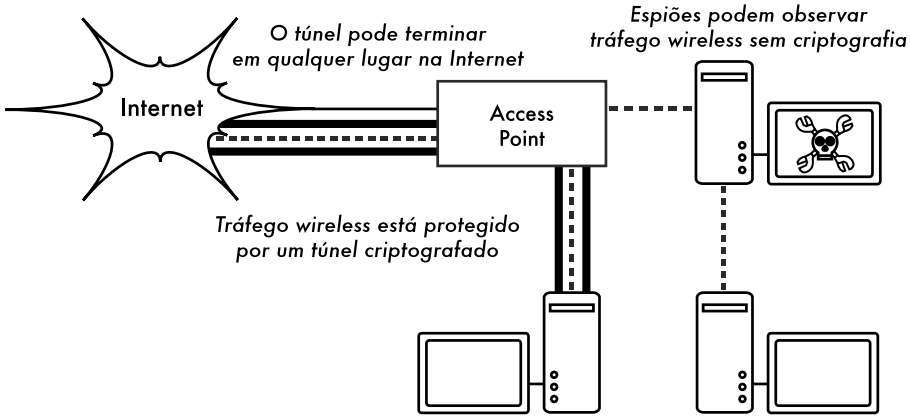


Figure 6.4: Espiões terão que quebrar a criptografia forte para conseguir monitorar o tráfego em um túnel criptografado. A conversação dentro de um túnel é idêntica à qualquer outra conversação sem criptografia.

SSL não é apenas usado para a navegação web. Protocolos inseguros de email como IMAP, POP e SMTP podem tornar-se seguros ao passarem por um túnel SSL. A maioria dos clientes modernos de email suportam IMAPS e POPS (IMAP e POP seguros), assim como SMTP protegido por SSL/TLS. Caso seu servidor de email não forneça suporte SSL, você ainda pode usar esta proteção com o uso de um pacote como o Stunnel (*http://www.stunnel.org/*). O SSL pode ser usado para tornar seguro praticamente qualquer serviço executado sobre o protocolo TCP.

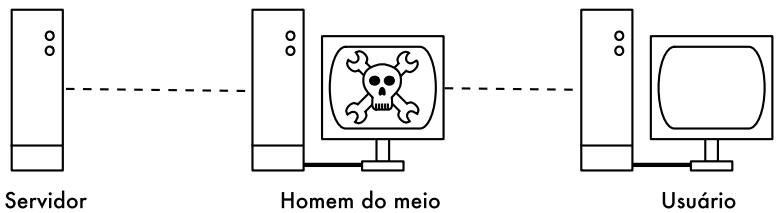


Figura 6.5: O "homem do meio" efetivamente controla tudo o que o usuário vê, podendo gravar e manipular todo o tráfego. Sem uma infra-estrutura de chave pública para verificar a autenticidade das chaves, apenas a criptografia forte não é proteção suficiente para este tipo de ataque.

SSH

Muitas pessoas pensam no SSH como uma alternativa segura ao **`telnet`**, assim como **`scp`** e **`sftp`** como os equivalentes seguros do **`rcp`** e **`ftp`**. Mas o SSH é muito mais do que um shell remoto criptografado. Como o SSL, ele usa criptografia forte com chave pública para validar o servidor remoto e criptografar

os dados. Ao invés da PKI, ele utiliza uma memória de "impressão digital" (*fingerprint*) de chaves que é verificada antes que uma conexão seja autorizada. Ele pode usar senhas, chaves públicas ou outros métodos para a autenticação do usuário.

Muitas pessoas também não sabem que o SSH pode atuar também como um túnel de criptografia genérico, ou mesmo como um proxy de criptografia para a web. Através do estabelecimento inicial de uma conexão SSH para uma localização próxima, confiável, de um servidor remoto (ou no próprio servidor), protocolos inseguros podem ser protegidos contra espionagem e ataques.

Mesmo que esta técnica seja um tanto avançada para muitos usuários, arquitetos de rede podem usar SSH para criptografar o tráfego entre links não confiáveis, como links ponto-a-ponto wireless. Como as ferramentas estão livremente disponíveis e podem ser usadas sobre o padrão TCP, qualquer usuário treinado pode implementar conexões SSH por si próprio, conseguindo sua própria criptografia fim-a-fim sem a intervenção do administrador.

O **OpenSSH** (*http://openssh.org/*) é provavelmente a implementação mais popular em plataformas do tipo Unix. Implementações livres como **Putty** (*http://www.putty.nl/*) e **WinSCP** (*http://winscp.net/*) estão disponíveis para o ambiente Windows. O OpenSSH também roda no Windows sobre o pacote **Cygwin** (*http://www.cygwin.com/*). Os exemplos abaixo assumem que você está usando a versão mais recente do OpenSSH.

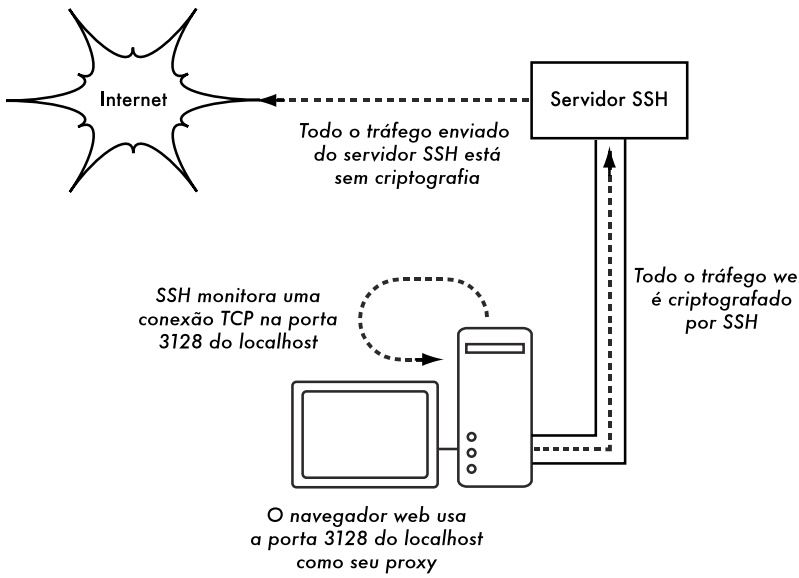


Figura 6.6: O túnel SSH protege o tráfego web até o servidor SSH.

Para estabelecer um túnel criptografado de uma porta na máquina local para uma porta no site remoto, use a chave `-L`. Por exemplo, suponha que você queira encaminhar todo o tráfego do proxy web sob um link criptografado para um servidor squid em squid.example.net. Faça o encaminhamento (forward) da porta 3128 (a porta padrão do proxy) usando o seguinte comando:

```
ssh -fN -g -L3128:squid.example.net:3128 squid.example.net
```

A chave **-fN** instrui o ssh para ficar no modo background (liberando a linha de comando) após a conexão. O **-g** permite que outros usuários de seu segmento de rede conectem-se à máquina local usando-a para a criptografia sobre o link não confiável. O OpenSSH irá usar uma chave pública para a autenticação, caso você tenha configurado uma, ou irá solicitar uma senha de acesso para o site remoto. Você também pode configurar seu navegador para conectar-se à porta local 3128, como seu serviço de proxy web. Todo o tráfego web será, então, criptografado antes da transmissão para o site remoto.

O SSH pode também atuar como um proxy dinâmico SOCKS4 ou SOCKS5. Isto permite que você crie um web proxy que fique responsável pela criptografia, sem a necessidade de configurar o Squid. Note que este não é um proxy de armazenamento local (*caching proxy*), ele simplesmente criptografa o tráfego.

```
ssh -fN -D 8080 remote.example.net
```

Configure seu navegador para usar SOCKS4 ou SOCKS5 na porta local 8080 e siga navegando.

O SSH pode criptografar os dados em qualquer porta TCP, incluindo as que são usadas para email. Ele pode até comprimir os dados enviados, o que pode diminuir a latência em links de baixa capacidade.

```
ssh -fNCg -L110:localhost:110 -L25:localhost:25 mailhost.example.net
```

A chave **-C** liga a compressão. Você pode adicionar tantas regras de encaminhamento de portas (*port forwarding*) quanto desejar, usando a chave **-L** múltiplas vezes. Note que, a fim de conectar-se a uma porta menor que a 1024, você deverá ter privilégios de usuário root na máquina local.

Estes são apenas alguns exemplos da flexibilidade do SSH. Com a implementação de chaves públicas e usando o SSH como agente de encaminhamento, você pode automatizar a criação de túneis criptografados por dentro de sua rede wireless, protegendo sua comunicação com criptografia forte e autenticação.

OpenVPN

O OpenVPN é uma implementação livre, de código aberto de ***VPN*** (***Virtual Private Network*** – Rede Virtual Privada), construída com criptografia SSL. Há implementações de clientes OpenVPN para uma grande variedade de sistemas operacionais, incluindo Linux, Windows 2000/XP e mais recentes, OpenBSD, FreeBSD, NetBSD, Mac OS X e Solaris. Como uma típica VPN, encapsula todo o tráfego (incluindo DNS e outros protocolos) em um túnel criptografado, e não apenas uma porta TCP. A maioria das pessoas consideram-no mais simples de entender e configurar do que o IPSEC.

O OpenVPN também tem algumas desvantagens, como uma latência relativamente alta. Alguma quantidade de latência é inevitável, uma vez que toda a criptografia/descriptografia é feita em espaço de usuário, mas com o uso de computadores relativamente novos em cada uma das pontas do túnel pode minimizar isto. Mesmo podendo usar chaves compartilhadas tradicionais, o OpenVPN realmente destaca-se com o uso de certificados SSL e autoridades

certificadoras. O OpenVPN tem muitas vantagens que o tornam uma boa opção para a segurança fim-a-fim.

Algumas das vantagens incluem:

- É baseado em um sistema de protocolo de criptografia comprovadamente robusto (SSL e RSA);
- É relativamente fácil de configurar;
- Funciona entre várias plataformas diferentes;
- É bem documentado;
- É livre e de código aberto.

O OpenVPN necessita conectar-se em uma única porta TCP ou UDP no site remoto. Uma vez estabelecida a conexão, ele pode encapsular todos os dados até a camada de rede, ou mesmo até a camada de link de dados, caso sua solução necessite disto. Você pode usá-lo para criar conexões VPN robustas entre máquinas individuais, ou simplesmente usá-lo para conectar roteadores sobre uma rede sem fio não confiável.

A tecnologia de VPN é complexa e seu detalhamento está um pouco além do escopo desta sessão. É importante entender como VPNs encaixam-se em sua estrutura de rede a fim de garantir a melhor proteção possível, sem causar problemas não intencionais para a sua organização. Há muitos recursos disponíveis online que tratam da instalação do OpenVPN no servidor e no cliente. Nós recomendamos este artigo do Linux Journal: *http://www.linuxjournal.com/article/7949* assim como o HOWTO oficial: *http://openvpn.net/howto.html*

Tor e anonimizadores

A Internet é, basicamente, uma rede aberta baseada na confiança. Quando você se conecta a um servidor web através da Internet, seu tráfego passa por muitos roteadores diferentes, pertencentes a uma grande variedade de instituições, corporações e indivíduos. A princípio, cada um destes roteadores tem a capacidade de expor totalmente seus dados, os endereços de destino e envio de mensagens e, com freqüência, também o conteúdo dos dados trafegados. Mesmo que seus dados estejam criptografados, com o uso de um protocolo seguro, é possível ao seu provedor de acesso monitorar a quantidade de dados transferidos, assim como a origem e o destino destes dados. Isto é o bastante para reunir um perfil completo de suas atividades online.

A privacidade e a ***anonimidade*** são importantes e estão intimamente ligadas. Há muitas razões válidas para considerar a proteção de sua privacidade através da anonimidade de seu tráfego de rede. Suponha que você queira oferecer conexão à Internet para a sua comunidade local, configurando um certo número de access points para que as pessoas utilizem. Quer você cobre ou não pelo acesso, há sempre o risco de que as pessoas usem a rede para algo que não é legal em seu país ou região. Você pode alegar junto ao sistema judiciário que uma ação ilegal não foi feita por você, mas pode ter sido feita por qualquer pessoa conectada à sua rede. Este problema é elegantemente contornado se for

tecnicamente impossível, para você, a determinação da origem e destino de seu tráfego. E o que dizer sobre a censura online? A publicação anônima de páginas web pode também ser necessária para evitar a censura governamental.[3]

Há ferramentas que permitem a você tornar seu tráfego anônimo de forma relativamente fácil. A combinação do ***Tor*** (*http://www.torproject.org/*) com o ***Privoxy*** (*http://www.privoxy.org/*) constitui uma poderosa forma de implementação de um servidor proxy local que irá passar o seu tráfego de Internet através de um grande número de servidores, tornando muito difícil de seguir a trilha da informação. O Tor pode ser executado em PC local, sobre o Microsoft Windows, Mac OS X, Linux e uma variedade de sistemas BSD, onde ele anonimiza o tráfego desta máquina. O Tor e o Privoxy podem também ser instalados em um gateway ou mesmo em um pequeno access point (como o Linksys WRT54G) onde ele provê a anonimidade para todos os usuários da rede, automaticamente.

O Tor (*The Onion Router* – O Roteador Cebola) funciona pelo contínuo espalhamento aleatório de conexões TCP através de um número de servidores espalhados pela Internet, assim como pelo encapsulamento dos dados de roteamento em uma série de camadas criptografadas (de onde vem o termo "*onion routing*"—***roteamento cebola***) que são "descascadas" na medida em que o pacote move-se através da rede. Isto significa que, em qualquer ponto da rede, os endereços de origem e destino não podem ser associados um ao outro. Isto torna a análise do tráfego extremamente difícil.

A necessidade do proxy de privacidade Privoxy, em conjunto com o Tor, é devido ao fato de que a consulta por nomes de servidores (buscas no DNS), em muitos casos, não passa pelo servidor proxy. Assim, alguém que esteja analisando a sua rede pode facilmente verificar que você está tentando acessar um site específico (por exemplo, google.com) pelo fato de que você fez uma consulta ao DNS pra traduzir o nome google.com para o endereço IP apropriado. O Privoxy conecta-se ao Tor como um proxy SOCKS4a, que usa nomes de hosts (e não endereços IP) para buscar seus pacotes do destino pretendido.

Em outras palavras, o uso do Privoxy com o Tor é um meio simples e efetivo de evitar a análise do tráfego através da ligação de seu endereço IP com os serviços online que você utiliza. Combinado com protocolos de segurança e criptografia (como os que vimos neste capítulo), o Tor e o Privoxy fornecem um alto nível de anonimidade na Internet.

Monitoramento de rede

O monitoramento de rede é feito através do uso de ferramentas de registro e análise que determinam, corretamente, o fluxo de tráfego, utilização e outros indicadores de desempenho em uma rede. Boas ferramentas de monitoramento dão a você tanto números puros quanto representações gráficas do estado de sua rede. Isto ajuda a visualizar precisamente o que está acontecendo, de forma

---

3. N. do T. - A legislação brasileira exige a manutenção de uma série de registros de provimento de acesso à Internet, mesmo quando este é oferecido de forma pública. Antes de oferecer anonimizadores ou outros recursos como parte de uma infra-estrutura de rede, esteja certo de verificar a legislação vigente.

a que você saiba onde ajustes possam ser necessários. Estas ferramentas auxiliam na resposta à questões críticas como:

- Quais os serviços mais populares usados na rede?
- Quais são os usuários que mais utilizam a rede?
- Quais os demais canais wireless usados em minha área?
- Os usuários estão instalando access points em minha rede privada?
- Em quais momentos do dia a rede é mais utilizada?
- Quais os sites mais freqüentados pelos usuários?
- A quantidade de tráfego de entrada e saída está próxima da capacidade disponível em nossa rede?
- Há indicações de situações incomuns que estejam consumindo largura de banda ou causando outros problemas?
- Nosso provedor de acesso à Internet está fornecendo o nível de serviço para o qual estamos pagando? Isto deve ser respondido em termos de largura de banda disponível, perda de pacotes, latência e disponibilidade de uma maneira geral.

E, talvez, a questão mais importante de todas

- O padrão observado de tráfego está de acordo com suas expectativas

Vamos ver como um administrador de sistemas típico pode fazer bom uso destas ferramentas de monitoramento de rede.

Um exemplo efetivo de monitoramento de rede

Para o propósito deste exemplo, vamos assumir que você é o responsável por uma rede que está em funcionamento há três meses. Ela consiste de 50 computadores e três servidores (para email, web e proxy). Mesmo que, inicialmente, tudo estava indo bem, os usuários começaram agora a reclamar de velocidade baixa da rede e o aumento de emails indesejados (*spam*). Com o passar do tempo, o desempenho dos computadores degrada-se muito (mesmo quando a rede não é utilizada), causando considerável frustração em seus usuários.

Com as freqüentes queixas e uma utilização muito baixa dos computadores, a diretoria está questionando a necessidade de tanto investimento em equipamentos de rede. A diretoria também quer evidências de que a largura de banda, pela qual a empresa está pagando, é usada efetivamente. Como administrador de rede, é você quem está recebendo todas estas queixas. Como você pode diagnosticar a súbita queda de desempenho de sua rede e computadores, ao mesmo tempo em que justifica os custos do hardware e da largura de banda?

Monitorando a LAN (tráfego local)

Para ter uma idéia exata do que está causando a queda de velocidade da rede, você deve começar pela observação do tráfego na rede local (LAN – Local Area Network). Há várias vantagens no monitoramento do tráfego local:

- A análise de problemas é enormemente simplificada;
- Vírus podem ser detectados e eliminados;
- Usuários maliciosos podem ser detectados, permitindo que se lide com eles;
- Recursos de hardware de rede podem ser justificados com estatísticas realistas.

Assumimos que todos os switches suportam o ***SNMP*** (***Simple Network Management Protocol***—Protocolo Simples de Gerenciamento de Rede). O SNMP é um protocolo de camada de aplicação projetado para facilitar a troca de informações de gerência entre dispositivos de rede. Ao designar um endereço IP para cada switch, você será capaz de monitorar todas as interfaces deste switch, observando a rede inteira a partir de um único ponto. Isto é muito mais fácil do que habilitar o SNMP em todos os computadores da rede.

Com o uso de uma ferramenta livre, como o MRTG (veja a **Página 190**), você pode monitorar cada porta do switch e apresentar dados de forma gráfica, como um valor agregado em um período de tempo. Estes gráficos são acessíveis através da web, de forma que você poderá acessá-los de qualquer máquina, a qualquer momento.

Com o monitoramento através do MRTG em execução, torna-se óbvio que a rede interna está inundada com muito mais tráfego que a conexão com a Internet pode suportar, mesmo quando o laboratório está desocupado. Esta é uma indicação clara de que alguns dos computadores estão infectados com um vírus de rede. Depois de instalar um bom software antivírus e anti-spyware em todas as máquinas, o tráfego da rede acomoda-se dentro do nível esperado. As máquinas passam a ter um desempenho melhor, emails indesejados são reduzidos e a moral dos usuários melhora rapidamente.

Monitorando a WAN (tráfego externo)

Adicionalmente à observação do tráfego da rede interna, você precisa demonstrar que a largura de banda pela qual a organização está pagando é a que está sendo fornecida pelo provedor de acesso. Você consegue isto através do monitoramento do ***tráfego externo***.

O tráfego externo é geralmente classificado como qualquer coisa enviada através da ***WAN*** (***Wide Area Network*** – Rede de Área Ampla). Qualquer coisa recebida ou enviada entre outra rede que não seja a sua rede interna também é classificada como tráfego externo. As vantagens do monitoramento de tráfego externo incluem:

- Custos de largura de banda para a Internet são justificados através da exibição da utilização real e a verificação de que este uso corresponde às taxas cobradas pelo provedor de acesso;

- O planejamento de necessidades futuras são estimados pela observação de tendências de uso, que auxiliam na predição de padrões de crescimento;
- Intrusos vindos da Internet são detectados e filtrados antes que possam causar problemas.

O monitoramento do tráfego é feito de forma fácil com o uso do MRTG em um dispositivo com o SNMP habilitado, como um roteador. Caso seu roteador não suporte SNMP, você pode adicionar um switch entre a conexão de seu roteador com o provedor de acesso, monitorando o tráfego da mesma forma que faria na rede interna.

Detectando quedas na rede

Com as ferramentas de monitoramento instaladas, você tem meios para medir precisamente a quantidade de banda que sua organização está utilizando. Esta medida deve estar de acordo com o que o provedor de acesso está cobrando. Ela pode indicar também se a real taxa de transmissão (*throughput*) utilizada está próxima da capacidade disponível em momentos de pico. Um gráfico com uma linha máxima plana é uma indicação clara de que você está operando na capacidade total. A **Figura 6.7** mostra esta linha máxima em picos de tráfego de saída acontecendo no meio de cada dia, exceto aos domingos.

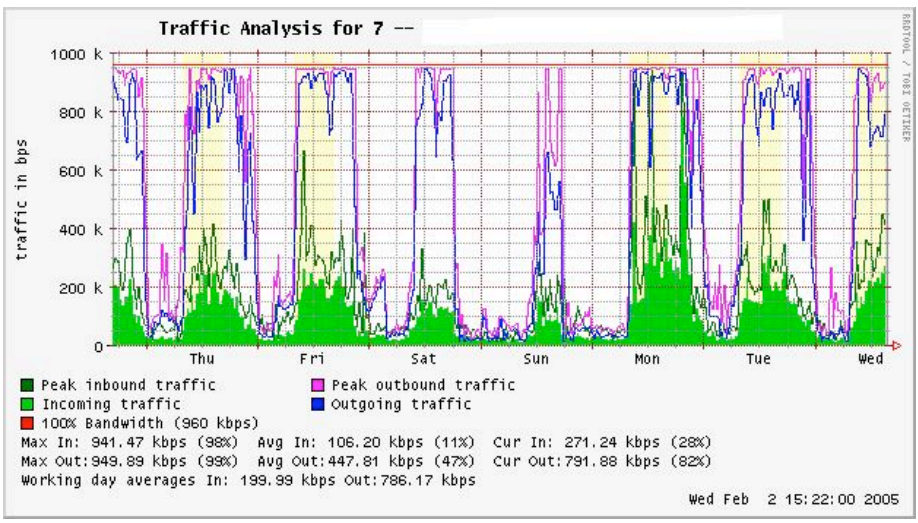


Figura 6.7: Um gráfico com uma linha máxima plana, indicando super utilização.

Isto mostra claramente que sua conexão com a Internet é super utilizada em momentos de pico, causando atrasos na rede. Após a apresentação desta informação para a diretoria, você pode criar um plano para uma otimização posterior da sua conexão existente (atualizando seu servidor proxy e usando outras técnicas deste livro) e estimar quando deverá melhorar sua conexão para que ela esteja de acordo com a demanda. Este é também o momento apropriado para rever sua política operacional com a diretoria, discutindo formas de fazer com que a utilização real esteja de acordo com esta política.

Chegando perto do final de semana, você recebe uma chamada de emergência no final da tarde. Aparentemente, nenhum usuário do laboratório consegue navegar na web ou enviar email. Você corre para o laboratório e reinicializa o servidor proxy, sem resultados. A seguir, você reinicializa o roteador, ainda sem sucesso. Você continua a eliminar os possíveis pontos de falha um a um, e então percebe que o switch de rede está desligado – um cabo de energia solto é o culpado. Uma vez ligado à tomada, a rede volta a funcionar.

Como você poderia diagnosticar este problema sem consumir tanto tempo em tentativa e erro? É possível ser notificado de quedas quando elas ocorrem ao invés de esperar pela reclamação de um usuário? Uma forma de fazer isto é com o uso de um programa como o ***Nagios***, que fica continuamente verificando os dispositivos de rede e notificando quando algum deixa de funcionar. O Nagios registra a disponibilidade de várias máquinas e serviços, alertando-os quando algum deles apresentar problemas. Além de mostrar o estado da rede graficamente em uma página web, ele enviará notificações via SMS ou email, alertando-o imediatamente no caso de problemas.

Com o uso de boas ferramentas de monitoria, você pode justificar o custo de equipamento e banda através da demonstração efetiva da forma como a organização faz uso dos mesmos. Você será notificado automaticamente de problemas, terá a estatística histórica de uso dos equipamentos e saberá do desempenho dos dispositivos de rede. Você pode comparar o desempenho atual com o histórico para encontrar diferenças de comportamento e lidar com os problemas antes que se tornem críticos. Quando os problemas aparecerem, será simples de determinar a causa e a natureza dos mesmos. Seu trabalho será simplificado, a diretoria estará satisfeita e seus usuários muito mais felizes.

Monitorando a sua rede

A gestão de uma rede sem monitoramento é similar à direção de seu veículo sem o velocímetro ou indicadores de combustível e com os seus olhos fechados. Como você saberia a que velocidades está dirigindo? Ou se o carro está consumindo combustível da forma eficiente como prometida pelo vendedor? Se você fizer um ajuste do motor seis meses depois, o carro será mais rápido e eficiente que antes?

De forma similar, como você pagaria por uma conta de consumo de água ou energia elétrica sem verificar o registro dos medidores? Você deve ter a contabilidade da utilização da largura de banda de sua rede a fim de justificar os custos de serviços e a compra de hardware, assim como acompanhar as tendências de utilização.

Há muitos benefícios na implantação de um bom sistema de monitoramento para a sua rede.

1. **Orçamentos para a rede e seus recursos são justificados**. Boas ferramentas de monitoramento podem demonstrar, sem deixar dúvidas, que a infra-estrutura de rede (largura de banda, hardware e software) está adequada e é capaz de lidar com as necessidades de seus usuários.

2. **Intrusos na rede são detectados e filtrados**. Com a observação de seu tráfego de rede, você pode detectar invasores e evitar o acesso a serviços e servidores internos críticos.
3. **Vírus de rede são facilmente detectados**. Você pode ser alertado da presença de vírus de rede e tomar a ação apropriada antes que eles consumam sua largura de banda e desestabilizem sua rede.
4. **A análise de problemas de rede é tremendamente simplificada**. Ao invés de usar o método de tentativa e erro para diagnosticar problemas de rede, você pode ser instantaneamente notificado sobre problemas específicos. Alguns tipos de problemas podem até ser automaticamente resolvidos.
5. **O desempenho da rede pode ser altamente otimizado**. Sem o monitoramento efetivo, é impossível fazer o ajuste de dispositivos e protocolos para que atinjam o melhor desempenho possível.
6. **O planejamento de capacidade é mais fácil**. Com registros confiáveis do histórico de desempenho, você não precisará "adivinhar" quanta banda será necessária na medida em que sua rede cresce.
7. **O uso apropriado da rede pode ser enfatizado**. Quando a largura de banda é um limite escasso, a única maneira de ser justo com todos os usuários é garantir que a rede está sendo usada para o propósito pretendido.

Felizmente, o monitoramento de rede não precisa ser uma tarefa cara. Há muitas ferramentas de código aberto livremente disponíveis que irão mostrar exatamente o que acontece em sua rede, em considerável detalhamento. Esta sessão irá ajudá-lo a identificar muitas ferramentas inestimáveis e como fazer o melhor uso delas.

O servidor dedicado de monitoramento

Mesmo que o monitoramento de serviços possa ser adicionado a um servidor de rede, na maioria das vezes é desejável dedicar uma máquina (ou mais, se necessário) para isto. Algumas aplicações (como o ***ntop***) necessitam de recursos consideráveis para a sua boa execução, especialmente em redes de muita ocupação. Mas a maioria dos programas de registro e monitoria têm requisitos modestos de RAM e utilização de disco, com pouco consumo de CPU. Uma vez que sistemas operacionais de código aberto (como o Linux ou o BSD) fazem o uso muito eficiente de recursos de hardware, é possível a construção de um servidor de monitoramento com boa capacidade a partir de peças recicladas de um PC. Normalmente, não existe a necessidade de adquirir um servidor novo para as tarefas de monitoria.

A exceção a esta regra são instalações de porte muito grande. Caso sua rede possua mais de algumas centenas de nós, ou consuma mais de 50 Mbps de largura de banda de Internet, você provavelmente terá que dividir as tarefas de monitoramento entre algumas máquinas dedicadas. Isto depende bastante da quantidade exata de coisas que você quer monitorar. Se você quer contabilizar

todos os serviços associados por cada endereço MAC, isto irá consumir muito mais recursos do que a simples medida do tráfego de rede na porta de um switch. Mas, para a maioria das instalações, uma única máquina dedicada será o suficiente.

A consolidação dos serviços de monitoria em uma máquina única irá facilitar a administração e as atualizações, assim como garantir um melhor monitoramento contínuo. Por exemplo, se você instalar estes serviços em um servidor web, e este apresentar problemas, então o monitoramento pode ficar inativo até que o problema seja resolvido.

Para um administrador de rede, os dados coletados sobre o desempenho da rede são quase tão importantes quanto a própria rede. Sua monitoria deve ser robusta e protegida de quedas de serviços o melhor possível. Sem as estatísticas de rede, você está cego aos problemas da rede.

Onde este servidor será colocado em minha rede?

Se você está apenas interessado em coletar estatísticas de tráfego de um roteador, você pode fazer isto de praticamente qualquer lugar da rede local. Isto dará dados simples sobre a utilização da rede, mas não poderá fornecer detalhes completos sobre padrões de uso. A **Figura 6.8** mostra um típico gráfico MRTG gerado por um roteador Internet. A utilização do link para o tráfego de entrada e saída são claros, mas não há detalhes sobre os computadores, usuários e protocolos que estão usando a banda.

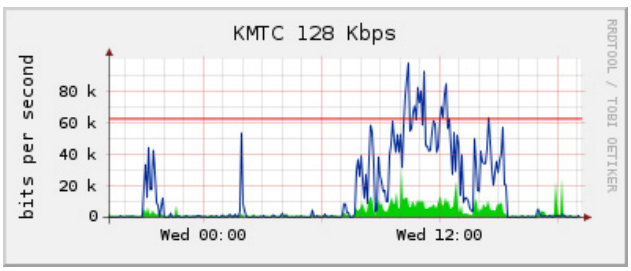


Figura 6.8: A verificação de um roteador no limite da rede pode fornecer dados genéricos sobre sua utilização, mas não permitirá que os dados sejam expandidos em detalhes de uso por máquina, serviços e usuários.

Para que forneça mais detalhes, o servidor dedicado de monitoramento (*monitor*) deve ter acesso a tudo o que precisa ser observado. Na prática, isto significa que ele deve ter acesso a toda a rede. Para monitorar uma conexão WAN, como o link para a Internet fornecido pelo provedor de acesso, o monitor deve ser capaz de enxergar o tráfego passando pelo roteador no limite da rede. Para monitorar a LAN, o monitor deve ser conectado à porta de monitoramento do switch. Se múltiplos switches são utilizados, o monitor deve estar conectado a todos eles. Esta conexão pode ser feita com um cabo físico ou, caso seu switch de rede tenha suporte a isto, com uma VLAN especificamente configurada para monitorar o tráfego.

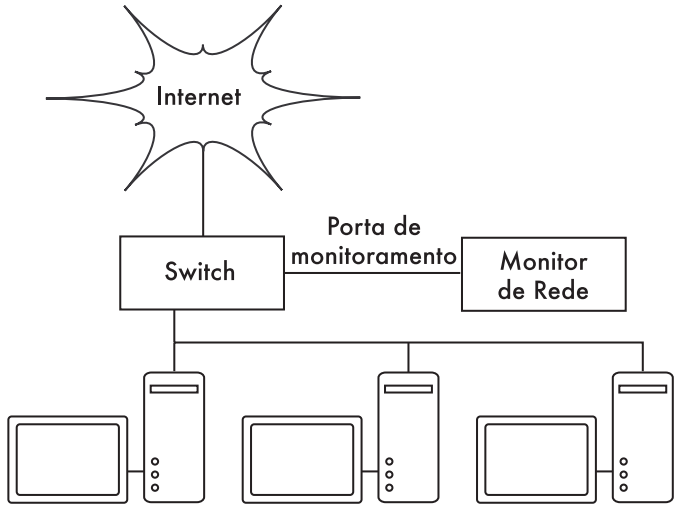


Figura 6.9: Use a porta de monitoramento em seu switch para observar o tráfego entre todas as portas de sua rede.

Caso a porta de monitoramento não esteja disponível em seu switch, o monitor pode ser instalado entre a sua rede interna e a Internet. Mesmo que este método funcione, ele introduz um ponto único de falha para a rede, já que o acesso à Internet ficará indisponível em caso de falha do monitor. Isto também pode consistir em um gargalo de desempenho, no caso do monitor não conseguir lidar com a demanda de tráfego da rede.

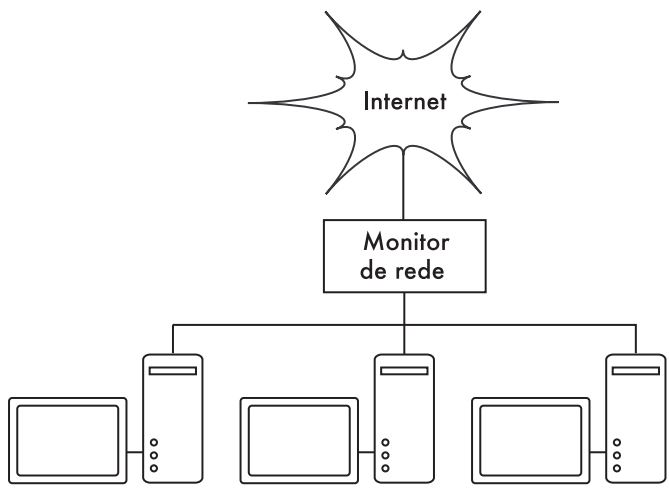


Figura 6.10: Você pode colocar o monitor entre a sua LAN e a conexão para a Internet, observando todo o tráfego da rede.

Uma solução melhor é o uso de um hub de rede (não um switch), conectando o monitor à rede interna e ao roteador de acesso à Internet. Mesmo que isto ainda consista em um ponto único de falhas para a rede (uma vez que o

acesso à Internet será impossível no caso de uma falha do hub), os hubs são geralmente mais confiáveis que roteadores. Eles também são facilmente substituíveis em caso de falhas.

Com o seu monitor instalado, você está pronto para começar a coletar dados.

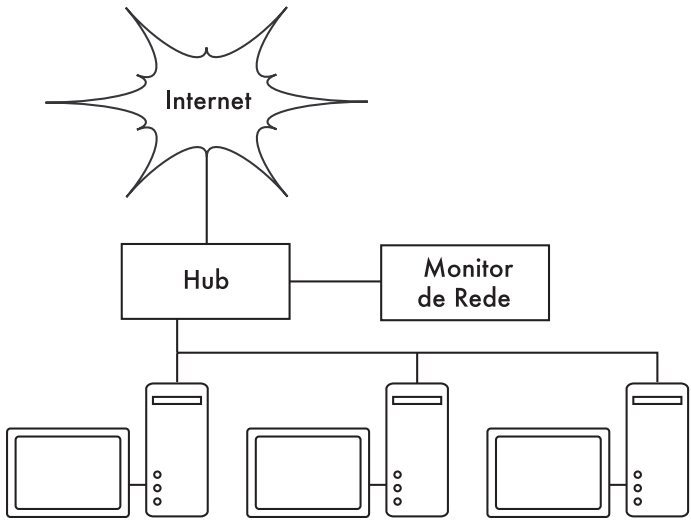


Figura 6.11: Caso seu switch não forneça uma porta de monitoramento, você pode colocar um hub entre seu roteador para a Internet e a LAN, conectando o monitor ao hub.

O que monitorar?

É possível fazer o registro de, praticamente, qualquer evento de rede, observando seu valor em um gráfico em função do tempo. Como cada rede tem suas peculiaridades, você deve decidir quais informações são importantes a fim de monitorar seu desempenho.

Aqui estão alguns indicadores importantes que muitos administradores de rede irão registrar, geralmente.

Estatísticas da rede wireless

- Sinal recebido e nível de ruído em todos os nós principais;
- Número de estações (nós, dispositivos em geral) conectadas;
- Redes e canais adjacentes detectados;
- Retransmissões excessivas;
- Taxas de transmissão de rádio (no caso de usar algum mecanismo automático de ajuste de taxas de transmissão).

Estatísticas do switch

- Uso de largura de banda por porta;
- Uso de largura de banda por protocolo;
- Uso de largura de banda por endereço MAC;
- Mensagens de broadcast comparadas com o número total de pacotes;
- Perda de pacotes e taxa de erros.

Estatísticas de Internet

- Uso de largura de banda de Internet por servidor e protocolo;
- Requisições atendidas pelo servidor proxy;
- Os 100 sites mais acessados;
- Buscas de DNS;
- Número de emails recebidos, spam, emails rejeitados;
- Tamanho da fila de emails a serem enviados;
- Disponibilidade de serviços críticos (servidores web, de email, etc);
- Tempos de "ping" e taxa de perda de pacotes para seu provedor de acesso;
- Estado das cópias de segurança.

Estatísticas de saúde do sistema

- Uso de memória;
- Uso de arquivo de paginação de memória (swap);
- Número de processos, processos zumbis;
- Carga do sistema;
- Voltagem e carga do no-break;
- Temperatura, velocidade do ventilador e voltagens do sistema;
- Estado SMART do disco rígido;
- Estado dos discos RAID.

Você deve usar estas sugestões como um ponto de partida. Com o amadurecimento da sua rede, você provavelmente encontrará novos indicadores importantes para seu desempenho, devendo acompanhá-los também. Há muitas ferramentas livres que mostram tantos detalhes quantos desejados acerca do que está acontecendo em sua rede. Você também deve monitorar a disponibilidade de qualquer recurso que, em caso de falha, afete os usuários de sua rede.

Por exemplo, seus usuários podem usar uma conexão discada para acessar sua localidade remotamente. Caso todos os modems estejam ocupados ou algum deles não esteja funcionando, alguns usuários podem ter seu acesso negado e provavelmente reclamarão. Você pode prever e evitar tais problemas monitorando o número de modems disponíveis e provisionando alguma capacidade extra antes de seu esgotamento.

Não se esqueça de monitorar a própria máquina que faz o monitoramento, como seu uso de CPU e espaço em disco, a fim de ser avisado prontamente no caso de sobrecarga ou falhas. Um monitor com recursos esgotados pode ter afetada a sua habilidade de monitorar efetivamente a rede.

Tipos de ferramentas de monitoramento

Vamos olhar agora várias classes diferentes de ferramentas de monitoramento. Ferramentas de ***detecção de rede*** ficam atentas às notificações enviadas pelos pontos de acesso sem fio, mostrando informações sobre o nome da rede, intensidade do sinal recebido e canais utilizados. Ferramentas de ***checagem pontual*** são projetadas para a análise de problemas, rodando de forma interativa por curtos períodos de tempo. Um programa como o **`ping`** pode ser considerado uma ferramenta de checagem pontual ativa, uma vez que gera tráfego ao acessar uma máquina em particular. Ferramentas de checagem pontual passiva incluem ***analisadores de protocolo***, que inspecionam cada pacote na rede e fornecem detalhes completos sobre cada troca de informações (incluindo endereços de envio e destino, informações sobre o protocolo e mesmo dados de aplicações). Ferramentas de ***tendência*** fazem o monitoramento, sem interação com o usuário, por longos períodos de tempo, tipicamente exibindo os resultados em um gráfico. Ferramentas de ***monitoramento em tempo*** real fazem um tipo similar de monitoramento, mas notificam os administradores imediatamente, caso detectem algum problema. Ferramentas de ***teste de throughput*** mostram o estado atual da largura de banda disponível entre dois pontos de uma rede. Ferramentas de ***detecção de intrusos*** observam o tráfego de rede inesperado ou indesejável, tomando a ação apropriada (normalmente bloqueando o acesso e/ou notificando o administrador da rede). Finalmente, ferramentas de ***medidas de desempenho*** estimam o desempenho máximo de um serviço ou conexão de rede.

Detecção de rede

As ferramentas de monitoramento wireless mais simples fornecem apenas uma lista das redes disponíveis, em conjunto com informações básicas (como a intensidade do sinal e o canal utilizado). Elas permitem que você rapidamente detecte redes vizinhas e determine se elas estão no mesmo alcance ou se estão causando interferências.

- **O cliente embarcado** (*built-in*). Todos os sistemas operacionais modernos fornecem o suporte para redes wireless. Isto tipicamente inclui a habilidade de procurar por redes disponíveis, permitindo ao usuário a escolha de uma delas em uma lista. Mesmo que todos os dispositivos wireless tenham, garantidamente, uma ferramenta simples de busca por

redes, as funcionalidades podem variar bastante entre as várias implementações. Estas ferramentas são normalmente úteis apenas para configurar um computador em casa ou em um ambiente de escritório. Elas tendem a fornecer pouca informação, além dos nomes das redes e intensidade de sinal do access point que está acessando.

- **Netstumbler** (*http://www.netstumbler.com/*). Esta é a ferramenta mais popular para a detecção de redes sem fio com o uso do Microsoft Windows. Ela suporta uma variedade de cartões wireless e é muito fácil de usar, detectando redes abertas e criptografadas (mas não pode detectar redes fechadas). Ela também possui um medidor da relação sinal/ruído que exibe os dados do receptor de rádio em um gráfico em função do tempo. Pode também ser integrada com dispositivos GPS para registrar a localização precisa e a informação sobre a força do sinal. Isto torna o Netstumbler uma ferramenta útil para uma pesquisa informal de uma localidade.
- **Ministumbler** (*http://www.netstumbler.com/*). Dos mesmos fabricantes do Netstumbler, o Ministumbler fornece a mesma funcionalidade da versão Windows, mas roda em uma plataforma Pocket PC. O Ministubler pode ser usado em um dispositivo de mão (*handheld*) PDA (*Personal Digital Assistant*) para detectar access points em uma região.
- **Macstumbler** (*http://www.macstumbler.com/*). Mesmo sem relação direta com o Netstumbler, o Macstumbler fornece boa parte de sua funcionalidade, mas para a plataforma Mac OS X. Ele funciona com todos os cartões Airport da Apple.
- **Wellenreiter** (*http://www.wellenreiter.net/*). O Wellenreiter é um detector de redes wireless gráfico para o Linux. Requer Perl e GTK e suporta os cartões Prsm2, Lucent e Cisco.

Ferramentas de checagem pontual

O que você faz quando sua rede falha? Se você não consegue acessar uma página web ou um servidor de email, e clicar no botão “recarregar” não resolve o problema, então você deverá ser capaz de descobrir a exata localização do problema. Estas ferramentas irão ajudá-lo a determinar exatamente onde está o problema de conexão.

Esta sessão é simplesmente uma introdução às ferramentas mais comuns para a análise de problemas. Para uma discussão mais detalhada sobre problemas comuns de rede e seu diagnóstico, veja o **Capítulo 9**, **Análise de problemas**.

ping

Quase todos os sistemas operacionais (incluindo Windows, Mac OS X e, claro, Linux e BSD) incluem uma versão do utilitário ***ping***. Ele usa pacotes ICMP para tentar o contato com um servidor específico, informando quanto tempo leva até receber uma resposta.

Saber o que "pingar"[4] é tão importante como saber como "pingar". Caso você constate que não é possível a conexão a um determinado serviço através de seu navegador (como *http://yahoo.com/*), você pode fazer um teste com o 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
```

Pressione simultaneamente as teclas control-C quando terminar de coletar os dados. Se os pacotes demorarem muito tempo para voltar, pode haver congestionamento na rede. Se os pacotes que retornam tiverem um ***tempo de vida*** (***TTL*** – *Time To Live*) incomum, você pode ter problemas de roteamento entre a sua máquina e o servidor remoto. Mas e se o ping não retorna dado algum? Se você está dando o ping em um nome, ao invés de um endereço IP, você pode ter problemas de DNS.

Tente pingar um endereço IP na Internet. Caso você não consiga, é uma boa idéia ver se você consegue pingar o roteador padrão:

```
$ 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
```

Se você não consegue pingar o roteador padrão, então as chances são de que você não conseguirá acessar a Internet. Se você não conseguir pingar nenhum outro endereço em sua rede local, então é a hora de verificar a sua conexão. Caso esteja usando Ethernet, o cabo está conectado? Caso esteja usando wireless, você está conectado à rede correta? Ela está a seu alcance?

A análise de problemas da rede com o ping é quase uma arte, mas é útil aprender. Como você terá o ping disponível em praticamente todas as máquinas com as quais irá trabalhar, é uma boa idéia saber como utilizá-lo bem.

traceroute e mtr

Da mesma forma que o ping, o ***traceroute*** é encontrado na maioria dos sistemas operacionais (ele é chamado de tracert em algumas versões do

4. N. do T. - O verbo "*to ping*", popularmente usado em inglês para descrever os vários usos do comando ping, foi livremente traduzido pelos administradores de rede brasileiros. Assim, é comum ouvir coisas do tipo "Você tentou pingar o servidor?", ou "Você já deu um ping no servidor?".

Microsoft Windows). Ao executar o traceroute, você consegue localizar problemas entre o seu computador e qualquer outro ponto na 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 * * *
```

A chave **-n** instrui ao traceroute que não resolva nomes através do DNS, fazendo a análise ser executada mais rapidamente. Você pode notar que no *hop* (salto) número sete, a viagem de ida e volta leva mais do que dois segundos, enquanto os pacotes parecem ser descartados no *hop* oito. Isto pode indicar um problema naquele ponto da rede. Caso esta parte da rede esteja sob a sua responsabilidade, vale a pena começar a análise de problemas nesta localidade.

My TraceRoute (***mtr***, *http://www.bitwizard.nl/mtr/*) é um programa bastante útil, que combina o ping e o traceroute em uma única ferramenta. Ao rodar o mtr você pode obter médias da latência e perda de pacote atuais para um servidor específico, ao invés do simples retrato momentâneo fornecido pelo ping e pelo 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
```

Os dados são continuamente atualizados, com sua média calculada em função do tempo. Como no ping, ao pressionar control-C você finaliza a observação dos dados. Você deve ter privilégios de usuário root para executar o mtr.

Mesmo que estas ferramentas não revelem precisamente o que está errado em sua rede, elas podem dar informação suficiente para que se saiba aonde continuar o diagnóstico.

Analisadores de protocolos

Analisadores de protocolos fornecem bastante detalhe sobre o fluxo de informação em uma rede, permitindo a inspeção de pacotes individuais. Em redes cabeadas, você pode inspecionar pacotes a partir do nível de conexão de dados ou acima. Para redes sem fio, você pode inspecionar a informação até o

nível de quadros (*frames*) individuais do 802.11. Aqui estão vários analisadores de protocolos de redes em software livre:

Kismet

O ***Kismet*** (*http://www.kismetwireless.net/*) é um poderoso analisador de protocolo wireless para muitas plataformas, incluindo Linux, Mac OS X e mesmo a distribuição embarcada OpenWRT Linux. Ele funciona com qualquer cartão wireless que suporte o modo de monitoramento passivo. Além da detecção de redes, o Kismet irá registrar passivamente todos os *frames* 802.11 para o disco ou para a rede em um formato padrão PCAP, para análise posterior por ferramentas como a Ethereal. O Kismet também fornece informações sobre clientes conectados, impressão digital (*fingerprinting*) do AP, detecção de Netstumbler e integração com GPS.

Sendo um monitor passivo, ele pode até detectar redes wireless fechadas através da análise do tráfego enviado por clientes wireless. Você pode executar o Kismet em várias máquinas simultaneamente, reunindo seus resultados em uma interface central de usuário. Isto permite o monitoramento de uma grande área, como uma universidade ou toda a extensão de uma empresa.

Figura 6.12: Kismet rodando em um Tablet Internet Nokia 770.

KisMAC

Exclusivamente para a plataforma MAC OS X, o ***KisMAC*** (*http://kismac.macpirate.ch/*) faz tudo o que o Kismet faz, mas com uma interface gráfica no estilo MAC. É um analisador passivo que irá registrar dados em um disco, no formato PCAP, compatível com o Wireshark. Ele suporta a varredura passiva com cartões AirportExtreme, assim como com uma variedade de adaptadores wireless USB.

tcpdump

O ***tcpdump*** (*http://www.tcpdump.org/*) é uma ferramenta de linha de comando para o monitoramento de tráfego de rede. Ele não tem todas as funcionalidades do Wireshark mas, em contrapartida, consome menos recursos. O tcpdump pode capturar e exibir toda a informação dos protocolos de rede até a camada de conexão de dados. Ele pode mostrar todos os cabeçalhos dos pacotes e dados recebidos, ou apenas aqueles que correspondem a um determinado critério. Os pacotes capturados pelo tcpdump podem ser carregados no Wireshark para a análise visual e diagnóstico posterior. Isto é especialmente útil no caso do monitoramento na interface de uma máquina remota, que pode ser analisado em uma máquina local. A ferramenta está disponível para o Unix e seus derivados (Linux, BSD e Mac OS X). Há uma versão para Windows chamada WinDump, disponível em *http://www.winpcap.org/windump/*.

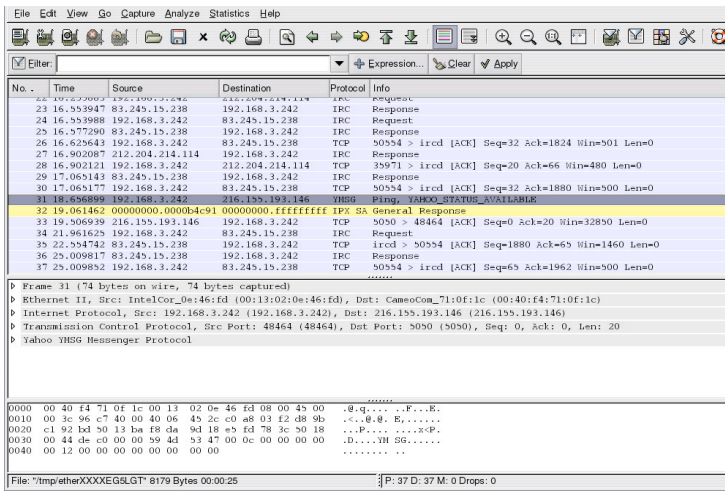


Figura 6.13: O Wireshark (antigamente conhecido como Ethereal) é um poderoso analisador de protocolos de rede que pode mostrar tanto detalhe quanto desejado sobre qualquer pacote.

Wireshark

Conhecido antigamente como Ethereal, o ***Wireshark*** (*http://www.wireshark.org/*) é um analisador de protocolos livre para Unix e Windows. É conhecido como "O Analisador de Protocolos de Rede mais popular em todo o Mundo."

O Wireshark permite que você analise dados de uma rede em funcionamento "ao vivo" ou a partir de um arquivo armazenado em disco, analisando e organizando os dados capturados de forma interativa. Tanto a informação resumida quanto a detalhada está disponível para cada pacote, incluindo o cabeçalho integral e porções de dados. O Wireshark possui uma série de funções poderosas, incluindo uma linguagem rica para a filtragem de visualização e a habilidade de exibir um fluxo reconstruído de uma sessão TCP.

Pode ser um tanto complicado para novos usuários, ou para aqueles que não estão familiarizados com as camadas OSI. Ele é tipicamente usado para isolar e analisar o tráfego específico de entrada ou saída para um endereço IP,

mas pode também ser usado como uma ferramenta genérica para a detecção de falhas. Por exemplo, uma máquina infectada com um verme ou vírus de rede pode ser identificada através da constatação de que a mesma está enviando o mesmo tipo de pacotes TCP/IP para grandes grupos de endereços IP.

Ferramentas de tendência

Ferramentas de tendência são usadas para ver como a sua rede é utilizada dentro de um longo período de tempo. Elas funcionam através do monitoramento periódico de sua atividade de rede, mostrando um resumo em uma forma legível (como um gráfico). Ferramentas de tendência coletam os dados, analisam os mesmos e produzem relatórios.

Abaixo, alguns exemplos de ferramentas de tendência. Algumas necessitam ser usadas em conjunto com outras, já que não executam todas as funções sozinhas.

MRTG

O ***Multi Router Traffic Grapher*** (***MRTG*** – Visualizador gráfico de tráfego multi-roteador, *http://oss.oetiker.ch/mrtg/*) monitora a carga do tráfego na rede usando SNMP. O MRTG gera gráficos que fornecem uma representação visual do tráfego de entrada e saída, e são tipicamente exibidos em uma página web.

A configuração do MRTG pode ser um pouco confusa, especialmente se você não está familiarizado com o SNMP. Mas uma vez instalado, o MRTG requer pouquíssima manutenção, a não ser que você mude alguma coisa no sistema que está sendo monitorado (como um endereço IP).

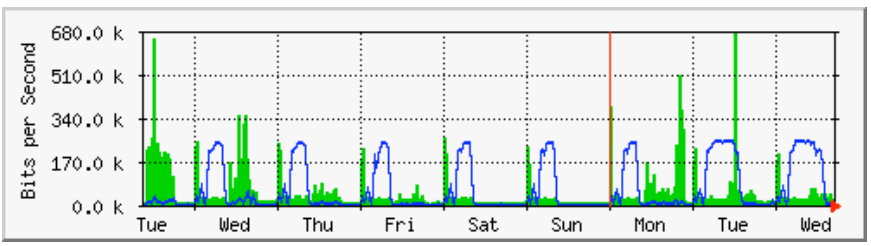


Figura 6.14: O MRTG é provavelmente o visualizador gráfico de tráfego de rede mais utilizado.

RRDtool

RRD é a abreviatura de ***Round Robin Database***. RRD é uma base de dados que armazena a informação de uma forma compacta, que não aumenta com o tempo. ***RRDtool*** (*http://oss.oetiker.ch/rrdtool/*) refere-se a um conjunto de ferramentas que serve para criar e modificar bases de dados RRD, assim como gerar gráficos úteis para a apresentação destes dados. É usado para a observação de dados em séries de tempo (como a largura de banda da rede, temperatura do ambiente das máquinas, média de carga dos servidores) e pode exibir tais dados como uma média no tempo.

Note que o RRDtool não contata diretamente os dispositivos de rede para obter os dados. Ele é simplesmente uma ferramenta para a manipulação da

base de dados. Você pode usar um script simples (normalmente em shell ou Perl) para fazer este trabalho. O RRDtool é usado também por muitas interfaces com funcionalidades completas, que fornecem a possibilidade de configuração e visualização através da web. Os gráficos RRD oferecem mais controle sobre as opções de visualização, assim como o maior número de itens disponíveis para os gráficos, em comparação com o MRTG.

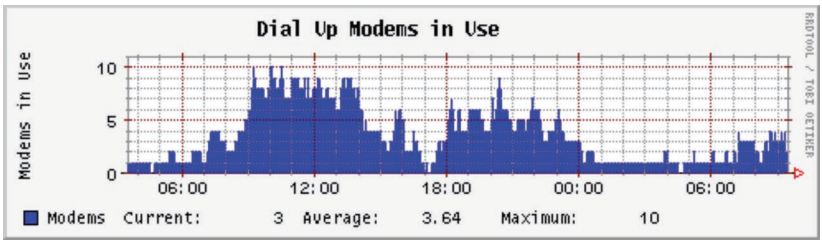


Figura 6.15: RRDtool dá a você muita flexibilidade sobre a forma como os dados são coletados e exibidos.

O RRDtool está incluído em praticamente todas as distribuições Linux recentes e pode também ser obtido de *http://oss.oetiker.ch/rrdtool/*.

ntop

Você certamente irá querer investigar o ***ntop*** (*http://www.ntop.org*) para a análise histórica de tráfego e utilização da rede. Este programa fornece um relatório detalhado, em tempo real, do tráfego de rede, exibindo-o em um navegador web. Ele integra-se com o RRDtool, produzindo gráficos e mapas que mostram a forma como a rede está sendo utilizada. Em redes de tráfego intenso, o ntop pode utilizar bastante CPU e espaço em disco, mas ele fornece uma extensa visualização da utilização da rede. Ele está disponível para Linux, BSD, Mac OS X e Windows.

Algumas de suas funcionalidades mais interessantes incluem:

- A organização dos dados visualizados dentro de vários critérios (fonte, destino, protocolo, endereço MAC, etc.);
- Estatísticas de tráfego agrupadas por protocolo e número de porta;
- Matriz de tráfego IP mostrando as conexões entre as máquinas;
- Fluxo de rede para roteadores e switches que suportem o protocolo NetFlow;
- Identificação do sistema operacional dos servidores;
- Identificação de tráfego P2P;
- Numerosas representações gráficas;
- API para a integração com as linguagens Perl, PHP e Python.

O ntop está disponível em *http://www.ntop.org/* e possui pacote de instalação para a maioria dos sistemas operacionais. Ele é freqüentemente

incluído em muitas distribuições Linux populares como RedHat, Debian e Ubuntu. Ainda que possa ficar em execução para a coleta de dados históricos, o ntop pode consumir bastante CPU dependendo da quantidade de tráfego observada. Caso você o deixe em execução por muito tempo, monitore também a utilização da CPU onde o mesmo está rodando.

Global TCP/UDP Protocol Distribution

TCP/UDP Protocol	Data	Flows	Accumulated Percentage / Historical Protocol View
FTP	17.8 KB	53	0%
HTTP	40.8 MB	1,410	88.2%
DNS	543.8 KB	4,851	1.1%
NBios-IP	35.4 KB	391	0%
Mail	1.2 MB	166	2.5%
SNMP	0.1 KB	1	0%
NNTP	0.4 KB	4	0%
Gnutella	0.3 KB	2	0%
BitTorrent	18.0 KB	2	0%
Messenger	4.0 KB	3	0%
Other TCP/UDP-based Protocols	3.7 MB	6,129	7.9%

Accumulated View

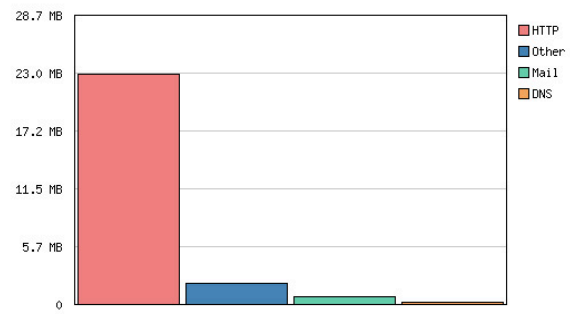


Figura 6.16: O ntop exibe uma grande quantidade de informação sobre a utilização da rede por vários clientes e protocolos.

A principal desvantagem do ntop é que ele não fornece informações instantâneas, apenas totais e estatísticas de longo termo. Isto pode tornar difícil a sua utilização na identificação de problemas repentinos.

Cacti

O ***Cacti*** (*http://www.cacti.net/*) é uma interface, escrita em PHP, para o RRDtool. Ele armazena, em uma base MySQL, toda a informação necessária para criar os gráficos. O Cacti assume o trabalho de manutenção dos gráficos, fontes de dados e a obtenção destes dados. Fornece o suporte para dispositivos SNMP e scripts customizados podem ser facilmente escritos para o monitoramento de qualquer evento de rede imaginável.

O Cacti pode ser um tanto confuso de configurar, mas uma vez que você leia a documentação e os exemplos, ele poderá produzir gráficos impressionantes. Há centenas de templates para vários sistemas, disponíveis no website do Cacti, e o código está em rápido desenvolvimento.

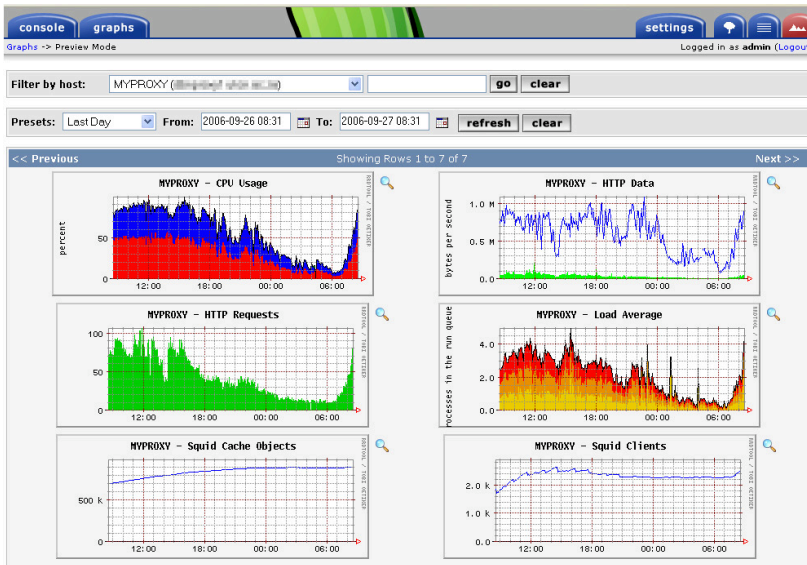


Figura 6.17: O Cacti pode gerenciar o monitoramento de seus dispositivos de rede, construindo visualizações bastante informativas e complexas do comportamento da rede.

NetFlow

O ***NetFlow*** é um protocolo para a coleta de informações de tráfego IP, criado pela Cisco. Do website da Cisco:

> *O Cisco IOS NetFlow fornece, eficientemente, um conjunto de serviços para aplicações IP, incluindo a contabilidade do tráfego de rede, bilhetagem da utilização da rede, planejamento de rede, segurança, capacidade de monitoramento de ataques de negação de serviços e monitoramento de rede. O NetFlow provê valiosas informações sobre os usuários e aplicações de rede, horários de pico de utilização e roteamento de tráfego.*

Os roteadores Cisco podem gerar a informação NetFlow, disponível na forma de pacotes UDP. O NetFlow consome menos CPU em roteadores Cisco do que o SNMP. Ele também fornece dados mais granulares que o SNMP, permitindo a obtenção de maiores detalhes sobre a utilização de portas e protocolos.

Esta informação é capturada por um coletor NetFlow, que armazena e apresenta os dados como um agregado em função do tempo. Através da análise do fluxo de dados, pode ser construído um gráfico do fluxo e volume de tráfego em uma rede ou uma conexão. O ntop é uma ferramenta livre que pode funcionar como um coletor de dados NetFlow. Outra é o Flowc (veja abaixo).

Pode ser desejável usar o NetFlow como uma ferramenta de checagem pontual, observando apenas uma fotografia momentânea dos dados durante uma crise da rede. Pense no NetFlow como uma alternativa ao SNMP para dispositivos Cisco. Para mais informações sobre o NetFlow, visite *http://en.wikipedia.org/wiki/Netflow* .

Flowc

O ***Flowc*** (*http://netacad.kiev.ua/flowc/*) é um coletor em código aberto para o NetFlow (ver acima). É leve e fácil de configurar, usando uma base MySQL para armazenar informação agregada sobre o tráfego. Desta forma, é possível criar os seus próprios relatórios usando o SQL ou usando os geradores de relatórios incluídos no programa. Estes produzem relatórios em HTML, texto puro, ou em um formato gráfico.

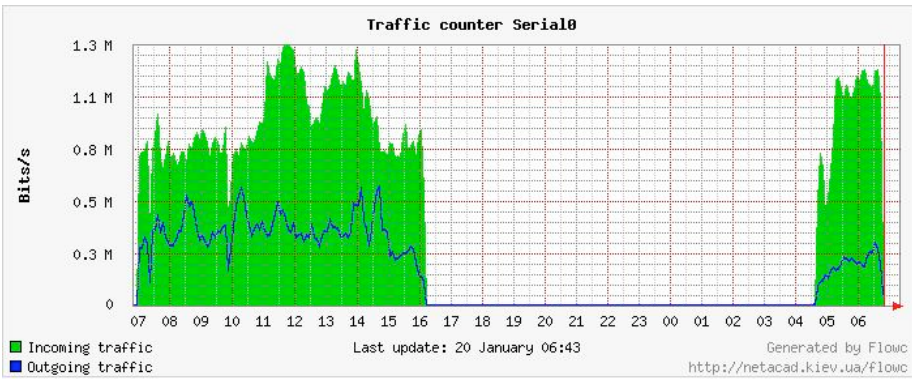


Figura 6.18: Um gráfico típico gerado pelo Flowc.

Um intervalo grande nos dados indica, possivelmente, uma queda de rede. Ferramentas de tendência não irão, tipicamente, notificá-lo de falhas, mas apenas registrar a ocorrência. Para ser notificado da ocorrência de problemas, use uma ferramenta de monitoramento em tempo real, como o ***Nagios*** (veja a **Página 200**).

SmokePing

O ***SmokePing*** (*http://oss.oetiker.ch/smokeping/*) é uma sofisticada ferramenta para a medida de latência escrita em Perl. Ele pode medir, armazenar e exibir a latência, a distribuição da latência e a perda de pacotes em um único gráfico. O SmokePing usa o RRDtool para o armazenamento de dados e pode produzir gráficos bastante informativos que apresentam a informação quase em tempo real do estado de sua conexão de rede.

É bastante útil a execução do SmokePing em um servidor com boa conectividade para toda a sua rede. Com o tempo, revelam-se tendências que podem apontar todo o tipo de problemas de rede. Combinado com o MRTG (veja a **Página 190**) ou o Cacti (veja a **Página 192**), você pode observar o efeito que o congestionamento de rede tem na perda de pacotes e na latência. O SmokePing pode, opcionalmente, enviar alertas quando determinadas condições são atingidas, como o excesso de perda de pacotes em um link num período extenso de tempo. Um exemplo do SmokePing em ação é mostrado na **Figura 6.19**.

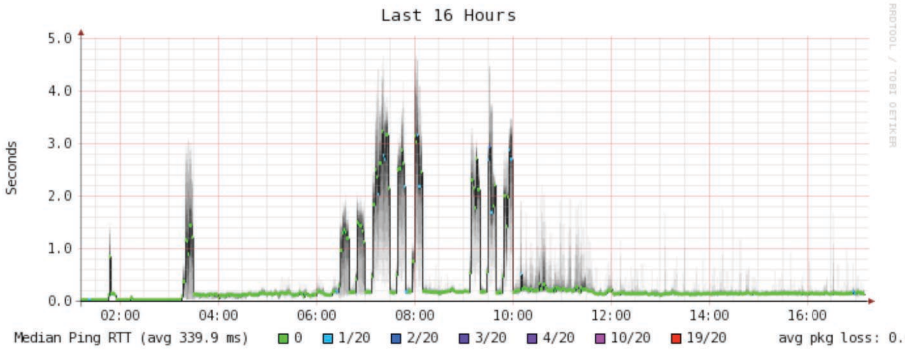


Figura 6.19: O SmokePing pode mostrar, simultaneamente, a perda de pacotes e a latência em um único gráfico.

EtherApe

O **EtherApe** (*http://etherape.sourceforge.net/*) exibe uma representação gráfica do tráfego da rede. Os servidores e links são representados em tamanhos diferentes, dependendo da quantidade de tráfego enviada ou recebida. As cores mudam para representar o protocolo mais utilizado. Como no Wireshark e no tcpdump, os dados são capturados em tempo real de uma conexão de rede ativa ou lidos a partir de um arquivo de captura do tcpdump.

O EtherApe não mostra tantos detalhes quanto o ntop, mas seu consumo de recursos é bem menor.

Argus

Argus (*http://qosient.com/argus/*) significa ***Audit Record Generation and Utilization System*** (Sistema de geração de registros de auditoria e utilização). Argus também é o nome do deus da mitologia grega, que tem centenas de olhos.

Do website do Argus:

> *O Argus gera estatísticas de fluxo de dados como conectividade, capacidade, demanda, perdas, atrasos e ruídos em uma transação entre pares. O Argus pode ser usado para analisar e gerar relatórios sobre os arquivos de captura de conteúdos de pacotes ou pode ser executado como um monitor contínuo, examinando os dados de uma interface de rede em funcionamento; gerando registros de auditoria para toda a atividade de rede observada no fluxo de pacotes. O Argus pode ser instalado para monitorar sistemas individuais ou a atividade de rede de uma organização inteira. Como um monitor contínuo, o Argus fornece modelos de tratamento de dados push e pull (empurra e puxa) para oferecer estratégias flexíveis à coleta de dados de auditoria de rede. Os clientes de dados Argus suportam uma variedade de operações como ordenação, arquivamento e relatório.*

O Argus consiste de duas partes: um coletor principal que lê os pacotes de um dispositivo de rede e um cliente, que conecta-se ao coletor principal e exibe as estatísticas de uso. Ele roda em BSD, Linux e na maioria dos outros sistemas Unix.

iptraf

O ***iptraf*** (*http://iptraf.seul.org/*) é um monitor de rede local leve e poderoso. Ele tem uma interface ncurses e roda a partir da linha de comando. O iptraf leva um momento para medir o tráfego observado e, então, exibe várias informações estatísticas da rede, incluindo conexões TCP e UDP, informações ICMP e OSPF, fluxo de tráfego, erros de IP (*checksum errors*) e mais. É um programa simples de usar e que utiliza recursos mínimos do sistema.

Mesmo sem manter dados históricos, ele é muito útil na exibição de relatórios instantâneos de utilização da rede.

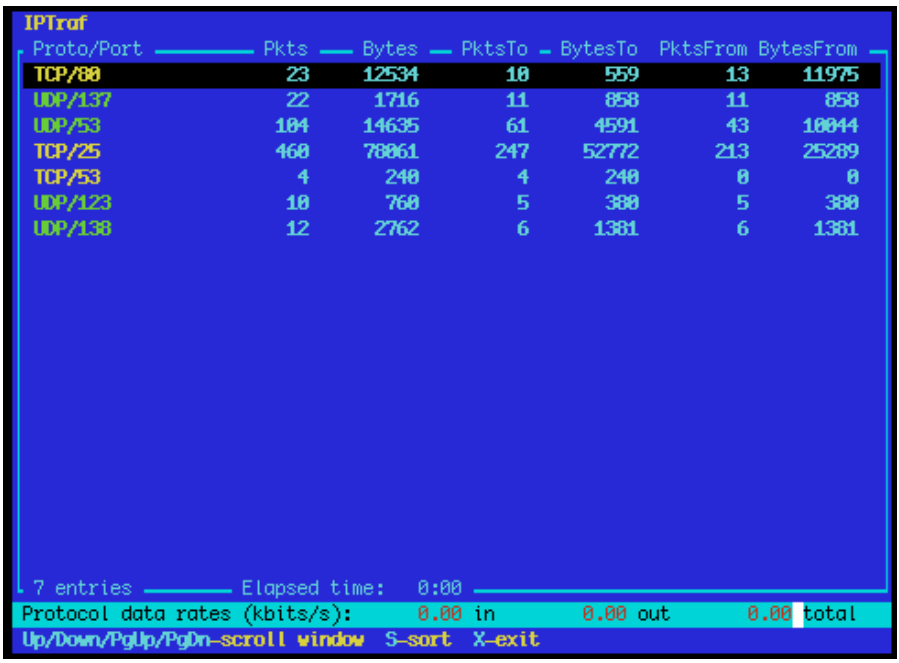


Figura 6.20: Divisão estatística do tráfego entre várias portas com o uso do iptraf.

NeTraMet

NeTraMet (*http://freshmeat.net/projects/netramet/*) é outra ferramenta popular para a análise de fluxo. Como o Argus, o NeTraMet também é dividido em duas partes: um coletor que reúne as estatísticas via SNMP e um gerente que especifica quais fluxos devem ser observados. Os fluxos são definidos através de uma linguagem de programação simples, que especificam os endereços usados em cada ponta da comunicação, e podem incluir Ethernet, IP, informação de protocolo ou outros identificadores. O NeTraMet roda no DOS e na maioria dos sistemas Unix, incluindo o Linux e o BSD.

Testes de throughput

A que velocidade sua rede pode ir? Qual a real capacidade que pode ser usada em uma conexão de rede em particular? Você pode ter uma estimativa

muito boa destas capacidades através da injeção de tráfego no link e medindo quanto tempo é necessário para que os dados sejam transmitidos.

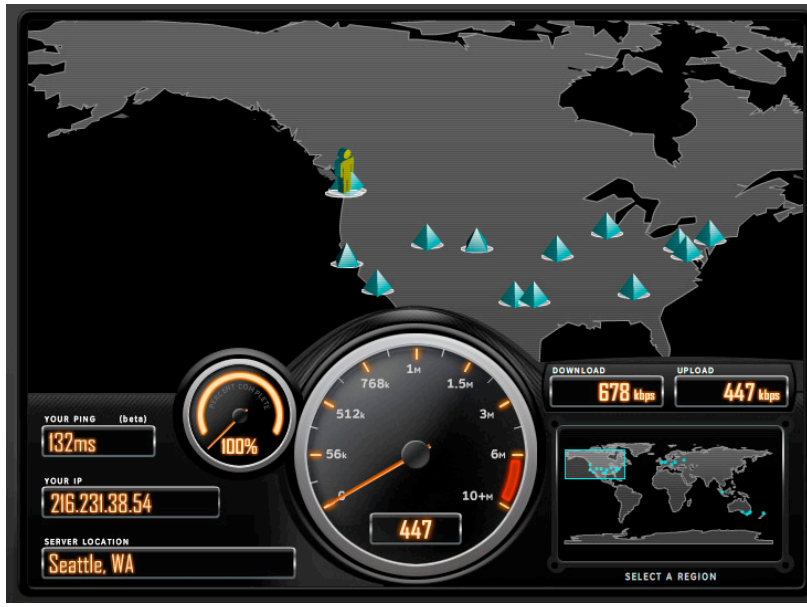


Figura 6.21: Ferramentas como esta, da SpeedTest.net, são visualmente atrativas, mas nem sempre dão a você um retrato fiel do desempenho da rede.

Mesmo que existam páginas web que realizam um "teste de velocidade" em seu navegador (como *http://www.dslreports.com/stest* ou *http://speedtest.net/*), estes testes são crescentemente incorretos na medida em que você está longe da fonte de teste. Pior que isto, elas não permitem que você teste a velocidade de um link específico, mas apenas a velocidade de seu link até uma localidade em particular na Internet. Aqui estão algumas ferramentas que irão permitir que você faça testes de velocidade (*throughput*) em suas redes.

ttcp

Agora um padrão na maioria dos sistemas baseados em Unix, ***ttcp*** (*http://ftp.arl.mil/ftp/pub/ttcp/*) é uma ferramenta simples para o teste de desempenho de rede. Uma instância do programa roda em cada lado do link que você quer testar. O primeiro nó roda em modo de recepção e o outro em transmissão:

```
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
```

Depois de coletar os dados em uma direção, você deve reverter os parceiros de transmissão e recepção no link, testando na direção oposta. Ele

pode testar o fluxo de dados UDP e TCP, podendo alterar vários parâmetros do TCP e tamanhos de buffer para dar um bom exercício à rede. Ele pode também ser alimentado com dados fornecidos pelo usuário, ao invés de enviar dados aleatórios. Lembre-se de que a leitura da velocidade é feita em kilobytes, não em kilobits. Multiplique o resultado por oito para obter a velocidade em kilobits por segundo.

A única desvantagem do ttcp é a de que ele não está sendo desenvolvido por muitos anos. Felizmente, seu código foi tornado de domínio público e ele está livremente disponível. Como o ping e o traceroute, ttcp é encontrado como uma ferramenta padrão em muitos sistemas.

iperf

De forma similar ao ttcp, o ***iperf*** (*http://dast.nlanr.net/Projects/Iperf/*) é uma ferramenta de linha de comando para a estimativa de throughput em uma conexão de rede. Ele suporta muitas das funções do ttcp, mas usa um modelo cliente/servidor ao invés de um par de recepção e transmissão. Para rodar o iperf, execute o servidor em um lado do link e o cliente em outro:

```
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
```

O lado cliente continuará monitorando e aceitando conexões do cliente na porta 5001, até que você pressione as teclas control-C. Isto pode ser útil na execução de múltiplos testes a partir de várias localizações.

A maior diferença entre ttcp e iperf é que este último está em ativo desenvolvimento e tem muitas funcionalidades novas (incluindo o suporte a IPv6). Isto o torna uma boa escolha como ferramenta de performance na construção de novas redes.

bing

Ao invés de inundar uma conexão com dados e ver em quanto tempo a transferência se completa, o ***bing*** (*http://fgouget.free.fr/bing/index-en.shtml*) tenta estimar o throughput disponível em uma conexão ponto-a-ponto através da análise dos tempos de viagem ida-e-volta para pacotes ICMP de vários tamanhos. Mesmo não sendo tão preciso quanto um teste de injeção, ele pode fornecer uma boa estimativa sem a transmissão de um grande número de bytes.

Como o bing trabalha utilizando pedidos de eco ICMP padrão, ele pode estimar a largura de banda disponível sem a necessidade de que um cliente específico esteja rodando do outro lado da rede. E, como ele usa relativamente pouca largura de banda, o bing pode lhe dar uma idéia estimada do desempenho de sua rede sem a carga que um teste de injeção certamente causaria.

Ferramentas de monitoramento em tempo real

É muito desejável saber quando há tentativas de invasão em sua rede ou quando alguma parte dela apresenta problemas. Como nenhum administrador de sistema pode observar toda a rede em todo o tempo, existem programas que fazem o constante monitoramento do estado da rede, enviando alertas quando eventos importantes ocorrem. A seguir, algumas ferramentas de código aberto que ajudarão a realizar esta tarefa.

Snort

Snort (*http://www.snort.org/)* é um espião (*sniffer*) de pacotes e registrador (*logger*) que pode ser usado como um sistema leve para a detecção de intrusos. Ele tem a capacidade de registrar eventos com base em regras e pode executar a análise de protocolo, busca por conteúdo e comparação de pacotes. É usado para detectar uma variedade de ataques e sondagens, como varreduras de portas (*port scans*), ataques CGI, sondas SMB, tentativas de identificação do sistema operacional e muitos outros tipos de padrões anômalos de tráfego. O Snort possui a capacidade de alertas em tempo real, que podem notificar administradores sobre os problemas no momento em que ocorrem, de várias maneiras.

A instalação e execução do Snort não é trivial e, dependendo da quantidade de tráfego na rede, possivelmente irá requerer uma máquina monitora dedicada, com recursos consideráveis. Felizmente, o Snort é muito bem documentado e tem uma forte comunidade de usuários. Ao implementar um conjunto de regras completas para o Snort, você pode identificar comportamentos inesperados que, de outra maneira, poderiam consumir toda a sua largura de banda de Internet.

Veja *http://snort.org/docs/* para uma extensa lista de recursos de instalação e configuração.

Apache: mod_security

ModSecurity (*http://modsecurity.org*) é um mecanismo em código aberto para a detecção e prevenção de intrusão para aplicações web. Este tipo de ferramenta de segurança é também conhecido como firewall para aplicações web. ModSecurity aumenta a segurança das aplicações web, protegendo-as contra ataques conhecidos e desconhecidos. Ele pode ser usado de forma independente ou como um módulo do servidor Apache (*http://www.apache.org/*).

Há muitos recursos para a manutenção das regras do mod_security atualizadas que ajudam a proteger contra as mais recentes características de ataques. Um recurso excelente é o GotRoot, que mantém um imenso, freqüentemente atualizado, repositório de regras:

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

A segurança para aplicações web é importante na defesa de ataques a seu servidor web, que podem resultar no roubo de dados de valor ou pessoais, ou permitir que o servidor seja usado para lançar outros ataques ou ainda enviar spam para outros usuários da Internet. Assim como constituem-se em um dano para a Internet como um todo, tais intrusões também reduzem seriamente sua largura de banda utilizável.

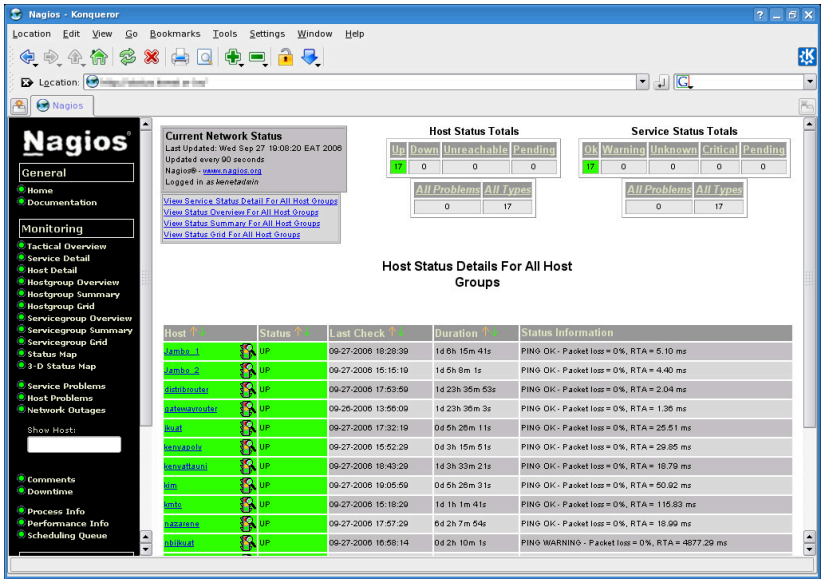


Figura 6.22: O Nagios o informa no momento em que uma falha da rede ou uma queda de serviço ocorrem.

Nagios

Nagios (*http://nagios.org*) é um programa que monitora computadores e serviços em sua rede, notificando-o imediatamente quando surge algum problema. Ele pode enviar notificações por email, SMS ou executar algum script. Estas notificações podem ser enviadas para pessoas ou grupos, de acordo com a natureza do problema. O Nagios pode rodar em Linux ou BSD e fornece uma interface web para exibir o estado atualizado da rede em tempo quase real.

O Nagios é extensível e pode monitorar o estado de praticamente qualquer evento de rede. Ele faz suas verificações através da execução de pequenos scripts em intervalos regulares, comparando-os com a resposta esperada. Isto permite testes muito mais sofisticados do que uma simples sondagem da rede. Por exemplo, o ping (**Página 185**) pode dizer qual máquina está funcionando e conectada à rede, o nmap pode relatar que uma porta TCP responde à solicitações, mas o Nagios pode buscar uma página da web ou acessar uma base de dados, verificando que a resposta não consiste em um erro.

Zabbix

Zabbix (*http://www.zabbix.org/*) é uma ferramenta de monitoramento em tempo real que é quase um híbrido entre o Cacti e o Nagios. Ele usa uma base de dados SQL para o armazenamento de dados, tem seu próprio software para a geração de gráficos e realiza todas as funções que se pode esperar de um monitor moderno, em tempo real (como a checagem de SNMP e a notificação instantânea de condições de erro). O Zabbix é distribuído sob a licença GNU/GPL.

Outras ferramentas úteis

Com freqüência, é muito bom para o entendimento de uma rede mesh ter a capacidade de exibir a topologia da rede de forma gráfica. O plugin olsrd_dot_draw gera a topologia da rede em formato de pontos na porta TCP 2004. As ferramentas graphviz podem então ser usadas para desenhar os gráficos.

Driftnet e Etherpeg

Estas ferramentas decodificam dados gráficos (como arquivos JPEG e GIF), exibindo-os na forma de uma colagem. Como mencionado anteriormente, estas ferramentas são de uso limitado para a análise de problemas, mas são de grande valor para a demonstração da insegurança de protocolos sem criptografia. A Etherpeg pode ser obtida em *http://www.etherpeg.org/* e o Driftnet pode ser baixado de *http://www.ex-parrot.com/~chris/driftnet/*.

Figura 6.23: Uma colagem web gerada pelo Etherpeg.

ngrep

O ***ngrep*** fornece a maior parte dos padrões de comparação do GNU grep, aplicando-os ao tráfego de rede. Atualmente, ele reconhece Ipv4 e IPv6, TCP, UDP, ICMP, IGMP, PPP, SLIP, FDDI, Token Ring e muito mais. Como ele faz uso extensivo de comparações com o uso de expressões regulares, acaba sendo uma ferramenta adequada para usuários mais avançados (ou para aqueles que tenham um bom conhecimento de expressões regulares).

Mas não é necessário ser um especialista em expressões regulares para a utilização básica do ngrep. Por exemplo, para ver todos os pacotes que contém a expressão GET (presumivelmente solicitações HTTP), tente o seguinte:

```
# ngrep -q GET
```

A comparação de padrões pode ser melhorada para que corresponda a protocolos, portas, ou outro critério utilizando filtros BPF. Esta é a linguagem de filtros usada por ferramentas comuns de espionagem (*sniffing*), como o tcpdump e o snoop. Para ver as expressões GET ou POST enviadas para a porta 80, use o seguinte comando:

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

Com o uso criativo do ngrep você pode detectar qualquer coisa, desde atividade de vírus até spam. Você pode baixar o programa do site *http://ngrep.sourceforge.net/*

O que é normal?

Se você está procurando pela resposta definitiva para a forma como deve ser seu padrão de tráfego, você ficará desapontado. Não há resposta certa para esta pergunta mas, com algum trabalho, você poderá determinar o que é o normal para a sua rede. Mesmo que todos os ambientes sejam diferentes, alguns dos fatores que podem influenciar a aparência de seu padrão de rede são:

- A capacidade de sua conexão com a Internet;
- O número de usuários que tem acesso à sua rede;
- A política social (carga de bytes, cotas, meritocracia, etc.);
- A quantidade, tipos e níveis de serviços ofertados;
- A saúde da rede (presença de vírus, broadcasts excessivos, rotas circulares, retransmissão aberta de emails, ataques de negação de serviços, etc.);
- A competência de seus usuários;
- A localização e configuração de estruturas de controle (firewalls, servidores proxy, cache, e outros).

Esta não é uma lista definitiva, mas deve dar uma idéia do quanto são amplos os fatores que podem afetar seus padrões de ocupação de banda. Com isto em mente, vamos observar algumas regras básicas.

Estabelecendo um comportamento básico

Já que cada ambiente é diferente, é necessário que você determine como seus padrões de tráfego devem se parecer em situações normais. Isto é importante, pois permite a você identificar as mudanças com o passar do tempo, sejam elas súbitas ou graduais. Estas mudanças podem indicar um problema ou um potencial problema futuro em sua rede.

Por exemplo, imagine que sua rede chegue a um ponto onde nada funcione e você não sabe qual é a causa. Felizmente, você decidiu, anteriormente, manter um gráfico do tráfego de broadcast como um percentual do tráfego total da rede. Caso este gráfico mostre um súbito aumento do tráfego de broadcast, isto pode significar que sua rede foi infectada por um vírus. Sem uma idéia do que seria o "normal" para a sua rede (um comportamento básico), você não seria capaz de ver que o número de mensagens de broadcast aumentou, mas talvez apenas que ele está "relativamente alto", o que poderia não significar um problema.

Gráficos e números que representam um comportamento básico também são úteis para analisar os efeitos de mudanças feitas na rede. Normalmente, é útil testar estas mudanças, tentando diferentes configurações. O conhecimento do comportamento básico irá mostrar se as mudanças foram para melhor ou para pior.

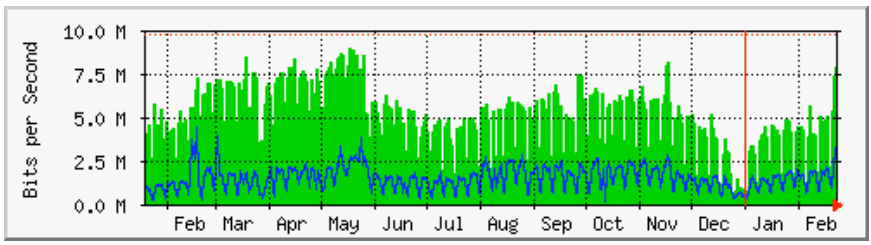


Figura 6.24. Através da coleta de dados em um longo período de tempo, você pode prever o crescimento de sua rede, aplicando mudanças de acordo com a necessidade, antes da ocorrência de problemas.

Na **Figura 6.24** podemos ver o o efeito que a implementação de pesquisas de atrasos causaram na utilização da Internet por volta do mês de maio. Caso não tivéssemos mantido os gráficos de utilização da rede, poderíamos não ter detectado o efeito desta mudança no transcurso do tempo. Ao observar o gráfico completo depois de aplicar mudanças, não assuma que, por falta de mudanças do gráfico, seu esforço foi inútil. Você pode ter removido tráfego inútil de sua rede, que foi então ocupada por tráfego útil. Você pode combinar seu comportamento básico com outros, por exemplo, os 100 sites mais acessados, ou a média de utilização de seus 20 usuários mais ativos, para determinar se os hábitos mudaram. Como veremos adiante, MRTG, RRDtool e Cacti são ferramentas excelentes que você pode usar para manter seu comportamento básico.

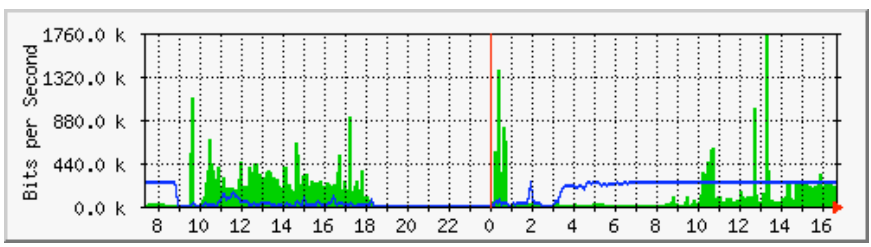


Figura 6.25: O tráfego registrado em um único dia pela Aidworld.

A **Figura 6.25** mostra o tráfego de um firewall Aidworld em um período de 24 horas. Não há nada de errado, aparentemente, com este gráfico, mas os usuários estão reclamando da lentidão no acesso à Internet.

A **Figura 6.26** mostra que o uso da banda para upload (área escura) era maior durante o horário de trabalho no último dia do que nos dias anteriores. O período de upload intenso começou a cada manhã, as três horas da madrugada, e normalmente termina às nove da manhã, mas no último dia ele ainda estava acontecendo até as 16h30. Uma investigação posterior mostrou que o problema estava no programa de cópias de segurança, que deveria terminar as três horas da madrugada, todos os dias.

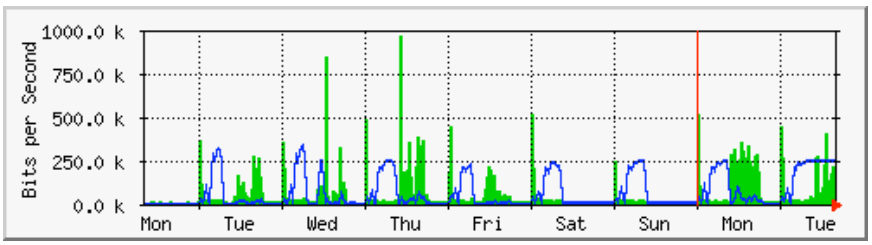


Figura 6.26: O mesmo tráfego de rede registrado durante uma semana inteira revela um problema com as cópias de segurança, que causou congestionamento inesperado para os usuários da rede.

A **Figura 6.27** mostra as medidas de latência da mesma conexão, através do programa SmokePing. A posição dos pontos mostra a latência média, enquanto a fumaça cinza indica a distribuição da latência. As cores dos pontos indicam o número de pacotes perdidos. Este gráfico, exibindo o período de quatro horas, não ajuda na identificação de problemas na rede.

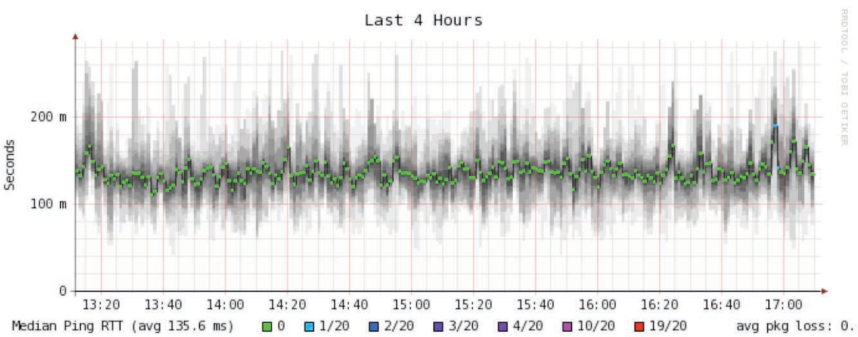


Figura 6.27: Quatro horas de latência e perda de pacotes.

A próxima figura (**Figura 6.28**) mostra os mesmos dados em um período de 16 horas. Isto indica que os valores do gráfico acima estão próximos do nível normal (comportamento básico), mas que há um aumento significativo da latência várias vezes pela manhã (cerca de 30 vezes o valor observado no

comportamento básico). Em função disto, conclui-se que uma atenção adicional deve ser dada a estes períodos matinais a fim de estabelecer a causa da alta latência, que provavelmente é causada por algum alto volume de tráfego qualquer.

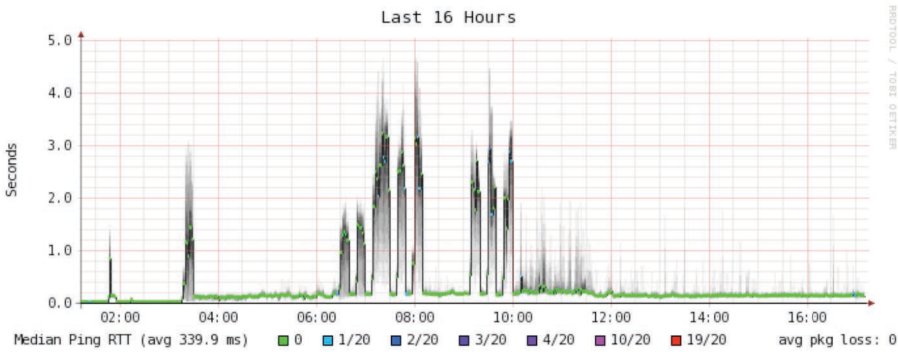


Figura 6.28: Um espalhamento maior de latência revela-se em um registro de 16 horas.

A **Figura 6.29** mostra que a terça-feira foi, de forma significativa, pior que o domingo ou segunda-feira em termos de latência, especialmente no período da manhã. Isto pode indicar que algo mudou na rede.

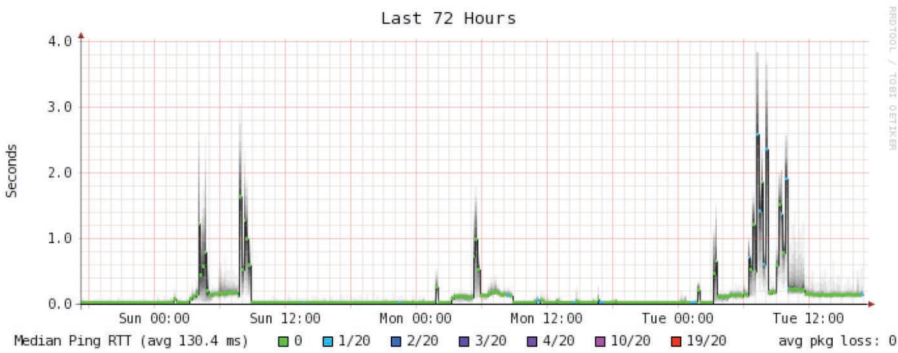


Figura 6.29: Na visão da semana, evidencia-se a repetição do aumento de latência causada pela perda de pacotes nas primeiras horas da manhã.

Como interpreto o gráfico de tráfego?

Em um gráfico básico de fluxo da rede (como o que é gerado pelo monitor de rede MRTG), a área verde representa o ***tráfego de entrada*** e a linha azul indica o ***tráfego de saída***. O tráfego de entrada é aquele originado de uma rede externa (tipicamente a Internet) e é endereçado a algum computador dentro de sua rede. O tráfego de saída é o originado em sua rede e endereçado a algum computador em qualquer lugar da Internet. Dependendo de seu ambiente, o gráfico o ajudará a entender como sua rede está sendo usada. Por exemplo, o

monitoramento de servidores apresentará uma grande quantidade de tráfego de saída, já que servidores atendem pedidos (como enviar emails ou apresentar páginas web), enquanto o monitoramento de máquinas clientes pode revelar quantidades maiores de tráfego de entrada, uma vez que estas recebem os dados dos servidores.

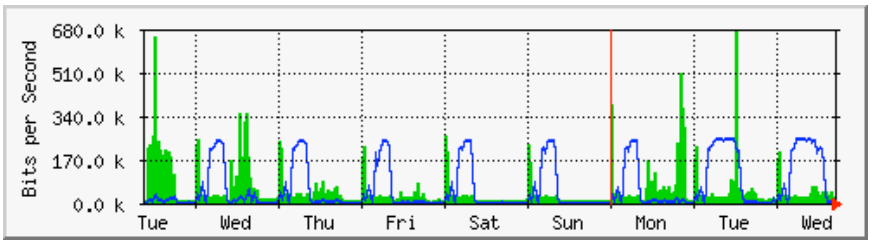


Figura 6.30: O gráfico clássico de tráfego em uma rede. A área escura representa o tráfego de entrada, enquanto a linha representa o tráfego de saída. Os arcos repetidos de tráfego de saída representam os momentos onde foram feitas as cópias de segurança.

Os padrões de tráfego variam com o que está sendo monitorado. Um roteador irá mostrar mais tráfego de entrada do que de saída, já que os usuários baixam arquivos da Internet. Um excesso de tráfego de saída que não é originado de seus servidores pode indicar um cliente P2P (Kazaa e outros), um servidor não autorizado ou mesmo um vírus em um ou mais de seus clientes. Não há uma métrica estabelecida que diga como deve se parecer a relação entre o tráfego de entrada e o de saída. Você deve estabelecer o comportamento básico para entender qual deve ser o padrão de tráfego em sua rede.

Detectando sobrecarga na rede

A **Figura 6.31** mostra o gráfico de uma conexão sobrecarregada à Internet.

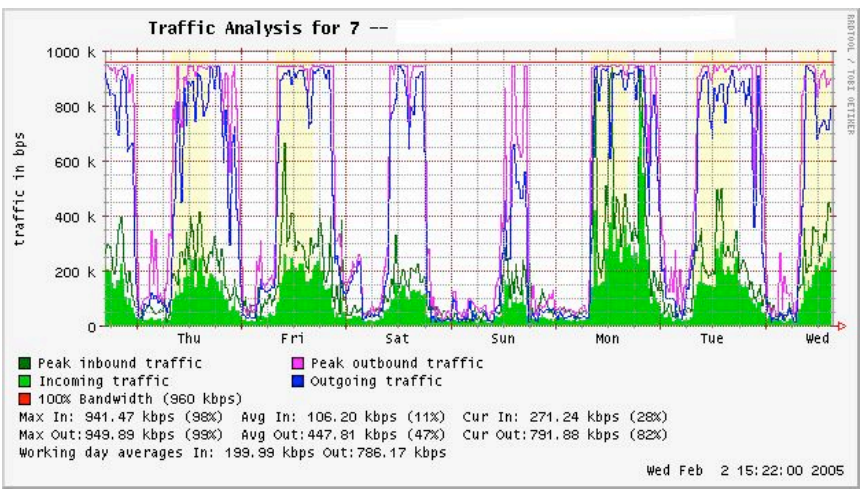


Figura 6.31: Um gráfico com linhas planas em seu topo indica que o link está consumindo a totalidade da largura de banda, sendo super utilizado nestes períodos.

O sinal mais visível de sobrecarga são as linhas planas no topo do gráfico que representam o tráfego de saída no meio de cada dia. Estas linhas planas indicam sobrecarga, mesmo que estejam abaixo da capacidade teórica do link. Neste caso, isto pode significar que você não está recebendo a largura de banda que você espera de seu provedor.

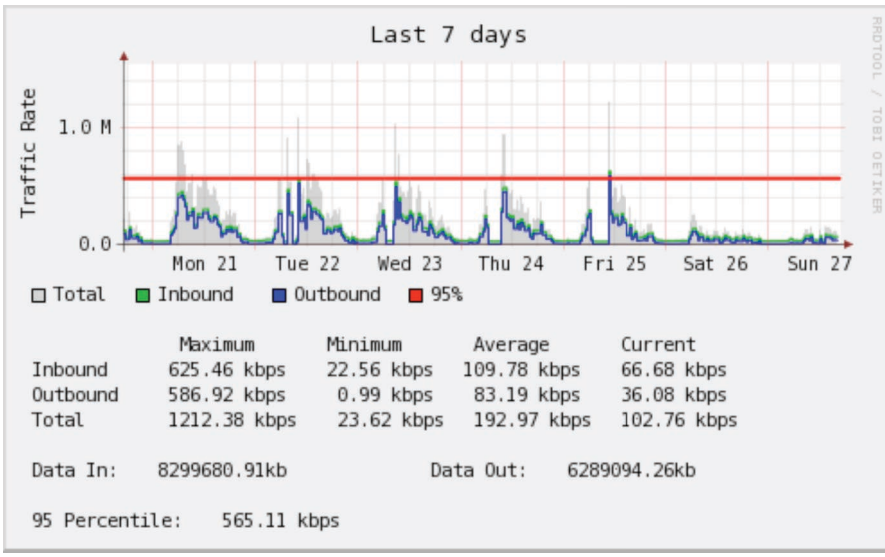


Figura 6.32: A linha horizontal mostra o valor do 95° percentil.

Medindo o percentil 95°

O percentil 95° é amplamente usado em cálculos matemáticos para avaliar a utilização regular e sustentável de um conduto de rede. Seu valor mostra o máximo consumo de tráfego por um período de tempo. O cálculo do 95° percentil mostra que 95% do tempo o uso está abaixo de um certo valor, e 5% do tempo está acima deste valor. O 95° percentil é um bom valor para demonstrar que a rede é realmente utilizada, ao menos 95% do tempo.

Tanto o MRTG quanto o Cacti calculam o 95° percentil para você. Este é um gráfico exemplo que representa uma conexão de 960 kbps. O 95° percentil está em 945 kbps, depois do descarte do tráfego alto de 5%.

Monitorando memória e uso de CPU

Por definição, servidores fornecem serviços críticos que devem estar constantemente disponíveis. Os servidores recebem pedidos de máquinas clientes e os atendem, provendo acesso a serviços que são a razão principal de se ter uma rede. Por isso, servidores devem ter capacidade suficiente de hardware para acomodar a carga de trabalho. Isto significa ter a quantidade adequada de memória RAM, armazenamento em disco e capacidade de processamento que permitam atender aos pedidos vindos das máquinas clientes. De outra forma, o servidor pode demorar muito tempo para responder ou, na pior das hipóteses, ser incapaz de responder. Já que recursos de

hardware são finitos, é importante monitorar como os recursos do sistema são utilizados. Se um servidor principal (como um proxy ou servidor de email) está sobrecarregado de pedidos, os tempos de acesso tornam-se longos. Isto é freqüentemente percebido pelos usuários como um problema na rede.

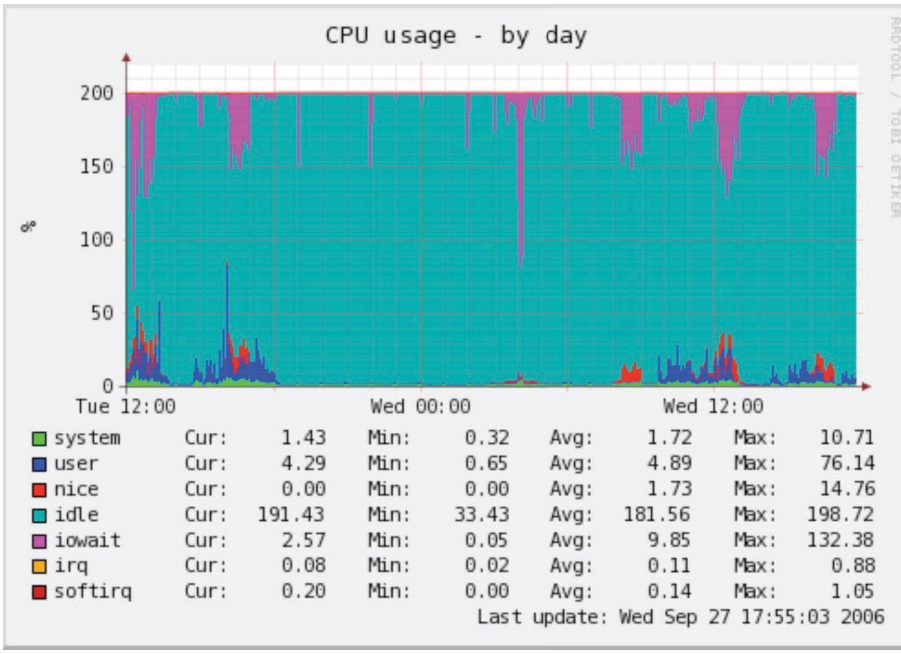


Figura 6.33: RRDtool pode exibir dados arbitrários, como o uso de CPU e memória, expressos em uma média no tempo.

Há muitos programas que podem ser usados para monitorar os recursos de um servidor. O método mais simples, em uma máquina Windows, é acessar o Gerenciador de Tarefas usando a combinação de teclas **`Ctrl + Alt + Del`** e então selecionar a aba Desempenho (ou Performance). Em uma máquina Linux ou BSD, você pode digitar ***top*** em uma janela de terminal. Para manter registros históricos deste desempenho, MRTG ou RRDtool (**Página 190**) podem também ser usados.

Os servidores de email devem ter espaço em disco suficiente, já que algumas pessoas podem preferir deixar suas mensagens nele por longos períodos de tempo. As mensagens podem acumular e encher o disco, especialmente se um sistema de quotas não estiver sendo usado. Caso o disco ou o espaço disponível na partição utilizada para armazenamento de email esteja completamente ocupado, o servidor não poderá receber emails. Se este disco for também usado pelo sistema, todo o tipo de problema pode ocorrer se o sistema operacional ficar sem espaço para memória temporária.

Servidores de arquivo precisam ser monitorados mesmo quando possuem discos de alta capacidade. Os usuários encontrarão meios de ocupar toda a capacidade de discos de qualquer tamanho muito mais rápido do que você

imagina. O uso de espaço em disco pode ser limitado pelo uso de quotas, ou simplesmente monitorado, avisando as pessoas quando elas estão ocupando muito espaço. O Nagios (**Página 200**) pode notificá-lo quando o espaço em disco, a utilização de CPU ou outros recursos do sistema passam de um limite crítico.

Caso uma máquina deixe de responder ou torne-se muito lenta e as medidas mostram que algum recurso do sistema está sendo muito utilizado, esta pode ser uma indicação de que uma ampliação de capacidade é necessária. Se o uso do processador constantemente excede 60% do total, pode ser a hora de trocá-lo por outro mais potente. Velocidades baixas podem ser também o resultado de memória insuficiente. Certifique-se de verificar o uso geral de CPU, RAM e espaço em disco antes de tomar a decisão de atualizar algum componente.

Uma maneira simples de verificar se a máquina está com memória insuficiente é observar a luz do disco rígido. Quando ela permanece ligada com certa freqüência, isto normalmente significa que a máquina está constantemente paginando espaços de memória para o disco rígido. Isto é chamado de thrashing e é extremamente ruim para o desempenho do sistema. Isto pode ser corrigido com a investigação de qual processo está utilizando mais memória, terminando-o ou reconfigurando-o. Caso isto não funcione, o sistema precisa de mais memória RAM.

Você sempre deve verificar se é mais econômico atualizar um componente individual ou adquirir uma nova máquina. Alguns computadores são difíceis ou mesmo impossíveis de serem atualizados, e freqüentemente sai mais cara a substituição de componentes individuais do que a de todo o computador. Uma vez que a disponibilidade de componentes e sistemas varia bastante nos muitos locais do mundo, além de comparar o custo de componentes e de um novo sistema, você deve incluir custos de transporte e taxas alfandegárias para poder determinar o custo real de uma atualização.

7
Energia solar

Este capítulo é uma introdução aos componentes de um ***sistema fotovoltaico independente***. A palavra independente refere-se ao fato de que o sistema trabalha sem a conexão a uma rede já estabelecida de energia elétrica. Neste capítulo vamos apresentar os conceitos básicos da geração e armazenamento de energia solar fotovoltaica. Também forneceremos um método para o projeto de um sistema solar, mesmo onde existe acesso limitado a informação e recursos.

Discutiremos aqui apenas o uso da energia solar na produção direta de eletricidade (***energia solar fotovoltaica***). A energia solar pode também ser usada para aquecer fluidos (***energia solar térmica***) que podem tanto ser usados como fonte de calor como para alimentar uma turbina que irá gerar eletricidade. A energia solar térmica está além do escopo deste capítulo.

Energia solar

Um sistema fotovoltaico está baseado na habilidade de certos materiais em converter a energia irradiada pelo sol em energia elétrica. A quantidade de energia solar que ilumina uma determinada área é chamada de ***irradiação*** (***G***) e é medida em ***watts por metro quadrado*** (***W/m²***). Os valores desta medida são, normalmente, a média de um período de tempo, assim é comum falar sobre a irradiação total por hora, dia ou mês.

Claro que a quantidade precisa de radiação que chega à superfície da Terra não pode ser prevista com alta precisão, devido à variação das condições do tempo. Por isto é necessário trabalhar com dados estatísticos baseados no "histórico solar" de um lugar em particular. Estes dados são coletados por uma estação meteorológica em um longo período de tempo e estão disponíveis de várias formas, como tabelas ou bases de dados. Na maioria dos casos, pode ser difícil de encontrar informação detalhada sobre uma determinada área, necessitando que você trabalhe com valores aproximados.

Algumas organizações produziram mapas que apresentam médias de irradiação global para diferentes regiões. Estes valores são conhecidos como ***horas de pico de sol*** (*peak sun hours*) ou ***PSH***s. Você pode usar o valor do PSH de sua região para simplificar seus cálculos. Uma unidade de "pico de sol"

corresponde à radiação de 1000 Watts por metro quadrado. Se verificamos que uma determinada área tem 4 PSH no pior mês, sabemos que em tal mês não devemos esperar uma irradiação diária maior que 4000 W/m^2 (por dia). Horas de pico de sol são uma maneira fácil de representar a média do pior caso de irradiação por dia.

Mapas PSH de baixa resolução estão disponíveis em várias fontes online, como *http://www.solar4power.com/solar-power-global-maps.html* ou *http://eosweb.larc.nasa.gov/cgi-bin/sse/sse.cgi?+s01+s03#s01.* Para mais informações, consulte um fornecedor de energia solar ou uma estação meteorológica.

E sobre energia eólica?

É possível usar um gerador eólico ao invés de painéis solares quando um sistema autônomo é projetado para a instalação em uma colina ou montanha. Para que isto funcione, a velocidade média do vento deve ser de ao menos 3 a 4 metros por segundo e o gerador eólico deve estar 6 metros mais alto que qualquer outro objeto em um raio de 100 metros. Uma localidade longe do litoral geralmente não tem ventos suficientes para suportar um sistema eólico de produção de energia.

De maneira geral, sistemas fotovoltaicos são mais confiáveis que sistemas eólicos, já que a luz solar está disponível de forma mais consistente do que o vento na maioria dos lugares. Por outro lado, geradores eólicos podem carregar baterias mesmo à noite, desde que haja vento suficiente. Claro que é possível usar geradores eólicos e solares em conjunto, auxiliando na cobertura de tempos quando há muitas nuvens ou quando não há vento suficiente.

Para a maioria das localidades, o custo de um gerador eólico não se justifica, considerando a quantidade de potência que ele irá agregar ao sistema completo. Este capítulo irá, portanto, focar-se no uso de painéis solares para a geração de eletricidade.

Componentes de sistemas fotovoltaicos

Um sistema fotovoltaico básico é composto de quatro componentes principais: o ***painel solar***, as ***baterias***, o ***regulador*** e a ***carga***. Os painéis são responsáveis por coletar a energia solar e gerar eletricidade. A bateria armazena a energia para uso posterior. O regulador garante que o painel e a bateria estão trabalhando em conjunto da melhor forma possível. A carga é qualquer dispositivo que necessita de energia elétrica e é a soma do consumo de energia de todos os equipamentos conectados ao sistema. É importante lembrar que os painéis solares e baterias usam ***corrente contínua*** (***DC*** – *direct current*).

Caso os níveis operacionais de voltagem de seu equipamento não sejam compatíveis com o que é fornecido pela bateria, você precisará incluir também algum tipo de ***conversor***. Se o equipamento que você pretende ligar usa uma voltagem de corrente contínua diferente da fornecida pela bateria, você precisará de um ***conversor DC/DC***. Se algum equipamento requerer corrente alternada, você precisará de um ***conversor DC/AC***, também conhecido como ***inversor***.

Todo sistema elétrico deve incorporar também dispositivos de segurança, para a eventualidade de alguma coisa dar errado. Estes dispositivos incluem o

cabeamento apropriado, disjuntores, fusíveis, barras de aterramento, supressores de raios e outros.

O painel solar

O ***painel solar*** é composto de células solares que coletam a energia solar, transformando-a em energia elétrica. Esta parte do sistema é comumente chamada de ***módulo solar*** ou ***gerador fotovoltaico***. ***Matrizes de painéis*** solares podem ser feitas através da conexão de uma série de painéis em série ou em paralelo a fim de prover a energia necessária para uma determinada carga. A corrente elétrica fornecida por um painel solar varia de acordo com a radiação solar, que muda de acordo com as condições climáticas, a hora do dia e a época do ano.

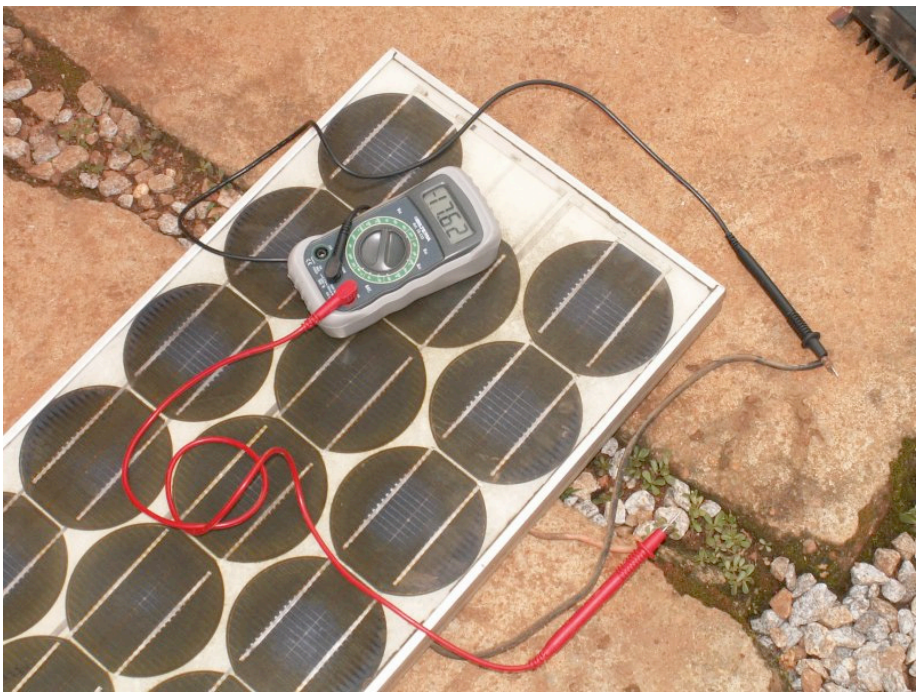


Figura 7.1: Um painel solar.

Muitas tecnologias são usadas na fabricação de células solares. A mais comum é a de cristal de silício, que pode ser tanto monocristalino como policristalino. Silício amorfo pode ser mais barato, mas é menos eficiente na conversão de energia solar em eletricidade. Com uma expectativa de vida pequena e uma eficiência de apenas 6 a 8% de transformação de energia, silício amorfo é tipicamente usado em equipamentos de baixo consumo de potência, como calculadoras portáteis. Novas tecnologias solares, como fitas de silício e finos filmes fotovoltaicos, estão em desenvolvimento. Estas tecnologias prometem níveis mais altos de eficiência, mas ainda não estão disponíveis em larga escala.

A bateria

A ***bateria***, também chamada de ***acumulador***, armazena a energia produzida pelos painéis que não é imediatamente consumida pela carga. A energia armazenada pode ser usada em períodos de pouca irradiação solar. Baterias armazenam eletricidade na forma de energia química. O tipo mais comum de bateria usada em aplicações solares é a ***bateria selada de chumbo-ácido***, também chamada de ***recombinante*** ou ***VLRA*** (*valve regulated lead acid* – ***chumbo-ácido regulada por válvula***).

Figura 7.2: Uma bateria de chumbo-ácido de 200 Ah. O terminal negativo está quebrado por causa do peso em cima do mesmo durante o transporte.

Além de armazenar energia, baterias seladas de chumbo-ácido ainda prestam-se a duas importantes funções:

- Elas são capazes de fornecer potência instantânea superior à que pode ser gerada pelos painéis solares. Esta potência instantânea é necessária para dar a partida em alguns dispositivos, como o motor de uma geladeira ou uma bomba.
- Elas determinam a voltagem operacional de sua instalação.

Para instalações de pequena potência, ou onde limites de espaço devem ser considerados, outros tipos de baterias (como as de NiCd, MiMh ou Li-ion) podem ser usadas. Estes tipos de bateria requerem um carregador/regulador apropriado e não podem substituir diretamente baterias de chumbo-ácido.

O regulador

O ***regulador*** (mais formalmente, o ***regulador de carga de potência solar***) garante que a bateria está funcionando em condições apropriadas. Ele evita a

sobrecarga ou a descarga excessiva da bateria, condições que reduzem a vida útil da mesma. Para garantir a carga e descarga apropriada da bateria, o regulador mantém o registro do ***estado de carga*** (*State of Charge* – ***SoC***) da bateria. O SoC é estimado com base na voltagem real da bateria. Através da medida desta voltagem e do conhecimento da tecnologia de armazenamento usada pela bateria, o regulador pode saber os pontos precisos nos quais a bateria pode estar sobrecarregada ou excessivamente descarregada.

Figura 7.3: Um controlador de carga solar de 30 Amp.

O regulador pode incluir outras funcionalidades que adicionam informação e controle de segurança ao equipamento. Estas funcionalidades incluem amperímetros, voltímetros, medidas de ampere-hora, temporizadores, alarmes, etc. Mesmo que sejam convenientes, nenhuma destas funções são requisitos para o funcionamento de um sistema fotovoltaico.

O conversor

A eletricidade fornecida pelo painel solar e a bateria é de corrente contínua, com uma voltagem fixa. Tal voltagem pode não ser a mesma que a requerida pela sua carga. Um ***conversor de corrente contínua para alternada*** (***DC/AC***), também conhecido como ***inversor*** pode ser necessário. Você também pode precisar de conversores que apenas modifiquem a voltagem de corrente contínua fornecida pelo sistema: ***conversores DC/DC***. Toda a conversão implica em alguma perda de energia. Para a ótima operação, você deve projetar seu sistema de energia solar para que produza a voltagem DC igual à requerida pela carga.

Figura 7.4: Um conversor DC/AC (inversor) de 800 Watts.

A carga

A ***carga*** é o equipamento que consome a potência gerada por seu sistema de energia. A carga pode incluir equipamentos wireless, roteadores, lâmpadas, aparelhos de TV, modems VSAT, etc. Mesmo não sendo possível calcular precisamente o consumo total de seu equipamento, é de vital importância a sua boa estimativa. Neste tipo de sistema é absolutamente necessário o uso de equipamentos eficientes e de baixo consumo, para evitar o desperdício de energia.

Colocando tudo junto

O sistema fotovoltaico completo incorpora todos estes componentes. O painel solar gera eletricidade quando a energia solar está disponível. O regulador garante a mais eficiente operação do painel e previne danos às baterias. O banco de baterias armazena a energia coletada para uso posterior. Conversores e inversores adequam a energia armazenada à requerida pela sua carga. Finalmente, a carga consome a energia armazenada para seu funcionamento. Quando todos os equipamentos estão balanceados e mantidos apropriadamente, o sistema funcionará de forma independente durante vários anos.

Agora examinaremos os componentes individuais do sistema fotovoltaico em maior detalhe.

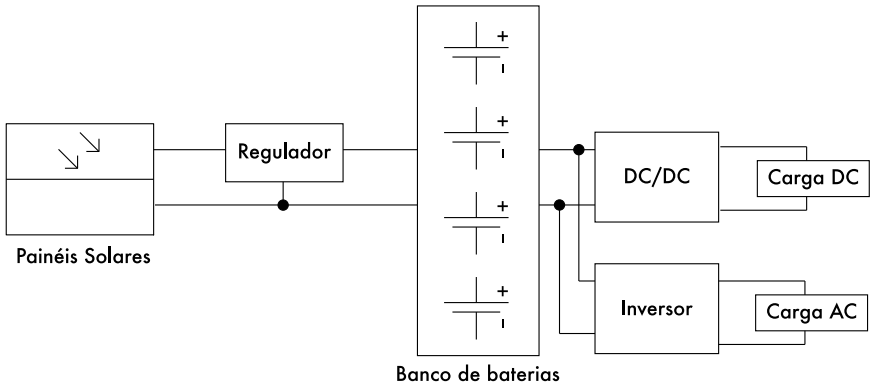


Figura 7.5: Uma instalação solar com cargas AC e DC.

O painel solar

Um único painel solar é composto de muitas células solares. As células são conectadas eletricamente para fornecer uma determinada corrente e voltagem. As células individuais são devidamente encapsuladas para seu isolamento e proteção contra umidade e corrosão.

Figura 7.6: O efeito da água e corrosão em um painel solar.

Há diversos tipos de módulos no mercado, dependendo da demanda de potência de sua aplicação. Os módulos mais comuns são compostos de 32 ou 36 células solares de cristal de silício. Estas células são todas de igual tamanho, conectadas em série e encapsuladas entre vidro e material plástico, usando uma resina de polímero (EVA) como isolante térmico. A área de superfície do módulo varia normalmente entre 0,1 e 0,5 m^2. Painéis solares têm, usualmente, dois contatos elétricos, um positivo e outro negativo.

Alguns painéis também incluem contatos extra que permitem a instalação de ***diodos de passagem*** entre células individuais. Diodos de passagem protegem o painel de um fenômeno conhecido como "*hot-spots*" (***pontos quentes***). Um hot-spot acontece quando algumas células estão na sombra, enquanto o resto do painel está totalmente iluminado pelo sol. Ao invés de produzir energia, as células que estão na sombra comportam-se como uma carga, consumindo-a e transformando-a em calor. Nesta situação, sua temperatura pode ficar entre 85 e 100°C. Diodos de passagem previnem hot-spots em células sombreadas, mas reduzem a voltagem máxima do painel. Eles devem ser apenas usados quando sombras são inevitáveis. Sempre que possível, é melhor buscar a exposição de todo o painel à luz do sol.

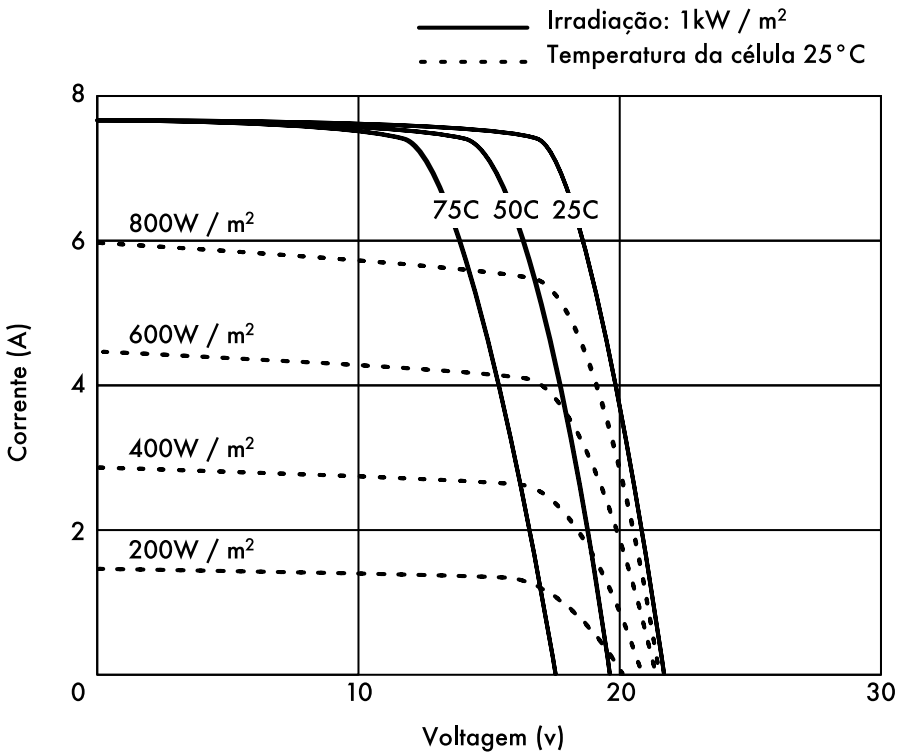


Figura 7.7: Diferentes curvas de corrente e tensão (curvas IV). A corrente (A) muda com a irradiação e a tensão (V) muda com a temperatura.

O desempenho de um módulo solar é representado pela curva de característica IV (corrente e tensão) que representa qual corrente é fornecida em função da voltagem gerada por certa irradiação solar.

Parâmetros do painel solar

Os principais parâmetros que caracterizam um painel fotovoltaico são:

1. **Corrente de curto circuito** (I_{SC}): a máxima corrente fornecida pelo painel quando seus conectores são colocados em curto circuito.

2. **Voltagem de circuito aberto** (V_{OC}): a máxima voltagem que o painel fornece quando seus terminais não estão conectados à carga alguma (circuito aberto). Este valor é normalmente de 22 V para painéis que trabalharão em sistemas de 12 V, e é diretamente proporcional ao número de células conectadas em série.

3. **Máximo ponto de potência** (P_{max}): é o ponto onde a potência fornecida pelo painel atinge seu valor máximo, onde $P_{max} = I_{max} \times V_{max}$. O máximo ponto de potência do painel é medido em Watts (W) ou Watts de pico (W_p). É sempre importante lembrar que em condições normais o painel não irá operar em condições de pico, já que a voltagem de operação é mantida fixa pelo regulador. Valores típicos de V_{max} e I_{max} devem ser um pouco menores que I_{SC} e V_{OC}.

4. **Fator de preenchimento** (FF): é a relação entre a máxima potência que o painel realmente pode fornecer e o produto $I_{SC} \times V_{OC}$. Isto dá uma idéia da qualidade do painel, uma vez que esta é uma indicação da característica da curva IV. Quanto mais próximo de 1 for o valor de FF, mais potência o painel pode fornecer. Valores típicos estão entre 0,7 e 0,8.

5. **Eficiência** (h): é a razão entre a máxima potência elétrica que o painel pode fornecer a uma carga e a potência da radiação solar (P_L) que incide no painel. Isto varia, normalmente, entre 10 e 12%, dependendo do tipo de células (monocristalina, policristalina, amorfa ou filme fino).

Considerando as definições do ponto de máxima potência e o fator de preenchimento vemos que:

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

Os valores I_{SC}, V_{OC}, I_{Pmax} y V_{Pmax} são fornecidos pelo fabricante e referem-se a condições padrão de medida com irradiação G = 1000 W/m^2, ao nível do mar, para uma temperatura de Tc = 25°C das células.

Os valores dos parâmetros do painel variam para outras condições de irradiação e temperatura. Algumas vezes os fabricantes podem incluir gráficos o tabelas com os valores para condições diferentes dos padrões. Você deve procurar verificar os valores das temperaturas no painel que mais se aproximam de sua instalação em particular.

Esteja ciente de que dois painéis podem ter a mesma W_p, mas comportamento muito diferente em condições operacionais diversas. Quando adquirir um painel, é importante verificar, quando possível, que seus parâmetros (ao menos I_{SC} e V_{OC}) estão de acordo com os prometidos pelo fabricante.

Parâmetros do painel para o dimensionamento do sistema

Para calcular o número de painéis necessários para cobrir uma determinada carga, você precisa saber apenas a corrente e a voltagem no ponto de máxima potência: I_{Pmax} e V_{Pmax}.

Você deve estar sempre ciente de que o painel não irá desempenhar sob perfeitas condições, já que a carga ou o sistema regulador não estarão, constantemente, trabalhando no ponto de máxima potência de seu painel. Assuma uma perda de eficiência de 5% em seus cálculos para compensar isto.

Interconexão de painéis

Uma ***matriz de painéis solares*** é uma coleção de painéis eletricamente interconectados e instalados em algum tipo de estrutura de suporte. O uso de uma matriz de painéis solares permite que você gere tensões e correntes maiores do que as que seriam possíveis com um único painel. Os painéis são interconectados de forma a que a voltagem gerada seja próxima (mas maior que) o nível de voltagem das baterias e que a corrente gerada seja suficiente para alimentar o equipamento e carregar as baterias.

A conexão de painéis solares em série aumenta a voltagem gerada. A conexão em paralelo aumenta a corrente. O número de painéis utilizados deve ser aumentado até que a quantidade de potência gerada supere levemente a demanda de sua carga.

É muito importante que todos os painéis em sua matriz sejam os mais idênticos possíveis. Em uma matriz você deve usar painéis da mesma marca e de mesmas características, uma vez que qualquer diferença em suas condições operacionais irá provocar um grande impacto no desempenho e na saúde de seu sistema. Mesmo painéis que possuem medidas de desempenho idênticas irão apresentar, normalmente, alguma variação em suas características devido ao processo de manufatura. As mesmas características operacionais de dois painéis do mesmo fabricante podem variar até cerca de 10%.

Sempre que possível, é bom testar o desempenho real de painéis individuais para verificar suas características operacionais antes de montá-los em uma matriz.

Como escolher um bom painel

Uma métrica óbvia, usada na compra de um painel solar, é a comparação da potência nominal de pico (W_p) com o preço. Isto lhe dará uma idéia básica do custo por Watt em diferentes painéis. Mas há uma série de considerações que você também deve manter em mente.

Se você for instalar um painel solar em uma área onde partículas em suspensão no ar (de poeira, areia ou grãos) podem ser um problema, considere a aquisição de painéis com baixa afinidade para a retenção de poeira. Estes painéis são feitos de material que aumentam a possibilidade dele ser limpo automaticamente pelo vento ou chuva.

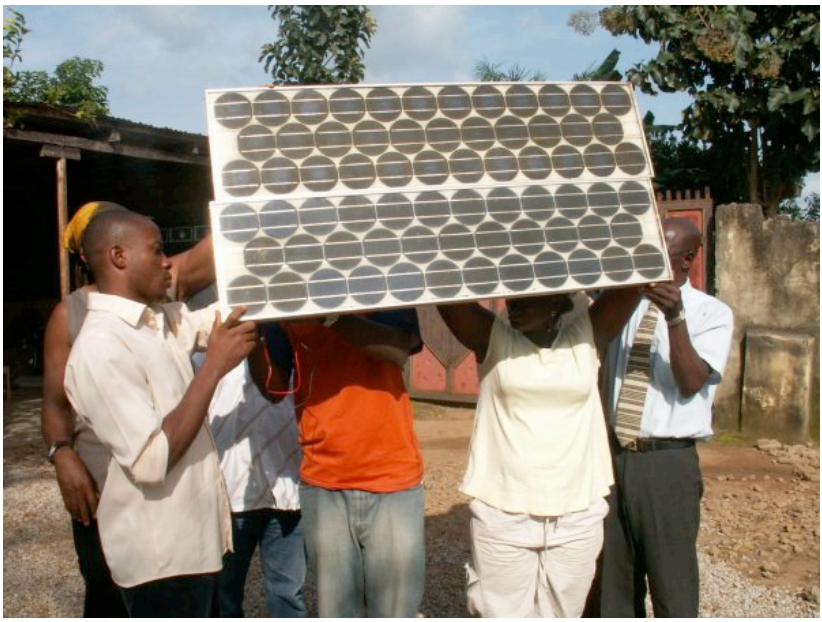


Figura 7.8: Interconexão de painéis em paralelo. A voltagem permanece a mesma, enquanto a corrente duplica (Foto: Fundação Fantsuam, Nigéria).

Sempre verifique a construção mecânica de cada painel. O vidro deve ser endurecido e a moldura de alumínio robusta e bem construída. As células solares dentro do painel podem durar mais de 20 anos mas elas são muito frágeis, cabendo ao painel protegê-las de ações mecânicas que podem prejudicá-las. Procure na garantia de qualidade por termos que mencionam a potência esperada de saída e dados sobre a construção mecânica.

Finalmente, certifique-se de que o fabricante não fornece apenas a potência nominal de pico do painel (W_p) mas também a variação da potência em função da irradiação e da temperatura. Isto é particularmente importante quando os painéis forem usados em matrizes, já que variações nos parâmetros operacionais podem ser de grande impacto na qualidade da potência gerada e no tempo de vida útil dos painéis.

A bateria

A bateria é o local onde acontece um tipo de reação química reversível capaz de armazenar energia elétrica, que pode ser posteriormente utilizada. A energia elétrica é transformada em energia química quando a bateria é carregada e o reverso acontece quando a bateria é descarregada.

Uma bateria é formada por um conjunto de elementos ou ***células*** organizadas em série. Baterias de chumbo-ácido consistem de dois eletrodos de chumbo imersos em uma solução eletrolítica de água e ácido sulfúrico. Existe uma diferença de potencial de cerca de 2 volts entre os eletrodos, dependendo do estado de carga da bateria. As baterias mais comuns para aplicações solares

fotovoltaicas tem uma voltagem nominal de 12 ou 24 volts. Uma bateria de 12 V possui, então, seis células em série.

A bateria tem dois propósitos importantes em um sistema fotovoltaico: fornecer energia elétrica para o sistema quando o mesmo não está sendo suprido pela matriz de painéis solares e armazenar a energia produzida em excesso pelos painéis, sempre que ela for maior que a consumida pela carga. A bateria passa por um processo cíclico de carga e descarga, dependendo da presença ou ausência da luz do sol. Durante as horas em que a luz do sol está presente, a matriz de painéis produz energia. A energia que não é imediatamente consumida é usada para carregar a bateria. Na ausência de luz solar, qualquer demanda de energia é suprida pela bateria, descarregando-a.

Estes ciclos de carga e descarga ocorrem sempre que a energia produzida pelos painéis não condiz com a requerida para o suporte à carga. Quando existe luz do sol suficiente e a carga é pequena, as baterias irão carregar. Obviamente, as baterias irão descarregar à noite, sempre que qualquer potência for requerida. As baterias também irão descarregar quando a irradiação for insuficiente para atender aos requerimentos da carga (devido à variações climáticas naturais, nuvens, poeira, etc).

Caso a bateria não armazene energia suficiente para atender a demanda nos períodos sem iluminação, o sistema esgotará seus recursos e ficará indisponível para o uso. Por outro lado, o superdimensionamento do sistema (adicionando muitos painéis e baterias) é caro e ineficiente. Quando projetamos um sistema independente devemos estabelecer um compromisso entre o custo de seus componentes e a disponibilidade de potência para o sistema. Uma forma de fazer isto é estimar a necessidade de ***número de dias de autonomia***. No caso de um sistema de telecomunicações, o número de dias de autonomia depende da criticidade de sua função dentro de seu projeto de rede. Se o equipamento for um repetidor e é parte da espinha dorsal de sua rede, você irá desejar que o sistema fotovoltaico tenha uma autonomia entre cinco e sete dias. Por outro lado, se o sistema solar for responsável por prover energia a um equipamento cliente, você provavelmente poderá reduzir os dias de autonomia para dois ou três. Em áreas de baixa irradiação este valor pode necessitar ser aumentado ainda mais. De qualquer forma, você sempre deve encontrar o equilíbrio entre o custo e a confiabilidade.

Tipos de baterias

Há muitas tecnologias diferentes para baterias, prestando-se ao uso em uma variedade de aplicações. O tipo que melhor serve a aplicações fotovoltaicas é a ***bateria estacionária***, projetada para ficar em um local fixo e em cenários onde o consumo de potência é mais ou menos irregular. Baterias estacionárias podem acomodar grandes ciclos de descarga, mas não são projetadas para produzir altas correntes por períodos curtos de tempo.

As baterias estacionárias podem usar um eletrólito alcalino (como as de níquel-cádmio) ou ácido (como as de chumbo-ácido). Sempre que possível, as de níquel-cádmio são recomendadas por sua alta confiabilidade e resistência. Infelizmente, elas tendem a ser muito mais caras e difíceis de obter do que as baterias seladas de chumbo-ácido.

Em muitos casos, quando for difícil encontrar localmente baterias estacionárias (a importação de baterias não é barata), você será forçado a utilizar baterias projetadas para o mercado automobilístico.

Usando baterias de automóveis

As baterias de automóveis não são as que melhor se prestam para aplicações fotovoltaicas, uma vez que são projetadas para fornecer uma corrente substancial por apenas alguns segundos (na partida do motor) ao invés de manter uma corrente baixa por um longo período de tempo. Esta característica de projeto das baterias de automóvel (também chamadas de ***baterias de tração***) resulta em um tempo de vida útil menor quando de sua utilização em sistemas fotovoltaicos. Baterias de tração podem ser usadas em aplicações pequenas, onde o custo é a consideração mais importante, ou quando outras baterias não estiverem disponíveis.

Baterias de tração são projetadas para veículos e carrinhos de mão motorizados. Elas são mais baratas que baterias estacionárias e podem servir para instalações fotovoltaicas, apesar de necessitarem, neste caso, de manutenção muito mais freqüente. Estas baterias nunca devem ser profundamente descarregadas porque isto reduz bastante a habilidade das mesmas de manterem uma carga. Uma bateria de caminhão nunca deve descarregar mais do que 70% de sua capacidade total. Isto significa que você pode usar um máximo de 30% da capacidade nominal de uma bateria de chumbo-ácido antes dela necessitar de recarga.

Você pode estender a vida de uma bateria de chumbo-ácido usando água destilada. Usando um densímetro ou hidrômetro você pode medir a densidade do eletrólito da bateria. Uma bateria típica tem a gravidade específica de 1,28. A adição de água destilada, baixando a densidade para 1,2, auxilia na redução da corrosão do ânodo, com o custo da respectiva redução da capacidade geral da bateria. Se você for ajustar a densidade do eletrólito da bateria, você **deve** usar água destilada, já que a água da torneira ou de poço irá danificar permanentemente a bateria.

Estados de carga

Há dois estados especiais de carga que podem acontecer durante o ciclo de carga e descarga da bateria. Ambos devem ser evitados a fim de preservar a vida útil da bateria.

Sobrecarga

A ***sobrecarga*** acontece quando a bateria atinge o limite de sua capacidade. Se a energia aplicada à bateria está acima de seu ponto máximo de carga, o eletrólito começa a se decompor, produzindo bolhas de oxigênio e hidrogênio em um processo conhecido como gaseificação. Isto resulta na perda de água, oxidação do eletrodo positivo e, em casos extremos, o perigo de explosão.

Por outro lado, a presença de gás evita a estratificação do ácido. Depois de vários ciclos contínuos de carga e descarga, o ácido tende a concentrar-se no fundo da bateria, reduzindo sua capacidade efetiva. O processo de gaseificação agita o eletrólito e evita a estratificação.

Mais uma vez, é necessário encontrar um ponto de equilíbrio entre as vantagens (evitar a estratificação do eletrólito) e desvantagens (perda de água e produção de hidrogênio). Uma solução é permitir uma leve condição de sobrecarga de vez em quando. Um método típico é permitir uma voltagem de 2,35 a 2,4 Volts para cada elemento da bateria a cada espaço de alguns dias, a 25°C. O regulador deve garantir estas sobrecargas periódicas e controladas.

Descarga excessiva

Da mesma forma que há um limite superior, existe um limite inferior para o estado de carga da bateria. A descarga além deste limite irá resultar em deterioração. Por isso, o regulador evita que mais energia seja extraída da bateria, desconectando-a quando a voltagem de cada célula atingir o limite de 1,85 V em 25°C.

Se a descarga da bateria for profunda e a bateria permanece descarregada por longo tempo, acontecem três coisas: a formação de sulfato cristalizado nas placas da bateria, a perda de material ativo na placa da bateria e a colagem das placas. O processo de formação de cristais estáveis de sulfato é chamado de sulfatação. Isto é particularmente negativo já que os cristais grandes que se formam não fazem mais parte da reação química, podendo inutilizar a bateria.

Parâmetros de bateria

Os principais parâmetros que caracterizam a bateria são:

- ***Voltagem nominal***, V_{NBat}: o valor mais comum é 12 V.
- ***Capacidade nominal***, C_{NBat}: a máxima quantidade de energia que pode ser extraída de uma bateria completamente carregada, expressa em ***Ampere-hora*** (***Ah***) ou ***Watt-hora*** (***Wh***). A quantidade de energia que pode ser obtida de uma bateria depende do tempo durante o qual o processo de extração acontece. A descarga de uma bateria em um longo período de tempo irá proporcionar mais energia do que a possível com a descarga da bateria em menor período de tempo. A capacidade da bateria é, portanto, especificada em tempos diferentes de descarga. Para aplicações fotovoltaicas, este tempo deve ser maior que 100 horas (C100).
- ***Máxima profundidade de descarga***, DoD_{max}: a profundidade de descarga é a quantidade de energia extraída da bateria em um único ciclo de descarga, expressa como percentagem. A expectativa de vida útil da bateria depende de quão profundamente ela é descarregada, em cada ciclo. O fabricante deve fornecer gráficos que relacionem o número de ciclos de carga e descarga com a vida útil da bateria. Como regra geral, você deve evitar ciclos de descarga que ultrapassem 50% da capacidade da bateria. Baterias de tração devem ser descarregadas apenas 30%.
- ***Capacidade utilizável***, C_{UBat}: é a capacidade real (utilizável) de uma bateria. É igual ao produto da capacidade nominal e o máximo DoD. Por

exemplo, uma bateria estacionária de capacidade nominal (C100) de 120 Ah e profundidade de descarga de 70%, tem a capacidade utilizável de (120 x 0,7) 84 Ah.

Medindo o estado de carga da bateria

Uma bateria selada de chumbo-ácido de 12 V fornece voltagens diferentes, dependendo do estado de carga. Quando a bateria está completamente carregada, em circuito aberto, a voltagem de saída é de cerca de 12,8 V. Ela cai rapidamente para 12,6 V quando cargas são ligadas. Como a bateria constantemente fornece corrente durante sua operação, a voltagem reduz-se linearmente de 12,6 para 11,6 V, dependendo do estado da carga. Uma bateria selada de chumbo-ácido fornece 95% de sua energia dentro destes limites de voltagem. Assumindo que uma bateria totalmente carregada tem a voltagem de 12,6 V e 11,6 V quando descarregada, podemos estimar que a bateria descarregou 70% quando atingir a voltagem de 11,9 V. Estes valores são apenas uma estimativa aproximada, uma vez que eles também dependem do tempo de vida e qualidade da bateria, da temperatura, etc.

Estado de carga	Voltagem da Bateria de 12 V	Voltagem por célula
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

De acordo com esta tabela e considerando que uma bateria de caminhão não deve ser descarregada em mais de 20 a 30%, podemos determinar que a

capacidade utilizável de uma bateria de 170 Ah varia entre 34 Ah (20%) e 51 Ah (30%). Usando a mesma tabela, verificamos que o regulador deve ser programado de forma a prevenir que a bateria descarregue-se abaixo de 12,3 V.

Proteção da bateria e do regulador

Disjuntores termomagnéticos ou fusíveis devem ser usados para proteger a bateria e a instalação contra curto-circuitos e outros problemas de mal funcionamento. Há dois tipos de fusíveis: ***queima lenta*** (*slow blow*) e ***queima rápida*** (*quick blow*). Fusíveis de queima lenta devem ser usados com cargas indutivas ou capacitivas onde uma alta corrente pode ocorrer no momento em que são ligados. Estes fusíveis permitem a passagem de uma corrente maior do que seu valor por um curto período de tempo. Fusíveis de queima rápida queimam assim que a corrente que passa por eles for maior do que sua corrente nominal.

O regulador é conectado à bateria e às cargas, assim, dois tipos diferentes de proteção devem ser considerados. Um fusível deve ser colocado entre a bateria e o regulador, protegendo a bateria de um curto no caso de uma falha do regulador. Um segundo fusível necessita proteger o regulador de uma corrente excessiva de carga. Este segundo fusível é, normalmente, integrado ao próprio regulador.

Figura 7.9: Um banco de baterias de 3600 Ah. A corrente chega a 45 A durante o carregamento.

Cada fusível é marcado com a máxima corrente e voltagem utilizável. A máxima corrente de um fusível deve ser 20% maior do que a máxima corrente esperada. Mesmo em baterias de voltagem baixa, um curto-circuito pode produzir uma corrente muito alta que pode, facilmente, atingir algumas centenas de amperes. Grandes correntes podem causar incêndios, danificar o equipamento e as baterias e mesmo causar choque elétrico no corpo humano.

Se um fusível queimar, nunca o substitua por um fio ou fusível de maior valor. Primeiro determine a causa do problema e depois troque o fusível por outro de características idênticas.

Efeitos da temperatura

A temperatura ambiente tem vários efeitos importantes nas características da bateria:

- A capacidade nominal da bateria (que o fabricante fornece para uma temperatura de 25°C) aumenta com a temperatura a uma taxa de cerca de 1%/°C. Mas se a temperatura é muito alta, a reação química que acontece na bateria se acelera, causando o mesmo tipo de oxidação que acontece em uma sobrecarga. Isto irá, obviamente, reduzir a expectativa de vida da bateria. Este problema pode ser parcialmente compensado em baterias de automóvel com o uso de uma menor densidade da solução (uma gravidade específica de 1,25 quando a bateria está totalmente carregada).
- Quando a temperatura é reduzida, a vida útil da bateria aumenta. Mas se a temperatura é muito baixa, há risco de congelamento do eletrólito. A temperatura de congelamento depende da densidade da solução, que também está relacionada com o estado de carga da bateria. Quanto mais baixa a densidade, maior o risco de congelamento. Em áreas de baixas temperaturas, você deve evitar a descarga profunda das baterias (assim, o DoD_{max} é efetivamente reduzido).
- A temperatura também muda a relação entre a voltagem e a carga. É preferível usar um regulador que ajuste os parâmetros de desconexão em voltagem baixa e reconexão de acordo com a temperatura. O sensor de temperatura do regulador deve ser fixado na bateria com o uso de fita adesiva ou outro método simples.
- Em áreas quentes, é importante manter as baterias tão resfriadas quanto possível. Elas devem ser armazenadas em uma área sombreada e nunca devem ser expostas diretamente ao sol. Também é desejável montá-las em um pequeno suporte para permitir o fluxo de ar sobre elas, aumentando a ventilação.

Como escolher uma boa bateria

A escolha de uma boa bateria pode constituir-se em um desafio nas regiões em desenvolvimento. Baterias de alta capacidade são pesadas, volumosas e caras para importar. Uma bateria de 200 Ah pesa cerca de 50 kg e não pode ser transportada como bagagem de mão. Se você quiser baterias de longa vida (mais de cinco anos) livres de manutenção, prepare-se para pagar o preço.

Uma boa bateria sempre vem com especificações técnicas, incluindo a capacidade em diferentes taxas de descarga (C20, C100), temperatura operacional, pontos de corte de tensão e requisitos dos carregadores.

As baterias não devem ter rachaduras, vazamentos ou qualquer sinal de danos e seus terminais não devem estar enferrujados. Como testes de laboratório são necessários para obter dados completos sobre a real capacidade e vida útil, espere encontrar lotes de baterias de baixa qualidade (incluindo falsas) em mercados locais. O típico preço (não incluído o frete e taxas de importação) é de cerca de 3 a 4 dólares por Ah para baterias de chumbo-ácido de 12 V.

Expectativa de vida versus número de ciclos

Baterias são os únicos componentes de um sistema solar que devem ser amortizadas em um período pequeno de tempo e precisam ser regularmente trocadas. Você pode aumentar a vida útil de uma bateria reduzindo a profundidade de sua descarga por ciclo. Mesmo as baterias que são projetadas para um ciclo profundo de descarga terão sua vida aumentada se esta profundidade (> 30%) for reduzida.

Se você descarrega a bateria completamente, todos os dias, você provavelmente terá que trocá-la em menos de um ano. Se você usar apenas 1/3 da capacidade da bateria, ela pode durar mais de três anos. Pode ser mais barato comprar uma bateria com três vezes a capacidade de uma outra do que ter que trocá-la a cada ano.

O regulador de potência de carga

O regulador de potência de carga também é chamado de controlador de carga, regulador de voltagem e controlador de carga e descarga. O regulador fica entre a matriz de painéis, as baterias e seu equipamento ou cargas.

Lembre-se que a voltagem de uma bateria, ainda que sempre perto dos 2 V por célula, varia de acordo com o estado de sua carga. Através do monitoramento da voltagem da bateria, o regulador previne a sobrecarga ou excessiva descarga.

Reguladores usados em aplicações solares devem ser conectados em série: eles desconectam a matriz de painéis da bateria para evitar a sobrecarga e desconectam a bateria dos equipamentos para evitar a descarga excessiva. A conexão e desconexão é feita por meio de chaves, que podem ser de dois tipos: eletromecânico (relés) ou de estado sólido (transistor bipolar, MOSFET). Reguladores jamais devem ser conectados em paralelo.

A fim de proteger a bateria contra a gaseificação, a chave desconecta o circuito de carregamento da bateria quando atinge sua ***voltagem alta de desconexão*** (***HVD*** – *high voltage disconnect*) ou ponto de corte. A ***baixa voltagem de desconexão*** (***LVD*** – *low voltage disconect*) previne a bateria de uma descarga excessiva, desconectando os equipamentos alimentados por ela. Para evitar sucessivas conexões e desconexões, o regulador não irá reconectar as cargas até que a bateria atinja uma ***voltagem baixa de reconexão*** (***LVR*** – *low reconnect voltage*).

Valores típicos para uma bateria de chumbo-ácido de 12 V são:

Ponto de Voltagem	Voltagem
LVD	11,5
LRV	12,6
Voltagem regulada constante	14,3
Equalização	14,6
HVD	15,5

Os reguladores mais modernos são também capazes de desconectar os painéis durante a noite, evitando a descarga da bateria. Eles podem também, periodicamente, sobrecarregar a bateria para aumentar sua vida útil, valendo-se de um mecanismo conhecido como ***modulação de largura de pulso*** (***PWM*** – *pulse width modulation*) para prevenir a gaseificação excessiva.

Como o ponto de potência de pico em matrizes de painéis pode variar com a temperatura e iluminação solar, novos reguladores são capazes de monitorar o máximo ponto de potência dos painéis. Esta função é conhecida como monitoramento do ***ponto de potência máxima*** (***MPPT*** — *maximum power point tracking*).

Parâmetros do regulador

Quando for escolher um regulador para o seu sistema, você deve conhecer ao menos a ***voltagem de operação*** e a ***corrente máxima*** com as quais ele poderá lidar. A voltagem (ou tensão) de operação será de 12, 24 ou 48 V. A corrente máxima deve ser 20% maior que a fornecida pela matriz de painéis conectada ao regulador.

Outras funcionalidades e dados interessantes incluem:

- Valores específicos para LVD, LRV e HVD.
- Suporte para compensação de temperatura. A voltagem que indica o estado de carga da bateria varia com a temperatura. Por isto, alguns reguladores são capazes de medir a temperatura da bateria e corrigir os diferentes valores de corte e reconexão.
- Instrumentação e medidores. Os instrumentos mais comuns medem a voltagem dos painéis e baterias, o estado de carga (SoC) e a profundidade de descarga (DoD). Alguns reguladores incluem alarmes especiais para indicar que os painéis ou cargas foram desconectados, LVD ou HVD foram alcançados, etc.

Conversores

O regulador fornece corrente contínua (DC) a uma voltagem específica. Conversores e inversores são usados para ajustar a voltagem para que ela corresponda à requerida pelos equipamentos utilizados.

Conversores DC/DC

Conversores DC/DC transformam uma voltagem em corrente contínua para outra de diferente valor, também em corrente contínua. Há dois métodos de conversão que podem ser usados para adaptar a voltagem fornecida pelas baterias: ***conversão linear*** e ***conversão por chaveamento***.

A conversão linear reduz a voltagem das baterias, convertendo a energia excedente em calor. Este método é muito simples, mas claramente ineficiente. A conversão por chaveamento geralmente utiliza um componente magnético para armazenar a energia e transformá-la em uma outra voltagem. A voltagem resultante pode ser maior que, menor que, ou o inverso (negativo) de a voltagem de entrada.

A eficiência de um regulador linear decresce na medida que a diferença entre as voltagens de entrada e saída aumenta. Por exemplo, se queremos converter de 12 para 6 V, o regulador linear terá uma eficiência de apenas 50%. Um conversor por chaveamento padrão terá uma eficiência de ao menos 80% no mesmo caso.

Inversor ou conversor DC/AC

Inversores são usados quando o seu equipamento necessita de corrente alternada. Os inversores cortam e invertem a corrente contínua, formando uma onda quadrada que é depois filtrada para que se aproxime a uma onda senoidal, eliminando harmônicos indesejáveis. Poucos inversores conseguem fornecer uma onda senoidal em sua saída. A maioria dos modelos disponíveis no mercado produzem o que é conhecido como uma “onda senoidal modificada”, já que a forma de sua voltagem de saída não é uma senóide pura. Em termos de eficiência, inversores de onda senoidal modificada desempenham melhor que inversores de senóide pura.

Saiba, porém, que nem todo equipamento irá aceitar uma onda senoidal modificada como voltagem de entrada. Mais comumente, algumas impressoras a laser não irão funcionar com este tipo de inversor. Motores irão funcionar, mas podem consumir uma potência maior do que se fossem alimentados com uma senóide pura. Adicionalmente, fontes de alimentação DC tendem a esquentar mais e amplificadores de áudio podem emitir um zunido.

Além do tipo da forma de onda, outras características importantes dos inversores incluem:

- **Confiabilidade na presença de surtos**. Os inversores têm duas potências nominais: uma para a potência contínua e outra, maior, para a potência de pico. Eles são capazes de fornecer uma potência de pico por um período bem curto de tempo, por exemplo, na partida de um motor. O inversor deve ser capaz também de desligar a si mesmo com segurança

(com um disjuntor ou fusível) no caso de um curto-circuito, ou na eventualidade da potência requerida dele ser muito alta.

- **Eficiência de conversão**. Inversores operam de forma mais eficiente quando fornecendo entre 50 e 90% de sua potência contínua nominal. Você deve selecionar um inversor que corresponda com mais exatidão as necessidades de seu equipamento. O fabricante normalmente fornece o desempenho do inversor a 70% de sua potência nominal.
- **Carga de bateria**. Muitos inversores também incorporam a função inversa: a possibilidade de carregar baterias na presença de uma fonte alternativa de energia (rede elétrica, gerador, etc). Este tipo de inversor é conhecido como carregador/inversor.
- **Seleção automática de fontes** (*fail-over*). Alguns inversores podem chavear automaticamente entre diferentes fontes de energia (rede elétrica, gerador, painel solar), dependendo da que está disponível no momento.

Quando utilizar equipamentos de telecomunicação, o melhor é evitar o uso de conversores DC/AC e alimentá-los diretamente de uma fonte DC. Muitos equipamentos de comunicação aceitam uma ampla variação de voltagens de entrada.

Equipamento ou carga

Deve ser óbvio que, na medida em que os requerimentos de potência aumentam, a despesa com o sistema fotovoltaico também aumenta. Por isto, é crítico casar o dimensionamento do sistema, o melhor possível, com a carga esperada. Ao projetar o sistema você deve, primeiramente, fazer uma estimativa realista do consumo máximo. Depois de instalado, o consumo máximo estabelecido deve ser respeitado a fim de evitar falhas na entrega de potência.

Aparelhos domésticos

O uso de energia solar não é recomendado para aplicações de troca de calor (aquecedores elétricos, refrigeradores, torradeiras, etc). Sempre que possível, a energia deve ser distribuída com parcimônia, usando equipamentos de baixo consumo.

Aqui estão alguns pontos que devem ser considerados na escolha de equipamentos apropriados para o uso com energia solar:

- A energia solar presta-se bem para a iluminação. Neste caso, o uso de lâmpadas halogenas ou fluorescentes é obrigatório. Mesmo que estas lâmpadas sejam mais caras, elas são muito mais eficientes do que lâmpadas incandescentes. Lâmpadas LED também são uma boa escolha já que, além de eficientes, são alimentadas por corrente contínua.
- É possível usar potência fotovoltaica para aparelhos que requerem consumo constante e baixo (um típico caso é o aparelho de TV). Televisores pequenos usam menos potência que os maiores. Leve

também em conta que uma TV preto e branco consome a metade da potência de uma colorida.

- A energia fotovoltaica não é recomendada para nenhum aparelho que transforme energia em calor (energia térmica). Use painéis de aquecimento solar (não os fotovoltaicos!) ou gás butano como alternativa.
- Lavadoras convencionais irão funcionar, mas você deve evitar programas de lavagem que incluam a centrifugação com água quente.
- Caso você precise usar refrigeradores, eles devem consumir o mínimo possível de potência. Há refrigeradores especiais que trabalham com energia DC, mas seu consumo pode ser elevado (cerca de 1000 Wh/dia).

A estimativa de consumo total é um passo fundamental no dimensionamento de seu sistema de energia solar. A tabela abaixo dá uma idéia geral do consumo de potência que você pode esperar de diferentes aparelhos:

Equipamento	Consumo (Watts)
Computador portátil	30-50
Lâmpada de baixa potência	6-10
Roteador WRAP (um rádio)	4-10
Modem VSAT	20-30
PC (sem monitor LCD)	20-30
PC (com monitor LCD)	200-300
Switch de rede (16 portas)	6-8

Equipamento de telecomunicação wireless

A economia de potência com a escolha do equipamento correto evita gasto de dinheiro e problemas em excesso. Por exemplo, um link de longa distância não necessita de um amplificador que consuma muita potência. Um cartão Wi-Fi com um receptor de boa sensitividade e uma zona fresnel com ao menos 60% de espaço livre irá funcionar melhor que um amplificador, economizando também no consumo de potência. Um ditado comum em rádio-amadorismo cabe também aqui: o melhor amplificador é uma boa antena. Mais medidas para a redução do consumo incluem o escalonamento (*throttling*) da velocidade da CPU, a redução da potência de transmissão, para o valor mínimo, necessária para fornecer um link estável, aumento de tempo entre intervalos de envio de sinais (*beacon*) e o desligamento dos equipamentos quando não estão em uso.

Muitos sistemas solares autônomos trabalham em 12 ou 24 Volts. Preferencialmente, um dispositivo wireless que aceita corrente na voltagem de 12 V, fornecida pela maioria das baterias de chumbo-ácido, deve ser utilizado. A transformação da voltagem fornecida pela bateria para AC, ou o uso de uma

voltagem de entrada no access point diferente da fornecida pela bateria, causará um desperdício desnecessário de energia. Um access point que aceite 8-20 Volts DC é perfeito.

A maioria dos access points baratos tem, internamente, um regulador de voltagem chaveado que irá trabalhar dentro destes limites de voltagem sem modificação e sem super-aquecimento (mesmo que o dispositivo inclua uma fonte de alimentação de 5 ou 12 Volts).

ATENÇÃO: Usar seu access point com uma fonte de alimentação diferente que a fornecida pelo fabricante irá, certamente, anular qualquer garantia e pode causar danos ao equipamento. Mesmo que a técnica a seguir normalmente funcione como descrita, lembre-se que ao reproduzi-la você o está fazendo por sua conta e risco.

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

Abra seu access point e procure, perto da entrada da alimentação DC, por dois capacitores relativamente grandes e um indutor (um anel de ferrite com fio de cobre enrolado nele). Caso eles estejam presentes, o dispositivo tem uma fonte chaveada e a voltagem de entrada deve ser um pouco abaixo daquela impressa nos capacitores. Usualmente, estes capacitores têm uma voltagem nominal de 16 ou 25 Volts. Saiba que uma fonte de alimentação sem regulagem tem uma oscilação (*ripple*), podendo fornecer ao seu access point um valor

muito maior de voltagem do que o valor nominal impresso nela. Assim, conectar uma fonte de alimentação não-regulada de 24 Volts em um dispositivo com capacitores de 25 Volts não é uma boa idéia. Claro que, ao abrir seu dispositivo, você estará anulando qualquer garantia existente. Não tente fazer o access point funcionar com uma voltagem maior que a indicada se ele não tiver um regulador chaveado. Ele irá aquecer, funcionar de forma instável ou queimar.

Equipamentos baseados no tradicional processador Intel x86 consomem muito mais potência, em comparação com arquiteturas RISC como os processadores ARM ou MIPS. Um dos cartões com o menor consumo de potência é o da plataforma Soekris, que usa um processador AMD ElanSC520. Outra alternativa ao AMD (ElanSC ou Geode SC1100) são os equipamentos com processadores MIPS. Os processadores MIPS têm melhor desempenho que o AMD Geode, mas consomem entre 20 a 30% a mais de energia.

O popular Linksys WRT54G funciona em qualquer voltagem entre 5 e 20 Volts DC, consumindo cerca de 6 Watts, mas possui também um switch Ethernet. Claro que um switch é útil, mas ele consome potência adicional. A Linksys fornece um access point chamado WAP54G que consome apenas 3 Watts e pode rodar o firmware OpenWRT e o Freifunk. O Accesscube 4G Systems consome cerca de 6 Watts quando equipado com uma única interface Wi-Fi. Caso o 802.11b seja suficiente, cartões mini-PCI com o chipset Orinoco têm bom desempenho e um mínimo consumo de potência.

A quantidade de potência requerida por um equipamento wireless depende não apenas da sua arquitetura mas também do número de interfaces de rede, rádios, tipo de memória e tráfego. Como regra geral, um cartão wireless de baixo consumo irá requerer entre 2 e 3 W e um rádio de 200 mW consome cerca de 3 W. Cartões de alta potência (como o Ubiquity de 400 mW) consomem perto de 6 W. Uma estação repetidora com dois rádios pode consumir entre 8 e 10 W.

Mesmo que o padrão IEEE 802.11 incorpore um modo de economia de energia (PS – *power saving*), isto não é um benefício tão grande quanto se possa esperar. O mecanismo de economia de energia é permitir que as estações coloquem seus cartões wireless "para dormir", utilizando um circuito temporizador. Quando o cartão "acorda", ele verifica se existe um sinal de indicação de tráfego pendente. Desta forma, a economia de energia apenas ocorre no lado do cliente, já que os access points necessitam funcionar permanentemente para enviar os sinais e armazenar o tráfego dos clientes. O modo de economia de energia pode ser incompatível entre os diferentes fabricantes, o que pode causar instabilidade nas conexões wireless. É praticamente melhor desabilitar o modo de economia de energia em todos os equipamentos, já que as dificuldades criadas não compensam a quantidade economizada de energia.

Selecionando a voltagem

A maioria dos sistemas independentes de baixa potência usam baterias de 12 V como a voltagem operacional comum para baterias seladas de chumbo-ácido. No projeto de um sistema de comunicação wireless, você deve levar em conta a voltagem mais eficiente para a operação de seu equipamento. Mesmo que

seja possível uma ampla variedade de valores de tensão de entrada, você deve certificar-se que, de maneira geral, o consumo de potência do sistema é mínimo.

Fiação

Um componente importante da instalação é a sua fiação, já que o cabeamento correto irá garantir a eficiência na transferência de energia. Algumas boas práticas a serem consideradas incluem:

- Use parafusos para prender bem o cabo ao terminal da bateria. Conexões mal-feitas irão desperdiçar potência.
- Espalhe vaselina ou graxa mineral nos terminais da bateria. Conexões enferrujadas tem maior resistência elétrica, resultando em perdas.
- Para correntes baixas (menos que 10 A) considere o uso de conectores do tipo *Faston* ou *Anderson*. Para correntes maiores, utilize anéis metálicos para a conexão.

A largura do fio é normalmente definida em AWG (*American Wire Gauge*), padrão americano que define a bitola (largura, diâmetro) do fio. Em seus cálculos, você precisará converter entre AWG e mm^2 a fim de estimar a resistência dos cabos. Por exemplo, um cabo AWG #6 tem um diâmetro de 4,11 mm e pode suportar uma corrente de até 55 A. Uma tabela de conversão, incluindo a resistência estimada e a capacidade de transporte de corrente, está disponível no **Apêndice D**. Tenha também em mente que a capacidade de corrente também pode variar, dependendo do tipo de isolamento e aplicação. Na dúvida, consulte o fornecedor para mais informação.

Orientação dos painéis

A maioria da energia que vem do sol chega à superfície em uma linha reta. O módulo solar irá capturar mais energia quando sua face estiver diretamente apontada para o sol, perpendicularmente à linha reta entre a posição da instalação e o sol. Claro que a posição do sol varia constantemente em relação à Terra, então precisamos descobrir qual é a ótima posição para nossos painéis. A orientação dos painéis é determinada por dois ângulos, o ***azimuth a*** e a ***inclinação*** ou ***elevação ß***. O azimuth é o ângulo que mede o desvio em relação ao sul no hemisfério norte, e o desvio em relação ao norte no hemisfério sul. A inclinação é o ângulo formado pela superfície do módulo em relação ao plano horizontal.

Azimuth

Você deve instalar o módulo inclinado em direção ao equador terrestre (em direção ao sul, no hemisfério norte, e ao norte, no hemisfério sul) de forma que, durante o dia, o painel capture a maior quantidade possível de radiação (a = 0).

É muito importante que nenhuma parte dos painéis fique sobre uma sombra! Estude os elementos que cercam o painel (árvores, construções, paredes, outros painéis, etc.) para ter certeza de que eles não produzirão sombras sobre

o painel em nenhuma parte do dia ou do ano. É aceitável girar os painéis +/- 20% em direção ao leste ou oeste, se necessário (a = ± 20°).

Inclinação

Uma vez que você tenha fixado o azimuth, o parâmetro chave para nossos cálculos é a inclinação do painel, expressa pelo ângulo beta (ß). A altura que o sol atinge a cada dia irá variar, a máxima ocorrendo no solstício de verão e a mínima no solstício de inverno. Idealmente os painéis deveriam acompanhar esta variação, mas isto não é normalmente possível em função dos custos envolvidos.

Em instalações com equipamento de telecomunicações, o normal é instalar os painéis com uma inclinação fixa. Na maioria dos cenários de telecomunicações, a energia que é demandada pelo sistema é constante durante o ano. Dimensionando a energia suficiente durante o "pior mês" garantirá o bom funcionamento no restante do ano.

O valor de ß deve maximizar a razão entre a oferta e a demanda de energia.

- Para instalações com consumo consistente (ou quase consistente) durante o ano, é preferível otimizar a captura da máxima radiação durante os meses de inverno. Você deve usar o valor absoluto da latitude lo local (o ângulo F), acrescido de 10° (ß = l F l + 10°).
- Para instalações com menos consumo durante o inverno, o valor da latitude do local pode ser usado como a inclinação do painel solar. Desta forma, o sistema estará otimizado para os meses de primavera e outono (ß = l F l).
- Para instalações que são usadas apenas no verão, você deve usar o valor absoluto da latitude do local (ângulo F) decrescido de (ß = l F l - 10°).

A inclinação do painel nunca deve ser menor que 15° para evitar o acúmulo de poeira e/ou umidade no painel. Nas áreas onde neve e gelo ocorrem, é muito importante proteger os painéis e incliná-los em um ângulo de 65° ou mais.

Caso existe um notável aumento no consumo durante o verão, você deve considerar o arranjo de duas inclinações fixas: uma para os meses de verão e outra para os meses de inverno. Isto pode exigir estruturas especiais de suporte e um planejamento regular para a troca de posição dos painéis.

Como dimensionar seu sistema fotovoltaico

Quando escolher um equipamento que atenda a seus requisitos de potência, você deve ao menos determinar o seguinte:

- O número e o tipo de painéis solares necessários para capturar energia solar suficiente para suportar sua carga.

- A capacidade mínima de sua bateria. A bateria precisará armazenar potência suficiente para fornecer energia elétrica à noite e nos dias de pouco sol. É ela que irá determinar o número de dias de autonomia.
- As características de todos os outros componentes (o regulador, cabeamento, etc.) necessários para dar suporte à quantidade de energia gerada e armazenada.

Os cálculos de dimensionamento do sistema são importantes porque, a não ser que todos os componentes estejam balanceados, energia (e, em conseqüência, dinheiro) será desperdiçada. Como exemplo, se instalarmos mais painéis solares para produzir mais energia, as baterias devem ter capacidade suficiente para armazenar a energia adicional produzida. Caso o banco de baterias seja pequeno e a carga não use toda a energia, ela deve ser descartada. Um regulador com uma capacidade de corrente menor do que a necessária, ou mesmo um único cabo subdimensionado, pode ser a causa de falha (ou mesmo incêndio) que torna a instalação inutilizável.

Nunca esqueça que a capacidade de produção e armazenamento de energia fotovoltaica é limitada. Deixar uma lâmpada ligada acidentalmente durante o dia pode, facilmente, drenar suas reservas antes do período noturno, a ponto de nenhuma energia adicional poder ser utilizada. A disponibilidade de combustível (luz do sol) para o sistema fotovoltaico pode ser difícil de prever. De fato, nunca é possível a certeza absoluta de que um sistema independente será capaz de fornecer energia em um momento em particular. Sistemas de energia solar são projetados para um determinado consumo e, caso o usuário exceda os limites planejados de fornecimento, ele irá falhar.

O método de projeto que propomos consiste na consideração dos requerimentos de energia e, com base nestes, calculamos um sistema que funcione para o máximo período de tempo, tornando-o o mais confiável possível. Claro, se mais painéis e baterias forem instalados, mais energia poderá ser coletada e armazenada. Este aumento de confiabilidade implicará também em um aumento no custo.

Em algumas instalações fotovoltaicas (como as que provisionam energia para equipamentos de telecomunicações em uma rede central) o fator de confiabilidade é mais importante que o custo. Em uma instalação cliente, a manutenção de um custo baixo é provavelmente o fator mais importante. Encontrar o equilíbrio entre o custo e a confiabilidade não é tarefa fácil, mas independente da situação, você deve ser capaz de determinar o que é esperado de suas escolhas para o projeto, e o preço delas.

O método que iremos usar para o dimensionamento do sistema é conhecido como o ***método do pior mês***. Nós simplesmente calculamos as dimensões de um sistema independente, de forma que ele funcione no mês em que a demanda de energia é a maior, com relação à totalidade da energia solar disponível, ou seja, o pior mês do ano.

Usando este método, a ***confiabilidade*** é tomada em consideração fixando-se o máximo número de dias em que o sistema pode funcionar sem receber a luz do sol (isto é, quando todo o consumo será atendido pela energia armazenada na bateria). Isto é dado pelo ***número máximo de dias de autonomia*** (***N***) e pode ser pensado como o número consecutivo de dias

nublados, nos quais os painéis não conseguem coletar nenhuma quantidade significativa de energia.

Ao escolher N, é necessário conhecer as condições climáticas do local em questão, assim como a relevância social e econômica da instalação. Ela será usada para iluminar casas, um hospital, uma fábrica, um link de rádio ou outra aplicação? Lembre-se que com o aumento de N, aumenta também o investimento em equipamentos e manutenção. É também importante avaliar todos os custos da logística de substituição de um equipamento. Não é a mesma coisa substituir uma bateria em uma instalação no meio da cidade em comparação a mesma tarefa no topo de uma torre de comunicação que está a várias horas ou dias de distância.

Determinar o valor de N não é uma tarefa fácil, já que são muitos os fatores envolvidos e muitos deles não podem ser facilmente avaliados. Sua experiência terá um papel importante nesta parte do dimensionamento do sistema. Um valor comumente usado para equipamentos críticos de telecomunicação é N = 5, e para equipamentos clientes de baixo custo é possível reduzir a autonomia para N = 3.

No **Apêndice E** incluímos várias tabelas que auxiliarão na coleta de dados para o dimensionamento do sistema. O restante deste capítulo irá cobrir detalhadamente as informações que você precisa coletar ou estimar, e como usá-las no método do pior mês.

Dados a coletar

- Latitude da instalação. Lembre-se de usar um sinal positivo no hemisfério norte e negativo no hemisfério sul.
- Dados de radiação solar. Para o método do pior mês é suficiente saber doze valores, um para cada mês do ano. Os doze números serão os valores médios da irradiação global diária em um plano horizontal ($G_{dm}(0)$, em kWh/m² por dia). O valor mensal é a soma de todos os valores diários de irradiação global, dividida pelo total de números de dias do mês.

Se você tiver este dado disponível em Joules (J), aplique a seguinte fórmula de conversão:

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

Os dados de irradiação $G_{dm}(0)$ de muitos lugares do mundo podem ser obtidos de tabelas e bases de dados. Você deve verificar estes dados em uma estação meteorológica próxima à instalação de seu sistema, mas não se surpreenda se você não conseguir encontrar estes dados em formato eletrônico. Sempre é uma boa idéia consultar as empresas que instalam sistemas fotovoltaicos em sua região, já que a experiência delas pode ser de grande valor.

Não confunda “horas de sol” com o número de “horas de pico de sol”. O número de horas de pico de sol não tem nada a ver com o número de horas sem nuvens, mas refere-se à média da irradiação diária. Um dia com cinco horas de sol, sem nuvens, não tem necessariamente estas cinco horas com o sol em seu zênite (ponto mais alto).

Uma hora de pico de sol é um valor normalizado da radiação solar de 1000 W/m² a 25°C. Então, quando nos referimos a cinco horas de pico de sol, isto implica uma radiação solar de 5000 W/m².

Características elétricas dos componentes do sistema

As características elétricas dos componentes de seu sistema devem ser fornecidas pelos fabricantes. É aconselhável que você faça as suas próprias medidas para verificar desvios dos valores nominais. Infelizmente, desvios dos valores prometidos pelos fabricantes podem ser grandes e devem ser esperados.

Há um conjunto mínimo de valores que você deve obter antes de começar o dimensionamento de seu sistema:

Painéis

Você precisa saber a voltagem V_{Pmax} e a corrente I_{Pmax} no ponto de máxima potência em condições padrão.

Baterias

Devem ser conhecidas a capacidade nominal (para 100 horas de descarga) C_{NBat}, voltagem operacional V_{NBat} e a máxima profundidade de descarga (ou a máxima capacidade utilizável C_{UBat}). Você deve decidir também o tipo de bateria que planeja usar: chumbo-ácido, gel, AGM, tração modificada, etc. O tipo de bateria é importante na decisão dos pontos de corte do regulador.

Regulador

Você deve conhecer a voltagem nominal V_{NReg} e a máxima corrente na qual ele pode operar I_{maxReg}.

Conversor/Inversor DC/AC

Caso você esteja usando um conversor, você precisa conhecer a voltagem nominal V_{NConv}, a potência instantânea PIConv e a performance a 70% da carga máxima H_{70}.

Equipamento ou carga

É necessário conhecer a voltagem nominal V_{NC} e a potência nominal de operação P_C para cada peça de equipamento alimentada pelo sistema.

A fim de conhecer a energia total que sua instalação irá consumir, também é muito importante considerar o tempo em que cada equipamento será utilizado. Ele é constante? Ou será usado uma vez por dia, semana, mês, ano? Lembre-se que qualquer mudança no uso pode impactar a quantidade de energia necessária (uso sazonal, períodos de aula ou treinamento, etc).

Outras variáveis

Além das características elétricas dos componentes e sua carga, é necessário decidir sobre outras duas informações antes de dimensionar o sistema fotovoltaico. Estas decisões são o número de dias de autonomia requeridos e a voltagem operacional do sistema.

N, número de dias de autonomia

Você precisa decidir sobre qual valor de N irá contrabalançar as condições meteorológicas através do tipo de instalação e seu custo. É impossível determinar um valor concreto de N que seja válido para todas as instalações, mas a tabela a seguir recomenda alguns valores. Tome estes valores como uma mera aproximação e consulte um projetista experiente antes de chegar a uma decisão final.

Luz do sol disponível	Instalação doméstica	Instalação Crítica
Muito nublado	5	10
Variável	4	8
Ensolarado	3	6

V_N, voltagem nominal da instalação

Os componentes de seu sistema devem ser escolhidos para operar na voltagem nominal V_N. Esta voltagem é usualmente 12 ou 24 Volts para sistemas pequenos e, caso o consumo total ultrapasse 3 kW, a voltagem será 48 V. A seleção de V_N não é arbitrária e depende da disponibilidade dos equipamentos.

- Caso o equipamento permita, tente fixar a voltagem nominal para 12 ou 24 V. Muitos cartões para redes wireless aceitam uma ampla variação de tensão de entrada, podendo ser usados sem um conversor.
- Caso você necessite de muitos tipos de equipamentos que trabalhem com diferentes voltagens nominais, calcule a que minimiza o consumo de energia em geral, considerando as perdas na conversão DC/DC e DC/AC.

Procedimento de cálculo

Há três passos principais que devem ser seguidos para o cálculo apropriado do tamanho de um sistema:

1. **Calcule a energia solar disponível (a oferta)**. Com base em dados estatísticos de radiação solar, na orientação e inclinação ótima dos painéis, calculamos a energia solar disponível. Esta estimativa é feita em intervalos mensais, reduzindo os dados estatísticos a 12 valores.

Assim chegamos a um razoável equilíbrio entre precisão e simplicidade.

2. **Estime os requerimentos de energia elétrica (a demanda)**. Registre as características de consumo de potência do equipamento escolhido, assim como sua estimativa de uso. A seguir, calcule a energia elétrica que será requerida mensalmente. Você deve considerar flutuações no uso devido às variações entre outono e inverno, períodos de chuva e seca, férias ou atividade escolar, etc. O resultado serão 12 valores de demanda de energia, um para cada mês do ano.

3. **Calcule o tamanho ideal do sistema (o resultado)**. Com os dados do pior mês, quando a relação entre a energia demandada e a disponível é a maior, calculamos:

   - A corrente que a matriz de painéis deve suprir, que irá determinar o número mínimo de painéis;
   - A quantidade de armazenamento de energia que deve cobrir o mínimo número de dias de autonomia, que determinará o número necessário de baterias;
   - As características elétricas do regulador;
   - O comprimento e bitola dos cabos para as conexões elétricas.

Corrente requerida no pior mês

Para cada mês, você precisa calcular o valor de I_m, que é a corrente máxima diária que a matriz de painéis precisa fornecer em voltagem nominal V_N, em um dia com uma irradiação G_{dm} para o mês "m" com painéis com inclinação ß graus.

O I_m (PIOR MÊS) será o maior valor de Im, e o dimensionamento do sistema é baseado nos dados deste pior mês. Os cálculos de G_{dm}(ß) para um determinado local podem ser baseados em G_{dm}(0) usando o auxílio de softwares como PVSYST (*http://www.pvsyst.com/*) ou PVSOL (*http://www.solardesign.co.uk/*).

Devido a perdas no regulador e baterias e também ao fato de que os painéis nem sempre funcionam em seu ponto de máxima potência, a corrente requerida I_{mMAX} é calculada assim:

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

Uma vez determinado o pior mês, o valor I_{mMAX} e o total de energia requerida E_{TOTAL} (PIOR MÊS), você pode seguir para os cálculos finais. E_{TOTAL} é a soma de todas as cargas DC e AC, em Watts. Para calcular o E_{TOTAL} veja o **Apêndice E**.

Número de painéis

Combinando painéis solares em série ou paralelo, podemos obter a voltagem e corrente desejadas. Quando os painéis são conectados em série, sua voltagem é igual à soma das voltagens individuais de cada módulo, enquanto a corrente fornecida não muda. Quando conectados em paralelo, as correntes são somadas enquanto a voltagem não muda. É muito importante utilizar painéis de características aproximadamente idênticas na construção de uma matriz.

Você deve tentar adquirir painéis com um V_{Pmax} um pouco maior que a voltagem nominal do sistema (12, 24 ou 48 V). Lembre-se que você precisa fornecer alguns volts além da voltagem nominal da bateria para poder carregá-la. Caso não seja possível encontrar um painel único que satisfaça estes requerimentos, você deverá conectá-los em série para atingir a voltagem desejada. O número de painéis em série N_{PS} é igual à voltagem nominal do sistema dividida pela voltagem de um painel único, arredondado para o número inteiro mais próximo.

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

Para calcular o número de painéis em paralelo (N_{PP}), você precisa dividir o I_{mMAX} pela corrente de um painel único no ponto de máxima potência I_{Pmax}, arredondando para o número inteiro mais próximo.

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

O número total de painéis resulta da multiplicação do número de painéis em série (para a voltagem necessária) e o número dos painéis em paralelo (para a corrente).

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

Capacidade da bateria ou acumulador

A bateria determina a voltagem do sistema de uma forma geral e precisa ter capacidade suficiente para fornecer energia aos equipamentos quando não há necessária irradiação solar.

Para estimar a capacidade da bateria, primeiro calculamos a capacidade de energia requerida pelo sistema (capacidade necessária, C_{NEC}). A capacidade necessária depende da energia disponível durante o pior mês e do número desejado de dias de autonomia (N).

$$C_{NEC}\ (Ah) = E_{TOTAL}(\text{PIOR MÊS})(Wh) / V_N(V) \times N$$

A capacidade nominal da bateria C_{NOM} precisa ser maior que C_{NEC}, já que não podemos descarregar totalmente a bateria. Para calcular o tamanho da bateria que necessitamos, temos que considerar a máxima profundidade de descarga (DoD) permitida pela mesma:

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

A fim de calcular o número de baterias em série (N_{BS}), dividimos a voltagem nominal de nossa instalação (V_N) pela voltagem nominal de uma única bateria(V_{NBat}):

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

Regulador

Uma observação importante: sempre use reguladores em série, nunca em paralelo. Caso seu regulador não suporte a corrente requerida por seu sistema, você deve comprar um outro regulador com uma capacidade maior de corrente.

Por razões de segurança, um regulador deve ser capaz de operar com uma corrente I_{maxReg} ao menos 20% maior que a máxima intensidade fornecida pela matriz de painéis:

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

Inversor DC/AC

A energia total necessária para um equipamento AC é calculada incluindo-se todas as perdas que são introduzidas pelo conversor DC/AC, ou inversor. Na escolha de um inversor, tenha em mente que o desempenho do mesmo varia de acordo com a quantidade de potência requerida. Um inversor tem seu melhor desempenho quando opera na proximidade de sua potência nominal. O uso de um inversor de 1500 W em uma carga de 25 W é extremamente ineficiente. A fim de evitar o desperdício de energia, é importante considerar não a potência de pico de todos os seus equipamentos, mas a potência de pico dos equipamentos que poderão estar simultaneamente em operação.

Cabos

Uma vez que você saiba o número de painéis e baterias e o tipo de reguladores e inversores que precisará usar, é necessário calcular o comprimento e bitola dos cabos que irão conectar todos estes componentes.

A ***comprimento*** depende da localização dos equipamentos. Você deve tentar minimizar o comprimento dos cabos entre o regulador, painéis e baterias. Usando cabos curtos, você minimiza a perda de energia e o investimento em cabos.

A grossura (***bitola***) é escolhida com base no tamanho do cabo e na máxima corrente que irá passar pelo mesmo. O objetivo é minimizar quedas de tensão. A fim de calcular a bitola S de um cabo é necessário conhecer:

- A máxima corrente I_{MC} que irá passar pelo cabo. No caso de um subsistema painel-bateria, ela é a I_{mMAX} calculada para cada mês. No subsistema bateria-carga, ela depende da forma como as cargas estão conectadas.

- A queda de voltagem ($V_a - V_b$) é a que consideramos aceitável para o cabo. Ela resulta da adição de todas as possíveis quedas e é expressa como um percentual da voltagem nominal da instalação. Valores máximos típicos são:

Componente	Queda de voltagem (% da V_N)
Matriz de painéis -> Bateria	1%
Bateria -> Conversor	1%
Linha principal de alimentação	3%
Linha principal para iluminação	3%
Linha principal para equipamentos	5%

Queda de voltagem aceitável em cabos

A bitola S de um cabo é determinada pela lei de Ohm:

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

onde S é a bitola (seção ou "grossura") do cabo, r é a resistividade (propriedade intrínseca do material: para o cobre, 0,01286 $\Omega mm^2/m$) e L o comprimento.

O S é escolhido levando-se em consideração os cabos disponíveis no mercado. Você deve escolher a bitola imediatamente superior àquela obtida com o uso da fórmula acima. Por razões de segurança, há alguns valores mínimos: para o cabo que conecta os painéis e a bateria, o mínimo é de 6 mm^2. Para outros usos, o mínimo é de 4 mm^2.

Custo de uma instalação de energia solar

Mesmo que a energia solar seja gratuita, o equipamento necessário para transformá-la em energia elétrica útil não é. Você não apenas necessita comprar o equipamento que transforma a energia solar em eletricidade e a armazena para o uso, mas também deve ser capaz de substituir e fazer a manutenção dos vários componentes do sistema. A questão da substituição de equipamentos é freqüentemente esquecida, mas um sistema de energia solar deve ser implementado com um plano de manutenção apropriado.

A fim de calcular o real custo de sua instalação, fornecemos um exemplo. A primeira coisa a fazer é calcular o investimento inicial (valores em dólares americanos).

Descrição	Quantidade	Custo Unitário	Subtotal
Painel solar de 60W (cerca de $4 / W)	4	$300	$1.200
Regulador de 30A	1	$100	$100
Cabos (metros)	25	$1 / metro	$25
Baterias de 50 Ah de ciclo de descarga profunda	6	$150	$900
		Total:	$2.225

O cálculo de nosso investimento é relativamente fácil uma vez que o sistema foi bem dimensionado. Você necessita apenas adicionar o preço para cada componente e o custo de mão-de-obra para instalar e conectar os equipamentos. Para simplificar, não incluímos os custos de transporte e instalação, mas você não deve esquecer deles.

Para saber quanto o sistema realmente irá custar, devemos estimar quanto tempo cada componente irá durar e com que freqüência devemos substituí-lo. Em contabilidade, isto é chamado de amortização. Nossa nova tabela, contemplando estes fatores, ficará assim (valores em dólares americanos):

Descrição	#	Custo Unitário	Subtotal	Tempo de vida (anos)	Custo Anual
Painel solar de 60W (cerca de $4 / W)	4	$300	$1.200	20	$60
Regulador de 30A	1	$100	$100	5	$20
Cabos (metros)	25	$1 / metro	$25	10	$2,50
Baterias de 50 Ah de ciclo de descarga profunda	6	$150	$900	5	$180
		Total:	$2.225	Custo Anual:	$262,50

Como você pode notar, uma vez que o investimento inicial foi feito, um custo anual de $ 262,50 é esperado. O custo anual é uma estimativa da quantidade de dinheiro necessária anualmente para substituir componentes que atinjam o final de sua vida útil.

8
Construindo um nó externo

Há muitas considerações a serem levadas em conta na instalação externa de equipamentos eletrônicos. Obviamente, eles devem estar protegidos da chuva, vento, sol e outros elementos que podem danificá-los. Energia deve ser fornecida a eles e a antena deve ser montada em uma altura suficiente. Sem aterramento apropriado raios que atinjam as proximidades, flutuações da energia elétrica e mesmo uma brisa leve em um clima seco podem aniquilar seu link wireless. Este capítulo dará alguma idéia dos problemas práticos que você poderá enfrentar quando da instalação externa de equipamentos wireless.

Gabinetes à prova d'água

Gabinetes apropriados, à prova d'água, estão disponíveis em várias formas. Plástico ou metal podem ser usados para criar um gabinete selado contra a água para equipamentos externos.

Claro que os equipamentos precisam de energia para funcionar e possivelmente necessitarão estar conectados a uma antena ou cabo Ethernet. Cada furo que você faz em um gabinete à prova d'água é um novo local por onde a água poderá entrar.

A *National Electrical Manufacturers Association* (*NEMA*)[1] fornece normas para a proteção de equipamentos elétricos contra a chuva, gelo, poeira e outros elementos contaminantes. Um gabinete com a graduação ***NEMA 3*** ou melhor é suficiente para o uso externo em um clima ameno. Um ***NEMA 4X*** ou ***NEMA 6*** fornecem excelente proteção, mesmo contra água sob pressão e gelo. Para proteger furos feitos no gabinete (para conexão de cabos), a *International Electrotechnical Commission* (IEC) designa uma graduação para proteção de inserção (IP – *ingress protection*). Uma proteção de inserção com graduação ***IP66*** ou ***IP67*** irá proteger furos contra jatos de água bem fortes. Um bom gabinete externo deve também fornecer proteção contra raios ultravioleta, para prevenir o desgaste da vedação da exposição ao sol, assim como proteger o equipamento dentro do gabinete.

---

1. N. do T. - Para saber mais sobre as normas NEMA em português, visite o website da Associação Nacional de Fabricantes de Produtos Elétricos NEMA Brasil, em *http://www.nemabrasil.org.br*

Encontrar gabinetes classificados pela NEMA ou IEC pode ser um desafio em sua localidade. Freqüentemente, peças disponíveis localmente podem ser recicladas na construção de gabinetes de proteção. Caixas de metal ou de plástico resistente, conduítes elétricos ou mesmo embalagens plásticas de comida podem ser utilizadas. Quando furar um gabinete, use juntas de borracha de boa qualidade ao redor do cabo para vedar a abertura. Composto de silicone com proteção UV ou outros selantes podem ser usados para instalações temporárias, mas lembre-se que os cabos flexionam-se com o vento, e juntas coladas irão enfraquecer, permitindo a entrada de umidade.

Você pode aumentar tremendamente a vida de um gabinete plástico providenciando alguma proteção contra o sol. A montagem da caixa debaixo de uma sombra, esteja ela já disponível ou feita com uma folha de metal especificamente para este propósito irá adicionar um bom tempo de vida para o gabinete, assim como para o equipamento dentro dele.

Antes de colocar qualquer equipamento eletrônico dentro de uma caixa selada, certifique-se de que a mesma atende a requisitos mínimos de dissipação de calor. Caso sua placa-mãe necessite de um ventilador ou um grande dissipador de calor, lembre-se de que não haverá fluxo de ar no gabinete e seu equipamento pode assar até a morte na torre onde o gabinete será montado. Apenas use componentes eletrônicos projetados para serem embutidos em um ambiente selado.

Fornecendo energia elétrica

É claro que a alimentação DC pode ser fornecida simplesmente através de um furo em seu gabinete, passando um fio por ele. Se o gabinete for grande o suficiente (por exemplo, um gabinete elétrico externo) você pode até mesmo ligar uma tomada AC em seu lado externo. Mas os fabricantes estão, cada vez mais, fornecendo suporte a uma funcionalidade que elimina a necessidade de furos adicionais na caixa: ***Eletricidade via Ethernet*** (***POE*** – *Power over Ethernet*).

O padrão 802.3af define um método para fornecer energia a dispositivos através de pares não utilizados em um cabo Ethernet padrão. Aproximadamente 13 Watts de potência podem ser fornecidos com segurança em um cabo CAT5 sem interferência na transmissão de dados no mesmo cabo. Novos switches Ethernet, compatíveis com o padrão 802.3af (chamados de *end span injectors* – ***injetores de fim de caminho***) fornecem energia diretamente aos dispositivos conectados. Switches injetores podem fornecer potência nos mesmos cabos usados para a transmissão de dados (pares de fios 1-2 e 3-6) ou em pares não utilizados (4-5 e 7-8). Outros equipamentos, chamados de *mid span injectors* (***injetores de meio de caminho***) são colocados entre o switch Ethernet e o dispositivo a ser alimentado. Estes injetores fornecem energia através dos pares não utilizados.

Caso seu roteador wireless suporte o padrão 802.3af, você pode simplesmente conectá-lo a um injetor. Infelizmente alguns fornecedores (notadamente, a Cisco) discordam na polaridade da energia e a conexão de um dispositivo incompatível pode danificar o injetor ou o equipamento conectado a ele. Leia detalhadamente as instruções e certifique-se de que o injetor e seu

equipamento wireless estão em concordância quanto aos pinos e a polaridade usada para a alimentação.

Caso seu equipamento wireless não suporte a alimentação pela Ethernet, você ainda pode valer-se dos pares não utilizados em um cabo CAT5 para o transporte da energia. Você pode usar tanto um ***injetor POE passivo*** como simplesmente construir um você mesmo. Estes dispositivos permitem a conexão manual de energia aos pares não utilizados em uma ponta do cabo e a conexão da outra ponta em uma barra de conexão inserida na entrada de energia do equipamento alimentado. Um par de dispositivos POE passivos pode ser adquirido por menos de 20 dólares.

Para construir o seu, você precisará descobrir a potência que o dispositivo necessita para operar, provendo ao menos a quantidade necessária de tensão e corrente, em adição às perdas no cabo Ethernet. Você não irá querer fornecer muita potência, já que a resistência de um cabo fino pode apresentar perigo de incêndio. Utilize a calculadora online fornecida neste site para obter a queda de voltagem para uma determinada distância em um cabo CAT5: *http://www.gweep.net/~sfoskett/tech/poecalc.html*

Uma vez sabendo da potência e polaridade necessárias em seu equipamento wireless, monte um cabo CAT5 usando apenas os pares para os dados (1-2 e 3-6). Agora, simplesmente conecte o transformador aos pares 4-5 (normalmente azul / azul-branco) e 7-8 (marrom / marrom-branco) em uma ponta e ao conector correspondente na outra.

Considerações de montagem

Em muitos casos, o equipamento pode ser montado dentro de uma construção, desde que exista uma janela com um vidro comum através do qual o feixe possa viajar. O vidro comum irá introduzir pouca atenuação, mas vidros com alguma coloração atenuam de forma inaceitável o sinal. Este tipo de montagem simplifica muito a distribuição de energia e resolve problemas de interferência da umidade e do clima, mas normalmente só é possível em regiões populadas.

Ao montar antenas em torres, é muito importante utilizar um suporte de isolamento, nunca conectando a antena diretamente à torre. Este suporte irá auxiliar em muitas funções além do próprio isolamento da antena, como seu alinhamento e proteção.

Os suportes e braçadeiras de montagem de antenas devem ser fortes o suficiente para agüentar seu peso, mantendo-a no lugar mesmo em dias com vento. Lembre-se que antenas podem funcionar como pequenas velas, colocando muita força em seu suporte em dias de ventania. Ao estimar a resistência ao vento, toda a superfície da estrutura da antena deve ser considerada, assim como a distância do centro da antena até seu ponto de conexão mecânica com a torre ou construção onde o suporte está montado. Antenas grandes, como discos parabólicos sólidos ou painéis setoriais de alto ganho tem uma considerável resistência ao vento (exercendo grandes forças sobre seus suportes). O uso de uma parabólica de grade metálica ao invés de um disco sólido ajudará a reduzir a resistência ao vento, sem maiores efeitos no

ganho da antena. Certifique-se que as braçadeiras de montagem e a estrutura de suporte são sólidas o bastante, ou sua antena ficará desalinhada com o passar do tempo (ou pior, cairá da torre!).

O suporte de montagem deve ter uma distância suficiente da torre para permitir o direcionamento da antena. Mas, a distância não deve ser grande a ponto de dificultar o acesso à antena em caso de manutenção.

Figura 8.1: Uma antena com seu suporte sendo alçado em uma torre.

O cano onde a antena é montada no suporte deve ser cilíndrico, pois a antena girará nele para seu direcionamento. Este cano deve ser montado sempre na vertical. Caso a antena seja montada em uma torre cônica, o suporte deve ser projetado adequadamente.

Como o equipamento estará montado externamente durante toda a sua vida em serviço, é importante que o aço usado tenha uma cobertura à prova d'água. O aço inoxidável é, normalmente, muito caro para a instalação de torres. A galvanização à quente é a tecnologia preferida, mas pode não estar disponível em algumas áreas. A pintura de todo o aço com uma boa tinta à prova de ferrugem também funciona. Caso a opção seja pela tinta, é importante planejar uma inspeção anual da montagem, pintando novamente sempre que necessário.

Torres estaiadas

Uma torre estaiada escalável é uma escolha excelente para muitas instalações, mas para estruturas muito altas, uma torre auto-sustentável pode ser necessária.

Na montagem de torres estaiadas, uma polia presa ao topo de um guindaste irá facilitar o trabalho. O guindaste é firmado junto à primeira seção da torre, já montada, enquanto outras duas seções são montadas à primeira com o uso de uma junta articulada. Uma corda, passando pela polia presa ao guindaste, auxilia no levantamento das próximas seções. Uma vez feito o nivelamento da nova seção, ela deve ser bem presa à seção anterior. O guindaste é removido e a operação pode ser repetida para quantas seções de torre forem necessárias, até atingir a altura desejada[2].

Figura 8.2: Uma torre estaiada escalável.

Torres auto-sustentáveis

Torres auto-sustentáveis são caras, mas algumas vezes necessárias, especialmente quando uma elevação muito grande é requerida. Elas podem ser simples como um poste pesado enterrado em uma base de concreto, ou complicadas como uma torre de rádio profissional.

---

2. N. do T. - É difícil visualizar este processo apenas com a leitura do texto e o guindaste aqui mencionado é específico para a montagem de torres. No site *http://www.tower-technologies.com/GinPole.htm* você tem uma boa representação gráfica do que o texto descreve. Prenda as estaias cuidadosamente, certificando-se de usar a mesma tensão em todos os pontos de âncora apropriados. Escolha estes pontos de forma que os ângulos formados pela linha entre eles e o centro da torre estejam tão igualmente espaçados quanto possível.

Figura 8.3: Uma torre auto-sustentável simples.

Uma torre já existente pode, algumas vezes, ser disponibilizada para o uso de “inquilinos”, mas torres com antenas de transmissão de estações AM devem ser evitadas, já que toda a estrutura é ativa (não apenas a antena). Torres com antenas de FM são aceitáveis, desde que alguns metros de separação seja possível entre as antenas. Saiba que mesmo que antenas transmissoras adjacentes possam não influir em sua conexão wireless, antenas FM de alta potência podem gerar interferências em seu cabeamento wireless. Sempre que usar uma torre de antena altamente populada, seja muito cuidadoso com o aterramento e use sempre cabos blindados.

Figura 8.4: Uma torre muito mais complexa.

Montagens em telhados

Suportes não invasivos podem ser usados para a montagem de antenas em telhados planos. Eles consistem em um tripé, montado em uma base de metal ou madeira. A base é fixada com o peso de tijolos, sacos de areia, galões de água ou qualquer outro peso. O uso de um suporte deste tipo elimina a necessidade de furos no telhado, evitando potenciais vazamentos.

Figura 8.5: Esta base metálica pode ser fixada com sacos de areia, pedras ou garrafas de água para a estabilidade da plataforma, sem a necessidade de furos no telhado.

Montagens de parede ou amarras de metal podem ser usadas em estruturas existentes como chaminés ou as laterais de prédios. Se as antenas tiverem que ser montadas acima de quatro metros do telhado, uma torre escalável pode ser uma solução melhor para permitir o fácil acesso ao equipamento e evitar o movimento da antena em caso de ventania.

Metais dissimilares

Para minimizar a corrosão eletrolítica quando dois metais diferentes fazem contato em um meio úmido, seus potenciais eletrolíticos devem ser o mais próximo possível. Use graxa dielétrica na conexão entre dois metais diferentes para a precaução contra o efeito da eletrólise.

O cobre nunca deve estar em contato direto com material galvanizado sem a devida proteção da junção. A água que entra em contato com o cobre contém íons e irá remover a cobertura galvanizada (zinco) da cobertura da torre. O aço inoxidável pode ser usado como material de proteção entre o cobre e a torre galvanizada, mas lembre-se que o aço inoxidável não é um bom condutor. Desta forma, a área de superfície de contato deve ser grande e a proteção de aço inoxidável deve ser fina. O material de junção pode também ser montado na forma de uma cobertura de proteção, evitando o contato da água com os metais dissimilares.

Protegendo conectores de microondas

Vazamentos de umidade em conectores são, provavelmente, a causa mais observada de falhas em links de rádio. Aperte firmemente os conectores, mas nunca use alicates ou outras ferramentas para fazer isso. Lembre-se que metais expandem e contraem de acordo com mudanças de temperatura e conectores muito apertados podem quebrar quando estas mudanças forem extremas.

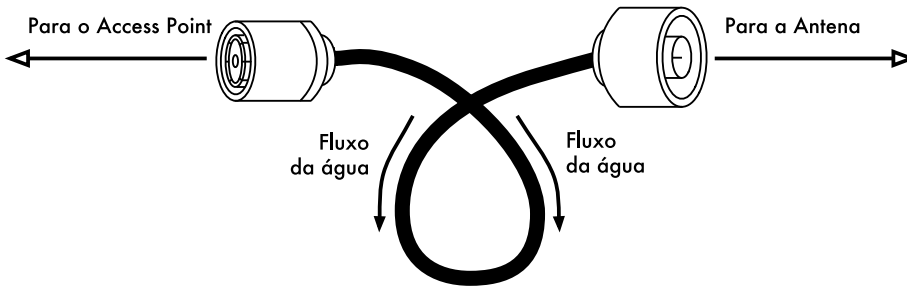


Figura 8.6: Um anel de gotejamento força a água da chuva para fora dos conectores.

Uma vez presos, os conectores devem ser protegidos por uma camada de fita isolante, coberta por uma camada de fita selante e, finalmente, coberta por outra camada de fita isolante. O selante protege o conector da água que possa escorrer por ele, enquanto a outra camada de fita isolante protege o selante dos danos causados por raios ultravioleta (UV). Os cabos devem ter um anel de gotejamento (ver **Figura 8.6**) para evitar que a água escorra para dentro do transceptor.

Segurança

Sempre use equipamento de segurança preso à torre quando necessitar trabalhar no alto da mesma. Caso você nunca tenha trabalhado em uma torre, contrate um profissional para fazê-lo. Em muitos países, apenas trabalhadores especialmente treinados podem trabalhar em torres acima de uma determinada altura.

Evite trabalhar em torres na presença de fortes ventos ou tempestades. Sempre escale com um parceiro e sempre na presença de muita luminosidade. O trabalho em uma torre normalmente toma mais tempo do que o planejado. Lembre-se que é **extremamente** perigoso trabalhar no escuro. Reserve bastante tempo para o trabalho antes do sol se por. Caso comece a escurecer, saiba que a torre estará lá na manhã seguinte, aí você pode retomar o trabalho depois de uma boa noite de sono.

Alinhando antenas em um link de longa distância

Para alinhar propriamente as antenas em uma longa distância você irá precisar de algum tipo de ferramenta em que pode observar instantaneamente a potência do sinal recebido no alimentador da antena. Assim você poderá fazer pequenas mudanças no alinhamento da antena enquanto observa o que acontece com o sinal, fixando a antena quando a maior potência do sinal for encontrada.

O melhor conjunto de ferramentas para o alinhamento de antenas consiste em um ***gerador de sinal*** e um ***analisador de espectro***, de preferência um em cada lado do link. Com o gerador de sinal em uma ponta do link e o analisador de espectro na outra, você pode observar a potência recebida no sinal em tempo real, de acordo com as várias posições da antena. Assim que a potência máxima for encontrada em um lado do link, o analisador e o gerador podem ser trocados de lugar e o processo repetido para o outro lado.

O uso de um gerador de sinal é melhor do que usar o próprio rádio do cartão wireless, já que o gerador pode emitir uma portadora constante de rádio-freqüência. Um cartão Wi-Fi emite muitos pacotes discretos de informação, ligando e desligando muito rapidamente o transmissor. Isto pode ser difícil de ser verificado com um analisador de espectro, especialmente em áreas de muito ruído.

Obviamente, o custo de um gerador de sinal calibrado e de um analisador de espectro que trabalhe na freqüência de 2,4 GHz (ou mesmo de 5 GHz, no caso do 802.11a) está além do orçamento da maioria dos projetos. Felizmente, existe um bom número de ferramentas baratas que podem ser utilizadas em substituição.

Um gerador de sinal barato

Há muitos transmissores baratos que usam a banda ISM de 2,4 GHz. Por exemplo, telefones sem fio, monitores de bebês e transmissores de televisão em miniatura geram um sinal contínuo de 2,4 GHz. Transmissores de TV (também chamados de ***emissores de vídeo***) são bastante úteis, já que freqüentemente incluem um conector SMA para antena externa e podem ser alimentados por uma bateria pequena.

Os transmissores de vídeo usualmente têm o suporte para três ou quatro canais. Mesmo que eles não correspondam diretamente aos canais Wi-Fi, eles permitem que você teste a faixa baixa, média e alta da banda.

Para que funcione em 5 GHz, você deve usar o transmissor de vídeo combinado com um conversor de 2,4 GHz para 5 GHz. Eles são um tanto caros (de 300 a 400 dólares cada) mas ainda assim mais baratos do que um gerador de sinal de 5 GHz e um analisador de espectro.

Independente do que você escolher como fonte de sinal, você precisará de uma maneira de visualizar o nível do sinal recebido na outra ponta do link. Mesmo que o preço dos analisadores de espectro de 2,4 GHz esteja caindo lentamente, eles ainda custam alguns milhares de dólares, mesmo usados.

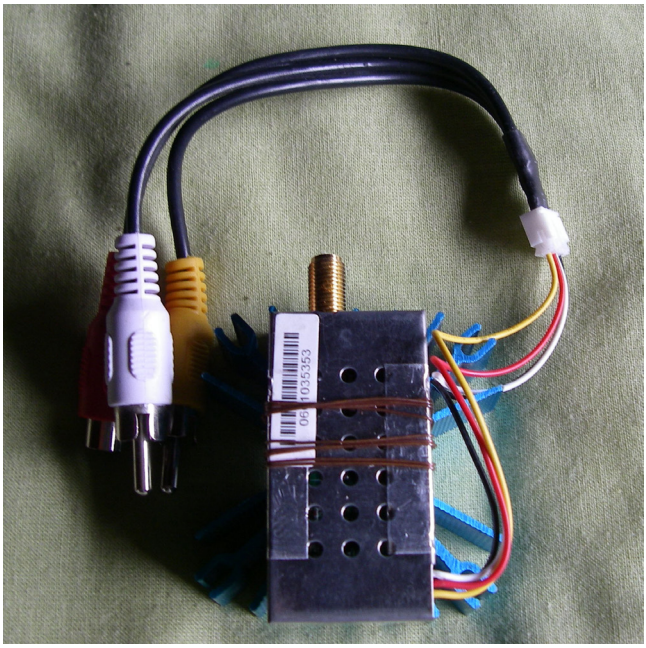


Figura 8.7: Um transmissor de vídeo de 2,4 GHz com um conector SMA para a antena externa.

Wi-Spy

O Wi-Spy é um analisador de espectro USB fabricado pela MetaGeek (*http://www.metageek.net/*). Ele é um receptor bastante sensível em um formato pequeno (o mesmo de um cartão de memória USB).

Figura 8.8: O analisador de espectro USB Wi-Spy.

A versão mais recente do Wi-Spy possui uma melhor dinâmica de variação de freqüências e um conector para antena externa. Ele também vem com um software analisador de espectro, muito bom, para Windows chamado Chanalyzer. Ele fornece visualizações instantânea, média, níveis máximos, topográfica e espectral.

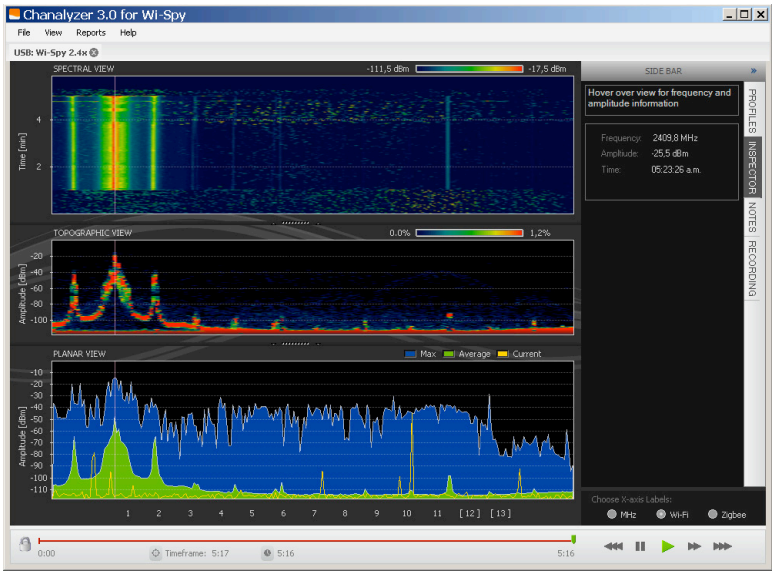


Figura 8.9: O pico que pode ser notado à esquerda do gráfico foi causado por um transmissor de TV de 2,4 GHz de alta potência.

Há um software gratuito excelente para o Mac OS X chamado EaKiu (*http://www.cookwareinc.com/EaKiu/*). Além das visualizações padrão, ele também fornece uma visualização animada em 3D e tem o suporte a múltiplos dispositivos Wi-Spy.

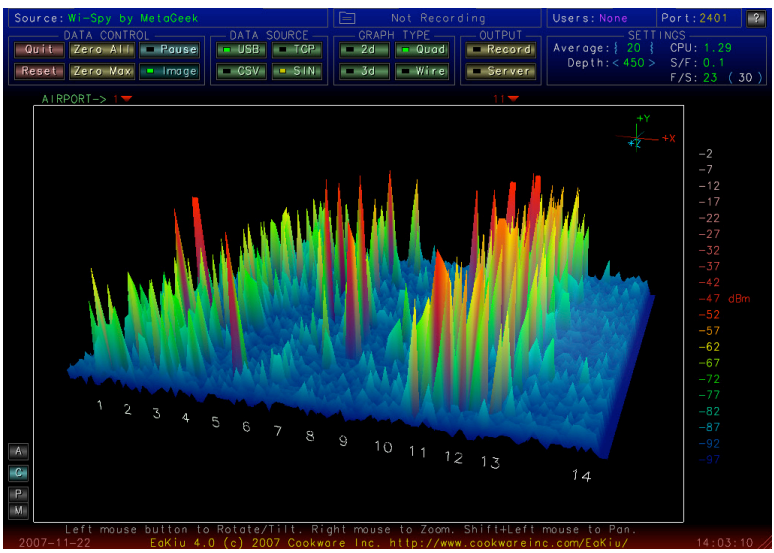


Figura 8.10: La presentación EaKiu en 3D le permite rotar y agrandar cualquier parte del gráfico en tiempo real. Hay probablemente una red Wi-Fi en el canal 11, con otras fuentes de ruido más abajo en la banda.

Para os usuários do Linux, o Wi-Spy é suportado pelo projeto Kismet Spectrum-Tools (*http://kismetwireless.net/spectools/*). Este pacote inclui ferramentas de linha de comando e uma interface gráfica construída com o GTK.

Outros métodos

Alguns roteadores wireless (como o Mikrotik) fornecem uma ferramenta de alinhamento de antena, que mostra uma barra que se movimenta para representar a potência recebida. Quando a barra está na posição máxima, a antena está alinhada. Em alguns roteadores você pode ativar um modo de informação em áudio, fazendo com que o roteador emita um tom grave que muda de afinação de acordo com a potência recebida.

Caso você não tenha um analisador de espectro, um Wi-Spy ou um dispositivo com um modo de alinhamento de antena, você precisará usar o sistema operacional para ter informação sobre a qualidade do link wireless. Um método simples de fazer isto no Linux é deixar o comando **`iwconfig`** rodando constantemente, como no exemplo abaixo:

```
wildnet:~# while :; do clear; iwconfig; sleep 1; done
```

Isto irá mostrar o estado de todos os cartões de rádio no sistema, atualizando a informação a cada segundo. Note que isto apenas funciona do lado cliente de um link. No access point (em modo master) você deve usar o comando **`iwspy`** para coletar estatísticas para o endereço MAC do 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
```

Você pode usar o laço **`while`** (como no exemplo anterior) para atualizar continuamente o estado do link.

```
wildnet:~# while :; do clear; iwspy; sleep 1; done
```

Procedimento para o alinhamento da antena

A chave para o sucesso no alinhamento de antenas em um link de grande distância é a comunicação. Caso você mude muitas variáveis simultaneamente (digamos, um time começa a mexer em uma antena enquanto outro tenta fazer a leitura da força do sinal), o processo irá levar o dia inteiro e resultará, provavelmente, em antenas desalinhadas.

Você terá duas equipes. Idealmente, cada equipe deve ter, no mínimo, duas pessoas: uma equipe fará a leitura dos sinais, comunicando-os para a equipe remota. A outra equipe irá manipular a antena. Mantenha estes pontos em mente quando trabalhar com links de longa distância.

1. **Teste previamente todo o equipamento**. Você não irá querer mexer em ajustes quando for a campo. Antes de separar o material e prepará-lo para o transporte, ligue todos os equipamentos, conecte todos os cabos e antenas e garanta que você têm uma conexão

funcional entre os dispositivos. Você deve ser capaz de conseguir novamente a mesma conexão sem a necessidade de um novo acesso como administrador ao equipamento ou mudar alguma coisa. Agora é o momento ideal para um acordo sobre a polarização da antena (veja o **Capítulo 2** caso você não saiba o que significa polarização).

2. **Tenha equipamentos reserva para a comunicação**. Mesmo que telefones celulares sejam o suficiente para o trabalho em cidades, a recepção pode ser ruim ou inexistente em áreas rurais. Tenha consigo um rádio FRS ou GMRS potente ou, caso a equipe tenha licença para a operação de rádio-amador, eles também podem ser usados. O trabalho à distância pode ser frustrante se você tiver que ficar constantemente perguntando "estão me ouvindo agora?". Escolha seu canal de comunicação e teste seus rádios e baterias antes de sair a campo.

3. **Leve uma máquina fotográfica**. Reserve tempo para documentar a localização da torre, incluindo a vista ao redor do local e obstruções. Isto pode ser muito útil depois para determinar a viabilidade de um novo link para o mesmo local, sem que para isto seja necessário um novo deslocamento. Caso esta seja sua primeira viagem ao local, marque também as coordenadas com um GPS, assim como a sua elevação.

4. **Comece estimando a direção da antena e a elevação**. Para começar, ambas as equipes devem usar triangulação (usando coordenadas fornecidas por um GPS ou um mapa) para ter uma idéia básica da posição da outra ponta do link. Com a ajuda de uma bússola, faça um alinhamento prévio da antena. Pontos de referência grandes também auxiliam no direcionamento. Caso você consiga enxergar a outra ponta do link com um binóculo, melhor ainda. Uma vez que você estimou a direção, comece a fazer a leitura da potência do sinal. Se você está perto o suficiente da outra ponta do link e fez uma boa estimativa, é bem provável que você já tenha um sinal.

5. **Se tudo o mais falhar, construa seu próprio ponto de referência**. Alguns tipos de terrenos tornam difícil determinar a direção da outra ponta do link. Caso você esteja construindo seu link em uma área com poucos pontos de referência, um feito à mão, como uma pandorga (pipa), balão, luz de sinalização, fogos de artifício ou mesmo sinais de fumaça, pode ajudar. Você não necessita obrigatoriamente de um GPS para ter uma idéia da direção para a qual apontar a sua antena.

6. **Teste o sinal em ambas as direções, mas não simultaneamente**. Uma vez que ambas as pontas fizeram suas estimativas, aquela que tiver a antena de menor ganho deve fixá-la em sua posição. Usando uma boa ferramenta de monitoramento (como Kismet, Netstumbler ou um cliente wireless integrado), a equipe com a antena de maior ganho deve movê-la lentamente na posição horizontal, observando o

medidor de sinal. Quando a melhor posição for alcançada deve-se tentar alterar a elevação da antena. Depois que o melhor sinal for detectado, a antena deve ser firmemente fixada e a outra equipe deve ser avisada para que tente posicionar a sua antena. Repita este processo algumas vezes até que a melhor posição possível para as duas antenas seja encontrada.

7. **Não toque a antena enquanto fizer leituras de sinal**. Seu corpo irá afetar o padrão de irradiação da antena. Não toque na antena e não fique na direção do sinal enquanto estiver fazendo leitura da força do sinal. O mesmo vale para a equipe do outro lado do link.

8. **Não tenha medo de mover a antena além do melhor sinal recebido**. Como vimos no **Capítulo 4**, padrões de irradiação podem incorporar muitos lóbulos menores de sensitividade, além do lóbulo principal. Se o sinal recebido for misteriosamente pequeno, você pode ter encontrado um lóbulo lateral. Continue movendo vagarosamente a antena além deste lóbulo para ver se você detecta o lóbulo principal.

9. **O ângulo da antena pode parecer completamente errado**. O lóbulo principal da antena freqüentemente irradia levemente para um lado ou outro do centro visual da antena. Alguns pratos parabólicos podem parecer apontar muito para baixo, ou mesmo diretamente para o chão. Não se preocupe com a aparência da antena. Sua preocupação deve ser encontrar a posição que proporcione o maior nível de sinal recebido.

10. **Verifique duplamente a polarização**. Pode ser frustrante tentar alinhar uma antena parabólica e descobrir, depois de algum tempo, que a equipe na outra ponta do link está usando uma polarização oposta. A polarização deve ser discutida antes da saída à campo, quando as equipes devem estar de acordo sobre a forma como ela será feita. Mas caso um link apresente um sinal que teima em ser fraco, uma nova verificação da polarização é sempre aconselhável.

11. **Se nada funcionar, verifique todos os componentes, um de cada vez**. Os dispositivos de ambos os lados do link estão ligados? Os conectores e seus cabos estão devidamente conectados, sem nenhum dano ou componentes suspeitos? Conforme discutimos no **Capítulo 8**, técnicas apropriadas de diagnósticos economizam tempo e evitam frustrações. Trabalhe com calma e sempre comunique o estado de sua análise ao time da outra ponta, que também deve fazer o mesmo.

Através do trabalho metódico e da boa comunicação você irá completar o trabalho de alinhamento das antenas em pouco tempo. Feito de maneira apropriada, este trabalho será divertido!

Proteção contra surtos elétricos e raios

A alimentação elétrica é o maior desafio para grande parte das instalações no mundo em desenvolvimento. Mesmo onde existem redes elétricas, elas são, com freqüência, pouco controladas, com flutuações dramáticas de tensão e suscetíveis a raios. A proteção contra surtos é crítica não apenas para preservar os equipamentos wireless, mas todos os demais equipamentos conectados à eles.

Fusíveis e disjuntores

Fusíveis são extremamente importantes e freqüentemente negligenciados. Em áreas rurais, e mesmo em muitas áreas urbanizadas de regiões em desenvolvimento, fusíveis são difíceis de encontrar. Apesar de serem mais caros, é sempre mais prudente a utilização de disjuntores. Pode ser que eles tenham que ser importados, mas não devem ser deixados de lado. Com muita freqüência, fusíveis são substituídos por moedas disponíveis nos bolsos. Em um caso recente, todos os equipamentos eletrônicos de uma estação de rádio, na zona rural, foram destruídos quando um raio atravessou os circuitos sem um disjuntor ou mesmo um fusível instalado para a proteção.

Como fazer o aterramento

O aterramento apropriado não é, necessariamente, um trabalho complicado. No aterramento você deve atender a dois requisitos: fornecer um curto-circuito para um raio elétrico e fornecer um circuito para que o excesso de energia seja dissipado.

O primeiro passo é proteger o equipamento de ser atingido por um raio direto ou próximo. O segundo passo é fornecer um caminho para dissipar a energia em excesso que, de outra maneira, poderia gerar eletricidade estática. A estática pode causar significativa degradação na qualidade do sinal, especialmente em receptores sensíveis (como VSAT, por exemplo). Fornecer o curto-circuito é fácil. A pessoa responsável pela instalação deve simplesmente tornar o mais curto possível o caminho entre o ponto mais alto da superfície condutiva (um pára-raios) e o chão. Quando um raio atinge o pára-raios, a energia irá viajar pelo caminho mais curto até o chão, sem passar pelo equipamento. O chão deve estar preparado para suportar altas voltagens (você precisará de fio de grosso calibre para o aterramento, como um AWG 8 trançado).

Para aterrar o equipamento, monte um pára-raios acima do mesmo, em uma torre ou outra estrutura. Depois, use um fio condutor grosso para conectar o pára-raios a algo que esteja devidamente aterrado. Tubos de cobre subterrâneos podem constituir um bom aterramento (dependendo de sua profundidade, umidade, salinidade, quantidade de metal e conteúdo orgânico no solo). Em muitos locais do oeste africano os canos não estão enterrados e aterramentos instalados previamente são freqüentemente inadequados devido à má condutividade do solo (típico em estações secas em regiões tropicais). Há três maneiras fáceis de se medir a eficiência de seu aterramento:

1. O menos preciso consiste em ligar um no-break de boa qualidade ou uma barra de tomadas em um circuito que tenha um detector de aterramento (um LED indicativo). Este LED é iluminado pela energia que é dissipada pelo circuito de aterramento. Um aterramento efetivo irá dissipar pequenas quantidades de energia para a terra. Algumas pessoas de fato usam isto para piratear um pouco de iluminação grátis, já que esta energia não aparece na tarifação da eletricidade.
2. Pegue um soquete com uma lâmpada de baixa potência (30 Watts), ligue um conector do soquete ao aterramento e o outro a um fio fase da rede elétrica. Se o aterramento for bom, a lâmpada deve ter um bom brilho.
3. A forma mais sofisticada é a simples medida da impedância entre o circuito positivo e o aterramento.

Caso o aterramento não seja eficiente, você precisará enterrá-lo em maior profundidade (onde o solo é mais úmido, com mais matéria orgânica e metais) ou tornar o solo mais condutivo. Uma técnica comum, em casos onde não existe muito solo disponível, é cavar um buraco de um metro de diâmetro e dois metros de profundidade. Coloque neste buraco uma peça condutiva de metal com algum peso. Isto é, algumas vezes, chamado de um "chumbo", mas pode representar qualquer peça de metal que pese 50 kg ou mais, como uma roda metálica ou uma bigorna de ferro. A seguir, preencha o buraco com carvão e sal, tapando com terra. Encharque a área de forma que o carvão e o sal se desmanchem no buraco, compondo uma área condutiva ao redor de seu "chumbo", melhorando a eficiência do aterramento.

Se um cabo de rádio está sendo utilizado, ele também pode servir para aterrar a torre, ainda que um projeto mais confiável consista na separação do aterramento da torre e do cabo. Para aterrar o cabo, simplesmente remova um pedaço de seu encapamento no ponto próximo ao aterramento, antes de sua entrada no local da instalação dos equipamentos. A seguir, conecte o cabo ao aterramento neste ponto onde sua capa foi removida, soldando-o ou usando um conector de boa condutividade. Esta conexão, então, precisa ser protegida contra a água.

Estabilizadores de potência e reguladores

Há muitas marcas de estabilizadores de potência, mas a maioria deles é digital ou eletromecânico. Estes últimos são mais baratos e comuns. Estabilizadores eletromecânicos pegam a energia em 220 V, 240 V ou 110 V e usam esta energia para girar um motor, que sempre irá produzir a voltagem desejada (normalmente 220 V). Isto costuma funcionar, mas estes dispositivos oferecem pouca proteção contra raios ou outros surtos de energia. Eles costumam queimar ao primeiro raio. Uma vez queimados, eles podem gerar uma outra voltagem de saída, tipicamente errada.

Reguladores digitais estabilizam a energia usando resistores e outros componentes de estado sólido. Eles são mais caros, mas menos suscetíveis à queimas.

Sempre que possível, use um regulador digital. Eles compensam o custo adicional e oferecem uma melhor proteção ao restante do equipamento. Certifique-se de inspecionar todos os componentes em seu sistema de energia (incluindo o estabilizador) depois de uma tempestade elétrica.

9
Diagnósticos

A forma como está estabelecida a estrutura de suporte de sua rede é tão importante quanto o tipo de equipamento utilizado. Ao contrário do que acontece com redes cabeadas, os problemas em redes sem fio são freqüentemente invisíveis e podem requerer mais habilidade e tempo para seu diagnóstico e solução. Interferência, vento e novas obstruções físicas podem fazer com que um link, estável há muito tempo, deixe de funcionar. Este capítulo irá detalhar uma série de estratégias que o ajudarão na construção de uma equipe que irá dar o efetivo suporte à sua rede.

Montando seu time

Cada vila, empresa ou família possui indivíduos apaixonados por tecnologia. Eles são os que vemos instalando um cabo de televisão, consertando um rádio ou colocando um novo acessório em uma bicicleta. Estas pessoas se interessarão por sua rede e buscarão aprender o máximo possível sobre ela. Mesmo que estas pessoas constituam-se em recursos inestimáveis, você deve evitar concentrar todo o conhecimento especializado sobre redes wireless em apenas uma pessoa. Caso seu único especialista perca o interesse ou encontre algum emprego melhor, ele levará todo o conhecimento com ele quando partir.

Podem existir também muitos adolescentes ou jovens adultos ambiciosos e interessados que dedicarão o tempo necessário para ouvir, ajudar e aprender sobre sua rede. Novamente, eles ajudam bastante e aprendem rapidamente, mas as pessoas que mais devem interessar à equipe de suporte são aquelas que poderão estar presentes nos próximos meses e anos. Os jovens partirão para universidades ou encontrarão empregos, especialmente aqueles mais ambiciosos que querem estar constantemente envolvidos no trabalho. Os mais jovens também costumam ter pouca influência na comunidade, enquanto os mais velhos são, normalmente, mais capazes de tomar decisões que afetem a rede de uma forma integral. Mesmo que estes tenham menos tempo para aprender e possam parecer menos interessados, seu envolvimento e treinamento adequado sobre o sistema pode ser crítico.

Por isso, uma estratégia-chave na construção de uma equipe de suporte é o equilíbrio e a distribuição do conhecimento entre aqueles melhor colocados para

o suporte à rede por um longo período. Você deve envolver os jovens, mas sem deixar que eles capitalizem o uso ou o conhecimento dos sistemas. Encontre pessoas que estejam comprometidas com a comunidade, tenham raízes nela, possam ser motivados e então os ensine. Uma estratégia complementar é segmentar funções e tarefas, documentando toda a metodologia e processos. Desta forma, as pessoas podem ser facilmente treinadas e substituídas com pouco esforço.

Por exemplo, em um projeto a equipe selecionou um jovem brilhante que havia se formado na universidade e retornado à sua vila. Ele estava muito motivado e aprendeu rapidamente. Por causa disso, ele foi treinado ainda mais do que havia sido feito anteriormente e era capaz de lidar com toda uma variedade de problemas: desde consertar um PC até refazer um cabo Ethernet. Infelizmente, dois meses após o lançamento do projeto ele recebeu uma oferta de emprego do governo e deixou a comunidade. Nem mesmo um salário melhor poderia mantê-lo, uma vez que a perspectiva de estabilidade em um emprego no governo era muito atrativa. Todo o conhecimento sobre a rede e como dar suporte a ela partiu com ele. A equipe de treinamento foi obrigada a retornar e começar um novo processo educativo. A estratégia seguinte foi dividir funções e treinar pessoas com raízes fixas na comunidade: pessoas com casas e filhos, já empregadas. O tempo consumido no treinamento destas pessoas foi três vezes maior do que aquele consumido para a preparação do jovem graduado, mas a comunidade irá reter este conhecimento por muito mais tempo.

Mesmo que isto pareça uma sugestão para que você mesmo selecione os que devem estar envolvidos, esta não é normalmente a melhor idéia. Com freqüência, o melhor é encontrar uma empresa local parceira, ou um gerente local, que trabalhe no encontro da equipe técnica certa. Valores, história, política local e muitos outros fatores são importantes para pessoas locais, enquanto são totalmente desconhecidos para as que não fazem parte da comunidade. O melhor é preparar seu parceiro local, fornecendo a ele bons critérios de seleção e estabelecendo limites. Estes limites podem incluir regras sobre nepotismo e favoritismo, ainda que estas regras devam considerar situações específicas do local. Pode ser impossível dizer que não devam ser contratados parentes, mas é aconselhável fornecer meios que garantam o equilíbrio e possíveis verificações. Quando um candidato for algum parente, critérios claros devem ser estabelecidos e uma segunda autoridade, não familiar ao candidato, deve tomar a decisão final. Também é importante que o parceiro local tenha garantida sua própria autoridade e que ela não seja colocada em questão pelos organizadores do projeto, comprometendo sua gestão. Ele será capaz de julgar quem será a melhor pessoa com a qual trabalhar. Com o devido treinamento neste processo, seus requerimentos devem ser satisfeitos.

O diagnóstico e suporte à tecnologia é uma arte abstrata. Na primeira vez que você olha para uma pintura abstrata, ela pode parecer um monte de pinceladas aleatórias. Depois de refletir, por algum tempo, sobre a composição você começará a apreciar a obra como um todo e uma coerência, ainda que invisível, passará a ser real. O novato que observa uma rede wireless pode ver antenas, fios, computadores, mas demorará um tempo até apreciar a função de uma rede invisível. Em áreas rurais freqüentemente existe um grande salto de compreensão antes que os usuários locais apreciem a rede invisível que passou

a existir em sua vila. Desta forma, uma introdução em fases pode ser necessária para facilitar o acesso das pessoas ao conhecimento sobre o suporte à tecnologia e sistemas. O melhor método é o envolvimento. Uma vez que os participantes estão escolhidos e comprometidos com o projeto, envolva-os o máximo possível. Deixe que eles tomem a direção. Dê a eles a ferramenta para "crimpar" os cabos (firmar os conectores aos fios dos cabos) ou o teclado e mostre como fazer o trabalho. Mesmo que você não tenha tempo para explicar todos os detalhes e mesmo que isto demore, eles precisam ser "fisicamente" envolvidos e ver não apenas o que foi feito, mas como isto foi feito.

O método científico é ensinado em praticamente todas as escolas ocidentais. Muitas pessoas aprendem sobre ele quando chegam às aulas de Ciências do ensino médio. De forma simplificada, toma-se um conjunto de variáveis e elimina-se, lentamente, tais variáveis através de testes binários até que restem poucas possibilidades, ou apenas uma. Com estas possibilidades em mente, completa-se o experimento. Verifica-se, então, se o experimento apresenta algo similar ao resultado esperado. Caso contrário, recalcula-se o que deve ser esperado e tenta-se novamente o experimento. O habitando de uma vila agrícola pode até ter sido apresentado a este método, mas provavelmente não teve a oportunidade de experimentá-lo com problemas complexos. Mesmo que eles tenham familiaridade com o método científico, eles podem não ter pensado em utilizá-lo na solução de problemas reais.

Este método é muito eficaz, apesar de consumir tempo. Ele pode ser acelerado ao se assumir premissas lógicas. Por exemplo, se um access point que está ativo há muito tempo pára de funcionar depois de uma tempestade, você pode suspeitar de um problema relacionado à fonte de alimentação e, assim, economizar algumas etapas do processo de análise. As pessoas encarregadas do suporte devem ser treinadas em diagnósticos com o uso deste método, já que existirão ocasiões onde o problema não será conhecido ou estará evidente. Árvores de decisão simples ou fluxogramas para o teste de variáveis podem ser feitos, auxiliando na eliminação destas variáveis até que o problema seja isolado. Mas obviamente, estes fluxogramas não devem ser seguidos cegamente.

Com freqüência é mais fácil ensinar este método ilustrando-o com um problema que não seja totalmente tecnológico. Por exemplo, faça com que seus estudantes desenvolvam um procedimento de solução de um problema que seja simples e familiar, envolvendo um televisor que funciona com pilhas. Comece sabotando o aparelho, colocando nele baterias descarregadas. Desligue a conexão com a antena. Coloque um fusível queimado. Teste os alunos, deixando claro que cada problema tem sintomas específicos. Uma vez consertado o televisor, faça com que eles apliquem o mesmo método a problemas mais complexos. Em uma rede, você pode modificar um endereço IP, trocar ou danificar um cabo, usar um SSID errado ou orientar uma antena na direção errada. É importante que eles desenvolvam métodos e procedimentos para a solução destes problemas.

Técnicas apropriadas para o diagnóstico

Nenhum método de diagnóstico pode cobrir completamente todos os problemas que você irá encontrar no trabalho com redes wireless. Mas com freqüência, os problemas reduzem-se a alguns erros comuns. Aqui estão alguns pontos que devem ser mantidos em mente e que ajudarão a manter seu diagnóstico na direção correta.

- **Não entre em pânico**. Se você está diagnosticando um sistema, isto significa que em algum momento ele estava funcionando, provavelmente há pouco tempo. Antes de partir para a aplicação de mudanças, faça uma pesquisa do ambiente e verifique exatamente o que deixou de funcionar. Caso você tenha registros ou estatísticas a partir dos quais pode trabalhar, ótimo. Certifique-se de coletar, primeiro, toda a informação de forma a tomar decisões acertadas antes de aplicar mudanças.

- **Isto está ligado?** Este é o primeiro passo, que é muitas vezes esquecido até que vários outros caminhos sejam explorados. Tomadas podem ser acidentalmente (ou intencionalmente) desligadas com muita facilidade. As barras de tomadas estão conectadas a uma boa fonte de energia? Há alimentação chegando a seu equipamento? A luz de "ligado" está acesa? Isto pode parecer bobagem, mas você se sentirá ainda mais bobo quando você passar um longo tempo verificando uma antena apenas para descobrir que o AP estava todo o tempo desligado. Acredite, isto acontece muito mais do que qualquer um admita que seja verdade.

- **Qual foi a última mudança?** Se você é a única pessoa com acesso ao sistema, qual a última mudança que você fez? Caso outros tenham acesso ao sistema, quais as mudanças aplicadas por eles e quando? Quando o sistema estava funcional mais recentemente? Freqüentemente, mudanças no sistema têm conseqüências não intencionais que podem não ser notadas imediatamente. Traga o sistema para o estado anterior à última mudança e veja qual o efeito disto no problema.

- **Faça cópias de segurança** (*backups*). Isto aplica-se tanto para antes de você notar um problema quanto para depois. Caso você faça uma modificação complexa no software do sistema, um backup irá garantir que você possa trazê-lo ao estado anterior à mudança, permitindo que você recomece. Ao diagnosticar problemas muito complexos, é indicado ter uma configuração razoavelmente funcional do que outra que sequer funcione (e que será difícil de refazer confiando apenas na memória).

- **O *bom conhecido***. Esta idéia aplica-se tanto a hardware quanto a software. O bom conhecido é qualquer componente que você possa substituir em um sistema complexo para verificar se seu equivalente está em boas condições de funcionamento. Por exemplo, você deve ter um cabo Ethernet testado em seu conjunto de ferramentas. Caso você suspeite de um problema em um cabo, você pode trocar o cabo suspeito pelo bom conhecido e ver se as coisas melhoram. Este é um processo muito mais rápido e menos sujeito a erros do que recolocar os conectores em um cabo, mostrando

imediatamente se a mudança resolveu o problema. Da mesma forma, tenha sempre uma bateria reserva, cabo de antena e um CD-ROM com uma boa e conhecida configuração de seu sistema. Quando estiver resolvendo problemas complexos, salvar seu trabalho em determinados pontos permitirá sempre o retorno ao bom conhecido, mesmo que o problema ainda não esteja completamente resolvido.

- **Altere uma variável de cada vez**. Quando se está sob pressão para restabelecer o funcionamento de um sistema, tem-se a tentação de economizar passos e mudar muitas variáveis de uma única vez. Se você faz isto e o problema desaparece, você nunca será capaz de saber o que fez com que ele aparecesse. Pior do que isto, suas mudanças podem ter resolvido o problema original mas podem levar a novas conseqüências não intencionais que farão com que outras partes do sistema deixem de funcionar. Ao modificar uma variável de cada vez, você entenderá precisamente o que houve de errado inicialmente e será capaz de ver os efeitos diretos de cada mudança que aplicar.

- **Não piore as coisas**. Se você não entende completamente como o sistema trabalha, não tenha receio de chamar um especialista. Caso você não esteja certo do efeito de uma mudança em particular, que poderá causar danos em outra parte do sistema, chame alguém com mais experiência ou encontre alguma forma de testar a sua mudança sem causar danos. Colocar uma moeda no lugar de um fusível pode resolver um problema imediato mas também pode fazer com que o prédio pegue fogo.

É improvável que as pessoas que projetaram sua rede estejam disponíveis para atendê-lo 24 horas por dia na eventualidade de um problema. Sua equipe de diagnóstico deve ter boas técnicas para a solução de problemas, mas pode não ser competente o suficiente para configurar um roteador a partir do zero ou montar um conector LMR-400. Normalmente é mais eficiente a manutenção de um estoque de componentes reserva, treinando a equipe para que substitua integralmente um componente defeituoso. Isto pode significar ter um access point ou roteador pré-configurado, devidamente etiquetado e mantido em um armário trancado junto com cabos e fontes de alimentação de reserva. Sua equipe pode substituir o equipamento com defeito, mandando-o para o conserto por um especialista, ou solicitar um novo equipamento reserva. Presumindo-se que os equipamentos reserva são mantidos em segurança e são substituídos quando usados, este processo economizará muito tempo e dinheiro para todos.

Problemas comuns de rede

Problemas de conectividade costumam ser causados por falhas em componentes, mau tempo ou configurações erradas. Uma vez que a sua rede está conectada à Internet ou aberta ao público em geral, ameaças consideráveis podem vir dos próprios usuários. Estas ameaças podem variar de benignas a terrivelmente malignas, mas todas terão impacto em sua rede se ela não estiver

propriamente configurada. Esta seção relata alguns problemas comuns encontrados em redes que são utilizadas por seres humanos reais.

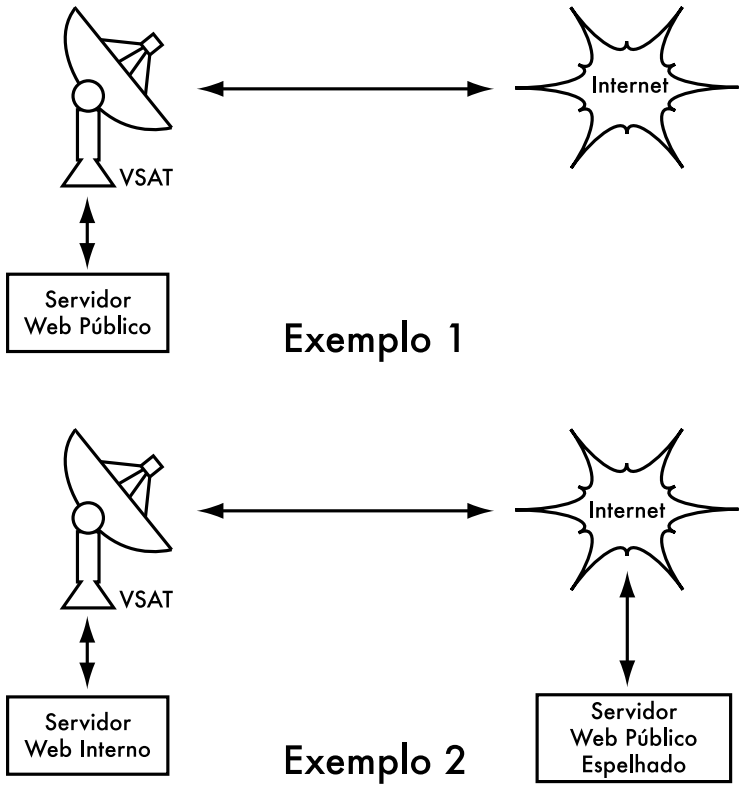


Figura 9.1: No Exemplo 1, todo o tráfego originado na Internet para o website deve atravessar o link VSAT. No Exemplo 2, o website público está hospedado em um provedor de alta velocidade na Europa, enquanto uma cópia é mantida no servidor local para o rápido acesso interno. Isto melhora a conexão VSAT e reduz o tempo de carga para os usuários do website.

Websites hospedados localmente

Caso uma universidade hospede seu website localmente, os visitantes vindos de fora do campus e do resto do mundo irão competir, com aqueles que estão na universidade, por largura de banda para a Internet. Isto inclui o acesso automático feito por mecanismos de busca que periodicamente varrem seu site inteiro. Uma solução para este problema é usar *split* DNS e espelhamento. A universidade espelha uma cópia de seus websites em um serviço de hospedagem na Europa, por exemplo, e usa o *split* DNS para direcionar o tráfego de todos os usuários de fora da universidade para o site espelho, enquanto os usuários internos acessam o mesmo site localmente. Mais detalhes sobre este tipo de configuração são fornecidos no **Capítulo 3**.

Proxies abertos

Um servidor proxy deve ser configurado para apenas aceitar conexões da rede da universidade, não do restante da Internet. Isto porque pessoas em qualquer lugar irão conectar-se e usar proxies abertos por muitas razões, como evitar o pagamento de uso de largura de banda internacional. A maneira de configurar isto depende do servidor proxy que você está utilizando. Por exemplo, você pode especificar o intervalo de IPs usado na rede de seu campus em seu arquivo **`squid.conf`**. Assim, apenas os IPs definidos poderão usar o Squid. Alternativamente, caso seu servidor proxy esteja atrás de um firewall, você pode configurar o firewall para que ele permita apenas que computadores internos tenham acesso à porta do proxy.

Servidores de email abertos (relays)

Um servidor de email mal configurado será descoberto por pessoas inescrupulosas na Internet, e será usado como um servidor de retransmissão (*relay*) de emails para o envio de mala-direta e spam. Elas fazem isto para esconder a real fonte do spam e assim não serem descobertas. Para verificar se um servidor de email está aberto, o seguinte teste deve ser feito (também em todos os servidores SMTP que estejam no perímetro da rede de seu campus, caso exista mais que um). Use o comando telnet para abrir uma conexão à porta 25 do servidor em questão (em algumas versões Windows do **`telnet`**, pode ser necessário digitar 'set local_echo' antes do texto ser visível):

```
telnet mail.uzz.ac.zz 25
```

Agora, se uma conversa interativa em modo texto se iniciar (como o exemplo a seguir), o servidor de email está aberto e pode ser usado como relay:

```
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
```

Ao invés disto, a resposta logo após **`MAIL FROM`** deve ser:

```
550 Relaying is prohibited.
```

Uma ferramenta online para este teste está disponível em sites como *http://www.ordb.org* , que também traz mais informações sobre este problema. Aqueles que enviam malas-diretas em grande quantidade (*bulk mailers*) possuem métodos automatizados para encontrar servidores abertos. Uma instituição que não protege seus servidores de emails pode estar praticamente certa de que eles serão encontrados e abusados. A configuração de um servidor, para que ele não se torne um relay aberto, consiste na especificação das redes e servidores que podem trafegar emails através de seu ***MTA*** (*Mail Transfer Agent* – ***Agente de Transferência de Mail***), como o Sendmail, Postfix, Exim ou Exchange. Esta especificação provavelmente conterá o intervalo de IPs da rede do campus.

Redes peer-to-peer

O abuso da largura de banda por programas de compartilhamento de arquivos *peer-to-peer* (P2P) como o Kazaa, Morpheus, BitTorrent, WinMX e BearShare pode ser evitado das seguintes maneiras.

- **Tornando impossível a instalação de novos programas nos computadores do campus**. Através da não concessão do acesso administrativo dos PCs aos usuários é possível evitar a instalação de programas como o Kazaa. Muitas instituições também padronizam uma instalação de desktops, onde disponibilizam o sistema operacional requerido, as aplicações necessárias e o configuram para o melhor desempenho. Este PC também é configurado de forma a evitar que os usuários instalem novas aplicações. Uma imagem em disco deste PC é então clonada para os demais, utilizando softwares como o Partition Image (*http://www.partimage.org/*) ou o Drive Image Pro (*http://www.powerquest.com/*).[1]

  De tempos em tempos, os usuários podem ter sucesso na instalação de um novo software ou causar danos ao software instalado no computador (fazendo com que este trave com freqüência, por exemplo). Quando isto acontece, o administrador pode simplesmente restaurar a imagem do disco, voltando a configuração do computador ao padrão especificado.

- **O bloqueio destes protocolos não é uma solução**. Isto porque o Kazaa e outros protocolos são inteligentes o suficiente para contornar as portas bloqueadas. O padrão do Kazaa é utilizar a porta 1214 para a conexão inicial mas se ela não estiver disponível ele irá tentar usar as portas de 1000 a 4000. Se estas estiverem bloqueadas, ele utilizará a porta 80, passando-se por tráfego web. Por esta razão, os provedores de acesso não bloqueiam, mas restringem estes protocolos P2P usando ferramentas de gestão de largura de banda.

- **Caso a limitação de largura de banda não seja uma opção, mude o leiaute da rede**. Se o servidor proxy e os servidores de email estão configurados com duas interfaces de rede (como descrito no **Capítulo 3**) e os mesmos estão configurados para não encaminhar pacotes, isto deve bloquear todo o tráfego P2P. Isto irá bloquear também todos os outros tipos de tráfego, como o Microsoft NetMeeting, SSH, softwares de VPN e quaisquer outros serviços que não sejam especificamente permitidos pelo proxy. Em redes de largura de banda pequena, a simplicidade desta configuração pode estar acima das suas desvantagens. Uma decisão sobre isto pode ser necessária e não pode ser tomada de forma leviana. Administradores de rede não conseguem simplesmente prever como os usuários farão uso criativo e inovador de

---

1. N. do T. - Vale a pena também conferir o projeto Silab (*http://www.codeplex.com/silab*), que permite a gestão de imagens de instalação de múltiplos ambientes operacionais e a sua rápida instalação em laboratórios de informática, telecentros, escritórios ou qualquer outro ambiente onde seja necessária uma instalação padronizada.

uma rede. O bloqueio forçado de todo o acesso irá evitar que os usuários façam uso de qualquer serviço (mesmo os que não consumam muita banda) que seu servidor proxy não suportar. Mesmo que isto possa ser desejável em circunstâncias onde a largura de banda é extremamente limitada, esta política de acesso não deve ser considerada como uma boa prática genérica.

Programas que se auto-instalam através da Internet

Existem programas que se instalam automaticamente e passam a consumir a largura de banda – por exemplo, o chamado Bonzi-Buddy, o Microsoft Network e alguns tipos de vermes (*worms*). Alguns destes programas são *spywares* que continuamente enviam informações sobre os hábitos de navegação web dos usuários para uma empresa em algum lugar da Internet. Tais programas podem ser evitados até algum limite com o treinamento dos usuários e do travamento dos PCs para prevenir ações administrativas por parte dos usuários normais. Em outros casos, existem soluções de software que encontram e removem estes programas problemáticos, como o Spychecker (*http://www.spychecker.com/*) ou o Ad-Aware (*http://www.lavasoft.de/*).

Atualizações do Windows

As mais recentes versões do sistema operacional Microsoft Windows assumem que um computador com uma conexão com a rede local tem também um bom link para a Internet e, automaticamente, faz o download de atualizações de segurança, correções de erros e melhorias do sistema do site da Microsoft. Isto pode consumir uma enorme quantidade de banda em um link caro para a Internet. Há duas providências que podem ser tomadas neste caso:

- **Desabilite as atualizações do Windows em todos os PCs**. As atualizações de segurança são muito importantes para os servidores, mas a necessidade destas atualizações nas estações de trabalho que estão protegidas em uma rede privada, como a de um campus, é discutível.
- **Instale um servidor para as atualizações de software**. Isto pode ser feito a partir de um programa gratuito da Microsoft que permite que você baixe as atualizações durante a madrugada para um servidor local e as distribua para os PCs a partir deste servidor. Desta forma, as atualizações do Windows não irão consumir nenhuma banda da Internet durante o dia. Infelizmente, todos os PCs clientes precisam ser configurados para usar o servidor de atualizações para que isto funcione. Caso você tenha um servidor DNS flexível, você pode configurá-lo para que receba as solicitações que vão para *windowsupdate.microsoft.com*, direcionando-as para o seu próprio servidor de atualizações. Esta opção presta-se bem para grandes redes e economiza uma enorme porção de largura de banda.

O bloqueio das atualizações do Windows no servidor proxy não é uma boa solução, porque o serviço de atualização do sistema (atualizações automáticas) fica tentando buscá-las de maneira mais agressiva e, se todas as estações de

trabalho fizerem isso, o proxy terá que lidar com uma carga de trabalho altíssima. O texto abaixo foi extraído do registro de um proxy (Squid access log) onde isto foi feito com o bloqueio de arquivos "*cabinet*" da Microsoft (.cab).

A maior parte do arquivo de log do Squid estava assim:

```
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
```

Mesmo que isto possa ser tolerável em uma rede com poucos PCs, o problema aumenta significativamente com a adição de mais computadores na rede. Ao invés de forçar o proxy a atender a pedidos dos clientes que sempre resultarão em uma resposta negativa, faz mais sentido redirecionar os clientes de atualizações de software para um servidor local que atenda a estes pedidos.

Programas que assumem a existência de um link de alta velocidade

Adicionalmente às atualizações do Windows, muitos outros programas e serviços assumem que a largura de banda não é um problema e, por isso, a consomem por motivos que o usuário não tem como prever. Por exemplo, programas de antivírus (como o Norton AntiVirus) que periodicamente se atualizam de forma automática, via Internet. Também é melhor que estas atualizações sejam concentradas em um servidor local para a posterior distribuição.

Outros programas, como o reprodutor de vídeos RealNetworks, baixam automaticamente atualizações e propagandas, assim como enviam padrões de utilização para um site na Internet. Pequenas aplicações (*applets*) aparentemente inócuas (como o Konfabulator e várias decorações para o Desktop) ficam continuamente buscando informações atualizadas em servidores na Internet. Estas buscas podem consumir poucos recursos da rede (como atualizações sobre o clima ou notícias) ou muitos recursos (como webcams). Estas aplicações podem necessitar de ajustes em seu consumo de banda (*throttle*) ou ser totalmente bloqueadas.

As mais recentes versões do Windows e MAC OS X também possuem um serviço de sincronização de horário. Isto mantém preciso o relógio do computador, através da conexão com servidores de horário na Internet. É mais

eficiente instalar um servidor de horário local e distribuir o tempo preciso a partir dele, ao invés de lotar o link de Internet com este tráfego.

Tráfego Windows no link Internet

Computadores Windows comunicam-se entre si através de ***NetBIOS*** ou ***SMB*** (*Server Message Block* – ***Bloco de Mensagem do Servidor***). Estes protocolos trabalham sobre o TCP/IP ou outros protocolos de transporte. Eles trabalham por um princípio de ***eleições*** para determinar qual computador será o ***master browser*** (navegador mestre). O master browser é um computador que mantém a lista de todos os computadores, compartilhamentos e impressoras que você pode ver na vizinhança da rede (*Network Neighborhood*) ou em "Meus locais de rede" (*My Network Places*). As informações sobre compartilhamentos disponíveis também são enviadas a todos os computadores em intervalos regulares de tempo.

O protocolo SMB é projetado para redes locais e pode causar problemas quando o computador Windows está conectado à Internet. A não ser que o tráfego SMB seja filtrado, ele tende a espalhar-se para o link Internet, desperdiçando a largura de banda contratada. Os seguintes passos devem ser tomados para que isto seja evitado:

- **Bloqueio do tráfego de saída SMB/NetBIOS no limite do roteador ou firewall**. Este tráfego consome a conexão com a Internet e, pior que isto, apresenta um risco potencial de segurança. A maioria dos vermes de Internet e ferramentas de invasão monitoram ativamente compartilhamentos SMB, explorando estas conexões para conseguir acesso à sua rede.
- **Instalação do ZoneAlarm em todas as estações de trabalho (não no servidor)**. Uma versão gratuita pode ser obtida em *http://www.zonelabs.com/*. Este programa permite ao usuário determinar quais aplicações podem (e quais não podem) estabelecer conexões com a Internet. Por exemplo, o Internet Explorer precisa conectar-se com a Internet, mas o Windows Explorer não. O ZoneAlarm pode impedir o Windows Explorer de fazer isto.
- **Redução dos compartilhamentos de rede**. Idealmente, apenas o servidor de arquivos deve possuir compartilhamentos. Você pode usar uma ferramenta como a SoftPerfect Network Scanner (de *http://www.softperfect.com/*) para identificar com facilidade todos os compartilhamentos de sua rede.

Vermes e vírus

Vermes e vírus podem gerar enormes quantidades de tráfego. O verme W32/Opaserv, por exemplo, ainda é predominante, mesmo que seja antigo. Ele espalha-se pelos compartilhamentos Windows e é detectado por outras pessoas na Internet em função de sua tentativa de seguir espalhando-se. Por isso é essencial que alguma proteção antivírus esteja instalada em todos os PCs. Além disso, o treinamento do usuário sobre a execução de arquivos anexados e a

resposta a emails não solicitados é extremamente importante. De fato, deve ser política de uso que nenhuma estação de trabalho ou servidor executem serviços desnecessários. Por exemplo, servidores Windows e Unix costumam executar, como padrão, um servidor web. Isto deve estar desabilitado caso o servidor tenha outra funcionalidade que não esta. Quanto menos serviços um computador estiver rodando, menor é a quantidade de ataques possíveis.

Loops de encaminhamento de emails

Ocasionalmente, um único usuário que comete um erro pode causar um problema. Por exemplo, uma usuária cuja conta de email na universidade está configurada para encaminhar toda a sua correspondência para uma conta no Yahoo. Esta usuária sai de férias. Todos os emails enviados a ela, em sua ausência, ainda são encaminhados a esta conta do Yahoo, que pode acumular mensagens até um determinado limite. Quando a conta no Yahoo fica lotada, os emails retornam ao emissor (a conta na universidade) que novamente os encaminha à conta do Yahoo. O "*loop*" formado pode enviar centenas de milhares de emails entre as contas, gerando um tráfego massivo e mesmo derrubando os servidores de email.

Há funcionalidades nos programas de servidores de email que podem reconhecer loops. Elas devem estar habilitadas por padrão. Os administradores devem tomar o cuidado de não desabilitar estas funcionalidades por engano ou instalar um servidor de encaminhamento SMTP que modifique os cabeçalhos dos emails de tal forma que o servidor de email não seja mais capaz de reconhecer o *loop*.

Grandes downloads

Um usuário pode iniciar, simultaneamente, o download de vários arquivos, em algumas vezes arquivos grandes, como imagens iso de 650 MB. Desta forma, um único usuário pode usar a maior parte da banda. As soluções para este tipo de problema baseiam-se em treinamento, baixa "*offline*" de arquivos e monitoramento (incluindo monitoramento em tempo real, como discutido no **Capítulo 6**). O download "*offline*" pode ser implementado ao menos de duas formas:

- Na University of Moratuwa, um sistema foi implementado com o uso de redirecionamento de URLs. Os usuários que acessam URLs do tipo ftp:// são direcionados para uma listagem onde cada arquivo possui dois links, um para o download regular e outro para o download offline. Caso o link offline seja selecionado, o arquivo é colocado em uma fila para o download posterior e o usuário é notificado por email quando o mesmo está completo. O sistema mantém armazenados os arquivos baixados recentemente, buscando-os caso sejam novamente solicitados. A fila de downloads é organizada por ordem de tamanho. Assim, os arquivos menores são baixados primeiro. Como alguma largura de banda é reservada ao sistema, mesmo em horários de pico, os usuários que solicitarem arquivos pequenos podem recebê-los em minutos, algumas vezes mais rapidamente que um download online.

- Outra solução consiste na criação de uma interface web onde os usuários podem digitar a URL dos arquivos que desejam baixar. Os arquivos serão então baixados durante a noite ou madrugada, com o uso de uma tarefa agendada (***cron job***). Este sistema funcionaria apenas para usuários que não são impacientes e sabem que arquivos grandes constituem problemas quando baixados durante o horário de trabalho.

Envio de arquivos grandes

Quando os usuários necessitam enviar arquivos grandes para colaboradores em outros lugares na Internet, eles devem ser ensinados como agendar este envio. No Windows, o envio de um arquivo para um servidor FTP remoto pode ser feito através de um script FTP, que é um arquivo de texto contendo comandos FTP, similar ao que está abaixo (salvo como **`c:\ftpscript.txt`**):

```
open ftp.ed.ac.uk
gventer
mysecretword
delete data.zip
binary
put data.zip
quit
```

Para executá-lo, digite o seguinte na linha de comando:

```
ftp -s:c:\ftpscript.txt
```

Em computadores com o Windows NT, 2000 e XP, este comando pode ser salvo em um arquivo como **`transfer.cmd`** e ser agendado para execução noturna com Scheduled Tasks (Start ➔ Settings ➔ Control Panel ➔ Scheduled Tasks) . No Unix, o mesmo pode ser feito com o uso dos comandos **`at`** ou **`cron`**.

Usuários trocando arquivos entre si

Os usuários precisam freqüentemente enviar, uns aos outros, grandes arquivos. É um desperdício de banda o envio destes arquivos pela Internet, caso o destinatário seja local. Um compartilhamento de arquivos deve ser criado no servidor Windows/Samba/Novell, onde o usuário pode colocar os arquivos para que os outros os acessem.

Alternativamente, uma interface web pode ser escrita para que o servidor web local aceite o arquivo grande e o disponibilize em uma área para download. Depois de enviar o arquivo ao servidor web, o usuário recebe a URL para o mesmo. Ele pode, então, disponibilizar esta URL para seus colaboradores locais ou externos que, ao acessar a URL, poderão baixar o arquivo. Foi desta maneira que a University of Bristol construiu seu servidor para armazenamento e distribuição de arquivos chamado FLUFF, disponibilizado em seu website *http://www.bristol.ac.uk/fluff/*. Os arquivos que estão lá armazenados podem ser acessados por qualquer um a quem se forneça o endereço. A vantagem desta solução é que os usuários podem permitir o acesso externo a seus arquivos, enquanto um mecanismo de compartilhamento apenas permite o acesso aos

usuários que estão na rede do campus. Um sistema como este pode ser facilmente implementado como um script CGI, usando Python e Apache.[2]

2. N. do T. - Existem hoje, na web, sistemas de compartilhamento de arquivos gratuitos que, dependendo do grau de privacidade da informação a ser compartilhada, podem ser utilizados. A maioria deles oferece algum grau de privacidade e limites de compartilhamento. Dentre os que se destacam está o SkyDrive da Microsoft (*http:/skydrive.live.com*).

10
Sustentabilidade Econômica

Atingir a sustentabilidade de longo prazo é, talvez, o objetivo mais difícil quando se projeta e operacionaliza redes wireless e telecentros em países em desenvolvimento. O custo proibitivo de conectividade com a Internet em muitos países em desenvolvimento impõe uma substancial despesa operacional que torna estes modelos sensíveis a flutuações econômicas e exige inovação para que se consiga a sua viabilidade. Um progresso substancial no uso de redes sem fio para a comunicação rural foi conseguido ao longo dos últimos anos, em grande parte graças aos avanços tecnológicos. Links de longa distância foram construídos, projetos de grande largura de banda são possíveis e meios seguros de acesso a redes estão disponíveis. Por outro lado, tem havido pouco sucesso no desenvolvimento de modelos de negócios sustentáveis para redes sem fio e telecentros, especialmente em regiões remotas. Baseado na experiência dos autores e na observação de redes existentes, assim como no conhecimento de melhores práticas de desenvolvimento empresarial, este capítulo irá se focar na documentação de métodos para a construção de redes wireless e telecentros sustentáveis.

Na última década houve um tremendo crescimento no acesso à Internet no mundo em desenvolvimento, onde muitas cidades têm agora acesso wireless ou ADSL e conexões de fibra ótica, o que significa uma melhoria substancial. Ainda assim, fora das áreas urbanas, o acesso à Internet ainda é um desafio formidável. Há pouca estrutura cabeada fora das grandes cidades. Assim, as redes sem fio se mantêm como uma das poucas escolhas para o fornecimento de acesso de baixo custo à Internet. Há modelos comprovados, atualmente, para o acesso rural com o uso de wireless. Na Macedônia, o projeto Macedonia Connects já conectou a maioria das escolas do país à Internet. Este livro foi escrito para aqueles que desejam conectar suas comunidades. Os modelos descritos aqui são em pequena escala e utilizam projetos de baixo custo. Nosso objetivo é fornecer exemplos de como redes wireless podem ser projetadas para ampliar o acesso sustentável onde grandes empresas de telecomunicação ainda

não instalaram suas redes, em áreas nas quais modelos tradicionais não seriam economicamente viáveis.

Duas concepções errôneas devem ser eliminadas. A primeira é de que muitas pessoas assumem que existe um modelo preferencial de negócios que irá funcionar em todas as comunidades do mundo em desenvolvimento e que a chave do sucesso é encontrar esta solução "eureca". Na prática, isso não acontece. Cada comunidade, cidade ou vila é diferente. Não há como prescrever um modelo que sirva às necessidades de todas as áreas do mundo em desenvolvimento. Apesar do fato de que alguns lugares podem ser similares em termos econômicos, as características de um modelo de negócios sustentável variam de comunidade à comunidade. Mesmo que um modelo funcione em uma vila, uma vila vizinha pode não possuir as mesmas qualidades necessárias para que o mesmo modelo seja sustentável. Nesta circunstância, outros modelos inovativos podem ser personalizados para que se encaixem no contexto desta comunidade em particular.

Outra concepção errada é que a sustentabilidade tem a mesma definição para todas as pessoas. Ainda que este termo geralmente signifique que um sistema é construído para persistir indefinidamente, este capítulo irá focar-se mais na discussão das condições econômicas (financeiras e gerenciais) do que em qualquer outro aspecto da sustentabilidade. Além disso, ao invés de se trabalhar com um horizonte de tempo indeterminado, iremos nos centrar em um período de cinco anos – o período esperado de utilidade para a infra-estrutura de informática e tecnologias wireless. Desta forma, o termo sustentabilidade será usado para encapsular um sistema projetado para durar aproximadamente cinco anos ou mais.

Na implementação e determinação do melhor modelo para uma rede sem fios ou telecentros, vários fatores-chave ajudam a garantir o sucesso. Este capítulo não tem a intenção de ser um guia para gestão de redes sem fio sustentáveis. Ao invés disto, este "how-to" (um guia de como fazer as coisas) pretende apresentar um método que irá permitir a você encontrar o modelo que mais se encaixa à sua situação. As ferramentas e informações contidas neste capítulo pretendem ajudar as pessoas, que estão começando a implantar redes sem fio no mundo em desenvolvimento, a fazer as perguntas corretas e reunir os dados necessários para definir os componentes mais apropriados em seu modelo. Tenha em mente que a determinação do melhor modelo não é um método seqüencial, onde cada passo é seguido até o final. Todos os passos estão integralmente conectados uns aos outros e, com freqüência, você irá refazer alguns passos várias vezes em seu progresso.

Crie uma declaração de Missão

O que você pretende alcançar ao implantar a sua rede? Esta parece ser uma questão simples. Mesmo assim, muitas redes wireless são instaladas sem uma visão clara do que se espera atingir, no futuro, com elas. O primeiro passo implica em documentar esta visão com as sugestões de toda a sua equipe ou grupo de funcionários. Qual é o propósito desta rede wireless? A quem esta rede pretende servir? O que a rede faz para agregar valor e atender às necessidades

da comunidade? Quais os princípios que norteiam esta rede? Uma boa declaração de missão expressa o propósito de sua rede de forma concisa, ao mesmo tempo em que explicita seus valores e serviços. Acima de tudo, sua missão fornece uma visão das aspirações de sua rede wireless.

É importante que toda a equipe que trabalha na construção de sua rede wireless esteja incluída no processo de desenvolvimento da missão, o que ajuda a criar um comprometimento ainda maior. O compromisso deve vir não apenas de sua equipe, mas também dos clientes, parceiros e doadores, que o auxiliarão a atingir seus objetivos. No mundo dinâmico da tecnologia, as necessidades dos clientes e as maneiras pelas quais elas podem ser melhor satisfeitas variam rapidamente. Desta forma, o desenvolvimento de sua missão é um processo contínuo. Depois de definir a missão inicial com sua equipe, você deve procurar saber se ela está alinhada com a realidade de seu ambiente. Com base na análise do ambiente externo e de suas competências internas, você deve modificar constantemente a sua missão, durante todo o ciclo de vida de sua rede wireless.

Avalie a demanda para as potenciais ofertas

O próximo passo na definição de seu modelo de negócios envolve a pesquisa de demanda para os produtos e serviços da rede. Em primeiro lugar, identifique os indivíduos, grupos e organizações, dentro da comunidade, que têm necessidade de informações e podem se beneficiar dos serviços oferecidos por uma rede wireless. Os usuários em potencial podem ser uma ampla variedade de indivíduos e organizações que incluem, mas não estão limitados, aos seguintes grupos:

- Associações de produtores rurais e cooperativas
- Grupos de mulheres
- Escolas e universidades
- Empresas e profissionais liberais
- Clínicas de saúde e hospitais
- Grupos religiosos
- Organizações internacionais e não governamentais (ONGs)
- Agências de governo locais e nacionais
- Estações de rádio
- Organizações na indústria de turismo

Uma vez estabelecida a lista de todos os grupos de usuários em potencial, você deve determinar quais as necessidades que eles têm em termos de informação e comunicação. Com freqüência, as pessoas confundem serviços com necessidades. Um fazendeiro pode precisar de informações sobre os preços do mercado e condições climáticas para planejar sua colheita e suas

vendas. Talvez, a forma como ele obtém esta informação seja através da Internet, mas ele também poderia recebê-la através de SMS (serviço de mensagens curtas) em seu telefone celular ou mesmo através de voz sobre IP (***VoIP—Voice over Internet Protocol***). É importante estabelecer a diferença entre os serviços e as necessidades porque podem existir diversas maneiras diferentes de satisfazer a uma única necessidade. Sua rede wireless deve explorar a melhor maneira de atender à necessidade do fazendeiro e, desta forma, criar valor ao menor custo para o usuário.

Ao atender as necessidades da comunidade, é importante descobrir de que forma a rede pode trazer o maior valor para seus usuários. Por exemplo, na pequena cidade de Douentza, em Mali, o gerente de um telecentro avaliou os potenciais benefícios do estabelecimento de uma rede wireless através da discussão com várias organizações locais. Ele entrevistou uma ONG local que tinha a necessidade de enviar relatórios mensais para sua matriz na cidade de Bamako. Naquele tempo, não havia acesso à Internet em Douentza. Para enviar uma cópia do relatório por email, a ONG enviava um de seus empregados à cidade de Mopti uma vez por mês, o que implicava em custos de viagem e hospedagem, além do próprio custo da ausência deste empregado por vários dias a cada mês. Quando o gerente do telecentro calculou o custo total da ONG neste processo, ele pôde provar o valor de uma conexão à Internet através da economia de custos para a organização.

O apoio de parceiros também pode ser necessário para a garantia da sustentabilidade de sua rede wireless. Durante esta fase, você deve estabelecer contato com parceiros em potencial, explorando o benefício de uma colaboração mútua.

Você pode avaliar a demanda em sua comunidade através do contato com seus clientes em potencial e fazendo perguntas diretamente através de pesquisas, grupos de teste, entrevistas ou reuniões com os representantes da comunidade. A realização de uma pesquisa em documentos estatísticos, relatórios de empresas, censos, revistas, jornais e outras fontes de dados também pode ajudar na construção de um retrato do ambiente local. O objetivo da coleta destes dados é a obtenção de um conhecimento aprofundado da demanda por informação e comunicação em sua comunidade, de forma que a rede que está sendo criada possa atender a esta necessidade. Freqüentemente, as redes wireless que não obtêm sucesso no mundo em desenvolvimento são aquelas que esqueceram deste passo. Toda a sua rede deve estar baseada na demanda da comunidade. Se você implementar uma rede wireless na qual a comunidade não encontre valor, ou não seja capaz de pagar por seus serviços, ela não terá sucesso.

Estabelecendo incentivos apropriados

Na maioria das vezes, há pouco incentivo econômico para o acesso participativo, de subsistência, à Internet. Além disso, o custo de aquisição de um computador, o treinamento em seu uso e a obtenção de um acesso à Internet é muito maior do que o retorno econômico que possa vir disto. Alguns desenvolvimentos recentes endereçam esta falta de incentivo, como sistemas de

informações de mercado, padrões de qualidade impostos por países importadores e troca de mercadorias. O acesso à Internet torna-se uma vantagem óbvia em situações onde o conhecimento da variação diária de preços de produtos podem representar uma diferença significativa nos lucros.

O estabelecimento de incentivos econômicos apropriados é primordial para o sucesso da rede. A rede deve fornecer valor econômico para seus usuários de forma que este seja maior que o seu custo, ou deve ser barata o suficiente para que seu custo seja marginal e viável para seus usuários. É crucial o projeto de uma rede com uso economicamente viável e custos inferiores ao valor fornecido por ela. Mais do que isto, para criar uma estrutura de incentivo apropriada, você deve envolver a comunidade, desde o princípio, na criação do projeto da rede, garantindo que a iniciativa é orgânica e não externamente imposta. Para começar, você deve tentar responder às seguintes questões:

1. Que valor econômico esta rede pode gerar para a economia local, e para quem?
2. Como pode ser quantificado o valor econômico gerado?
3. Os obstáculos existentes podem ser ultrapassados para permitir o retorno econômico?

Com a resposta a estas questões, a rede será capaz de explicitar claramente sua proposta de valor aos usuários. Por exemplo, "com o uso desta rede você poderá aumentar sua margem de lucro na venda de mercadorias em 2%", ou "a Internet irá permitir a você a economia de $X em gastos telefônicos e custos de transporte por mês". Você deve descobrir de que maneira sua rede poderá melhorar a eficiência, reduzir custos ou aumentar o lucro de seus clientes.

Por exemplo, se você fornecer informações de mercado para a indústria de milho local, terminais de sua rede devem estar perto do local onde os fazendeiros trazem sua colheita para a venda. Sua rede poderia, então, estar conectada a sistemas de informação de mercado, fornecendo planilhas diárias de preço (a um dólar cada), ou terminais para o acesso de vendedores e negociantes (a dois dólares por hora). Sua rede também poderia fornecer, aos fazendeiros, o acesso à leitura sobre novas técnicas e meios de compra de novos produtos. A conexão wireless também poderia ser oferecida aos negociantes, assim como o aluguel de dispositivos para o acesso à Internet. Caso o mercado seja pequeno, você poderá reduzir custos limitando o acesso a imagens e a outros serviços que consumam muita banda. Novamente, ao saber qual o valor que sua rede poder criar para estes negociantes, você poderá estimar o quanto eles serão capazes de pagar pelos seus serviços.

Pesquise a regulamentação local para o uso de comunicações wireless

A regulamentação local sobre redes sem fio pode afetar o tipo de modelo de negócio a ser implementado. Em primeiro lugar, pesquise o direito de uso de freqüências de 2,4 GHz sem a necessidade de licenças. Na maioria das situações, a freqüência de 2,4 GHz está liberada para o uso no mundo todo.

Ainda assim, alguns países restringem o uso sobre quem pode operar tais freqüências ou mesmo exigem o pagamento de licenças caras para esta utilização. Mesmo que redes sem fio sejam legais na Ucrânia, o governo exige uma licença bastante cara para o uso de freqüências na faixa de 2,4 GHz, o que torna o seu uso compartilhado proibitivo. Tipicamente, apenas provedores de acesso à Internet bem estabelecidos no país têm fluxo de caixa suficiente para poder pagar por essa licença de uso. Esta restrição torna difícil a uma comunidade pequena o compartilhamento de uma rede sem fio com outros parceiros ou organizações interessadas. Outros países, como a República de Mali, são mais permissivos. Uma vez que em Mali não há restrições como as da Ucrânia, é viável o compartilhamento de uma conexão à Internet em pequenas comunidades. Você deve tomar conhecimento da legislação do local onde estabelecerá sua rede, garantindo que ela esteja dentro das leis do país e da comunidade local. Alguns gerentes de projetos foram forçados a desligar suas redes wireless simplesmente porque não sabiam que estavam agindo fora da lei.

Você também deve verificar a legislação relativa a serviços de voz sobre IP (VoIP). Muitos países em desenvolvimento ainda não definiram se VoIP é permitido. Em tais países, nada impede que você ofereça serviços de VoIP. Há casos porém, onde existem normas complicadas, como na Síria, onde o VoIP é proibido em qualquer tipo de rede, não apenas em wireless. Na Ucrânia, o VoIP é permitido apenas para ligações internacionais.

Analise os competidores

A próxima fase na avaliação de sua comunidade envolve a análise da competição em redes wireless. Tal competição inclui organizações que fornecem produtos e serviços similares (por exemplo, outro provedor de acesso wireless à Internet), organizações que são vistas como alternativas aos produtos e serviços oferecidos por sua rede (como um cybercafé) e organizações definidas como estreantes no mercado wireless. Assim que seus competidores forem identificados, você deve fazer uma pesquisa profunda sobre eles. Você poderá obter informações através da Internet, contato telefônico, materiais de propaganda e marketing, pesquisa entre clientes e visita às empresas. Crie uma pasta para cada competidor. A informação competitiva que você reúne pode incluir uma lista de serviços (incluindo informações de preço e qualidade), público-alvo, técnicas de atendimento aos clientes, reputação, marketing, etc. Certifique-se de coletar qualquer coisa que poderá ajudá-lo a determinar como posicionar sua rede dentro da comunidade.

A avaliação de seus competidores é importante por muitos motivos. Em primeiro lugar, ela ajuda a determinar o nível de saturação do mercado. Há muitos casos onde um telecentro subsidiado foi estabelecido por uma organização doadora em uma pequena vila, com demanda limitada, apesar do fato de já existir um cybercafé pertencente a alguém da comunidade. Em determinada circunstância, o telecentro subsidiado pôde manter os preços baixos, já que não tinha o compromisso de cobrir seus custos. Isto acabou por forçar o cybercafé a abandonar o negócio. Quando o subsídio acabou, o telecentro também abandonou o negócio devido ao baixo lucro e alto custo. É

necessário conhecer o que já está disponível para determinar de que forma sua rede pode agregar valor à comunidade. Adicionalmente, a análise competitiva pode estimular idéias inovadoras para a sua oferta de serviços. Há algo que você possa fazer melhor do que seus competidores para que seus serviços atendam mais eficientemente as necessidades da comunidade? Finalmente, ao analisar seus competidores a partir do ponto de vista dos clientes, entendendo suas forças e fraquezas, você pode determinar suas vantagens competitivas na comunidade. Vantagens competitivas são aquelas que não podem ser facilmente reproduzidas pelos competidores. Por exemplo, uma rede wireless que possa oferecer exclusivamente uma conexão de maior velocidade para a Internet do que os competidores é uma vantagem competitiva que facilita a utilização pelos clientes.

Determine custos iniciais, recorrentes e seus preços

Quando você planeja o estabelecimento e a operacionalização de sua rede wireless, você deve determinar os recursos necessários para iniciar o projeto assim como os custos operacionais recorrentes. Os custos iniciais incluem tudo aquilo que você deve adquirir para estabelecer sua rede wireless. Estas despesas variam do investimento inicial feito em hardware, instalações, equipamentos para os access points, hubs, switches, cabos, no-breaks, etc, aos custos para o registro de sua organização como uma entidade legal. Custos recorrentes são aqueles que você deve pagar para continuar operando sua rede wireless, incluindo o custo do acesso à Internet, telefone, pagamento de empréstimos, eletricidade, salários, aluguel, manutenção e conserto de equipamentos e investimentos regulares para a substituição de dispositivos que deixam de funcionar ou tornam-se obsoletos.

Cada equipamento pode, eventualmente, quebrar ou ficar obsoleto em algum momento e você deve reservar recursos para a sua substituição. Uma recomendação, além de prática comum para lidar com isto, é tomar o preço do equipamento e dividi-lo pelo período de tempo estimado de sua duração. Este processo é chamado de ***depreciação***. Aqui está um exemplo: um computador médio deve durar, supostamente, entre dois e cinco anos. Se o custo inicial deste computador foi de mil dólares e você pode usar este computador por cinco anos, a depreciação anual será de 200 dólares. Em outras palavras, você irá reservar 16,67 dólares a cada mês para que possa, eventualmente, substituir este computador. Para que seu projeto seja sustentável é de fundamental importância que você economize dinheiro que sirva para compensar a depreciação do equipamento a cada mês. Mantenha esta economia até que você necessite utilizá-lo na compra de um equipamento substituto. Alguns países possuem legislação tributária que determina o tempo de depreciação para diversos tipos de dispositivos. De qualquer maneira, você deve tentar ser o mais realista possível quanto ao tempo de vida de todos os equipamentos instalados, planejando cuidadosamente sua depreciação.

Tente levantar todos os seus custos antecipadamente e fazer estimativas realistas de suas despesas. A tabela a seguir (que continua na próxima página) apresenta uma forma de classificar e listar todos os seus custos. Ela é uma boa

ferramenta para estruturar os diferentes tipos de custos e o ajudará a distinguir entre custos iniciais e recorrentes.

É importante pesquisar os custos iniciais antecipadamente, fazendo estimativas realistas das despesas recorrentes. Sempre é melhor superestimar um orçamento do que subestimá-lo. Em cada projeto de redes sem fio sempre existem custos imprevistos, especialmente durante o primeiro ano de operação, quando você está aprendendo como melhor gerenciar sua rede.

Categorias de custos

Para melhorar suas chances de sustentabilidade, o melhor é manter o menor custo para a estrutura de sua rede. Em outras palavras, mantenha seu nível de despesas o mais baixo possível. Leve o tempo que for necessário para pesquisar os fornecedores, especialmente o provedor de acesso à Internet, e busque as melhores condições em serviços de qualidade. Mais uma vez, certifique-se de que o que você adquire de seus fornecedores corresponde à demanda da comunidade. Antes de instalar um link VSAT caro, tenha a certeza de que existe um número suficiente de indivíduos e organizações em sua comunidade que estão dispostos a pagar o preço para utilizá-lo. Dependendo da demanda por acesso à informação e a habilidade para o pagamento, um método alternativo de conectividade pode ser mais apropriado. Não tenha medo de "pensar fora da caixa" e de usar a sua criatividade ao determinar a melhor solução.

A manutenção de um baixo custo não deve ser conseguida em detrimento da qualidade. Equipamentos de baixa qualidade estão mais sujeitos a mal funcionamento, fazendo com que você gaste mais em manutenção ao longo do tempo. A quantidade de dinheiro que será gasta na manutenção de sua estrutura de informática e comunicação é difícil de estimar. Quanto maior e mais complexa se torna a sua infra-estrutura, mais recursos humanos e financeiros precisam ser alocados à sua manutenção.

	Custos iniciais	Custos recorrentes
Custos de trabalho	• Análises e consultorias • Custos de desenvolvimento de programas, testes, integração, etc. • Custos de instalação • Custos de recrutamento • Custos de treinamento (introdução)	• Custos de contratos de serviços e salários para empregados, incluindo seus próprios custos • Manutenção de equipamentos e custos de suporte para software, hardware e equipamentos acessórios • Equipe de segurança • Custos de treinamento (reforços)

	Custos iniciais	Custos recorrentes
Custos materiais (não de trabalho)	• Custos de aquisição e produção (para hardware como PCs, VSAT, equipamento e software para o link de rádio) • Equipamentos acessórios (como switches, cabos, geradores, no-breaks e outros) • Proteção e segurança de dados • Inventário inicial (cadeiras, mesas, iluminação, cortinas, azulejos e carpetes) • Custos para as premissas (nova construção, reforma, ar condicionado, instalação elétrica e caixas de distribuição, grades de segurança) • Custos legais, como o do registro da organização • Licenças iniciais (VSAT) • Custos iniciais de marketing (panfletos, adesivos, pôsteres, festa de lançamento)	• Custos operacionais para o hardware e sistemas operacionais (acesso à Internet, telefone, etc.) • Taxas de aluguel ou leasing • Licenças de uso • Materiais de consumo e de escritório (por exemplo, mídia para armazenamento de dados, papéis, pastas, clipes) • Custos operacionais para manutenção, proteção e segurança de dados • Mensalidades (prêmios) de seguros • Custos de energia e de garantia de fornecimento • Pagamentos de empréstimos, custos capitais para o pagamento dos custos iniciais • Custos de propaganda • Taxas locais • Serviços de contabilidade e advocacia

Muitas vezes, esta relação não é linear, mas exponencial. Se um problema de qualidade manifestar-se em seu equipamento depois de instalado, a solução custará uma grande quantidade de dinheiro. Em função disto, suas vendas irão diminuir, já que o equipamento não está em pleno funcionamento. Um exemplo interessante é o de um grande provedor de acesso wireless à Internet que possuía mais de três mil pontos de acesso em operação durante um período de tempo. Este provedor nunca deixou de funcionar, mas teve que gastar muito dinheiro para manter todos os pontos de acesso. Além disso, a empresa subestimou o pequeno ciclo de vida destes dispositivos. O hardware usado em informática e comunicação tende a tornar-se mais barato e melhor com o passar do tempo. Tão logo a empresa investiu tempo e dinheiro para instalar a versão da primeira e cara geração dos pontos de acesso 802.11b, o novo padrão “g” foi criado. Novos competidores projetaram pontos de acesso melhores e mais baratos, oferecendo acesso à Internet por um custo menor. Afinal, o provedor original foi obrigado a fechar, mesmo sendo, inicialmente, o líder do mercado. Observe a tabela a seguir para entender melhor o rápido desenvolvimento de padrões e equipamentos wireless:

Protocolo	Data de Lançamento	Taxa de transmissão típica
802.11	1997	< 1 Mbps
802.11b	1999	5 Mbps
802.11g	2003	20 Mbps
802.11a	1999, mas raro até 2005	23 Mbps
802.11y	Até o final de 2008 (estimado)	23 Mbps
802.11n	Junho de 2009 (estimativa)	75 Mbps

Tenha em mente a rápida evolução e mudanças tecnológicas e pense sobre como e quando pode ser o melhor momento para reinvestir em dispositivos novos e mais baratos (ou melhores) para manter sua infra-estrutura competitiva e atualizada. Como mencionado anteriormente, é muito importante economizar o suficiente para se ter o que gastar quando for necessário.

Uma vez identificados e mapeados seus custos, você deve determinar o quanto irá cobrar por seus serviços. Esta é uma tarefa complicada, que toma tempo para ser corretamente concluída. Estas dicas irão ajudá-lo a tomar decisões sobre o preço:

- Calcule os preços que irá cobrar de forma que eles cubram todos os custos para o fornecimento dos serviços, incluindo as despesas recorrentes
- Examine os preços de seus competidores
- Avalie quanto os clientes desejam pagar (e podem pagar) por seus serviços e certifique-se de que seus preços estejam de acordo.

É absolutamente essencial ter o plano financeiro antes de iniciar. Você precisa listar todos os seus custos iniciais e recorrentes e fazer alguns cálculos para descobrir se seu projeto pode ser sustentável.

Garantindo o investimento

Uma vez determinados os custos iniciais e recorrentes e criado o seu plano financeiro, você sabe qual o investimento necessário para ter uma rede wireless de sucesso. O próximo passo é pesquisar e garantir a quantidade apropriada de dinheiro para iniciar e colocar em funcionamento seu projeto.

O método mais tradicional de garantir o investimento para redes wireless no mundo em desenvolvimento é através de recursos vindos de doadores. Um doador é uma organização que contribui com recursos financeiros, e de outros tipos, para outra organização (ou consórcio de organizações) auxiliando-a a gerenciar projetos ou apoiar causas sociais. Como este investimento é fornecido na forma de doação, não existe a expectativa de que ele seja devolvido pelas organizações nem por seus beneficiários. Entre os doadores estão grandes

organizações internacionais como a Organização das Nações Unidas (ONU) e várias de suas agências especializadas, como o Programa das Nações Unidas para o Desenvolvimento (PNUD) e a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO). Agências governamentais especializadas em desenvolvimento internacional, como a Agência Americana para o Desenvolvimento Internacional (USAID), o Departamento do Reino Unido para o Desenvolvimento Internacional (DFID) e a Agência Canadense de Desenvolvimento Internacional (CIDA), também são consideradas doadores. Grandes fundações, como a Bill & Melinda Gates Foundation e a Soros Foundation Network, assim como empresas privadas são outros tipos de doadores.

Tipicamente, para se candidatar a estes investimentos é necessário passar por um processo competitivo ou não competitivo. O processo não competitivo é menos freqüente, de forma que este capítulo irá focar-se no processo competitivo, em um nível bem alto. Muitos doadores têm procedimentos complicados para a distribuição de recursos. Os autores deste livro não querem, de maneira alguma, simplificar demais a profundidade dos sistemas de regras e legislações. O que se pretende aqui é apenas proporcionar uma compreensão geral deste processo para as comunidades que tentam estabelecer redes wireless no mundo em desenvolvimento. Durante o processo de seleção competitiva, o doador cria um ***pedido de proposta*** (*request for proposal* – ***RFP***) ou um ***pedido para aplicação*** (*request for application* – ***RFA***), solicitando que várias organizações não governamentais, empresas privadas e seus parceiros submetam propostas detalhando seus planos para projetos dentro dos limites, objetivos e regras estabelecidas pelo doador. Em resposta a este RFP ou RFA, as ONGs e outras organizações competem através da submissão de suas propostas, que são avaliadas pelos doadores com base nos critérios previamente especificados. Finalmente, a organização doadora seleciona a proposta mais apropriada, de maior pontuação na avaliação para financiar seu projeto. Em algumas ocasiões, os doadores também fornecem fundos para o suporte operacional das organizações, mas este tipo de doação é menos comum do que o processo competitivo.

Outra forma de acesso aos fundos necessários para iniciar e manter uma rede wireless é através de ***microfinanciamento***, ou provisão de empréstimos, poupança e outros serviços financeiros básicos disponíveis às pessoas mais pobres do mundo. Iniciado de forma pioneira nos anos 70 por organizações como a ACCION International e o Grameen Bank, o microcrédito, um tipo de microfinanciamento, permite a indivíduos de baixa renda e empreendedores o recebimento de empréstimos em pequenas quantidades de dinheiro para o início de pequenos empreendimentos. Apesar do fato desses indivíduos não possuírem a maior parte das qualificações tradicionais necessárias para a obtenção de empréstimos, como situação financeira verificável, garantias hipotecárias ou emprego fixo, os programas de microcrédito têm um grande sucesso em muitos países em desenvolvimento. Normalmente, o processo requer que um indivíduo ou grupo submeta uma aplicação na expectativa de receber um empréstimo e que a organização ou indivíduo que empresta o recurso o faça na condição de que o receberá de volta com juros.

O uso de microcrédito para o financiamento de redes sem fio impõe um limite, já que este tipo de empréstimo envolve pequena quantidade de recursos financeiros. Infelizmente, pois uma grande quantidade de capital é necessária para a compra do equipamento inicial para a instalação da rede, algumas vezes o microcrédito não será suficiente. Entretanto, existem muitas outras aplicações de sucesso no uso de microcrédito que trouxeram tecnologia e seu valor para o mundo em desenvolvimento. Um exemplo é a história de operadores de telefone em uma vila. Estes empresários utilizaram empréstimos de microcrédito para adquirir telefones celulares e créditos de ligações. Eles alugam os telefones para membros da comunidade, cobrando por chamada e fazendo dinheiro suficiente para pagar seu débito e ter um retorno financeiro para eles e suas famílias.

Outro mecanismo para a obtenção de recursos para iniciar uma rede wireless é através de um fundo *angel funding*. Investidores anjos (*angel*) são aqueles indivíduos ricos que fornecem capital para o estabelecimento de negócios em troca de uma alta taxa de retorno de seu investimento. Como os negócios nos quais investem são empresas que estão se estabelecendo e, com freqüência, de alto risco, os investidores anjos tendem a esperar algo além do retorno financeiro. Muitos esperam uma posição na diretoria ou alguma outra função na organização.

Alguns investidores anjos querem um papel na empresa, enquanto outros preferem a participação em cotas da empresa que poderão ser negociadas posteriormente, garantindo sua saída do negócio. Para proteger seu investimento, os anjos pedem que a organização não tome certas decisões sem que eles sejam consultados. Por causa do alto risco envolvido em mercados em desenvolvimento, é difícil, mas não impossível, encontrar investidores anjo que apóiem a implantação de uma rede wireless. A melhor maneira de encontrar investidores em potencial é através de sua rede social e da pesquisa online.

Avalie forças e fraquezas da situação interna

Uma rede é tão boa quanto as pessoas que nela trabalham. A equipe que você montar fará a diferença entre o sucesso e o fracasso. Por isso, é importante refletir sobre a qualificação e habilidade de sua equipe, incluindo os que são seus empregados e os voluntários, levando em conta as competências necessárias para um projeto wireless. Primeiro, liste as competências necessárias para o sucesso de um projeto wireless. Áreas de capacidade devem incluir tecnologia, recursos humanos, contabilidade, marketing, vendas, negociação, jurídico e operações, entre outras. A seguir, identifique recursos locais que podem preencher estas capacidades. Faça um mapa das habilidades de sua equipe em função das competências necessárias, identificando onde podem existir vazios.

Uma ferramenta que é usada com freqüência para o apoio a esta avaliação é a análise de forças, fraquezas, oportunidades e ameaças chamada SWOT (do

inglês: *strengths*, *weaknesses*, *opportunities* and *threats*)[1]. Para conduzir esta análise, identifique suas forças e fraquezas internas e as explore com relação às oportunidades e ameaças externas em sua comunidade. É importante se trabalhar de forma realista e honesta sobre o que você é capaz de fazer bem e o que está faltando. Certifique-se de fazer a distinção entre o início de seu empreendimento e onde ele poderá estar no futuro. Suas forças e fraquezas permitem que você avalie suas capacidades internas e entenda melhor o que sua organização pode fazer, assim como os seus limites. Com o entendimento de suas forças e fraquezas e a comparação com aquelas de seus competidores, você pode determinar suas vantagens competitivas no mercado. Você pode também descobrir áreas nas quais deve melhorar. Oportunidades e ameaças são externas, permitindo a você analisar as condições do mundo real e a forma como estas condições influenciam sua rede.

O diagrama abaixo irá ajudá-lo na criação de sua própria análise SWOT para sua organização. Certifique-se de responder a todas as questões e listar suas forças, fraquezas, oportunidades e ameaças nos espaços apropriados.

Forças	Fraquezas
• O que você faz bem? • Quais os recursos individuais nos quais você pode confiar para o seu crescimento? • O que os outros vêem como suas forças? • ?	• O que você pode melhorar? • - Quais recursos você tem em menor quantidade que outros? • - O que os outros vêem como suas fraquezas? • ?
Oportunidades	**Ameaças**
• Quais as boas oportunidades que estão abertas para você? • De quais tendências você pode tirar vantagem? • O que pode tornar suas forças em oportunidades? • ?	• Quais tendências podem prejudicá-lo? • O que seus competidores estão fazendo? • A quais ameaças suas fraquezas estão expostas? • ?

Colocando tudo junto

Após ter toda a informação coletada, você pode colocar tudo junto e decidir qual o melhor modelo para uma rede wireless em sua comunidade. Baseado nos resultados de sua análise interna e externa, você pode refinar sua missão e sua oferta de serviços. Todos os fatores que você pesquisou nos passos anteriores

1. N. do T. - Em português, é comum ver a tradução deste tipo de análise para o acrônimo FOFA, de forças, oportunidades, fraquezas e ameaças.

estão em jogo na determinação de sua estratégia geral. É essencial a aplicação de um modelo que capitalize suas oportunidades e trabalhe dentro dos limites do ambiente local. Para isto você deve encontrar, com freqüência, soluções inovadoras para garantir a sustentabilidade. Com a exploração de vários exemplos e a discussão dos componentes dos modelos implementados em várias condições, você irá entender melhor como chegar a um modelo apropriado para o seu caso.

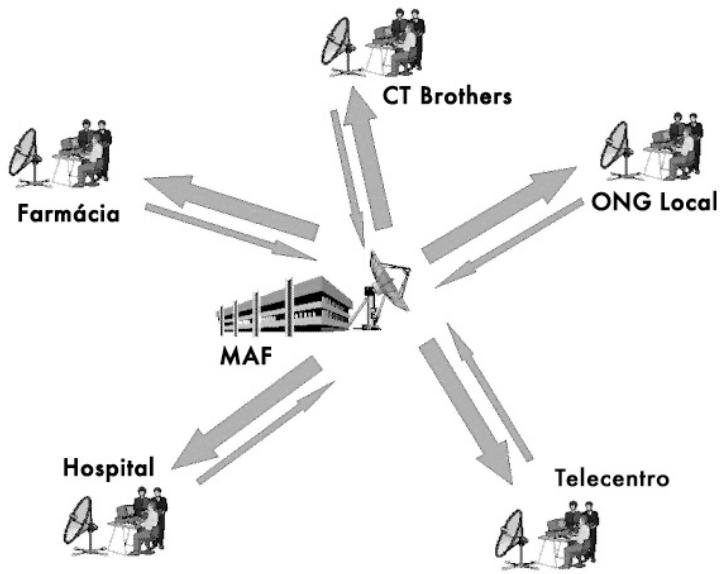


Figura 10.1: Internet compartilhada em uma rede wireless.

Na selva distante da República Democrática do Congo, há um hospital rural em uma vila chamada Vanga, na província de Bandundu. Ele é tão distante que os pacientes viajam por semanas para conseguir chegar, freqüentemente a pé e pelo rio. Esta vila, fundada por missionários Batistas em 1904, serve como hospital há muitos anos. Mesmo sendo extremamente distante, ele é renomado por sua excelente qualidade e tem tido o apoio de missionários alemães e americanos, que mantêm o hospital em funcionamento. Em 2004, um projeto patrocinado pelo USAID estabeleceu um telecentro na vila para ajudar na melhoria da educação nesta comunidade isolada. As instalações de Internet foram também bastante utilizadas pela classe educada da comunidade – os funcionários do hospital. O centro é de grande serventia à comunidade, oferecendo acesso ao conhecimento global e mesmo proporcionando a consulta com colegas distantes na Suíça, França e Canadá. O centro necessitou de subsídio quase integral para sua implantação e a cobertura de seus custos, mas o subsídio acabou em 2006. Mesmo que o centro trouxesse muito valor à comunidade, ele teve seus problemas técnicos, econômicos e políticos que limitaram sua sustentabilidade. Um estudo foi feito para considerar opções para seu futuro. Uma vez revisada a estrutura de custos do centro, foi determinada a necessidade de sua redução e de encontrar formas de aumentar seu lucro. As

maiores despesas eram de eletricidade e acesso à Internet. Assim, modelos criativos precisavam ser construídos para a redução dos custos do telecentro e para o provimento de acesso de forma sustentável.

Desta forma, um VSAT tradicional foi usado para a conectividade. A forma de contornar a limitada capacidade de pagamento por serviços de acesso à Internet foi o compartilhamento deste acesso através de uma rede wireless. Este modelo funciona graças a condições específicas: a percepção e o reconhecimento do valor da Internet entre os membros-chave da comunidade, os recursos necessários para o suporte ao acesso à Internet e um sistema legal que permite o compartilhamento através da rede sem fio. Em Vanga, várias organizações, incluindo um hospital, uma farmácia, vários grupos missionários, um centro comunitário e algumas ONGs sem fins lucrativos, têm a necessidade de acesso à Internet, assim como recursos para pagar por isto. Este arranjo permitiu, a esta rede de organizações, uma melhor qualidade de conexão a um custo baixo. Além disto, uma organização na vila tem a capacidade e o desejo de gerenciar vários aspectos de operação da rede, incluindo a bilhetagem e cobrança, suporte técnico e manutenção e a operação geral da rede. Assim, este modelo funciona bem em Vanga porque foi personalizado para atender às demandas da comunidade, utilizando recursos econômicos disponíveis localmente.

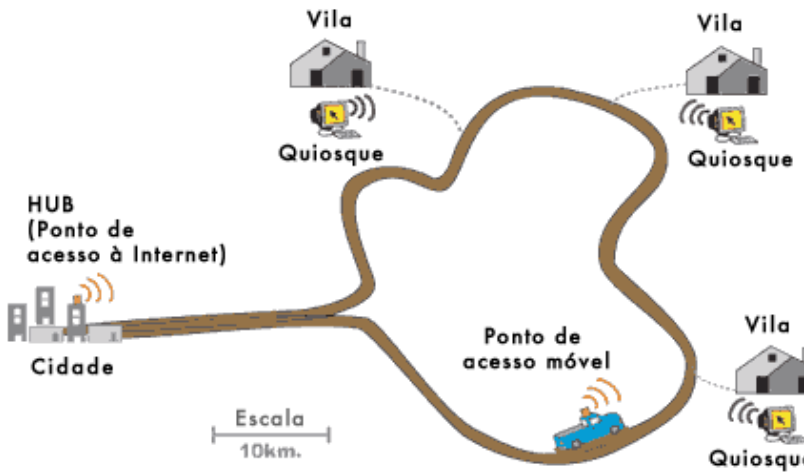


Figura 10.2: Ponto de acesso móvel da DakNet.

Outro exemplo de um modelo adaptado a um contexto local é o *First Mile Solutions*' DakNet. Este modelo foi implementado em vilas na Índia, Camboja, Ruanda e Paraguai. Levando em consideração o baixo poder aquisitivo dos habitantes das vilas, este modelo atende suas necessidade de comunicação de maneira inovadora. No modelo DakNet há uma franquia existente no país e empreendedores locais são contratados e treinados para operar os quiosques equipados com antenas Wi-Fi. Usando cartões pré-pagos, os habitantes da vila podem, de forma assíncrona, enviar e receber emails, textos e mensagens de voz, fazer buscas na Internet e participar de comércio eletrônico. Todas estas

comunicações são armazenadas no servidor local do quiosque. Quando um ônibus ou motocicleta com um access point móvel passa pelo quiosque, o veículo automaticamente recebe os dados armazenados no quiosque e entrega os dados destinados a ele. Quando o veículo atinge o hub com conexão à Internet, ele processa as solicitações, entrega os emails, mensagens e arquivos compartilhados.

O modelo DakNet integra o acesso móvel a um sistema de franquias para entregar valor a pessoas em vilas remotas. Para que este modelo seja sustentável, muitas condições precisam estar presentes. Em primeiro lugar, uma organização de franquias deve existir para garantir o suporte financeiro e institucional, incluindo investimento inicial, capital de giro para custos recorrentes, aconselhamento para as práticas de implantação, treinamento gerencial, processos padronizados, relatórios e ferramentas de marketing. Adicionalmente, este modelo requer um indivíduo dinâmico e altamente motivado na vila, com habilidades apropriadas para a gestão do negócio e a determinação de trabalhar dentro dos requerimentos da franquia. Como estes empreendedores devem comprometer seus próprios recursos na implantação do quiosque, eles devem ter acesso suficiente a recursos financeiros. Finalmente, para garantir a auto-sustentabilidade do modelo, deve haver demanda suficiente de serviços de informação e comunicação, além de poucos competidores na comunidade.

Conclusão

Não há um modelo de negócio único que irá fazer com que redes sem fio sejam sustentáveis em todos os ambientes do mundo em desenvolvimento. Modelos diferentes devem ser usados e adaptados de acordo com o que ditam as circunstâncias. Cada comunidade tem características únicas e uma análise deve ser feita na localidade do projeto para determinar qual o modelo mais apropriado. Esta análise deve considerar vários pontos chave no ambiente local, incluindo a demanda da comunidade, competidores, custos, recursos econômicos, etc. Mesmo que o planejamento adequado e sua boa execução maximizem as chances de que sua rede seja sustentável, não há garantias de sucesso. Mas, com o uso dos métodos detalhados neste capítulo, você irá ajudar a garantir que sua rede traga valor para a comunidade de uma forma que corresponda às necessidades dos usuários.

11
Estudos de Caso

Não importa quanto planejamento seja feito para a construção de um link ou de um nó de comunicação em uma localidade, em algum momento você terá que começar a trabalhar e instalar alguma coisa. Este momento da verdade irá demonstrar a validade de suas estimativas e predições.

É raro o dia em que tudo funciona precisamente como foi planejado. Mesmo depois da instalação de seu 1º, 10º ou 100º nó, você ainda irá descobrir que as coisas nem sempre funcionam da forma planejada. Este capítulo descreve alguns dos mais memoráveis projetos de rede. Quer você esteja embarcando em seu primeiro projeto de rede ou seja um macaco velho, é bom saber que há sempre mais para se aprender.

Recomendações gerais

As economias de países em desenvolvimento são muito diferentes daquelas do mundo desenvolvido e, assim, uma solução criada para um país mais desenvolvido pode não servir para o oeste da África ou o sul da Ásia. Especialmente, o custo de materiais produzidos localmente e o custo de mão-de-obra podem ser muito baixos, enquanto mercadorias importadas podem ser muito mais caras em comparação com os custos do mundo desenvolvido. Por exemplo, é possível fabricar e instalar uma torre de antenas a um décimo do custo desta mesma torre nos Estados Unidos, mas o preço da antena pode ser o dobro. Soluções que capitalizam nas vantagens competitivas locais, como o trabalho barato e materiais encontrados localmente, serão as mais fáceis de serem reproduzidas.

Encontrar o equipamento correto é uma das tarefas mais difíceis em mercados em desenvolvimento, pois a economia e sistemas de comunicação e transporte não estão plenamente desenvolvidos. Um fusível, por exemplo, é difícil de ser encontrado, assim, encontrar um fio que queime com uma certa corrente e possa substituir o fusível já é uma grande vantagem. A busca e o encontro de substitutos na região também incentiva empreendimentos locais, propriedade local e pode proporcionar a economia de dinheiro.

Proteção para os equipamentos

Plásticos baratos são encontrados em qualquer lugar do mundo em desenvolvimento, mas eles são feitos com materiais pobres e têm espessura fina, por isso pouco adequados para a construção de proteção para equipamentos. Tubos de PVC são muito mais resistentes e construídos para serem à prova d'água. No oeste da África, o tipo mais comum de PVC é encontrado em encanamentos, variando de 90mm a 220mm de diâmetro. Pontos de acesso como os Routerboard 500 e 200 cabem nestes canos e, com o uso de coberturas que podem ser soldadas a fogo em suas extremidades, podem ser feitas proteções a prova d'água bastante robustas. Eles também têm o benefício de serem aerodinâmicos e de pouca atração para as pessoas que passam por eles. O espaço deixado ao redor do equipamento garante uma boa circulação de ar. Também é conveniente fazer um furo de exaustão no fundo da proteção de PVC. O autor descobriu que este furo, porém, pode tornar-se um problema. Em uma ocasião, formigas decidiram fazer seu ninho 25 metros acima do solo, dentro de um tubo de PVC que continha um access point. O uso de uma tela contra insetos, que pode estar disponível localmente, é recomendável para evitar a infestação.

Mastros de antena

A recuperação de materiais usados tornou-se uma indústria importante para os países mais pobres. De carros usados a televisores, qualquer material que tenha algum valor será desmontado, vendido ou reutilizado. Por exemplo, você verá veículos desmontados, peça por peça, todos os dias. O material resultante é organizado e colocado em um caminhão para ser vendido. Pessoas que trabalham com metais costumam estar familiarizadas com técnicas de construção de mastros de antenas de TV a partir de restos de metal. Depois de algumas poucas adaptações, estes mesmos mastros podem ser utilizados para redes sem fio.

O mastro típico é o poste de cinco metros, constituído de um cano de 30mm de diâmetro plantado em uma base de concreto. O melhor é construir o mastro em duas partes, com um mastro removível que se encaixe a uma base um pouco maior em diâmetro. Alternativamente, o mastro pode ser feito com braços que possam ser presos a uma parede. Este projeto é fácil, mas requer o uso de uma escada para ser completado e, por isso, recomenda-se cuidado.

Este tipo de mastro pode ser aumentado em vários metros com o uso de estaias. Para reforçar o poste, fixe três linhas (estaias) espaçadas de 120 graus, formando um ângulo de ao menos 33 graus com a torre.

Acima de tudo: envolva a comunidade local

O envolvimento da comunidade local é imperativo para a garantia do sucesso e sustentabilidade do projeto. O envolvimento da comunidade em um projeto pode ser um grande desafio, mas se a mesma não estiver envolvida, a tecnologia não atenderá às suas necessidades ou sequer será aceita. Além disso, a comunidade pode sentir-se ameaçada e poderá sabotar a iniciativa.

Independente da complexidade desta tarefa, um projeto de sucesso necessita do suporte e do convencimento daqueles a quem irá servir.

Uma estratégia efetiva na obtenção do suporte é encontrar um patrocinador local respeitável, cujos motivos sejam de fácil aceitação pela comunidade. Encontre a pessoa ou pessoas que provavelmente estarão interessadas no projeto. Com freqüência, você precisará envolvê-las em determinadas funções, tais como conselheiras ou membros do comitê diretor. Estas já devem ter a confiança da comunidade, saber quais outros devem ser contatados e falar a língua da comunidade. Tome o tempo necessário e seja seletivo na busca das pessoas certas para o seu projeto. Nenhuma outra decisão afetará mais o seu projeto do que ter pessoas locais eficazes e de confiança em sua equipe.

Adicionalmente, anote o nome de pessoas chave em uma instituição ou comunidade. Identifique aqueles que podem ser oponentes ou proponentes para seu projeto. O mais cedo possível, busque conseguir o apoio dos potenciais proponentes e dissipe os oponentes. Esta é uma tarefa difícil que requer o conhecimento profundo da instituição ou comunidade. Caso o projeto não tenha um aliado local, ele deve primeiramente dispor de algum tempo para adquirir o conhecimento e a confiança da comunidade.

Seja cuidadoso na escolha de seus aliados. Uma reunião da comunidade é freqüentemente um bom local para a observação da política local, alianças e tudo o que está em discussão. A partir daí é mais fácil decidir a quem se aliar, quem pode ser o patrocinador local e aqueles que devem ser evitados. Tente não criar entusiasmo que não tenha garantias. É importante ser honesto, franco e não fazer promessas que não poderão ser mantidas.

Em comunidades onde a maioria das pessoas sejam analfabetas, foque em serviços como Internet para estações de rádio, impressão de artigos e fotos e aplicações não textuais. Não tente introduzir tecnologia em uma comunidade sem antes entender quais aplicações realmente podem servi-la. Com freqüência, a comunidade não terá idéias sobre a forma pela qual novas tecnologias podem ajudar em seus problemas. A simples oferta de novas funcionalidades é inútil, sem que exista o entendimento de como a comunidade pode se beneficiar delas.

Ao coletar informações, verifique os dados que são fornecidos. Se você quiser saber da saúde financeira de uma empresa ou organização, peça para ver uma conta de energia elétrica ou de telefone. Eles estão pagando as contas? Em muitos momentos, os beneficiários em potencial irão comprometer seus próprios valores na esperança de receber recursos ou equipamentos. Mas com mais freqüência, parceiros locais que confiam em você serão francos, honestos e estarão dispostos a ajudá-lo.

Outro problema comum é aquele que chamo de síndrome dos “pais divorciados”, onde ONGs, doadores e parceiros não estão em sintonia e nem envolvidos com o beneficiário. Beneficiários espertos e mal-intencionados conseguem boas recompensas ao permitir que ONGs e doadores forneçam-lhes equipamentos, treinamento e recursos financeiros. É importante saber quais são as outras organizações envolvidas para que você entenda as suas atividades e a forma como elas podem impactá-lo. Por exemplo, uma vez eu fiz um projeto para uma escola rural em Mali. Minha equipe instalou um sistema de código aberto em computadores usados e passou vários dias treinando as pessoas em sua utilização. O projeto estava fadado ao sucesso, mas logo após a instalação

apareceu um outro doador com computadores Pentium 4 novos, rodando Windows XP. Os estudantes rapidamente abandonaram os computadores velhos e passaram a usar os novos. Teria sido muito melhor negociar antecipadamente com a escola, descobrindo seu real compromisso com o projeto. Caso eles agissem com honestidade, os computadores que agora estão sem uso poderiam ter sido instalados em outra escola onde poderiam ser bem aproveitados.

Em muitas comunidades rurais, em economias subdesenvolvidas, a lei e a política são fracas e os contratos podem não ter relevância alguma. Com freqüência, outras garantias devem ser descobertas. Nestes casos, serviços pré-pagos são a melhor opção, já que não necessitam de um acordo legal. O compromisso é garantido pelo investimento prévio nos serviços que serão fornecidos.

O comprometimento também requer o investimento daqueles envolvidos no projeto. Não há mal em pedir por alguma reciprocidade financeira aos membros da comunidade.

Acima de tudo, a opção válida de não se iniciar o projeto deve ser levada em conta. Caso não exista um aliado local ou a comunidade não esteja comprometida, o melhor é considerar uma outra comunidade ou beneficiário. Uma negociação sempre é necessária: equipamentos, dinheiro e treinamento não podem ser considerados como "presentes". A comunidade deve estar envolvida e também deve contribuir.

—Ian Howard

Quebrando barreiras com uma bridge simples em Timbuktu

Redes devem, em seu mais importante propósito, conectar pessoas. Isto implica em um componente político. O custo da Internet em economias pouco desenvolvidas é alto e a capacidade de pagar por ele é baixa, implicando em desafios políticos. De nada adianta a imposição de uma rede digital onde uma rede "humana" não funciona. Tentar fazer isto pode colocar o projeto em uma base social instável, ameaçando sua existência ou continuidade. Neste caso, o baixo custo e a mobilidade de uma rede sem fio podem ser uma vantagem.

Os financiadores pediram à equipe do autor que definisse como conectar uma estação de rádio rural com um telecentro muito pequeno (dois computadores) à Internet em Timbuktu, a capital do deserto de Mali. Timbuktu é bastante conhecida como um posto comercial na mais remota área do mundo. Neste local, a equipe decidiu implementar um modelo que foi então chamado de ***modelo wireless parasítico***. Este modelo pega uma alimentação wireless que é dividida de uma rede existente e estende a rede a uma localidade cliente usando uma simples bridge. Este modelo foi escolhido por não exigir nenhum investimento significativo da organização mantenedora. Mesmo acrescentando uma fonte de renda ao telecentro, isto não trouxe nenhum custo operacional adicional. Com esta solução, a localidade cliente pôde obter um acesso barato à Internet, ainda que não tão rápido ou confiável quanto o de uma solução

dedicada. Já que os padrões de uso eram opostos entre o escritório e o telecentro, não foi percebida nenhuma queda de velocidade da rede em nenhuma localidade. Mesmo que uma solução ideal pudesse ser melhor para encorajar um maior desenvolvimento do pequeno telecentro, transformando-o em um provedor de acesso, nem o telecentro ou mesmo o mercado local estavam preparados para isto naquele momento. Desta forma, a solução adotada minimizou o investimento inicial ao mesmo tempo em que atingiu dois objetivos: o primeiro foi levar à Internet ao beneficiário, uma estação de rádio, com baixo custo; o segundo, adicionar uma fonte adicional de recursos para o telecentro, sem a adição de custos operacionais ou aumento de complexidade ao sistema.

As pessoas

Mesmo com renome mundial, Timbuktu é uma localidade remota. Sendo um símbolo de local distante, muitos projetos querem ter uma bandeira nas areias desta cidade no deserto. Assim, há um bom número de atividades de tecnologia de informação e comunicação (TIC) neste local. Na mais recente verificação existiam oito conexões via satélite em Timbuktu, a maioria atendendo a interesses especiais, exceto por duas delas: SOTELMA e Ikatel. Elas atualmente usam VSAT para conectar suas redes telefônicas ao resto do país. Este telecentro utilizava uma conexão X.25 para uma destas empresas de telefonia, que então levava a conexão até a cidade de Bamako. Com relação a outras cidades do país, Timbuktu tem um bom número de pessoas treinadas em informática, três telecentros, mais o recém instalado na estação de rádio. A cidade está, de certo modo, saturada com acessos à Internet de baixo custo, o que dificulta a implantação de novas ofertas competitivas.

Escolhas de projeto

Nesta instalação, a localidade do cliente estava a apenas 1 km de distância, com linha de visão direta. Dois access points Linksys, utilizando o firmware OpenWRT e configurados em modo bridge foram instalados. Um foi colocado na parede do telecentro e o outro em uma altura de 5 metros, no mastro da estação de rádio. Os únicos parâmetros de configuração necessários em ambos os dispositivos foram o ssid e o canal. Duas antenas simples de painel, de 14 dBi (de *http://hyperlinktech.com/*) foram utilizadas. No lado da Internet, os access points e a antena foram presos com gesso e parafusos ao lado do prédio, apontando para a localidade cliente. Do lado do cliente, um mastro de antena já existente foi utilizado. O access point e a antena foram montados com anéis de canos.

Para desconectar o cliente, o telecentro simplesmente desliga a bridge local. Uma localidade adicional poderá, eventualmente, ser instalada de forma similar, com uma nova bridge. Assim, o pessoal do telecentro pode desligar a bridge caso o cliente não pague a mensalidade. Mesmo bastante crua, esta solução é efetiva e reduz o risco de erros que poderiam ser introduzidos caso fossem necessárias reconfigurações de sistema. Ter uma bridge dedicada à uma conexão também simplificou a instalação da localidade central, já que a equipe de instalação pode escolher o melhor local para a conexão com os clientes.

Mesmo não sendo o ideal criar bridges em uma rede (a não ser para rotear o tráfego de rede), quando não há muito conhecimento técnico e é necessário instalar apenas um sistema muito simples, esta pode ser uma solução razoável para redes pequenas. A bridge faz com que sistemas instalados em locais remotos (à estação de rádio) pareçam estar conectados à rede local.

Modelo financeiro

O modelo financeiro aqui é simples. O telecentro cobra uma tarifa mensal de cerca de 30 dólares por computador conectado à estação de rádio. Isto é muito mais barato que outras alternativas. O telecentro está localizado na corte da prefeitura e os funcionários dela são os principais clientes do mesmo. Isto foi importante porque a estação de rádio não queria competir por clientes com o telecentro e os sistemas da estação de rádio são para o uso exclusivo de seus funcionários. Esta bridge reduziu custos, já que esta base seletiva de clientes poderia suportar o custo da Internet sem competir com o telecentro, seu fornecedor. O telecentro pode facilmente desconectar a estação de rádio na eventual falta de pagamento. Este modelo também permitiu o compartilhamento dos recursos da rede. Por exemplo, a estação de rádio possui uma impressora à laser nova, enquanto o telecentro tem uma impressora colorida. Como os clientes estão na mesma rede, as impressoras de ambas as localidades podem ser utilizadas.

Treinamento

Para o suporte a esta rede foi necessário muito pouco treinamento. Mostrou-se ao pessoal do telecentro como instalar o equipamento, assim como técnicas básicas de diagnóstico, como a reinicialização dos pontos de acesso e a substituição no caso de falhas. Isto possibilita à equipe do autor simplesmente enviar a peça de substituição, economizando os dois dias de viagem a Timbuktu.

Sumário

A instalação foi considerada como uma medida temporária, até que seja possível a implantação de uma solução mais completa. Ela foi um sucesso no sentido em que não foi necessário investimento na construção de infra-estrutura física adicional. Além de levar a estrutura de TIC para a estação de rádio, ela reforçou os relacionamentos entre clientes e fornecedores.

Ainda hoje, o acesso à Internet é uma tarefa cara em Timbukti. A política local e iniciativas subsidiadas estão mudando isto, mas esta simples solução provou ser ideal para o caso. A equipe levou vários meses entre análise e pensamento crítico para chegar a ela, mas ao final, concluiu-se que a solução mais simples foi a que trouxe o maior benefício.

—Ian Howard

Encontrando um terreno sólido em Gao

A um dia de viagem ao leste de Timbuktu, em Mali Ocidental, está a cidade de Gao. Esta cidade rural que mais se parece com uma grande vila, está na beira do rio Niger, um pouco antes dele virar ao sul em direção à Nigéria. A cidade espalha-se suavemente à margem do rio e tem poucos prédios maiores que dois andares. Em 2004, um telecentro foi instalado em Gao. O objetivo do projeto era fornecer informação à comunidade na esperança de que uma comunidade informada produziria cidadãos mais saudáveis e educados.

O centro fornecia informações através de CD-ROMs, filmes e rádio, mas a principal fonte de informação para o centro é a Internet. É um telecentro padrão, com 8 computadores, uma impressora multifuncional (incluindo scanner e fax), um telefone e uma câmera digital. Um pequeno prédio de dois andares foi construído para acomodar o telecentro. Ele está localizado um pouco fora do centro da cidade, o que não é um local ideal para atrair clientes, mas foi escolhido em função de seu simpático anfitrião. O local recebeu investimento para toda a construção necessária, assim como para o equipamento e treinamento inicial. A expectativa de que o telecentro se tornasse auto-sustentável era de um ano.

Muitos meses depois de sua abertura, o telecentro atraía apenas poucos clientes. Ele usava um modem para a conexão discada a um provedor na capital. A conexão era muito lenta e pouco confiável e assim o patrocinador providenciou a instalação de um sistema VSAT. Há um bom número de sistemas VSAT hoje disponíveis na região, sendo que a maioria deles entrou em produção recentemente. Anteriormente, apenas sistemas de banda C (que cobre uma área maior que a banda Ku) estavam disponíveis. Recentemente, fibras óticas foram instaladas em praticamente todos os túneis de metrô e canais através da Europa e assim substituíram os serviços via satélite mais caros. Como resultado, os provedores estão agora redirecionando seus serviços de VSAT para novos mercados, incluindo a África Central e Ocidental e o sul da Ásia. Isto levou a vários projetos que usam sistemas de satélite para a conexão à Internet.

Depois que o VSAT foi instalado, a conexão forneceu 128 kbps para a recepção e 64 kbps para a transmissão, ao custo de cerca de 400 dólares ao mês. A localidade estava tendo dificuldades para receber o suficiente para pagar este alto custo mensal e o telecentro pediu ajuda. Um consultor local, que havia sido treinado pelo autor pra instalar sistemas wireless, foi contratado. O sistema iria dividir a conexão entre três clientes: um segundo beneficiário, uma estação de rádio e o telecentro, cada um pagando 140 dólares. A parceria coletiva cobriu os custos do VSAT e a renda extra do telecentro e da estação de rádio cobriram o suporte e a administração do sistema.

As pessoas

Mesmo tendo capacidade e vontade, a equipe do autor não fez a instalação. Ao invés disto, encorajamos o telecentro a contratar um consultor local para fazer isto. Tranqüilizamos o cliente concordando em treinar e dar suporte ao consultor durante a instalação. A razão deste procedimento foi desencorajar a dependência e ao mesmo tempo ajudar a construir relações de confiança entre

os prestadores de serviços locais e seus clientes. A decisão acabou provando-se frutífera, mesmo tomando bastante tempo da equipe do autor – talvez o dobro do tempo que normalmente levaria – mas o investimento já começou a se pagar. As redes continuam a ser instaladas e o autor e sua equipe já estão de volta a seus lares na Europa e América do Norte.

Escolhas de projeto

A idéia inicial era a de que a conexão à Internet seria feita diretamente na estação de rádio, que já possuía uma torre de 25 metros. Esta torre seria usada para a transmissão aos demais clientes, evitando a necessidade de se instalar outras torres nas localidades dos clientes, já que ela estava bastante acima de qualquer obstáculo na cidade. Para se fazer isto, três opções foram discutidas: a instalação de um access point em modo repetidor, usando o protocolo WSD ou usando um protocolo mesh de roteamento. Um repetidor não era desejável, já que ele introduziria latência (devido ao problema do repetidor de um só braço) a uma conexão que já era lenta. Conexões VSAT necessitam enviar os pacotes até o satélite e recebê-los novamente, introduzindo até 3000 ms de atraso para a viagem de ida e volta. Para evitar este problema, decidiu-se por usar um rádio para conectar aos clientes e um segundo rádio para a conexão à Internet. Para tornar as coisas mais simples, este link seria uma bridge simples, de forma que o access point na estação de rádio pareceria estar na mesma LAN física do telecentro.

Em testes esta opção funcionou mas, no mundo real, seu desempenho era muito ruim. Depois de muitas mudanças, incluindo a troca dos access points, o técnico decidiu que deveria haver algum problema de software ou hardware afetando o projeto. O instalador decidiu, então, colocar o access point diretamente no telecentro, usando um pequeno mastro de 3 metros e não mais usando a transmissão a partir da estação de rádio. Com isto, as demais localidades clientes também precisaram de pequenos mastros. Todos os locais puderam ser conectados, apesar da conexão ser algumas vezes muito ruim, introduzindo grande perda de pacotes.

Mais tarde, durante a temporada de poeira, estas conexões tornaram-se mais erráticas e ainda menos estáveis. Os clientes estavam distantes entre 2 e 5 km, usando 802.11b. A teoria da equipe era a de que as torres estavam muito baixas em todos os locais, cortando muito da zona Fresnel. Depois de discutir muitas teorias, a equipe também descobriu o problema com o desempenho na estação de rádio: a freqüência de rádio de 90,0 MHz era mais ou menos a mesma que a da conexão Ethernet (100BT) de alta velocidade. Durante a transmissão, o sinal de FM (a 500 watts) estava consumindo completamente o sinal no cabo Ethernet. Assim, um cabo blindado seria necessário ou a freqüência do link Ethernet deveria ser mudada. Os mastros foram aumentados e, na estação de rádio, a velocidade da Ethernet foi mudada para 10 Mbps. Isto mudou a freqüência no fio para 20 MHz, evitando a interferência da transmissão de FM. Estas mudanças resolveram ambos os problemas, aumentando a força e a confiabilidade da rede. A vantagem de usar mesh ou WDS seria a de que os clientes poderiam conectar-se a qualquer access point, diretamente ao telecentro ou à estação de rádio. Eventualmente, a remoção do repetidor na estação tornou a instalação mais estável ao longo do tempo.

Modelo financeiro

O sistema de satélite utilizado custou aproximadamente 400 dólares ao mês. Em muitos casos de desenvolvimento de estruturas de TI, este é um custo mensal difícil de gerenciar. Muitas vezes, estes projetos podem arcar com a compra de equipamentos e o estabelecimento da rede sem fio, mas não têm a capacidade de pagar pelo custo da rede após um curto período de tempo (incluindo as taxas recorrentes de acesso à Internet e custos operacionais). É necessário encontrar um modelo onde os custos mensais da rede podem ser divididos entre aqueles que a utilizam. Para muitos telecentros comunitários ou estações de rádio, o custo é simplesmente muito alto. Para tornar a Internet mais viável, este local utilizou a rede wireless para compartilhar a Internet com a comunidade, permitindo o acesso de um maior número de organizações e minimizando o custo por cliente.

Em Mali, a comunidade rural tem apenas algumas poucas organizações ou empresas que poderiam pagar por uma conexão à Internet. Onde há poucos clientes e o custo de acesso à Internet é alto, o modelo desenvolvido pela equipe incluiu ***clientes âncora***: clientes sólidos e de baixo risco. Para esta região, ONGs estrangeiras, as agências das Nações Unidas e grandes empresas comerciais então entre os muito poucos que se qualificam como âncoras.

Dentre os clientes selecionados para este projeto, três eram clientes âncora que coletivamente pagaram o custo total mensal para a conexão via satélite. Um segundo beneficiário, uma estação de rádio comunitária, também foi conectado. Todo o lucro vindo dos beneficiários contribuiu para um depósito para custos futuros, mas não foi contabilizado em função das pequenas margens com as quais os serviços comunitários operavam. Estes clientes podem ser desconectados e reconectados, de acordo com sua possibilidade de arcar ou não com os custos.

Treinamento necessário: quem, o quê, por quanto tempo

O consultor contratado ensinou ao técnico do telecentro o básico para o suporte à rede, o que foi bastante rudimentar. Qualquer tarefa fora da rotina, como a adição de um novo cliente, era contratada externamente. Desta forma, não era imperativo treinar a equipe do telecentro em como dar o total suporte ao sistema.

Lições aprendidas

Com o compartilhamento da conexão, o telecentro é agora auto-sustentável e, além disso, três outras localidades têm acesso à Internet. Mesmo tendo levado mais tempo e, talvez, custado mais, é de grande valor encontrar talentos locais e encorajá-los a construir relacionamentos com os clientes. Um implementador local será capaz de fornecer o suporte posterior, necessário para a manutenção e expansão da rede. Esta atividade está construindo conhecimento local e demanda, que permitirá novos projetos de TIC a partir desta base.

—Ian Howard

Rede wireless comunitária da Fundação Fantsuam

Kafanchan é uma comunidade de 83.000 pessoas localizada a 200 km ao noroeste de Abuja, na região central da Nigéria. A cidade costumava ser conhecida como um local movimentado e em crescimento, já que sediava uma das principais junções da ferrovia nacional. Quando a indústria ferroviária estava em crescimento, cerca de 80% da população de Kafanchan estava ligada, de alguma maneira, a esta indústria. Após a falência completa do sistema ferroviário da Nigéria, a população de Kafanchan foi forçada a voltar à sua fonte original de receita, a agricultura.

Kafanchan é uma área pobre em conexões, tanto em termos de telefonia fixa como de Internet. Hoje, nenhum tipo de telefonia fixa está disponível na área e o GSM foi introduzido apenas em 2005. Ainda assim, a cobertura do GSM é tão ruim quanto a qualidade do serviço. No momento, mensagens SMS são a forma de comunicação mais confiável, já que as conversações com voz tendem a ser cortadas pela metade e sofrem com muito ruído.

O acesso ruim à eletricidade traz ainda mais desafios ao povo de Kafanchan. A companhia elétrica nacional da Nigéria, chamada NEPA (*National Electric Power Authority*) é mais conhecida aos nigerianos como "*Never Expect Power Always*" (nunca espere a energia sempre disponível). Em 2005, a NEPA trocou seu nome para PHCN (*Power Holding Company of Nigeria*).

Kafanchan está recebendo energia elétrica da NEPA em uma média de 3 horas por dia. Nas 21 horas restantes a população utiliza caros geradores a diesel e querosene para a iluminação e cozinha. Quando a energia da NEPA está disponível, ela fornece uma voltagem não regulada entre 100 e 120 Volts em um sistema projetado para 240 V. Esta voltagem deve ser regulada para 240 V antes que a maioria das cargas possa ser conectada. Apenas lâmpadas incandescentes podem ser ligadas diretamente à energia, já que elas podem lidar com a baixa voltagem se maiores danos.

Participantes do projeto

Dado o cenário desafiante de Kafanchan, como alguém poderia ter a idéia de estabelecer o primeiro provedor rural de acesso sem fio à Internet na Nigéria, justamente na cidade? A Fundação Fantsuam teve esta idéia e a tornou realidade.

A Fundação Fantsuam é uma organização local, não governamental, que tem trabalhado com a comunidade de Kafanchan desde 1996 no combate à pobreza e desvantagens através de programas integrados de desenvolvimento. O foco da Fantsuam está em micro-finanças, serviços de TIC e desenvolvimento social nas comunidades rurais da Nigéria. Tornar-se o primeiro provedor rural de acesso sem fio à Internet era parte de sua missão para ser reconhecida como líder no provisionamento de iniciativas de desenvolvimento rural, assim como a organização que mais promove a economia de conhecimento rural no país.

O provedor wireless da Fundação Fantsuam, conhecido como ***Zittnet***, é mantido financeiramente pelo IDRC (*International Development Research Centre of Canada* – Centro de Pesquisa e Desenvolvimento Internacional do Canadá).

IT +46, uma empresa de consultoria sueca com foco em TIC para o desenvolvimento, trabalhou junto com a equipe do Zittnet para fornecer o suporte técnico às comunicações wireless, gestão da largura de banda, energia solar, sistemas de reserva de energia e serviços de VoIP.

Objetivos

O principal objetivo do Zittnet é melhorar o acesso à comunicações na área de Kafanchan, implementando uma rede de comunicações sem fio. A rede fornece acesso à intranet e Internet para os parceiros locais na comunidade. A rede comunitária é formada por organizações com base na comunidade, como instituições educacionais, instituições religiosas, serviços de saúde, pequenas empresas e indivíduos.

Sistema de reserva de energia

A fim de fornecer um serviço confiável à comunidade, o Zittnet precisava ser equipado com um sistema de reserva de energia estável, capaz de fazer com que a rede funcionasse independentemente da NEPA.

Um sistema híbrido de energia foi projetado para a Fantsuam, consistindo em bancos de baterias de ciclo profundo e painéis solares de 2 kW (pico). O sistema pode ser carregado a partir de três fontes diferentes: um gerador a diesel, uma matriz solar e a NEPA, quando a eletricidade está disponível. O centro de operações da rede é alimentado totalmente a partir da energia solar. O resto das instalações da Fantsuam utiliza a energia da NEPA ou do gerador, através do banco de baterias que fornece voltagem estável e ininterrupta. As cargas do centro de operações estão separadas das demais cargas da Fantsuam para assegurar uma fonte confiável de energia para a infra-estrutura crítica do centro, mesmo quando o banco de baterias estiver operando com potência baixa.

Figura 11.1: 24 painéis solares com a potência nominal de 80 W foram montados no telhado do centro de operações para garantir a alimentação ininterrupta ao sistema.

Simulações com os melhores dados sobre a irradiação solar revelaram que o estado de Kaduna, onde Kafanchan está localizada, recebe ao menos 4 horas de pico de sol durante os piores meses, que vão de junho a agosto (a temporada das chuvas).

Cada painel solar (Suntech, 80 W no pico) fornece um máximo de 5 A de corrente (quando a irradiação solar está em seu máximo durante o dia). Nos piores meses do ano, a expectativa de produção não é menor que 6 Kwh/dia.

O sistema solar foi projetado para fornecer saídas de 12 e 24 V DC a fim de casar com a voltagem de entrada de todos os servidores de baixa potência e estações de trabalho para a infra-estrutura do centro de operações e das salas de treinamento.

Os painéis solares usados são os ***Suntech STP080S-12/Bb-1***, com as seguintes especificações:

- Voltagem de circuito aberto (V_{OC}): **21.6 V**
- Voltagem operacional ótima (V_{MP}): **17.2 V**
- Corrente de curto circuito (I_{SC}): **5 A**
- Corrente operacional ótima (I_{MP}): **4.65 A**
- Potência máxima em STC (P_{MAX}): **80 W (Pico)**

O mínimo de 6 Kwh/dia que alimenta o centro de operações é usado para alimentar os seguintes equipamentos:

Dispositivos	Horas/dia	Unidades	Potência (W)	Wh
Access points	24	3	15	1080
Servidores de baixa potência	24	4	10	960
Telas de LCD	2	4	20	160
Laptops	10	2	75	1500
Lâmpadas	8	4	15	480
Modem VSAT	24	1	60	1440
			Total:	**5620**

O consumo de potência dos servidores e telas de LCD está baseado nos dados fornecidos por Inveneo's *Low Power Computing Station*, *http://www.inveneo.org/?q=Computingstation*.

A estimativa de consumo total do centro de operações, que é menor do que a energia gerada pelo painel solar no pior mês, é de 5,6 kWh/dia.

Centro de Operações da Rede (NOC – Network Operating Center)

Um novo centro de operações foi criado para hospedar o sistema de reserva de energia e a sala de servidores. O centro foi projetado para prover um lugar protegido contra poeira, com boa qualidade de refrigeração para as baterias e inversores. O centro usa métodos naturais e foi construído com materiais disponíveis localmente.

O prédio compreende quatro salas: uma sala para o armazenamento das baterias, uma para o servidor, uma área de trabalho e outra para o estoque de equipamentos.

A sala de armazenamento de baterias contém 70 baterias de 200 Ah de ciclo profundo, assim como cinco inversores (um deles de onda senoidal pura), dois reguladores solares, estabilizadores de potência e disjuntores DC e AC. As baterias estão empilhadas verticalmente em uma prateleira metálica para o melhor resfriamento.

Figura 11.2: O centro de operações foi construído localmente com tijolos de laterita, produzidos por jovens na cidade de Kafanchan.

O espaço do servidor acomoda um rack para os servidores e um ventilador. A sala não possui janelas regulares, para evitar a poeira e o super aquecimento. As salas do servidor e das baterias estão de frente para o sul, a fim de aumentar o resfriamento natural e mantê-las em uma temperatura apropriada.

Estas salas necessitam de um resfriamento eficaz, de baixo custo e baixo consumo de energia, já que precisam operar ininterruptamente. Para atingir este objetivo, técnicas de resfriamento natural foram introduzidas no projeto do centro de operações: pequenos ventiladores e exaustores e paredes duplas de tijolos na direção do pôr do sol.

O lado sul da construção contém os 24 painéis solares em uma área livre de sombras em seu teto metálico. O teto foi projetado com uma inclinação de 20 graus para a montagem dos painéis, limitando a corrosão e a poeira. Esforços extras foram feitos para manter os painéis facilmente acessíveis para a limpeza e manutenção. O teto também foi fortalecido a fim de poder suportar um peso extra de 150 a 200 kg.

O prédio do centro de operações foi construído com tijolos de lama de laterita produzidos localmente, de forma manual, utilizando uma técnica de baixa pressão. O material é barato, já que é freqüentemente utilizado e vem da parte de cima do solo. O centro de operações é o único deste tipo no estado de Kaduna.

Figura 11.3: Omolayo Samuel, uma das pessoas da equipe do Zittnet, não tem medo da altura de 45 m da torre onde ela está alinhando as antenas montadas em seu topo.

Infra-estrutura física: uma torre de comunicações

Muitos clientes potenciais do Zittnet estão localizados entre 1 e 10 km das instalações da Fantsuam. A fim de atingir estes clientes, a Fantsuam montou uma torre de comunicações em suas instalações. Em outubro de 2006, uma torre de 45 m auto-sustentável foi instalada na Fundação Fantsuam. A torre foi equipada com aterramento e proteção contra raios, assim como uma luz sinalizadora obrigatória.

Um anel de metal foi enterrado na base da torre, a uma profundidade de 1,22 m. Todas as três pernas da torre foram conectadas ao circuito de aterramento. Um pára-raios foi montado no ponto mais alto da torre para a proteção do equipamento contra tempestades elétricas. Este pára-raios é feito de puro cobre e está conectado no anel de aterramento na base da torre com o uso de uma cinta de cobre.

A luz de sinalização montada no topo da torre é um requerimento das autoridades de aviação civil. Ela é equipada com uma fotocélula que faz com que ela ligue e desligue automaticamente, de acordo com a iluminação ambiente. Assim, a luz é ligada à noite e desligada durante o dia.

Infra-estrutura wireless

A infra-estrutura wireless é feita com o uso de access points multi-banda SmartBridges e unidades clientes da série Nexus PRO™ TOTAL. Estas unidades são projetadas para provedores de serviços e empresas, a fim de estabelecer um alto desempenho em links wireless ponto-a-multiponto externos. Elas possuem uma antena multi-setorial, multi-banda integrada que pode operar nas freqüências de 2,4 GHz e 5,1 a 5,8 GHz. A série Nexus PRO™ TOTAL oferece QoS para a priorização do tráfego e gestão de largura de banda por cliente usando as extensões compatíveis com o padrão WMM (Wi-Fi Multimedia) do IEEE 802.11e.

Atualmente, a topologia da rede é uma estrela, com dois access points na torre de comunicações das instalações da Fantsuam. Um access point possui uma antena setorial de 90 graus (linhas pontilhadas azuis) e o outro access point fornece cobertura omnidirecional para as áreas vizinhas (anel pontilhado vermelho). Os clientes localizados dentro da área entre as linhas pontilhadas azuis são atendidos pela antena setorial, enquanto os demais são conectados à antena omnidirecional.

Há planos para a expansão da oferta da rede com a colocação de dois repetidores wireless. Um repetidor será colocado na cidade de Kafanchan usando uma torre existente da NITEL para ampliar a cobertura da rede no centro da cidade. O segundo repetidor será colocado em Kagoro Hills, um pequeno grupo de montanhas com altitude de 500 m em relação a Kafanchan e localizado a cerca de 7 km da cidade. Este repetidor irá fornecer cobertura para muitas cidades vizinhas e pode tornar viável um link de longa distância para Abuja.

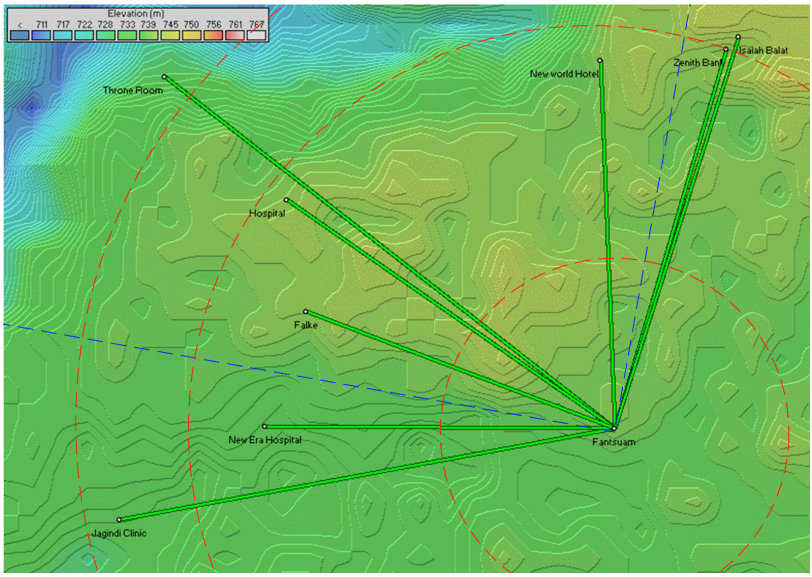


Figura 11.4: A topologia de rede do Zittnet em outubro de 2007.

O Zittnet conectou seu primeiro cliente no início de agosto de 2007. Dois meses mais tarde, não menos que oito clientes estavam conectados. Estes clientes incluem:

- O hospital geral
- Hospital New Era
- Jagindi Street Clinic (clínica de saúde)
- Zenith Bank (para uso privado)
- Isaiah Balat (Internet café)
- New World Hotel
- Throne Room GuestHouse
- Fulke

Problemas encontrados

Algumas áreas problemáticas que estavam constantemente presentes durante todo o projeto estão listadas a seguir.

Construções baixas

Muitas instalações de clientes estão localizadas em prédios de apenas um andar, com uma altura não maior que 3 metros. Muitas casas têm telhados com estruturas fracas, impedindo a montagem do equipamento neles, já que o acesso físico é impossível. Os prédios baixos nos forçaram a montar os equipamentos em alturas bastante baixas, já que os clientes não tinham recursos para investir em pequenos mastros (10 m) para a instalação do equipamento. Muitas

instalações foram feitas em caixas d'água ou em um poste metálico de 3 metros montado na parede do prédio.

Quando a montagem do equipamento é baixa, a primeira zona Fresnel não está livre, resultando em uma baixa velocidade da conexão. Mesmo que o cenário de Kafanchan seja bastante plano, a vegetação, composta por grossas mangueiras, facilmente bloqueia a linha de visão.

Raios

Fortes tempestades são freqüentes durante a estação de chuvas de Kafanchan. Em setembro de 2007, um raio que caiu nas proximidades danificou o equipamento montado em um mastro, assim como a sua fonte de alimentação. No momento, o access point e seu injetor PoE estão aterrados à própria torre. Novos meios devem ser investigados para prevenir danos causados por raios que caiam nas proximidades. A equipe do Zittnet está atualmente trabalhando na melhoria da proteção contra surtos, adicionando novos supressores coaxiais de surtos. Além disto, a blindagem do cabo UTP que conecta o access point ao centro de operações será aterrada com o uso de blocos de aterramento e braçadeiras.

Equipamentos de baixa qualidade

Infelizmente, a falta de qualidade em produtos no mercado é um problema espalhado em todo o continente africano. Como a maioria dos países abaixo do deserto do Sahara não possuem políticas para a garantia de qualidade para mercadorias importadas, o mercado é inundado por artigos baratos e de baixíssima qualidade. Uma vez que produtos de qualidade são difíceis de serem encontrados, você acaba comprando mercadorias localmente disponíveis que quebram mesmo antes de entrar em operação. Como não há nenhuma garantia para estas pequenas compras, isto se torna muito caro. Este problema está quase sempre presente em acessórios comuns como tomadas elétricas, réguas de alimentação, conectores RJ45, cabos CAT5 e outros equipamentos de pouca tecnologia.

Modelo de negócios

A única alternativa para o acesso à Internet em Kafanchan é via satélite. Durante 2006, a Fantsuam tinha uma assinatura de um link dedicado de 128/64 kbps a um custo de 1.800 dólares mensais. Este altíssimo custo mensal de conectividade era um grande fardo para a Fantsuam e um motivo constante de stress para o fechamento mensal das contas.

Como alternativa ao modelo de taxa fixa, de alto risco, a Fantsuam implementou um sistema chamado ***HookMeUp***, fornecido pela Koochi Communications. O sistema oferece taxas flexíveis para o pagamento por uso de banda larga em conexões VSAT para a Internet em países de toda a África ao sul do Sahara.

Este tipo de modelo de acesso é tipicamente encontrado em aeroportos, hotéis ou grandes shopping centers em países ocidentais, onde os usuários compram cartões pré-pagos online e fazem o login no sistema usando um código de acesso.

O sistema HookMeUp oferece uma conexão VSAT dedicada, de 512/256 Kbps para Fantsuam (a partir de sua estação-base no Reino Unido). A Fantsuam compra os créditos da Koochi Communications e os revende a seus clientes locais em Kafanchan. Desta forma, a Fantsuam não mais está presa a um custo mensal fixo, tendo apenas que pagar para a Koochi a banda que realmente utilizou. O risco de aquisição de largura de banda internacional, cara, foi transferido para o provedor de Internet ao custo de um maior preço para o usuário final.

A Fundação Fantsuam agora funciona como uma revenda de créditos da Koochi e como fornecedora da infra-estrutura wireless para seus usuários. A *Wireless Community Network* (Rede Comunitária Wireless) agora garante à Fantsuam cinco fontes de renda:

1. Instalação de equipamento no local do cliente (uma vez a cada cliente);
2. Aluguel de equipamento wireless (custo mensal por cliente);
3. Revenda de equipamento wireless (uma vez a cada cliente);
4. Instalação de um ponto de acesso (*hotspot*) no local do cliente (uma vez a cada cliente);
5. Revenda de créditos (continuamente).

O sistema de créditos é baseado em três parâmetros: ***tempo de acesso***, ***limite de dados*** e ***tempo de validade***. O primeiro parâmetro que se esgotar primeiro invalidará o crédito.

Tempo de acesso	Limite de dados (MB)	Tempo limite	Preço (dólares)	Dólares/ hora	Dólares/ 700 MB
30 min	5	1 dia	0,80	1,60	112,00
60 min	10	5 dias	1,28	1,28	89,60
12 horas	60	14 dias	10,40	0,87	121,33
24 horas	150	30 dias	26,00	1,08	121,33
1 mês	500	1 mês	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

A maior vantagem deste sistema é que a Fantsuam Foundation não tem mais o fardo da alta conta mensal para a conexão internacional. A manutenção de um modelo de custo fixo implica em que você seja forçado a vender uma certa quantidade de banda a cada mês. Com modelos do tipo "pague enquanto usa", o lucro da Fantsuam na venda de créditos depende de quanta banda seus clientes consomem. Os clientes pagam antecipadamente (modelo pré-pago) e o resultado disto é que a Fantsuam nunca fica em débito com o provedor.

O modelo pré-pago funciona bem na África, já que as pessoas estão acostumadas a utilizá-lo em telefonia móvel. Ele é até utilizado por empresas de energia elétrica em alguns países. As pessoas costumam gostar deste modelo pois ele auxilia no controle de suas despesas. Uma das principais limitações do modelo é sua falta de flexibilidade e transparência. O modelo atual fornece pouca informação ao usuário sobre seu consumo de tempo e volume de dados. Apenas quando o usuário é desconectado é que é informado sobre quantos minutos ainda estão disponíveis para seu uso.

Mesmo assim, este modelo parece encaixar-se bem à realidade local de Kafanchan e muitas outras comunidades rurais da África também. Existe espaço para a melhoria, mas a vantagem de evitar dívidas é muito superior às desvantagens. Com o tempo, o número de clientes foi aumentando e eles hoje podem contar com uma entrada substancial de recursos vindos da rede wireless, podendo ser vantagem voltar novamente ao sistema de taxa mensal fixa.

Clientes

Os clientes podem usar a Internet para qualquer propósito. Por exemplo, Isaiah Balat revende créditos (comprados da Fantsuam) para seus clientes. Seu Internet café possui dez computadores, todos conectados ao Zittnet. Os clientes compram os créditos do proprietário que tem uma margem de lucro de 25% sobre o preço oferecido pela Fantsuam. Em retorno, os clientes que não possuam um computador conectado à Internet podem acessar à rede nos que são oferecidos pelo Café Isaiah Balat.

O New World Hotel é outro cliente que planeja criar um modelo similar, mas em maior escala. Eles irão prover acesso sem fio à Internet em todos os seus apartamentos, oferecendo a conexão do Zittnet através da revenda de créditos.

—Louise Berthilson

A cruzada pela Internet de baixo custo na zona rural de Mali

Por muitos anos, a comunidade internacional de desenvolvimento tem promovido a idéia da eliminação da barreira digital, este abismo invisível que foi formado para a riqueza de acesso às tecnologias de informação e comunicação (TIC) entre os países desenvolvidos e em desenvolvimento. Ferramentas de acesso à informação e comunicações causam um impacto dramático na qualidade de vida. Para muitos doadores, fatigados por décadas de suporte a atividades tradicionais de desenvolvimento, a instalação de um telecentro em um

país em desenvolvimento parece ser um trabalho possível e válido. Em função de uma infra-estrutura inexistente, é muito mais cara e difícil a realização desta tarefa no mundo em desenvolvimento do que no Ocidente. Além disto, existem poucos modelos que mostram como estas atividades podem ser suportadas. Para ajudar a minimizar alguns dos custos de levar a Internet para áreas rurais do mundo desenvolvido, a equipe do autor tem promovido o uso de sistemas wireless para compartilhar o custo de uma conexão à Internet. Em novembro de 2004, um projeto afiliado pediu que a equipe do autor implantasse um sistema deste tipo em um telecentro recentemente instalado na região rural de Mali, oito horas ao sudoeste de Bamako, a capital, em um veículo de tração nas quatro rodas.

A cidade rural, localizada à margem de uma reserva construída pelo homem, armazena água do manancial Manitali que gera energia para um terço do país. Esta região é afortunada, já que a energia hidrelétrica é mais estável e disponível que a gerada com diesel. Mas mesmo que a energia de geradores a diesel seja muito menos estável, algumas comunidades rurais tem sorte de, ao menos, receber algum tipo de energia.

A cidade é também dotada de uma das regiões mais férteis do país, em seu cinturão de algodão, a principal geração de renda em colheitas de Mali. Acreditava-se que esta região seria a de maior dificuldade para a instalação de um telecentro auto-sustentável. Como em muitos experimentos-piloto, esta instalação constituiu-se de muitos desafios.

Tecnologicamente, a tarefa era simples. Em 24 horas a equipe instalou uma rede wireless 802.11b que compartilha a conexão VSAT para a Internet do telecentro com outros cinco serviços locais: a prefeitura, o escritório do governo, o serviço de saúde, o conselho distrital e o conselho tutelar da comunidade.

Estes clientes foram selecionados em uma viagem de reconhecimento, dois meses antes. Durante esta viagem, a equipe entrevistou clientes em potencial e determinou quais poderiam ser conectados sem a necessidade de instalações caras ou complicadas. O próprio telecentro hospedava uma estação de rádio comunitária. Estações de rádio tendem a ser bons lugares para a instalação de redes wireless na zona rural de Mali, já que elas costumam estar bem localizadas, possuem eletricidade, segurança e pessoas que entendem ao menos o básico sobre transmissão de rádio. Elas também são um ponto de encontro natural para uma vila. O provimento de conexão Internet a uma estação de rádio melhora a qualidade de informação para seus ouvintes. Para uma cultura que é principalmente oral, o rádio acaba sendo o meio mais eficaz de fornecer informações.

Da lista de clientes acima, você logo percebe que todos são organizações governamentais ou para-governamentais. Isto provou ser uma mistura complicada, já que existia considerável animosidade e ressentimento entre os vários níveis de governo, com disputas contínuas a respeito de impostos e outras questões fiscais. Felizmente, o diretor da estação de rádio, o incentivador da rede, foi bastante dinâmico e capaz de ultrapassar estas questões políticas, mesmo que não completamente.

Escolhas de projeto

A equipe determinou que o ponto de acesso seria instalado a 20 metros de altura, na torre da estação de rádio, logo abaixo dos dipolos de rádio FM, mas não tão alto a ponto de causar interferência para os clientes localizados na depressão, em formato de uma tigela, onde a maioria deles se encontrava. A equipe focou-se então na forma de conexão de cada localidade cliente até este ponto central. Uma antena omnidirecional de 8 dBi (da Hyperlinktech, *http://hyperlinktech.com/*) seria suficiente, fornecendo cobertura para as localidades de todos os clientes. A antena de 8 dBi escolhida tem uma largura de feixe de 15 graus na vertical, garantindo que os dois clientes que estariam a menos de um quilômetro de distância ainda receberiam um forte sinal. Algumas antenas têm uma largura de feixe muito estreita, emitindo sinal com intensidade além da necessária para locais das proximidades. Antenas de painel foram consideradas, mesmo que neste caso ao menos duas seriam necessárias em conjunto com um segundo rádio ou um divisor de canal. Isto provou-se desnecessário para esta instalação. Os cálculos a seguir mostram como estimar o ângulo formado entre a antena no local do cliente e a antena na estação base, usando trigonometria.

```
tan(x) = diferença de altura
       + altura da antena da estação base
       - altura da antena no cliente
       / distância entre os locais

    tan(x) = 5m + 20m - 3m / 400m
         x = tan-1 (22m / 400m)
         x =~ 3 graus
```

Além do equipamento no telecentro (quatro computadores, uma impressora a laser e um switch de 16 portas), a estação de rádio já possuía uma estação de trabalho Linux instalada pelo autor do projeto para a edição de áudio. Um pequeno switch foi instalado na estação de rádio, ligado a um cabo de Ethernet que foi passado por um tubo plástico e enterrado a 5 cm no solo até o telecentro, passando pelo quintal.

Do switch principal, dois cabos sobem até o access point Mikrotik RB220. Os RB220 têm duas portas Ethernet, uma para a conexão ao VSAT através de um cabo cross-over e a segunda para a conexão com o switch central da estação de rádio. O RB 220 está acomodado em um gabinete de PVC construído manualmente e a antena omni de 8 dBi está montada diretamente no topo da tampa do gabinete de PVC.

O RB220 roda uma versão derivada do Linux, a Mikrotik versão 2.8.27. Ele controla a rede, fornecendo DHCP, firewall e serviços de DNS-caching, ao mesmo tempo em que roteia o tráfego para o VSAT usando NAT. O Mikrotik oferece uma poderosa linha de comando e uma interface gráfica completa e relativamente amigável. Ele é um pequeno computador baseado na arquitetura x86, projetado para o uso como access point ou sistema embarcado. Estes access points estão preparados para PoE, têm duas portas Ethernet, uma porta mini-pci, duas entradas para cartões PCMCIA, um leitor de memória flash (usado como memória não volátil), toleram variações de temperatura e têm o suporte a uma variedade de sistemas operacionais. Apesar do software Mikrotik exigir licença, já existia uma base de usuários substancial em Mali. A interface

gráfica poderosa e amigável do sistema provou ser superior a outros produtos. Por causa disto, a equipe concordou em utilizar estes sistemas, incluindo seu software, para o controle destas redes. O custo total do RB220, com nível de licença 7, Atheros mini-pci a/b/g e PoE foi de US$ 461,00. Você pode encontrar esta configuração online em *http://www.mikrotik.com/routers.php#linx1part0*

A rede foi projetada para permitir a expansão através da divisão em várias sub-redes para cada cliente; sub-redes privadas de 24 bits foram alocadas. O AP tem uma interface virtual em cada sub-rede e faz todo o roteamento entre elas, além de permitir o fiwerall na camada de IP. Observação: isto não fornece um firewall na camada de rede, assim, o uso de um sniffer de rede como o tcpdump irá permitir a visualização de todo o tráfego no link wireless.

Para limitar o acesso aos assinantes, a rede usou o controle de acesso pelo endereço MAC. Pouco risco de segurança foi percebido para a rede. Neste primeiro momento, um sistema de segurança mais eficaz foi deixado para a implantação futura, quando seria possível o tempo para encontrar uma interface mais simples para o controle de acesso. Os usuários foram encorajados a usar protocolos seguros, como https, pops, imaps, etc.

O projeto afiliado instalou um sistema VSAT de banda B (DVB-S). Estes sistemas de satélite são normalmente mais confiáveis e freqüentemente utilizados por provedores de acesso. É um equipamento grande e caro, neste caso com um prato parabólico de 2,2 metros de diâmetro, custando aproximadamente US$ 12.000,00 incluindo a instalação. Sua operação também é cara. Um link de recepção de 128 kbps e 64 kbps de transmissão para a Internet custa aproximadamente US$ 700,00 ao mês. Este sistema tem muitas vantagens se comparado a um sistema de banda Ku, incluindo um melhor desempenho em condições climáticas ruins, baixa taxa de contenção (número de usuários competindo pelo mesmo serviço) e é mais eficiente no tráfego de dados.

A instalação deste VSAT não foi a ideal. Uma vez que o sistema rodava o Windows, os usuários foram capazes de, rapidamente, mudar algumas configurações, incluindo a adição de uma senha para a conta de usuário padrão. O sistema não tinha um no-break ou uma reserva de energia em baterias, por isso, assim que houve uma queda de energia o sistema reinicializou e ficou aguardando por uma senha que já havia sido esquecida. Para piorar a situação, já que o software do VSAT não foi configurado para rodar como um serviço, ele não inicializou automaticamente para o restabelecimento do link. Mesmo que os sistemas de banda C sejam confiáveis, esta instalação causou paradas desnecessárias que poderiam ter sido evitadas com o uso de um no-break, configuração apropriada do software do VSAT como um serviço e com o limite de acesso físico ao modem. Como qualquer proprietário de um novo equipamento, o pessoal da estação de rádio queria exibi-lo, deixando-o bem à mostra. Preferencialmente, um espaço com portas de vidro teria mantido o equipamento visível, mas ainda assim em segurança.

O sistema wireless era bastante simples. Todos os clientes selecionados estavam localizados a uma distância dentro de um raio de 2 km da estação de rádio. Cada localidade possuía uma parte de sua construção através da qual se poderia fisicamente avistar a estação de rádio. No lado do cliente, a equipe optou por utilizar pontos de acesso comerciais comuns, tomando como base principal o seu preço. Foram utilizados equipamentos Powernoc 802.11b CPE

bridge com antenas SuperPass de 7 dBi e adaptadores construídos artesanalmente para Power Over Ethernet (PoE). Para facilitar a instalação, o access point e a antena foram montados em uma pequena peça de madeira que depois seria instalada do lado de fora do prédio, apontando para a estação de rádio.

Em alguns casos, a peça de madeira era cortada em ângulo para otimizar a posição da antena. Do lado interno, um adaptador PoE feito com um amplificador de sinal de televisão de 12V foi utilizado como fonte de energia para os equipamentos. Nos clientes não existiam redes locais, assim a equipe teve que instalar o cabeamento e hubs apropriados para levar a Internet a cada computador. Em alguns casos foi necessária a instalação de placas de Ethernet e seus drivers (o que não havia sido levantado inicialmente no projeto). Como as redes dos clientes eram simples, foi decidido que o mais fácil seria implementar uma bridge entre elas. Caso fosse necessário, a arquitetura IP permitiria o futuro particionamento da rede e o equipamento Powernoc adquirido já tinha o suporte para isto. O custo de cada bridge Powernoc foi de US$ 249,00.

Uma equipe local esteve envolvida durante toda a instalação da rede wireless. Um programa desenvolvido logo após a instalação capacitou a equipe em todos os aspectos da rede, desde o cabeamento até o posicionamento das antenas. Este treinamento intensivo durou várias semanas e buscou ensinar à equipe local tudo o que era necessário para o cumprimento diário de suas tarefas, assim como a análise básica de problemas da rede.

Um jovem recém formado que havia retornado à comunidade foi escolhido para dar o suporte ao sistema, com exceção da instalação dos cabos, que ficou à cargo do técnico da estação de rádio. O cabeamento de redes Ethernet é bastante similar aos reparos e instalações de cabos coaxiais com os quais o técnico já estava familiarizado. O jovem recém formado também precisou de pouco treinamento. A equipe de implantação passou boa parte de seu tempo ensinando-o técnicas de suporte básico para o sistema e o telecentro. Assim que o telecentro foi inaugurado, estudantes enfileiraram-se para os cursos de informática, que ofereciam treinamento e uso da Internet por uma taxa mensal de US$ 40,00, uma pechincha comparada aos US$ 2,00 por hora de acesso à Internet. O fornecimento deste curso proporcionou um ganho significativo e foi uma tarefa na qual o jovem formado, apaixonado por computadores, encaixou-se muito bem.

Infelizmente, mas sem que isto causasse surpresa, o jovem graduado partiu para a capital, Bamako, depois de receber uma oferta para um trabalho no governo. Isto deixou o telecentro órfão. Seu membro com maior conhecimento técnico e o único treinado para o suporte ao sistema havia ido embora. A maior parte do conhecimento necessário para o trabalho foi embora com ele. Depois de muitas discussões, a equipe decidiu que o melhor não seria buscar um outro jovem com conhecimento técnico e sim focar-se na equipe local permanente, mesmo que tivessem uma experiência técnica limitada. Isto levou muito mais tempo. Nossa equipe de treinamento teve que retornar para ministrar um total de 150 horas de cursos. Várias pessoas foram treinadas em cada função e as tarefas do telecentro foram divididas entre todos.

O treinamento não parou aqui. Uma vez que os serviços comunitários foram conectados, eles também precisavam de acesso. Notou-se que, mesmo que estivesse participando do projeto, a equipe diretora, incluindo o prefeito, não

estava utilizando os sistemas. A equipe deu-se conta da importância de garantir que os tomadores de decisão usassem o sistema e assim forneceu treinamento para eles e seus funcionários. Isto removeu, de fato, um pouco do misticismo da rede e fez com que os tomadores de decisão também se envolvessem.

Passado o treinamento, a equipe do projeto ainda monitorou a localidade e começou a colaborar com idéias, avaliando formas pelas quais este modelo poderia ser melhorado. As lições aprendidas aqui foram aplicadas em outras localidades.

Modelo financeiro

O telecentro comunitário já estava estabelecido em um modelo sem fins lucrativos e passou a ser exigido que se tornasse auto-sustentável com a venda de seus serviços. O sistema wireless foi incluído como uma fonte suplementar de receita já que projeções financeiras indicavam que o telecentro não seria capaz, em breve, de pagar por sua conexão VSAT.

Baseado em pesquisa e em consultas à estação de rádio que gerencia o telecentro, vários clientes foram selecionados. A estação de rádio negociou os contratos com alguma ajuda de sua mantenedora. Para esta primeira fase, os clientes foram selecionados com base na facilidade de instalação e capacidade de pagamento. Os clientes foram solicitados a pagar uma taxa de assinatura, como descrito adiante.

A decisão sobre o quanto deveria ser cobrado foi uma das principais atividades e necessitou de consultorias e conhecimento que a comunidade não possuía em suas projeções financeiras. O equipamento foi pago com uma doação, para ajudar a diminuir os custos impostos à comunidade, mas os clientes ainda tiveram que pagar uma taxa de assinatura, que serviu para garantir o seu compromisso. A taxa de assinatura era equivalente a um mês da taxa de serviços.

Para determinar o custo mensal de fatias iguais da largura de banda, começamos com a seguinte fórmula:

```
VSAT + salários + despesas (eletricidade, suprimentos) =
 lucro do telecentro + lucro do cliente wireless
```

Estimamos que o telecentro deveria receber entre 200 e 300 dólares de lucro mensal. As despesas totais foram estimadas em US$ 1.050,00 ao mês, assim divididas: US$ 700,00 para o VSAT, US$ 100,00 para salários, US$ 150,00 para eletricidade e cerca de US$ 100,00 para suprimentos. Cerca de US $ 750,00 de lucro vindo dos clientes wireless eram necessários para equilibrar a equação. Isto resultou em aproximadamente US$ 150,00 para cada cliente. O valor era tolerável pelos clientes e parecia viável, mas requeria um bom clima e não havia margem para complicações.

Uma vez que isto estava tornando-se complicado, trouxemos os especialistas de negócios, que modificaram a fórmula da seguinte maneira:

```
Despesas mensais + amortização + fundos de segurança =
 lucro total
```

Os especialistas de negócios rapidamente nos mostraram a necessidade de amortização do equipamento, ou fundos de reinvestimento assim como fundos de segurança que asseguram que a rede possa continuar na desistência de um

cliente ou no caso de quebra de um equipamento. Isto adicionou cerca de US$ 150,00 ao mês para a amortização (equipamentos avaliados em cerca de US$ 3.000,00, amortizados em 24 meses) e o valor de um cliente para a eventual falta de pagamentos em US$ 100,00. Foram adicionados mais 10% para contar com a desvalorização financeira (US$ 80), o que totaliza uma despesa de US$ 1.380,00 ao mês. Ao tentar implementar este modelo, foi decidido que a amortização era um conceito muito difícil de ser passado à comunidade e que eles não considerariam que os clientes poderiam falhar seus pagamentos. Assim, ambas as fórmulas foram usadas, a primeira para o telecentro e a segunda para a nossa análise interna.

Como logo foi descoberto, pagamentos regulares não fazem parte da cultura da zona rural de Mali. Em uma sociedade agrária, onde tudo é sazonal, o mesmo acontece com a receita financeira. Isto significa que a receita da comunidade flutua bastante. Além disso, como muitas instituições públicas estão envolvidas, eles têm longos ciclos de orçamento com pouquíssima flexibilidade. Mesmo que eles tivessem, teoricamente, o orçamento para pagar pelo serviço, poderia levar meses até que estes pagamentos fossem feitos. Outras complicações fiscais também surgiram. Por exemplo, o prefeito aprovou e utilizou impostos devidos pela estação de rádio para pagar por sua assinatura. Isto, obviamente, não contribuiu para o fluxo de caixa. Infelizmente, provedores de VSAT têm pouca flexibilidade e paciência, já que eles têm uma largura de banda limitada e apenas têm espaço para aqueles que podem pagar.

A gestão do fluxo de caixa tornou-se uma grande preocupação. Primeiro porque o lucro previsto nas projeções mostrou que, mesmo com uma visão otimista, não apenas não existiria o lucro necessário para pagar pelas taxas, mas o transporte do dinheiro para o banco de Bamako também era um problema. As estradas próximas à vila podem ser perigosas devido a contrabandistas da Guiné e rebeldes da Costa do Marfim. Como projetado, o telecentro não pôde pagar por seus serviços e ele foi suspenso, desta forma foram suspensos também os pagamentos recebidos pelos clientes.

Antes que o projeto fosse capaz de encontrar soluções para estes problemas, o próprio custo do VSAT já havia começado a levar o telecentro ao débito. Depois de vários meses, devido a problemas técnicos assim como às preocupações levantadas pela análise, o equipamento VSAT de banda C foi substituído por outro mais barato de banda Ku, que ainda atendia às necessidades da rede. Este sistema custava apenas US$ 450,00 e, uma vez desconsiderada a amortização e margem de segurança, poderia ser pago pela rede. Infelizmente, devido a falhas de pagamento, a rede não pode pagar pela conexão VSAT após o período inicial de subsídio.

Conclusões

A construção de uma rede wireless é relativamente fácil, mas torná-la operacional é mais uma questão de negócios do que técnica. Um modelo de pagamento que considere o reinvestimento e riscos é uma necessidade, caso contrário a rede irá falhar. Neste caso, o modelo de pagamento não era apropriado, já que não estava em conformidade com os ciclos fiscais dos clientes e nem com suas expectativas sociais. Uma análise de riscos apropriada

teria concluído que US$ 700,00 (ou mesmo US$ 450,00) de receita mensal deixaria uma margem muito estreita entre a receita e a despesa, incapaz de compensar problemas não previstos. Alta demanda e necessidades educacionais limitaram a expansão da rede.

Após o treinamento, a rede operou por oito meses sem nenhum problema técnico significativo. Então, um surto de energia causado por um raio destruiu a maioria do equipamento na estação, incluindo o access point e o VSAT. Como resultado, o telecentro ainda estava fora do ar no momento em que este livro foi escrito. Na ocasião, a fórmula já apontava que a solução implementada não era a apropriada.

—Ian Howard

Ofertas comerciais no Leste da África

Esta sessão descreve a implantação de soluções wireless comerciais na Tanzânia e no Quênia que garantem 99,5% de disponibilidade no acesso à Internet e conectividade de dados em países em desenvolvimento. Em contraste com projetos destinados ao acesso ubíquo, nós focamos a oferta de serviços a organizações, tipicamente aquelas com necessidades críticas de comunicação internacional. Descreverei duas soluções comerciais radicalmente diferentes para a conectividade wireless, sumarizando as principais lições aprendidas em dez anos no Leste da África.

Tanzânia

Em 1995, com Bill Sangiwa, fundei o CyberTwiga, um dos primeiros provedores de acesso à Internet na África. Serviços comerciais, limitados ao tráfego de email em um link SITA de 9,6 kbps (custando mais de US$ 4.000 ao mês!) começaram em meados de 1996. Frustrado com a má qualidade dos serviços de telefonia pública e incentivado pelo sucesso na implantação de uma rede multiponto com três nós pela Autoridade dos Portos da Tanzânia, negociamos com uma empresa de telefonia celular para a colocação de uma estação base PMP (ponto-a-multiponto) em sua torre central. Com a conexão de algumas corporações a esta LAN wireless proprietária de 2,4 GHz no final de 1998, nós validamos o mercado e nossa capacidade técnica para o fornecimento de serviços wireless.

Como os competidores anarquicamente implantaram redes de 2,4 GHz, dois fatos apareceram: um mercado para serviços wireless já existia, mas um aumento do ruído de RF nas redes de 2,4 GHz iria diminuir a qualidade da rede. Nossa incorporação à empresa de telefonia móvel, em meados do ano 2000, incluía planos para uma rede nacional sem fio, construída com o uso da infra-estrutura existente para celulares (torres e linhas de transmissão) e alocação de espectro RF proprietário.

Como a arquitetura já existia (torres de celulares, linhas de transmissão, etc) o projeto da rede de dados e sua implantação ocorreram de forma rápida e direta. A cidade de Dar es Salaam é bastante plana e como o parceiro de telefonia celular operava uma rede analógica, as torres eram muito altas. Uma

empresa irmã no Reino Unido, Tele2, havia começado suas operações com equipamentos Breezecom (agora Alvarion) na freqüência de 3,8/3,9 GHz, assim, seguimos o mesmo caminho.

No final de 2000, estabelecemos a cobertura em várias cidades utilizando circuitos E1 fracionados para o link principal (backbone) da rede. Em muitos casos, o tamanho pequeno das cidades conectadas justificou o uso de uma simples estação base omnidirecional PMP. Apenas na capital comercial, Dar es Salaam, foi que instalamos estações base de três setores. Os limites de largura de banda foram configurados diretamente nos rádios clientes, aos quais normalmente configuramos um endereço IP público e único. Os roteadores em cada estação-base enviavam o tráfego aos endereços IP estáticos nas localidades clientes e evitavam que o tráfego broadcast inundasse a rede. As pressões do mercado mantiveram os preços baixos, em cerca de US$ 100,00 ao mês para 64 kbps, mas naquele tempo (meados do ano 2000) os provedores de acesso podiam operar com rádios de contenção muito impressionantes e lucrativos. Aplicações famintas por rede, como as de compartilhamento de arquivos peer-to-peer, voz e ERPs simplesmente não existiam no Leste da África. Com o alto custo das redes internacionais de telefonia, as empresas rapidamente mudaram o tráfego via fax para email, mesmo que a compra de seus equipamentos wireless custassem entre 2 e 3 mil dólares.

Capacidades técnicas foram desenvolvidas internamente, fazendo com que a equipe recebesse treinamento internacional em matérias como SNMP e UNIX. Além de melhorar o conjunto de habilidades da empresa, estas oportunidades de treinamento contribuíram para a lealdade da equipe. Tínhamos que competir com empresas de mineração de ouro, as Nações Unidas e outras agências internacionais por um limitado mercado de mão-de-obra em TI.

Para garantir a qualidade nas instalações clientes, um instalador local de rádio e telecomunicações altamente qualificado foi contratado, com o acompanhamento detalhado do processo em cartões de trabalho. Temperaturas altas, uma forte luz solar equatorial, chuvas fortes e tempestades elétricas estavam entre os insultos naturais aos quais os componentes externos eram submetidos. A integridade do cabeamento RF era vital.

A maioria dos clientes não possuía uma equipe competente de TI, obrigando nossos empregados à tarefa de configurar muitas espécies de hardware e topologias de rede.

Obstáculos legais e de infra-estrutura impediam nossas operações com freqüência. A operadora de celular controlava rigidamente suas torres de forma que, na eventualidade de um problema técnico em uma estação base, horas ou dias poderiam se passar antes que o acesso à torre fosse concedido. Mesmo com geradores reservas e no-breaks em cada localidade, a energia elétrica sempre foi um problema. Para a operadora de celular, o fornecimento principal de energia elétrica nas estações-base não era tão crítico, já que os assinantes simplesmente associavam-se a uma outra estação-base, enquanto nossos clientes wireless fixos ficavam offline.

No lado legal, o problema maior aconteceu quando a autoridade de telecomunicações decidiu que nossa operação era a responsável por interferências nas operações de satélite em banda C em todo o país, ordenando que desligássemos nossa rede.

Mesmo mostrando evidências definitivas de que a culpa não era nossa, a agência reguladora conduziu um bloqueio, com grande publicidade, de nosso equipamento. Obviamente, a interferência persistiu e mais tarde foi determinado que ela vinha de um radar russo envolvido no acompanhamento de atividades espaciais. Nós negociamos silenciosamente com a agência reguladora e, ao final, fomos recompensados com duas faixas de 42 MHz no espectro proprietário das bandas de 3,4/3,5 GHz. Os clientes foram migrados para linhas discadas durante o período de pouco mais de um mês para que as estações bases fossem reconfiguradas e novos equipamentos fossem instalados nos clientes.

Por fim, a rede cresceu para cerca de 100 nós fornecendo boa (mesmo que não ótima) conectividade para sete cidades em mais de 3000 quilômetros de linhas de transmissão. Apenas a união com a operadora de celular tornou esta rede possível – a escala de negócios de Internet e dados, unicamente, não teria justificado a construção de uma rede de dados destas dimensões e o investimento necessário para as freqüências proprietárias. Infelizmente, a operadora de celular decidiu encerrar seu negócio de Internet em meados de 2002.

Nairóbi

No início de 2003 eu fui contatado por uma empresa do Quênia, AccessKenya, com fortes negócios com o Reino Unido e retaguarda técnica para projetar e instalar uma rede wireless em Nairóbi e redondezas. Beneficiados com profissionais soberbos nas áreas de negócios e redes, hardware wireless de qualidade, progressos em redes Internet e um mercado maior, nós projetamos uma rede de alta disponibilidade, alinhada com as imposições legais.

Duas questões de legislação direcionaram nosso projeto de rede. Naquela época, no Quênia, a licença para os serviços de Internet era separada daquela dos operadores públicos de dados e uma única empresa não poderia ter ambas as licenças. Para carregar o tráfego de provedores múltiplos ou usuários corporativos, a rede deveria ter total neutralidade. As freqüências proprietárias de 3,4/3,5 GHz não eram licenciadas para um provedor único e estávamos preocupados com interferências e a vontade técnica e política da agência reguladora. Além disso, o espectro na freqüência de 3,4/3,5 GHz era caro, custando cerca de mil dólares ao ano por estação-base. Dito de outra forma, uma estação-base utilizando 2 x 12 MHz implicava em taxas de licenças acima de 10 mil dólares ao ano. Como Nairóbi é uma cidade de colinas, com muitas árvores e vales, as redes wireless de banda larga requeriam muitas estações-base. A sobrecarga de licenças não era negligenciável. Por outro lado, as freqüências de 5,7/5,8 GHz eram sujeitas apenas a uma licença anual de cerca de 120 dólares por rádio instalado.

Para atender ao primeiro requisito legal, optamos prover serviços utilizando túneis VPN ponto-a-ponto e não através da rede ou de rotas estáticas de IP. Um provedor nos entregaria um endereço IP público em seu centro de operações. Nossa rede faria a conversão do IP público para privado e o tráfego ocorreria em nossa rede no espaço privado de endereços. No lado do cliente, uma conversão de IP privado para público entregaria ao cliente um endereço (ou conjunto de endereços) IP roteável globalmente para a sua rede.

A segurança e criptografia contribuíram para a neutralidade, flexibilidade e propriedades únicas de venda para a nossa rede. A largura de banda era limitada no nível do túnel VPN. Com base na experiência operacional de nossa empresa irmã no Reino Unido, VirtualIT, selecionamos a Netscreen (agora uma subsidiária da Juniper Networks) como o fornecedor dos firewall roteadores VPN.

Nosso critério para os equipamentos wireless de banda larga eliminou canos grandes e equipamentos cheios de funcionalidades, de alta performance. Formatos padrão, confiabilidade e facilidade de instalação e gerenciamento eram mais importantes do que velocidade. Todas as conexões internacionais para o Quênia em 2003, e até o momento em que escrevo, são feitas via satélite. Com custos cem vezes superiores à fibra ótica, as conexões via satélite impõem um limite financeiro na quantidade de banda que é adquirida pelos usuários finais. Nós julgamos que a grande parte da população necessitava de uma capacidade da ordem de 128 a 256 kbps. Selecionamos a recém lançada plataforma Canopy da Motorola para nosso modelo de rede e negócios.

A empresa Broadband Access, Ltd, estreou em julho de 2003, lançando a rede "Blue". Começamos pequenos, com uma única estação-base. Queríamos que a demanda direcionasse o crescimento de nossa rede, ao invés de confiar na estratégia da construção de grandes canos e a esperança de que eles seriam preenchidos.

Os equipamentos Canopy e melhorias de terceiros, como estações-base omnidirecionais, nos permitiram crescer nossa rede de acordo com o crescimento do tráfego, aliviando despesas capitais iniciais. Sabíamos que o preço disto era o de, com a expansão da rede, termos que setorizar o tráfego e realinhar rádios de clientes. A curva suave de aprendizagem em uma rede pequena trouxe dividendos posteriores. A equipe técnica adquiriu conforto com o suporte aos problemas dos clientes em um ambiente de rede simples, ao invés de ter que lidar com eles na complexidade de um ambiente lógico e de RF. A equipe técnica participou de dois dias de sessões de treinamento fornecidos pela Motorola.

Foi um projeto PMP típico, com estações-base conectadas a um ponto central através de um backbone de microondas de alta velocidade Canopy. A rede foi instalada em telhados de prédios e não em torres de antenas. Todas as localidades contratadas asseguravam um acesso 24x7 para a equipe, energia elétrica e, criticamente, protegiam a exclusividade das nossas freqüências de rádio. Não queríamos restringir os senhorios na oferta de espaço no telhado para nossos competidores, mas apenas a garantia de que nossos próprios serviços não seriam interrompidos.

A instalação em telhados fornece muitas vantagens. O acesso físico ilimitado, mesmo durante a noite ou com chuva ajudou-nos a atingir nosso objetivo de 99,5% de disponibilidade da rede. Grandes prédios também hospedam muitos clientes grandes, sendo possível conectá-los diretamente em nossa rede principal de microondas. A instalação em telhados tem o contraponto de um tráfego maior de pessoas – trabalhadores fazendo a manutenção de equipamentos, consertando vazamentos e, ocasionalmente, danificando cabos. Como resultado disto, todas as estações-base eram montadas com dois conjuntos de cabos para todos os elementos de rede, um primário e um reserva.

Pesquisas locais confirmaram a disponibilidade do link de rádio e os requerimentos dos clientes. A equipe de pesquisa registrou a posição GPS para cada cliente e levava um detector de altura a laser para registrar também a altura dos obstáculos. Assim que receberam o pagamento pelo hardware, os contratados, sob a supervisão de uma pessoa da equipe técnica, realizaram a instalação dos equipamentos. O Canopy tem a vantagem de que tanto os equipamentos para a instalação nos clientes como os elementos da estação-base são leves, de forma que a maioria das instalações não necessitou de trabalho extenso de construção ou estaias. O cabeamento do Canopy também é simples, com uma conexão externa UTP ligando os rádios diretamente às redes dos clientes. Com o planejamento apropriado, a maioria das instalações foi completada em menos de uma hora, sem a necessidade de treinamento avançado dos contratados ou ferramentas especiais.

Conforme compilávamos centenas de posições GPS dos clientes, começamos a nos aproximar de uma empresa de pesquisas local, para colocar estas localidades em mapas topográficos. Isto tornou-se uma ferramenta chave para o planejamento de instalação de estações-base.

Observe que a arquitetura ponto-a-ponto com túnel VPN, com suas camadas física e lógica separadas, necessitava que os clientes adquirissem tanto os equipamentos wireless para banda larga como o de VPN. A fim de controlar fortemente a qualidade, nós nos recusamos categoricamente a aceitar que os clientes fornecessem seu próprio hardware – eles tinham que adquirí-los de nós a fim de ter garantias de serviço e do hardware. Cada cliente tinha o mesmo pacote de hardware. Instalações típicas custavam cerca de US$ 2.500,00, em comparação com os custos mensais de 500 a 600 dólares para 64 a 128 kbps de largura de banda. O benefício do túnel VPN é que nós podíamos impedir que o tráfego do cliente passasse pela rede lógica (no caso de sua rede estar infectada por um verme, ou se eles não pagassem a conta) enquanto a camada de rádio permanecia intacta e gerenciável.

Como isto cresceu de uma estação-base para dez, e os serviços foram expandidos para Mombasa, o projeto da rede RF evoluiu e, sempre que possível, os elementos de rede (roteadores) foram configurados com tolerância a falhas (*failover*) ou redundância (*hot swap*). Grandes investimentos tiveram que ser feitos em inversores e no-breaks em cada estação-base para garantir a estabilidade face à errática rede elétrica. Depois que um certo número de problemas em clientes (queda de conexões VPN) foi causado por quedas de energia, passamos a incluir um pequeno no-break como parte integral do pacote de equipamentos.

A adição de um analisador portátil de espectro ao nosso capital inicial de investimento foi custosa, mas altamente justificada na operação de nossa rede. A detecção de roteadores desonestos, a confirmação de características operacionais de nosso equipamento e a verificação da cobertura de RF melhoraram nosso desempenho.

A fanática atenção ao monitoramento nos permitiu melhorar o desempenho de nossa rede e coletar dados históricos valiosos. Registramos em gráficos feitos com o MRTG ou Cacti (como descrito no **Capítulo 6**) parâmetros como variação (*jitter*), RSSI e tráfego oriundo de roteadores desonestos, deterioração de cabos ou conectores e presença de vermes em redes de clientes. Não era

incomum que clientes reclamassem que o serviço em sua localidade havia sido interrompido por horas ou dias, exigindo crédito para cobrir isto. O monitoramento histórico verificou ou invalidou estas reclamações.

A rede Blue combinou várias lições da Tanzânia com uma melhor tecnologia de rede e RF.

Lições aprendidas

Durante alguns anos os circuitos de satélite ainda irão prover toda a conectividade Internet internacional no Leste da África. Muitos grupos têm oferecido propostas para a conexão submarina com fibras óticas, o que irá melhorar as telecomunicações quando acontecer. Comparado a regiões com conectividade com fibra, o custo da banda no Leste da África permanecerá muito alto.

Redes wireless de banda larga para a entrega de serviços Internet, portanto, não devem focar-se na velocidade. Ao invés disto, a ênfase deve ser colocada em confiabilidade, redundância e flexibilidade.

A confiabilidade de nossas redes sem fio era nosso ponto chave para a venda. No lado da rede, isto traduziu-se em investimentos consideráveis em substituição de infra-estrutura, como torres reserva, e atenção a detalhes como a montagem de conectores e cabeamento. A causa mais comum para que um cliente deixasse de ter conectividade eram cabos ou conectores. Não se ouvia falar, essencialmente, de falhas de rádios. Uma vantagem competitiva importante em nosso processo de instalação em clientes é que as equipes contratadas eram forçadas a aderir a especificações rigorosas. Era comum em sites bem gerenciados de clientes que a conexão ficasse ativa por centenas de dias, sem nenhuma parada que não fosse programada. Nós controlávamos o máximo possível de toda a nossa infra-estrutura (por exemplo, os telhados dos prédios).

Mesmo sendo atrativa uma potencial aliança com operadores de celular, nossa experiência mostrou que eles trazem mais problemas do que podem resolver. No Leste da África os negócios com Internet representam uma fração dos lucros de telefonia móvel, um lucro marginal para operadoras de celulares. A manutenção da rede de uma estrutura que não lhe pertence é, do ponto de vista da operadora de celular, um gesto de boa vontade, o que torna impossível atender aos compromissos da oferta do serviço.

A implantação de redes completamente redundantes, com tolerância a falhas e capacidade de *hot swap* é uma proposta cara na África. Apesar disto, os roteadores e o hardware VPN em nosso ponto central de presença são completamente redundantes, configurados para a tolerância transparente a falhas e testados rotineiramente. Para as estações-base decidimos não instalar roteadores duplos, mas manter roteadores reserva em estoque. Julgamos que 2 a 3 horas de indisponibilidade no pior caso (uma falha a 1h da manhã de um domingo com chuva) seria aceitável pelos clientes. Nos finais de semana, os membros da equipe têm acesso a um estoque de emergência que contém reservas para os equipamentos dos clientes, como rádios e fontes de alimentação.

A flexibilidade foi incluída no projeto lógico e de RF da rede. A arquitetura de túnel VPN ponto-a-ponto instalada em Nairóbi era extremamente flexível ao atender as necessidades de rede dos clientes. As conexões aos clientes

poderiam ser aceleradas (modo *burst*, ou rajada) durante as horas de pico para permitir cópias de backup para locais remotos, por exemplo. Nós também podíamos vender múltiplos links para destinos diferentes, aumentando o retorno de investimentos de rede, enquanto lançávamos novos serviços (como o monitoramento remoto de câmeras de vigilância) a nossos clientes.

No lado de RF tínhamos espectro suficiente para planejar expansões, assim como implementar um projeto alternativo de rede via rádio no caso de interferências. Com o crescente número de estações-base, provavelmente 80% de nossos clientes tinham duas estações ao alcance visual. Assim, se uma torre fosse destruída, poderíamos restaurar rapidamente o serviço.

A separação das camadas lógica e de RF da rede Blue introduziu um nível adicional de complexidade e custo. Levando em conta que, no longo prazo, as tecnologias de rádio irão avançar mais rapidamente que as tecnologias de rede, esta separação nos dá, em teoria, a flexibilidade para a substituição da rede RF sem atrapalhar a rede lógica. Ou podemos instalar uma rede diferente de rádio, alinhada com a evolução tecnológica (WiMax) ou a necessidade dos clientes, enquanto mantemos a rede lógica.

Finalmente, devemos nos render ao óbvio ponto que a exótica rede que instalamos seria completamente inútil se não tivéssemos um compromisso incansável com a qualidade de serviços aos nossos clientes. Era para isto, afinal, que éramos pagos.

Mais informações

- Broadband Access, Ltd.: *http://www.blue.co.ke/*
- AccessKenya, Ltd.: *http://www.accesskenya.com/*
- VirtualIT: *http://www.virtualit.biz/*

—Adam Messer, Ph.D

Rede Mesh sem fio na Comunidade Dharamsala

A Rede Mesh sem fio na Comunidade Dharamsala foi inaugurada em fevereiro de 2005, logo após a desregulamentação do Wi-Fi para o uso externo na Índia. No final do mesmo mês, a rede mesh já havia conectado oito campi.

Testes extensivos durante fevereiro de 2005 mostraram que o difícil terreno montanhoso é mais apropriado para redes mesh, já que as redes ponto-a-multiponto não conseguiam ultrapassar as limitações de linha de visão apresentadas pelas montanhas. A topologia mesh também ofereceu uma área de cobertura muito maior, já que a natureza de "auto cura" do roteamento mesh provou ser essencial em lugares onde o fornecimento de energia elétrica era, na melhor das hipóteses, errático.

A rede mesh inclui mais de 30 nós, todos compartilhando um único canal de rádio. Serviços de Internet de banda larga são fornecidos a todos os membros da rede mesh. O número total de largura de banda disponível é de 6 Mbps. Há

mais de 2.000 computadores conectados, colocando uma grande carga sobre a rede. No momento, o sistema parece lidar com esta carga sem aumento de latência ou perda de pacotes, mas está claro que a escalabilidade se tornará um problema se continuarmos a usar um único canal de rádio. Para resolver este problema, novos roteadores mesh com o suporte a múltiplos canais de rádio estão sendo desenvolvidos e testados em Dharamsala, com ênfase em produtos que atendam nossos requisitos técnicos e nossa viabilidade econômica. Os resultados iniciais são bastante promissores.

A rede mesh está baseada na implantação recorrente de um dispositivo de hardware projetado e construído localmente – conhecido como o ***Himalayan-Mesh-Router*** (*http://drupal.airjaldi.com/node/9*). Os mesmos roteadores mesh são instalados em todas as localidades, apenas com antenas diferentes, dependendo da localização geográfica e outras necessidades. Nós usamos uma grande variedade de antenas, omnidirecionais de 8 a 11 dBi e direcionais de 12 a 24 dBi e, ocasionalmente, algumas antenas setoriais de alto ganho (e alto custo).

A rede mesh é usada primariamente para:

- Acesso à Internet;
- Aplicações de compartilhamento de arquivos;
- Backups remotos;
- Reprodução de vídeo de alta qualidade a partir de arquivos remotos.

Uma central de VoIP, baseada em um PBX por software (Asterisk) fornece serviços avançados de telefonia para os membros. O PBX Asterisk também possui interface com a rede de telefonia pública. Entretanto, por questões legais, o PBX é utilizado apenas para chamadas internas dentro da rede mesh. Os assinantes usam uma ampla variedade de telefones por software, assim como vários ATAs (Adaptadores para Telefones Analógicos) e telefones IPs com funcionalidades completas.

Figura 11.5: Instalador de Dharamsala trabalhando em uma torre.

A rede mesh criptografada não permite o acesso a dispositivos móveis (como notebooks e PDAs). Assim, colocamos vários pontos de acesso 802.11b em várias das mesmas localizações onde os roteadores mesh estão instalados. A rede mesh fornece a infra-estrutura, enquanto estes APs fornecem o acesso a dispositivos móveis, quando necessário.

O acesso à rede mesh só é possível através de roteadores mesh. Clientes wireless simples não têm a inteligência necessária para "falar" o protocolo de roteamento da rede mesh e suas políticas estritas de acesso. O canal mesh é criptografado (WPA) e também "escondido" para prevenir que os dispositivos móveis o encontrem o tentem acessá-lo. A permissão do acesso à rede mesh apenas para os roteadores mesh permite um controle estrito de políticas de acesso e limitações aos dispositivos instalados nos clientes (CPE – *Client Premises Equipment*). Este controle é um elemento crucial para que se consiga a segurança fim-a-fim, limitação de tráfego e qualidade de serviço.

O consumo de um roteador mesh é menor que 4 Watts. Isto os torna ideais para o uso com painéis solares. Muitos dos roteadores mesh do Dharamsala são alimentados unicamente por pequenos painéis solares. O uso de energia solar, combinado com antenas pequenas e roteadores de baixa potência é ideal para áreas sujeitas a desastres, já que eles provavelmente irão sobreviver quando outras infra-estruturas de comunicação sofrerem danos.

—AirJaldi, http://airjaldi.com/

Rede no estado de Mérida

A cidade de Mérida está localizada ao pé da mais alta montanha da Venezuela, em um platô a cerca de 1.600 metros. É a capital do estado de Mérida e o lar de duas universidades centenárias, com cerca de 35.000 estudantes. A Universidade de Los Andes (ULA) instalou a primeira rede acadêmica de computadores em 1989. Esta rede, apesar das limitações econômicas, cresceu de forma a incorporar um link de 26 km de fibra ótica, através do qual circula o tráfego de redes TDM e ATM (*asynchronous transfer mode* – modo de transferência assíncrono). Em 2006, sobre o mesmo cabo de fibra ótica, uma rede de 50 km de Gigabit Ethernet foi instalada.

Figura 11.6: Mérida é um dos três estados montanhosos da Venezuela, onde os Andes atingem 5.000 m.

Ainda assim, muitas áreas da cidade e das vilas vizinhas estão fora do alcance do anel de fibra ótica. A universidade opera um servidor de comunicação com linhas telefônicas para prover o acesso remoto a sua rede, mas ligações locais são tarifadas por minuto e muitas vilas sequer possuem telefone.

Por estas razões, esforços para o desenvolvimento de acesso wireless à rede da universidade, chamada de RedULA, foram realizados desde o princípio. As primeiras tentativas aproveitaram-se de uma rede existente de pacotes, operada por rádio-amadores. Logo no início de 1987, eles tinham um gateway com uma estação de ***HF*** (*High Frequency* – ***Alta Freqüência***) trabalhando a 300 bps para contatos além-mar, assim como várias estações ***VHF*** (*Very High Frequency* – ***Freqüência Muito Alta***) conectadas a 1200 bps que cruzavam o país.

Enquanto as montanhas acidentadas da região são um grande obstáculo para a passagem de cabos e construção de estradas, elas podem ser muito úteis na implantação de uma rede de rádio. Esta tarefa ainda teve a ajuda de um sistema de bondinhos a cabo, reconhecidamente o maior do mundo, que liga a cidade a um pico de 4.765 metros.

Figura 11.7: Em seu caminho para o pico da montanha, o bondinho passa por uma estação intermediária chamada "La Aguada", que tem 3.450 m de altura e uma belíssima vista da cidade de Mérida e outras vilas, à distâncias de até 50 km.

Pacotes por rádio (packet radio)

Rádio-amadores locais operam uma rede de pacotes por rádio. Inicialmente ela funcionava a 1200 bps, usando rádios amadores de FM em VHF conectados a um computador pessoal através de um ***TNC*** (***terminal node controller***). O TNC é a interface entre o rádio analógico e os sinais digitais tratados pelo PC.

O TNC é responsável por assumir os circuitos *Push To Talk* (aperte para falar) mudando-o entre os modos de transmissão e recepção, realizar a modulação/demodulação e a montagem/desmontagem de pacotes usando uma variante do protocolo X.25 chamada de ***AX.25***. Gateways entre os rádios VHF e HF foram construídos com a conexão de dois modems entre o mesmo TNC e computador. Normalmente, um gateway conectaria a estação de pacotes VHF

local a outras estações do outro lado do oceano com o uso de estações de HF que poderiam atingir milhares de quilômetros, mas a uma velocidade de apenas 300 bps. Uma rede nacional de pacotes por rádio também foi construída, utilizando apenas dois ***digipeaters*** (*digital repeaters*—***repetidores digitais***, essencialmente um TNC conectado a dois rádios com antenas apontando em diferentes direções) para estender a rede de Mérida a Caracas. Os digipeaters operavam a 1200 bps e permitiam o compartilhamento de programas e alguns arquivos de texto entre os rádio-amadores.

Phil Karn, um rádio-amador com um bom conhecimento de redes de computadores, escreveu o programa KA9Q, que implementa TCP/IP sobre AX. 25. Usando este programa, cujo nome é o sinal de chamada de seu desenvolvedor, os rádio-amadores de todo o mundo logo foram capazes de se conectar à Internet usando vários tipos de rádios. O KA9Q mantém as funções do TNC em um nível mínimo, utilizando a capacidade dos PCs conectados a ele para a maior parte de suas funções de processamento. Isto permite uma maior flexibilidade e facilidade de atualizações. Em Mérida, nós logo conseguimos atualizar nossa rede para 9600 bps com o uso de modems mais avançados e muitos rádio-amadores agora podiam acessar a Internet através da rede cabeada RedULA. O limite da largura de banda de rádio disponível em VHF impõe um máximo na velocidade que pode ser atingida. Para aumentar a velocidade, é necessário aumentar a freqüência da portadora.

Rádio-amadores têm a permissão para usar canais com largura de 100 kHz utilizando sinais ***UHF*** (*Ultra High Frequency* – ***Freqüência Ultra Alta***). Rádios digitais acoplados com modems de 19,2 kbps dobraram a capacidade de transmissão. Um projeto com o uso desta tecnologia foi desenvolvido para conectar a "Casa de Ciência" na cidade de El Vigia até Mérida e a Internet. Antenas UHF foram construídas no LabCom, o laboratório de comunicações da ULA.

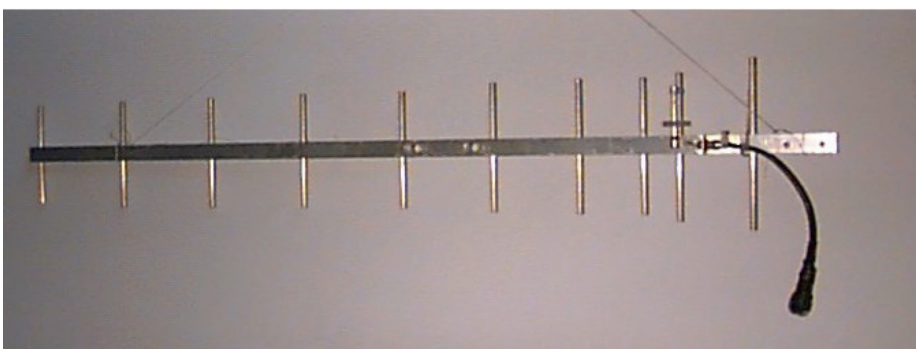


Figura 11.8: Uma antena UHF para packet radio desenvolvida no LabCom da ULA.

Mesmo que El Vigia esteja situada a apenas 100 km de Mérida através da estrada, o terreno montanhoso exigiu o uso de dois repetidores. Um está localizado em La Aguada, a 3.600 m de altitude, e outro em Tusta, a 2.000 m. O projeto foi financiado pela FUNDACITE MERIDA, uma instituição governamental que promove a ciência e tecnologia no estado. A FUNDACITE também opera um conjunto de modems telefônicos de 56 kbps para fornecer acesso à Internet para

instituições e indivíduos. A necessidade de duas estações repetidoras enfatiza as limitações impostas pelo uso de portadoras de alta freqüência, que requerem uma linha de visão para o estabelecimento de uma transmissão confiável. Na banda mais baixa, VHF, os sinais são facilmente refletidos e podem atingir além das colinas.

Algumas vezes é possível a utilização de um ***repetidor passivo*** para refletir sinais, o que é feito com a conexão de duas antenas direcionais conectadas em suas costas com um cabo coaxial, sem o uso de rádio. Este esquema foi testado para conectar a minha residência ao LabCom. A distância era de apenas 11 km, mas há uma colina que bloqueia os sinais de rádio. A conexão foi feita com o uso de um repetidor passivo para refletir o sinal vindo de La Aguada, com as duas antenas do repetidor apontando direções separadas em 40 graus. Mesmo que isto seja bastante atraente e certamente muito mais barato que o acesso através de modems para linhas telefônicas, um meio mais rápido obviamente seria necessário para uma rede wireless conectando vilas remotas.

Nós ainda exploramos o uso de modems de 56 kbps desenvolvidos por Dale Heatherington. Estes modems são montados em um cartão PI2 construído por rádio-amadores de Ottawa e conectados diretamente a um PC usando o Linux como sistema operacional de rede. Mesmo que estes sistemas funcionem muito bem, o surgimento da web e seu grande conjunto de imagens e outros tipos de arquivos que consomem banda deixou claro que, se quiséssemos satisfazer as necessidades de escolas e hospitais, nós deveríamos implantar uma solução de maior largura de banda, ao menos na infra-estrutura central da rede. Isto implicava no uso de freqüências portadoras ainda maiores no espectro de microondas, o que aumentaria os custos.

Felizmente, uma tecnologia alternativa largamente utilizada em aplicações militares estava tornando-se disponível para o uso civil a preços acessíveis. Chamada de ***spread spectrum*** (espectro espalhado), seu primeiro uso em aplicações civis foi em redes locais de pequeno alcance, mas logo provou-se também muito útil em lugares onde o espectro eletromagnético não está congestionado, permitindo cobrir distâncias de vários quilômetros.

Spread spectrum

O spread spectrum usa sinais de baixa potência com seu espectro expandido, com o propósito de ocupar toda a largura de banda alocada ao mesmo tempo em que permite que outros usuários compartilhem o meio, usando códigos diferentes para cada assinante.

Há duas formas de se conseguir isto: ***Direct Sequence Spread Spectrum*** (***DSSS*** – Seqüência direta de espalhamento do espectro) e ***Frequency Hoping Spread Spectrum*** (***FHSS*** – Espalhamento de espectro em intervalo de freqüência).

- No DSSS a informação a ser transmitida é multiplicada digitalmente por uma seqüência de freqüência mais alta aumentando, desta forma, a largura de banda da transmissão. Mesmo que isto pareça ser um desperdício de largura de banda, o sistema de recuperação é tão eficiente que pode decodificar sinais muito fracos, permitindo o uso simultâneo do mesmo espectro por várias estações.

- Em FHSS, o transmissor constantemente muda a freqüência portadora dentro da banda alocada, de acordo com um código especificado. O receptor deve conhecer este código a fim de acompanhar a freqüência portadora.

Ambas as técnicas trocam potência de transmissão por largura de banda, permitindo que muitas estações compartilhem uma determinada porção do espectro. Durante a Primeira Escola Latino Americana de Redes (EsLaRed '92) que ocorreu em Mérida, em 1992, nós conseguimos demonstrar esta técnica. Estabelecemos vários testes utilizando antenas externas construídas no LabCom, conseguindo transmissões em muitos quilômetros. Em 1993, o Ministério de Comunicações da Venezuela permitiu o uso de quatro bandas para o uso com DSSS:

- 400 - 512 MHz
- 806 - 960 MHz
- 2,4 – 2,4835 GHz
- 5,725 – 5,850 GHz

Em qualquer das bandas acima, a máxima potência de transmissão foi restrita a 1 Watt e o máximo ganho de antena a 6 dBi, para uma EIRP (*effective isotropic radiated power*—potência de radiação isotrópica efetiva) de 36 dBm. Esta normatização pavimentou o caminho para o desenvolvimento de uma rede DSSS com uma largura de banda nominal de 2 Mbps na freqüência de 900 MHz. Esta tecnologia satisfez a necessidade criada pelo surto de atividade na web.

A rede começou no LabCom, onde havia a disponibilidade de uma conexão com a RedULA. O LabCom instalou uma antena Yagi construída localmente, apontando a um refletor em Aguada. Isto forneceu um feixe com a largura de 90 graus, cobrindo a maior parte da cidade de Mérida. Muitas localidades assinantes, todas compartilhando a largura de banda nominal de 2 Mbps, estavam logo trocando arquivos, incluindo imagens e clipes de vídeo. Alguns assinantes que necessitavam de longos cabos entre a antena e o rádio de espectro espalhado foram atendidos com o uso de amplificadores bidirecionais.

Estes resultados encorajadores foram passados a um grupo estabelecido no Centro Internacional de Física Teórica (*International Centre for Theoretical Physics* – ICTP) em Trieste, na Itália, em 1995. Este grupo tinha o objetivo de prover conectividade entre o Centro de Informática, o Instituto de Ciências Físicas e o Instituto de Tecnologia na Universidade de Ile-Ife, na Nigéria. Mais tarde, no mesmo ano, a rede foi construída pela equipe do ICTP, com recursos da Universidade das Nações Unidas e está em funcionamento até hoje, provando ser uma solução muito mais efetiva em termos de custos do que a solução em fibra ótica planejada originalmente poderia ter sido.

De volta à Mérida, com o aumento do número de locais conectados, a velocidade de acesso por usuário caiu. Começamos a averiguar a banda de 2,4 GHz para fornecer capacidade adicional. Esta banda pode suportar, simultaneamente, três fluxos independentes de 2 Mbps cada, mas o alcance efetivo é menor do que o possível com a banda de 900 MHz. Estávamos muito ocupados no planejamento da extensão da rede usando 2,4 GHz quando

soubemos de uma nova empresa que oferecia uma solução que prometia a cobertura de maiores distâncias, velocidade dramaticamente mais alta e a possibilidade de reutilização de freqüências com microondas de banda estreita.

Sistema de entrega de banda larga

Após uma visita às instalações da Spike Technologies, em Nashua, New Hampshire, nos Estados Unidos, estávamos convencidos de que seus sistemas proprietários de rádio e antena eram a melhor solução para os requisitos de nossa rede estadual pelas seguintes razões:

Seu sistema de entrega de banda larga emprega uma antena setorial especial (**Figura 11.9**) com ganho de 20 dBi em cada um dos 22 setores independentes. Cada setor transmite e recebe em um canal independente a 10 Mbps, full duplex, em um agregado de 440 Mbps. A reutilização da freqüência em setores intercalados faz com que o sistema utilize o espectro de forma eficiente.

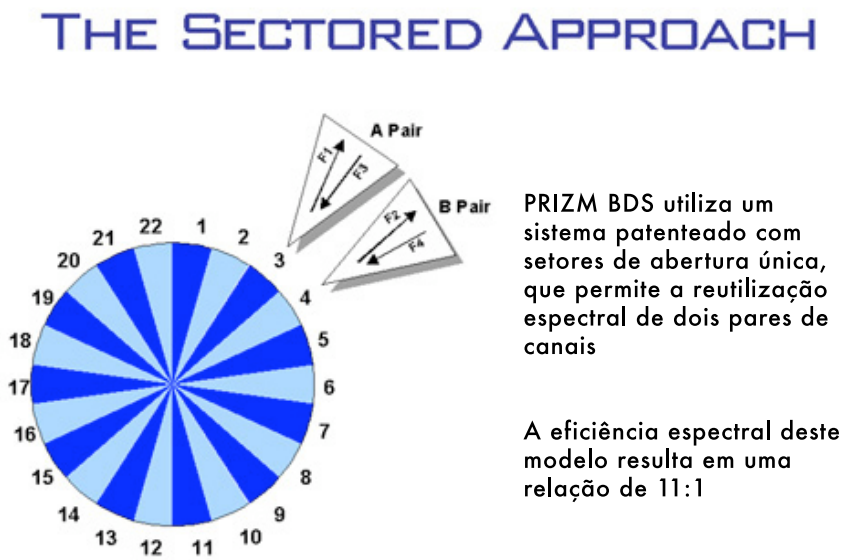


Figura 11.9: Sistema setorial de alta densidade full duplex, da Spike Technologies.

Os rádios digitais de banda estreita podem operar em qualquer freqüência entre 1 e 10 GHz, com uma cobertura de até 50 km. Os rádios trabalham com uma variedade de modems de TV a cabo, fornecendo uma conexão 10Base-T padrão para o assinante. Na estação-base, os setores são conectados com um switch de alta velocidade e baixíssima latência (veja a **Figura 11.10**), permitindo aplicações como streaming de vídeo de até 30 quadros por segundo. Cada setor funciona como uma LAN Ethernet independente.

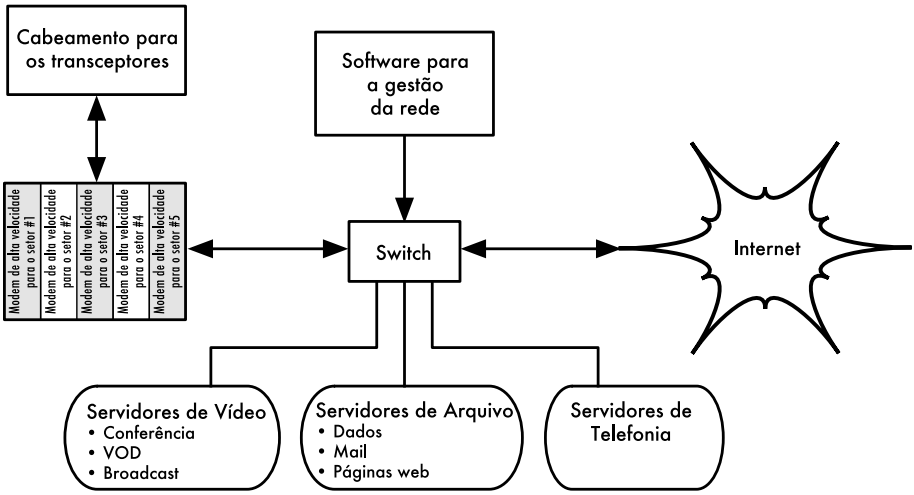


Figura 11.10: Interconexão entre sistemas da Spike Technologies.

No lado do assinante, um rádio similar e um modem fornecem uma conexão 10BaseT para a Ethernet local.

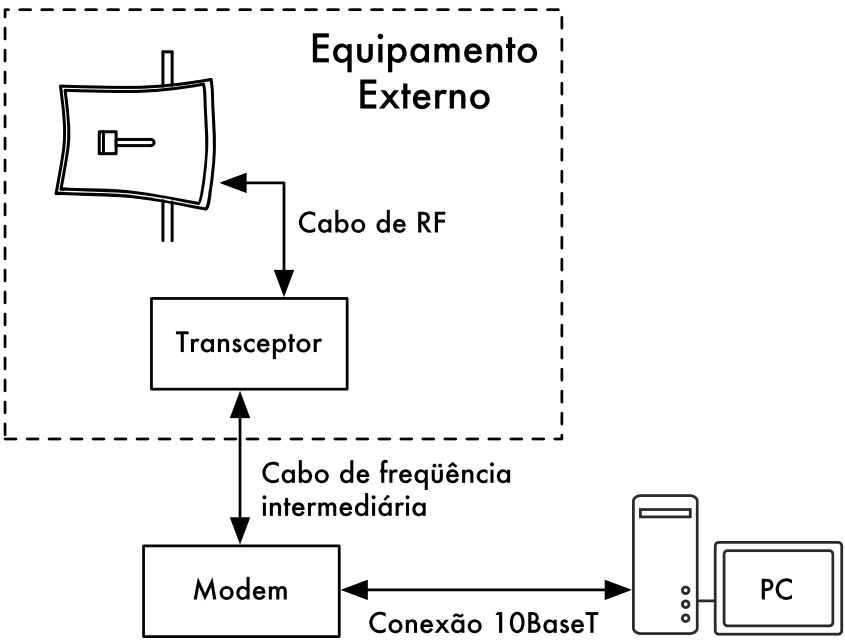


Figura 11.11: O link na localidade do assinante.

Com o financiamento da Fundacite, um sistema de teste logo foi instalado em Mérida, com a estação-base localizada logo acima da estação do bondinho em La Aguada, a uma altura de 3.600 metros.

Figura 11.12: Instalação acima de Mérida em La Aguada, a 3.600 metros de altitude.

Inicialmente, apenas cinco setores foram instalados, com uma largura de feixe de 16 graus cada. O primeiro assinante estava nas instalações da Fundacite, onde um sistema de satélite fornece o acesso à Internet. O segundo setor atendeu ao Palácio do Governador. O terceiro serviu à FUNDEM, uma fundação de apoio a vítimas de desastres mantida pelo governo local. O setor quatro foi usado na conexão de uma penitenciária próxima à cidade de Lagunillas, cerca de 35 km distante de Mérida. O quinto setor transmitia a um repetidor no topo de uma montanha próxima à vila de La Trampa, a 40 km de La Aguada. De La Trampa, um outro link de 41 km estendeu a rede para a Casa da Ciência na cidade de Tovar.

Em 31 de janeiro de 1998, uma videoconferência entre a penitenciária e o Palácio da Justiça de Mérida provou que, além de prover acesso à Internet, o sistema também permitia a transmissão de vídeo. Neste caso, ele foi usado para a acusação de prisioneiros, evitando a inconveniência e os riscos de seu transporte.

O sucesso deste teste fez com que o governo alocasse fundos para sua implementação completa, dando acesso de alta velocidade à Internet para o sistema de saúde do estado, o sistema educacional, bibliotecas, centros comunitários e várias agências de governo. Em janeiro de 1999, tínhamos três hospitais, seis instituições educacionais, quatro instituições de pesquisa, dois jornais, uma estação de TV, uma biblioteca pública e 20 organizações sociais e governamentais compartilhando informações e acessando a Internet. Os planos incluíam a conexão de 400 localidades dentro deste ano, com velocidade de 10 Mbps full duplex, com recursos já alocados para este propósito.

A **Figura 11.13** mostra um mapa do estado de Mérida. As linhas escuras mostram o backbone inicial, enquanto as linhas claras mostram a sua extensão.

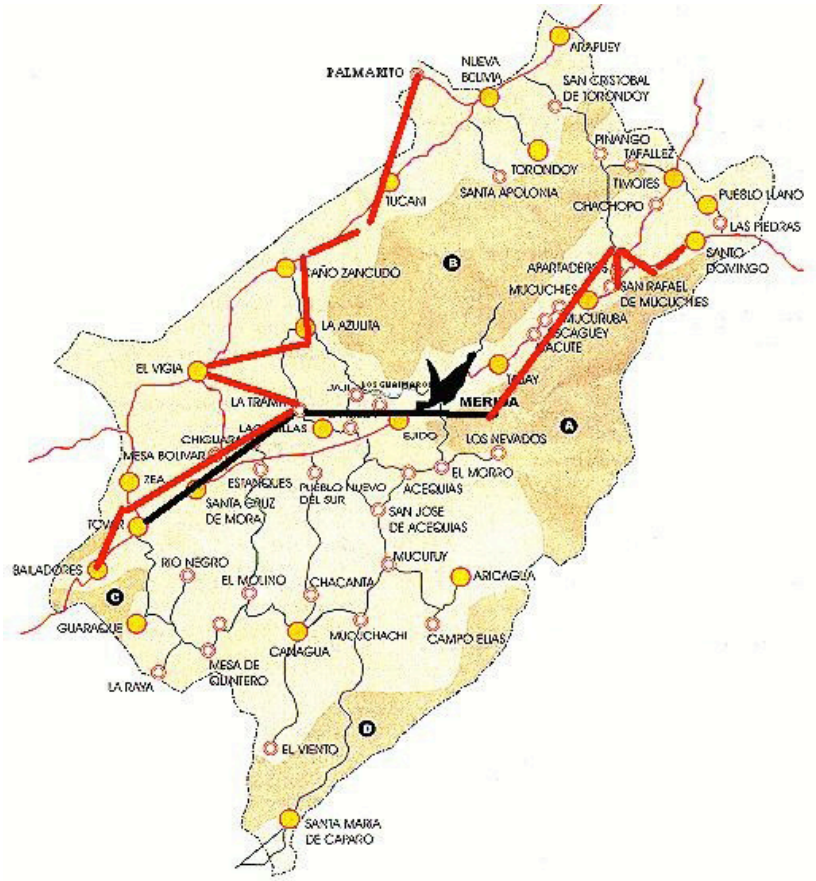


Figura 11.13: A rede do estado de Mérida.

Dentre as muitas atividades suportadas pela rede, é importante mencionar as seguintes:

- **Educacional**: As escolas encontraram uma fonte infindável de material de alta qualidade para seus alunos e professores, especialmente nas áreas de geografia, idiomas e ciências, assim como uma ferramenta para a comunicação com outros grupos que compartilham interesses comuns. As bibliotecas têm salas com computadores com capacidade plena de acesso à Internet que podem ser acessados pelo público em geral. Os jornais e estações de TV têm uma fantástica fonte de informações que podem disponibilizar para suas audiências.
- **Saúde**: O hospital da universidade tem um link direto para uma unidade de tratamento intensivo onde uma equipe de médicos especialistas está sempre de plantão. Estes doutores podem ser acessados por seus colegas em vilas remotas para a discussão de casos específicos. Um grupo de pesquisadores na universidade está desenvolvendo várias aplicações de telemedicina baseadas na rede.

- **Pesquisa**: O observatório astronômico de Llano del Hato, localizado em uma montanha de 3.600 m e a 8 graus do equador será conectado em breve, permitindo aos astrônomos de todo o mundo o acesso às imagens ali coletadas. Pesquisadores de campo, em muitas vilas, poderão contar com o acesso à Internet.
- **Governo**: Muitas agências de governo já estão conectadas e começaram a disponibilizar informações online para os cidadãos. Esperamos que isto tenha um profundo impacto na relação entre os cidadãos e o governo. Agências humanitárias e de policiamento fazem grande uso da rede.
- **Entretenimento e Produtividade**: Para as pessoas que vivem fora da cidade, as oportunidades oferecidas pela rede tiveram um impacto significativo em sua qualidade de vida. Nós esperamos que isto ajude a reverter a tendência de migração para fora das regiões do interior, aliviando a superpopulação das áreas urbanas. Fazendeiros têm acesso à informação sobre os preços de mercado de suas colheitas e suprimentos, assim como sobre melhores práticas para a agricultura.

Durante o SUPERCOMM '98, que aconteceu em junho na cidade de Atlanta, a rede de banda larga de Mérida recebeu o prêmio SUPERQuest na categoria 8-Remote Access como o melhor entre os indicados.

Treinamento

Desde nossos esforços iniciais para estabelecer uma rede de computadores, notamos que o treinamento era de fundamental importância para as pessoas envolvidas na construção, gestão e manutenção da rede. Em função de nosso orçamento limitado, tivemos que unir o que tínhamos com os recursos de outras pessoas que também necessitavam de treinamento. Em 1990, o ICTP organizou a Primeira Escola Internacional em gestão e análise de redes de computadores, da qual participaram os professores Jose Silva e Luiz Nunez de nossa universidade. Em seu retorno à Mérida, eles propuseram que devíamos de alguma forma replicar esta atividade em nossa universidade. Para isto, tomando vantagem de minhas férias sabáticas, passei três meses na Bellcore, em Morristown, Nova Jersey, Estados Unidos e mais três meses no ICTP, auxiliando na preparação da Escola de Redes em 1992, onde meu colega Professor Edmundo Vitale passou a trabalhar comigo. Passei o restante de minhas férias na SURANET, em College Park, Maryland, sob a tutela do Dr. Glenn Ricart, que apresentou-se ao Dr. Saul Hahn da Organização dos Estados Americanos, que ofereceu suporte financeiro para uma atividade de treinamento na América Latina. Estas experiências permitiram que lançássemos a primeira Escola Latino-Americana de Redes (EsLaRed'92) em Mérida, que contou com 45 participantes de oito países da região, com instrutores da Europa, Estados Unidos e América Latina. Este treinamento prático durou três semanas e as tecnologias wireless tiveram ênfase.

EsLaRed'95 aconteceu novamente em Mérida, com 110 participantes e 20 instrutores. EsLaRed'97 tinha 120 participantes e foi recomendada pela Internet Society, que também patrocinou o Primeiro Workshop em Português e Espanhol

para a América Latina e o Caribe, que aconteceu no Rio de Janeiro em 1998, com a EsLaRed sendo responsável pelo conteúdo do treinamento. Agora, dez anos depois, a EsLaRed continua a expandir seus esforços de treinamento em toda a América do Sul.

Considerações Finais

A Internet tem um impacto ainda mais profundo nos países em desenvolvimento do que em qualquer outro lugar em função dos altos custos de chamadas telefônicas internacionais, fax, revistas e livros. Isto é altamente exacerbado pela baixa renda da população. Alguns moradores em vilas remotas, que não têm telefones, estão experimentando a transição direta do século 19 ao século 21, graças a redes sem fio. Espera-se que isto contribua para a melhoria de vida nas áreas de saúde, educação, entretenimento e produtividade, assim como crie uma relação mais equilibrada entre os cidadãos e o governo.

Referências

- 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, Comision Nacional de Comunicaciones, Ministerio de Transporte y Comunicaciones, "NORMAS PARA LA OPERACION DE SISTEMAS DE TELECOMUNICACIONES CON TECNOLOGIA DE BANDA ESPARCIDA (SPREAD SPECTRUM)," Caracas, 17 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

Tecnologias recentes de transmissão sem fio de dados permitiram a criação de redes separadas geograficamente, de alta velocidade, a um custo relativamente baixo. Caso estas redes sejam construídas dentro da idéia de remover restrições no acesso à informação, as chamamos de ***redes livres***. Tais redes podem trazer grandes benefícios a todos os usuários, independente de suas condições políticas, sociais ou econômicas. Este tipo de rede é uma resposta direta ao modelo comercial normalmente restritivo que está imposto sobre a maioria da sociedade ocidental.

A fim de que redes livres floresçam, tecnologias wireless devem ser adequadas e postas a seu melhor uso possível. Isto é feito por grupos de

hackers que fazem a pesquisa, investigação, desenvolvimento e implantação de projetos, permitindo livre acesso ao conhecimento por eles adquirido.

A **Chilesincables.org** tem como objetivo a promoção e organização de redes wireless livres no Chile, de forma profissional. Fazemos isto ao prover educação sobre os aspectos técnicos e legais de redes sem fio, encorajar a adaptação de novas tecnologias através de pesquisas adequadas e estimular estas tecnologias para que atendam necessidades específicas das comunidades e da sociedade chilena.

Descrição da tecnologia

Empregamos uma grande variedade de tecnologias wireless, incluindo o IEEE 802.11.a/b/g. Também investigamos inovações neste campo, como o WiMAX. Na maioria dos casos, o equipamento foi modificado a fim de aceitar antenas externas construídas localmente e que estejam de acordo com as normas locais de telecomunicações.

Mesmo que a maior parte do hardware wireless disponível no mercado atendesse a nossos objetivos, encorajamos a utilização e exploração daqueles poucos fornecedores que permitiam um maior controle e a adaptação às nossas necessidades (sem que isto correspondesse necessariamente a um aumento de custos). Isto inclui os cartões Wi-Fi com arquitetura Atheros, Prism, Orinoco e Ralink, assim como modelos de access points fabricados pela Linksys, Netgear e Motorola. A comunidade hacker tem desenvolvido firmware que adiciona novas funcionalidades a estes equipamentos.

Para a infra-estrutura da rede utilizamos sistemas operacionais de código aberto, incluindo o GNU/Linux, FreeBSD, OpenBSD e Minix. Isto atendeu nossas necessidades nas áreas de roteamento e na implementação de serviços como servidores proxy, web e ftp. Além disto, estes sistemas compartilham a filosofia de nosso projeto, que é a de usar tecnologia livre com programas de código aberto.

Usos e aplicações

As redes implementadas disponibilizam, até o momento, as seguintes tarefas:

- Transferência de dados através de FTP ou servidores web;
- Serviços de VoIP;
- Streaming de áudio e vídeo;
- Mensagens instantâneas;
- Exploração e implementação de novos serviços como LDAP, resolução de nomes, novos métodos de segurança, etc.;
- Serviços fornecidos pelos clientes. Os usuários são livres para alterar a infra-estrutura da rede a fim de criar seus próprios serviços.

Administração e manutenção

A unidade operacional da rede é o ***nó***. Cada nó permite ao cliente associar-se à rede e obter serviços básicos. Obrigatoriamente, cada nó deve estar associado ao menos a outro nó. Isto permite que a rede cresça de forma o tornar mais serviços disponíveis para cada cliente.

Um nó é mantido por um administrador, que é um membro da comunidade comprometido com as seguintes tarefas:

- Manutenção da taxa adequada de disponibilidade (maior que 90%);
- Provimento de serviços básicos (normalmente o acesso web);
- Manutenção dos clientes atualizados sobre os serviços oferecidos pelo nó (por exemplo, quem pode acessar a rede). Isto é geralmente feito através do portal cativo.

A administração geral da rede (especialmente tarefas relacionadas à implantação de novos nós, seleção de localidades, topologia de rede, etc.) é feita pelo comitê diretor da comunidade ou por técnicos treinados para este propósito.

Chilesincables.org está atualmente no processo de transformação para uma organização legal, um passo que permitirá a regulamentação de seus processos administrativos internos e a formalização da comunidade como nossa associada.

Treinamento e formação de capacidades

Chilesincables.org considera de vital importância o treinamento de seus membros e clientes pelas seguintes razões:

- O espectro de rádio deve ser mantido o mais limpo possível, de forma a garantir a qualidade das comunicações wireless. Desta forma, o treinamento em técnicas de comunicação de rádio é essencial.
- O uso de materiais e métodos aprovados pela legislação vigente é requerimento para o desenvolvimento normal das atividades.
- A fim de atender os padrões da Internet, nossos administradores de rede são treinados em redes TCP/IP.
- Para garantir a continuidade de nossas operações de rede, o conhecimento desta tecnologia deve ser transferido aos usuários.

Para dar suporte a estes princípios, Chilesincables.org é responsável pelas seguintes atividades:

- **Workshop de Antenas**. Os participantes são treinados na construção de antenas e nos conceitos básicos de comunicação por rádio.
- **Workshop de Sistemas Operacionais**. Treinamento na implantação de roteadores e outros dispositivos baseados no GNU/Linux e outros softwares como m0n0wall ou pfsense. Conceitos básicos de rede são também ensinados.

- **Promoção e Divulgação**. Os mesmos objetivos são promovidos, mesmo para diferentes comunidades. Isto inclui workshops em faculdades, aulas, reuniões sobre software livre, etc.
- **Atualização de Materiais**. Chilesincables.org mantém um bom número de documentos e materiais disponibilizados para pessoas interessadas em atividades específicas.

As fotografias nas páginas seguintes apresentam um breve resumo das atividades em nossa comunidade.

Figura 11.14: Workshop sobre antenas omnidirecionais encaixadas. Nesta sessão, os participantes aprenderam sobre a construção de antenas e a teoria relacionada a isto.

Figura 11.15: Um dos membros de nossa equipe dando uma aula sobre a utilização de um roteador baseado no m0n0wall na administração de um nó.

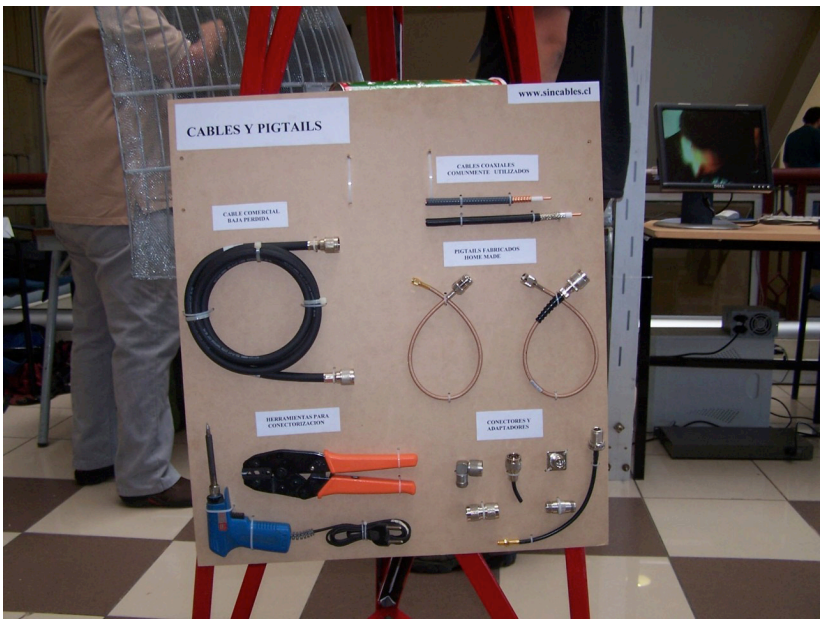


Figura 11.16: Detalhes de uma mini-torre, com amostras de antenas, cabos e conectores.

Figura 11.17: Estação wireless e antena parabólica usadas para a transmissão do evento Santiago-2006 FLISOL via streaming de vídeo.

Figura 11.18: Localização da outra extremidade do link.

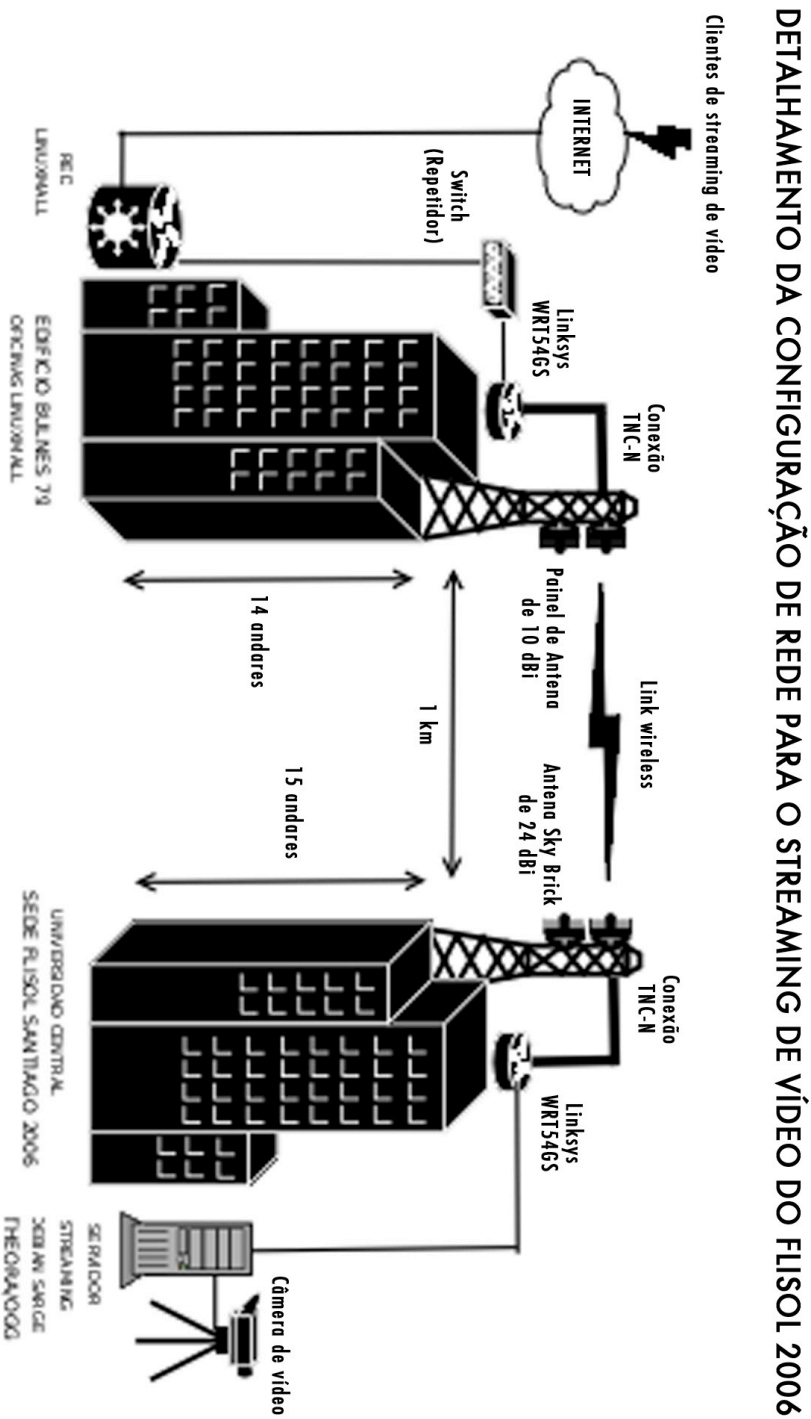


Figura 11.19: Esquema representando o streaming de vídeo da transmissão do Santiago-2006 FLISOL com o uso de software livre. A transmissão wireless conseguida tinha 36 Mbps em 1 km.

Figura 11.20: Nó de Quiani. Este é um dos nós mais altos do mundo. Está localizado a uma altura de 4.000 m, cerca de 2.000 km ao norte da capital do país.

Figura 11.21: Nó na região sul de Santiago, formado por uma torre de 15 m, uma antena Trevos Marshall 16+16 e 30 clientes. Este nó está conectado a outro no centro da cidade, a mais de 12 km de distância.

Figura 11.22: Vista panorâmica a partir do topo da torre de um dos nós.

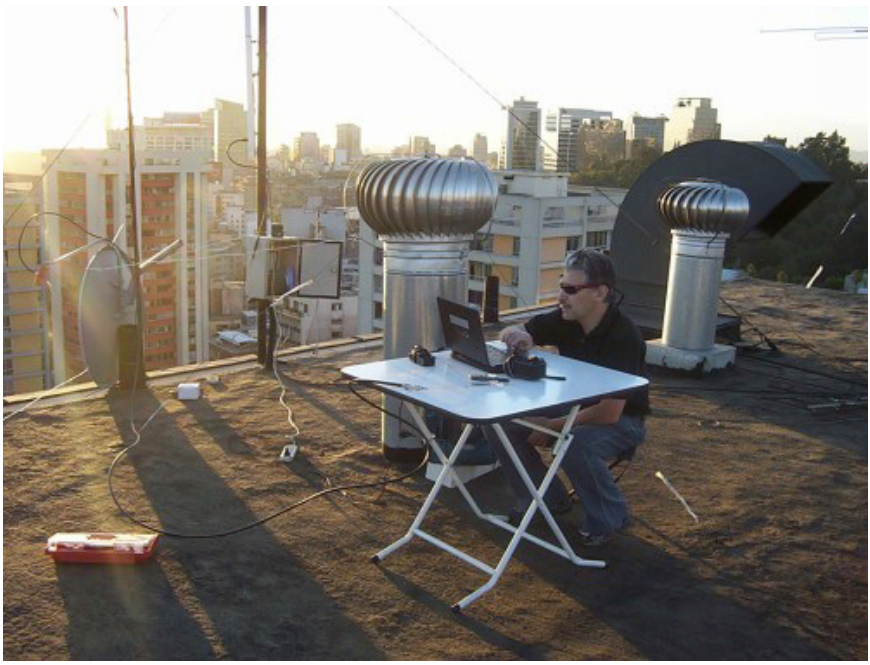


Figura 11.23: Nó central de Santiago, conectado ao nó no sul da cidade. Repare na antena parabólica para esta conexão e a antena omnidirecional encaixada para a conexão com os clientes.

Figura 11.24: Implantação de um nó em uma caixa d'água em Batuco, na região metropolitana, que provê o link para o telecentro Cabrati.

Figura 11.25: Workshop sobre antenas Yagi, organizado por nossa comunidade. Os participantes estão construindo suas próprias antenas.

Créditos

Nossa comunidade é formada por um grupo de associados voluntários comprometidos com nosso trabalho, dentre os quais destacamos:

Felipe Cortez (Pulpo), Felipe Benavides (Colcad), Mario Wagenknecht (Kaneda), Daniel Ortiz (Zaterio), Cesar Urquejo (Xeuron), Oscar Vasquez (Machine), Jose San Martin (Packet), Carlos Campano (Campano), Christian Vasquez (Crossfading), Andres Peralta (Cantenario), Ariel Orellana (Ariel), Miguel Bizama (Picunche), Eric Azua (Mr. Floppy), David Paco (Dpaco), Marcelo Jara (Alaska).

—*Chilesincables.org*

Longa Distância com 802.11

Graças a sua topografia favorável, a Venezuela já possui alguns links WLAN de longa distância, como o de 70 km operado pela Fundacite Mérida entre o Pico Espejo e a cidade de Canagua.

Para testar os limites desta tecnologia é necessário encontrar um caminho com uma linha de visão direta com um espaço de ao menos 60% para a primeira zona Fresnel.

Enquanto procurava um terreno na Venezuela, buscando por uma área com duas elevações altas em cada extremidade e um solo baixo entre elas, foquei-me primeiro na região de Guayana. Ainda que uma série de terras altas tenham sido encontradas, particularmente os famosos "tepuys" (mesas altas com paredes íngremes), existiam muitos obstáculos no caminho entre entre elas.

Minha atenção mudou-se para os Andes que, com suas encostas íngremes subindo abruptamente das planícies, provaram-se adequados para a tarefa. Durante muitos anos eu tenho viajado entre áreas pouco populadas em função da minha paixão por "*mountain biking*". Mantenho na minha memória uma série de locais diferentes que podem servir para a comunicação de longa distância.

O Pico del Águila é um local muito favorável. Ele tem uma altura de 4.200 m e está cerca de duas horas de viagem da cidade de Mérida, onde vivo. Para a outra ponta, finalmente localizei a cidade de El Baúl, no estado de Cojedes. Usando o software livre Radio Mobile (disponível em *http://www.cplus.org/rmw/english1.html*) descobri que não havia nenhuma obstrução para a primeira zona Fresnel (em uma distância de 280 km) entre o Pico del Águila e El Baúl.

Plano de ação

Uma vez satisfeito com a existência de um trajeto viável, buscamos pelo equipamento necessário para atingir o objetivo. Usamos os cartões Orinoco há muitos anos. Com uma potência de saída de 15 dBm e uma sensibilidade de recepção de -84 dBm, eles são robustos e confiáveis. A perda no espaço livre em 282 km é de 149 dB. Assim, precisaríamos de antenas de 30 dBi em ambos os lados e, mesmo assim, isto deixaria uma margem pequena para outras perdas.

Por outro lado, o popular roteador wireless Linksys WRT54G roda o Linux. A comunidade Open Source escreveu uma série de versões de firmware para ele, permitindo a completa customização de todos os parâmetros de transmissão. Em particular, o firmware OpenWRT permite o ajuste do tempo de reconhecimento da camada MAC, assim como a potência de saída. Outro firmware, o DD-WRT, tem uma interface gráfica e uma ferramenta muito conveniente para o levantamento das características de uma localidade. Além disto, o Linksys pode ser instalado mais próximo a uma antena do que um laptop. Assim, decidimos por um par destes dispositivos. Um foi configurado como AP (access point) e o outro como cliente. O WRT54G pode operar com 100 mW de potência de saída com boa linearidade, podendo até ser forçado a 200 mW. Mas em um valor tão alto, a perda de linearidade é severa, com a geração de sinais espúrios que devem ser evitados. Mesmo sendo um equipamento para o consumidor final e relativamente barato, depois de muitos anos que o utilizamos tínhamos a confiança de que ele poderia servir ao nosso propósito. Mas é claro que, por via das dúvidas, mantivemos um conjunto de reserva por precaução.

Com a configuração da potência de saída para 100 mW (20 dBm), poderíamos obter uma vantagem de 5 dB em comparação com o cartão Orinoco. Desta maneira, a decisão final recaiu sobre a utilização de um par de WRT54Gs.

Levantamento dos dados do Pico del Águila

Em 15 de janeiro de 2006, fui até o Pico del Águila para certificar o local que o Radio Mobile relatou como viável. O azimute em direção a El Baúl é de 86°, mas com a declinação magnética de 8°16', assim, nossa antena deveria apontar a uma direção magnética de 94°.

Infelizmente, ao olharmos na direção de 94°, encontramos uma linha de visão obstruída por um obstáculo que não foi mostrado pelo software, em função da resolução limitada dos mapas de elevação que estavam disponíveis de forma livre.

Andei com minha mountain bike por várias horas, examinando as redondezas e procurando por um caminho livre em direção ao leste. Identifiquei vários locais promissores e tirei fotos de todos eles, anotando as coordenadas com um GPS para o processamento posterior com o Radio Mobile. Isto permitiu que eu refinasse a seleção do meu caminho, resultando naquele que é mostrado na **Figura 11.26** com o uso do Google Earth:

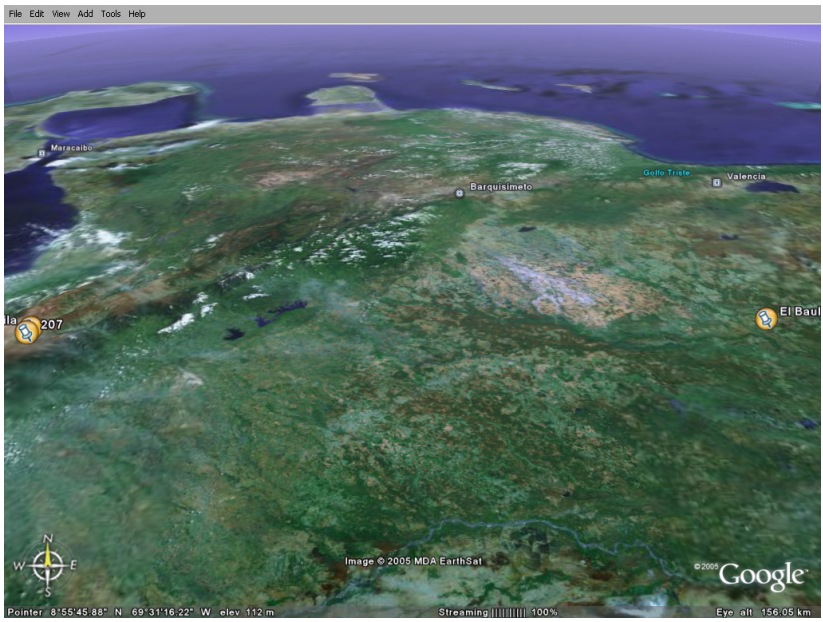


Figura 11.26: Vista do link de 280 km. O lago Maracaibo está ao oeste e a península de Paraguaná ao norte.

O perfil de rádio obtido com o Radio Mobile é mostrado na **Figura 11.27**:

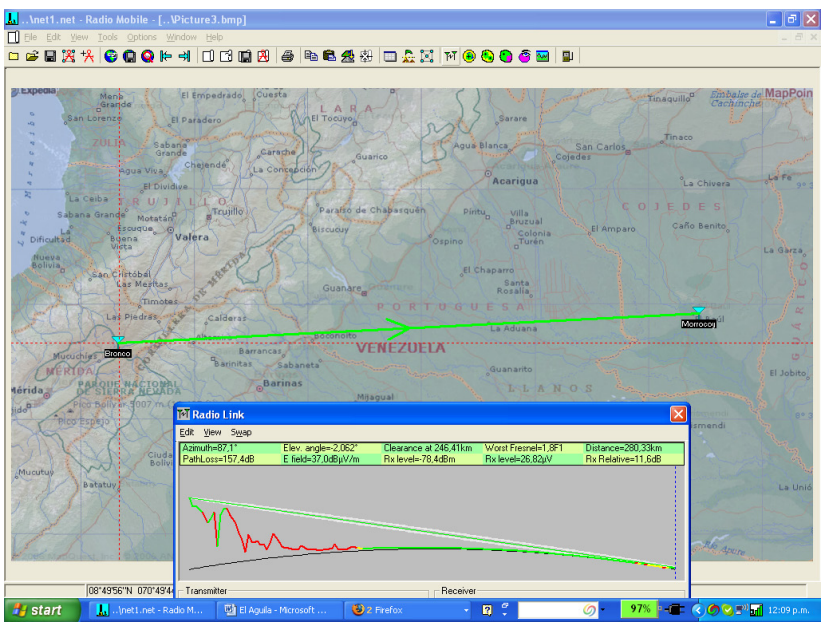


Figura 11.27: Mapa e perfil do caminho proposto entre o Pico Águila e a colina Morrocoy, próxima à cidade de El Baúl.

Os detalhes do link wireless são mostrados na **Figura 11.28**:

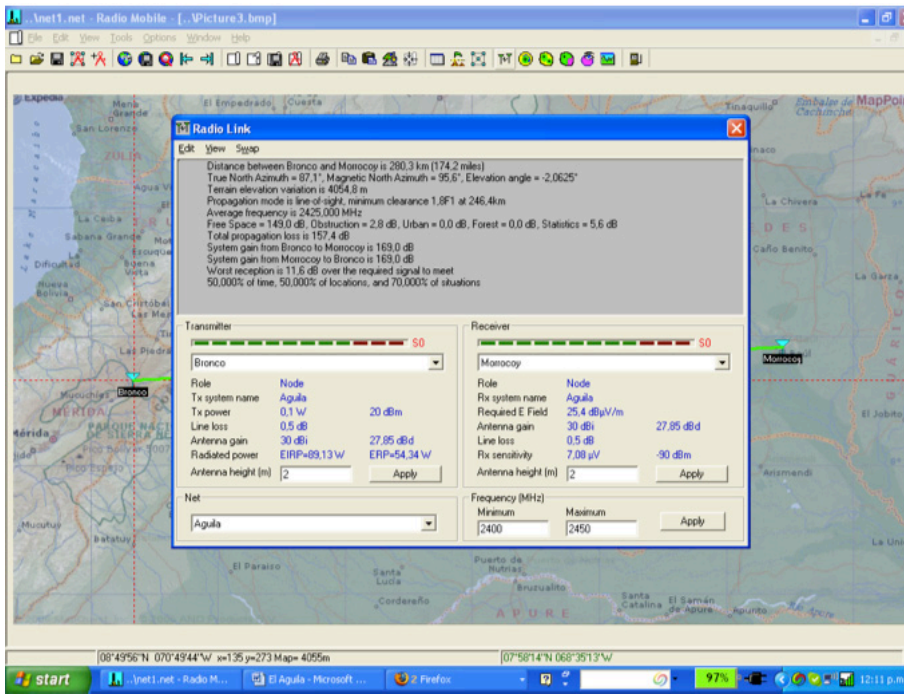


Figura 11.28: Detalhes de propagação do link de 280 km.

Antenas

Antenas de alto ganho para a banda de 2,4 GHz não estão disponíveis na Venezuela. Os custos de importação são consideráveis. Assim, decidimos por reciclar refletores parabólicos (anteriormente usados para serviços de satélites) e substituir sua alimentação de rádio por uma projetada para 2,4 GHz. Fizemos a prova de conceito com um prato de 80 cm. O ganho era muito baixo. Testamos então com um refletor de 2,4 m. Isto nos deu um alto ganho, apesar de algumas dificuldades no direcionamento do feixe de 3,5°. O offset (diferença angular) de 22,5° significa que o prato parece apontar para baixo quando está alinhado horizontalmente.

Vários testes foram realizados com o uso de várias cantennas (veja **Capítulo 4**) e uma Yagi de 12 dBi como alimentadoras. Apontamos a antena para uma estação base da universidade que estava localizada a 11 km, em uma montanha de 3.500 m de altitude. A localidade dos testes está a 2.000 m e, em função da diferença de alturas e da distância, o ângulo de elevação é de 8°. Por causa do offset da alimentação, apontamos o prato 14° para baixo, como pode ser visto na ilustração a seguir:

Figura 11.29: Refletor e seu alimentador, focando uma antena de 12 dBi, apontando 14° para baixo. A direção da elevação real resultante é de 8° para cima.

Conseguimos estabelecer o link com a estação base em Aguada, mas nossos esforços para medir o ganho da configuração, usando o Netstumbler, não tiveram sucesso. Havia muita flutuação nos valores medidos para a potência de recepção com o tráfego real.

Para uma medida significativa do ganho precisávamos de um gerador de sinal e de um analisador de espectro. Estes instrumentos também foram necessários para a ida a campo quando do alinhamento apropriado das antenas.

Enquanto esperávamos por este equipamento, procuramos pela antena a ser usada na outra ponta, assim como um sistema de direcionamento apropriado para o feixe estreito de rádio.

Em fevereiro de 2006, viajei para Trieste a fim de participar do evento anual de treinamento wireless, que freqüento desde 1996. Lá, falei sobre o projeto para meu colega Carlo Fonda, que ficou entusiasmado e ansioso para participar.

A colaboração entre a ***Escola Latino-Americana de Redes*** (***EsLaRed***) e o ***Centro Internacional Abdus Salam para a Física Teórica*** (***ICTP***) data de 1992, quando a primeira Escola de Redes aconteceu em Mérida, com o patrocínio do ICTP. Desde então, membros de ambas as instituições têm colaborado em várias atividades. Algumas delas incluem uma escola anual de treinamento em redes wireless (organizada pelo ICTP) e outra em redes de computadores (organizada pela EsLaRed) que acontecem em vários países da América Latina. Desta forma, não foi difícil de persuadir o Dr. Sandro Radicella, chefe do Laboratório de Aeronomia e Propagação de Rádio do ICTP, a

patrocinar a viagem de Carlo Fonda no início de abril para a Venezuela, a fim de que participasse do experimento.

Em meu retorno para casa, encontrei uma antena parabólica de grade, de 2,75 m, na casa de um vizinho. O Sr. Ismael Santos gentilmente emprestou sua antena para a experiência.

A **Figura 11.30** mostra a desmontagem do refletor de grade.

Figura 11.30: Carlo e Ermanno desmontando o prato de satélite fornecido pelo Sr. Ismael Santos.

Trocamos o alimentador de rádio pelo de 2,4 GHz e apontamos a antena para um gerador de sinais instalado no topo de uma escada a 30 m de distância. Com um analisador de espectro medimos o sinal máximo e localizamos o foco. Também localizamos o melhor posicionamento para o alimentador e o offset das antenas. Isto é mostrado na **Figura 11.31**:

Figura 11.31: Encontrando o foco das antenas com o alimentador de 2,4 GHz.

Também comparamos o sinal recebido com a saída de uma antena comercial de 24 dBi. Isto mostrou uma diferença de 8 dB, o que nos levou a concluir que o ganho geral de nossa antena era de cerca de 32 dBi. Claro que há alguma incerteza neste valor. Nós estávamos recebendo sinais refletidos, mas o valor estava de acordo com o calculado para as dimensões da antena.

Levantamento dos dados de El Baúl

Como estávamos satisfeitos com o funcionamento apropriado e o direcionamento de ambas as antenas, decidimos fazer o levantamento dos dados do outro lado do link, em El Baúl. Carlo Fonda, Gaia Fior e Ermanno Pietrosemoli chegaram à cidade no dia 8 de abril. No dia seguinte encontramos uma colina, ao sul da cidade, com duas torres de telecomunicações das duas operadoras de telefonia celular e outra que pertencia à prefeitura de El Baúl. A colina de Morrocoy está cerca de 75 m acima da área a seu redor e cerca de 125 m acima do nível do mar. Isto garante uma vista sem obstruções em direção a El Águila. Há uma estrada de terra até seu topo, uma grande vantagem para nós em função do peso da antena.

Realizando a experiência

Em 12 de abril, uma quarta-feira, Javier Triviño e Ermanno Pietrosemoli viajaram em direção a El Baúl, com a antena carregada em um caminhão com tração nas quatro rodas. Na manhã do dia 13 de abril instalamos a antena e a

apontamos a uma direção de 276°, dada a declinação de 8° e, desta forma, resultando no azimute real de 268°.

Ao mesmo tempo, a outra equipe (composta por Carlo Fonda e Gaya Fior do ICTP, com a ajuda de Franco Bellarosa, Lourdes Pietrosemoli e José Triviño) dirigiu-se até a área de Pico del Águila, onde o levantamento já havia sido feito, em um caminhão Bronco que carregava a antena de grade de 2,7 m.

Figura 11.32: Mapa do Pico del Águila e redondezas, com o caminhão Bronco.

Mau tempo é comum em uma altitude de 4.100 m acima do nível do mar. A equipe Águila terminou a instalação e o direcionamento da antena apenas um pouco antes da neblina se formar e começar a chover e nevar. A Figura 11.33 mostra a antena e a corda usada para o direcionamento do feixe de rádio de 3o.

A energia elétrica para o gerador de sinal foi fornecida pelo caminhão, com um inversor de 12 VDC para 120 VAC. Às 11 da manhã em El Baúl conseguimos observar um sinal de -82 dBm que estava de acordo com a freqüência de 2.450 MHz, com o uso do analisador de espectro. Para ter certeza de que havíamos encontrado a fonte correta de sinal, pedimos que Carlo o desligasse. Desta forma, o analisador passou a mostrar apenas ruídos, o que confirmou que o sinal que recebíamos era o originado a 280 km de distância.

Depois de ligar novamente o gerador de sinal, realizamos os ajustes finos de elevação e azimute em ambas as pontas. Quando estávamos certos de que conseguimos a máxima potência de recepção de sinal, Carlo removeu o gerador, substituindo-o pelo roteador wireless Linksys WRT54G configurado como access point. Javier substituiu o analisador da outra ponta pelo WRT54G configurado como cliente.

Figura 11.33: Direcionando a antena em El Águila.

Imediatamente começamos a receber os sinais de sincronização e conexão, mas não conseguíamos fazer com que os pacotes de ping atravessassem o link.

Isto era esperado, uma vez que a propagação de uma onda de rádio em um link de 200 km é de 1 ms. Isto faz com que se passem ao menos 2 ms para que o sinal de reconhecimento atinja o transmissor.

Felizmente, o firmware OpenWRT permite que seja ajustado o tempo de reconhecimento (ACK). Depois que Carlo o ajustou para 3 ordens de grandeza acima do padrão esperado pelo link Wi-Fi, começamos a receber os pacotes com um atraso de cerca de 5 ms.

Figura 11.34: Instalação da antena em El Baúl. A inclinação real é de 1° para cima, já que o offset da antena é de 22,5°.

Começamos a transferir vários arquivos PDF entre os laptops de Carlo e Javier. O resultado é exibido na **Figura 11.35**.

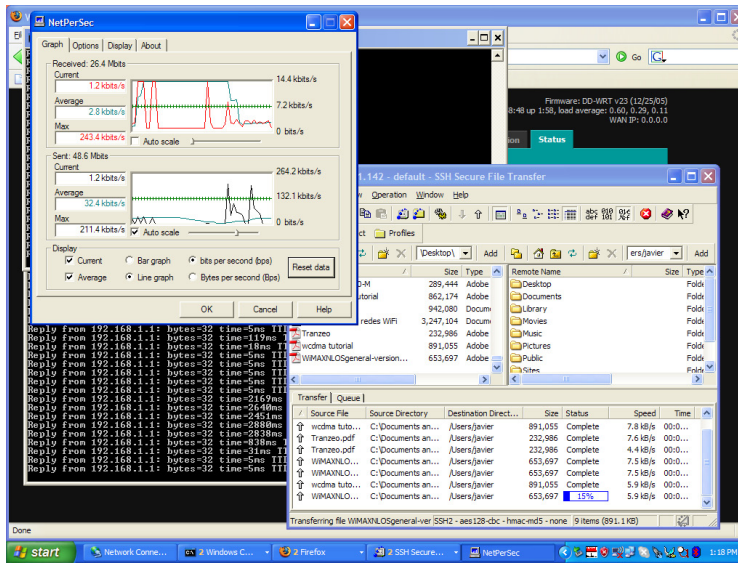


Figura 11.35: Captura de tela do laptop de Javier, mostrando os detalhes da transmissão de arquivos PDF do laptop de Carlo a 280 km de distância, usando dois roteadores WRT54G sem amplificadores.

Note o tempo de ping de alguns milisegundos.

Figura 11.36: Javier Triviño (à direita) e Ermanno Pietrosemoli transmitindo a partir da antena de El Baúl.

Figura 11.37: Carlo Fonda na instalação de Águila

Mérida, Venezuela, 17 de abril de 2006

Um ano depois de realizar esta experiência, conseguimos o tempo e os recursos para repeti-la. Usamos duas antenas comerciais de 30 dBi e um par de roteadores wireless modificados pelo grupo TIER, liderado pelo Dr. Eric Brewer da Universidade de Berkeley.

O propósito da modificação do padrão Wi-Fi MAC é para permitir seu uso em aplicações de longa distância, substituindo controles de acesso CSMA por TDMA. Este último aplica-se melhor para links ponto-a-ponto de longa distância, já que não requer a recepção de ACKs. Isto elimina a necessidade de espera por uma viagem de ida e volta de 2 ms em um link de 300 km.

Em 28 de abril de 2007, a equipe formada por Javier Triviño, José Torres e Francisco Torres instalou uma das antenas em El Águila. A outra equipe, formada por Leonardo González V., Leonardo González G., Alejandro González e Ermanno Pietrosemoli instalou a outra antena em El Baúl.

Um link sólido foi rapidamente estabelecido com o uso dos roteadores WRT54G. Isto permitiu a transmissão de vídeo com uma velocidade medida de 65 kbps. Com os roteadores TDMA, a velocidade medida foi de 3Mbps em cada direção. Isto resultou em um total de 6 Mbps, de acordo com o previsto nas simulações executadas em Berkeley.

Podemos melhorar?

Entusiasmados com estes resultados, que pavimentaram o caminho para links de banda larga de longa distância realmente baratos, a segunda equipe dirigiu-se para uma outra localidade previamente identificada a 382 km de El Águila, em um local chamado Platillón. Platillón está a 1.500 m acima do nível do mar e não há obstrução na primeira zona Fresnel em direção a El Águila (localizada 4.200 m acima do nível do mar). O caminho proposto é mostrado na **Figura 11.38**:

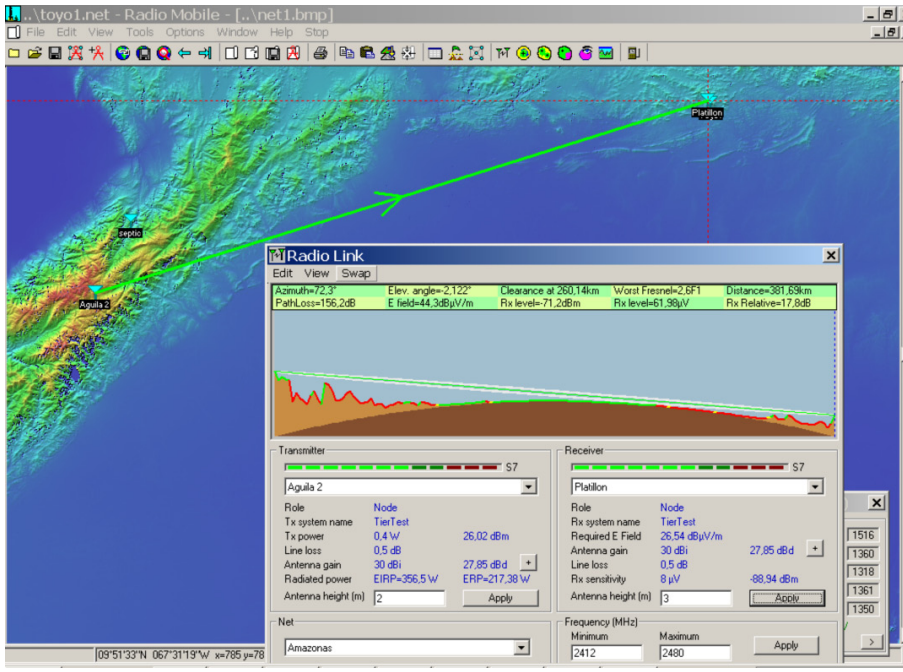


Figura 11.38: Mapa e perfil do caminho de 380 km.

Como antes, o link foi rapidamente estabelecido com o equipamento Linksys e os roteadores fornecidos pelo TIER. O Linksys apresentou uma perda de pacotes de aproximadamente 1%, com o tempo de transmissão e recepção (ida e volta) de 12 ms. O equipamento TIER não apresentou perda de pacotes e o tempo de propagação foi menor que 1 ms. Isto possibilitou a transmissão de vídeo, mas o link não era estável. Percebemos flutuações consideráveis do sinal que interrompiam freqüentemente a comunicação.

Apesar disto, quando o sinal recebido estava em cerca de -78 dBm, a velocidade medida era de 6 Mbps em ambas as direções com os roteadores TIER implementando TDMA.

Figura 11.39: A equipe em El Águila, a partir da esquerda: José Torres, Javier Triviño e Francisco Torres.

Mesmo que testes adicionais devam ser feitos para garantir os limites de uma velocidade estável, temos a certeza de que a tecnologia Wi-Fi tem grande potencial para a comunicação de banda larga em longa distância. Isto atende particularmente bem regiões rurais, onde o espectro ainda não está super populado e a interferência não é um problema, desde que exista uma boa linha de visão para o sinal de rádio.

Agradecimentos

Gostaríamos de expressar nossos agradecimentos ao Sr. Ismael Santos, que emprestou sua antena para a instalação no El Águila, e ao Engenheiro Andrés Pietrosemoli por fornecer as juntas especiais usadas na instalação e transporte das antenas.

Também queremos agradecer o Centro Internacional Abdus Salam de Física Teórica, que patrocinou a viagem do Carlo Fonda da Itália até a Venezuela.

Figura 11.40: A equipe em Platillon, a partir da esquerda: Leonardo González V., Leonardo González G., Ermanno Pietrosemoli e Alejandro González.

O experimento de 2006 foi executado por Ermanno Pietrosemoli, Javier Triviño da EsLaRed, Carlo Fonda e Gaya Fior do ICTP, com a ajuda de Franco Bellarosa, Lourdes Pietrosemoli, e José Triviño.

Nos experimentos de 2007, o Dr. Eric Brewer da Universidade de Berkeley University forneceu os roteadores com o MAC modificado para longa distância e a ajuda entusiástica de seu colaborador, Sonesh Surana. A RedULA, CPTM, a Diretoria de Serviços da ULA, Universidad de los Andes e a Fundacite de Mérida também contribuíram para estes testes.

Este trabalho foi financiado pelo ICA-IDRC.

Referências

- Fundación Escuela Latinoamericana de Redes, *http://www.eslared.org.ve/*
- Centro Internacional Abdus Salam de Física Teórica, *http://wireless.ictp.it/*
- OpenWRT Open Source firmware para Linksys, *http://openwrt.org/*
- Fundacite Mérida, *http://www.funmrd.gov.ve/*

—Ermanno Pietrosemoli

Apêndices

Apêndice A: Recursos

Recomendamos estes recursos para que se possa aprender mais sobre vários aspectos de redes sem fio. Para mais links e recursos, acesse nosso website: *http://wndw.net/*.

Antenas e projetos de antena

- Artigos técnicos práticos sobre projetos de antena e propagação de ondas de rádio, *http://www.cushcraft.com/comm/support/technical-papers.htm*
- Projetos de antenas livres, *http://www.freeantennas.com/*
- Hyperlink Tech, *http://hyperlinktech.com/*
- Pasadena Networks LLC, *http://www.wlanparts.com/*
- SuperPass, *http://www.superpass.com/*
- Arquivos de código não oficiais do ***NEC2***, *http://www.nec2.org/*
- Website não oficial da ferramenta para modelagem de rádio ***NEC2***, *http://www.nittany-scientific.com/nec/*
- Projetos de pratos parabólicos para USB Wi-Fi, *http://www.usbwifi.orcon.net.nz/*

Ferramentas para a análise de problemas de rede

- Ferramenta de medida de velocidade ***Bing***, *http://fgouget.free.fr/bing/index-en.shtml*
- Pacote de monitoramento de redes ***Cacti***, *http://www.cacti.net/*
- Ferramenta de testes de velocidade e largura de banda DSL Reports, *http://www.dslreports.com/stest*

- Ferramenta de análise de espectro ***EaKiu***, *http://www.cookwareinc.com/EaKiu/*
- Monitor de tráfego de rede ***EtherApe***, *http://etherape.sourceforge.net/*
- Coletor NetFlow de código aberto ***Flowc***, *http://netacad.kiev.ua/flowc/*
- Ferramenta para testes de desempenho de redes ***Iperf***, *http://dast.nlanr.net/Projects/Iperf/*
- Ferramenta de monitoramento de redes ***IPTraf***, *http://iptraf.seul.org/*
- Ferramenta para monitoramento de redes e geração de gráficos ***MRTG***, *http://people.ee.ethz.ch/~oetiker/webtools/mrtg/*
- Ferramenta de diagnóstico de redes ***TraceRoute***, *http://www.bitwizard.nl/mtr/*
- Ferramenta de notificação de eventos e monitoramento de redes ***Nagios***, *http://www.nagios.org/*
- ***NetFlow***, o protocolo Cisco para a coleta de informações de tráfego IP, *http://en.wikipedia.org/wiki/Netflow*
- Utilitário de segurança de rede para a busca de padrões em fluxos de dados ***ngrep***, *http://ngrep.sourceforge.net/*
- Tutoriais e guias de implementação de monitoramento de redes, *http://wiki.debian.org/Network_Monitoring*
- Ferramenta de monitoramento de redes ***Ntop***, *http://www.ntop.org/*
- Utilitário gráfico ***RRDtool***, *http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/*
- Monitor de latência de rede e perda de pacotes ***SmokePing***, *http://people.ee.ethz.ch/~oetiker/webtools/smokeping/*
- Ferramentas de análise de rede ***SoftPerfect***, *http://www.softperfect.com/*
- Tutorial para a implantação de um proxy transparente baseado no ***Squid***, *http://tldp.org/HOWTO/TransparentProxy.html*
- Ferramenta de teste de desempenho de rede ***ttcp***, *http://ftp.arl.mil/ftp/pub/ttcp/*
- Analisador de protocolo de rede ***Wireshark***, *http://www.wireshark.org/*

Segurança

- Informações e ferramentas para contornar o proxy http ***AntiProxy***, *http://www.antiproxy.com/*
- Ferramentas anti-spyware, *http://www.spychecker.com/*

- Utilitário de monitoramento de rede ***Driftnet***, *http://www.ex-parrot.com/~chris/driftnet/*
- Utilitário de monitoramento de rede ***Etherpeg***, *http://www.etherpeg.org/*
- Introdução ao ***OpenVPN***, *http://www.linuxjournal.com/article/7949*
- Ferramenta de remoção de spyware ***Lavasoft Ad-Aware***, *http://www.lavasoft.de/*
- Software de administração e segurança para o Linux, *http://www.linux.org/apps/all/Networking/Security_/_Admin.html*
- Ferramenta para túneis e shell seguro ***OpenSSH***, *http://openssh.org/*
- Guia de configuração de túneis criptografados ***OpenVPN***, *http://openvpn.net/howto.html*
- Proxy para filtragem web ***Privoxy***, *http://www.privoxy.org/*
- Cliente ***PuTTY*** SSH para Windows, *http://www.putty.nl/*
- Analisador de log ***Sawmill***, *http://www.sawmill.net/*
- Segurança do algoritmo WEP, *http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html*
- Wrapper universal para SSL ***Stunnel***, *http://www.stunnel.org/*
- Roteador cebola ***Tor***, *http://www.torproject.org/*
- Fraquezas no algoritmo de programação de chaves do RC4, *http://www.crypto.com/papers/others/rc4_ksaproc.ps*
- Cliente Windows SCP, *http://winscp.net/*
- *Your 802.11 Wireless Network has No Clothes* (Sua rede wireless 802.11 está pelada), *http://www.cs.umd.edu/~waa/wireless.pdf*
- Firewall pessoal ***ZoneAlarm*** para Windows, *http://www.zonelabs.com/*

Otimização do tamanho de banda

- Hierarquias de cache com Squid, *http://squid-docs.sourceforge.net/latest/html/c2075.html*
- Servidor DHCP e caching DNS com dnsmasq, *http://www.thekelleys.org.uk/dnsmasq/doc.html*
- *Enhancing International World Wide Web Access in Mozambique Through the Use of Mirroring and Caching Proxies* (Melhorando o acesso à Internet em Moçambique através do uso de espelhamento e caching proxies), *http://www.isoc.org/inet97/ans97/cloet.htm*
- Utilitário de distribuição de arquivos ***Fluff***, *http://www.bristol.ac.uk/fluff/*
- Tutorial de controle de tráfego e roteamento avançado no Linux, *http://lartc.org/*

- ***Microsoft Internet Security and Acceleration Server***, *http://www.microsoft.com/isaserver/*
- Site de recursos sobre o ***Microsoft ISA Server Firewall and Cache***, *http://www.isaserver.org/*
- Otimizando a largura de banda da Internet em países em desenvolvimento, *http://www.inasp.info/pubs/bandwidth/index.html*
- *Pittsburgh Supercomputing Center's guide to Enabling High Performance Data Transfers* (Guia do centro de supercomputação de Pittsburgh para a habilitação de tranferência de dados de alto desempenho), *http://www.psc.edu/networking/perf_tune.html*
- Blog Planet Malaysia sobre gestão de largura de banda, *http://planetmy.com/blog/?p=148*
- RFC 3135: *Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations* (Proxies para a melhoria de desempenho destinados a minimizar degradações relativas ao link), *http://www.ietf.org/rfc/rfc3135*
- ***Squid*** web proxy cache, *http://squid-cache.org/*

Redes mesh

- Software para redes sem fio da comunidade Champaign-Urbana, *http://cuwireless.net/download*
- ***Firmware*** mesh Freifunk OLSR para o Linksys WRT54G, *http://www.freifunk.net/wiki/FreifunkFirmware*
- Projeto ***Roofnet*** do MIT, *http://pdos.csail.mit.edu/roofnet/doku.php*
- Serviço (daemon) de redes mesh OLSR, *http://www.olsr.org/*
- Visualizador de topologias OLSR em tempo real, *http://meshcube.org/nylon/utils/olsr-topology-view.pl*
- Roteador mesh AirJialdi, *http://drupal.airjaldi.com/node/9*

Sistemas operacionais e drivers para Wireless

- ***HostAP***, driver wireless para a arquitetura Prism 2.5, *http://hostap.epitest.fi/*
- ***m0n0wall***, sistema operacional para roteadores sem fio, *http://m0n0.ch/wall/*
- ***MadWiFi***, driver wireless para a arquitetura Atheros, *http://madwifi.org/*
- ***Metrix Pyramid***, sistema operacional para roteadores sem fio, *http://pyramid.metrix.net/*

- ***OpenWRT***, sistema operacional para access points Linksys, *http://openwrt.org/*
- ***Tomato***, sistema operacional para access points Linksys, *http://www.polarcloud.com/tomato*

Ferramentas para redes sem fio

- Portal cativo ***Chillispot***, *http://www.chillispot.info/*
- *Interactive Wireless Network Design Analysis Utilities* (Utilitários interativos para análise de projeto de redes sem fio), *http://www.qsl.net/n9zia/wireless/page09.html*
- ***KisMAC***, monitor wireless para Mac OS X, *http://kismac.macpirate.ch/*
- ***Kismet***, ferramenta de monitoramento para redes wireless, *http://www.kismetwireless.net/*
- ***MacStumbler***, ferramenta de detecção de redes sem fio para Mac OS X, *http://www.macstumbler.com/*
- ***NetStumbler***, ferramenta de detecção de redes sem fio para Windows e Pocket PC, *http://www.netstumbler.com/*
- Portal cativo ***NoCatSplash***, *http://nocat.net/download/NoCatSplash/*
- Sistema pré-pago de bilhetagem ***PHPMyPrePaid***, *http://sourceforge.net/projects/phpmyprepaid/*
- Ferramenta de modelagem de desempenho de radio ***Radio Mobile***, *http://www.cplus.org/rmw/*
- Ferramentas para o cálculo de link wireless Terabeam, *http://www.terabeam.com/support/calculations/index.php*
- ***Wellenreiter***, ferramenta de detecção de redes wireless para Linux, *http://www.wellenreiter.net/*
- Portal cativo ***WiFiDog***, *http://www.wifidog.org/*
- Ferramenta de análise de link de redes wireless através de GBPRR, *http://my.athenet.net/~multiplx/cgi-bin/wireless.main.cgi*

Informações gerais relacionadas com redes sem fio

- Concurso DefCon de wireless de longa distância sem amplificação, *http://www.wifi-shootout.com/*
- Projetos caseiros de hardware wireless, *http://www.w1ghz.org/*
- Informações sobre access point wireless Linksys, *http://linksysinfo.org/*
- Guia de recursos do Linksys WRT54G, *http://seattlewireless.net/index.cgi/LinksysWrt54g*

- Comunidade sobre redes sem fio NoCat, *http://nocat.net/*
- Hardware ótico para a comunicação de dados Ronja, *http://ronja.twibright.com/*
- Comunidade sobre redes sem fio SeattleWireless, *http://seattlewireless.net/*
- Página de comparação de hardware do SeattleWireless, *http://www.seattlewireless.net/HardwareComparison*
- Calculadora de Power Over Ethernet (PoE) do Stephen Foskett, *http://www.gweep.net/~sfoskett/tech/poecalc.html*

Serviços de rede

- Access Kenya ISP, *http://www.accesskenya.com/*
- Broadband Access Ltd., operadora de banda larga wireless, *http://www.blue.co.ke/*
- Virtual IT serviços de terceirização, *http://www.virtualit.biz/*
- wire.less.dk consultoria e serviços, *http://wire.less.dk/*

Educação e treinamento

- Projetos de conectividade wireless da Association for Progressive Communications, *http://www.apc.org/wireless/*
- International Network for the Availability of Scientific Publications (Rede internacional para a disponibilização de publicações científicas), *http://www.inasp.info/*
- Universidade Makere, Uganda, *http://www.makerere.ac.ug/*
- Radio Communications Unit of the Abdus Salam International Center for Theoretical Physics (Unidade de comunicações de rádio do Centro Internacional Abdus Salam para a Física teórica), *http://wireless.ictp.trieste.it/*
- World Summits on Free Information Infrastructures (Encontros mundiais sobre infra-estruturas para a livre informação), *http://www.wsfii.org/*

Links diversos

- ***Cygwin***, ambiente do tipo Linux para Windows, *http://www.cygwin.com/*
- ***Graphvis***, ferramenta de visualização gráfica, *http://www.graphviz.org/*
- Simulador de largura de banda ICTP, *http://wireless.ictp.trieste.it/simulator/*
- ***ImageMagick***, ferramentas e bibliotecas para a manipulação de imagens, *http://www.imagemagick.org/*

- NodeDB, base de dados de mapas war driving, *http://www.nodedb.com/*
- Base de dados de relays abertos, *http://www.ordb.org/*
- ***Partition Image***, utilitário de disco para Linux, *http://www.partimage.org/*
- RFC 1918: *Address Allocation for Private Internets* (Alocação de endereços para Internets privadas), *http://www.ietf.org/rfc/rfc1918*
- Conceitos de redes Linux do Rusty Russell, *http://www.netfilter.org/documentation/HOWTO/ networking-concepts-HOWTO.html*
- Ubuntu Linux, *http://www.ubuntu.com/*
- Introdução ao VoIP-4D, *http://www.it46.se/voip4d/voip4d.php*
- ***wget***, utilitário web para Windows, *http://xoomer.virgilio.it/hherold/*
- WiFiMaps, bases de dados de mapas war driving, *http://www.wifimaps.com/*
- WiSpy, ferramenta de análise de espectro, *http://www.metageek.net/*

Livros

- *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

Apêndice B: Alocações de Canal

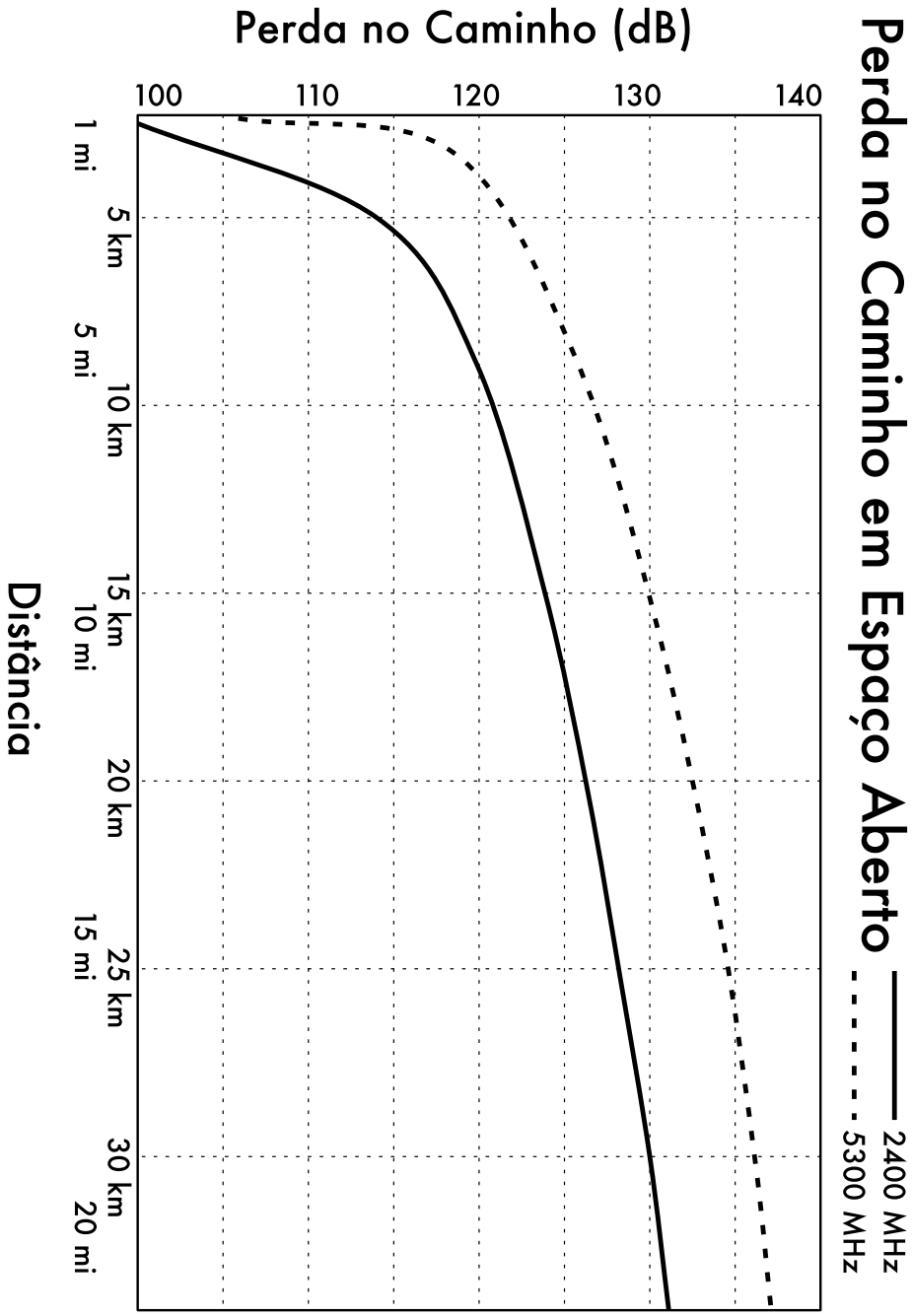
As seguintes tabelas listam os números dos canais e freqüências centrais usadas nos padrões 802.11a e 802.11b/g. Note que, mesmo que estas freqüências sejam das bandas livres ISM e U-NII, nem todos os canais estão disponíveis em todos os países. Muitas regiões impõem restrições na potência de saída para o uso interno e externo no uso de alguns canais. Estas regras mudam rapidamente, desta forma verifique a sua legislação local antes de transmitir.

Note que estas tabelas mostram a freqüência central para cada canal. Os canais têm 22MHz de largura no 802.11b/g, e 20MHz no 802.11a.

802.11b / g			
Canal #	Freqüência Central (GHz)	Canal #	Freqüência 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 #	Freqüência 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

Apêndice C: Perdas no Caminho



Apêndice D: Tamanhos de Cabo

Bitola do fio, diâmetro, capacidade de corrente e resistência à 20°C. Estes valores podem variar de um cabo a outro. Na dúvida, consulte as especificações do fabricante.

Bitola AWG	Diâmetro (mm)	Ohms / Metro	Corrente máxima em Amperes
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

Apêndice E: Dimensionamento Solar

Utilize estas tabelas para coletar os dados necessários para estimar o tamanho requerido de seu sistema de energia solar.

Dados Gerais

Nome da Localidade	
Latitude da Localidade (°)	

Dados de Irradiação

$G_{dm}(0)$, en kWh / m² por dia

Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez
Mês com a pior irradiação											

Confiabilidade e Voltagem do Sistema Operacional

Dias de Autonomia (N)	
Voltagem Nominal (V_{NEquip})	

Características dos Componentes

Painéis Solares	
Voltagem na Potência Máxima(V_{pmax})	
Corrente na Potência Máxima (I_{pmax})	
Tipo de Painel/Modelo e Potência (W_p)	

Baterias	
Capacidade Nominal em 100 H(C_{NBat})	
Voltagem Nomina (V_{NBat})	
Profundidade Máxima de Descarga(DoD_{MAX}) ou Capacidade Utilizável(C_{UBat})	

Regulador de Tensão	
Voltagem Nominal(V_{NReg})	
Corrente Máxima (I_{maxReg})	

Inversor DC/AC (se necessário)	
Voltagem Nominal (V_{NConv})	
Potência Instantânea (P_{IConv})	
Desempenho em 70% de carga	

Cargas

Estimativa de Energia Consumida pelas Cargas (DC)				
			Mês de Maior Consumo	
Descrição	Número de Unidades	x Potência Nominal	x Uso Horas / Dia	= Energia (Wh / dia)
			E_{TOTAL} DC	

Estimativa de Energia Consumida pelas Cargas (AC)				
			Mês de Maior Consumo	
Descrição	Número de Unidades	x Potência Nominal	x Uso Horas/Dia	= Energia (Wh/Dia)
			E_{TOTAL} AC (antes da conversão)	
			E_{TOTAL} AC (depois da conversão) = E_{TOTAL} AC / 70%	

Encontrando o Pior Mês

Nome da Localidade	
Latitude da Localidade (°)	

Voltagem Nominal da Instalação V_N												
(Mes)	J	F	M	A	M	J	J	A	S	O	N	D
Inclinação ß												
G_{dm} (ß) (kWh/m^2 × dia)												
E_{TOTAL} (DC) (Wh/dia)												
E_{TOTAL} (AC) (Wh/dia)												
E_{TOTAL} (AC + DC)=												
I_m (A) = E_{TOTAL} (Wh/dia) × 1kW/m^2/ (G_{dm}(ß) x V_N)												

Sumário do Pior Mês	
Pior Mês	
I_m (A)	
I_{mMAX} (A) = 1.21 x I_m	
E_{TOTAL} (AC + DC)	

Cálculos finais

Painéis		
Painéis em Série (N_{PS})	$N_{PS} = V_N / V_{Pmax} =$	
Painéis em Paralelo (N_{PP})	$N_{PP} = I_{mMAX} / I_{Pmax} =$	
Número Total de Painéis	$N_{TOT} = N_{PS} \times N_{PP} =$	

Baterias		
Capacidade Necessária (C_{NEC})	E_{TOTAL}(PIOR MÊS) / $V_N \times N$	
Capacidade Nominal (C_{NOM})	C_{NEC} / DoD_{MAX}	
Número de Baterias em Série (N_{BS})	V_N / V_{NBAT}	

Cabos			
	Painéis para Baterias	Baterias para Conversor	Linha Principal
Queda de Voltagem (V_a - V_b)			
Espessura (Seção) $r \times L \times I_{mMAX} / (V_a - V_b)$			

Para o cálculo da espessura do cabo, r = 0,01286 λ mm²/m (para cobre) e L é o tamanho em metros.

Glossário

0–9

802.11. Família de protocolos para a comunicação wireless, usada principalmente para redes locais. Suas variantes populares incluem o 802.11b, 802.11g e 802.11a. Veja também: ***Wi-Fi***.

A

AC. Veja: ***Corrente Alternada***.

access point (***AP***). Dispositivo que cria uma rede wireless a partir de uma conexão a uma rede cabeada Ethernet. Veja também: ***CPE***, ***modo mestre***.

access points desonestos. Um ponto de acesso não autorizado, incorretamente instalado por usuários legítimos ou por alguma pessoa maliciosa que pretende coletar dados ou danificar a rede.

acumulador. Um outro nome para ***bateria***.

Address Resolution Protocol (***ARP – Protocolo de Resolução de Endereço***). Um protocolo largamente utilizado em redes Ethernet para a tradução de endereços IP em endereços MAC.

alvo (***target***). No netfilter, a ação a ser tomada quando um pacote corresponde a uma determinada regra. Alguns alvos possíveis do netfilter incluem ***ACCEPT*** (***aceita***), ***DROP*** (***descarta***), ***LOG*** (***registra***) e ***REJECT*** (***rejeita***).

amortização. Técnica contábil usada para a gestão do custo de substituição e obsolescência de equipamentos com o passar do tempo.

amplificador. Dispositivo usado para aumentar a potência de transmissão de um dispositivo wireless.

amplitude. A distância do centro de uma onda ao extremo de um de seus picos.

analisador de espectro. Um dispositivo que fornece a visualização de um espectro eletromagnético. Ver também: ***Wi-Spy***.

analisador de protocolo. Programa de diagnóstico utilizado para a observação e desmontagem de pacotes de rede. Analisadores de protocolo fornecem o maior detalhe possível de cada pacote, individualmente.

anonimidade. Em redes de computadores, a comunicação que não pode ser ligada diretamente a um único indivíduo é chamada de anônima. A relação entre a anonimidade e a responsabilidade em comunicações é uma grande discussão e leis sobre a anonimidade em comunicações variam muito ao redor do mundo. Veja também: ***autenticado***.

antena dipolo. A forma mais simples de uma ***antena omnidirecional***.

antena direcional. Uma antena que irradia fortemente em uma direção particular. Exemplos de antenas direcionais incluem a yagi, prato parabólico e antenas de guia de onda. Veja também: ***antena omnidirecional***, ***antena setorial***.

antena isotrópica. Uma antena hipotética que distribui igualmente a potência em

todas as direções, que pode ser aproximada a um dipolo.

antena omnidirecional. Uma antena que irradia quase igualmente em todas as direções do plano horizontal. Veja também: ***antena direcional***, ***antena setorial***.

antena setorial. Uma antena que irradia primariamente em uma área específica. O feixe pode ter uma largura tão grande quanto 180 graus ou tão estreita quanto 60 graus. Veja também: ***antena direcional***, ***antena omnidirecional***.

AP. Veja: ***Access Point***.

Argus. Veja: ***Audit Record Generation and Utilization System***.

ARP. Veja: ***Protocolo de Resolução de Endereços***.

associado. Um rádio 802.11 está associado a um ponto de acesso quando está pronto para comunicar-se com a rede. Isto significa estar sintonizado ao canal apropriado, ao alcance do AP, usando o SSID correto assim como os demais parâmetros de autenticação.

at. Uma função do Unix que permite a execução temporizada de programas. Veja também: ***cron***

atenuação. A redução da potência de rádio disponível pela sua absorção através de um caminho, como a causada por árvores, paredes, construções ou outros objetos. Veja também: ***perda no espaço livre***, ***espalhamento***.

autenticado. Um usuário de rede que provou sua identidade a um serviço ou dispositivo (como um access point) sem nenhuma sombra de dúvida, usualmente com o auxílio de algum tipo de criptografia. Veja também: ***anonimidade***.

Autoridade Certificadora. Uma entidade confiável que emite chaves criptográficas. Veja também: ***Infra-estrutura de chaves públicas***, ***SSL***.

Autoridades Regionais de Registro de Internet (***RIR – Regional Internet Registrars***). Os quatro bilhões de endereços IP disponíveis são administrados pela IANA. O espaço foi dividido em grandes sub-redes, delegadas a cada uma das cinco Autoridades Regionais de Registro, cada uma atendendo uma larga área geográfica regional.

azimute. O ângulo que mede o desvio em relação ao sul no hemisfério norte e em relação ao norte no hemisfério sul. Veja também: ***inclinação***.

B

banda ISM. ISM é a abreviatura de Industrial, Científica (*Scientific*) e Médica. A banda ISM é um conjunto de freqüências de rádio reservadas para o uso sem licença.

bateria. Dispositivo utilizado para o armazenamento de energia em um sistema fotovoltaico. Veja também: ***painel solar***, ***regulador***, ***carga***, ***conversor***, ***inversor***.

baterias de chumbo-ácido. Baterias que consistem em dois eletrodos de chumbo submersos em uma solução eletrolítica de água e ácido sulfúrico. Veja também: ***baterias estacionárias***.

bateria de chumbo-ácido regulada por válvula (***VRLA*** - ***valve regulated lead acid battery***). Veja: ***bateria de chumbo-ácido***.

baterias estacionárias. Baterias projetadas para a montagem em um local fixo, em cenários onde o consumo de potência é mais ou menos irregular. Baterias estacionárias podem acomodar ciclos de descarga profundos, mas não são projetadas para produzir correntes altas por curtos períodos de tempo. Veja também: ***baterias de chumbo-ácido***.

baterias de tração. Veja: ***baterias de chumbo-ácido***.

baterias recombinantes. Veja: ***baterias de chumbo-ácido***.

benchmarking. Teste de desempenho máximo de um serviço ou dispositivo. O benchmarking de uma conexão de rede normalmente é feito com a inundação de tráfego no link e a medida da velocidade real na transmissão e recepção.

BGAN. Veja: ***Broadband Global Access Network***.

bom conhecido. No diagnóstico de problemas, um “bom conhecido” é qualquer componente que possa ser substituído para a verificação de que seu equivalente está em boas condições de funcionamento.

borda. Ou ***limite***, é o local onde a rede de uma organização encontra-se com outra. Bordas são definidas pela localização do

roteador externo, que freqüentemente atua também como ***firewall***.

bridge. Um dispositivo de rede que conecta duas redes na mesma camada de comunicação de dados. As bridges não fazem o roteamento dos pacotes na camada de rede. Elas simplesmente repetem os pacotes entre duas redes em conexão local. Veja também: ***roteador*** e ***firewall de bridge transparente***.

bridge-utils. Um pacote de software para Linux que é necessário para a criação de bridges Ethernet 802.1d. *http://bridge.sourceforge.net/*

Broadband Global Access Network (***BGAN***). Um dos vários padrões usados para o acesso à Internet via satélite. Veja também: ***Digital Video Broadcast*** (***DVB-S***) e ***Very Small Aperture Terminal*** (***VSAT***).

C

cache transparente. Método de implementação de um web cache para uma toda uma instalação que não exige a configuração dos navegadores. As solicitações web são transparentemente redirecionadas ao cache, que faz a solicitação no lugar do cliente. Veja também: ***cache web para todo o site***, ***Squid***.

cache web para todo o site (***site-wide web cache***). Mesmo que todos os navegadores modernos forneçam a facilidade de armazenamento local de dados, grandes organizações podem aumentar a eficiência da rede com um cache web para todo a sua instalação, por exemplo com o Squid. Um cache web irá manter a cópia de todas as solicitações de páginas feitas dentro da organização, atendendo os pedidos subseqüentes com as páginas armazenadas localmente. Veja também: ***Squid***.

caching de DNS. Ao instalar um servidor DNS em sua rede local, as solicitações de DNS para toda a rede são armazenadas localmente, melhorando o tempo de resposta. Esta técnica é chamada de caching de DNS.

Cacti (*http://www.cacti.net/*). Uma ferramenta popular, baseada na web, para monitoramento, escrita em PHP.

camada de aplicação. A camada mais acima nos modelos de rede OSI e TCP/IP.

camada de apresentação. A sexta camada do modelo de rede OSI. Esta camada lida com a representação de dados, como a codificação MIME ou compressão de dados.

camada de conexão de dados. A segunda camada nos modelos de rede OSI e TCP/IP. As comunicações nesta camada acontecem diretamente entre os nós. Em redes Ethernet, ela é também chamada de camada MAC.

camada de Controle de Acesso ao Meio. Veja: ***camada de conexão de dados***.

camada de Internet. Veja: ***camada de rede***.

camada de sessão. A quinta camada do modelo OSI, a camada de sessão gerencia as conexões lógicas entre as aplicações.

camada de transporte. A terceira camada de um modelo de rede OSI e TCP/IP, responsável por fornecer um método para que se alcance um serviço em particular em um dado nó de rede. Exemplos de protocolos que operam nesta camada são o ***TCP*** e o ***UDP***.

camada física. A mais baixa camada nos modelos de rede OSI e TCP/IP. A camada física é o meio usado para a comunicação, como fios de cobre, fibra ótica ou ondas de rádio.

camada MAC. Veja: ***camada de conexão de dados***.

canal. Um intervalo bem definido de freqüências usado para a comunicação. Canais 802.11 utilizam 22 MHz de largura de banda separados por 5 MHz. Veja também: ***Apêndice B***.

camada de rede. Também chamada de camada de Internet. É a terceira camada dos modelos OSI e TCP/IP, onde opera o IP e acontece o roteamento de Internet.

cancelamento. Caso específico de interferência por ***multicaminhos*** onde o sinal recebido na antena é anulado pela ***interferência destrutiva*** dos sinais recebidos.

capacidade. A máxima quantidade teórica de tráfego que pode ser fornecida por uma linha de comunicação. Freqüentemente usada em substituição ao termo ***largura de banda***.

capacidade de canal. A máxima quantidade de informação que pode ser enviada utilizando uma determinada largura de banda. Veja também: ***largura de banda***, ***throughput***, ***taxa de transmissão de dados***.

Capacidade Nominal (***C_N***). A quantidade máxima de energia que pode ser extraída de uma bateria completamente carregada. É expressa em Ampere-hora (Ah) ou Watt-hora (Wh).

Capacidade Útil (***C_u***). A capacidade utilizável de uma bateria, que é igual ao produto da ***Capacidade Nomina***l e a ***Máxima Profundidade de Descarga***.

carga. Equipamento em um sistema fotovoltaico que consome energia. Veja também: ***bateria***, ***painel solar***, ***regulador***, ***conversor***, ***inversor***.

célula. Painéis solares são compostos de várias células individuais, eletricamente conectadas para fornecer um determinado valor de corrente e tensão. Baterias também são formadas por células individuais conectadas em série, cada uma contribuindo com cerca de 2 volts para a tensão total.

chumbo. Uma peça de metal pesada, enterrada no solo para melhorar a conexão de aterramento.

CIDR. Veja: ***Classless Inter-Domain Routing***.

Classless Inter-Domain Routing (roteamento sem classe inter-domínio). O CIDR foi desenvolvido para melhorar a eficiência do roteamento na Internet, permitindo a agregação de rotas e máscaras de rede de tamanho arbitrário. O CIDR substitui o antigo esquema de endereços baseado em classes. Veja ***também***: ***Redes classe A, B e C***.

cliente. Um cartão de rádio 802.11 em modo gerenciado. Clientes wireless podem juntar-se a uma rede criada por um access point, mudando automaticamente seu canal para que corresponda ao do AP. Veja também: ***access point***, ***mesh***.

clientes âncora. Assinantes de serviços que podem ser considerados confiáveis e de baixo risco.

coax. Um cabo coaxial cilíndrico com um fio central envolvido em um isolante, um condutor externo e um revestimento resistente. Cabos de antena são tipicamente coaxiais. Coax é a abreviatura de "*of common axis*" (de eixo comum).

colisão. Em uma rede Ethernet, uma colisão ocorre quando dois dispositivos conectados ao mesmo segmento físico tentam transmitir ao mesmo tempo. Na detecção de uma colisão, os dispositivos atrasam a retransmissão por um período breve, selecionado aleatoriamente.

comprimento de onda. A distância medida de um ponto da onda ao próximo ponto equivalente da parte seguinte, por exemplo, entre um pico e o seguinte. Também conhecido por ***lambda*** (λ).

condição de correspondência. No netfilter, uma condição de correspondência (*match condition*) especifica o critério que determina o destino final para um determinado pacote. Os pacotes podem ter a correspondência de endereço MAC, endereços IP de destino ou origem, número da porta, conteúdo dos dados ou qualquer outra propriedade.

condutor. Material que permite a fácil passagem de corrente elétrica ou energia térmica sem apresentar muita resistência. Veja também: ***dielétrico***, ***isolante***.

conector BNC. Um conector de cabo coaxial que utiliza um mecanismo de encaixe rápido, do tipo baioneta. Estes conectores são tipicamente encontrados em cabos coaxiais Ethernet 10base2.

conector N. Um conector resistente para microondas comumente encontrado em componentes de rede para a instalação externa, como antenas ou access points.

conector TNC. Um conector comum e robusto para cabos de microondas.

contadores de portas. Switches e roteadores gerenciados fornecem estatísticas para cada porta de rede, os contadores. Estas estatísticas podem incluir os pacotes que entram e saem da rede, bytes transmitidos, assim como erros e retransmissões.

controles. No ***NEC2***, controles definem a fonte de RF em um modelo de antena. Ver também: ***estrutura***.

conversão chaveada. Método de conversão de voltagem DC que usa um componente magnético para armazenar temporariamente a energia, transformando-

a em uma tensão diferente. A conversão chaveada é muito mais eficiente que a ***conversão linear***.

conversão linear. Um método de conversão de corrente contínua que diminui a voltagem convertendo a energia excedente em calor. Veja também: ***conversão chaveada***.

conversor DC/AC. Dispositivo que converte corrente contínua em alternada, utilizada em muitos eletrodomésticos. Também conhecido como ***inversor***.

conversor DC/DC. Dispositivo que muda a voltagem de uma fonte de corrente contínua. Veja também: ***conversão linear***, ***conversão chaveada***.

coordenadas polares lineares. Um sistema gráfico com círculos concêntricos igualmente espaçados, representando valores absolutos de uma projeção polar. Estes gráficos são tipicamente usados para representar padrões de irradiação de antenas. Veja também: ***coordenadas polares logarítmicas***.

coordenadas polares logarítmicas. Um sistema gráfico com círculos concêntricos espaçados em intervalos logarítmicos, representando um valor absoluto em uma projeção polar. Tais gráficos são tipicamente usados para representar padrões de irradiação de uma antena. Veja também: ***coordenadas polares lineares***.

Corrente Alternada (***AC – Alternating Current***). Uma corrente elétrica que varia de forma cíclica no tempo. A corrente alternada é a normalmente usada para a iluminação e alimentação de eletrodomésticos. Veja também: ***Corrente Contínua***.

Corrente Contínua (***DC – Direct Current***). Corrente elétrica que se mantém constante com o tempo. Correntes DC são normalmente usadas por equipamentos de rede, como access points e roteadores. Veja também: ***Corrente Alternada***.

CPE. Veja: ***Customer Premises Equipment***.

criptografia de camada de conexão. Uma conexão criptografada entre dispositivos no link local, tipicamente um ***cliente*** wireless e um ***access point***. Veja também: ***criptografia fim-a-fim***.

criptografia de chave pública. Forma de criptografia usada por SSL, SSH e outros programas populares de segurança. A criptografia de chave pública permite que informação criptografada seja trocada em uma rede não confiável sem a necessidade de distribuição de uma chave secreta privada.

criptografia fim-a-fim. Uma conexão criptografada negociada por ambas as extremidades de uma sessão de comunicação. A criptografia fim-a-fim pode fornecer uma proteção mais forte que a criptografia na camada de comunicação quando usada em redes inseguras (como a Internet).

cron. Um utilitário Unix que facilita o agendamento e a execução múltipla de programas. Veja também: ***at***.

Curva característica de IV. Um gráfico que representa a corrente que é fornecida, baseada na voltagem gerada para uma certa irradiação solar.

Customer Premises Equipment. Equipamentos de rede (como roteador ou bridge) que são instalados na localidade do cliente.

D

dB. Veja: ***decibel***.

DC. Veja: ***Corrente Contínua***.

decibel (***dB***). Unidade logarítmica de medida que expressa a magnitude de potência em relação a um nível de referência. Unidades comumente usadas são dBi (decibéis relativos a um irradiador isotrópico) e dBm (decibéis relativos a um milliwatt).

Denial of Service (***DoS***). Ataque de negação de serviços. Um tipo de ataque a recursos da rede, normalmente feito através da geração de tráfego excessivo ou da exploração de problemas em uma aplicação ou protocolo de rede.

depreciação. Método contábil aplicado na reserva financeira para a cobertura de uma eventual quebra de equipamento.

descarga excessiva. Descarga de uma bateria além de sua ***Profundidade Máxima de Descarga***, que resulta em sua deterioração.

descasamento de polarização. Um estado onde as antenas de transmissão e recepção não utilizam a mesma polarização, resultando em perda de sinal.

detecção de redes. Ferramentas de diagnóstico que mostram informações sobre redes wireless, como o nome da rede, canal e método de criptografia utilizado.

DHCP. Veja: ***Dynamic Host Configuration Protocol***.

dielétrico. Um material não condutor que separa fios condutores dentro de um cabo.

Digital Video Broadcast (***DVB-S***). Um dos vários padrões para o acesso à Internet via satélite. Veja também: ***Broadband Global Access Network*** (***BGAN***) e ***Very Small Aperture Terminal*** (***VSAT***).

diodos de passagem. Uma funcionalidade encontrada em alguns painéis solares que evita a formação de hot-spots em células que estão na sombra, mas que também reduz a máxima voltagem do painel.

Direct Sequence Spread Spectrum (***DSSS – Seqüência Direta de Espalhamento de Espectro***). Esquema de modulação de rádio usado pelo 802.11b.

diretividade. A habilidade de uma antena em focar sua energia em uma direção particular quando transmitindo, ou de receber energia de uma direção particular quando recebendo.

diversidade. Veja: ***diversidade de antena***.

diversidade de antena. Uma técnica usada para contornar a interferência por multicaminhos com o uso de duas ou mais antenas de recepção fisicamente separadas.

DNS. Veja: ***Domain Name Service***.

DNS de horizonte dividido. Técnica usada para prover diferentes respostas de DNS, com base na fonte que faz a solicitação. O horizonte dividido é usado para direcionar os usuários internos para um conjunto diverso de servidores para os quais são direcionados os usuários da Internet.

dnsmasq. Um servidor de código aberto para o caching de DNS e DHCP, disponível em *http://thekelleys.org.uk/*

Domain Name Service (***DNS – Serviço de Nome de Domínios***). O amplamente utilizado protocolo de rede que mapeia nomes a endereços IP.

DoS. Veja: ***Denial of Service***.

DSSS. Veja: ***Direct Sequence Spread Spectrum***.

DVB-S. Veja: ***Digital Video Broadcast***.

Dynamic Host Configuration Protocol (***DHCP – Protocolo de Configuração Dinâmica de Host***). Um protocolo usado por computadores para a determinação automática de seus endereços IP.

E

elevação. Veja: ***inclinação***.

E lógico. Operação lógica que traz o resultado verdadeiro apenas quando todos os componentes avaliados são também verdadeiros. Veja também: ***OU lógico***.

encaminhamento. Quando roteadores recebem pacotes destinados a um computador ou rede diferente, eles encaminham o pacote para o roteador mais próximo do destino final do pacote. Este processo é chamado de encaminhamento.

endereço de broadcast. Em redes IP, o endereço de broadcast é utilizado para enviar dados para todos os computadores na sub-rede local. Em redes Ethernet, o endereço de broadcast MAC é usado para enviar dados a todas as máquinas no mesmo domínio de colisão.

endereço da rede. O menor número IP em uma determinada sub-rede. O endereço da rede é usado em tabelas de roteamento para especificar o destino a ser usado quando do envio de pacotes para um grupo lógico de endereços IP.

endereço MAC. Endereço individual de 48 bits designado a cada dispositivo de rede no momento de sua fabricação. O endereço MAC é usado para a comunicação em link local.

energia solar fotovoltaica. O uso de painéis solares para coletar energia solar na produção de eletricidade. Veja também: ***energia solar térmica***.

energia solar térmica. Energia coletada do sol na forma de calor. Veja também: ***energia solar fotovoltaica***.

espaço de endereços. Um grupo de endereços IP residindo na mesma sub-rede lógica.

espaço de endereços privados. Conjunto de endereços IP reservados, descritos no RFC1918. São freqüentemente usados dentro de uma organização em conjunto com a tradução de endereços de rede (NAT). Os espaços reservados de endereços privados incluem 10.0.0.0/8, 172.16.0.0/12 e 192.168.0.0/16. Veja também: ***NAT***.

espalhamento. Perda de sinal devida a objetos no caminho entre dois nós. Veja também: ***perda no espaço livre***, ***atenuação***.

espião. Alguém que intercepta tráfego de dados como senhas, emails, dados de voz ou conversas online.

espectro. Veja: ***espectro eletromagnético***.

espectro eletromagnético. A ampla variação de freqüência possível de energia eletromagnética. Entre as porções do espectro eletromagnético encontram-se o rádio, microondas, luz visível e raios X.

Estado de Carga (***SoC – State of Charge***). A quantidade de carga presente em uma bateria, determinada pela voltagem atual e pelo tipo da bateria.

estrutura. No ***NEC2***, uma descrição numérica sobre a localização das diferentes partes de uma antena e da forma como os fios estão conectados. Veja também: ***controles***.

EtherApe. Uma ferramenta de visualização de código aberto disponível em *http://etherape.sourceforge.net/*.

Ethereal. Veja: ***Wireshark***.

Extended Service Set Identifier (***ESSID***). O nome usado para identificar uma rede 802.11. Veja também ***rede fechada***.

F

ferramentas de checagem pontual. Ferramentas de monitoramento de rede que são executadas apenas quando é necessário diagnosticar um problema. Ping e traceroute são exemplos de ferramentas de checagem pontual.

ferramentas de teste de throughput. Ferramentas que medem a largura de banda real disponível entre dois pontos de uma rede.

filter. A tabela padrão usada em um firewall de filtros de rede é a tabela filter. Esta tabela é usada para determinar o tráfego que pode ser aceito ou negado.

filtragem MAC. Método de controle de acesso baseado no endereço MAC dos dispositivos de comunicação.

filtro de pacotes. Um firewall que opera na camada de Internet através da inspeção dos endereços IP de origem e destino, número das portas e protocolos. Os pacotes são aceitos ou descartados, conforme as regras de filtragem.

firestarter. Uma ferramenta gráfica para a configuração de firewalls Linux, disponível em *http://www.fs-security.com/*

firewall. Um roteador que aceita ou nega tráfego com base em alguns critérios. Os firewalls são uma ferramenta básica para a proteção de redes inteiras contra tráfego indesejado.

firewall de bridge transparente. Uma técnica de firewall que utiliza uma bridge para seletivamente encaminhar pacotes baseados nas regras de firewall. Um dos benefícios desta técnica é a de que ela não necessita de um endereço IP. Veja também: ***bridge***.

flush. A remoção de todas as entradas de uma tabela de roteamento ou cadeia de filtros de rede.

freqüência. O número de ondas completas que passam por um ponto fixo em um dado período de tempo. Veja também: ***comprimento de onda***, ***Hertz***.

full duplex. Equipamento de comunicação que pode enviar e receber ao mesmo tempo (como um telefone). Veja também: ***half duplex***.

fwbuilder. Ferramenta gráfica que permite a criação de scripts iptables em uma máquina à parte do servidor, que depois podem ser transferidos para ele. *http://www.fwbuilder.org/*

G

ganho. A habilidade de um componente de rádio (como uma antena ou amplificador) de aumentar a potência de um sinal. Veja também: ***decibel***.

ganho de antena. A quantidade de energia concentrada na direção da radiação mais

forte da antena, normalmente expressa em dBi. O ganho da antena é recíproco, o que significa que seu efeito é presente tanto na transmissão quanto na recepção.

gaseificação. Produção de bolhas de oxigênio e hidrogênio que ocorre quando uma bateria é ***sobrecarregada***.

gateway padrão. Quando um roteador recebe um pacote destinado a uma rede para a qual não existe uma rota explícita, o pacote é encaminhado ao *gateway* (passagem) padrão. O gateway padrão repete o processo, encaminhando o pacote ao seu próprio gateway padrão, até que o pacote atinja seu destino final.

gerador de sinal. Um transmissor que emite continuamente uma onda em uma determinada freqüência.

gerador fotovoltaico. Veja: ***painel solar***.

H

half duplex. Equipamentos de comunicação que podem enviar ou receber, nunca ao mesmo tempo (como rádios comunicadores portáteis). Veja também: ***full duplex***.

hardware gerenciado. Hardware de rede que fornece uma interface administrativa, estatísticas para as portas, SNMP ou outras funcionalidades interativas.

Heliax. Cabo coaxial de alta qualidade, com um condutor central sólido ou tubular e um condutor trançado exterior, que dá flexibilidade ao conjunto. Veja também: ***coax***.

Hertz (***Hz***). Unidade de medida de ***freqüência*** que significa o número de ciclos por segundo.

HF (***High Frequency***). Ondas de rádio entre 3 e 30 MHz. Redes de dados podem ser feitas com HF, operando em distâncias bastante longas mas com pouca capacidade de dados.

hop. Cada um dos elementos de roteamento em uma conexão de rede. Um servidor web pode estar a vários hops (saltos) distante de seu computador local, fazendo com que os pacotes sejam encaminhados de roteador a roteador até que cheguem a seu destino final.

Horas de Pico de Sol (***PSH – Peak Sun Hours***). Média diária de irradiação solar para uma determinada área.

hot-spot. Em redes wireless, um hot-spot é uma localidade que fornece acesso à Internet via ***Wi-Fi***, tipicamente com o uso de um ***portal cativo***. Em ***sistemas fotovoltaicos***, um hot-spot acontece quando uma ***célula*** única em um ***painel solar*** é sombreada, passando a atuar como uma carga resistiva ao invés de gerar energia.

hub. Um dispositivo de rede Ethernet que repete os dados recebidos em todas as portas conectadas. Veja também: ***switch***.

Hz. Veja: ***Hertz***.

I

IANA. Veja: ***Internet Assigned Numbers Authority***.

ICMP. Veja: ***Internet Control Message Protocol***.

ICP. Veja: ***Inter-Cache Protocol***.

impedância. O quociente da voltagem sobre a corrente em uma linha de transmissão, consistindo em uma resistência e uma reatância. A impedância da carga deve corresponder à impedância da fonte de energia para a transferência máxima de potência (50 Ω) para a maioria dos equipamentos de comunicação.

inclinação. Ângulo que marca o desvio de um plano horizontal. Veja também: ***azimute***.

Infra-estrutura de Chaves Públicas (***PKI – Public Key Infrastructure***). Mecanismo de segurança usado em conjunto com a ***criptografia de chave pública*** para evitar a possibilidade de ataques ***Man-In-The-Middle***. Veja também: ***autoridade certificadora***.

injetores de fim de caminho (***ou de fim de curso***). Um dispositivo 802.3af de Power over Ethernet que fornece energia através de um cabo Ethernet. Um switch Ethernet que fornece energia em cada uma de suas portas é um exemplo de injetor. Veja também: ***injetores de meio de caminho***.

injetores de meio de caminho (***ou meio de curso***). Um dispositivo de Power Over Ethernet inserido entre um switch Ethernet

e o dispositivo a ser alimentado. Veja também: ***injetores de fim de caminho***.

injetor POE passivo. Veja: ***Power over Ethernet***.

interferência construtiva. Quando duas ondas idênticas e em fase se combinam, a amplitude resultante é o dobro de cada uma das ondas. Isto é chamado de interferência construtiva. Veja também: ***interferência destrutiva***.

interferência destrutiva. Quando duas ondas idênticas são combinadas em fases opostas, a amplitude resultante é nula. Isto é chamado de interferência destrutiva. Veja também: ***interferência construtiva***.

Inter-Cache Protocol (***ICP***). Protocolo de alto desempenho usado para a comunicação entre caches web.

Internet Assigned Numbers Authority (***IANA***). Organização que administra as várias partes críticas da infra-estrutura da Internet, incluindo a alocação de endereços IP, servidores raiz de nomes e números de serviços de protocolos.

Internet Control Message Protocol (***ICMP***). Protocolo de camada de rede usado para informar os nós sobre o estado da rede. O ICMP é parte da suíte de protocolos Internet. Veja também: ***Suíte de protocolos Internet***.

Internet Protocol (***IP***). O protocolo de camada de rede mais comum em utilização. O IP define os computadores e redes que compõem a Internet global.

Intrusion Detection System (***IDS – Sistema de Detecção de Intrusos***). Programa que monitora o tráfego de rede, buscando por padrões suspeitos de dados ou de comportamento. Um IDS pode fazer o registro das ocorrências, notificar o administrador de rede ou tomar alguma ação direta em resposta ao tráfego indesejado.

inspeção de estado (***stateful inspection***). Regras de firewall que levam em conta o estado associado a um determinado pacote. O estado não é parte do pacote transmitido através da Internet, mas é determinado pelo próprio firewall. Conexões novas, estabelecidas e relacionadas podem ser levadas em consideração na filtragem dos pacotes. A inspeção de estado também é chamada de rastreamento de conexão.

inversor. Veja: ***Conversor DC/AC***.

IP. Veja: ***Internet Protocol***.

iproute2. O pacote de ferramentas avançadas para Linux, utilizado para a formatação de tráfego (*shaping*) e outras técnicas. Disponível em *http://linux-net.osdl.org/*

iptables. O comando principal usado na manipulação de regras de filtragem de rede em um firewall.

irradiação. A quantidade total de energia solar que ilumina uma área específica, em W/m2.

isolador. Veja: ***dielétrico***.

K

knetfilter. Utilitário gráfico para a configuração de firewalls Linux. Disponível em *http://venom.oltrelinux.com/*

L

lag. Termo comum utilizado para descrever uma rede com alta ***latência***.

lambda (**λ**). Veja: ***comprimento de onda***.

LAN. Veja: ***Rede Local***.

largura de banda. Medida de variação de freqüência normalmente usada em comunicações digitais. O termo largura de banda é também utilizado em substituição de capacidade, referindo-se a máxima velocidade teórica de transmissão de dados em uma linha de comunicação. Veja também: ***capacidade***, ***canal***, ***throughput***.

largura de feixe. Distância angular entre os pontos em qualquer dos lados do lóbulo principal de uma antena, onde a potência recebida equivale à metade do lóbulo principal. A largura de feixe de uma antena é usualmente indicada para os planos vertical e horizontal.

latência. A quantidade de tempo que um pacote leva para atravessar uma conexão de rede. Com freqüência (ainda que incorretamente) o termo é usado em substituição ao tempo de ida e volta (RTT – Round Trip Time), já que a medida do RTT para uma conexão em uma área ampla é simples, se comparado com a medida real da latência. Veja também: ***Round Trip Time***.

lease time. Em DHCP, os endereços IP são designados por um período de tempo limitado, conhecido como lease time (tempo de empréstimo). Depois que este período de tempo espira, os clientes devem solicitar um novo endereço IP ao servidor DHCP.

limite. Veja: ***borda***.

Linha de visão (***LOS – Line of Sight***). Se uma pessoa que está no ponto A tem uma visão desobstruída do ponto B, então diz-se que o ponto A tem uma linha de visão clara do ponto B.

linha de transmissão RF. A conexão (normalmente ***coax***, ***Heliax*** ou ***guia de onda***) entre um rádio e uma antena.

link local. Dispositivos de rede que estão conectados ao mesmo segmento físico, comunicando-se diretamente entre si, são ditos estar em link local. Uma conexão de link local não pode cruzar os limites de um roteador sem o uso de algum tipo de encapsulamento, como ***túnel*** ou ***VPN***.

listen. Diz-se que os programas que aceitam conexões em uma determinada porta TCP "escutam" (*listen*) naquela porta.

lóbulos laterais. Nenhuma antena é capaz de irradiar toda a energia apenas em uma única direção preferencial. Há sempre alguma irradiação em outras direções. Estes picos menores de irradiação são chamados de lóbulos laterais.

loops de encaminhamento. Uma rota desconfigurada, onde os pacotes são ciclicamente encaminhados entre dois ou mais roteadores. Falhas catastróficas de rede são evitadas com o uso do parâmetro TTL de cada pacote, mas loops de encaminhamento devem ser resolvidos para que a rede funcione apropriadamente.

LOS. Veja: ***Linha de visão***.

M

Man-In-The-Middle (***MITM – Homem do meio***). Um ataque de rede em que um usuário malicioso intercepta toda a comunicação entre o cliente e o servidor, permitindo que os dados sejam copiados ou manipulados.

Mapa Digital de Elevação (***DEM – Digital Elevation Map***). Dados que representam a altitude de um terreno para uma determinada área geográfica. Estes mapas são usados por programas como o ***Radio Mobile*** para modelar a propagação eletromagnética.

máscara de sub-rede. Veja: ***máscara de rede***.

máscara de rede (***netmask, network mask***). Uma máscara de rede é um número de 32 bits que divide os 16 milhões de endereços IP disponíveis em porções menores, chamadas de sub-redes. Todas as redes IP utilizam endereços IP em conjunto com máscaras para agrupar logicamente computadores e redes.

matriz de painéis solares. Um conjunto de ***painéis solares*** ligados em série ou paralelo com a finalidade de prover a energia necessária para uma determinada ***carga***.

Máxima Profundidade de Descarga (***DoD_{max}***). A quantidade de energia extraída de uma bateria em um único ciclo de descarga, expressa percentualmente.

Máximo Ponto de Potência (***P_{max}***). O ponto máximo de potência fornecida pelo painel solar.

MC-Card. Um conector de microondas muito pequeno encontrado em equipamentos Lucent / Orinoco / Avaya.

meio compartilhado. Uma rede de link local onde cada nó pode observar o tráfego de todos os demais.

mesh. Uma rede sem organização hierárquica, onde cada nó carrega o tráfego dos demais quando necessário. Boas implementações de redes mesh são auto-curáveis, o que significa que elas podem detectar problemas de roteamento e consertá-los sempre que preciso.

método do pior mês. Um método para o cálculo das dimensões de um sistema fotovoltaico independente, de forma que ele funcione no mês em que a demanda de energia é a maior com relação a energia solar total disponível.

MHF. Veja: ***U.FL***.

microfinança. A provisão de pequenos empréstimos, poupança ou outros serviços financeiros básicos para as pessoas mais pobres do mundo.

milliwatts (***mW***). Unidade de potência representando um milésimo de Watt.

MITM. Veja: ***Man-In-The-Middle***.

MMCX. Um conector de microondas muito pequeno, comumente encontrado em equipamentos fabricados pela Senao e Cisco.

modelo de rede OSI. Um modelo popular para comunicações em rede definido pelo padrão ISO/IEC 7498-1. O modelo OSI consiste de sete camadas interdependentes, da física à de aplicação. Veja também: ***modelo de rede TCP/IP***.

Modelo de rede TCP/IP. Uma simplificação popular do modelo de rede OSI que é usado em redes Internet. O modelo TCP/IP consiste de cinco camadas interdependentes, da física até a de aplicação. Veja também: ***Modelo de rede OSI***.

modo ad-hoc. Um modo de rádio usado por dispositivos 802.11 que permite a criação de uma rede sem um access point. Redes mesh freqüentemente usam rádios no modo ad-hoc. Veja também: ***modo gerenciado***, ***modo master***, ***modo monitor***.

modo de infra-estrutura. Veja: ***modo master***.

modo dominante. A freqüência mais baixa que pode ser transmitida por uma guia de onda de determinado tamanho.

modo gerenciado. Um modo de rádio usado por dispositivos 802.11 que permite que o rádio associe-se a uma rede criada por um access point. Veja também: ***modo master***, ***modo ad-hoc*** e ***modo monitor***.

modo master. Um modo de rádio usado por dispositivos 802.11 que permite a criação de uma rede como um access point. Veja também: ***modo gerenciado***, ***modo ad-hoc*** e ***modo monitor***.

modo monitor. Um modo de rádio usado por dispositivos 802.11 que não é normalmente utilizado para a comunicação, mas que permite o monitoramento passivo do tráfego de rádio. Veja também: ***modo gerenciado***, ***modo ad-hoc*** e ***modo master***.

módulo solar. Veja: ***painel solar***.

monitores em tempo real. Ferramentas de rede que realizam o monitoramento por longos períodos, notificando os administradores imediatamente quando do surgimento de um problema.

multicaminho (***multipath***). O fenômeno da reflexão de um sinal que atinge seu alvo através de diferentes caminhos, em tempos diferentes.

multiponto-para-multiponto. Veja: ***mesh***.

Multi Router Traffic Grapher (***MRTG***). Ferramenta de código aberto que gera gráficos estatísticos sobre o tráfego. Disponível em *http://oss.oetiker.ch/mrtg/*

mW. Veja: ***milliwatt***.

My TraceRoute (***mtr***). Ferramenta de diagnóstico de rede usada como alternativa ao tradicional programa traceroute. *http://www.bitwizard.nl/mtr/*. Veja também: ***traceroute*** / ***tracert***.

N

Nagios (*http://nagios.org*). Uma ferramenta de monitoramento em tempo real que armazena registros e notifica o administrador de sistemas sobre falhas de rede e de serviços.

NAT. Veja: ***Network Addrss Translation***.

nat. Tabela usada pelo sistema de firewall netfilter do Linux para a configuração de tradução de endereços de rede (Network Address Translation).

navegador principal (***master browser***). Em redes Windows, o navegador principal é o computador que mantém uma lista de todos os computadores, compartilhamentos e impressoras que aparecem em ***Network Neighborhood*** ou ***My Network Places***.

NEC2. Veja: ***Numerical Eletromagnetics Code***.

NetBIOS. Um protocolo de camada de sessão usado pela rede Windows para o compartilhamento de arquivos e impressoras. Veja também: ***SMB***.

netfilter. O sistema de filtragem de pacotes em kernels Linux modernos. Usa o comando iptables para manipular as regras de filtragem. *http://netfilter.org/*

NeTraMet. Uma ferramenta de código aberto para a análise de fluxo de tráfego em redes, disponível em *http://freshmeat.net/projects/netramet/*

Network Address Translation (***NAT***). Tecnologia que permite que muitos computadores compartilhem um único, globalmente roteável, endereço IP. Mesmo

que o NAT ajude a resolver o problema de limites de endereços IP, ele cria um desafio técnico para sistemas como Voz sobre IP.

network mask. Veja: ***máscara de rede***.

ngrep. Ferramenta de segurança em código aberto usada para encontrar padrões em fluxos de dados. Disponível em *http://ngrep.sourceforge.net/*.

nó. Um dispositivo capaz de enviar e receber dados em uma rede. Access points, roteadores, computadores e laptops são exemplos de nós.

notação CIDR. Um método usado para definir uma máscara de rede através da especificação de bits persistentes. Por exemplo, a máscara de rede 255.255.255.0 pode ser especificada como /24 na notação CIDR.

ntop. Ferramenta de monitoramento de rede que fornece detalhes sobre conexões e protocolos utilizados em uma rede local. ***http://www.ntop.org/***.

nulo. Em um padrão de irradiação de uma antena, um nulo é uma zona onde a potência irradiada está em seu valor mínimo.

número de dias de autonomia (***N***). O número máximo de dias que um sistema fotovoltaico pode operar sem receber energia solar.

Numerical Electromagnetics Code (***NEC2 – Código Numérico Eletromagnético***). Um pacote de software livre para a modelagem de antenas que possibilita a construção de um modelo em 3D e a análise da resposta eletromagnética da antena. *http://www.nec2.org/*.

O

OFDM. Veja: ***Orthogonal Frequency Division Multiplexing***.

onda eletromagnética. Uma onda que se propaga pelo espaço, sem a necessidade de um meio de propagação. Ela contém um componente elétrico e um componente magnético. Veja também: ***onda mecânica***.

onda mecânica. Uma onda causada quando algum meio ou objeto balança de maneira periódica. Veja também: ***onda eletromagnética***.

orçamento do link. A quantidade de energia de rádio disponível para suplantar as perdas no caminho. Se o orçamento do link for maior que a perda no caminho, a sensitividade mínima de recepção e demais obstáculos, então a comunicação deve ser possível.

Orthogonal Frequency Division Multiplexing (***OFDM - Multiplexação por Divisão Ortogonal de Freqüência***). Técnica de modulação baseada na idéia de multiplexação por divisão de freqüência (FDM) onde múltiplos sinais são enviados em diferentes freqüências.

OU lógico. Uma operação lógica que resulta em verdadeira se qualquer dos itens comparados é verdadeiro. Veja também: ***E lógico***.

oversubscribe. Superestimar. Permitir usuários além do que a máxima largura de banda disponível pode suportar.

P

pacote. Em redes IP, mensagens enviadas entre computadores são quebradas em pedaços menores chamados pacotes. Cada pacote inclui informações de origem, destino e outras usadas para rotear o pacote até o seu destino final, onde as mensagens são novamente montadas pelo TCP (ou outro protocolo) antes de serem passadas à aplicação.

padrão de antena. Um gráfico que descreve a força relativa de um campo de irradiação nas várias direções de uma antena. Veja também: ***plotagem retangular***, ***plotagem polar***, ***coordenadas polares lineares***, ***coordenadas polares logarítmicas***.

padrão de irradiação. Veja: ***padrão de antena***.

painel solar. O componente de um sistema fotovoltaico usado para converter a radiação solar em eletricidade. Veja também: ***bateria***, ***regulador***, ***carga***, ***conversor***, ***inversor***.

particionamento. Técnica usada por hubs de rede para limitar o impacto de computadores que transmitem excessivamente. Os hubs removem, temporariamente, o computador abusivo do resto da rede, reconectando-o após algum tempo. Particionamento excessivo indica a

presença de um elemento que está consumindo muita largura de banda, como um cliente peer-to-peer ou um vírus.

Par trançado sem blindagem (***UTP – Unshilded Twisted Pair***). Cabo usado para a Ethernet 10baseT e 100baseT, consistindo de quatro pares de fios trançados.

perda em espaço livre. Ou perda em espaço aberto, é a diminuição da potência devida ao espalhamento da frente de onda na medida em que ela se propaga no espaço. Veja também: ***atenuação***, ***Apêndice C***.

perda no caminho. Perda de sinal de rádio devida à distância entre as estações de comunicação.

perda no retorno. Uma taxa logarítmica, em dB, que compara a potência refletida pela antena com aquela que ela recebe da linha de transmissão. Veja também: ***impedância***.

pigtail. Um pequeno cabo de microondas que converte um conector fora do padrão a algo mais robusto e comumente disponível.

pilha de protocolos. Conjunto de protocolos de rede que fornecem camadas e funcionalidades interdependentes. Ver também: ***modelo de rede OSI*** e ***modelo de rede TCP/IP***.

ping. Uma ferramenta de diagnóstico de redes presente em todos os sistemas operacionais, que usa mensagens de eco ICMP para determinar o tempo de ida e volta até um computador da rede. O Ping pode ser utilizado para determinar a localização de problemas de rede, “pingando” computadores no caminho entre a máquina local e o destino final.

PKI. Veja: ***Infra-estrutura de Chaves Públicas***.

plataforma consistente. Custos de manutenção podem ser reduzidos com o uso de uma plataforma consistente, com o mesmo hardware, software e firmware para a maioria dos componentes da rede.

plotagem polar. Um gráfico onde os pontos estão localizados em uma projeção ao longo de um eixo de rotação (raio) em intersecção com vários círculos concêntricos. Veja também: ***plotagem retangular***.

plotagem retangular. Um gráfico onde os pontos estão localizados em uma grade simples. Ver também: ***plotagem polar***.

PoE. Veja: ***Power over Ethernet***.

polarização. A direção do componente elétrico de uma onda eletromagnética ao deixar a antena de transmissão. Veja também: ***polarização horizontal***, ***polarização vertical***, ***polarização circular***.

polarização circular. Um campo eletromagnético no qual o vetor do campo elétrico parece fazer um movimento circular na direção da propagação, fazendo uma volta completa para cada ciclo de RF. Veja também: ***polarização horizontal*** e ***polarização vertical***.

polarização horizontal. Um campo eletromagnético com um componente elétrico que se move linearmente na direção horizontal. Veja também: ***polarização circular***, ***polarização vertical***.

polarização linear. Uma ***onda eletromagnética*** onde o vetor do campo elétrico permanece no mesmo plano todo o tempo. O campo elétrico pode deixar a antena em uma orientação vertical, horizontal ou em algum ângulo entre estas duas. Veja também: ***polarização vertical***, ***polarização horizontal***.

polaridade reversa (***RP – reverse polarity***). Propriedade de conectores de microondas, baseada em um conector padrão com os gêneros invertidos. O ***RP-TNC*** é provavelmente o mais comum conector de polaridade reversa, mas outros, como o RP-SMA e o RP-N) também são usuais.

polarização vertical. Um campo eletromagnético com um componente elétrico que se move linearmente na direção vertical. A maioria dos dispositivos wireless de consumo usam a polarização vertical. Veja também: ***polarização circular***, ***polarização vertical***.

ponto-a-multiponto. Uma rede wireless formada por vários nós conectados a uma localidade central. O exemplo clássico de uma rede ponto-a-multiponto é um access point em um escritório, com vários laptops utilizando-o para o acesso à Internet. Veja também: ***ponto-a-ponto***, ***multiponto-a-multiponto***.

política. No netfilter, a política é a ação padrão a ser tomada quando nenhuma outra regra de filtragem pode ser aplicada.

Por exemplo, a ação padrão para qualquer conjunto de ações pode ser ACCEPT (aceita os pacotes) ou DROP (descarta os pacotes).

porta de gerenciamento. Em um switch gerenciado, uma ou mais portas de gerenciamento podem ser definidas para receber o tráfego enviado para todas as demais portas. Isto permite a conexão de um servidor de monitoramento de tráfego para observar e analisar os padrões de tráfego.

portal cativo. Mecanismo utilizado para redirecionar, de maneira transparente, a navegação web para uma nova localização. Portais cativos são freqüentemente utilizados para a autenticação ou para interromper a sessão online de um usuário (por exemplo, para apresentar a Política de Uso da Rede).

potência. Quantidade de energia em um certo período de tempo.

potência de transmissão. A quantidade de potência fornecida pelo transmissor de rádio, antes do ganho da antena ou perdas na linha.

Power over Ethernet (***PoE***). Técnica usada para fornecer energia DC para dispositivos através de um cabo Ethernet. Veja também: ***injetores de fim de caminho***, ***injetores de meio de caminho***.

PPP. Veja: ***Protocolo Ponto-a-Ponto***.

Princípio de Huygens. Um modelo de onda que propõe um número infinito de frentes de onda potenciais ao longo de cada ponto de uma frente de onda que avança.

Privoxy (*http://www.privoxy.org*). Um proxy web que fornece anonimidade através do uso de filtros. O Privoxy é comumente utilizado com o ***Tor***.

Protocolo de Integridade Temporária de Chave (***TKIP – Temporal Key Integrity Protocol***). Protocolo de criptografia usado em conjunto com o ***WPA*** para melhorar a segurança em uma sessão de comunicação.

protocolo independente de conexão. Um protocolo de rede (como o UDP) que não requer o início ou manutenção de uma sessão. Protocolos independentes de conexão são mais leves que os orientados à sessão, mas não oferecem a proteção dos dados ou a remontagem dos pacotes. Ver também: ***protocolo orientado à conexão***.

protocolo orientado a sessão. Um protocolo de rede (como o TCP) que requer sua inicialização antes que os dados podem ser trocados, assim como alguma limpeza depois que a troca foi concluída. Protocolos orientados a sessão costumam ter mecanismos de correção de erros e montagem de pacotes, enquanto protocolos que não são orientados a conexão não os têm. Veja também: ***protocolo independente de conexão***.

Protocolo Ponto-a-Ponto (***PPP***). Protocolo de rede normalmente usado em linhas seriais (como uma conexão discada) para fornecer conectividade IP.

proxy de anonimidade. Um serviço de rede que esconde a origem ou o destino das comunicações. Proxies de anonimidade podem ser usados para proteger a privacidade das pessoas ou para reduzir a responsabilidade legal pelos atos dos usuários de uma empresa.

proxy transparente. Veja: ***cache transparente***.

PSH. Veja: ***Horas de Pico de Sol***.

Q

queima rápida. Tipo de fusível que queima imediatamente caso a corrente que passe por ele seja maior que sua corrente nominal. Veja também: ***queima lenta***.

queima lenta. Um fusível que permite que uma corrente maior do que a sua corrente nominal o atravesse por um curto período de tempo. Veja também: ***queima rápida***.

R

rádio. A porção do espectro eletromagnético em que podem ser geradas ondas com a aplicação de corrente alternada a uma antena.

reciprocidade. A habilidade que uma antena tem de manter as mesmas características, seja na transmissão ou recepção.

rede de cano longo e grosso. Uma conexão de rede (como VSAT) de alta capacidade e alta latência. A fim de se conseguir o melhor desempenho possível, o

TCP/IP deve ser ajustado para corresponder ao tráfego de links deste tipo.

rede fechada. Um access point que não publica seu SSID. Técnica usada freqüentemente como medida de segurança.

Rede Local (***LAN – Local Area Network***). Uma rede (tipicamente Ethernet) usada dentro de uma organização. A parte da rede que existe imediatamente atrás de um roteador do provedor de acesso é geralmente considerada como parte da LAN. Veja também: ***WAN***.

Redes classe A, B e C. Por algum tempo, o espaço de endereços IP era alocado em blocos de três diferentes tamanhos. Estas eram as classes A (cerca de 16 milhões de endereços), B (cerca de 65 mil endereços) e C (255 endereços). Mesmo que o CIDR tenha substituído a alocação de endereços baseada em classes, ainda é comum referir-se a elas e usá-las internamente nas organizações, dentro do espaço privado de endereços. Ver também: ***notação CIDR***.

regulador. O componente de um sistema fotovoltaico que garante que a bateria trabalhe em condições apropriadas. Ele evita a sobrecarga e descarga excessiva da bateria, condições que diminuem a vida útil da mesma. Veja também: ***painel solar***, ***bateria***, ***carga***, ***conversor***, ***inversor***.

regulador de carga de energia solar. Veja: ***regulador***.

relação frente-costas. A relação da máxima ***diretividade*** de uma antena em relação à diretividade na direção oposta.

repetidor. Um nó que é configurado para reenviar todo o tráfego que não é direcionado a si próprio, freqüentemente usado para estender o alcance de uma rede.

repetidor de um braço só. Um repetidor wireless que utiliza apenas um rádio, com significativa redução de throughput. Veja também: ***repetidor***.

Request for Comments (***RFC – Solicitação de Comentários***). Os RFCs são uma série numerada de documentos publicados pela Internet Society que registram idéias e conceitos relacionados a tecnologias de Internet. Nem todos os RFCs são padrões reais, mas muitos são aprovados explicitamente pelo IETF ou tornam-se padrões de fato. Os RFCs podem ser consultados online em *http://rfc.net/*.

RIR. Veja: Autoridades Regionais de Registro de Internet.

rota padrão. Uma rota de rede que aponta para o gateway padrão.

roteamento cebola (***onion routing***). Ferramenta de privacidade (como o ***Tor***) que repetidamente reflete conexões TCP em um número de servidores espalhados pela Internet, envolvendo a informação de roteamento em várias camadas criptografadas.

roteamento reativo. Uma implementação de redes mesh onde as rotas são calculadas apenas quando há a necessidade de envio de dados a um nó específico. Veja também: ***roteamento proativo***.

roteamento proativo. Uma implementação de redes mesh, onde cada nó sabe da existência de qualquer outro nó na nuvem mesh, assim como quais deles podem ser usados para rotear tráfego. Cada nó mantém uma tabela de roteamento cobrindo toda a nuvem mesh. Veja também: ***roteamento reativo***.

Round Trip Time (***RTT – Tempo de Ida e Volta***). A quantidade de tempo que um pacote leva para ser reconhecido a partir do final de uma conexão. Freqüentemente confundido com ***latência***.

Round Robin Database (***RRD – Base de Dados "Round Robin"***). Um tipo de base de dados que armazena a informação de forma compacta e que não se expande com o passar do tempo. Este tipo de formato de dados é utilizado pela RRDtool e outras ferramentas de monitoramento de redes.

roteador. Dispositivo que encaminha pacotes entre redes diferentes. O processo de encaminhamento destes pacotes ao próximo hop da rede é chamado de ***roteamento***.

roteamento. Processo de encaminhamento de pacotes entre redes diferentes. O dispositivo responsável por este processo é chamado de ***roteador***.

roteável globalmente. Um endereço IP, fornecido por um provedor de acesso ou autoridade de atribuição de endereços, que pode ser acessado de qualquer ponto na Internet. No Ipv4 já há aproximadamente

quatro bilhões de endereços IP possíveis, mas nem todos são roteáveis globalmente.

RP. Veja: ***polaridade reversa***.

RP-TNC. Uma versão proprietária do conector TNC para microondas, com os gêneros invertidos. O RP-TNC é encontrado normalmente em equipamentos fabricados pela Linksys.

RRD. Veja: ***Round Robin Database***.

RRDtool. Conjunto de ferramentas que permite a criação e modificação de bases de dados RRD, assim como gerar gráficos úteis na representação de dados. O RRDtool é usado para o registro de uma série de dados históricos (como largura de banda, temperatura da sala de computadores, média de carga dos servidores) e pode mostrar estes dados como uma média no tempo. O RRDtool está disponível em *http://oss.oetiker.ch/rrdtool/*.

rsync (*http://rsync.samba.org/*). Ferramenta de código aberto para a transferência incremental de arquivos, usada para o espelhamento de dados.

RTT. Veja: ***Round Trip Time***.

S

SACK. Veja: ***Selective Acknowledgement***.

Secure Sockets Layer (***SSL – Camada segura de conexão***). Tecnologia para a criptografia fim-a-fim implementada por praticamente todos os navegadores web. SSL utiliza criptografia de chave pública e uma infra-estrutura de chaves públicas confiável para assegurar a comunicação de dados na web. Toda a vez em que você visita um site cuja URL se inicia com https, você está utilizando SSL.

Selective Acknowledgement (***SACK – Reconhecimento Seletivo***). Mecanismo usado na superação de ineficiências do TCP em redes de alta latência, como VSAT.

Server Message Block (***SMB***). Um protocolo usado em redes Windows para o serviço de compartilhamento de arquivos. Veja também: ***NetBIOS***.

Service Set ID (***SSID***). Veja: ***Extended Service Set Identifier***.

Shorewall (*http://shorewall.net*). Uma ferramenta de configuração para firewalls netfilter que não requer a aprendizagem da sintaxe do iptables.

Simple Network Management Protocol (***SNMP – Protocolo Simples de Gerenciamento de Rede***). Um protocolo projetado para facilitar a troca de informações gerenciais entre dispositivos de rede. O SNMP é tipicamente usado na consulta de switches de rede e roteadores para a obtenção de estatísticas operacionais.

sistema fotovoltaico. Um sistema de energia que gera a energia elétrica a partir da luz solar, armazenando-a para uso posterior. Um sistema fotovoltaico independente faz isto sem a conexão a nenhuma rede de fornecimento de energia já estabelecido. Veja também: ***bateria***, ***painel solar***, ***regulador***, ***carga***, ***conversor***, ***inversor***.

sistema fotovoltaico independente. Veja: ***sistema fotovoltaico***.

SMA. Um pequeno conector para cabo de microondas.

SMB. Veja: ***Server Message Block***.

SmokePing. Uma ferramenta para a medida de latência que mede, armazena e exibe dados sobre a latência, sua distribuição e perda de pacotes em um único gráfico. SmokePing está disponível em ***http://oss.oetiker.ch/smokeping/***.

SNMP. Veja: ***Simple Network Management Protocol***.

Snort (*http://www.snort.org/*). Um sistema bastante popular, em código aberto, para a detecção de intrusos. Veja também: ***Intrusion Detection System***.

sobrecarga. Estado de uma bateria que recebeu carga além de sua capacidade limite. Caso a energia seja aplicada além do máximo ponto de carga, o eletrólito começa a se decompor. ***Reguladores*** irão permitir um pequeno tempo de sobrecarga para evitar a ***gaseificação***, removendo a carga antes que a bateria seja danificada.

SoC. Veja: ***Estado de Carga***.

spoof. Técnica de fazer-se passar por um dispositivo de rede, usuário ou serviço.

Squid (*http://www.squid-cache.org/*). Um popular proxy para web cache em código aberto. Ele é flexível, robusto, com ampla funcionalidade e pode escalar para fornecer

o suporte a redes de praticamente qualquer tamanho.

SSID. Veja: ***Extended Service Set Identifier***.

SSL. Veja: ***Secure Sockets Layer***.

sub-redes. Um subconjunto de endereços de IP, definidos por ***máscara de rede***.

Suíte de protocolos Internet (***TCP/IP***). A família de protocolos de comunicação que são a base da Internet. Dentre estes protocolos estão TCP, IP, ICMP e UDP. Também chamada de ***suíte de protocolos TCP/IP*** ou simplesmente ***TCP/IP***.

switch. Um dispositivo de rede que provê uma conexão temporária, dedicada, entre dispositivos que estão se comunicando. Veja também: ***hub***.

T

tabela de roteamento. Uma lista de redes e endereços IP mantida pelo roteador para determinar quais pacotes devem ser encaminhados. Caso o roteador receba um pacote para uma rede que não se encontra em sua tabela de roteamento, ele usa sua rota padrão. Roteadores operam na camada de rede. Veja também: ***bridge*** e ***gateway padrão***.

tamanho de janela TCP. O parâmetro do TCP que define a quantidade de dados que pode ser enviada antes que um pacote de reconhecimento (ACK) seja recebido do destinatário. Por exemplo, um tamanho de janela de 3000 significa que dois pacotes de 1500 cada podem ser enviados até que o destinatário confirme que os recebeu ou solicite a sua retransmissão.

tabela MAC. Um switch de rede deve manter o registro dos endereços MAC usados em cada porta física a fim de distribuir eficientemente os pacotes. Esta informação é mantida na tabela MAC.

TCP. Veja: ***Transmission Control Protocol***.

TCP acknowledgment spoofing. Técnica usada em redes de alta latência para aumentar o tempo de reconhecimento (ACK) de pacotes TCP/IP.

tcpdump. Uma ferramenta popular, em código aberto, para a análise e captura de pacotes disponível em *http://www.tcpdump.org/*. Veja também: ***WinDump*** e ***Wireshark***.

TCP/IP. Veja: ***Suíte de protocolos Internet***.

Tempo de Vida (***TTL – Time to Live***). Este valor serve como um tempo de expiração ou parada de emergência, sinalizando o momento em que um dado deve ser descartado. Em redes TCP/IP, o TTL é um contador que começa com um determinado valor (como 64) e é decrementado a cada passagem (hop) por um elemento de roteamento da rede. Quando o TTL chega a zero, o pacote é descartado. Este mecanismo ajuda a reduzir os danos causados por loops de roteamento. Em DNS, o TTL define o tempo que um registro de zona deve ser mantido antes de ser atualizado. No Squid, o TTL define quanto tempo um objeto deve ser armazenado antes de ser novamente buscado de seu website original.

tendência. Tipo de ferramenta que faz o monitoramento de rede por longos períodos, colocando os resultados em um gráfico. Ferramentas de tendência permitem a você a previsão do comportamento futuro de sua rede, o que é útil no planejamento de atualizações e mudanças.

thrashing. O estado que um computador atinge ao esgotar toda a RAM disponível e passa a usar o disco rígido como memória temporária, com grande redução de desempenho do sistema.

throughput. A quantidade real de informação que flui a cada segundo em uma conexão de rede, descontadas as sobrecargas causadas pelo protocolo.

tipos de mensagem. Ao invés de usar números de portas, o tráfego ICMP usa tipos de mensagens para definir o tipo de informação que está sendo enviada. Veja também: ***ICMP***.

TKIP. Veja: ***Protocolo de Integridade Temporária de Chave***.

Tor (*http://www.torproject.org/*). Uma ferramenta de ***roteamento cebola*** que fornece boa proteção contra a análise de tráfego.

traceroute / ***tracert***. Utilitário ubíquo para o diagnóstico de rede, freqüentemente usado em conjunto com o ping para determinar a localização de problemas de rede. A versão Unix é chamada de traceroute e a versão

Windows de tracert. Ambas usam solicitações de eco ICMP com tempos crescente de TTL para determinar quais roteadores são utilizados para a conexão com um host remoto, mostrando também estatísticas de latência. Outra variante deste utilitário é o tracepath, que usa uma técnica similar para pacotes UDP. Veja também: ***mtr***.

tráfego de entrada. Pacotes de rede que se originam fora da rede local (tipicamente a Internet) e destinam-se à rede local. Veja também: ***tráfego de saída***.

tráfego de saída. Pacotes de rede originados na rede local e que têm como destino algum lugar fora da mesma (tipicamente algum lugar da Internet). Veja também: ***tráfego de entrada***.

tráfego externo. Tráfego de rede que se origina de, ou tem o destino em, um endereço IP fora de sua rede interna, como tráfego Internet.

transferência de ganho. Comparação de uma antena em testes em relação a uma antena conhecida, com ganho calibrado.

Transmission Control Protocol (***TCP – Protocolo de Controle de Transmissão***). Um protocolo orientado à sessão que opera na camada de transporte, provendo remontagem de pacotes, evitando congestionamentos e garantindo a entrega confiável. O TCP é um protocolo integrante de muitas aplicações de Internet, como HTTP e SMTP. Veja também: ***UDP***.

transmissor de vídeo. Um transmissor de vídeo de 2,4 GHz que pode ser usado como um ***gerador de sinal*** barato.

TTL. Veja: ***Tempo de Vida***.

túnel. Uma forma de encapsulamento que envolve uma pilha de protocolo dentro de outra. Isto é usado freqüentemente em conjunto com técnicas de criptografia para evitar que espiões tenham acesso aos dados trafegados, ao mesmo tempo em que se elimina a necessidade de suporte à criptografia no nível da aplicação. Os túneis são comumente usados em conjunto com ***VPN***s.

U

U.FL. Um conector de microondas muito pequeno, usado comumente em cartões de rádio do tipo mini-PCI.

UDP. Veja: ***User Datagram Protocol***.

usuários não intencionais. Usuários de laptops que se associam acidentalmente à rede wireless errada.

User Datagram Protocol (***UDP – Protocolo de Datagrama de Usuário***). ***Protocolo independente de conexão*** (na ***camada de transporte***) usado comumente para a transmissão de áudio e vídeo.

UTP. Veja: ***Par trançado sem blindagem***.

V

Velocidade. Um termo genérico usado como referência à capacidade de resposta de uma conexão de rede. Uma rede de alta velocidade deve ter baixa latência e mais do que a capacidade necessária para carregar o tráfego gerado por seus usuários. Veja também: ***largura de banda***, ***capacidade e latência***.

velocidade de dados. A velocidade (ou taxa) na qual rádios 802.11 trocam símbolos, que é sempre mais alta que o throughput disponível. Por exemplo, a velocidade de dados nominal do 802.11g é de 54 Mbps, enquanto o throughput máximo é de cerca de 20 Mbps. Veja também: ***throughput***.

Very Small Aperture Terminal (***VSAT – Terminal de abertura muito pequena***). Um dos vários padrões utilizados para o acesso à Internet via satélite. VSAT é a tecnologia de satélite mais largamente utilizada na África. Veja também: ***Broadband Global Access Network*** (***BGAN***) e ***Digital Video Broadcast*** (***DVB-S***).

Virtual Private Network (***VPN – Rede Privada Virtual***). Ferramenta utilizada para unir duas redes através de uma rede não confiável (como a Internet). As VPNs são usadas com freqüência na conexão de usuários remotos à rede de uma organização, quando os mesmos estão em viagem ou trabalhando a partir de suas casas. VPNs usam uma combinação de criptografia e túneis para assegurar todo o tráfego de rede, independente da aplicação utilizada. Veja também: ***túnel***.

VoIP (***Voz sobre IP***). Tecnologia que fornece funcionalidades similares às dos telefones em uma conexão Internet. Exemplos de clientes populares VoIP

incluem Skype, Gizmo Project, MSN Messenger e iChat.

Voltagem Nominal (***V_N***). A voltagem operacional de um sistema fotovoltaico, tipicamente 12 ou 24 volts.

VPN. Veja: ***Virtual Private Network***.

VSAT. Veja: ***Very Small Aperture Terminal***.

W

WAN. Veja: ***Wide Area Network***.

War drivers. Entusiastas wireless interessados em encontrar a localização física de redes wireless.

WEP. Veja: ***Wired Equivalent Privacy***.

wget (*http://www.gnu.org/software/wget/*). Ferramenta de linha de comando em código aberto para baixar páginas web.

Wide Area Nework (***WAN – Rede de Área Ampla***). Qualquer tecnologia de rede de longa distância. Linhas dedicadas, frame relay, DSL, wireless fixo e satélite implementam, todas elas, redes de área ampla. Veja também: ***LAN***.

Wi-Fi. Marca de marketing pertencente à Wi-Fi Alliance que é usada para referir-se a várias tecnologias de redes wireless (incluindo 802.11a/b/g). Wi-Fi é o diminutivo de *Wireless Fidelity* (Fidelidade Wireless).

Wi-Fi Protected Access (***WPA – Acesso Protegido Wi-Fi***). Protocolo de criptografia de camada de conexão razoavelmente forte suportado pela maioria dos equipamentos Wi-Fi modernos.

wiki. Um site web que permite ao usuário editar os conteúdos de qualquer uma de suas páginas. Um dos wikis públicos mais populares é *http://www.wikipedia.org/*

window scale (***ampliação de janela***). Melhoria ao TCP definida pelo RFC1323 que permite tamanhos de janela maiores que 64KB.

WinDump. A versão do tcpdump para Windows, disponível em *http://www.winpcap.org/windump/*

Wired Equivalent Privacy (***WEP – Privacidade Equivalente a Redes Cabeadas***). Um protocolo de criptografia em camada de conexão relativamente seguro, suportado por praticamente todos os equipamentos 802.11a/b/g.

Wireless Fidelity. Veja: ***Wi-Fi***.

wireshark (*http://www.wireshark.org/*). Um analisador de protocolos livre para Unix e Windows.

Wi-Spy. Um analisador de espectro de 2,4 GHz disponível em *http://www.metageek.net/*

WPA. Veja: ***Wi-Fi Protected Access***.

Z

Zabbix (*http://www.zabbix.org/*). Ferramenta de monitoramento em tempo real que registra ocorrências e notifica o administrador sobre quedas de serviço e problemas de rede.