Jaringan Wireless di Dunia Berkembang

Edisi ke Dua

Sebuah panduan praktis untuk merencanakan dan membuat infrastruktur telekomunikasi biaya murah

Jaringan Wireless di Dunia Berkembang

Untuk informasi tentang proyek ini, kunjungi kami di http://wndw.net/

Edisi pertama, Januari 2006
Edisi kedua, Desember 2007

Banyak istilah dan merek yang digunakan oleh para pabrikan dan vendor untuk membedakan produk mereka dan di klaim sebagai merek dagang. Jika ada istilah dan mereka tersebut muncul di buku ini, dan para penulis mengetahu akan klaim trademark, maka istilah dan merek tersebut akan di ketik dengan semua huruf besar atau awalnya huruf besar. Semua mereka dagang adalah milik dari para pemilik masing-masing.

Para penulis dan penerbit telah berusaha semaksimal mungkin untuk memperhatikan hal tersebut dalam menyiapkan buku ini, tapi tidak memberikan pernyataan atau implikasi garansi akan segala hal dan tidak bertanggung jawab jika ada kesalahan atau ketidak sengajaan. Tidak bertanggung jawab atas kecelakaan atau kerusakan yang berhubungan dengan atau terjadi karena penggunaan informasi yang ada di buku ini.

Daftar isi

Tentang Buku ini

Buku ini merupakan bagaian dari satu set materi yang behubungan dengan topik yang sama yaitu : Jaringan Wireless di negara berkembang. Proyek WNDM terdiri dari :

- Percetakan Buku, tersedia sesuai pesanan
- Beberapa terjemahan dalam bahasa : Perancis, Spanyol, Italia, Portugis, Aab, dan lain-lain
- DRM, terdapat versi gratis berupa PDF dan HTML
- Di dalam buku ini juga ada arsip hasil dari diskusi konsep dan teknik di Mailist
- Tambahan Studi Kasus, materi training, dan informasi lain yang terkait.

Untuk semua material ini dan lainnya, silahkan mengunjungi situs web kami di *http://wndw.net/*

Website juga akan memasukkan studi kasus tambahan, peralatan terkini, dan referensi situs web referensi. Relawan dan ide di persilahkan. Silahkan bergabung di Mailist dan kirimkan ide-ide anda.

Materi training yang telah di tulis untuk diberikan dalam buku ini di beri oleh Assosiasi Progressive Communications dan Abdus Salam International, lihat di website, *http://www.apc.org/wireless/* , atau di Center for Theoretical Physics, *http://wireless.ictp.trieste.it/*, untuk melihat lebih rinci tentang kuliah mereka dan materinya. Informasi tambahan telah disediakan oleh International Network, publikasi buku sains tersedia juga di *http://www.inasp.info/.* Beberapa materi nya juga sudah digabungkan langsung ke dalam buku ini. Materi tambahan di adaptasi dari buku " *How to Accelerate Your Internet'*, *http://bmwo.net/*

Kredit

Buku ini sudah mulai dibuat dalam Proyek BookSprint tahun 2005 bagian dari sesi WSFII, di London, England (*http://www.wsfii.org)*. Team inti terdiri dari 7 orang yang mengawali membuat outline buku itu, lalu hasilnya di presentasikan di acara konferensi, dan beberapa bulan kemudian mulai dibuat bukunya. Selama proyek ini berjalan, tim inti secara aktif

mengumpulkan kontribusi maupun masukan dari Komunitas Jaringan Wireless. Silahkan tambahkan masukan anda dan update ke WNDW Wiki di *http://wiki.wndw.net/*

- **Rob Flickenger** adalah yang memimpin penulis dan editor buku ini. Rob telah menulis beberapa buku tentang Jaringan Wireless dan Linux termasuk *"Wireless Hacks"* (O Reilly Media) dan "*How To Accelerate Your Internet"(*http://bwmo.net/). Dia bangga menjadi seorang Hacker, Sains amatir yang gila dan pengajur free network dimanapun.

- **Corinna "Elektra" Aichele.** Minat utama Elektra adalah Autonomous Power Systems dan wireless communication (antennas, wireless jarak jauh, mesh networking). Dia membuat Distro kecil Linux berdasarkan slackware pada wireless mesh networking. Informasi ini tentu akan berlebihan bila seseorang membaca buku ini. .. *http://www.scii.nl/~elektra*

- **Sebastian Büttrich** (*http://wire.less.dk/*) adalah seorang generalis dalam teknologi dengan latar belakang ahli fisika dan pemrograman Sains. Berasal dari Berlin, Jerman, Dia bekerja dengan IconMedialab di Copenhagen dari tahun 1997 sampai tahun 2002. Dia mendapatkan gelar Ph.D. Dalam bidang Fisika Kuantum dari Universitas Teknik Berlin Berlin. Latar belakangnya Fisika termasuk bidang lain seperti RF dan microwave spectroscopy, system photovoltaic , dan Matematika Lanjutan. Dia juga di kenal sebagai Musisi.

- **Laura M. Drewett** adalah salah satu penemu **Adapted Consulting Inc**., seorang pengusaha yang sosial, spesialisasi dalam aaptasi teknologi dan solusi bisnis untuk negara berkembang. Sejak pertama kali tinggal di Mali tahun 1990 dan menulis thesisnya tentang program pendidikan anak perempuan, dia telah berusaha keras untuk menemukan solusi untuk kesinambungan dari pengembangan program tersebut. Sebagai seorang ahli dalam kelangsungan Proyek di lingkungan negara berkembang, dia telah banyak mendesain dan mengelola proyek-proyek dari klien-klien yang berbeda di Afrika, Timur Tengah, dan Eropa Timur. Laura mendapatan gelar S1 dalam bidang Art (seni) dengan pembedaan dalam hubungan luar negeri dan Perancis (Distinction in Foreign Affairs and French) dari Universitas Virginia dan Gelar Master dalam bidang Manajemen Proyek dari Universitas George Washington School of Business.

- **Alberto Escudero-Pascual** dan **Louise Berthilson** adalah pemilik **IT +46**, Perusahaan Konsultasi Swedia dengan fokus pada Teknologi Informasi di daerah berkembang. IT +46 adalah perusahaan berskala international untuk mempromosikan dan implementasi infrastruktur Internet wireless di area pedesaan di Afrika dan Latin Amerika. Sejak tahun 2004, Perusahaannya telah mentraining lebih dari 350 orang di 14 negara dantelah merilis lebih dari 600 halaman dokumentasi di bawah lisensi creative common. Untuk informasi daat di lihat di *http://www.it46.se/*

- **Carlo Fonda**, adalah anggota Komunikasi Radio pada Abdus Salam International Center untuk Theoretical Physics di Trieste, Italy.

- **Jim Forster** telah menghabiskan karirnya dalam pengembangan software, rata-rata bekerja untuk System Operasi dan jaingan di produk-produk perusahaan. Dia berpengalaman dengan beberapa perusahaan baru di Silicon Valley yang gagal, dan hanya satu perusahaan yang berhasil yaitu Cisco Systems. Setelah banyak produk yang dikembangkan di sana, saat ini kegiatannya lebih banyak terlibat dalam proyek dan kebijakan untuk peningkatan Akses Internet di negara berkembang. Dia dapat dihubungi di j*rforster@mac.com.*

- **Ian Howard**. Setelah 7 tahun mengelilingi dunia sebagai penerjun Parasut di Militer Canada, memutuskan untuk menukar senjatanya untuk sebuah Komputer. Setelah dia menamatkan sekolahnya di Pengethauan Lingkungan, Universitas Waterloo, dia menulis proposal berjudul, *"Wireless technology has the opportunity to bridge the digital divide. Poor nations, who do not have the infrastructure for inter - connectivity as we do, will now be able to create a wireless infrastructure."* Sebagai penghargaan , Geekcorps mengirimnya ke Mali sebagai Manager Program Geekcorps Mali , dimana dia memimpin satu tim peralatan stasiun radio dengan menggunakan interkoneksi wireless dan mendesign konten system sharing. Dia sekarang konsultan dalam program-program Geekcorps.

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

- **Tomas Krag,** menghabiskan harinya bekerja dengan wire.less.dk, lembaga non profit dan tercatat, berkantor di Copenhagen, di dirikan bersama rekan dan koleganya Sebastian Büttrich di awal tahun 2002. wire.less.dk spesialisasinya di bidang Solusi Jaringan Wireless komunitas, dan mempunyai fokus spesial pada jaringan wireless murah untuk negara berkembang.
  Tomas juga berasosiasi dengan the Tactical Technology Collective, *http://www.tacticaltech.org/,* sebuah lembaga non-profit di Amsterdam “to strengthen social technology movements and networks in developing and transition countries, as well as promote civil society s effective, conscious and creative use of new technologies.” Saat ini energinya habis tercurah ke Roadshow Wireless (*http://www.thewirelessroadshow.org/*), sebuah proyek yang mendukung mitra masyarakat sipil di negara berkembang dalam pengembangan perencanaan , pembangunan dan solusi kesinambungan konektivitas berbasis pada spektrum unlicense, teknologi terbuka dan pengetahuan terbuka.

- **Gina Kupfermann,** Sarjana Teknik dalam bidang Manajemen Energi dan Bisnis. Di samping profesinya sebagai Kontrol Keuangan dia juga bekerja untuk pekerjaan pribadi untuk proyek komunitas dan juga LSM . Sejak tahun 2005 dia jadi anggota Dewan Executive untuk Asosiasi pengembang jaringan yang bebas, entitas legal dari freifunk.net.

- **Adam Messer.** Sesungguhnya dia adalah ahli serangga. Adam Messer berubah menjadi profesional di bidang Telekomunikasi setelah diberi kesempatan di tahun 1995, untuk memimpin ISP pertama di Afrika. Sebagai pioner dalam pelayanan data wireless di Tanzania, Messer bekerja selama 11 tahun di Afrika Timur dan Afrika Barat untuk Voice dan Komunikasi Data untuk karir pemula di bidang Selular multinasional.

Dia tinggal di Amman, Jordan.

- **Juergen Neumann** (*http://www.ergomedia.de/)*, mulai bekerja dalam bidang Teknologi Informasi tahun 1984 dan sejak saat itu selalu mencari cara untuk mengembangkan IT yang beguna bagi Organisasi dan Masyarakat. Sebagai seorang Konsultan untuk strategi dan implementasi IT, dia bekerja untuk Perusahaan besar bersekala international dan juga bekerja di banyak proyek-proyek non profit. Tahun 2002 dia memangun www.freifunk.net, suatu cara berkampanye menyebarluaskan Ilmu dan Jaringan Sosial tentang Jaringan Bebas dan Terbuka. Freifunk secara keseluruhan dikenal sebagai Proyek Komunitas yang paling berhasil di bidangnya.

- **Ermanno Pietrosemoli,** telah terlibat dalam perencanaan dan pembangunan Jaringan Komputer hampir 20 tahun terakhir. Sebagai Pemimpin Jaringan Sekolah Latin Amerika,Escuela Latinoamericana de Redes “EsLaRed”, *www.eslared.org.ve,* Dia telah mengajar Komunikasi data wireless di beberapa negara, tapi tempat tinggalnya di Merida, Venezuela.

- **Frédéric Renet,** adalah Pendiri Technical Solutions di Adapted Consulting, Inc. Frédéric telah terlibat di bidang IT lebih dari 10 tahun dan bekerja dengan komputer sejak masa kanak-kanak. Dia mulai karirnya di bidang IT pada awal tahun 1990, di Buletin Board System (BBS) dengan Modem Analog, dan terus membuat system yang dapat meningkatkan komunikasi. Sampai saat ini Frédéric menghabiskan waktunya lebih setahun ini bergabung di IESC/Geekcorps Mali sebagai konsultan. Dalam kapasitasnya, dia mendesain banyak solusi inovasi untuk penyiaran radio FM, Laboratorium Komputer Sekolah dan System penerangan di pedesaan.

- **Marco Zennaro,** aka marcusgennaroz, seorang insunyur teknik elektro pada ICTP di Trieste, Italy. Dia telah menggunakan BBS dan radio amatir sejak dia remaja, dia sangat senang menggabungkan keduanya dalam pekerjaan Jaringan Wireless, tapi dia masih berkarir di Apple Newton.

Pendukung

- **Lisa Chan** (*http://www.cowinanorange.com/)* adalah pemimpin di bagian Editor naskah.

- **Casey Halverson** (*http://seattlewireless.net/~casey/*) membantu di teknis untuk review dan usulan-usulan yang masuk.

- **Jessie Heaven Lotz** (*http://jessieheavenlotz.com/*) menyediakan beberapa Ilustrasi terbaru dalam edisi ini.

- **Richard Lotz** (*http://greenbits.net/~rlotz/*) menyediakan ulasan teknis usulan. Dia bekerja pada Proyek Wireless di Seattle, dan ingin melepaskan node dan rumahnya tidak di ketergantungan PLN.

- **Catherine Sharp** (*http://odessablue.com/*) menyediaka support untuk editing naskah.

- **Lara Sobel** mendesain cover buku WNDW edisi ke dua. Dia sorang artis yang tinggal di Seattle, WA

- **Matt Westervelt** (*http://seattlewireless.net/~mattw/)* menyediakan support untuk ulasan teknis and editing naskah. Matt adalah pendiri SeattleWireless (*http://seattlewireless.net/)* dan dia seorang pendakwah untuk FreeNetwork di seluruh dunia.

Petunjuk Tenaga Surya

Bab yang membahas Sumber materi tenaga surya telah diterjemahkan dan dikembangkan oleh Alberto Escudero-Pascual. Tahun 998, Organisasi Engineering without Borders (Federasi Spanyol) mempublikasikan edisi pertama buku pegangan dengan judul " Manual de Energía Solar Fotovoltaica y Cooperación al Desarrollo". Buku pegangan ini telah di tulis dan dipublikasikan oleh anggota LSM dan ahli dari Insitut Politeknik Surya Energi, universitas Madrid. Tanpa sengaja, tidak seorangpun dari anggota dari tim editor yang menyimpan dokumen dalam bentuk format elektronik dan oleh keranenya banyak edisi lanjutan tidak dibuat. Mereka melewati hampir 10 tahun dari edisi pertama sampai dengan dokumen ini berusaha di selamatkan dan juga mengembangkan lebih lanjut buku pegangan tersebut.

Sebagai bagian operasi penyelamatan Alberto ingin mengucapkan terima kasih kepada koordinator yang mengerjakan edisi pertama yang asli. Juga kepada mentornya di Universitas : Miguel Ángel Eguido Aguilera, Mercedes Montero Bartolomé y Julio Amador. Pekerjaan baru ini di bawah lisensi Creative Commons ***Attribution-ShareAlike 3.0.*** Kami berharap materi ini mejadi titik awal untuk ediri baru termasuk kontribusi baru oleh komunitas.

Edisi ke dua dan selanjutnya dari panduan tenaga surya telah menerima masukan yang sangat berharga dari Frédéric Renet dan Louise Berthilson.

Terima kasih yang istimewa

Tim inti ingin mengucapkan terima kasih kepada pengelola WSFII yang telah menyediakan tempat, support dan bandwith berkala yang menjadi inkubator untuk proyek ini. Kami juga berterima kasih kepada jaringan komunitas dimanapun, yang telah menghabiskan waktu dan energinya guna mewujudkan Internet global. Tanpa anda, Jaringan masyarakat tidak bisa berhasil. Publikasi pekerjaan ini juga di support oleh Canada's International Development Research Centre, *http://www.idrc.ca/.* Support lainnya juga diberikan oleh *NetworktheWorld.org*

Bab 1 Dimana harus Memulai

Buku ini dibuat oleh tim yang masing-masing individu, dalam bidangnya masing-masing, berpartisipasi secara aktif dalam memperluas jangkauan Internet dan mendorong lebih jauh dari sebelumnya. Popularitas jaringan nirkabel telah menyebabkan biaya peralatan untuk terus menukik, sementara kemampuan peralatan terus meningkat tajam. Kami percaya bahwa dengan mengambil keuntungan dari ini keadaan, masyarakat akan mampu membangun infrastruktur komunikasinya sendiri. Kami berharap tidak hanya untuk meyakinkan Anda bahwa ini mungkin, tetapi juga menunjukkan bagaimana kami telah dilakukan hal tersebut, dan untuk memberikan informasi dan perangkat yang diperlukan untuk memulai proyek jaringan lokal komunitas anda.

Infrastruktur nirkabel dapat dibangun untuk biaya sangat sedikit dibandingkan dengan alternatif kabel yang tradisional. Akan tetapi, penghematan biaya hanya sebagian dari pembangunan jaringan nirkabel. Dengan memberikan komunitas lokal ke akses ke informasi yang lebih murah dan mudah, mereka akan langsung merasakan manfaat yang di tawarkan oleh Internet. Waktu dan usaha yang dihemat dengan akses ke jaringan global akan langsung diterjemahkan pada kekayaan pada skala lokal, karena banyak pekerjaan dapat dilakukan dalam waktu singkat dan usaha yang lebih sedikit.

Demikian pula, jaringan akan lebih berharga saat semakin banyak orang yang tersambung ke jaringan tersebut. Komunitas terhubung ke Internet dengan kecepatan tinggi akan memiliki suara di pasar global, dimana transaksi terjadi di seluruh dunia pada kecepatan cahaya. Orang di seluruh dunia merasakan bahwa akses internet mereka memberikan suara untuk membahas masalah-masalah mereka, politik, dan banyak hal yang penting untuk kehidupan mereka, dengan cara yang tidak dapat di saingi oleh telepon dan televisi. Apa yang sampai saat ini di rasakan seperti fiksi ilmiah, sekarang menjadi kenyataan, dan kenyataan tersebut dibangun di atas jaringan nirkabel.

Bahkan tanpa adanya akses ke Internet, jaringan nirkabel komunitas memiliki nilai yang besar. Jaringan akan memungkinkan orang untuk melakukan kerja sama dalam proyek yang melingkupi jarak yang jauh. Komunikasi suara, email, dan data dapat dipertukarkan dengan biaya sangat murah. Dengan melibatkan komunitas lokal dalam pembuatan jaringan, pengetahuan dan kepercayaan akan tersebar keseluruh komunitas, dan orang mulai memahami pentingnya bagi mereka terlibat dalam infrastruktur komunikasi. Pada akhirnya, mereka menyadari bahwa jaringan komunikasi dibangun agar orang dapat terhubung satu dengan lainnya.

Dalam buku ini kita akan fokus pada teknologi jaringan data teknologi nirkabel keluarga 802.11. Sementara jaringan tersebut dapat membawa data, suara, dan video (termasuk juga traffik tradisional seperti web dan internet), jaringan yang akan dijelaskan dalam buku ini

adalah jaringan data. Kami tidak akan membahas GSM, CDMA, atau teknologi nirkabel suara lainnya, karena biaya implementasi teknologi tersebut diluar jangkauan kebanyakan proyek komunitas.

Tujuan dari buku ini

Sasaran keseluruhan dari buku ini adalah untuk membantu anda membuat teknologi komunikasi di komunitas lokal anda dengan harga terjangkau dan dengan sedapat mungkin menggunakan sumber daya yang ada. Menggunakan peralatan murah yang ada, anda bisa membuat jaringan data berkecepatan tinggi yang menghubungkan wilayah yang luas, menyediakan jaringan akses broadband di daerah-daerah yang dial-up saja tidak ada, dan akhirnya menghubungkan anda dan tetangga anda ke internet global. Dengan memakai bahan-bahan disekitar anda sebagai material dan membuat sendiri berbagai komponen-nya, anda bisa membuat sambungan jaringan yang bisa diandalkan dengan budjet yang sedikit. Dan dengan bekerja sama dengan komunitas sekitar, anda bisa membuat sebuah infrastruktur komunikasi yang menguntungkan semua orang yang berpartisipasi di dalamnya.

Buku ini bukan panduan untuk mengatur card wireless di laptop anda atau memilih peralatan terbaik untuk jaringan rumah anda. Titik berat buku ini adalah untuk membuat sambungan infrastruktur yang menjadi tulang punggung dari jaringan nirkabel wilayah luas luas. Dengan sasaran tersebut, informasi akan di berikan dari banyak sudut pandang, termasuk diantaranya adalah faktor teknik, sosial, dan finansial. Koleksi dari pembelajaran yang studi kasus beberapa kelompok yang mencoba untuk membuat jaringan ini, sumber daya yang digunakan untuk itu, dan hasil-hasil akhir dari percobaan tersebut.

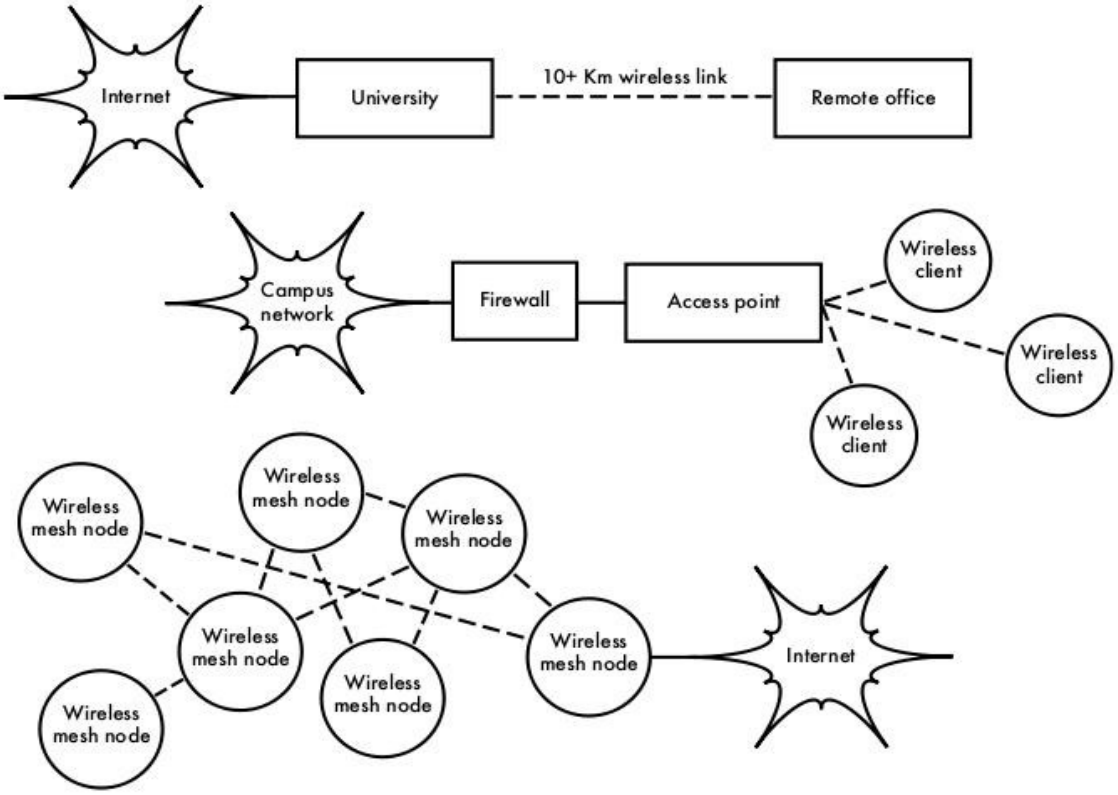
Dari experimen pemancar “spark gap” awal abad yang lalu, nirkabel telah menjadi teknologi komunikasi yang berkembang pesat. Dalam buku ini, kami menampilkan contoh spesifik tentang cara membuat sambungan data berkecapatan tinggi, teknik yang diterangkan di buku ini tidak dimaksudkan untuk mengganti infrastruktur kabel yang sudah ada (seperti telepon atau fiber optik). Teknik yang di terangkan disini lebih di maksudkan untuk memperbaiki sistem yang sudah ada, dan menyediakan sambungan di daerah-daerah dimana fiber atau kabel lainnya tidak mungkin digunakan.

Kami berharap, buku ini dapat menyelesaikan tantangan komunikasi anda.

Memasukkan nirkabel ke jaringan anda yang sudah ada

Jika anda adalah seorang adminstrator jaringan, anda mungkin bingung bagaimana nirkabel dapat dimasukkan ke infrastruktur jaringan anda yang sudah ada. Nirkabel dapat melayani dalam banyak kapasitas, dari sambungan sederhana (seperti beberapa kilometer kabel

Ethernet) sampai pusat distribusi (seperti hub yang besar). Berikut ini beberapa contoh bagaimana jaringan anda dapat diuntungkan oleh teknologi nirkabel.



Gambar 1.1: Beberapa contoh jaringan nirkabel

Protokol jaringan nirkabel

Tekonologi utama yang banyak digunakan untuk membuat jaringan nirkabel adalah keluarga protokol 802.11, dikenal juga sebagai ***Wi-Fi.*** Keluarga protokol 802.11 dari protokol radio (802.11a,802.11b, dan 802.11g) telah menikmati popularitas yang luar biasa di Amerika Serikat dan Eropa. Dengan menggunakan keluarga protokol yang sama, para produsen di seluruh dunia telah membuat peralatan yang saling interoperable. Keputusan ini telah tebukti menjadi anugrah yang luar biasa terhadap industri dan para konsumen. Konsumen dapat memakai peralatan yang menggunakan 802.11 tanpa harus takut terhadap ketergantungan terhadap suatu pedagang. Hasilnya, konsumen bisa membeli peralatan murah dalam volume yang sudah menguntungkan para produsen. Jika para produsen memilih untuk tetap memakai protokol mereka sendiri, sepertinya tidak mungkin jaringan nirkabel dapat semurah dan bisa ada dimana-mana seperti sekarang ini.

Sementara protokol-protokol baru seperti 802.16 (dikenal juga sebagi WiMax) sepertinya bisa

menyelesaikan beberapa kesulitan yang tampak pada 802.11, mereka tampaknya harus melalui jalan yang panjang untuk dapat menyaingi popularitas peralatan 802.11. Di penulisan, kami akan fokus pada keluarga 802.11.

Ada banyak protokol di keluarga 802.11, dan tidak semua berhubungan langsung dengan protokol radio itu sendiri. Ada tiga (3) standar nirkabel yang sekarang di implementasikan di kebanyakan peralatan yang sudah siap pakai, yaitu:

- **802.11b.** Disahkan oleh IEEE pada tanggal 16 September 1999, 802.11b mungkin adalah protokol jaringan nirkabel yang paling populer yang dipakai saat ini. Jutaan alat-alat untuk mendukungnya telah dikeluarkan sejak 1993. Dia memakai modulasi yang dikenal sebagai ***Direct Sequence Spread Spectrum (DSSS)*** di bagian dari ISM band dari 2.400 sampai 2.495 GHz. Dia mempunyai kecepatan maximum 11 Mbps, dengan kecepatan sebenernya yang bisa dipakai sampai 5 Mbps.

- **802.11g.** Karena belum disahkan sampai Juni 2003, 802.11g merupakan pendatang yang telat di pasar nirkabel. Biarpun terlambat, 802.11g sekarang menjadi standar protokol jaringan nirkabel de facto karena sekarang dia pada hakekatnya dipakai di semua laptop dan kebanyakan alat-alat handheld lainnya. 802.11g memakai ISM band yang sama dengan 802.11b, tetapi memakai modulasi yang bernama ***Orthogonal Frequency Division Multiplexing (OFDM)*****.** Dia punya kecepatan maximum data 54 Mbps (dengan throughput yang bisa dipakai sebesar 22 Mbps), dan bisa turun menjadi 11 Mbps DSSS atau lebih lambat untuk kecocokan dengan 802.11b yang sangat populer.

- **802.11a.** Disahkan juga oleh IEEE pada tanggal 16 September 1999, 802.11a memakai OFDM. Dia punya kecepatan maximum data 54 Mbps, dengan throughput sampai setinggi 27 Mbps. 802.11a beroperasi di ISM band antara 5.745 dan 5.805 GHz, dan di bagian dari UNII band diantara 5.150 dan 5.320 GHz. Ini membuatnya tidak cocok dengan 802.11b atau 802.11g, dan frekuensi yang lebih tinggi berarti jangkauannya lebih pendek dari pada 802.11b/g dengan daya pancar yang sama. Memang bagian dari spektrumnya relatif tidak dipakai dibandingkan dengan 2.4 GHz, sayangnya dia hanya legal digunakan di sedikit negara di dunia. Tanyakan kepada pihak yang berwenang sebelum memakai peralatan 802.11a, terutama untuk penggunaan di luar ruangan. Peralatan 802.11a sebetulnya relatif murah, tapi tidak sepopuler 802.11b/g.

Selain dari standar di atas, ada beberapa pengembangan pada peralatan, kecepatan yang tinggi, enkripsi yang lebih kuat, dan jangkauan lebih jauh, yang vendor-specific. Sayangnya pengembangan ini tidak bisa bekerja di antara peralatan-peralatan dari produsen lain, dan membeli mereka berarti mengharuskan anda memakai pedagang itu di semua bagian jaringan anda. Peralatan dan standar baru(seperti 802.11y, 802.11n, 802.16, MIMO dan WiMAX) menjanjikan pertambahan kecepatan dan bisa diandalkan yang signifikan, tetapi peralatan ini baru mulai dijual ketika penulisan ini dimulai, dan ketersediaan barang dan kecocokan dengan peralatan lain masih belum pasti.

Karena ketersediaan peralatan dimana-mana dan sifatnya yang tidak perlu ijin dari 2.4 GHz ISM band, buku ini akan fokus pada membuat jaringan menggunakan 802.11b dan 802.11g.

Tanya & Jawab

Jika anda masih pemula di jaringan nirkabel, anda biasanya mempunyai beberapa pertanyaan tentang apa yang dapat dilakukan oleh sebuah teknologi dan berapa biayanya. Berikut ini beberapa pertanyaan yang sering ditanyakan, dengan jawaban dan saran di halaman yang dicantumkan.

Listrik

- Bagaimana cara saya untuk memberi listrik pada peralatan radio saya, jika tidak ada PLN? **Halaman 241.**
- Apakah saya perlu menarik kabel listrik sampai ke atas menara? **Halaman 283**
- Bagaimana saya memakai panel surya untuk memberi listrik pada wireless node saya sambil tetap membiarkannya online semalaman? **Halaman 217**
- Berapa lama access point saya berjalan dengan memakai aki? **Halaman 238**
- Dapatkah saya memakai sebuah generator tenaga angin untuk memberi listrik pada peralatan saya waktu malam? **Halaman 212**

Manajemen

- Berapa bandwidth yang perlu saya beli untuk para pengguna? **Halaman 65**
- Bagaimana saya dapat mengamati dan mengurus access points jarak jauh dari kantor saya? **Halaman 174**
- Apa yang harus saya lakukan ketika jaringannya rusak? **Halaman 174, 267**
- Apa masalah yang biasa dihadapi di jaringan nirkabel, dan bagaimana cara saya memperbaikinya? **Halaman 267**

Jarak

- Seberapa jauhkah jangkauan dari akses point saya? **Halaman 67**
- Apakah ada rumus yang dapat saya gunakan untuk mengetahui jarak yang dapat saya jangkau dari sebuah akses point? **Halaman 67**
- Bagaimana saya dapat tahu jika sebuah daerah terpecil bisa terhubung melalui Internet dengan memakai sambungan nirkabel? **Halaman 67**
- Apakah ada software yang bisa membantu saya mengkalkulasi kemungkinan membangun sebuah sambungan nirkabel jarak jauh? **Halaman 74**

- Produsen mengatakan bahwa access point saya hanya mampu sampai 300 meter. Apakah itu benar? **Halaman 67**
- Bagaimana saya bisa menyediakan sambungan nirkabel ke banyak client jarak jauh, dan tersebar di seluruh kota? **Halaman 53**
- Apakah benar bahwa saya dapat mencapai jarak yang lebih jauh dengan menambah kaleng atau aluminium pada antena AP saya? **Halaman 116**
- Bisakah saya memakai nirkabel untuk menyambung ke sebuah site jarak jauh dan membagi sebuah sambungan Internet? **Halaman 51**
- Sambungan nirkabel saya kelihatannya akan perlu waktu yang terlalu lama untuk bekerja dengan baik. Bisakah saya menggunakan repeater di tengahnya untuk membuatnya lebih baik? **Halaman 77**
- Apakah sebaiknya saya memakai amplifier saja? **Halaman 115**

Instalasi

- Bagaimana cara saya menginstallasi AP indoor saya di atas sebuah tiang di atap saya? **Halaman 249**
- Apakah benar-benar berguna memasang penangkal petir pada tiang antena saya, atau bisakah saya tidak memakainya? **Halaman 263**
- Bisakah saya membuat tiang antena sendiri? Sampai berapa tinggi? **Halaman 251**
- Kenapa antena saya bekerja lebih baik ketika saya memasangnya “kesamping”? **Halaman 13**
- Kanal / channel mana yang sebaiknya saya pakai? **Halaman 15**
- Akankah gelombang radio melewati gedung dan pohon? Bagaimana dengan manusia? **Halaman 16**
- Dapatkah gelombang radio melewati bukit yang ada dihadapannya? **Halaman 17**
- Bagaimana cara saya membuat jaringan mesh? **Halaman 56**
- Apa jenis antena yang terbaik untuk jaringan saya? **Halaman 102**
- Bisakah saya membuat access point memakai PC daur ulang? **Halaman 143**
- Bagaimana cara saya install Linux di AP saya? Kenapa saya harus melakukannya? **Halaman 152**

Uang

- Bagaimana cara saya mengetahui jika sambungan wireless nirkabel bisa dicapai dengan dana terbatas? **Halaman 281**
- AP manakah yang paling bagus dengan harga yang paling murah? **Halaman 137**
- Bagaimana cara saya mengetahui dan menagih pelanggan saya yang menggunakan jaringan jaringan nirkabel saya? **Halaman 165, 190**

Mitra dan Pelanggan

- Jika saya memberikan sambungan jaringan, apakah saya masih perlu pelayaan dari ISP? Mengapa? **Halaman 27**
- Berapa banyak pelanggan yang diperlukan untuk menutup biaya saya? **Halaman 287**
- Berapa banyak pelanggan yang bisa saya support? **Halaman 65**
- Bagaimana cara saya membuat jaringan nirkabel saya lebih cepat? **Halaman 79**
- Apakah kecepatan sambungan Internet sudah maksimum? **Halaman 90**

Keamanan

- Bagaimana saya bisa melindungi jaringan nirkabel saya dari pencuri bandwidth? **Halaman 157**
- Apakah benar bahwa jaringan nirkabel selalu tidak terjaga dan terbuka untuk serangan dari hacker? **Halaman 160**
- Apakah benar bahwa memakai software open source membuat jaringan saya kurang aman? **Halaman 167**
- Bagaimana cara melihat apa yang sedang terjadi di jaringan saya? **Halaman 174**

Informasi dan perijinan

- Adakah buku lain yang dapat saya baca untuk menambah pengetahuan jaringan nirkabel saya? **Halaman 355**
- Dimana saya bisa mencari informasi tambahan online? **Halaman 349,** http://wndw.net/, http://www.wirelessu.org
- Bisakah saya memakai bagian-bagian dari buku ini untuk pengajaran saya sendiri? Bisakah saya print dan jual kopi dari buku ini? Ya. Lihat About This Book untuk lebih detilnya.

Bab 2 Pengenalan Praktis pada Fisika Radio

Komunikasi Wireless (nirkabel) menggunakan gelombang elektromagnet untuk mengirimkan sinyal jarak jauh. Dari sisi pengguna, sambungan wireless tidak berbeda jauh dengan sambungan jaringan lainnya: Web browser anda, e-mail, dan aplikasi jaringan lainnya akan bekerja seperti biasanya. Akan tetapi gelombang radio memiliki beberapa hal yang berbeda di bandingkan dengan kabel Ethernet. Contoh, sangat mudah melihat jalur yang di ambil oleh kabel Ethernet – lihat lokasi colokan LAN di komputer anda, ikuti kabel Ethernet sampai di ujung lainnya, dan anda akan menemukan jalur tersebut! Anda juga dapat secara mudah memasang banyak kabel Ethernet berdampingkan satu sama lain tanpa saling mengganggu, karena kabel akan sangat efektif untuk menjaga agar sinyal menjalan dalam kabel tersebut saja.

Bagaimana cara kita melihat pancaran gelombang dari card wireless yang kita gunakan? Apa yang terjadi jika gelombang terpantul oleh objek di ruangan atau bangunan di sambungan luar ruang? Apakah mungkin beberapa card wireless digunakan di sebuah lokasl yang sama tanpa saling berinterferensi (mengganggu)? Untuk dapat membangun sebuah sambungan wireless berkecepatan tinggi yang stabil, sangat penting untuk mengerti perilaku gelombang di dunia nyata.

Apakah gelombang?

Kita semua cukup terbiasa dengan getaran atau osilasi dalam berbagai bentuk – pendulum, pergerakan mengayun di angin, dawai (snar) dari sebuah gitar – semua adalah contoh dari osilasi.

Mereka semua mempunyai hal yang sama, sebuah media atau objek, akan berayun secara periodik, dengan jumlah ayunan / siklus tertentu per satuan waktu. Jenis gelombang ini kadang kala di sebut sebagai ***gelombang mekanik***, karena di bentuk oleh pergerakan dari sebuah objek, atau propagasi di media.

Pada saat ayunan / osilasi bergerak (saat ayunan tidak menetap di sebuah tempat saja) maka kita melihat sebuah propagasi gelombang di ruangan. Sebagai contoh, seorang penyanyi menghasilkan ayunan / osilasi gelombang suara pada pita suara di kerongkongannya. Osilasi gelombang secara periodik mengkompress dan men-dekompres udara, dan secara periodik mengubah tekanan udara yang kemudian meninggalkan mulut si penyanyi dan bergerak, pada kecepatan suara di udara. Contoh lain, batu kita lemparkan ke kolam akan menyebabkan gelombang, yang kemudian bergerak menyebrangi kolam sebagai ***gelombang.***

Sebuah gelombang mempunyai ***kecepatan, frekuensi*** dan ***panjang gelombang***. Masing-masing parameter berhubungan melalui hubungan yang sederhana,

```
Kecepatan = Frekuensi * Panjang Gelombang
```

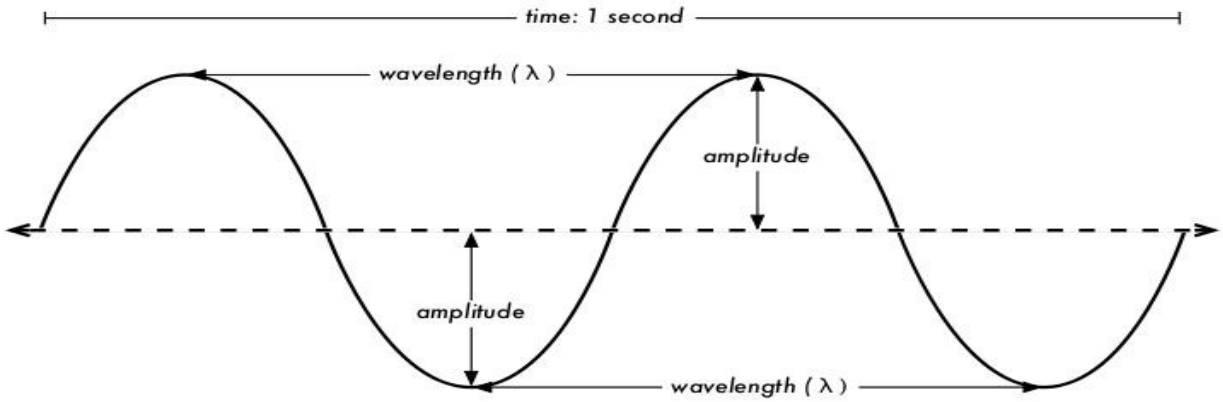
Panjang gelombang (biasanya di kenal sebagai ***lambda, λ***) adalah jarak yang di ukur dari satu titik dari sebuah gelombang ke titik yang sama di gelombang selanjutnya. Misalnya, dari puncak gelombang yang satu ke puncak gelombang yang selanjutnya. Frekuensi adalah jumlah dari gelombang yang melalui titik tertentu dalam sebuah perioda waktu. Kecepatan biasanya diukur dalam meter per detik, frekuensi biasanya di ukur dalam getaran per detik (atau Hertz, yang di singkat ***Hz***), dan panjang gelombang biasanya di ukur dalam meter.

Sebagai contoh, sebuah gelombang di air menjalar pada satu meter per detik, dan berosilasi lima kali per detik, maka setiap gelombang adalah dua puluh sentimeter panjangnya.

```
1 meter/detik = 5 ayunan/detik * W
W = 1 / 5 meter
W = 0.2 meter = 20 cm
```

Gelombang mempunyai sebuah parameter yang di sebut ***amplituda.*** Amplituda adalah jarak dari pusat gelombang ke puncak tertinggi gelombang, dan dapat di bayangkan sebagai “tinggi” dari gelombang di air. Hubungan antara frekuensi, panjang gelombang, dan amplituda tampak pada **Gambar 2.1.**

Gelombang di air sangat mudah untuk di visualisasikan. Jatuhkan sebuah batu ke kolam maka anda akan melihat gelombang akan bergerak di air. Dalam hal gelombang elektromagnet, bagian yang paling sukar untuk di mengerti adalah “Apa yang berayun?”. Untuk dapat mengerti, kita perlu mengerti adanya kekuatan elektromagnet.



Gambar 2.1: Panjang Gelombang, Amplituda, dan Frekuensi.

Untuk gelmbang ini, freluensinya adalah dua ayunan per detik, atau 2 Hz.

Kekuatan Elektromagnetik

Kekuatan elektromagnetik adalah kekuatan antara muatan listrik dan arus. Terutama bagi kita yang berada di dunia barat / Eropa / Amerika, kita dapat langsung merasakannya pada saat kita memegang pegangan pintu besi sesudah berjalan di atas karpet sintetik, atau menyentuh pagar listrik. Contoh yang lebih dahsyat dari kekuatan elektromagnetik adalah halilintar atau petir yang sering kita dapati pada saat hujan atau badai. ***Kekuatan listrik*** adalah kekuatan antara muatan listrik. Sementara ***kekuatan elektromagnetik*** adalah kekuatan antara arus listrik.

Elektron adalah partikel yang membawa muatan listrik negatif. Tentunya masih banyak jenis partikel yang lain, tapi elektron adalah yang banyak bertanggung jawab untuk hal-hal yang perlu kita ketahui tentang bagaimana perilaku radio.

Mari kita lihat apa yang terjadi pada sebuah kabel yang lurus, di dalam kabel tersebut kita dorong elektron untuk bergerak dari satu ujung ke ujung yang lain bolak balik secara periodik. Pada satu saat, ujung atas kabel akan bermuatan negatif – semua elektron negatif berkumpul di situ. Hal ini menyebabkan terjadinya medan listrik dari plus ke minus sepanjang kabel. Di saat yang lain, semua elektron di dorong ke ujung bawah kabel, dan medan listrik akan berbalik arah. Hal ini terjadi berulang ulang, vektor medan listrik (berarah dari plus ke minus) akan meninggalkan kabel, dan beradiasi menuju ruang di sekitar kabel.

Apa yang baru saja kita bahas biasanya di kenal sebagai dipole, karena ada dua pole / kutub, plus dan minus, atau lebih sering di kenal sebagai ***antenna dipole.*** Hal ini merupakan bentuk paling sederhana dari antenna omnidirectional (segala arah). Pergerakan medan listrik biasanya di kenal sebagai ***gelombang elektromagnetik.***

Mari kita kembali ke persamaan,

```
Kecepatan = Frekuensi * Panjang Gelombang
```

Untuk gelombang elektromagnetik, kecepatan adalah **c,** atau kecepatan cahaya,

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

Gelombang elektromagnetif berbeda dengan gelombang mekanik, mereka tidak membutuhkan media untuk menyebar / berpropagasi. Gelombang elektromagnetif bahkan akan ber-propagasi di ruang hampa seperti di ruang angkasa.

Pangkat sepuluhan

Dalam fisika, matematika, dan teknik, kita sering mengekspresikan angka dalam pangkat sepuluhanan. Kita akan bertemu dengan banyak istilah-istilah ini, misalnya, Giga-Hertz (GHz), Centimeter (cm), Micro-detik (μs), dan sebagainya

Kelipatan Sepuluh			
Nano-	10^{-9}	1/1000000000	n
Mikro-	10^{-6}	1/1000000	μ
Mili-	10^{-3}	1/1000	m
Senti-	10^{-2}	1/100	c
Kilo-	10^{3}	1 000	k
Mega-	10^{6}	1 000 000	M
Giga-	10^{9}	1 000 000 000	G

Dengan mengetahui kecepatan cara, kita dapat menghitung panjang gelombang untuk frekuensi tertentu. Mari kita ambil contoh frekuensi untuk jaringan wireless 802.11b, yaitu

```
f = 2.4 GHz
  = 2,400,000,000 getaran / detik

 panjang gelombang lambda (λ0 = c / f
                          = 3*10^8 / 2.4*10^9
                          = 1.25*10^-1 m
                          = 12.5 cm
```

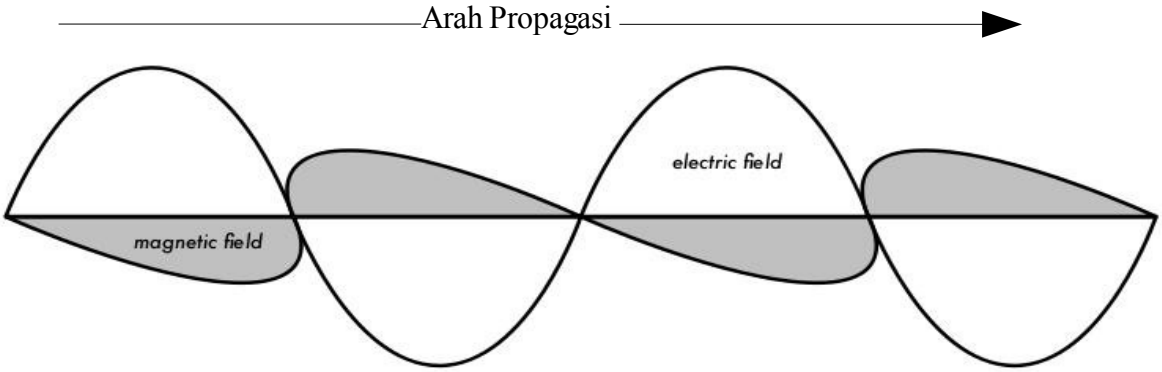
Frekuensi dan panjang gelombang akan menentukan sebagian besar dari perilaku gelombang elektromagnetik, mulai dari antenna yang kita buat sampai dengan objek yang ada di perjalanan dari jaringan wireless yang akan kita operasikan. Panjang gelombang juga akan bertanggung jawab pada berbagai perbedaan standard yang akan kita pilih. Oleh karena-nya, memahami dasar dari frekuensi dan panjang gelombang akan sangat menolong dalam pekerjaan praktis wireless network.

Polarisasi

Salah satu parameter penting yang menentukan kualitas gelombang elektromagnetik adalah

polarisasi. Polarisasi di jelaskan sebagai arah dari vektor medan listrik.

Jika kita bayangkan sebuah antenna dipole yang di pasang vertikal (atau sebuah kabel yang berdiri tegak), elektron akan bergerak naik dan turun, tidak ke samping, karena tidak ada ada tempat untuk bergerak ke samping,oleh karenanya medan listrik hanya akan mengarah ke atas atau ke bawah, secara vertikal. Medan yang meninggalkan kabel akan bergerak sebagai gelombang akan berpolarisasi sangat lurus, dalam hal ini vertikal. Jika antenna kita letakan datar sejajar dengan tanah, maka kita akan menemukan bahwa gelombang yang di hasilkan akan mempunyai polarisasi linier horizontal.



Gambar 2.2: Komponen medan listrik dan medan magnet sebuah gelombang elektromagnetik. Polarisasi menggambarkan orientasi medan listrik.

Polarisasi linear adalah salah satu kasus spesial, dan di alam jarang yang betul-betul sempurna, pada umumnya, kita akan melihat sedikit komponen dari medan yang mengarah ke arah yang lain. Kasus yang umum terjadi adalah polarisasi eliptik, dengan sebuah extrim linier (hanya satu arah) dan polarisasi sirkular (dua arah dengan kekuatan yang sama). Polarisasi antenna menjadi sangat penting pada saat kita melakukan pengarahan antenna. Jika kita tidak memperdulikan polarisasi antenna, kemungkinan kita akan memperoleh sinyal yang kecil walaupun menggunakan antenna yang paling kuat. Hal ini disebut sebagai ***ketidak cocokan polarisasi.***

Spektrum Elektromagnetik

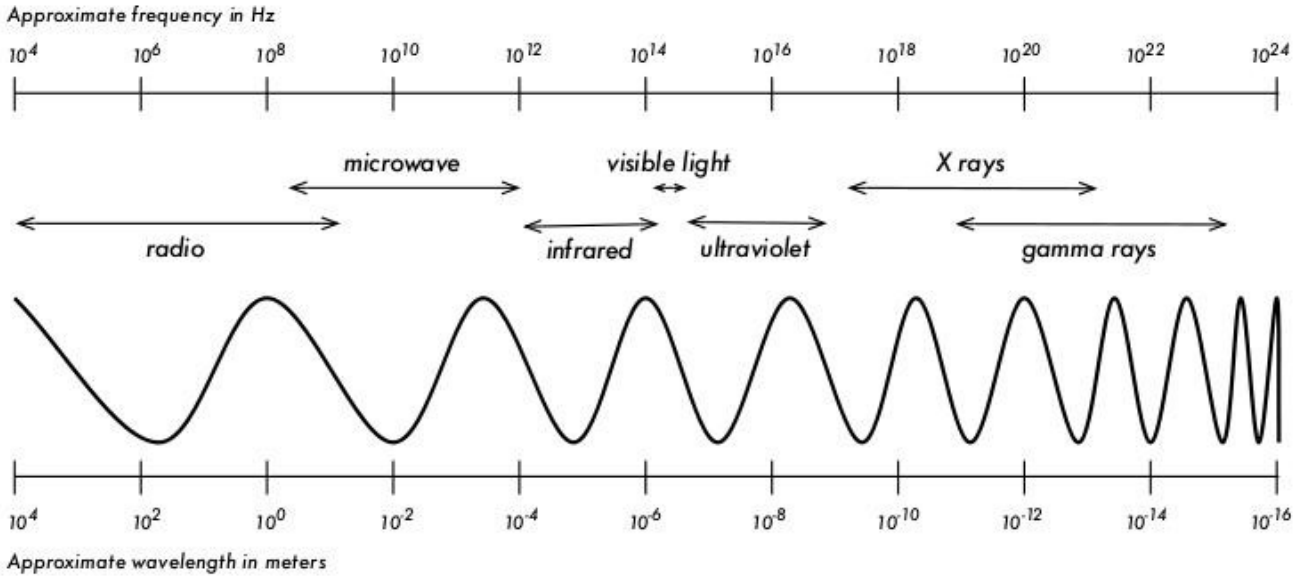
Gelombang elektromagnetik meliputi frekuensi, maupun panjang gelombang, yang sangat

lebar. Wilayah frekuensi dan panjang gelombang ini sering di sebut sebagai ***spektrum elektromagnetik.*** Bagian spektrum elektromagnetik banyak di kenali oleh manusia adalah cahaya, yang merupakan bagian spektrum elektromagnetik yang terlihat oleh mata. Cahaya berada pada kira-kira frekuensi $7.5*10^{14}$ Hz and $3.8*10^{14}$ Hz, atau kira-kira panjang gelombang 400 nm (violet/biru) sampai 800 nm (merah).

Kita juga sering kali terekspose ke wilayah spektrum elektromagnetik lainnya, termasuk ***Gelombang Arus Bolak Balik*** (listrik) pada 50/60Hz, Ultraviolet (pada frekuensi tinggi dari cahaya yang kita lihat), infrared (atau frekuensi rendah dari cahaya yang kita lihat), radiasi X-ray / roentgen, maupun banyak lagi lainnya. ***Radio*** menggunakan bagian dari spektrum elektromagnetik dimana gelombangnya dapat di bangkitkan dengan memasukan arus bolak balok ke antenna. Hal ini hanya benar pada wilayah 3 Hz sampai 300 GHz. Untuk pengertian yang lebih sempit, biasanya batas atas frekuensi akan sekitar 1GHz.

Jika kita berbicara tentang radio, maka sebagian besar orang akan berfikir tentang radio FM, yang menggunakan frekuensi sekitar 100MHz. Di antara radio dengan cahaya infrared, kita akan menemukan wilayah gelombang micro (microwave) – yang mempunyai frekuensi sekitar 1GHz sampai 300GHz, dengan panjang gelombang dari 30cm sampai 1 mm.

Penggunaan paling populer dari gelombang mikro adalah di oven microwave, yang kebetulan menggunakan frekuensi yang sama dengan frekuensi standard wireless yang akan kita gunakan. Spektrum frekuensi ini berada dalam band yang dibuat terbuka untuk penggunaan umum tanpa perlu lisensi. Di negara maju, wilayah band ini di kenal sebagai ***ISM band,*** yang merupakan singkatan dari Industrial, Scientific, and Medical. Sebagian besar dari spektrum elektromagnetik yang ada biasanya di kontrol secara ketat oleh pemerintah melalui lisensi. Lisensi frekuensi merupakan pemasukan yang lumayan bagi pemerintah. Hal ini terutama terjadi pada spektrum frekuensi yang digunakan untuk broadcasting (TV, radio) maupun komunikasi suara dan data. Di banyak negara, ISM band di alokasikan untuk digunakan tanpa perlu lisensi. Di Indonesia, berdasarkan KEPMEN Nomor 2/2005, pengunakan frekuensi 2.4GHz dapat dilakukan tanpa perlu lisensi dari pemerintah.



Gambar 2.3: Spektrum Elektromagnetik.

Frekuensi yang paling menarik untuk kita semua adalah 2.400 - 2.495 GHz, yang digunakan oleh standard radio 802.11b and 802.11g (panjang gelombang frekuensi tersebut sekitar 12.5 cm). Jenis peralatan lain yang juga sering digunakan menggunakan standard 802.11a yang beroperasi pada frekuensi 5.150 - 5.850 GHz (panjang gelombang frekuensi tersebut sekitar 5 sampai 6 cm).

Bandwidth

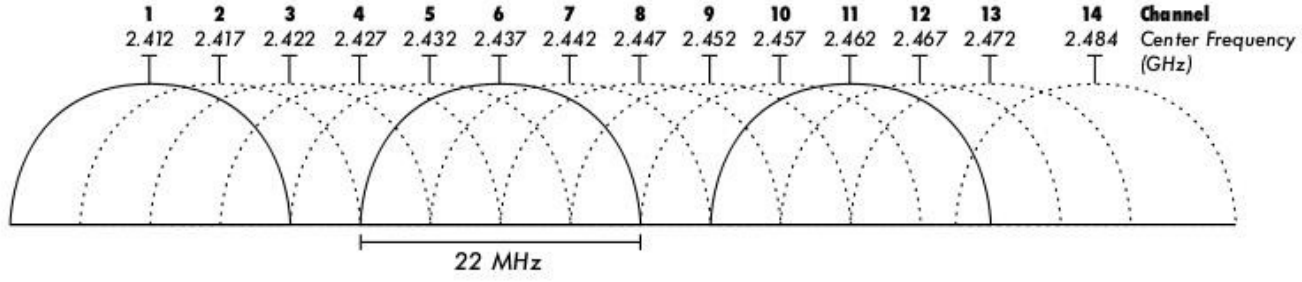
Istilah yang akan sering kita temui di fisika radio adalah ***bandwidth.*** Bandwith adalah ukuran dari sebuah wilayah / lebar / daerah frekuensi. Jika lebar frekuensi yang digunakan oleh sebuah alat adalah 2.40 GHz sampai 2.48 GHz maka bandwidth yang digunakan adalah 0.08 GHz (atau lebih sering di sebutkan sebagai 80MHz).

Sangat mudah untuk melihat bahwa bandwidth yang kita definisikan berhubungan erat dengan jumlah data yang dapat kita kirimkan di dalamnya – semakin lebar tempat yang tersedia di ruang frekuensi, semakin banyak data yang dapat kita masukan pada sebuah waktu. Istilah bandwidth kadang kala digunakan untuk sesuatu yang seharusnya di sebut sebagai kecepatan data, misalnya “Sambungan Internet saya mempunyai 1Mbps bandwidth”, artinya Internet tersebut dapat mengirimkan data pada kecepatan 1 megabit per detik.

Frekuensi dan Kanal

Mari kita lihat lebih dekat bagaimana band 2.4GHz digunakan di 802.11b. Spektrum 2.4GHz di bagi menjadi potongan kecil-kecil yang terdistribusi pada band sebagai satuan ***kanal.*** Perlu di catat bahwa lebar kanal adalah 22MHz, tapi antar kanal hanya berbeda 5MHz. Hal ini

berarti bahwa antar kanal yang bersebelahan saling overlap, dan dapat saling ber-interferensi. Hal ini dapat di representasikan secara visual di **Gambar 2.4.**



Gambar 2.4: Kanal dan frekuensi tengah untuk 802.11b.
Perlu di catat bahwa kanal 1, 6, dan 11 tidak saling overlap.

Untuk daftar lengkap kanal dan frekuensi tengahnya untuk 802.11b/g dan 802.11a, dapat di lihat di **Appendix B.**

Perilaku Gelombang Radio

Ada beberapa aturan yang sangat ampuh pada saat merencanakan pertama kali untuk jaringan nirkabel:

- Semakin panjang panjang gelombang, semakin jauh gelombang radio merambat.
- Semakin panjang panjang gelombang, semakin mudah gelombang melalui atau mengitari penghalang.
- Semakin pendek panjang gelombang, semakin banyak data yang dapat di kirim.

Aturan di atas, merupakan simplifikasi dari perilaku gelombang secara umum, mungkin akan lebih mudah di mengerti melalui contoh.

Gelombang panjang menjalar lebih jauh

Untuk daya pancar yang sama, gelombang dengan panjang gelombang yang lebih panjang cenderung untuk dapat menjalar lebih jauh daripada gelombang dengan panjang gelombang pendek. Effek ini kadang kala dapat terlihat di radio FM, jika di bandingkan jarak pancar pemancar FM di wilayah 88MHz dengan wilayah 108MHz. Pemancar dengan frekuensi yang lebih rendah cenderung untuk dapat mencapai jarak yang lebih jauh di bandingkan dengan pemancar dengan frekuensi yang tinggi pada daya yang sama.

Gelombang panjang lebih mudah melewati penghalang

Sebuah gelombang di air yang panjang gelombang-nya 5 meter tidak akan di hentikan oleh sebuah potongan kayu yang panjangnya 5 mm di air. Jika ada potongan kayu yang panjangnya 50 meter, misalnya kapal, maka potongan kayu tersebut akan terbawa oleh gelombang tersebut. Jarak sebuah gelombang dapat berjalan tergantung pada hubungan antara panjang gelombang dengan ukuran penghalang yang ada di jalur rambatan gelombang.

Lebih sulit untuk menggambarkan gelombang bergerak “menembus” objek padat, tapi hal ini merupakan salah satu hal biasa di gelombang elektromagnetik. Gelombang dengan panjang gelombang yang panjang (atau frekuensi makin rendah) cenderung untuk dapat menembus objek lebih baik di bandingkan dengan yang panjang gelombang-nya pendek (frekuensi-nya lebih tinggi).

Sebagai contoh, radio FM (88-108MHz) dapat menembus bangunan atau berbagai halangan dengan lebih mudah. Sementara yang gelombangnya lebih rendah, seperti, handphone GSM yang bekerja pada 900MHz atau 1800MHz, akan lebih sukar untuk menembus bangunan. Memang effek ini sebagian karena perbedaan daya pancar yang digunakan di radio FM dengan GSM, tapi juga sebagian karena pendek-nya panjang gelombang di sinyal GSM.

Gelombang yang pendek dapat membawa data lebih banyak

Semakin cepat gelombang berayun atau bergetar, semakin banyak informasi yang dapat dia bawa – setiap getaran atau ayunan dapat, contoh, digunakan untuk mengirimkan bit digital, '0' atau '1', 'ya' atau 'tidak'.

Ada sebuah prinsip yang dapat di lihat di semua jenis gelombang, dan amat sangat berguna untuk mengerti proses perambatan gelombang radio. Prinsip tersebut di kenal sebagai ***Prinsip Huygens,*** yang diambil dari nama Christiaan Huygens, seorang matematikawan, fisikawan, dan astronomer Belanda 1629 – 1695.

Bayangkan jika anda menggunakan sebuah tongkat kecil dan memasukan tongkat tersebut ke sebuah kolam yang airnya tenang, kemudian menyebabkan air bergoyang bahkan mungkin berdansa. Gelombang akan meninggalkan pusat dari tongkat – tempat anda memasukan tongkat – dalam bentuk lingkaran.

Jika kita perhatikan, jika ada partikel air yang bergoyang, mereka akan menyebabkan partikel tetangga-nya untuk melakukan hal yang sama dari semua pusat perubahan, maka gelombang sirkular yang baru akan di mulai. Hal ini, dalam bentuk yang sederhana, adalah prinsip Huygens. Dari terjemahan di wikipedia.org,

> *“Prinsip Huygens adalah metida analisis yang digunakan untuk masalah perambatan / propagasi gelombang di batasn medan jauh (far field). Prinsip Huygens memahami*

> *bahwa setiap titik dalam gelombang berjalan adalah pusat dari perubahan yang baru dan sumber dari gelombang yang lain, dan gelombang berjalan secara umum dapat dilihat sebagai penjumlahan dari gelombang yang muncul pada media yang bergerak. Cara pandang perambatan / propagasi gelombang yang demikian sangat membantu dalam memahami berbagai fenomena gelombang lainnya, seperti difraksi"*

Prinsip Huygens berlaku untuk gelombang radio maupun gelombang di air, maupun suara bahkan cahaya – hanya saja panjang gelombang cahaya sangat pendek sekali untuk memungkinkan manusia melihat efek Huygens secara langsung.

Prinsip ini membantu kita untuk mengerti difrasi maupun zone Fresnel, yang dibutuhkan untuk "line of sight" (LOS) maupun kenyataan bahwa kadang-kadang kita dapat mengatasi wilayah tidak "line of sight".

Mari kita melihat lebih dekat apa yang terjadi pada gelombang elektromagnetik pada saat merambat,

Absorsi / Penyerapan

Pada saat gelombang elektromagnetik menabrak sesuatu (suatu material), biasanya gelombang akan menjadi lebih lemah atau teredam. Berbanyak daya yang hilang akan sangat tergantung pada frekuensi yang digunakan dan tentunya material yang di tabrak. Kaca jendela bening transparan terhadap cahaya, sedang kaca rayband akan mengurangi intensitas cahaya yang masuk dan juga radiasi ultraviolet.

Seringkali, koefisien absorsi digunakan untuk menjelaskan efek material terhadap radiasi. Untuk gelombang mikro (microwave), ada dua (2) material utama yang menjadi penyerap, yaitu,

- **Metal.** Elektron bergerak bebas di metal, dan siap untuk berayun oleh karenanya akan menyerap energy dari gelombang yang lewat.
- **Air.** Gelombang mikro akan menyebabkan molekul air bergetar, yang pada proses-nya akan mengambil sebagian energi gelombang.[1]

Untuk kepentingan pembuatan jaringan nirkabel secara praktis, kita akan melihat metal dan air sebagai penyerap gelombang yang baik. Kita tidak mungkin dapat menembus mereka. Walaupun kalau ada lapisan air yang tipis sebagian dari daya gelombang akan dapat menembus. Lapisan air merupakan penghalang gelombang mikro, kira-kira sama dengan

1 Mitos yang banyak berkembang di masyarakat adalah air akan "beresonansi" pada frekuensi 2.4GHz oleh karena-nya digunakan 2.4GHz di microwave oven. Sebetulnya, air tidak "beresonansi" pada frekuensi tertentu. Yang ada, molekul air akan berputar dan bergetar karena adanya gelombang radio, dan panas akan muncul karena adanya daya yang tinggi dari gelombang radio pada semua frekuensi. Kebetulan saja 2.4GHz adalah frekuensi ISM yang tidak perlu lisensi, oleh karena itu secara politik merupakan pilihan yang baik untuk oven microwave.

tembok pada cahaya. Jika kita berbicara tentang air, kita harus ingat bahwa air mempunyai banyak bentuk: hujan, kabut, awan, dan banyak lagi yang harus di lalui oleh sambungan radio. Air mempunyai banyak dampak yang besar, dan dalam banyak kesempatan perubahan cuaca sangat mungkin untuk membuat sambungan radio menjadi putus.

Ada material lain yang mempunyai efek yang lebih kompleks terhadap penyerapan gelombang radio. Untuk **pohon** dan **kayu**, banyaknya penyerapan sangat tergantung pada jumlah air yang ada pada-nya. Kayu tua yang mati dan kering relatif transparan bagi gelombang mikro, sementara kayu masih masih segar dan basah biasanya akan menyerap cukup besar gelombang mikro.

Plastik dan materil yang sejenis pada umumnya tidak menyerap banyak energy radio tapi tergantung dari frekuensi dan tipe material. Sebelum kita menggunakan komponen dari plastik, misalnya, untuk memproteksi peralatan radio maupun antenna dari cuaca, sebaiknya kita ukur lebih dulu apakah material plastik yang kita gunakan akan menyerap gelombang radio sekitar frekuensi 2.4GHz. Cara paling sederhana untuk mengukur penyerapan sinyal 2.4GHz di plastik adalah dengan meletakan contoh plastik yang akan kita gunakan di oven microwave selama beberapa menit. Jika platik tersebut panas, berarti plastik tersebut menyerap energy microwave dan sebaiknya jangan digunakan untuk membuat proteksi anti cuaca untuk peralatan antenna & radio.

Terakhir, ada baiknya kita membicarakan tentang diri kita sendiri: manusia, dan tentunya juga hewan, yang sebagian besar mengandung air. Untuk jaringan nir kabel, manusia akan dilihat sebagai sebuah kantong yang besar berisi air, yang akan menyerap gelombang mikro cukup kuat. Mengarahkan sebuah akses point di kantor sehingga sinyal harus menembus banyak orang adalah kesalahan fatal dalam merancang jaringan di sebuah gedung perkantoran. Hal yang sama juga berlaku untuk hotspot, instalasi di cafe, perpustakaan maupun di instalasi luar ruangan.

Refleksi / Pantulan

Seperti hal-nya cahaya, gelombang radio juga akan terpantul jika gelombang tersebut bersentuhan dengan material yang cocok untuk itu. Untuk gelombang radio, sumber utama dari pantulan adalah metal dan permukaan air. Aturan terjadinya pantulan cukup sederhana, sudut masuknya gelombang ke permukaan akan sama dengan sudut sinyal di pantulkan. Perlu di perhatian bahwa dalam pandangan gelombang radio sebuah terali besi atau sekumpulan tiang besi yang rapat sama dengan sebuah permukaan yang padat, selama jarak antar tiang lebih kecil dari panjang gelombang radio-nya. Pada frekuensi 2.4GHz, metal grid dengan jarak satu cm akan berfungsi sama dengan panel metal.

Walaupun aturan refleksi sangat sederhana, segala sesuatu akan menjadi sangat kompleks jika kita bayangkan interior kantor dengan banyak sekali objek metal yang kecil dengan bentuk yang sangat kompleks. Hal yang sama juga terjadi di situasi pinggiran kota: perhatikan sekeliling anda di lingkungan kota coba untuk melihat semua objek metal yang

ada. Hal ini yang menyebabkan terjadinya ***efek multipath***, sinyal yang mencapai tujuan melalui jalur yang berbeda-beda, dan tentunya waktu yang berbeda-beda, yang mempunyai peranan yang sangat penting dalam jaringan nirkabel.

Permukaan air, dengan gelombang dan riak yang berubah setiap waktu, akan menyebabkan pantulan dari objek akan menjadi sulit untuk di hitung dan di perkirakan secara tepat.

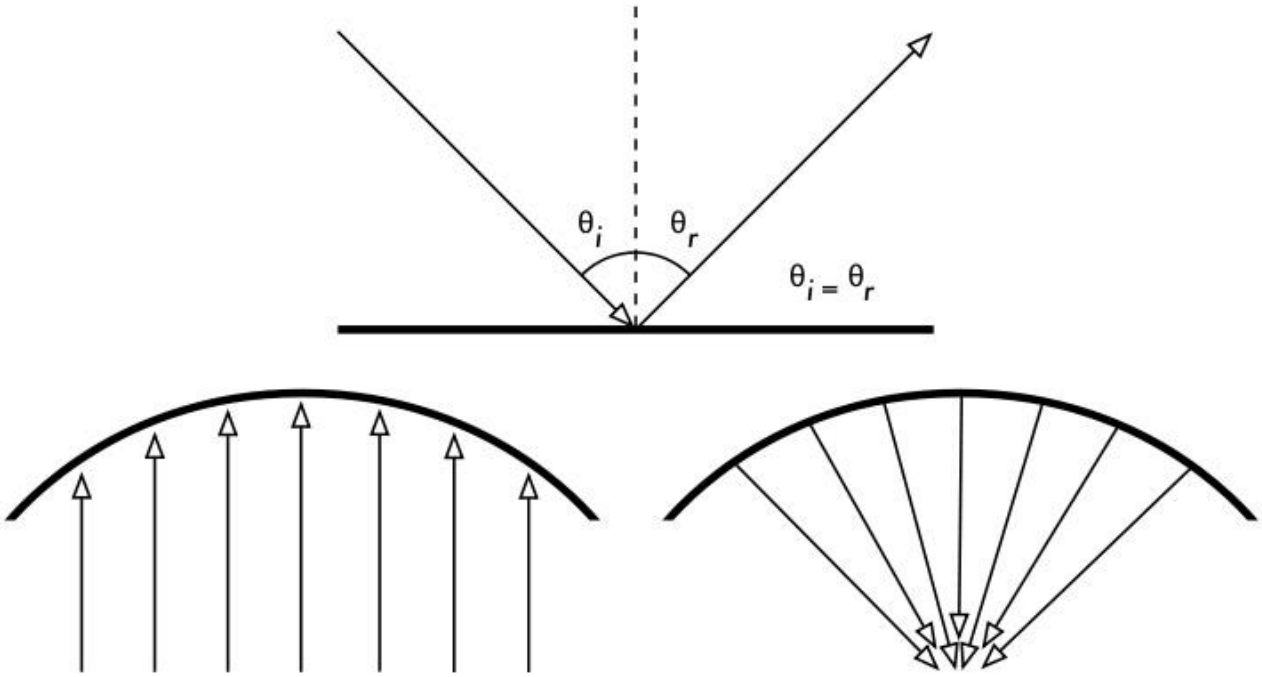


Figure 2.5: Pantulan dari gelombang radio. Sudut masuk gelombang akan sama dengan sudut dari pantulan. Sebuah bentuk parabolik akan menggunakan efek ini untuk mengkonsentrasikan gelombang radio yang tersebar di permukaannya menuju satu tujuan.

Kita juga harus menambahkan bahwa polarisasi gelombang juga ada efek-nya: gelombang dengan polarisasi yang berbeda pada umumnya akan di pantulkan secara berbeda.

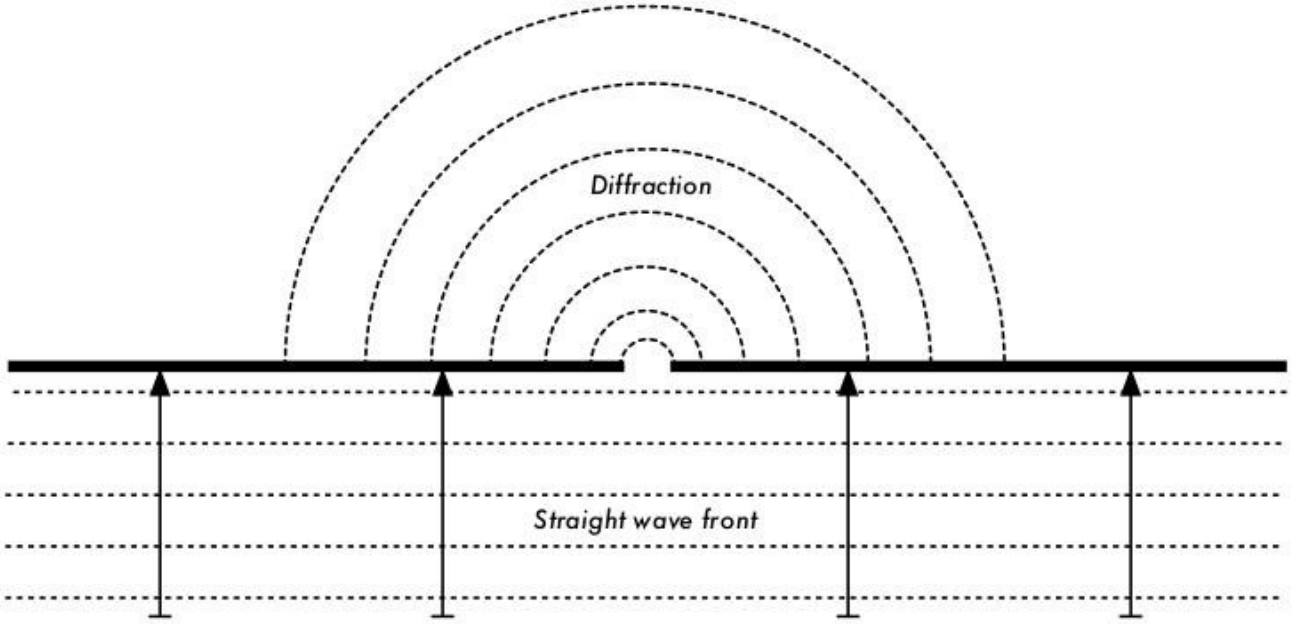
Kata dapat menggunakan refleksi untuk memperoleh keuntungan dalam membangun antena: misalnya kami menempatkan parabola besar di belakang radio pemancar / penerima yang kita gunakan untuk mengumpulkan dan membundel sinyal radio menuju titik yang kecil.

Difraksi

Difraksi akan tampak seperti pembelokan dari gelombang pada saat menabrak sebuah objek. Hal ini merupakan efek dari “gelombang akan mengitari pojokan”.

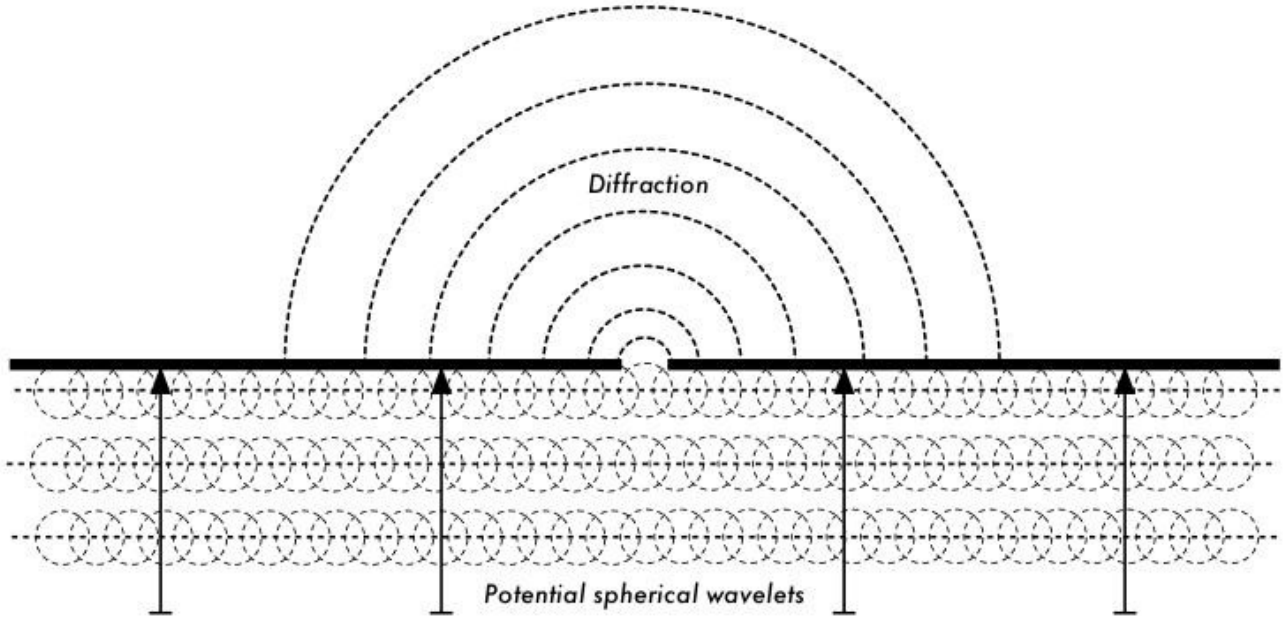
Bayangkan sebuah gelombang di air merambat dalam barisan gelombang yang lurus, seperti barisan gelombang yang sering kita lihat di pantai. Bayangkan jika kita meletakan penghalang

benda padat, misalnya pagar kayu yang rapat, yang menghalangi pergerakan gelobang. Jika kita memotong pagar tersebut, dan membuat bukaan sempit di pagar, seperti sebuah pintu yang kecil. Dari bukaan tersebut, sebuah gelombang sirkular akan di mulai, dan akan merambat ke berbagai tempat yang tidak garis lurus dari pembukaan yang kita buat, tapi juga ke lokasi-lokasi yang ada di samping pembukaan. Jika kita melihat barisan gelombang – yang mungkin saja berupa gelombang elektromagnetik – sebagai sinar yang lurus, akan susah untuk menerangkan bagaimana caranya mencapai titik-titik yang tersembunyi di balik penghalang. Dengan model barisan gelombang, maka fenomena ini menjadi masuk akal.



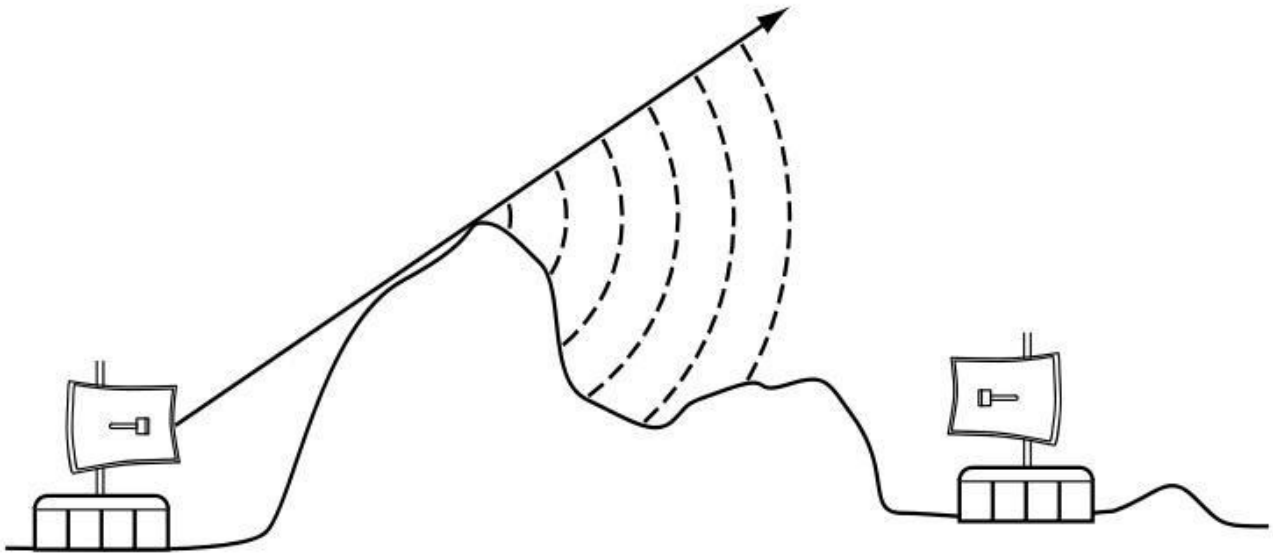
Gambar 2.6: Difraksi melalui celah sempit.

Prinsip Huygens memberikan sebuah model untuk mengerti perilaku ini. Bayangkan pada saat tertentu, semua titik di barisan gelombang menjadi titik awal dari gelombang kecil yang menyebar. Ide ini kemudian di kembangkan oleh Fresnel, apakah hal ini cukup untuk menjelaskan fenomena yang terjadi memang masih menjadi perdebatan. Akan tetapi untuk kebutuhan kita, model Huygens dapat menjelaskan effek yang terjadi dengan cukup baik.



Gambar 2.7: Prinsip Huygens

Melalui kemampuan untuk difrasi, gelombang akan “membelok” melewati pojokan atau melalui pembukaan kecil yang ada di penghalang. Untuk panjang gelombang cahaya biasanya terlalu kecil untuk manusia untuk melihat efek ini secara langsung. Pada gelombang mikro, dimana panjang gelombangnya beberapa centimeter, akan menampakan efek difraksi saat gelombang menabrak tembok, puncak gunung, dan berbagai halangan lainnya. Tampaknya seperti penghalang akan menyebabkan gelombang mengubah arah-nya dan mengitari sisi / pojokan penghalang.

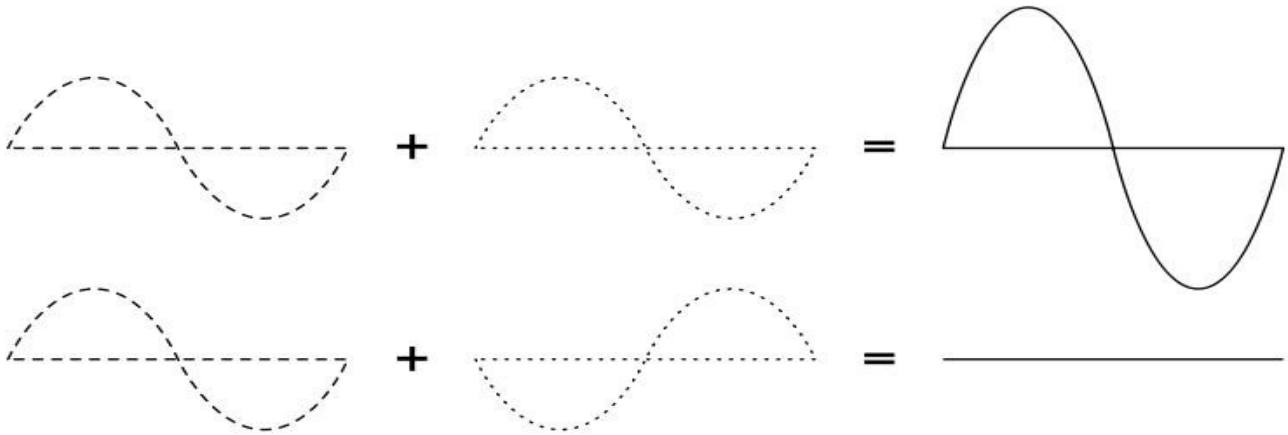


Gambar 2.8: Difraksi Melalui Puncak Gunung.

Perlu di catat bahwa difraksi akan membebani daya, energy dari gelombang yang terdifraksi akan sangat jauh lebih kecil dari barisan gelombang asal-nya. Pada aplikasi yang sangat spesifik, kita dapat mengambil keuntungan dari difraksi untuk mengatasi hambatan.

Interferensi

Jika kita bekerja dengan gelombang, satu tambah satu belum tentu sama dengan dua. Hasil-nya kadang-kadang bisa saja jadi nol.



Gambar 2.9: Interferensi Konstruktif dan Destruktif

Untuk dapat mengerti apa yang di maksud, bayangkan jika kita menggambar dua (2) gelombang sinus dan menjumlahkan amplitidanya. Pada saat saat puncak bertemu dengan puncak, maka kita akan memperoleh hasil yang maksimum (1 + 1 = 2). Hal ini disebu***t interferensi konstruktif.*** Akan tetapi, jika puncak bertemu dengan lembah, kita akan memperoleh penghilangan dari sinyal ((1 + (-)1 = 0) – ***interferensi destruktif.***

Kita sebetulnya dapat dengan mudah mencoba hal ini pada gelombang di air dan dua buah tongkat kecil untuk membuat gelombang melingkar – kita akan melihat bahwa pada tempat dimana dua gelombang bertemu, akan ada tempat yang mempunyai puncak gelombang yang tinggi sementara di beberapa tempat lainya hampir rata dan datar.

Agar seluruh barisan gelombang menjumlah atau meniadakan satu sama lain secara sempurna, kita harus mempunyai dua gelombang yang mempunyai panjang gelombang dan hubungan fasa yang tetap. Hal ini berarti jarak puncak gelombang yang satu dengan puncak gelombang yang lain tetap.

Dalam teknologi wireless, istilah interferensi biasanya digunakan untuk hal yang lebih luas, untuk gangguan dari sumber RF (Radio Frekuensi), seperti, dari kanal tetangga. Oleh karenanya, seorang wireless networker jika berbicara tentang interferensi biasanya mereka membicarakan berbagai gangguan oleh jaringan lain, atau sumber gelombang mikro lainnya. Interferensi merupakan salah satu kesulitan utama pada saat membangun sambungan wireless, terutama di lingkungan perkotaan atau ruangan yang tertutup, seperti, ruang seminar atau konferensi dimana banyak jaringan akan saling berkompetisi untuk menggunakan spektrum frekuensi yang ada.

Pada saat gelombang dengan amplituda yang sama tapi berbeda fasa saling bersilangan, gelombang akan salaing menghilangkan dan tidak akan ada sinyal yang di terima. Sering kali, gelombang akan bergabung satu sama lain membentuk gelombang bersama yang tidak berarti apa-apa sehingga tidak dapat digunakan untuk komunikasi. Teknik modulasi dan menggunakan banyak kanal akan menolong dengan masalah interferensi, tapi tidak dapat menghilangkan sama sekali.

Line of sight

Istilah ***Line of Sight,*** sering kali di singkat sebagai ***LOS,*** sangat mudah untuk di mengerti jika kita berbicara tentang cahaya tampak: Jika kita dapat melihat titik B dari titik A tidak ada penghalang antara A dan B, maka kita mempunyai Line of Sight.

Konsep Line of Sight menjadi lebih kompleks jika kita menggunakan gelombang mikro. Ingat bahwa sebagian besar karakteristik perambatan / propagasi gelombang elektromagnetik tergantung pada panjang gelombang-nya. Hal ini kira-kira mirip dengan pelebaran gelombang pada saat gelombang tersebut berjalan. Panjang gelombang cahaya sekitar 0.5 mikrometer, sementara gelombang mikro yang kita gunakan dalam jaringan wireless mempunyai panjang gelombang beberapa sentimeter. Konsekuensi-nya, pancaran gelombang mikro akan lebih

lebar – dalam bahasa yang sederhana gelombang mikro membutuhkan ruang / jalan yang lebih lebar.

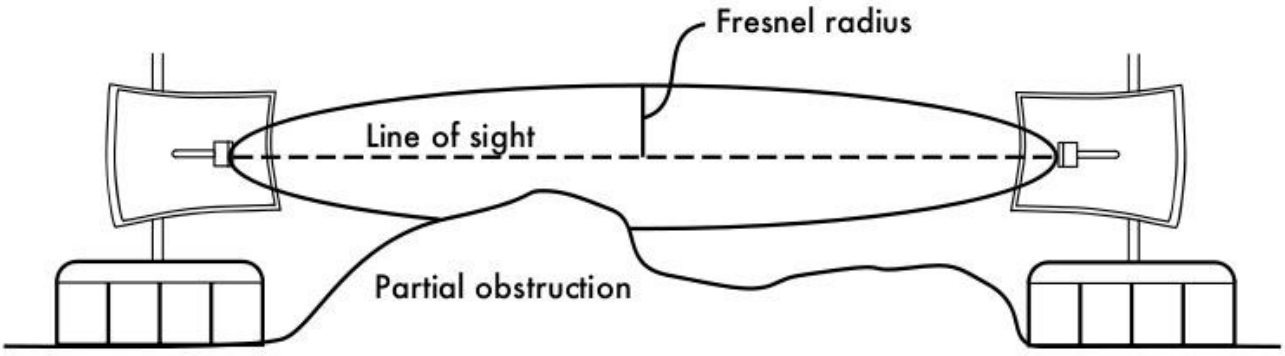
Perlu dicatat bahwa pancaran cahaya tampak juga akan melebar sama dengan dengan gelombang mikro, jika kita mengijinkan cahaya untuk bergerak cukup jauh, kita akan melihat pelebaran pancaran walaupun cahaya mempunyai panjang gelombang yang pendeik. Jika kita mengarahkan sinar laser yang sangat fokus ke bulan, maka pancaran sinar laser tersebut akan melebar sampai sekitar jari-jari 100 meter pada saat sinar laser tersebut menyentuh permukaan bulan. Kita dapat melihat dengan jelas efek ini di malam hari yang cerah dengan laser pointer, yang biasa digunakan untuk presentasi, dan keker / binokular. Kita tidak perlu mengarahkan ke bulan, coba saja arahkan ke gunung yang jauh, atau bangunan yang jauh, misalnya, tower tangki air. Kita akan melihat dengan jelas bahwa jari-jari pancaran akan bertambah dengan semakin jauh-nya jarak yang di tempuh.

Jadi Line of Sight yang kita butuhkan agar dapat terjadi sambungan wireless yang optimal antara A dan B sebetulnya lebih dari sekedar garis lurus yang tipis – tapi lebih berbentuk cerutu, atau sebuah elips. Lebar cerutu / elips tersebut di kenal sebagai konsep Fresnel zones.

Memahami Fresnel zone

Teori sesungguhnya dari Fresnel (di eja “Fray-nell”) zones sebetulnya cukup kompleks. Tapi konsep Fresnel cukup mudah untuk dipahami: kita mengetahui dari prinsip Huygens bahwa setiap titip dari barisan gelombang adalah tempat berawalnya gelombang sirkular. Kita mengetahui bahwa pancaran gelombang mikro akan melebar saat dia meninggalkan antenna. Kita juga tahu bahwa gelombang pada satu frekuensi akan berinterferensi satu sama lain.

Dari sudut yang sederhana, Teori Fresnel zone melihat garis lurus antara A dan B, dan ruang di sekitar garis lurus tersebut untuk melihat apa yang akan terjadi pada saat sinyal sampai di B. Beberapa gelombang akan merambat langsung dari A ke B, beberapa lainnya akan merambat keluar garis lurus. Akibatnya jalur yang di tempuh menjadi lebih panjang, hal ini menimbulkan perbedaan fasa antara sinyal yang langsung dengan yang tidak langsung. Pada saat perbedaan fasa adalah satu panjang gelombang, kita akan melihat interferensi konstruktur: sinyal pada dasarnya bertambah. Melihat kondisi ini dan menghitung, kita akan melihat adanya daerah lingkaran sekitar garis lurus antara A dan B yang akan berkontribusi terhadap sinyal yang tiba di B.



Gambar 2.10: Fresnel zone akan sebagian di blok pada hubungan ini, walaupun secara kasar mata tampaknya line of sight bebas hambatan.

Perlu dicatat bahwa ada banyak kemungkinan Fresnel zone, tapi kita hanya akan fokus pada wilayah / zone satu (1) saja. Jika di wilayah zone 1 terhalang oleh penghalang, seperti, pohon atau bangunan, maka sinyal yang akan tiba di ujung yang akan semakin kecil. Pada saat kita membuat hubungan wireless, kita perlu memastikan bahwa wilayah / zone tersebut bebas dari hambatan. Tentunya saja tidak ada yang sempurna, dalam jaringan wireless biasanya kita memastikan bahwa 60 persen dari radius dari Fresnel zone yang pertama bebas dari penghalang.

Berikut adalah rumus untuk menghitung Fresnel zone yang pertama:

$$r = 17.31 * \text{sqrt}((d1*d2)/(f*d))$$

dimana r adalah jari-jari dari zone tersebut dalam meter, d1 dan d2 adalah jarak dari penghalang ke kedua ujung dari sambungan wireless, d adalah jarak total sambungan dalam meter, dan f adalah frekuensi dalam MHz. Perlu di catat bahwa rumus di atas akan memberikan jari-jari / radius dari zone, bukan ketinggian dari atas tanah. Untuk menghitung ketinggian dari atas tanah, kita perlu mengurangi dari ketinggian garis lurus antara dua tower wireless yang saling berhubungan.

Sebagai contoh, mari kita menghitung jari-jari Fresnel zone yang pertama di tengah sambungan wireless yang panjangnya dua (2) km, bekerja pada frekuensi 2.437 GHz (802.11b kanal 6):

```
r = 17.31 sqrt((1000 * 1000) / (2437 * 2000))
r = 17.31 sqrt(1000000 / 4874000)
r = 7.84 meter
```

Jika kita asumsikan ke dua tower di kedua ujung tinggi-nya sepuluh (10) meter, maka Fresnel zone yang pertama akan berada sekitar 2.16 meter di atas tanah pada lokasi tengah-tengah sambungan. Berapa ketinggian bangunan pada titik tersebut jika 60% dari Fresnel zone yang

pertama harus bebas hambatan?

```
r = 0.6 * 17.31 sqrt((1000 * 1000) / (2437 * 2000))
r = 0.6 * 17.31 sqrt(600000 / 4874000)
r = 4.70 meter
```

bagikan hasil di atas ke 10 meter, kita dapat melihat bahwa sebuah bangunan dengan ketinggian 5.3 meter di tengah sambungan akan memblok sampai 40% dari Fresnel zone yang pertama. Hal ini biasanyadapat di terima, tapi untuk memperbaiki kondisi sambungan kita perlu menaikan antenna lebih tingi, atau mengubah arah sambungan untuk menghindari penghalang.

Daya

Semua gelombang elektromagnetik akan membawa enegry – kita dapat merasakan-nya pada saat kita menikmati (atau menderita) panas dari matahari. Jumlah energy yang di terima pada satu waktu tertentu di sebut ***daya.*** Daya **P** adalah kunci utama yang memungkinan sambungan wireless dapat beroperasi: kita akan membutuhkan daya minimal tertentu untuk agar sinyal yang di terima dengan baik.

Kita akan kembali ke berbagai detail tentang transmisi daya, redaman, penguatan dan sensitifitas radio di **Bab 3**. Berikut ini akan di diskusikan secara singkat bagaimana daya P di definisikan dan di ukur.

Medan listrik di ukur dalam V/m (beda potensial per meter), daya yang ada di dalam-nya setara dengan medan listrik di kuadratkan.

$$P \sim E^2$$

Secara praktis, kita dapat mengukur daya menggunakan sejenis penerima, misalnya, sebuah antenna dan voltmeter, power meter, oscilloscope atau bahkan radio / wifi card di laptop. Melihat secara langsung daya yang ada di sinyal pada dasarnya melihat kuadrat dari sinyal dalam Volt (tegangan).

Menghitung dengan dB

Teknik terpenting untuk menghitung daya adalah melakukan perhitungan dengan desibel (dB). Tidak ada teori fisika baru dibelakang dB – ini hanyalah cara yang dikembangkan agar proses perhitungan menjadi sangat sederhana.

Desibel adalah sebuah unit tanpa dimensi, yang di defisinikan berupa hubungan antara dua daya yang kita ukur. Desibel di definisikan sebagai:

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

dimana **P1** dan **P0** adalah dua nilai yang akan kita bandingkan. Biasanya dalam kasus yang kita tangani, nilai tersebut adalah daya. Mengapa desibel menjadi proses perhitungan menjadi mudah? Banyak fenomena alam terjadi dalam bentuk-bentuk exponensial. Sebagai contoh, telinga manusia akan merasakan suara dua kali suara yang lain jika suara tersebut secara fisik sepuluh kali lebih besar. Contoh lain, yang cukup dekat dengan apa yang kita akan bahas, adalah absorpsi / serapan. Misalnya ada sebuah tembok pada jalur sambungan wireless. Setiap meter dari tembok akan mengambil setengah dari sinyal yang tersedia. Hasil perhitungan akan sebagai berikut:

```
0 meter = 1 (full signal)
1 meter = 1/2
2 meter = 1/4
3 meter = 1/8
4 meter = 1/16
n meter = 1/2^n = 2^-n
```

Hal ini merupakan perilaku exponensial.

Jika kita telah mulai terbiasa dengan trik perhitungan menggunakan logaritma (log), maka segala sesuatu-nya akan menjadi lebih mudah, dari pada mengambil pangkat n, kita cukup mengalikan dengan n. Daripada mengalikan nilai, kita cukup menambahkan nilai.

Berikut adalah beberapa nilai yang sering penting untuk di ingat:

```
 +3 dB = daya dobel
 -3 dB = daya setengah
+10 dB = daya sepuluh kali lebih besar
-10 dB = daya seper sepuluh kali lebih kecil
```

Contoh lain dari unit yang tanpa dimensi adalah persen (%) yang juga digunakan dalam banyak besaran dan angka. Memang hasil pengukuran seperti meter atau gram adalah tetap, tapi unit tanpa dimensi memperlihatkan sebuah hubungan.

Lebih lanjut tentang unit tanpa dimensi dB, ada besaran relatif yang berbasis pada besaran P0 tertentu. Yang sangat relevan dengan apa yang kita akan gunakan adalah:

```
dBm  relatif ke P0 = 1 mW
dBi  relatif ke antenna isotropik yang ideal
```

Sebuah ***antenna isotropic*** adalah sebuah antenna ideal yang mendistribusikan daya secara merata ke segala arah. Antenna isotropic dapat di dekati dengan sebuah dipole, tapi sebuah antenna isotropic tidak mungkin dapat dibuat pada kenyataannya. Sebuah model antenna

isotropic sangat bermanfaat untuk menjelaskan penguatan relatif sebuah antenna di dunia nyata.

Sebuah cara yang umum digunakan untuk mengekspresikan daya adalah dalam ***miliwatt.*** Berikut adalah equivalen daya yang di ekspresikan dalam miliwatt dan dBm.

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

Fisika dalam dunia nyata

Jangan takut jika konsep dari bab ini tampaknya cukup menantang. Mengerti tentang bagaimana cara gelombang radio merambat dan berinteraksi dengan lingkungannya adalah sebuah bidang studi yang sangat kompleks. Banyak orang yang kesulitan untuk mengerti fenomena yang mereka lihat dengan mata mereka sendiri.

Pada saat ini kita harusnya sudah mengerti bahwa gelombang radio tidak merambat dalam jalur yang lurus dan terprediksi. Untuk membuat sambungan komunikasi yang andal, kita harus dapat menghubung berapa banyak daya yang harus kita berikan untuk merambat pada jarak tertentu, dan memprediksi bagaimana gelombang merambat pada jalurnya.

Ada banyak yang perlu di pelajari dari fisika radio daripada halaman yang tersedia di bab ini. Untuk informasi lebih lanjut tentang bidang yang berkembang ini, ada baiknya melihat daftar di **Appendix A.**

Bab 3 Disain Jaringan

Sebelum membeli peralatan atau menentukan hardware yang akan digunakan, kita harus mempunyai gambaran yang jelas tentang permasalahan komunikasi yang akan kita tangani. Kemunginan besar, anda membaca buku ini karena anda butuh menghubungkan kompter di jaringan untuk dapat berbagi sumber daya (resource) dan tersambungan ke jaringan global Internet.

Disain jaringan yang kita pilih untuk di implementasi harus memenuhi kebutuhan masalah komunikasi yang akan kita selesaikan. Apakah kita membutuhkan sambungan dari lokasi yang jauh ke pusat kampus? Apakah jaringan kita akan berkembang untuk menyambungkan beberapa lokasi yang jauh? Apakah komponen jaringan yang akan di install di lokasi yang tetap, atau jaringan berkembang untuk memberikan akses laptop atau berbagai peralatan yang mobile / berpindah-pindah?

Pada bab ini, kita akan mulai mereview konsep jaringan berbasis TCP/IP, yang merupakan keluarga protokol utama yang digunakan di Internet. Kita akan melihat beberapa contoh bagaimana orang membangun jaringan wireless untuk menjawab permasalahan komunikasi mereka, termasuk diagram dari struktur jaringan yang penting. Akhirnya, akan di presentasikan beberapa metoda umum untuk agar arus informasi lancar bergerak melalui jaringan yang kita buat maupun ke seluruh dunia.

Jaringan 101

TCP/IP mengacu pada keluarga protokol yang memungkinkan interaksi antar komputer terjadi pada Internet global. Dengan mengerti TCP/IP, kita dapat membuat jaringan yang dapat di skala-kan, di perbesar, atau di perkecil, ke hampir segala ukuran, dan pada akhirnya menjadi bagian dari Internet global.

Jika anda sudah cukup familiar dengan inti dari jaringan TCP/IP (termasuk pengalamatan, routing, switch, firewall dan router), anda dapat langsung melompat ke **Halaman 51** untuk **Disain Jaringan Fisik**. Selanjutnya, kita akan membahas dasar dari jaringan Internet.

Pendahuluan

Venice, Italy adalah kota yang sangat indah bagi anda untuk berkelana. Jalan-jalan di kota tersebut kira-kira seukuran jalan setapak yang menyebrangi air di ratusan tempat, dan tidak pernah menuju satu tempat melalui jalur yang lurus dan sederhana. Tukang pos di Venice menjadi seseorang yang sangat terlatih di dunia, dan biasanya hanya menspesialisasikan untuk menganter ke satu atau dua dari enam kelurahan yang ada di Venice. Hal ini menjadi

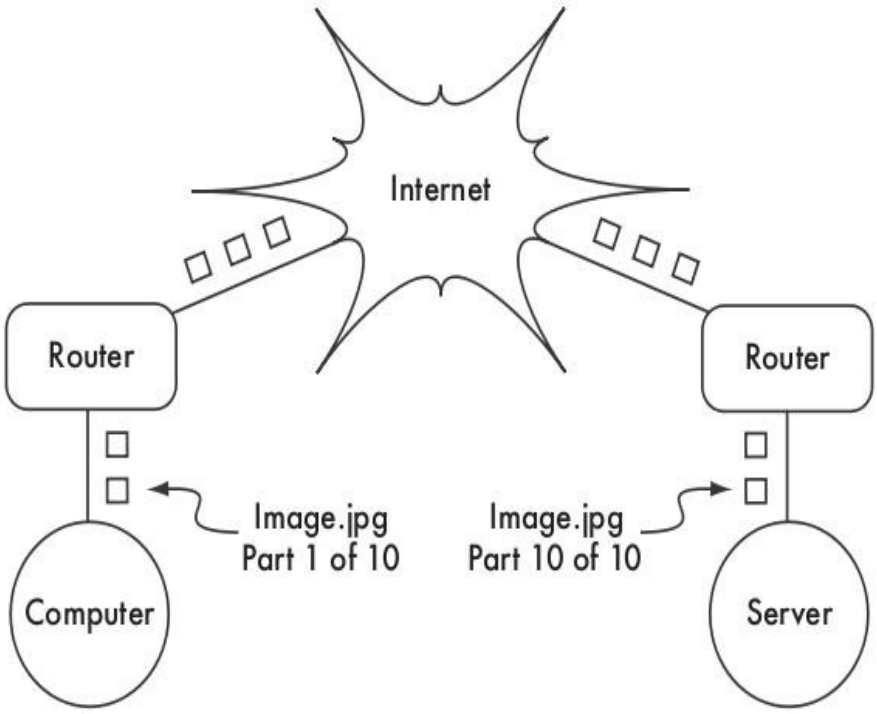
penting karena bentuk yang sangat kompleks dari kota tua. Banyak orang di Venice berpendapat bahwa mengetahui lokasi dari air dan matahari menjadi jauh lebih bermanfaat daripada nama jalan di peta.

Gambar 3.1: Jenis lain dari masker jaringan.

Bayangkan seorang turis yang kebetulan menemukan papier-mâché mask (masker kertas) sebagai suvenir, dan ingin agar masker tersebut dikirim dari studio di S. Polo, Venezia ke kantor di Seattle, USA. Hal ini tampaknya seperti suatu pekerjaan yang biasa (atau sesuatu yang sangat mudah), tapi mari kita lihat apa yang terjadi.

Pertama-tama sang seniman perlu membungkus masker ke kotak untuk pengiriman dan mengalamatkan ke kantor di Seattle, USA. Mereka kemudian memberikan kotak tersebut ke pegawai kantor pos, yang akan menempelkan formulir yang sudah di isi dan mengirimkan kotak tersebut ke pusat pemrosesan paket untuk tujuan internasional. Sesudah beberapa hari, paket akhirnya lolos dari beacukai Italia dan masuk ke penerbangan transatlantik, dan tiba di lokasi pusat pemrosesan import di Amerika Serikat. Setelah paket tersebut lolos dari beacukai Amerika Serikat, maka akan menuju pusat distribusi regional untuk wilayah utara barat Amerika Serikat, kemudian menuju pusat pemrosesan pos Seattle. Akhirnya paket akan di bawa oleh mobil box untuk pengantaran yang akan membawa-nya ke alamat yang tepat, jalan yang tepat, di RT/RW yang tepat. Seorang pegawai di kantor akan menerima paket tersebut dan memasukan ke kotak surat yang tepat. Setelah paket tersebut tiba, paket di ambil dan masker yang ditunggu-tunggupun di terima.

Pegawai kantor di Seattle tidak tahu dan tidak peduli bagaimana cara memperoleh Masker dari S. Polo, Venezia. Pekerjaannya hanya menerima paket yang tiba, dan memberikannya ke orang yang benar. Sama hal-nya, jasa pos di Venice tidak peduli bagaimana untuk mencapai jalan atau RT/RW yang tepat di Seattle. Kerja pos hanya mengambil paket dari pemrosesan lokal dan mengirimkan ke tempat pengumpulan selanjutnya dalam rantai pengiriman barang.



Gambar 3.2: Jaringan Internet. Paket dikirim antar router sampai mencapai tujuan akhir.

Proses di atas persis seperti proses routing di Internet. Sebuah berita akan di pecah / di potong menjadi banyak ***paket*** kecil-kecil, dan di beri label dengan sumber dan tujuan paket. Komputer kemudian akan mengirim paket ke ***router,*** yang kemudian menentukan kemana akan dikirim selanjutnya. Router hanya perlu mengetahui beberapa route saja, contoh, bagaimana cara mengirim ke jaringan lokal, route terbaik ke beberapa jaringan lokal, dan satu route ke arah gateway yang menghubungkan Internet yang besar. Tabel yang berisi daftar kemungkinan route di sebut ***tabel routing***. Saat paket tiba di router, alamat tujuan akan di periksa dan di bandingan dengan tabel routing di router tersebut. Jika router tidak mempunyai route yang dituju, router akan mengirimkan paket ke route yang paling cocok yang dapat di temukannya, biasanya lebih sering ke gateway Internet, melalui ***route default***. Router selanjutnya akan melakukan hal yang sama, dan seterusnya, sampai akhirnya paket tiba di tujuan.

Paket hanya mungkin melalui sistem pos internasional karena kita telah mengembangkan skema / teknik pengalamatan yang standard untuk paket. Sebagai contoh, alamat tujuan harus ditulis di muka paket, dan mencantumkan informasi penting, seperti nama yang dituju, alamat jalan, kota, negara, dan kode pos. Tanpa informasi ini, paket akan dikirim kembali ke pengirim atau hilang dalam sistem. Paket hanya mungkin berjalan melalui jaringan Internet global karena kita sepakat akan skema dan protokol yang sama untuk mengirim paket. Standard protokol komunikasi ini yang memungkinkan terjadinya pertukaran informasi dalam

skala global.

Kerjasama komunikasi

Komunikasi hanya mungkin dilakukan jika semua peserta berbicara dengan bahasa yang sama. Tapi pada saat komunikasi menjadi lebih kompleks daripada pembicaraan antara dua orang, tata cara komunikasi / protokol menjadi penting sepenting bahasa. Semua orang di sebuah auditorium berbicara bahasa Indonesia, tapi tanpa aturan untuk mengatur siapa yang berhak menggunakan mikrofon, maka komunikasi masing-masing individu ke seluruh ruangan menjadi tidak mungkin. Bayangkan sebuah auditorium sebesar dunia, penuh dengan komputer. Tanpa sekumpulan aturan / tata cara komunikasi / protokol untuk mengatur kapan dan bagaimana setiap komputer berbicara satu dengan lain, Internet akan sangat kacau karena setiap komputer akan berusaha untuk berbicara bersamaan. Manusia mengembangkan beberapa pola komunikasi untuk mengatasi masalah ini. Salah satu model yang sangat di kenal adalah ***model OSI***.

Model OSI

Standard internasional untuk Open Systems Interconnection (OSI) di definisikan dalam dokumen ISO/IEC 7498-1, yang dibuat oleh International Standards Organization dan International Electrotechnical Commission. Standard komplit-nya tersedia sebagai publikasi "ISO/IEC 7498-1:1994," yang dapat di ambil dari http://standards.iso.org/ittf/PubliclyAvailableStandards/.

Modem OSI membagi trafik jaringan menjadi beberapa l***apisan***. Setiap lapisan berdiri sendiri, tidak tergantung pada lapisan yang lain, dan masing-masing membangun berbasis pada jasa layer dibawahnya dan memberikan jasa pada lapisan di atasnya. Abstraksi antar lapisan membuatnya mudah untuk mendisain l***apisan protokol*** yang kompleks dan andal, seperti lapisan protokol ***TCP/IP***. Sebuah lapisan protokol adalah implementasi dari model komunikasi yang berlapis. Model OSI tidak mendefinisikan protokol yang digunakan di jaringan, tapi hanya mendelegasikan setiap “pekerjaan” ke sebuah lapisan yang telah di definisikan dalam urutan.

Sementara ISO/IEC 7498-1 menspesifikasikan secara detail bagaimana lapisan saling berinteraksi satu sama lain, standard ISO/IEC 7498-1 membebaskan detail implementasi kepada para pembuat. Setiap lapisan dapat di implementasikan dalam bentuk perangkat keras, terutama di lapisan bawah, atau perangkat lunak. Selama antar muka antar lapisan mengikuti standard, para peng-implementasi bebas memilih cara yang di inginkan untuk membuat lapisan protokol-nya. Hal ini berarti, sebuah lapisan yang dibuat oleh pembuat A akan dapat beroperasi degnan lapisan yang sama dari pembuat B, dengan asumsi bahwa

spesifikasi di implementasikan dan di interpretasikan dengan tepat.

Berikut adalah catatan singkat ke tujuh lapisan model jaringan OSI:

Lapisan	Nama	Penjelasan
7	Aplikasi	***Lapisan aplikasi*** adalah lapisan yang paling banyak di lihat / digunakan oleh pengguna jaringan. Pada lapisan ini interaksi dengan manusia dilakukan. HTTP, FTP, dan SMTP adalah contoh protokol di lapisan aplikasi. Manusia berada di lapisan ini dan berinteraksi dengan aplikasinya.
6	Presentasi	***Lapisan presentasi*** berurusan dengan presentasi data, sebelum data mencapai lapisan aplikasi. Pekerjaan di lapisan ini dapat berupa MIME enkoding, kompresi data, pengecekan format, pengurutan byte dsb.
5	Sesi	***Lapisan sesi*** mengatur sesi komunikasi secara logika (virtual) antara aplikasi. NetBIOS dan RPC adalah dua (2) contoh dari protokol di lapisan nomor lima.
4	Transport	***Lapisan transport*** memberikan metoda untuk mencapai jasa tertentu di sebuah node di jaringan. Contoh protokol yang bekerja pada lapisan ini adalah TCP dan UDP. Beberapa protokol yang bekerja pada lapisan ini adalah TCP dan UDP. Beberapa protokol pada lapisan transport, seperti TCP, akan memastikan bahwa semua data tiba di tujuan dengan selamat, dan akan merakit, dan memberikan ke lapisan selanjutnya dalam urutan yang benar. Sementara UDP adalah sebuah protokol “connectionless” yang biasanya digunakan untuk streaming video dan audio.
3	Jaringan	IP (Internet Protocol) adalah protokol yang sering digunakan pada ***lapisan jaringan (lapisan network).*** Lapisan ini adalah lapisan dimana proses routing terjadi. Paket akan meninggalkan sambungan jaringan lokal dan di kirim ulang ke jaringan lain. Router menjalankan fungsi ini di sebuah jaringan dengan mempunyai paling tidak dua antar muka jaringan, satu untuk setiap jaringan agar dapat saling terinterkoneksi. Node di Internet dapat dihubungi melalui alamat IP mereka yang unik secara global. Sebuah protokol di lapisan jaringan (network) yang sangat penting adalah ICMP, yang merupakan protokol khusus yang memberikan berbagai berita manajemen jaringan yang dibutuhkan untuk operasi IP yang benar. Lapisan ini kadang kala di kenal sebagai ***lapisan Internet.***
2	Data Link	Pada saat dua atau lebih node berbagi media fisik yang sama, contoh, beberapa komputer tersambung ke sebuah hub, atau sebuah ruangan yang penuh dengan peralatan wireless yang semua menggunakan kanal yang sama, maka mereka akan menggunakan ***lapisan data link*** untuk berkomunikasi satu sama lain. Contoh protokol data link yang

		sering digunakan adalah Ethernet, Token Ring, ATM, dan protokol jaringan wireless (802.11a/b/g). Komunikasi pada lapisan ini semua terjadi secara lokal, karena semua node yang tersambung pada lapisan ini berkomunikasi satu sama lain secara langsung. Lapisan ini kadang kala di kenal sebagai lapisan ***Media Access Control (MAC).*** Pada jaringan yang banyak kita gunakan menggunakan model Ethernet, node dikenali oleh ***alamat MAC*** mereka. Alamat MAC adalah nomor 48 bit yang unik yang di berikan ke semua peralatan / card jaringan pada saat dibuat.
1	Fisik	***Lapisan fisik*** adalah lapisan paling bawah pada model OSI, biasanya mengacu pada media fisik dimana komunikasi terjadi. Lapisan fisik dapat berupa kabel LAN CAT5, sekumpulan kabel fiber optik, gelombang radio, pada dasarnya medium yang dapat digunakan untuk mengirimkan sinyal. Kabel yang terpotong, fiber rusak dan kerusakan radio adalah masalah yang terjadi di lapisan fisik.

Model yang digunakan pada lapisan ini menggunakan nomor dari satu hingga tujuh, dengan nomor tujuh sebagai lapisan tertinggi. Hal ini dimaksudkan untuk menguatkan ide bahwa setiap lapisan sebetulnya di bangun, dan tergantung pada lapisan di bawahnya. Bayangkan model OSI ini sebagai sebuah bangunan, dengan fondasi di lapisan pertama, dan lapisan selanjutnya adalah lantai, dan atap pada lapisan ke tujuh. Jika kita menghilangkan salah satu lapisan, bangunan tidak akan berdiri. Hal yang sama, jika pada lantai ke empat terjadi kebakaran, maka tidak ada satu orang pun yang dapat melalui lapisan tersebut dari ke dua arah.

Tiga lapisan yang pertama (fisik, data link, dan jaringan) semua terjadi “di jaringan”. Maksudnya, semua aktifitas di lapisan ini di tentukan oleh konfigurasi dari kabel, switch, router, dan berbagai peralatan sekitar itu. Sebuah switch jaringan hanya dapat mendistribusikan paket menggunakan alamat MAC, oleh karenanya hanya perlu mengimplementasikan lapisan nomor satu dan dua saja. Sebuah router sederhana akan me-route-kan paket hanya menggunakan alamat IP mereka, oleh karenanya router perlu mengimplementasikan lapisan nomor satu hingga nomor tiga. Sebuah Web server atau kompuetr laptop menjalankan aplikasi, oleh karenanya harus mengimplementasikan ke tujuh lapisan. Beberapa router yang canggih dapat menjalakan lapisan ke empat atau di atasnya, untuk dapat mengambil keputusan berdasarkan isi informasi yang ada di lapisan yang lebih tinggi dalam sebuah paket, seperti nama dari situs web, atau attachment dari sebuah e-mail.

Model OSI diakui secara internasional, dan secara umum di akui sebagai model jaringan yang lengkap. Model OSI memberikan kerangka bagi pabrikan dan pembuat protokol jaringan yang akan digunakan di peralatan jaringan yang akan berinteroperasi dari semua tempat di dunia.

Dari perspektif seorang insinyur jaringan atau troubleshooter, model OSI akan tampak terlalu

kompleks. Khususnya, bagi orang yang membangun dan memperbaiki jaringan TCP/IP sangat jarang menangani masalah di lapisan Sesi dan Presentasi. Untuk sebagian besar pembuat jaringan Internet, model OSI bisa disederhanakan ke dalam lima lapisan saja.

Model TCP/IP

Tidak seperti model OSI, model TCP/IP bukan internasional standard dan definisinya dapat berbeda-beda. Namun demikian, sering dipakai sebagai model praktis untuk mengerti dan mencari kesalahan dalam jaringan Internet. Mayoritas Internet memakai TCP/IP, dan oleh sebab itu kami bisa membuat beberapa asumsi tentang jaringan-jaringan yang membuat mereka lebih mudah untuk mengerti. Model TCP/IP dari jaringan digambarkan dalam lima lapisan berikut,

Lapisan	Nama
5	Aplikasi
4	Transport
3	Internet
2	Data Link
1	Fisik

Dari sisi model OSI, lapisan ke lima hingga ke tujuh tergabung menjadi lapisan paling atas (lapisan aplikasi). Sementara empat lapisan yang pertama di kedua model identik. Banyak teknisi jaringan berfikir bahwa segalanya di atas lapisan empat "hanya data" yang berubah-ubah dari aplikasi ke aplikasi. Karena ketiga lapisan pertama interoperable di antara seluruh pembuat peralatan, dan lapisan ke empat bekerja di antara semua mesin yang memakai TCP/IP, dan semua di atas lapisan ke empat cenderung untuk digunakan di aplikasi yang spesifik, hal ini menyederhanakan model yang yang bekerja pada saat membuat dan mencari permasalahan di jaringan TCP/IP. Kami akan memakai model TCP/IP saat membicarakan jaringan di buku ini.

Model TCP/IP dapat dibandingkan dengan orang yang mengantarkan surat ke sebuah bangunan di pusat kota. Orang terlebih dulu perlu menggunakan jalan (lapisan Fisik), meperhatikan lalu-lintas lain di jalan (lapisan Data Link), belok di tempat yang benar untuk meneruskan perjalanan ke jalan lain dan tiba di alamat yang benar (lapisan Internet), pergi ke lantai dan kamar yang benar (lapisan Transport), dan akhirnya memberikannya kepada seorang resepsionis yang bisa mengambil surat tersebut (lapisan Lamaran). Saat surat di berikan kepada resepsionis, pengatar bebas untuk kembali. Kelima lapisan dengan mudah bisa diingat dengan memakai pembantu ingatan “Please Don't Look In The Attic,” yang merupakan singkatan untuk “Physical / Data Link / Internet / Transport / Application.”

Protokol Internet

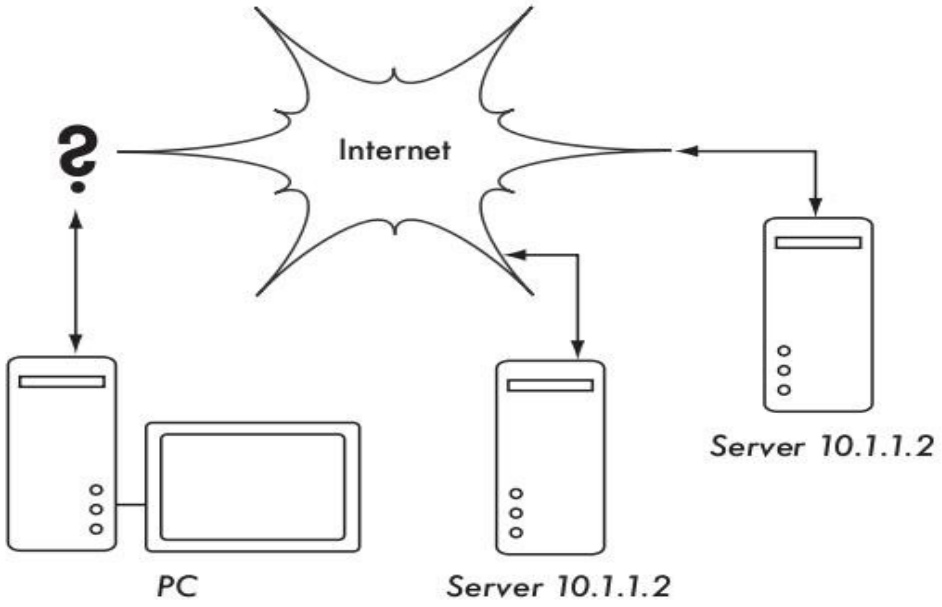
TCP/IP adalah tumpukan protokol yang sangat banyak digunakan di Internet global. Akronim TCP/IP mempunyai arti ***Transmission Control Protocol (TCP)*** dan ***Protokol Internet (IP),*** tetapi sebetulnya merujuk pada keluarga protokol komunikasi terkait. TCP/IP juga dianggap sebagai ***sekumpulan protokol Internet***, dan beroperasi pada lapisan ke tiga dan ke empat pada model TCP/IP.

Pada diskusi ini, kami akan memfokuskan pada protokol IP versi empat (IPv4) yang sekarang ini merupakan protokol yang paling banyak digunakan di Internet.

Pengalamatan IP

Di jaringan IPv4, alamat IP mengunakan nomor sebanyak 32 bit, biasanya ditulis sebagai nomor empat 8-bit di ungkapkan dalam bentuk desimal dan terpisah oleh titik. Contoh alamat IP adalah 10.0.17.1, 192.168.1.1, atau 172.16.5.23. Jika anda memerinci setiap alamat IP mungkin, alamat IP akan mencakup dari 0.0.0.0 sampai 255.255.255.255. Ini menghasilkan jumlah total sebanyak lebih dari empat milyar alamat IP yang mungkin (255 x 255 x 255 x 255 = 4.228.250.625); walaupun banyak dari alamat tersebut di reserved untuk maksud khusus dan tidak digunakan pada mesin / komputer. Masing-masing alamat IP dapat digunakan sebagai penunjuk yang unik untuk membedakan satu mesin dengan mesin lain di jaringan.

Jaringan yang saling tersambung harus menyetujui rencana pengalamatan IP. Alamat IP harus unik dan tidak digunakan di komputer lain di Internet; jika tidak, router tidak akan tahu bagaimana cara terbaik untuk mengarahkan paket ke mereka. Alamat IP dialokasikan oleh pusat autoritas penomoran yang menyediakan metode penomoran yang konsisten dan masuk akal. Hal ini untuk menjamin tidak ada duplikasi alamat yang digunakan pada jaringan berbeda. Authoritas penomoran akan mengalokasikan sebuah blok alamat berurut dalam jumlah besar kepada pemegang authoritas yang lebih kecil, yang pada gilirannya mengalokasikan blok berurutan yang lebih kecil dalam blok-nya pada yang authoritas lain-nya, atau kepada pelanggan mereka. Kelompok-kelompok alamat ini dianggap sub-jaringan, atau biasa di singkat ***subnet***. Subnet besar dapat dibagi lagi menjadi subnet yang lebih kecil. Sekelompok alamat yang saling terkait biasanya di rujuk sebagai ***ruang / wilayah alamat (address space).***



Gambar 3.3: Tanpa alamat IP yang unik, routing global yang tidak ambigu adalah. Jika komputer meminta halaman Web dari 10.1.1.2, akan mencapai server yang mana?

Subnet

Dengan memakai ***masker subnet / subnet mask*** (juga disebut ***masker jaringan***, atau ***netmask***) ke sebuah alamat IP, anda secara logis dapat mendefinisikan sebuah mesin atau jaringan tempat mesin tersebut berada. Secara tradisional, masker subnet diungkapkan menggunakan bentuk titik desimal, seperti alamat IP. Misalnya, 255.255.255.0 adalah sebuah netmask yang sering digunakan. Anda akan menemukan notasi ini dipakai waktu mengkonfigurasi antar muka jaringan, membuat rute, dll. Akan tetapi, masker subnet lebih ringkas diungkapkan menggunakan ***notasi CIDR,*** yang dengan sederhana memerinci jumlah bit di masker setelah tanda slash (/). Dengan demikian, 255.255.255.0 dapat di sederhanakan sebagai /24. CIDR adalah kependekan dari ***Classless Inter-Domain Routing,*** dan di definisikan di RFC15181[2].

Masker subnet menentukan ukuran sebuah jaringan. Menggunakan /24 netmask, 8 bit digunakan untuk mengalamati mesin (32 bit total - 24 bit netmask = 8 bit untuk mesin). Hal ini menghasilkan 256 alamat mesin yang mungkin (2^8 = 256). Berdasarkan kesepakatan, nilai pertama diambil sebagai ***alamat jaringan / network address*** (.0 atau 00000000), dan nilai terakhir di ambil sebagai ***alamat broadcast / broadcast address*** (,255 atau 11111111). Hal

2 RFC kependekan dari Request For Comments. RFC adalah sebuah serial dokumen bernomor yang dipublikasikan oleh Masyarakat Internet (*Internet Society*) yang mendokumentasikan ide dan konsep yang berhubungan tentang teknologi Internet. Tidak semua RFC berupa standard. RFC dapat dilihat secara online di http://rfc.net/

ini menyisakan 254 alamat yang dapat dibagi untuk mesin di jaringan ini..

Masker subnet beroperasi dengan melakukan operasi logik AND sampai jumlah sebanyak 32 bit nomor IP. Di bilangan biner notasi, bit "1" di mask menunjukkan bagian alamat jaringan, dan bit "0" menunjukkan bagian alamat mesin. Logik AND dilakukan dengan membandingkan dua bit. Hasil "1" diperoleh jika kedua bit yang dibandingkan ialah “1”. Jika tidak maka hasilnya adalah “0”. Berikut adalah semua hasil yang mungkin dari pembandingan AND antara dua bit.

Bit 1	Bit 2	Hasil
0	0	0
0	1	0
1	0	0
1	1	1

Untuk mengerti bagaimana netmask digunakan ke alamat IP, kita lebih baik terlebih dulu mengubah setiap angka ke biner. Netmask 255.255.255.0 di biner berisi dua puluh empat "1" bit:

```
255     255     255     0
11111111.11111111.11111111.00000000
```

Saat netmask tersebut digabungkan dengan alamat IP 10.10.10.10, kami bisa melakukan operasi logik AND pada masing-masing bit untuk menentukan alamat jaringan.

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

Hal ini menghasilkan jaringan 10.10.10.0/24. Jaringan ini terdiri atas mesin 10.10.10.1 sampai 10.10.10.254, dengan 10.10.10.0 sebagai alamat jaringan dan 10.10.10.255 sebagai alamat broadcast.

Masker subnet tidak terbatas hanya ke seluruh octets. Seseorang bisa menetapkan masker submask seperti 255.254.0.0 (atau /15 CIDR). Ini adalah blok alamat yang besar, berisi 131.072 alamat, dari 10.0.0.0 hingga 10.1.255.255. Bisa lebih jauh dibagi lagi, misalnya menjadi 512 subnet sebanyak 256 alamat masing-masing. Yang pertama akan menjadi 10.0.0.0-10.0.0.255, lalu 10.0.1.0-10.0.1,255, dan seterusnya hingga 10.1.255.0-10.1.255.255. Sebagai alternatif, bisa juga di bagi dalam 2 blok dengan 65.536 alamat, atau 8192 blok dengan 16 alamat, atau berbagai cara lainnya. Bisa juga di bagi dalam campuran ukuran blok yang berbeda, sepanjang tidak ada yang tumpang-tindih, dan masing-masing

berlaku subnet yang ukurannya adalah pangkat dua.

Walau banyak netmask yang mungkin, netmask yang biasa digunakan adalah:

CIDR	Desimal	Jumlah Mesin
/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

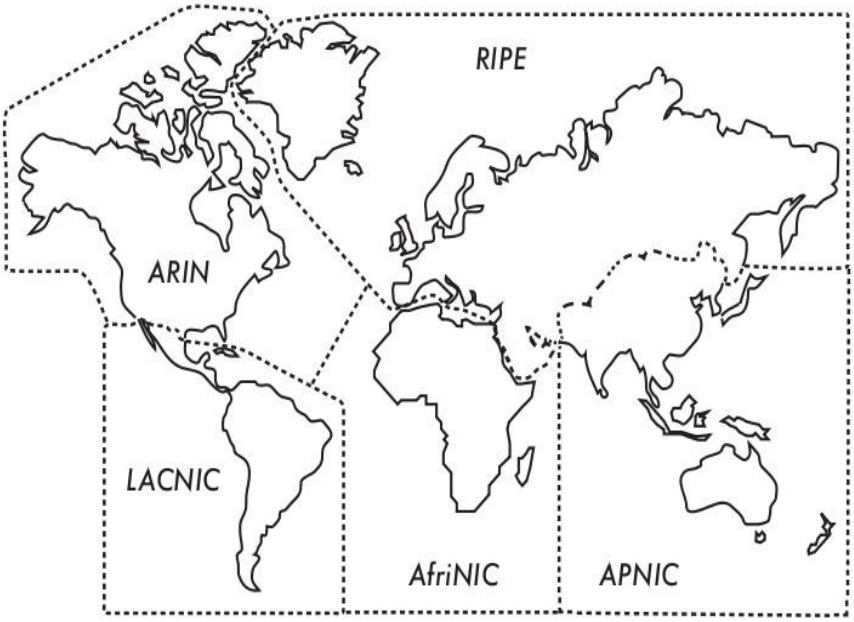
Dengan setiap penurunan di nilai CIDR maka jumlah alamat IP menjadi dobel. Ingat bahwa bahwa ada dua alamat IP dalam masing-masing jaringan yang gunakan untuk alamat network dan broadcast, dan tidak dapat digunakan untuk alamat mesin.

Ada tiga netmask yang mempunyai nama istimewa. Jaringan /8 (dengan netmask 255.0.0.0) mendefinisikan jaringan ***kelas A***. /16 (255.255.0.0) adalah ***Kelas B***, dan /24 (255.255.255.0) di sebut ***Kelas C.*** Nama ini telah digunakan jauh sebelum ada notasi CIDR, tetapi masih sering digunakan karena alasan sejarah saja.

Alamat IP Publik

Apakah anda pernah bertanya-tanya siapa yang menguasai alokasi alamat IP? ***Alamat IP secara global*** dialokasikan dan di distribusikan oleh ***Regional Internet Registrar (RIR)*** ke ISP. ISP kemudian memberikan blok IP yang lebih kecil kepada pelanggan mereka sesuai keperluan. Sebenarnya semua pemakai Internet mendapatkan alamat IP mereka dari ISP.

Ke-4 milyar alamat IP yang tersedia di atur oleh ***Internet Assigned Number Authority (IANA,*** http://www.iana.org/). IANA sudah membagi alamat IP ini ke dalam subnet besar, biasanya subnet /8 dengan 16 juta alamat masing-masing. Subnet ini di delegasikan ke satu dari lima Regional Internet Registrar (RIR) yang diberi kekuasaan untuk wilayah geografis yang besar.



Gambar 3.4: Otoritas untuk mengalokasi alamat Internet IP di delegasikan ke lima Regional Internet Registrar.

Ke lima RIR adalah:

- 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/)

ISP anda akan memperoleh alokasi alamat IP yang dapat di routing secara global dari kumpulan IP yang di berikan kepada ISP tersebut oleh RIR. Sistem pencatatan memastikan bahwa alamat IP tersebut tidak digunakan di jaringan manapun di dunia. Sesudah alokasi IP address disetujui, maka sangat mungkin untuk mengirim paket antar jaringan dan berpartisipasi di jaringan Internet global. Proses untuk mengirim paket antar jaringan di sebut ***routing.***

Alamat IP statik

Alamat IP statik adalah sebuah pemberian alamat yang tidak pernah berubah. Alamat IP statik penting karena server memakai alamat IP ini dan mungkin mempunyai pemetaan DNS

menunjuk kepada server tersebut, dan biasanya memberikan informasi kepada mesin lain (seperti email server, web server, dll.). Blok alamat IP statik mungkin diberi oleh ISP anda, baik dengan permintaan atau otomatis bergantung pada cara anda hubungan ke Internet.

Alamat IP dinamik

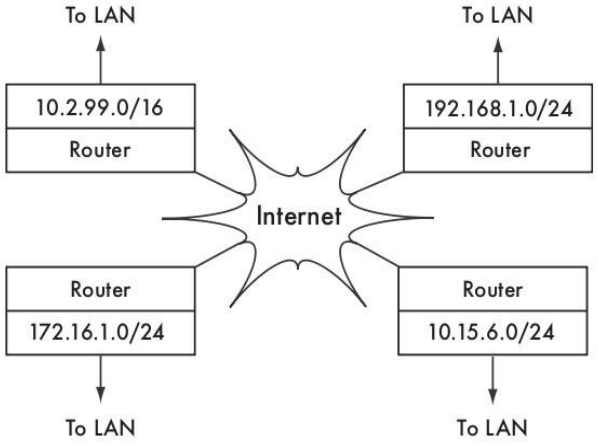
Alamat IP dinamik diberikan oleh ISP untuk node yang tidak permanen terhubung ke Internet, seperti komputer di rumah komputer yang menggunakan sambungan *dial-up*. Alamat IP dinamik diberi secara otomatis menggunakan protokol ***Dynamic Host Configuration Protocol (DHCP)***, atau ***Point-to-Point Protocol (PPP)***, bergantung pada tipe sambungan Internet. Node yang menggunakan DHCP terlebih dulu meminta alamat IP dari jaringan, dan otomatis mengkonfigurasi antar muka jaringannya. Alamat IP bisa diberi secara acak dari sebuah kumpulan alamat IP dari ISP anda, atau mungkin diberi menurut sebuah kebijakan. Alamat IP yang diberi oleh DHCP berlaku untuk waktu yang ditetapkan (dikenal sebagai ***waktu sewa / leased time***). Node harus memperbarui sewa DHCP sebelum waktu sewa berakhir. Segera setelah memulai lagi, node mungkin menerima alamat IP yang sama atau yang berbeda dari kumpulan alamat IP yang tersedia.

Alamat dinamik cukup populer diantara Internet Servis Provider, karena memungkinkan mereka memakai lebih sedikit alamat IP daripada jumlah total pelanggan mereka. Mereka hanya memerlukan alamat bagi masing-masing pelanggan yang **aktif di suatu saat.** Alamat IP yang dapat di routing secara global membutuhkan biaya, dapat dihancurkan secara global IP berharga uang, dan beberapa authoritas untuk alokasi alamat (seperti RIPE, RIR dari Europa) sangat keras dalam penggunaan alamat IP untuk ISP. Memberi alamat IP secara dinamik memungkinkan ISP untuk menghemat uang, dan mereka sering akan meminta tambahan yuang ke pelanggan yang meminta alamat IP statik.

Alamat IP Private

Kebanyakan jaringan private tidak membutuhkan jatah dari alamat IP publik yang dapat di routing secara global untuk setiap komputer di organisasi. Khususnya, komputer yang bukan server publik tidak perlu memperoleh alamat yang dapat dihubungi dari Internet publik. Sebuah organisasi biasanya memakai alamat IP dari wilayah alamat ***IP private*** untuk mesin di jaringan internal.

Saat ini ada tiga blok alamat private yang dialokasikan oleh IANA: 10.0.0.0/8, 172.16.0.0/12, dan 192.168.0.0/16. Yang ini didefinisikan di RFC1918. Alamat ini tidak dimaksudkan untuk diarahkan di Internet, dan biasanya unik hanya dalam organisasi atau kelompok organisasi yang pilih untuk mengikuti skema penomoran yang sama.



Gambar 3.5: RFC1918 alamat private mungkin dipakai dalam organisasi, dan tidak dirouting ke Internet global.

Jka anda pernah bermaksud menghubungkan jaringan private yang menggunakan alamat IP berdasarkan RFC1918, pastikan supaya memakai alamat unik di semua jaringan. Misalnya, anda mungkin memecah alamat 10.0.0.0/8 menjadi beberapa jaringan Kelas B (10.1.0.0/16, 10.2.0.0/16, dll.). Sebuah blok bisa dialokasikan berdasarkan lokasi fisiknya (kampus utama, cabang, kantor lapangan satu, kantor lapangan dua, asrama, dan semacamnya). Administrator jaringan di masing-masing lokasi kemudian bisa memerinci jaringan lebih jauh ke dalam beberapa jaringan Kelas C (10.1.1.0/24, 10.1.2.0/24, dll.) atau ke dalam blok ukuran logik lain-nya. Di masa mendatang, sebaiknya jaringan yang akan berhubungan (baik menggunakan sambungan fisik, sambungan wireless, atau VPN), maka semua mesin harus dapat dicapai dari titik yang mana pun di jaringan tanpa perlu berikan nomor ulang ke peralatan jaringan.

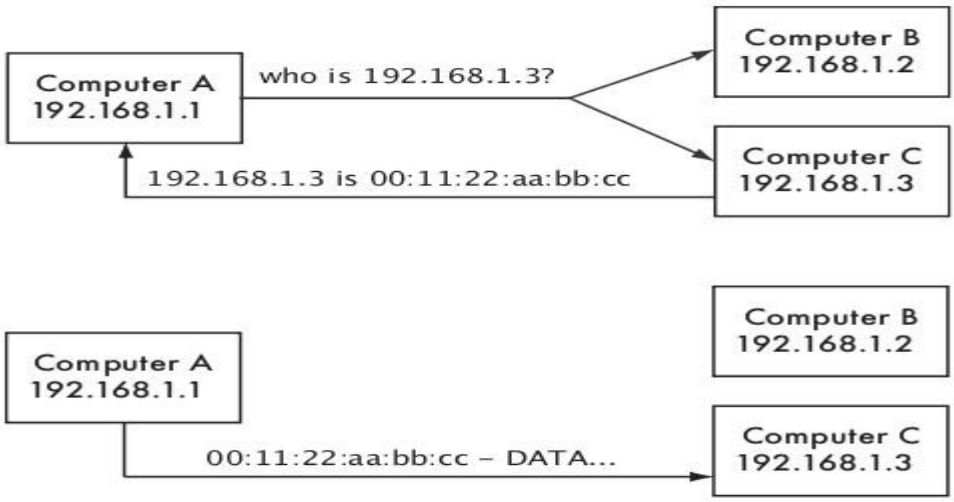
Beberapa Internet provider mungkin mengalokasi alamat private daripada alamat publik ke pelanggan mereka, walaupun ini mempunyai kerugian yang serius. Karena alamat ini tidak bisa diarahkan dari Internet, komputer yang mereka pakai bukan merupakan "sebagian" Internet, dan tidak secara langsung dapat di capai dari Internet. Untuk membolehkan mereka berkomunikasi dengan Internet, alamat private mereka harus diterjemahkan ke alamat publik. Proses translasi ini dikenal sebagai ***Network Address Translation (NAT)***, dan biasanya dilakukan di gateway / pintu gerbang antara jaringan private dan Internet. Kami akan melihat lebih dalam tentang NAT di **Halaman 43.**

Routing

Bayangkan sebuah jaringan dengan tiga buah mesin: A, B, dan C. Mereka menggunakan alamat IP berikut 192,168,1,1, 192,168,1,2 dan 192,168,1,3. Mesin tersebut merupakan bagian dari jaringan /24, masker network yang digunakan adalah 255.255.255.0).

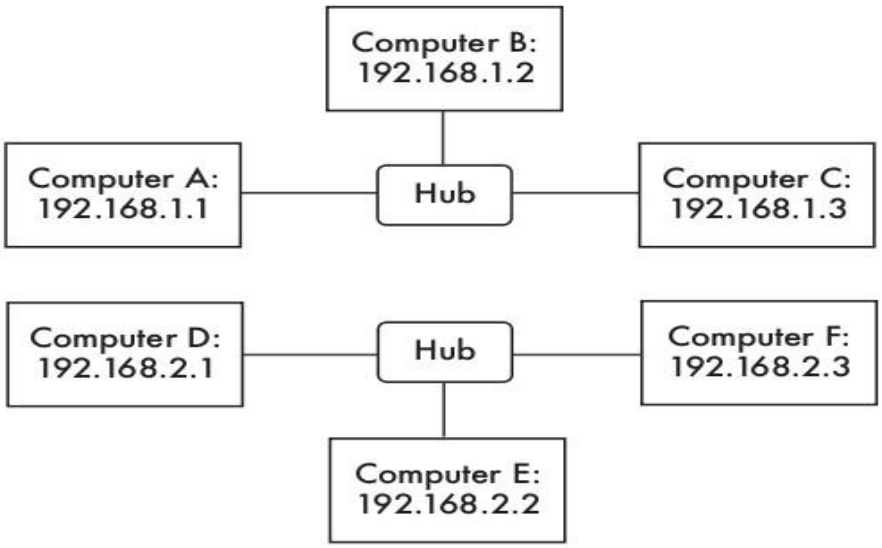
Bagi dua mesin berkomunikasi di jaringan lokal, mereka harus menentukan alamat MAC masing-masing. Sangat mungkin secara manual mengkonfigurasi setiap mesin dengan sebuah tabel yang memetakan dari alamat IP ke alamat MAC, tapi biasanya ***Address***

Resolution Protocol (ARP) digunakan untuk menentukan pemetaan secara automatis.



Gambar 3.6: Computer A ingin mengirimkan data ke 192.168.1.3. Tetapi terlebih dulu harus meminta kepada seluruh jaringan untuk memperoleh alamat MAC yang di tanggapi oleh 192.168.1.3.

Jika digunakan ARP, mesin A akan menanyakan ke semua mesin secara broadcast, “Siapa yang mempunyai alamat MAC bagi alamat IP 192.168.1.3?" Waktu mesin C melihat permohonan ARP untuk alamat IP-nya sendiri, mesin C menjawab dengan alamat MAC-nya.



Gambar 3.7: Dua jaringan IP yang terpisah.

Perhatikan sekarang jaringan lain dengan 3 mesin, D, E, dan F, dengan alamat IP 192.168.2.1, 192.168.2.2, dan 192.168.2.3. Ini adalah jaringan /24 lain, tetapi tidak satu keluarga dengan jaringan di atas. Ke tiga mesin dapat mencapai satu sama lain secara langsung (terlebih dulu mempergunakan ARP untuk memetakan alamat IP ke dalam alamat MAC, dan mengirim paket ke alamat MAC tersebut). Sekarang akan kami tambah mesin G. Mesin G mempunyai dua kartu jaringan (*network card*) yang tersambung ke masing-masing jaringan. Kartu jaringan yang pertama menggunakan alamat IP 192.168.1.4, dan yang lain menggunakan 192.168.2.4. Mesin G tersambung secara lokal ke kedua jaringan, dan dapat mengarahkan paket di antara jaringan tersebut.

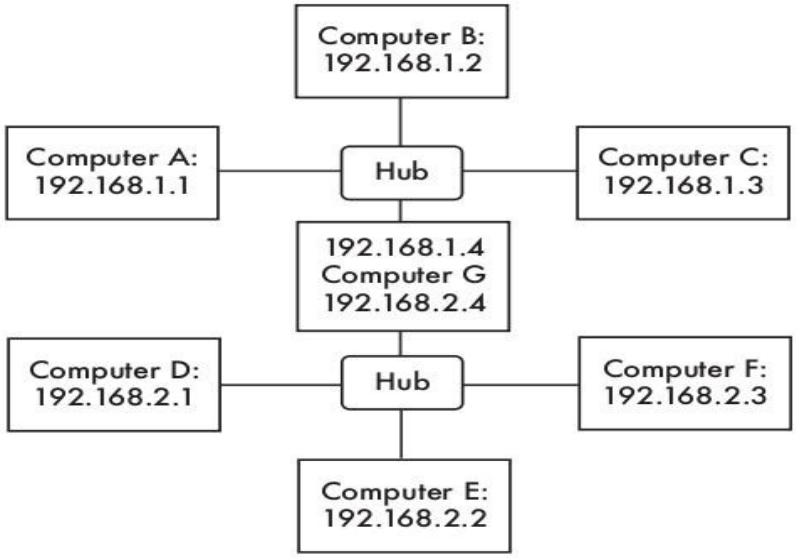
Tetapi bagaimana jika mesin A, B, dan C ingin menghubungi mesin D, E, dan F? Mereka perlu menambahkan rute untuk mencapai jaringan yang lain melalui mesin G. Sebagai contoh, mesin A-C akan menambahkan rute melalui 192.168.1.4. Di Linux, hal ini dapat dicapai menggunakan perintah berikut:

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

... dan mesin D-F perlu menambahkan perintah berikut:

ip route add 192.168.1.0/24 via 192.168.2.4

Hasilnya diperlihatkan di **Gambar 3.8.** Perhatikan bahwa rute ditambahan via alamat IP dari mesin G yang mempunyai hubungan lokal ke masing-masing jaringan. Host A tidak mungkin menambahkan rute via 192.168.2.4, meskipun secara fisik berada pada mesin yang sama sebagai 192.168.1.4 (mesin G), karena IP tersebut tidak berhubungan secara lokal.

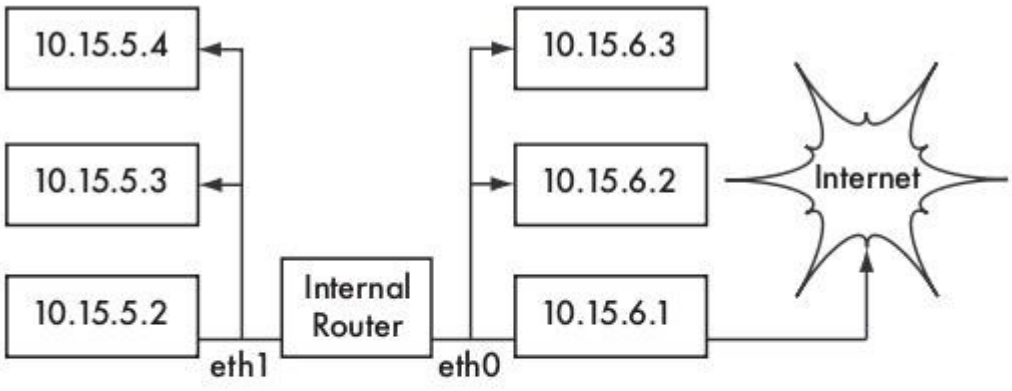


Gambar 3.8: Mesin G berfungsi sebagai router antara dua jaringan.

Rute mengatakan kepada Sistem Operasi bahwa jaringan yang diinginkan tidak terdapat pada jaringan yang terhubung lokal secara langsung, dan harus ***menyampaikan (memforward)*** trafik melalui router tertentu. Jika mesin A ingin mengirim paket ke mesin F, terlebih dulu akan mengirimkan paket tersebut ke mesin G. Mesin G kemudian akan mencari mesin F di tabel routing, dan melihat apakah ada sambungan secara langsung ke jaringan tempat mesin F berada. Akhirnya, mesin G akan memetakan alamat hardware (MAC) dari mesin F, dan mengirim paket tersebut ke situ.

Ini adalah contoh routing yang sangat sederhana, di mana tujuan adalah hanya satu hop jauhnya dari sumber. Saat jaringan menjadi lebih komplek, banyak ***hop*** yang mungkin perlu dilintasi untuk sampai di tujuan terakhir. Karena tidak praktis untuk setiap mesin di Internet untuk mengetahui rute kepada setiap mesin lain, kami memakai sebuah routing yang dikenal sebagai ***rute default*** (juga di kenal sebagai ***gateway default***).

Saat router menerima paket yang ditujukan untuk jaringan yang tidak ada rute secara jelas, paket akan disampaikan ke gateway default. Gateway default biasanya merupakan rute terbaik dari jaringan anda, biasanya di arah anda ISP. Contoh dari sebuah router yang menggunakan gateway default di tampilkan pada **Gambar 3.9.**




```
Routing table for internal router:

Destination     Gateway     Genmask         Flags  Metric  Iface
10.15.5.0       *           255.255.255.0   U      0       eth1
10.15.6.0       *           255.255.255.0   U      0       eth0
default         10.15.6.1   0.0.0.0         UG     0       eth0
```

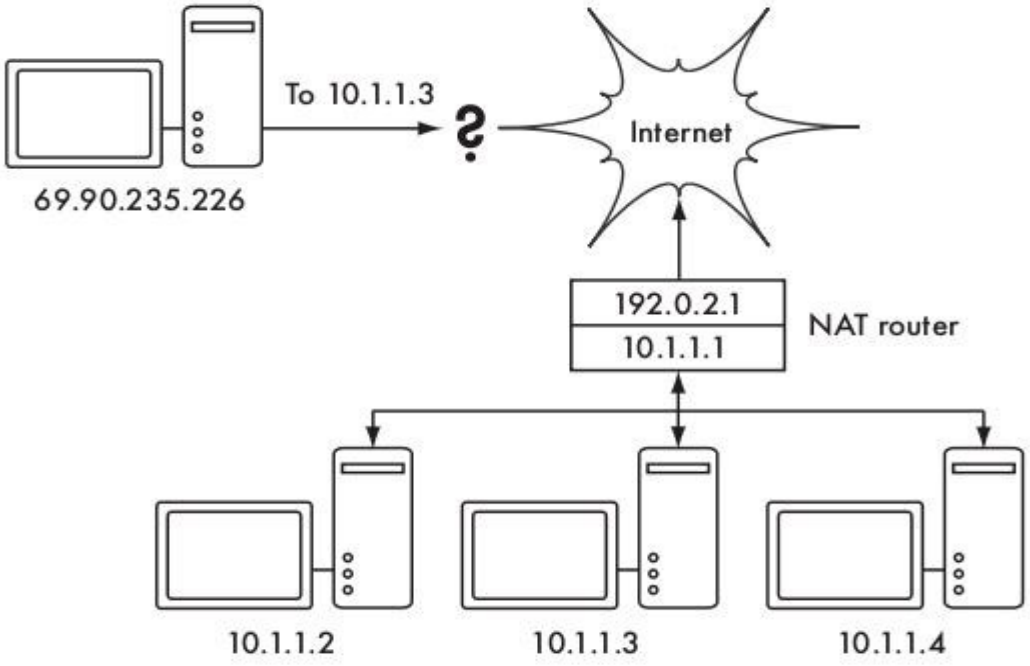
Gambar 3.9: Jika tidak ada rute gamblang ke tujuan tertentu, sebuah mesin akan menggunakan gateway default yang ada di tabel routingnya.

Rute dapat diperbarui secara manual, atau secara dinamis bereaksi pada saat ada jaringan yang putus atau peristiwa lain-nya. Beberapa contoh protokol routing dinamik yang populer ialah RIP, OSPF, BGP, dan OLSR. Mengkonfigurasi routing dinamik diluar lingkup buku ini, bagi anda yang tertarik dapat membaca referensi **Appendix A.**

Network Address Translation (NAT)

Agar dapat mencapai mesin di Internet, alamat RFC1918 harus diubah menjadi alamat IP publik yang dapat di routing di Internet global. Hal ini dapat dicapai menggunakan teknik yang dikenal sebagai ***Network Address Translation,*** atau ***NAT.*** Sebuah peralatan NAT adalah sebuah router yang memanipulasi alamat dari paket tidak sekedar mengirim / memforward saja. Di NAT router, sambungan Internet memakai satu (atau lebih) alamat IP yang dihubungi secara global, sedangkan jaringan private memakai alamat IP dari alamat IP RFC1918 yang private. Sebuah NAT router memungkinkan penggunaan alamat IP global / publik untuk di share dengan semua pengguna di dalam, yang semua memakai alamat private. NAT mengubah paket dari satu bentuk ke bentuk lain sewaktu paket melewatinya. Bagi para pengguna jaringan private, mereka mereka secara langsung dihubungkan dengan Internet dan tidak memerlukan perangkat atau driver khusus. Mereka hanya perlu memakai router NAT sebagai gateway default mereka, dan mengalamatkan paket seperti biasanya. Router NAT akan menterjemahkan paket keluar untuk memakai alamat global IP sewaktu mereka meninggalkan jaringan, dan menterjemahkan paket kembali sewaktu di terima dari Internet.

Akibat utama dari pemakaian NAT adalah mesin dari Internet tidak dapat dengan mudah menghubungi server yang ada di organisasi tanpa secara eskplisit mengkonfigurasi aturan fowarding di router. Memulai sambungan dari alamat private biasanya tidak ada masalah yang berarti, walaupun beberapa aplikasi (seperti VoIP dan beberapa aplikasi VPN) dapat memperoleh kesulitan dengan NAT.



Gambar 3.10: Network Address Translation memungkinkan anda saling berbagi satu alamat IP dengan banyak mesin di dalam, tetapi bisa membuatnya sulit untuk beberapa servis untuk bekerja dengan semestinya.

Bergantung pada sudut pandang anda, hal ini bisa dianggap sebagai sebuah bug (karena membuatnya lebih sukar membentuk komunikasi dua arah) atau sebuah ciri khas (karena secara efektif menyediakan firewall “gratisan” untuk seluruh organisasi anda). Alamat IP RFC1918 sebaiknya disaring di pinggir jaringan anda untuk mencegah lalu-lintas RFC1918 yang tidak baik yang masuk atau meninggalkan jaringan anda. Memang NAT melakukan beberapa fungsi seperti firewall, tapi bukan pengganti untuk firewall yang sebenarnya.

Keluarga Protokol Internet

Mesin di Internet menggunakan Protokol Internet (IP) untuk saling berhubungan, walaupun

terpisah oleh banyak mesin perantara. Ada sejumlah protokol yang beroperasi dengan IP yang menyediakan fitur penting pada operasi normal seperti IP sendiri. Setiap paket menetapkan nomor protokol yang mengidentifikasi paket sebagai salah satu dari protokol tersebut. Protokol yang paling banyak digunakan adalah ***Transmission Control Protocol*** (***TCP,*** nomor 6), **User Datagram Protocol** (***UDP,*** nomor 17), dan ***Internet Control Message Protocol*** (***ICMP,*** nomor 1). Sebagai sebuah kelompok, protokol ini (dan lain-lainnya) dikenal sebagai ***keluarga Protokol Internet,*** atau ***TCP/IP.***

Protokol TCP dan UDP memperkenalkan konsep nomor port. Nomor port memungkinkan menjalankan banyak servis pada sebuah alamat IP yang sama, dan masih dapat membedakan servis yang satu dengan yang lain. Setiap paket mempunyai nomor port sumber dan tujuan. Beberapa nomor port di definisikan sebagai standard, digunakan untuk mencapai servis yang banyak digunakan, seperti email dan web server. Sebagai contoh, web server biasanya ***mendengarkan*** pada TCP port 80, dan email SMTP server mendengarkan pada port 25. Yang kami maksud dengan servis “mendengarkan” pada sebuah port (seperti port 80), kami maksud adalah mesin menerima paket yang menggunakan IP sebagai alamat IP tujuan dan 80 sebagai port tujuan. Server biasanya tidak terlalu peduli tentang sumber IP atau sumber port, walaupun kadang kali mereka akan menggunakan hal tersebut untuk melihat identitas lawan bicaranya.

Pada saat mengirim balasan untuk paket tersebut, server akan menggunakan IP sendiri sebagai sumber IP, dan 80 sebagai sumber port. Saat sebuah klien tersambung ke sebuah servis, mungkin menggunakan nomor port sembarang yang tidak digunakan, tetapi harus tersambung dengan port yang benar di serverr (contoh, 80 untuk web, 25 untuk email). TCP adalah sebuah protokol yang ***berorientasi sesi (session oriented)*** yang akan menggaransi pengantaran dan memiliki fitur kontrol pengiriman (seperti pendeteksian dan mitigasi adanya kepadatan jaringan, pengiriman ulang, pengurutan paket dan assembling ulang, dsb). UDP dirancang untuk aliran informasi ***connectionless (tanpa sambungan),*** tidak ada garansi pengantaran sama sekali, atau pengurutan paket.

Protokol ICMP di rancang untuk debugging dan perawatan dari Internet. Daripada nomor port, ICMP mempunyai tipe pesan, yang juga berupa nomor. Tipe pesan yang berbeda dipergunakan untuk meminta jawaban sederhana dari komputer lain (meminta echo), memberitahukan pengirim akan kemungkinan adanya looping di routing (waktu melebihi), atau memberitahukan pengirim bahwa paket yang tidak bisa diantarkan karena peraturan firewall atau masalah lain (tujuan tak dapat dicapai).

Sekarang anda seharusnya sudah mempunyai pengertian yang kuat bagaimana pengalamatan komputer di jaringan, dan bagaimana informasi mengalir di atas jaringan di antara mereka. Sekarang marilah kita kami melihat secara ringkas perangkat keras fisik yang menggunakan protokol jaringan ini.

Ethernet

Ethernet adalah nama standard yang paling populer untuk menghubungkan komputer pada sebuah jaringan lokal ***Local Area Network (LAN).*** Ethernet kadang-kadang digunakan untuk menyambung sebuah komputer ke Internet, melalui sebuah router, modem ADSL, atau perangkat wireless. Namun, jika Anda terhubung satu komputer ke Internet, Anda mungkin tidak menggunakan Ethernet sama sekali. Nama Ethernet berasal dari konsep fisik dari eter, medium yang pernah untuk membawa cahaya melalui gelombang ruang. resmi disebut standar IEEE 802.3.

Ethernet yang paling umum adalah 100baseT. Ini mendefinisikan data kecepatan 100 megabits per detik, berjalan pada pasangan kawat yang diplintir *(twisted pair)*, dengan konektor RJ-45 di ujungnya. Topologi Jaringan adalah sebuah bintang *(star)*, dengan *switch* atau *hub* dipusat masing-masing bintang *(star),* dan akhir node (perangkat dan *switch* tambahan) di ujungnya.

Alamat MAC

Setiap perangkat terhubung ke jaringan memiliki alamat MAC yang unik, ditetapkan oleh produsen kartu jaringan. fungsinya adalah seperti yang alamat IP, karena dia berfungsi sebagai identifikasi unik sehingga memungkinkan perangkat untuk berbicara satu sama lain. Namun, lingkup sebuah alamat MAC yang terbatas untuk domain broadcast, yang terbatas hanya pada semua komputer yang terhubung pada kawat, hub, switch, dan bridge, yang sama, tapi tidak melalui router atau gateway Internet. Alamat MAC tidak pernah digunakan secara langsung di Internet, dan tidak dikirim melalui router.

Hub

Hub Ethernet menghubungkan banyak peralatan Ethernet menjadi satu. Mereka bekerja di lapisan fisik (yang terendah atau lapisan pertama). Mereka mengulang sinyal yang diterima oleh setiap port ke semua port yang lain. Oleh karena itu, hub akan dapat dianggap repeater sederhana. Karena desain ini, hanya satu port yang mengirim data pada satu saat. Jika dua perangkat mengirimkan pada saat yang sama, mereka akan merusak data yang dikirim masing-masing, dan keduanya menunda (back off) untuk mengirim ulang kembali paket yang rusak. Hal ini dikenal sebagai ***tabrakan***, dan setiap host tetap bertanggung jawab untuk mendeteksi tabrakan saat pengiriman data, dan mengirim ulang paket bila diperlukan.

Ketika masalah seperti tabrakan berlebihan terdeteksi pada sebuah port, beberapa hub dapat memutuskan ***(partisi)*** port untuk sementara waktu untuk membatasi dampaknya terhadap jaringan lainnya. Sementara port dipartisi, perangkat yang terpasang ke port tersebut tidak dapat berkomunikasi dengan jaringan. Jaringan berbasis hub umumnya lebih reliable dibandingkan Ethernet berbasis coax (juga dikenal sebagai 10base2 atau ThinNet), di mana

jika ada perangkat yang tidak baik dapat mematikan seluruh jaringan. Tetapi hub terbatas kegunaannya, karena hub dapat dengan mudah menjadi titik kemacetan di sebuah jaringan yang sibuk / padat.

Switch

Switch merupakan perangkat yang banyak beroperasi seperti hub, namun menyediakan sambungan khusus (atau ***switch)*** antar port. Tanpa mengirim ulang semua lalu lintas ke setiap port, switch dapat menentukan port yang saling berkomunikasi langsung dan menghubungkan antara kedua-nya saja. Switches umumnya akan memperoleh kinerja yang jauh lebih baik daripada hub, terutama pada jaringa yang sibuk dengan banyak komputer. Switch tidak jauh lebih mahal dari hub, dan menggantikan hub dalam banyak situasi.

Switch bekerja di lapisan data link (lapisan kedua), karena switch menginterpretasi dan bertindak atas alamat MAC pada paket yang mereka terima. Ketika sebuah paket tiba di port switch, switch akan mencatat alamat sumber MAC, yang berasosiasi dengan port tersebut. Switch menyimpan informasi ini dalam sebuah ***tabel MAC*** internal. Switch kemudian terlihat sampai alamat tujuan MAC dalam tabel MAC, dan mengirimkan paket pada port yang cocok. Jika alamat MAC tujuan tidak ditemukan di MAC tabel, paket ini kemudian dikirim ke semua antarmuka yang terhubung. Jika port tujuan sama dengan port masuk paket, paket tersebut akan disaring dan tidak diteruskan.

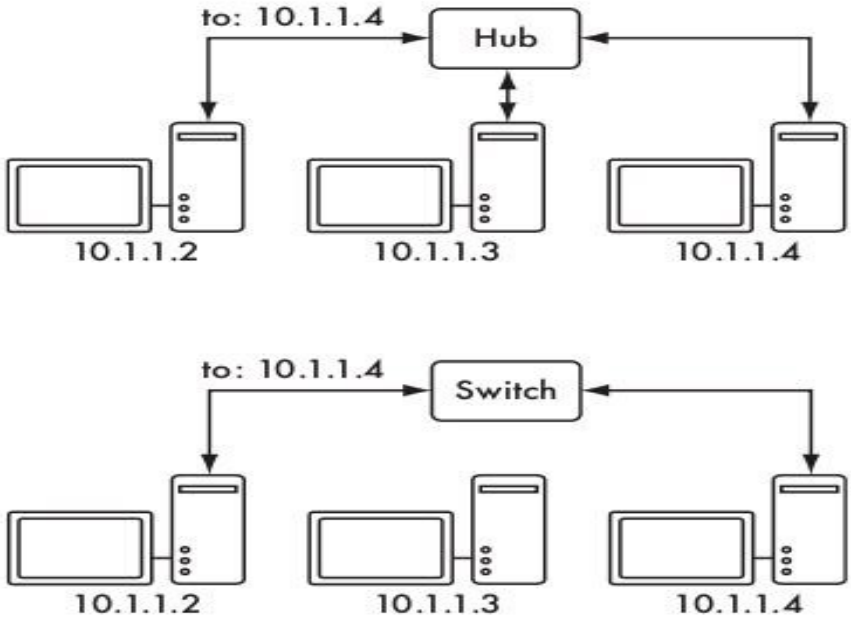
Hub vs. Switch

Hub dianggap perangkat yang sederhana, karena hub secara tidak efisien membroadcast semua trafik ke setiap port. Kesederhanaan ini menyebabkan penalty dari sisi kinerja maupun keamanan. Secara keseluruhan kinerja menjadi lebih lambat, karena bandwidth yang tersedia harus dibagi antara semua port. Karena semua lalu lintas terlihat oleh semua port, semua host di jaringan dapat dengan mudah memantau seluruh lalu lintas jaringan.

Switch membuat sambungan virtual antara port penerima dan pengirim. Ini menghasilkan kinerja yang lebih baik karena banyak sambungan virtual dapat dibangun secara bersamaan. Switch yang lebih mahal dapat men-switch trafik dengan menginspeksi paket di tingkat yang lebih tinggi (di lapisan aplikasi atau transport), memungkinkan pembuatan VLAN, melaksanakan dan fitur tingkat lanjutan lainnya.

Sebuah hub dapat digunakan jika dibutuhkan pengulangan traffik ke semua port; misalnya, bila Anda ingin sebuah mesin melakukan pemantauan untuk melihat semua lalu lintas pada jaringan. Kebanyakan switch menyediakan fungsi untuk ***memonitor port*** yang memungkinkan pengulangan traffik dari sebuah port tertentu yang ditugaskan secara khusus untuk tujuan ini.

Hub lebih murah daripada sekali switch. Namun, harga akan berkurang secara drastis di tahun-tahun belakangan ini. Oleh karena itu, jaringan yang menggunakan hub lama sebaiknya diganti dengan switch yang baru jika memungkinkan.



Gambar 3.11: Sebuah hub hanya mengulang semua trafik ke semua port, sementara switch akan membuat sambungan sementara antara port yang membutuhkan komunikasi.

Hub dan switch mungkin menawarkan layanan yang dikelola (*managed* servis). Beberapa dari layanan ini meliputi kemampuan untuk mengatur kecepatan link (10baseT, 100baseT, 1000baseT, *full* atau *half duplex*) per port, memungkinkan untuk memperhatikan kejadian di jaringan (seperti perubahan alamat MAC atau paket yang tidak baik / salah), dan biasanya termasuk penghitung trafik pada port untuk memudahkan bandwidth akunting. Sebuah *managed switch* yang menyediakan perhitungan upload dan download byte untuk setiap port fisik sehingga dapat sangat menyederhanakan pemantauan jaringan. Layanan ini biasanya tersedia melalui SNMP, atau dapat diakses melalui telnet, ssh, interface web, atau alat konfigurasi khusus.

Routers and firewalls

Sementara hub dan switch menyediakan konektivitas pada segmen jaringan lokal, tugas sebuah router adalah untuk meneruskan paket antara segmen jaringan yang berbeda.

Sebuah router biasanya memiliki dua atau lebih interface ke jaringan fisik. Router mungkin mendukung beberapa jenis media jaringan, seperti Ethernet, ATM, DSL, atau dial-up. Router dapat berupa perangkat keras khusus (seperti router Cisco atau Juniper) atau dapat dibuat dari sebuah PC standar dengan beberapa kartu jaringan dan software yang diperlukan.

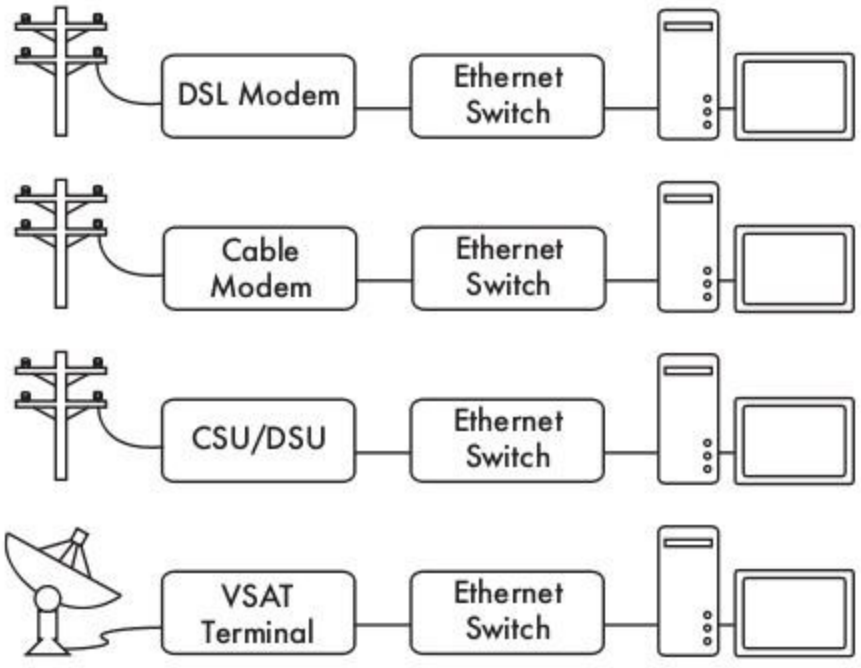
Router dapat berada di ***tepi*** dari dua atau lebih jaringan. Sesuai definisi, router memiliki satu sambungan untuk setiap jaringan, dan sebagai mesin perbatasan router dapat mengambil tanggung jawab lain serta routing. Banyak router yang memiliki kemampuan ***firewall*** menyediakan mekanisme untuk menyaring atau redirect paket yang tidak sesuai dengan kebijakan keamanan atau persyaratan akses. Router dapat juga memberikan layanan Network Address Translation (NAT).

Routers sangat bervariasi dalam biaya dan kemampuan. Biaya terendah dan tidak fleksibel biasanya sederhana, berupa perangkat keras khusus, seringkali dengan fungsi NAT, digunakan untuk berbagi koneksi internet antara beberapa komputer. Tingkat selanjutnya adalah router berbasis perangkat lunak, yang terdiri dari sebuah sistem operasi yang berjalan pada PC standar dengan beberapa antarmuka jaringan. Standar seperti sistem operasi Microsoft Windows, Linux, BSD dan semua yang mampu routing, dan jauh lebih fleksibel dibandingkan dengan router perangkat keras khusus yang murah. Namun, router ini menderita masalah yang sama dengan konvensional PC, seperti konsumsi daya tinggi, komponen yang jumlahnya besar dan kompleks dan berpotensi tidak andal, dan proses konfigurasi yang lebih kompleks.

Router yang paling mahal biasanya berupa hardware yang khusus kelas high-end, yang dibuat oleh perusahaan seperti Cisco dan Juniper. Router ini cenderung memiliki performa lebih baik, lebih banyak fitur, dan kehandalan yang lebih tinggi daripada perangkat lunak router pada PC. Disamping itu, sangat mungkin untuk membeli dukungan teknis dan kontrak pemeliharaan untuk router ini.

Kebanyakan router modern menawarkan mekanisme untuk memantau dan mencatat kinerja jarak jauh, biasanya melalui Simple Network Management Protokol (SNMP), walaupun perangkat yang paling murah sering mengabaikan fitur ini.

Perangkat Lainnya

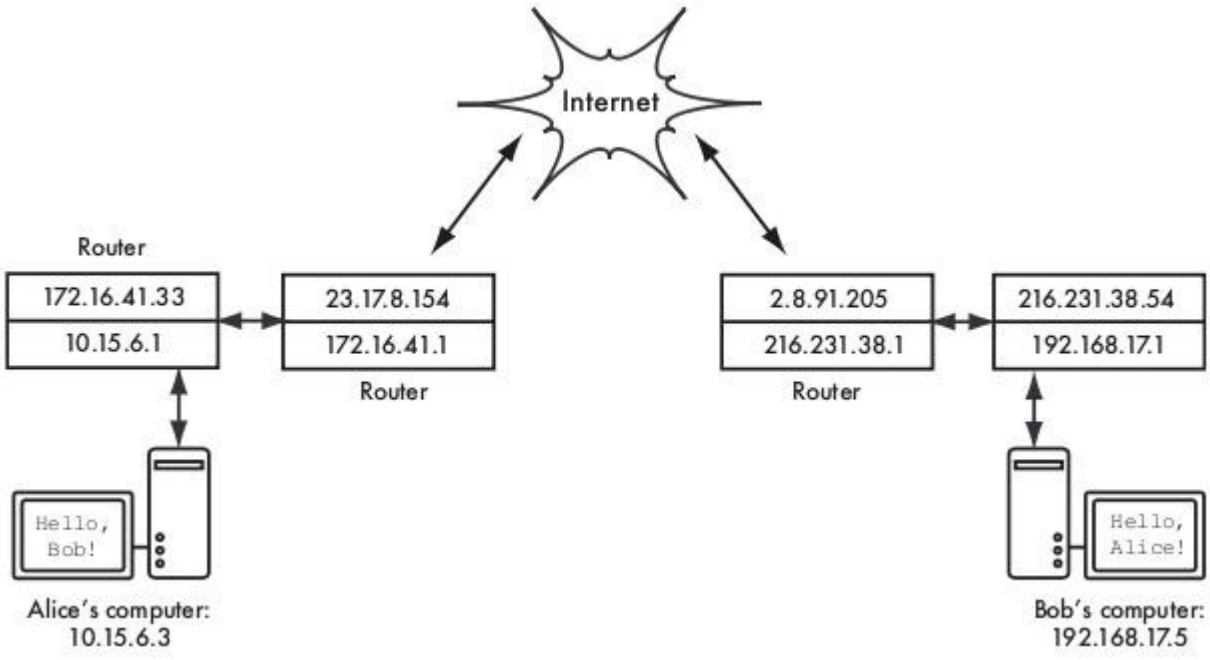


Gambar 3.12: Banyak DSL modem, kabel modem, CSU / DSUs, akses point nirkabel, terminal VSAT dan berakhir di jack Ethernet.

Setiap jaringan fisik memiliki sebuah peralatan terminal terkait. Misalnya, sambungan VSAT terdiri dari antena parabola terhubung ke terminal yang kemudian dapat di sambungkan ke card di PC, atau ke sambungan Ethernet. Kabel DSL menggunakan ***modem DSL*** sebagai jembatan kabel telepon lokal ke perangkat, baik jaringan atau sebuah komputer melalui USB. ***Kabel modem*** menjembatani televisi kabel untuk Ethernet, atau untuk card PC internal. Beberapa jenis sirkuit telekom (seperti T1 atau T3) menggunakan CSU / DSU menjembatani sirkuit telekom ke port serial atau Ethernet. Kabel dialup standard menggunakan modem untuk menghubungkan komputer ke telepon, biasanya melalui sebuah card modem plug-in atau port serial. Ada berbagai jenis peralatan jaringan nirkabel yang terhubung ke berbagai radio dan antena, tetapi hampir selalu berujung pada jack Ethernet.

Fungsi perangkat ini dapat sangat bervariasi antara produsen. Beberapa menyediakan mekanisme untuk memantau kinerja, sedangkan yang lain mungkin tidak. Karena koneksi Internet anda akan anda peroleh dari ISP anda, Anda sebaiknya mengikuti rekomendasi ISP anda ketika memilih peralatan yang akan menjembatani jaringan ISP ke jaringan anda.

Menyatukan Semua



Gambar 3.13: jaringan internet. Setiap segmen jaringan memiliki sebuah router dengan dua alamat IP, menjadikannya "sambungan lokal" ke dua jaringan yang berbeda. Paket diteruskan antara router hingga mencapai tujuan akhir mereka.

Setelah semua node memiliki alamat IP, mereka dapat mengirim paket data ke alamat IP lain node lain. Melalui penggunaan routing dan forwarding, paket ini dapat mencapai node pada jaringan yang secara fisik tidak terhubung ke node berasal. Proses ini menjelaskan banyak dari apa yang "terjadi" di Internet.

Dalam contoh ini, Anda dapat melihat jalur yang diambil pake saat Alice chatting dengan Bob menggunakan layanan Instan Messaging. Setiap garis titik-titik mewakili kabel Ethernet, sambungan wireless, atau fisik jaringan lainnya. Awan simbol yang umum digunakan untuk "Internet", dan mewakili banyak jaringan IP yang saling tersambung. Alice atau Bob tidak perlu khawatir dengan bagaimana jaringan yang beroperasi, sepanjang router melalukan trafik IP ke arah tujuan akhir. Jika bukan karena protokol Internet dan kerjasama dari semua orang di internet, komunikasi jenis ini tidak mungkin dilakukan.

Merancang jaringan fisik

Mungkin kelihatannya aneh untuk berbicara tentang "fisik" ketika membangun jaringan nirkabel. Padahal fisik adalah bagian dari jaringan bukan? Dalam jaringan nirkabel, fisik media yang digunakan untuk komunikasi jelas energi elektromagnetik. Tetapi dalam konteks bab ini, jaringan fisik merujuk kepada topik bagaimana untuk menempatkan sesuatu.

Bagaimana anda mengatur peralatan sehingga anda dapat mencapai pelanggan nirkabel anda? Apakah mereka mengisi sebuah bangunan kantor atau tersebar di wilayah yang luasnya beberapa kilometer, jaringan nirkabel yang alami ini diatur dalam tiga konfigurasi logis: ***sambungan point-to-point***, ***sambungan point-to-multipoint,*** dan ***awan multipoint-to-multipoint***. Sementara berbagai bagian dari jaringan anda dapat mengambil keuntungan dari semua ketiga konfigurasi ini, setiap sambungan akan menggunakan salah satu dari topologi ini.

Point-to-point

Sambungan ***point-to-point*** biasanya menyediakan sebuah koneksi internet dimana akses lain tidak tersedia. Satu sisi dari sambungan point-to-point memiliki koneksi internet, sementara yang lain menggunakan sambungan tersebut untuk mencapai Internet. Misalnya, sebuah universitas mungkin mempunyai sambungan frame relay atau VSAT yang cepat di tengah kampus, tetapi tidak mampu untuk membuat sambungan tersebut bagi bangunan penting yang ada di luar kampus. Jika bangunan utama di kampus memiliki pandangan terbuka ke bangunan diluar kampus, sambungan point-to-point dapat digunakan untuk membuat kedua bangunan tersebut tersambung. Hal ini dapat berupa tambahan atau bahkan menggantikan sambungan dial-up. Dengan antena yang tepat dan line of sight, sambungan point-to-point yang melebihi tiga puluh kilometer adalah mungkin.

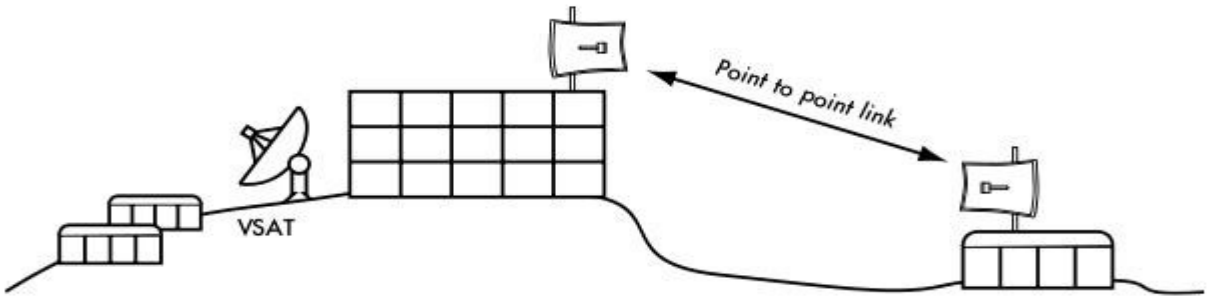


Figure 3.14: A point-to-point link allows a remote site to share a central Internet connection.

Gambar 3.14: Sebuah sambungan point-to-point yang memungkinkan sebuah pusat sambungan internet berbagi dengan lokasi yang jauh.

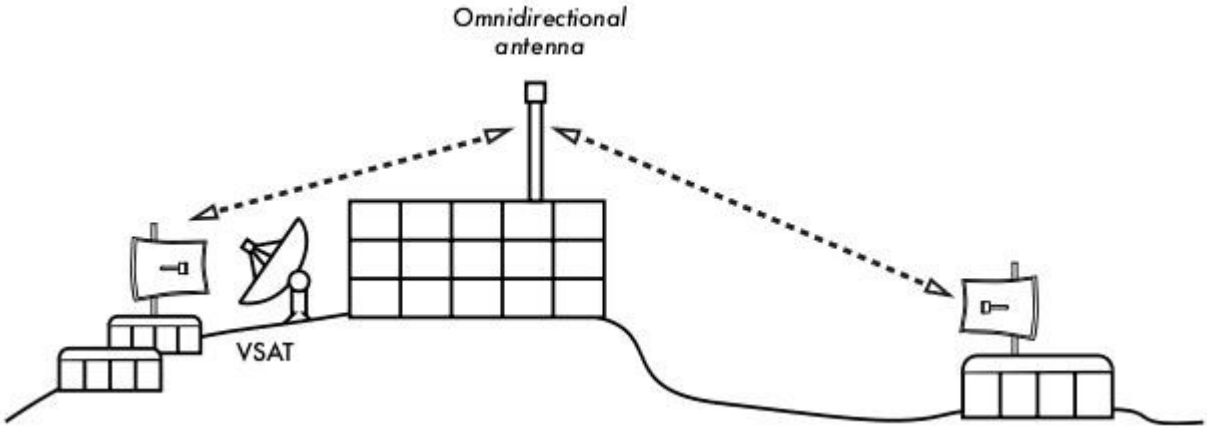
Tentu saja, setelah sebuah sambungan point-to-point dibuat, banyak yang dapat dilakukan untuk memperluas jaringan lebih lanjut. Jika bangunan jauh seperti di contoh berada di bagian atas bukit yang tinggi, mungkin dapat melihat lokasi penting lainnya yang tidak dapat dilihat secara langsung dari pusat kampus. Dengan menginstal sambungan point-to-point di daerah terpencil, node lain dapat bergabung dengan jaringan dan menggunakan koneksi internet dari pusat.

Sambungan point-to-point belum tentu harus melibatkan akses Internet. Misalnya anda harus

secara fisik berkendaraan ke stasiun pemantauan cuaca yang jauh, yang tinggi di bukit, dalam rangka untuk mengumpulkan data dan mencatat dari waktu ke waktu. Anda dapat menghubungkan tempat tersebut dengan menggunakan sambungan point-to-point, yang memungkinkan pemantauan data secara realtime, tanpa harus melakukan perjalanan ke situs. Jaringan nirkabel dapat menyediakan bandwidth yang cukup besar untuk membawa data yang besar (termasuk audio dan video) antara dua titik yang memiliki sambungan ke masing-masing, bahkan tanpa adanya sambungan langsung ke internet.

Point-to-multipoint

Tata letak jaringan yang juga sering dihadapi adalah ***point-to-multipoint***. Apabila beberapa node[3] berbicara ke pusat akses, ini merupakan aplikasi point-to-multipoint. Contoh yang khas dari tata letak point-to-multipoint adalah penggunaan ***akses point*** nirkabel yang menyediakan sambungan ke beberapa laptop. Laptop tidak berkomunikasi satu sama lain secara langsung, tetapi harus dalam wilayah akses point untuk dapat menggunakan jaringan.



Gambar 3.15: pusat VSAT berbagi dengan banyak situs jauh. Ketiga situs juga dapat berkomunikasi langsung dengan kecepatan jauh lebih cepat dari VSAT.

Jaringan point-to-multipoint dapat juga diterapkan pada contoh kami sebelumnya di universitas. Misalnya bangunan remote di atas bukit terhubung ke pusat kampus menggunakan sambungan point-to-point. Daripada menyiapkan beberapa sambungan point-to-point untuk mendistribusikan sambungan internet, sebuah antena dapat digunakan asalkan terlihat oleh beberapa bangunan remote tersebut. Ini adalah contoh klasik dari sambungan wide area point (daerah terpencil di bukit) untuk multipoint (banyak bangunan di lembah).

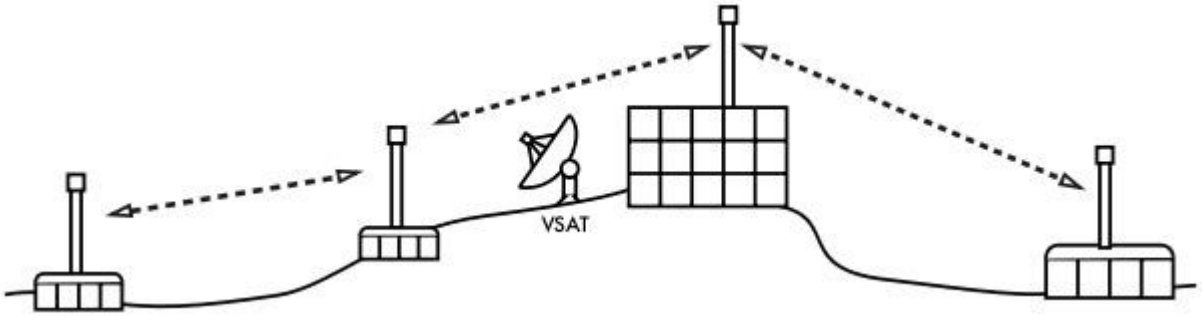
Perlu diketahui bahwa ada sejumlah masalah kinerja dengan penggunaan sambungan point-to-multipoint untuk jarak sangat jauh, yang akan dijelaskan kemudian dalam bab ini. Jenis sambungan tersebut mungkin digunakan dalam beberapa kondisi, tetapi jangan sampai

3 Sebuah node adalah sebuah perangkat yang mampu mengirim dan menerima data pada jaringan. Akses poin, router, komputer, dan laptop merupakan contoh dari node.

membuat kesalahan klasik dengan menginstalasi sebuah menara radio dengan daya besar di tengah kota dan mengharapkan agar dapat melayani ribuan pelanggan, seperti yang akan anda lakukan dengan sebuah stasiun radio FM . Seperti yang akan kita lihat, jaringan data dua arah mempunyai perilaku yang sangat berbeda dari radio siaran.

Multipoint-to-multipoint

Tipe tata letak jaringan yang ke tiga adalah jaringan ***multipoint-to-multipoint,*** yang juga disebut sebagai ***ad-hoc*** atau jaringan ***mesh.*** Dalam jaringan multipoint-to-multipoint, tidak ada kewenangan pusat. Setiap node pada jaringan dapat membawa lalu lintas data dari setiap node lainnya yang memerlukan, dan semua node berkomunikasi satu sama lain secara langsung.



Gambar 3.16: Sebuah multipoint-to-multipoint mesh. Setiap node dapat mencapai node lainnya pada kecepatan sangat tinggi, atau menggunakan koneksi VSAT terpusat untuk mencapai Internet.

Manfaat dari tipe topologi jaringan ini bahwa walaupun tidak ada satupun node yang tersambung ke akses point, mereka dapat tetap berkomunikasi satu sama lain. Implementasi jaringan mesh yang baik akan mampu menyembuhan diri sendiri, yang berarti bahwa mereka secara otomatis mendeteksi masalah routing dan memperbaikinya sesuai kebutuhan. Memperluas jaringan mesh sangat mudah sekali, sesederhana menambahkan node. Jika salah satu node dalam "awan jaringan" yang kebetulan berfungsi sebagai gateway internet, maka koneksi ke Internet dapat dibagi antara semua klien.

Dua (2) kerugian topologi mesh, yaitu, peningkatkan kompleksitas dan kinerja yang lebih rendah. Keamanan jaringan mesh dikhawatirkan, karena setiap peserta berpotensi membawa lalu lintas dari node lainnya. Jaringan multipoint-to-multipoint cenderung sulit untuk dilakukan troubleshoot, karena banyaknya perubahan variabel karena banyaknya node yang bergabung dan meninggalkan jaringan. Awan jaringan multipoint-to-multipoint biasanya mempunyai kapasitas yang lebih terbatas dibandingkan dengan jaringan point-to-point atau point-to-multipoint, karena tambahan overhead pengelolaan jaringan untuk routing dan peningkatan perebutan di spektrum radio.

Namun demikian, jaringan mesh berguna dalam banyak keadaan. Kami akan memperlihatkan sebuah contoh bagaimana membangun jaringan mesh multipoint-to-multipoint menggunakan routing protokol OLSR.

Menggunakan teknologi yang cocok

Semua disain jaringan dapat digunakan untuk melengkapi satu sama lain dalam jaringan yang luas, dan tentunya dapat diintegrasikan dengan teknik jaringan kabel yang tradisional jika di mungkinkan. Implementasi umum yang sering dilakukan, misalnya, untuk penggunaan jarak jauh digunakan sambungan nirkabel untuk menyediakan akses Internet ke lokasi terpencil, dan di bangun akses point lokal untuk menyediakan akses nirkabel lokal. Salah satu klien ini jalur akses mungkin juga bertindak sebagai node mesh, memungkinkan jaringan untuk berkembang secara organik antara pengguna laptop yang pada akhirnya bersatu menuju ke sambungan point-to-point untuk mengakses Internet. Sekarang kita telah memiliki gambaran yang jelas bagaimana jaringan nirkabel dapat di atur, kita dapat mulai memahami bagaimana komunikasi dapat dilakukan melalui jaringan tersebut.

Jaringan nirkabel 802.11

Sebelum paket dapat diteruskan dan diarahkan ke Internet, lapisan pertama (fisik) dan kedua (data link) harus terhubung. Tanpa konektivitas sambungan lokal, node di jaringan tidak dapat berbicara satu sama lain dan merouting paket.

Untuk menyediakan konektivitas fisik, perangkat jaringan nirkabel harus beroperasi di frekunsi yang sama dari spektrum radio. Seperti yang kita lihat di **Bab 2**, ini berarti bahwa radio 802.11a akan berbicara dengan radio 802.11a di sekitar 5 GHz, dan 802.11b / g akan berbicara dengan radio 802.11b/g lainnya di sekitar 2,4 GHz. Tetapi 802.11a sebuah perangkat tidak dapat interoperate dengan perangkat 802.11b/g, karena mereka menggunakan bagian spektrum elektromagnetik yang berbeda.

Secara khusus, card wireless harus setuju untuk menggunakan saluran yang sama. Jika sebuah card radio 802.11b diset ke saluran 2 sementara yang lain menggunakan saluran 11, maka radio tersebut tidak dapat berkomunikasi satu sama lain.

Ketika dua card wireless yang dikonfigurasi untuk menggunakan protokol yang sama pada saluran radio yang sama, maka mereka siap untuk bernegosiasi konektivitas pada lapisan data link. Setiap perangkat 802.11a/b/g dapat beroperasi menggunakan salah satu dari empat kemungkinan mode:

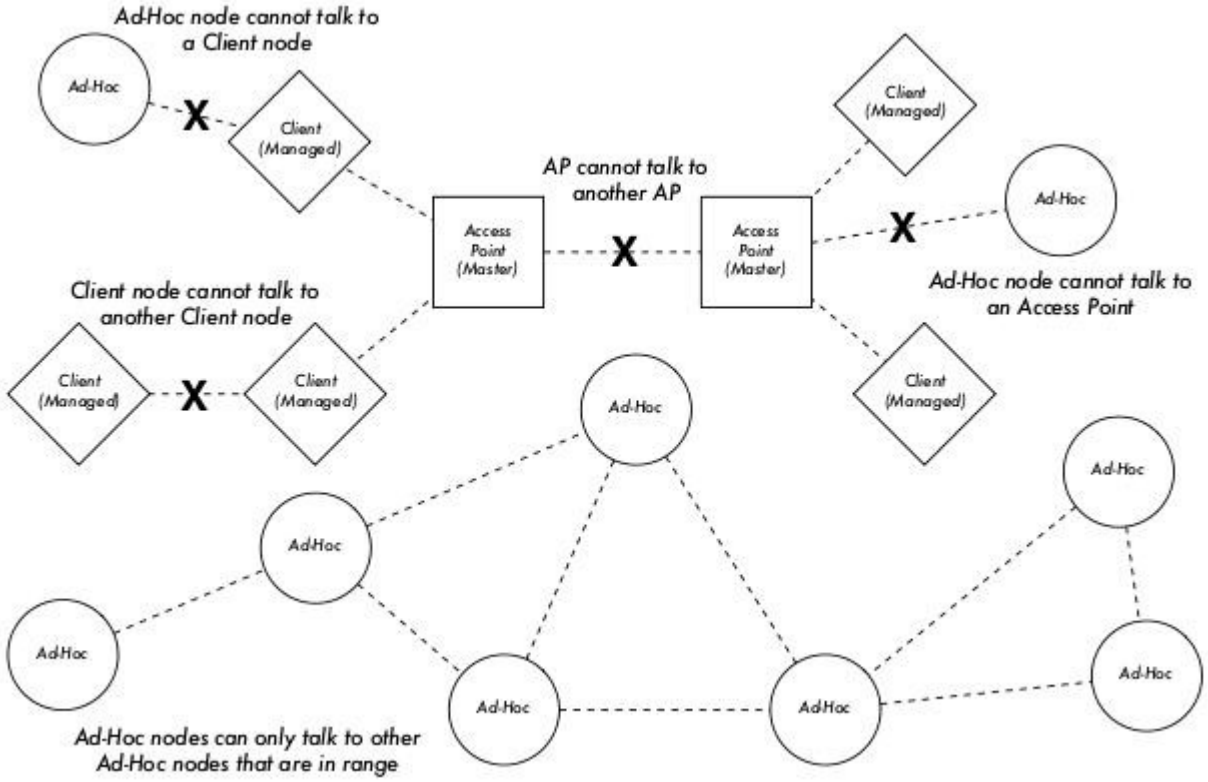
1. ***Modus Master*** (juga disebut ***AP*** atau ***mode infrastruktur)*** digunakan untuk memberikan layanan seperti jalur akses tradisional. Card nirkabel membuat jaringan dengan nama tertentu (disebut ***SSID***) dan kanal tertentu, dan menawarkan layanan untuk jaringan tersebut. Sementara dalam master mode, card nirkabel mengatur

semua komunikasi yang berhubungan dengan jaringan (authenticating klien nirkabel, penanganan perebutan kanal, pengulangan paket, dll). Card wireless pada mode master hanya dapat berkomunikasi dengan card yang terkait dengan itu di modus managed.

2. ***Modus Managed*** kadang-kadang juga disebut sebagai ***modus klien***. Card nirkabel di modus Managed akan bergabung dengan jaringan yang diciptakan oleh master, dan secara otomatis akan menyesuaikan ke kanal yang digunakan master. Mereka kemudian mengirimkan data kepercayaan (credential) kepada master, dan jika data kepercayaan diterima, mereka dikatakan ***berasosiasi (associated)*** dengan master. Card dalam Modus Managed tidak berkomunikasi dengan satu sama lain secara langsung, dan hanya akan berkomunikasi dengan master.

3. ***Modus ad-hoc*** membuat jaringan multipoint-to-multipoint di mana tidak ada satu master node atau AP. Dalam modus ad-hoc, setiap card nirkabel berkomunikasi langsung dengan tetangga. Node harus dalam jangkauan satu sama lainnya untuk berkomunikasi, dan harus setuju pada nama jaringan (SSID) dan kanal yang digunakan.

4. ***Modus monitor*** digunakan oleh beberapa alat (seperti **Kismet,** lihat **Bab 6**) untuk dapat secara pasif mendengarkan trafik data yang lewat pada satu saluran radio tertentu. Pada mode monitor, card nirkabel tidak dapat transmit / mengirim data. Hal ini berguna untuk menganalisis masalah pada sambungan nirkabel atau memerhatikan penggunaan spektrum di jaringan lokal. Modus monitor biasanya tidak digunakan untuk komunikasi.



Gambar 3.17: AP, Klien, and node Ad-Hoc.

Ketika mengimplementasi sambungan point-to-point atau point-to-multipoint, sebuah radio biasanya akan beroperasi dalam modus master, sedangkan yang lain beroperasi pada modus managed. Dalam jaringan multipoint-to-multipoint mesh, semua radio beroperasi pada modus ad-hoc sehingga mereka dapat berkomunikasi satu sama lain secara langsung.

Penting untuk mengerti berbagai mode tersebut ketika merancang tata letak jaringan anda. Ingat bahwa klien pada modus managed tidak dapat berkomunikasi satu sama lain secara langsung, sehingga kemungkinan anda akan menjalankan situs repeater pada modus master atau modus ad-hoc. Seperti yang akan kita lihat di bab ini, ad-hoc lebih fleksibel tetapi memiliki jumlah kinerja sebagai masalah dibandingkan dengan menggunakan modus master / managed.

Jaringan Mesh dengan OLSR

Kebanyakan WiFi beroperasi di jaringan bermodus infrastruktur - mereka terdiri dari akses point di suatu tempat (dengan radio yang beroperasi di mode master), yang tersambung ke kabel DSL atau jaringan kabel skala besar. Pada sebuah ***hotspot***, akses point biasanya

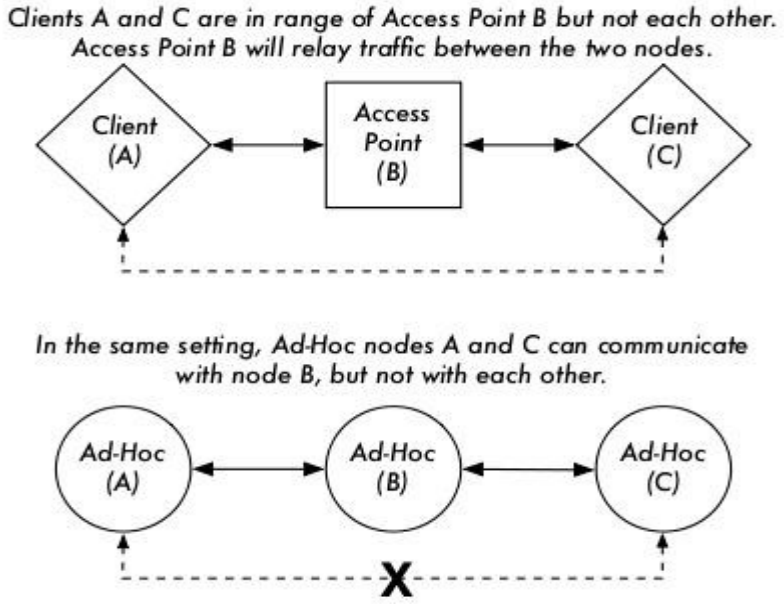
bertindak sebagai stasiun master yang mendistribusikan akses Internet kepada pelanggannya, yang beroperasi di modus Managed. Topologi ini mirip dengan layanan ponsel (GSM). Menghubungkan ponsel ke base station - tanpa kehadiran seperti base station mobiles tidak dapat berkomunikasi satu sama lain. Jika anda membuat panggilan ke teman yang duduk di seberang meja, telepon mengirim data ke base stasiun selular yang jauhnya ratusan kilometer kemudian mengirimkan data kembali ke telepon teman anda.

Card WiFi dalam modus managed tidak dapat berkomunikasi secara langsung satu sama lain. Klien - misalnya, dua laptop di meja yang sama - harus menggunakan akses point sebagai relay. Setiap trafik antara klien tersambung yang tersambung ke akses point akan dikirim dua kali. Jika klien A dan C berkomunikasi, klien A mengirimkan data ke akses point B, dan kemudian akses point B akan mengirim ulang data ke klien C. Dalam contoh kita, sebuah pengiriman data dapat mencapai kecepatan 600 kByte / detik (kecepatan maksimum yang dapat di capai oleh 802.11b). Dengan demikian, karena data harus dikirim ulang oleh akses point sebelum mencapai target, yang kecepatan effektif antara dua klien akan hanya 300 kByte / detik.

Dalam modus ad-hoc tidak ada hirarki hubungan master-klien. Node dapat berkomunikasi langsung selama mereka berada dalam jangkauan mereka antarmuka nirkabel. Dengan demikian, dalam contoh kita kedua komputer dapat mencapai kecepatan penuh ketika operasi ad-hoc, dalam kondisi ideal.

Kerugian pada modus ad-hoc adalah bahwa klien tidak mengulangi trafik yang diperuntukkan untuk klien lainnya. Dalam contoh penggunaan akses point, jika dua klien A dan C tidak dapat saling “melihat” secara langsung, mereka masih dapat berkomunikasi selama AP masih dalam jangkauan wireless dari kedua klien.

Node Ad-hoc secara default tidak melakukan fungsi relay / pengulangan, tetapi mereka dapat melakukan fungsi relay yang efektif jika ***routing*** diterapkan. Jaringan Mesh didasarkan pada strategi mengaktifkan setiap node mesh sebagai relay untuk memperluas jangkauan jaringan nirkabel. Semakin banyak node, semakin baik cakupan radio dan jangkauan awan mesh.



Gambar 3.18: Akses Point B akan me-relay trafik antara klien A dan C. Dalam mode Ad-Hoc, secara default node B tidak akan me-relay trafik antara A dan C.

Ada satu kekurangan besar yang harus disebutkan di sini. Jika perangkat hanya menggunakan satu antarmuka radio, bandwidth yang tersedia adalah berkurang secara signifikan setiap trafik diulang oleh node perantara pada perjalanan dari A ke B.

Selain itu, akan terjadi interferensi pada saluran transmisi karena node menggunakan pada kanal yang sama. Dengan demikian, jaringan mesh ad-hoc yang murah dapat menyediakan cakupan radio yang baik sebagai last mile dari jaringan nirkabel komunitas dengan penalti pada kecepatan - terutama jika banyak node dan daya pancar yang tinggi.

Jika sebuah jaringan ad-hoc hanya terdiri dari beberapa node yang berjalan dalam waktu yang lama, yang tidak bergerak dan yang mempunyai sambungan radio yang stabil – daftar panjang “yang” - sangat mungkin untuk menulis masing-masing tabel routing untuk semua node menggunakan tangan.

Sayangnya, kondisi tersebut jarang sekali ditemukan di dunia nyata. Node dapat gagal, peralatan WiFi cenderung untuk bergerak, dan interferensi akan dapat membuat sambungan radio tidak dapat digunakan. Dan tidak ada yang ingin meng-update tabel routing dengan tangan jika ada satu node ditambahkan ke jaringan. Dengan menggunakan routing protokol yang secara otomatis menjaga masing-masing tabel routing di semua node yang terlibat, kita dapat menghindari masalah ini. Routing protokol yang populer dari dunia kabel (seperti OSPF) tidak bekerja dengan baik dalam lingkungan semacam ini karena mereka tidak dirancang untuk menangani sambungan yang sangat tidak stabil atau topologi yang berubah dengan cepat.

Mesh routing dengan olsrd

Optimized Link State Routing Daemon - olsrd - dari olsr.org adalah sebuah aplikasi routing yang dikembangkan untuk routing di jaringan nirkabel. Kami akan berkonsentrasi pada perangkat lunak routing ini untuk beberapa alasan. Ini merupakan proyek Open Source yang mendukung sistem operasi Mac OS X, Windows 98, 2000, XP, Linux, FreeBSD, OpenBSD dan NetBSD. Olsrd tersedia untuk akses point yang menjalankan Linux seperti Linksys WRT54G, Asus Wl500g, AccessCube atau Pocket PC menjalankan Linux, dan merupakan standar pada Metrix kit yang menjalankan Pyramid. Olsrd dapat menangani beberapa antarmuka dan dapat kembangkan dengan plug-in. Ia mendukung IPv6 dan sangat aktif dikembangkan dan digunakan oleh komunitas jaringan di seluruh dunia.

Perlu di catat bahwa adalah beberapa implementasi dari Optimized Link State Routing (OLSR), yang dimulai sebagai konsep untuk IETF yang ditulis di INRIA Prancis. Pelaksanaan awal dari olsr.org adalah tesis master Andreas Toennesen di Universitas UniK. Berdasarkan pengalaman praktis dari komunitas free networking, routing daemon dimodifikasi. Olsrd sekarang berbeda secara signifikan dari konsep asli karena memasukan mekanisme Link Quality Extension yang mengukur paket loss antara node dan menghitung rute menurut informasi ini. Ekstensi ini merusak kompatibilitas dengan routing daemon yang mengikuti konsep INRIA. Olsrd yang tersedia dari olsr.org dapat dikonfigurasi untuk berperilaku sesuai dengan konsep IETF yang tidak memiliki fitur ini - tetapi tidak ada alasan untuk menonaktifkan Link Quality Extensions kecuali jika dibutuhkan untuk mengikuti implementasi yang lainnya.

Teori

Setelah olsrd berjalan untuk sementara waktu, sebuah node mengetahui keberadaan setiap node lain dalam awan mesh dan mengetahui node mana yang dapat digunakan untuk rute trafik. Setiap node mempunyai tabel routing yang meliputi seluruh awan mesh. Pendekatan ini untuk mesh routing disebut ***proaktif routing***. Sebaliknya, algoritma ***reaktif routing*** mencari rute hanya bila diperlukan untuk mengirim data ke node tertentu.

Ada kelebihan dan kekurangan untuk proaktif routing, dan ada banyak ide tentang cara lain untuk mesh routing yang mungkin layak disebut. Keuntungan terbesar dari routing proaktif adalah kita akan tahu siapa yang ada di keluar sana dan anda tidak perlu menunggu sampai rute ditemukan. Tinggi-nya overhead trafik protokol dan beban CPU yang besar adalah diantara kerugiannya. Di Berlin, komunitas Freifunk mengoperasikan awan mesh olsrd yang menyambungkan lebih dari 100 antarmuka. Rata-rata beban CPU yang disebabkan oleh olsrd pada Linksys WRT54G berjalan di 200 MHz adalah sekitar 30% di Berlin mesh. Ada batas yang jelas akan sejauh mana sebuah protokol proactive dapat di kembangkan - tergantung seberapa banyak antarmuka yang terlibat dan seberapa sering tabel routing diperbarui. Memelihara rute dalam awan mesh dengan node statis membutuhkan upaya lebih sedikit di bandingkan mesh dengan node yang terus bergerak, karena tabel routing lebih jarang diperbarui.

Mekanisme

Sebuah node olsrd yang sedang beroperasi akan secara periodik mem-broadcast 'Hello' sehingga tetangga dapat mendeteksi keberadaan node tersebut. Setiap node menghitung berapa 'Hello' yang hilang atau diterima dari setiap tetangga sehingga mendapatkan informasi tentang topologi dan kualitas sambungan node di lingkungan. Informasi topologi yang diperoleh di broadcast sebagai pesan Topology Control (pesan TC) dan diteruskan oleh tetangga yang dipilih olsrd sebagai multipoint relay.

Konsep multipoint relay merupakan ide baru di proaktif routing yang datang dengan konsep OLSR. Jika setiap node membrodcast ulang informasi topologi yang telah diterima, overhead yang tidak perlu akan terjadi di jaringan. Transmisi tersebut adalah berlebihan jika sebuah node memiliki banyak tetangga. Dengan demikian, sebuah node olsrd akan memutuskan tetangga yang baik sebagai multipoint relay yang harus mem-forward dengan pesan topologi kontrol. Catatan untuk multipoint relay hanya dipilih untuk tujuan penerusan pesan TC. Muatan di kirimkan ke semua node yang tersedia.

Dua jenis pesan lain yang ada di OLSR yang mengumumkan informasi: apakah sebuah node menawarkan gateway ke jaringan lain (pesan HNA) atau mempunyai beberapa interface (pesan MID). Tidak terlalu banyak yang dapat dikatakan tentang apa yang dilakukan pesan tersebut, kecuali fakta bahwa mereka ada. Pesan HNA membuat olsrd sangat nyaman saat menghubungkan perangkat mobile ke Internet. Ketika sebuah node menjelajah dia akan mendeteksi gerbang ke jaringan lain dan selalu memilih gateway yang memiliki rute terbaik. Namun, olsrd bukannya anti peluru. Jika node memberitakan bahwa dia adalah sebuah gateway Internet – padahal tidak karena memang bukan atau karena mati pada untuk sementara - node yang lain tetap percaya informasi tersebut. Gateway palsu adalah lubang hitam (black hole). Untuk mengatasi masalah ini, sebuah plugin gateway dinamis ditulis.

Plugin secara otomatis akan mendeteksi di gateway apakah dia benar-benar terhubung dan apakah link sambungan masih beroperasi. Jika tidak, olsrd berhenti untuk mengirim pesan HNA palsu. Sangat dianjurkan untuk membangun dan menggunakan plugin ini, bukan mengaktifan pesan statis HNA.

Praktek

Olsrd menerapkan routing berbasis IP di aplikasi pengguna - instalasi cukup mudah. Instalasi paket-paket yang tersedia untuk OpenWRT, AccessCube, Mac OS X, Debian GNU / Linux dan Windows. OLSR merupakan bagian dari standar Metrix Pyramid. Jika Anda harus kompilasi dari source code, silakan membaca dokumentasi yang disertakan dengan paket source code. Jika semuanya sudah

Pertama-tama, harus dipastikan bahwa setiap node memiliki alamat IP statis yang unik untuk setiap antarmuka yang digunakan untuk mesh. Tidak direkomendasikan untuk menggunakan DHCP di jaringan mesh berbasis IP. Sebuah permintaan DHCP tidak akan dijawab oleh DHCP server jika node meminta DHCP memerlukan sambungan multihop untuk tersambung, dan menerapkan dhcp relay yang menghubungkan seluruh mesh sepertinya tak berguna. Masalah ini dapat diselesaikan dengan menggunakan IPv6, karena ada banyak ruang yang tersedia untuk menghasilkan IP yang unik dari masing-masing alamat MAC card yang terlibat (seperti yang diusulkan dalam "IPv6 Stateless Address Autoconfiguration in large mobile ad hoc networks" by K. Weniger and M. Zitterbart, 2002).

Sebuah wiki-halaman dimana setiap orang yang tertarik dapat memilih alamat IPv4 individu

untuk setiap antarmuka dimana olsr daemon dijalankan dapat melayani tujuan cukup baik. Tidak ada cara yang mudah untuk mengotomatisasikan proses jika IPv4 digunakan.

Alamat broadcast harus 255.255.255.255 pada antarmuka mesh sebagai kesepakatan umum. Tidak ada alasan untuk memasukkan alamat broadcast secara eksplisit, karena olsrd dapat dikonfigurasi untuk mengabaikan broadcast dengan alamat default ini. Kita hanya harus memastikan bahwa konfigurasi sama di semua node. Olsrd dapat melakukannya sendiri. Ketika sebuah file konfigurasi default olsrd dikeluarkan, fitur ini harus diaktifkan untuk menghindari kebingungan kedua, yakni "mengapa node lain tidak dapat melihat mesin saya?"

Sekarang mengkonfigurasi antarmuka wireless. Berikut ini merupakan contoh bagaimana perintah untuk mengkonfigurasi kartu WiFi dengan nama wlan0 menggunakan Linux:

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

Verifikasi bahwa bagian nirkabel dari card WiFi telah dikonfigurasi sehingga memiliki sambungan ad-hoc ke node mesh lainnya dalam jangkauan langsung (satu hop). Pastikan antarmuka bergabung dengan kanal nirkabel yang sama, menggunakan jaringan nirkabel ESSID (Extended Service set identifier) yang sama dan memiliki sel-ID sama seperti semua lain WiFi-Card yang membangun jaringan mesh. Banyak WiFi atau kartu masing-masing driver sepenuhnya mengikuti standar 802,11 untuk jaringan ad-hoc dan gagal total untuk dapat tersambung ke sel. Mereka mungkin tidak dapat menyambung ke perangkat lain di meja yang sama, bahkan jika mereka menggunakan kanal dan nama jaringan wireless yang benar. Mereka mungkin bahkan membingungkan card lain yang berperilaku sesuai dengan standar dengan membuat sel-ID mereka sendiri pada kanal yang sama dengan nama jaringan wireless yang sama. Card WiFi yang dibuat oleh Intel yang dikirimkan dengan Centrino Notebook yang terkenal jahat dan suka melakukan hal ini.

Anda dapat memeriksa ini dengan perintah **iwconfig** ketika menggunakan GNU-Linux. Berikut adalah output pada mesin saya:

```
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
```

Penting untuk mengatur nilai ambang batas 'Request To Send' untuk operasi mesh. Tabrakan kadang kala akan terjadi pada kanal radio saat terjadi proses pengiriman data dari node pada kanal yang sama, dan RTS akan mengurangi kemungkinan tabrakan. RTS / CTS menambahkan sebuah proses negosiasi / handshake sebelum pengiriman setiap paket untuk

memastikan bahwa kanal tersebut kosong. Hal ini menambahkan overhead, tetapi meningkatkan kinerja dalam kasus node yang tersembunyi - dan node disembunyikan adalah biasa dalam sebuah mesh! Parameter ini menentukan ukuran paket terkecil (dalam satuan byte) yang akan menyebabkan node mengirimkan RTS.

Nilai ambang batas RTS harus lebih kecil dari ukuran paket IP dan nilai 'Fragmentation threshold' - disini di set ke 256 – jika tidak RTS akan dinonaktifkan. TCP sangat sensitif terhadap tabrakan, sehingga sangat penting untuk mengaktifkan RTS. Fragmentasi memungkinkan untuk membagi sebuah paket IP dalam potongan / fragmen kecil yang dikirim pada media. Hal ini menambahkan overhead, tetapi dalam lingkungan yang padat, hal ini mengurangi error dan memungkinkan paket untuk melalui gangguan interferensi.

Mesh jaringan sangat bising / padat karena semua node menggunakan kanal yang sama dan oleh karena itu saluran transmisi akan saling mengganggu satu sama lain. Parameter ini menentukan ukuran maksimum paket data sebelum dibagi dan dikirim - nilai yang sama dengan ukuran maksimum paket IP akan menonaktifkan mekanisme, sehingga nilai parameter ini harus lebih kecil dari ukuran paket IP. Menetapkan ambang batas fragmentasi sangat disarankan. Setelah alamat IP dan netmask yang valid diberikan dan antarmuka wireless telah beroperasi, file konfigurasi olsrd harus diubah agar olsrd menemukan dan menggunakan antarmuka yang dimaksudkan untuk bekerja.

Untuk Mac OS-X dan Windows ada GUI yang baik untuk mengkonfigurasi dan memonitoring keberadaan daemon. Sayangnya hal ini akan mendorong pengguna yang mempunyai pengetahuan terbatas untuk melakukan hal yang bodoh – seperti mengumumkan 'black hole'. Di BSD dan Linux, filr konfigurasi **/etc/olsrd.conf** harus di edit menggunakan editor text.

Sebuah olsrd.conf sederhana

Tidak praktis untuk menyediakan sebuah file konfigurasi lengkap di sini. Berikut adalah beberapa

```
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
```

```
}
```

Ada banyak pilihan yang tersedia di **olsrd.conf,** tapi pilihan dasar di atas cukup untuk anda memulai. Setelah langkah-langkah tersebut dilakukan, olsrd dapat dimulai dengan perintah sederhana di terminal:

olsrd -d 2

Saya rekomendasikan untuk menjalankannya dengan opsi debug -d 2 bila digunakan pada sebuah workstation, terutama untuk pertama kalinya. Anda dapat melihat apa yang dilakukan olsrd dan memantau seberapa baik sambungan ke tetangga anda. Pada perangkat embedded tingkat debug harus 0 (off), karena debug menciptakan banyak beban CPU. Outputnya harus terlihat seperti ini:

```
---     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
```

Menggunakan OLSR pada Ethernet dan banyak interface

Untuk menggunakan olsrd kita tidak perlu memiliki antarmuka wireless - meskipun olsrd dirancang untuk antarmuka wireless. OLSRD dapat digunakan pada sembarang NIC. Antarmuka WiFi tidak harus selalu beroperasi pada modus ad-hoc untuk membentuk mesh jika node mesh memiliki lebih dari satu antarmuka. Untuk sambungan khusus / dedicated mungkin pilihan yang lebih baik jika di operasikan pada mode infrastruktur. Banyak WiFi card dan driver yang bermasalah / buggy dalam modus ad-hoc, tetapi modus infrastruktur berfungsi dengan baik - karena semua orang berharap setidaknya fitur ini untuk bekerja.

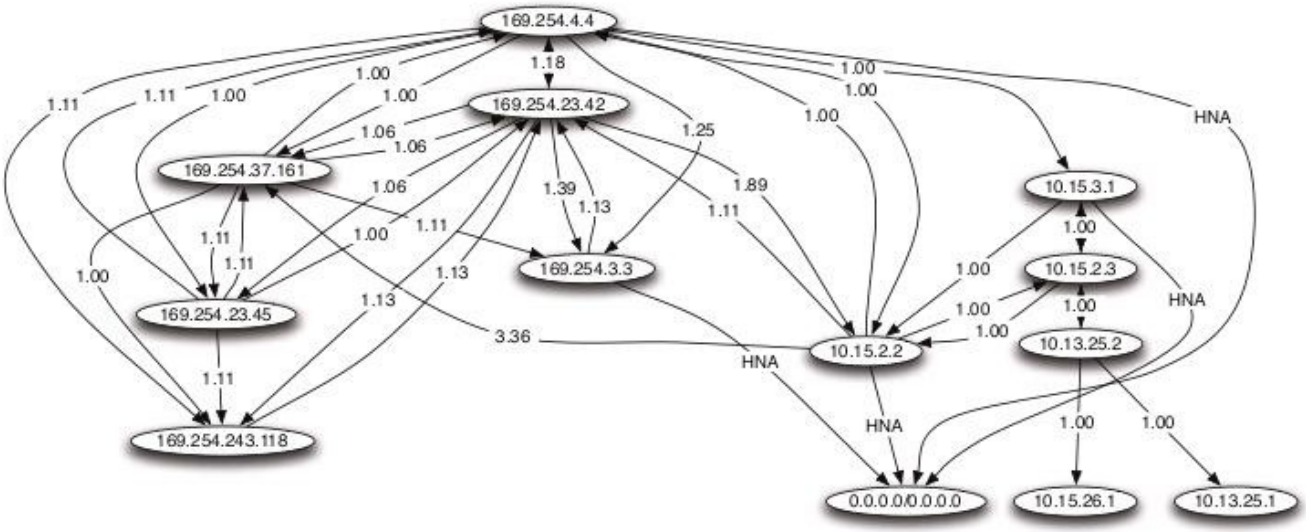
Modus ad-hoc tidak memiliki banyak pengguna hingga saat ini, sehingga implementasi dari modus ad-hoc lebih lambat dilakukan oleh banyak produsen. Dengan meningkatnya popularitas jaringan mesh, kondisi driver lebih membaik saat ini.

Banyak orang menggunakan olsrd pada kabel dan antarmuka nirkabel - mereka tidak berpikir tentang arsitektur jaringan. Mereka hanya menyambungkan antena ke card WiFi mereka, menyambungkan kabel ke card Ethernet mereka, mengaktifkan olsrd untuk berjalan di semua komputer dan semua antarmuka dan menjalankannya. Hal ini sebenarnya penyalahgunaan dari sebuah protokol yang dirancang untuk membangun nirkabel pada sambungan yang sangat rentan - tetapi - mengapa tidak?

Mereka berharap olsrd untuk memecahkan setiap masalah jaringan. Jelas tidak diperlukan untuk mengirim pesan 'Hello' pada antarmuka kabel setiap dua detik - tetapi hal ini berhasil. Hal ini jangan dijadikan sebagai rekomendasi - hanya menakjubkan apa yang dilakukan orang terhadap protokol dan bahkan mereka sukses. ide untuk memiliki protokol yang dapat melakukan semua hal bagi pemula yang ingin memiliki jaringan LAN berukuran kecil yang dapat di routing menjadi sangat menarik.

Plugins

Ada sejumlah plugin yang tersedia untuk olsrd. Simak situs olsr.org untuk memperoleh daftar lengkapnya. Berikut sedikit HOWTO untuk visualisasi topologi jaringan menggunakan plugin **olsrd_dot_draw.**



Gambar 3.19: Sebuah topologi jaringan OLSR yang dihasilkan secara otomatis.

Seringkali sangat baik untuk pengertian tentang jaringan mesh jika kita dapat menampilkan

topologi jaringan secara grafis. **olsrd_dot_draw** mengeluarkan topologi dalam file berformat dot pada port TCP 2004. Graphviz dapat kemudian digunakan untuk gambar grafiknya.

Instalasi Plugin dot_draw

Compile olsr plugins secara terpisah dan instal. Untuk me-load plugin menambahkanbaris berikut ke **/etc/olsrd.conf.** Parameter "accept" menetapkan komputer mana yang akan diterima untuk melihat Informasi Topologi (saat ini hanya satu) dan mesin tersebut adalah "localhost" secara default. Parameter "port" menentukan port TCP.

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

Kemudian restart olsr dan periksa apakah anda mendapatkan output pada TCP Port 2004

telnet localhost 2004

Setelah beberapa saat anda harus mendapatkan beberapa teks output.

Sekarang Anda dapat menyimpan penjelasan output grafik dan menjalankan software atau **dot** atau **neato** form dari paket graphviz untuk mendapatkan gambar.

Bruno Randolf telah menulis sebuah skrip perl kecil yang terus-menerus mengambil informasi dari topologi olsrd dan menampilkan dengan menggunakan paket graphviz dan Imagemagick.

Pertama, instal paket berikut pada workstation anda:

- graphviz, http://www.graphviz.org/
- Imagemagick, http://www.imagemagick.org/

Download script dari: http://meshcube.org/nylon/utils/olsr-topology-view.pl
Sekarang Anda dapat menjalankan skrip sengan **. /olsr-topologi-view.pl** dan melihat topologi di-update secara realtime.

Mengatasi masalah

Selama card WiFi dapat 'melihat' satu sama lain secara langsung, maka harusnya anda dapat melakukan ping dengan atau tanpa olsrd. Hal ini berlaku karena netmask yang besar secara efektif membuat setiap node menjadi lokal, sehingga masalah routing yang pertama

dapat di singkirkan. Hal ini harus di periksa pertama kali jika semua tampaknya seperti beroperasi seperti sebagaimana yang di harapkan. Sebagian besar pusing kepala karena harus berhadapan dengan modus WiFi Ad-Hoc disebabkan oleh kenyataan bahwa implementasi modus ad-hoc di driver dan card banyak yang tidak baik. Jika gagal dalam melakukan ping ke node terdekat secara langsung maka kemungkinan besar adalah isu card / driver, atau konfigurasi jaringan anda yang salah.

Jika mesin dapat ping satu sama lain, tetapi tidak menemukan rute olsrd, maka alamat IP, netmask dan alamat broadcast perlu diperiksa. Terakhir, apakah anda menjalankan firewall? Pastikan firewall tidak memblokir UDP port 698.

Estimasi kapasitas

Sambungan wireless dapat secara signifikan memberikan ***throughput*** lebih besar daripada sambungan Internet tradisional, seperti VSAT, dialup, atau DSL. Throughput juga disebut sebagai ***kapasitas kanal,*** atau ***bandwidth*** (walaupun ini adalah istilah yang tidak ada hubungannya dengan bandwidth di radio). Penting untuk memahami bahwa perangkat nirkabel mencantumkan kecepatan (***data rate***) merujuk ke kecepatan radio dapat bertukar simbol, bukan throughput yang akan anda lihat. Seperti yang disebutkan sebelumnya, satu sambungan 802.11g dapat menggunakan radio 54 Mbps, tetapi hanya akan menyediakan throughput hingga 22 Mbps saja. Sisanya adalah overhead yang dibutuhkan radio untuk proses koordinasi mereka menggunakan protokol 802.11g.

Perlu di catat bahwa throughput adalah sebuah ukuran bit dari waktu ke waktu. 22 Mbps berarti bahwa dalam suatu waktu, hingga 22 megabits dapat dikirim dari satu tempat ke tempat yang lain. Jika pengguna mencoba untuk mendorong lebih dari 22 megabits melalui sambungan tersebut, akan diperlukan lebih dari satu detik. Karena data tidak dapat dikirim secara langsung, data diletakkan dalam ***antrian***, dan dikirim secepat mungkin. Antrian data ini akan meningkatkan waktu yang diperlukan untuk menyeberangkan bit terakhir di antrian. Waktu yang diperlukan untuk menyeberang data disebut ***latensi,*** latensi tinggi umumnya disebut '***lag***'. Sambungan anda pada akhirnya akan mengirimkan semua trafik di antrian, namun pengguna anda mungkin akan mengeluh karena lag meningkat.

Berapa besar throughput yang dibutuhkan pengguna anda? Hal ini tergantung pada berapa banyak pengguna anda, dan bagaimana mereka menggunakan sambungan nirkabel. Berbagai aplikasi Internet yang berbeda memerlukan throughput yang berbeda pula.

Aplikasi	**BW / Pengguna**	**Catatan**
Pesan teks / IM	<1 kbps	Karena lalu lintas adalah jarang dan asynchronous, IM akan mentolerir latensi tinggi.
Email	1-100 kbps	Seperti IM, dan e-mail asynchronous tidak perlu tersambung terus, sehingga akan mentolerir latensi. Besar lampiran,

		virus, spam dan menambahkan untuk penggunaan bandwidth. Catatan bahwa email layanan web (seperti Yahoo atau Hotmail) harus dianggap sebagai akses web, tidak seperti email.

Aplikasi	**BW / Pengguna**	**Catatan**
Web	50-100+ kbps	Web browser hanya menggunakan jaringan bila ada data yang diminta. Komunikasi adalah asinkron, sehingga lag sampai jumlah tertentu masih dapat di tolerir. Jika web browser meminta lebih banyak data (gambar yang besar, download yang lama, dll) penggunaan bandwidth akan naik secara signifikan.
Streaming audio	96-160 kbps	Setiap pengguna layanan streaming audio akan menggunakan bandwith yang relatif besar secara konstan selama di mainkan / di request. Latensi dapat ditolerir sementara dengan menggunakan buffer yang besar pada klien. Tetapi lag yang terlalu panjang akan menyebabkan audio yang putus-putus atau kegagalan.
Voice over IP	24-100 kbps	Seperti halnya dengan audio streaming, VoIP yang menggunakan bandwidth yang konstan untuk setiap pengguna selama panggilan. Tetapi dengan VoIP, bandwidth yang digunakan adalah dua arah dan sama besarnya. Latency pada VoIP akan langsung terasa pada pengguna. Lag yang lebih besar dari beberapa mili detik tidak dapat di terima oleh pengguna VoIP.
Streaming video	64-200 kbps	Seperti streaming audio, beberapa delay latensi dihindari dengan menggunakan buffer pada klien. Streaming video memerlukan throughput yang tinggi dan latensi rendah untuk bekerja dengan benar.
Peer-to-peer aplikasi file sharing (BitTorrent, KaZaA, Gnutella, eDonkey, dll)	0-tidak terbatas Mbps	Sementara aplikasi yang lain mentolerir sejumlah latensi, aplikasi ini cenderung menghabiskan semua bandwidth yang tersedia dengan cara mengirim ke sebanyak mungkin client, secepat mungkin. Pengguna aplikasi ini cenderung akan menyebabkan masalah di jaringan kecuali jika anda menggunakan bandwidth manajemen yang baik.

Untuk memperkirakan keperluan throughput yang anda perlukan di jaringan anda, kalikan jumlah pengguna diharapkan dengan aplikasi yang mungkin mereka gunakan. Misalnya, 50 pengguna yang terutama browsing web akan mengkonsumsi 2,5 sampai 5 Mbps atau lebih

dari throughput saat trafik puncak, dan akan mentolerir beberapa latensi. Di sisi lain, 50 penggunaan serentak VoIP akan memerlukan 5 Mbps atau lebih dari throughput **dalam kedua arah,** tanpa adanya latensi. Karena peralatan nirkabel 802.11g adalah ***half duplex*** (artinya, hanya menerima atau mengirim / transmit bergantian, tidak keduanya secara bersamaan) anda perlu mengali dua throughput yang di perlukan, untuk total **10 Mbps.** Penyedia sambungan wireless harus menyediakan kapasitas tersebut setiap detik, atau percakapan VoIP yang dilakukan akan terasa delay / lag.

Karena pengguna anda juga tidak mungkin untuk menggunakan sambungan di saat yang sama, hal yang sering dilakukan adalah membeli lebih (***oversubscribe)*** dari throughput yang tersedia (yang, memungkinkan lebih banyak pengguna daripada jumlah maksimum bandwidth yang tersedia). Oversubscribe dengan faktor 2 sampai 5 sangat umum. Pada umumnya, anda akan oversubscribe ketika membangun jaringan infrastruktur. Dengan pemantauan throughput secara hati-hati diseluruh jaringan anda, anda akan dapat untuk merencanakan kapan meng-upgrade berbagai bagian jaringan, dan berapa banyak sumber daya tambahan akan diperlukan.

Bersiaplah bahwa tidak peduli berapa kapasitas pasokan anda, pengguna anda akan menemukan aplikasi yang akan menggunakan semua. Seperti kita akan lihat pada akhir bab ini, menggunakan teknik membentuk bandwidth dapat membantu mengurangi beberapa masalah latensi. Dengan menggunakan manajemen bandwidth, web cache, dan teknik lainnya, anda dapat secara signifikan mengurangi latensi dan meningkatkan throughput keseluruhan jaringan. Untuk mendapatkan merasa lag yang sangat lambat pada sambungan, ICTP telah membuat sebuah bandwidth simulator. Ini akan men-download secara bersamaan di halaman web kecepatan penuh dan pada kecepatan yang anda pilih. Demonstrasi ini akan memberikan Anda pemahaman langsung bagaimana throughput rendah dan tinggi latensi mengurangi kegunaan dari Internet sebagai alat komunikasi. Ini tersedia di *http://wireless.ictp.trieste.it/simulator/*

Perencanaan Sambungan

Sebuah sistem komunikasi sederhana terdiri dari dua radio, masing-masing yang terkait dengan antena, kedua nya terpisah oleh path yang harus di lalui. Agar terjadi komunikasi antara keduanya, radio akan memerlykan sinyal minimal ditangkap oleh antena dan masukan kepada konektor antenna di radio. Menentukan apakah sebuah sambungan layak adalah proses yang disebut perhitungan ***link budget.*** Apakah sebuah sinyal dapat atau tidak dilalukan antar radio tergantung pada kualitas dari peralatan yang digunakan dan pada kehilangan sinyal karena jarak, biasa disebut ***path loss (kerugian path).***

Perhitungan link budget

Daya yang tersedia dalam sebuah sistem 802,11 dapat dikarakterisasi oleh faktor berikut:

- **Daya pancar.** Dinyatakan dalam milliwatts atau di dBm. Daya pemancar berkisar 30mW sampai 200mW atau lebih. Daya pancar maksimum yang legal di Indonesia adalah 100mW. Daya TX seringkali tergantung pada kecepatan transmisi. Daya TX yang diberikan perangkat biasanya di tentukan dalam manual yang diberikan oleh pabrik, namun terkadang sulit untuk menemukan. Database online seperti yang disediakan oleh SeattleWireless *(http://www.seattlewireless.net/HardwareComparison*) dapat membantu.

- **Penguatan Antena.** Antena adalah perangkat pasif yang dapat membuat efek amplifikasi berdasarkan bentuk fisik mereka. Antena memiliki karakteristik yang sama ketika menerima dan transmisi. Jadi antena 12 dBi hanya sebuah 12 dBi antena, tanpa perlu menentukan menggunakan modus pengiriman atau penerimaan jenis apa. Antena parabola mempunyai penguatan 19-24 dBi, omnidirectional antena memiliki 5-12 dBi, antena sektoral yang memiliki penguatan sekitar 12-15 dBi.

- **Minimal Received Signal Level** (RSL), atau cukup, sensitivitas dari penerima. Minimum RSL selalu dinyatakan sebagai dBm negatif (- dBm) dan terendah adalah kekuatan sinyal radio dapat dibedakan. RSL minimum adalah tergantung kecepatan, dan sebagai aturan umum kecepatan terendah (1 Mbps) mempunyai sensitivitas terbesar. Minimum RSL biasanya dalam kisaran antara -75 ke -95 dBm. Seperti daya TX, spesifikasi RSL harus disediakan oleh pabrik pembuat peralatan.

- **Kerugian kabel**. Beberapa energy sinyal akan hilang di kabel, di konektor atau pada perangkat lain, pada saat sinyal merambat dari radio ke antena. Hilangnya tergantung pada jenis kabel dan panjangnya. Kerugian sinyal untuk coaxial kabel pendek termasuk konektornya biasanya cukup rendah, yang berkisar antara 2-3 dB. Adalah lebih baik untuk memiliki kabel sependek mungkin.

Ketika menghitung path loss, beberapa efek harus dipertimbangkan. Kita harus mempertimbangkan ***kerugian di udara / ruang (free space loss)***, ***redaman*** dan ***penyebaran.*** Daya sinyal akan berkurang oleh penyebaran geometris dari muka gelombang, umumnya dikenal sebagai free space loss. Dengan mengabaikan semua hal, dua radio yang jauh, penerimaan sinyal yang kecil lebih banyak karena free space loss. Hal ini tidak tergantung lingkungan, hanya tergantung pada jarak. Hal ini terjadi karena kehilangan energy sinyal yang terpancar / menyebar sebagai fungsi jarak dari pemancar.

Menggunakan decibel untuk ungkapan kehilangan dan menggunakan 2,45 GHz sebagai frekuensi sinyal, maka persamaan untuk free space loss

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

L_{fsl} dinyatakan dalam dB dan r adalah jarak antara pemancar dan penerima, dalam meter.

Sumbangan kedua kepada path loss adalah redaman. Hal ini terjadi karena sebagian

kekuatan sinyal diserap ketika gelombang melalui benda padat seperti pohon, dinding, jendela dan lantai bangunan. Redaman dapat bervariasi, tergantung pada struktur objek yang dilalui sinyal, dan sangat sulit untuk mengukur. Cara yang paling nyaman untuk mengemukakan kontribusinya terhadap total kerugian adalah dengan menambahkan "loss yang diijinkan" ke free space loss. Misalnya, pengalaman menunjukkan bahwa pohon menambahkan 10 hingga 20 dB loss pada path yang langsung / direct, sementara dinding berkontribusi 10 hingga 15 dB tergantung konstruksi.

Sepanjang perjalanan sambungan radio, energi RF meninggalkan antena pengirim dan energi akan menyebar. Beberapa energi RF mencapai penerimaan antena secara langsung, sedangkan beberapa akan dipantulkan oleh tanah. Sebagian dari energi RF yang dipantulkan oleh tanah akan mencapai penerimaan antena. Sejak sinyal yang dipantulkan harus menempuh jalan yang lebih jauh, ia tiba di antena menerima lebih lambat dari sinyal yang langsung. Efek ini disebut ***multipath,*** atau dispersi sinyal. Dalam beberapa kasus sinyal yang dipantulkan akan berakumulasi / menambahkan nilai sinyalnya tapi tidak menimbulkan masalah. Ketika sinyal berakumulasi / bertambah pada fasa yang berbeda, sinyal yang diterima akan tidak berguna. Dalam beberapa kasus, penerimaan sinyal di antena dapat menjadi hilang oleh sinyal yang di pantulkan. Hal ini dikenal sebagai fading yang ekstrim, atau ***nulling***. Ada teknik sederhana yang digunakan untuk menangani multipath, disebut ***keragaman antenna (antenna diversity)***. Teknik ini menambahkan antena kedua untuk radio. Multipath adalah fenomena yang terjadi di lokasi yang spesifik. Jika dua sinyal yang berbeda fasa saling menghilangkan di satu lokasi, mereka tidak akan saling menghilangkan di lokasi ke dua, di dekat lokasi pertama. Jika terdapat dua antena, setidaknya satu dari antenna tersebut akan dapat menerima sinyal yang bermanfaat, bahkan jika lain menerima sinyal yang rusak. Dalam perangkat komersial, antena switching diversity digunakan: ada beberapa antena pada beberapa masukan, dengan satu penerima. Sinyal yang diterima hanya melalui satu antena pada suatu waktu. Saat memancar, radio akan menggunakan antena terakhir digunakan untuk penerimaan. Distorsi yang diberikan oleh multipath mengurangi kemampuan dari penerima untuk menangkap sinyal seperti yang terjadi pada sinyal loss. Cara sederhana untuk memperhitungan efek dari penyebaran dalam perhitungan path loss adalah mengubah nilai eksponen dari faktor jarak dari rumus free space loss. Nilai eksponen cenderung meningkat pada lingkungan yang banyak penghamburan (scattering). Nilai eksponen 3 dapat digunakan di luar ruangan dengan pohon-pohon, sedangkan 4 dapat digunakan untuk lingkungan indoor.

Ketika free space loss, redaman, dan penyebaran (scattering) digabungkan, path loss adalah:

$$L\,(dB) = 40 + 10 * n * \log(r) + L\,(diizinkan)$$

Untuk perkiraan kasar kelayakan sambungan, kita dapat mengevaluasi dengan hanya free space loss. Lingkungan dapat membawa kerugian sinyal lebih lanjut, dan harus dianggap sebuah evaluasi dari sambungan yang lebih tepat. Lingkungan hidup sebenarnya adalah salah satu faktor penting, dan tidak boleh dilalaikan.

Untuk mengevaluasi apakah sebuah sambungan layak, kita harus mengetahui karakteristik

dari peralatan yang digunakan dan mengevaluasi path loss. Perlu diketahui bahwa bila Anda melakukan perhitungan ini, anda hanya perlu menambahkan daya TX dari satu sisi link. Jika anda menggunakan radio yang berbeda di kedua sisi sambungan, anda harus menghitung path loss dua kali, sekali untuk setiap arah (menggunakan daya TX yang sesuai untuk setiap perhitungan). Menambah semua penguatan dan mengurangi kerugian akan memberikan,

TX Power Radio 1
+ Antenna Gain Radio 1
- Cable Losses Radio 1
+ Antenna Gain Radio 2
- Cable Losses Radio 2

= Total Gain

Mengurangi Path Loss dari Total Penguatan:

Total Gain
- Path Loss

= Level signal di salah satu sisi sambungan

Jika sinyal yang dihasilkan lebih besar dari level penerima sinyal minimum, maka sambungan tersebut adalah layak! Sinyal yang diterima cukup kuat bagi radio untuk digunakan. Ingat bahwa minimum RSL selalu dinyatakan sebagai negatif dBm, sehingga -56 dBm adalah lebih besar dari -70 dBm. Pada suatu path, variasi di path loss selama periode waktu tertentu dapat sangat besar, sehingga margin (perbedaan antara tingkat sinyal dan menerima sinyal minimum tingkat) harus dipertimbangkan. Margin ini adalah jumlah sinyal di atas kepekaan radio yang harus diterima untuk memastikan yang sambungan radio yang stabil dan kualitas tinggi selama cuaca buruk dan gangguan atmosfir lainnya. Margin antara 10 hingga 15 dB biasanya cukup. Untuk memberikan ruang untuk redaman dan untuk multipath dalam menerima sinyal radio, margin 20dB harusnya cukup aman.

Setelah Anda menghitung link budget di satu arah, ulangi perhitungan arah yang lain. Substitusi daya pancar untuk radio yang kedua, dan membandingkan hasil minimum terhadap tingkat menerima sinyal dari radio pertama.

Contoh perhitungan link budget

Sebagai contoh, kami ingin memperkirakan kelayakan sambungan 5 km, dengan satu akses point dan satu klien radio. Akses point terhubung ke sebuah antena omnidirectional dengan penguatan 10 dBi, sementara klien terhubung ke antenna sectorial dengan penguatan 14 dBi. Daya pancar AP adalah 100mW (atau 20 dBm) dan sensitivitas adalah -89 dBm. Daya pancar

klien adalah 30mW (15 dBm) dan sensitivitas adalah -82 dBm. Kabel yang cukup pendek, dengan kerugian 2dB di setiap sisi.

Menambah semua penguatan dan mengurangi loss untuk AP ke sambungan klien akan memberikan:

```
 20 dBm    (TX Power Radio 1)
+ 10 dBi   (Antenna Gain Radio 1)
-  2 dB    (Cable Losses Radio 1)
+ 14 dBi   (Antenna Gain Radio 2)
-  2 dB    (Cable Losses Radio 2)
--------------------------------------------------
 40 dB = Total Gain
```

Path loss untuk sambungan 5 km, hanya mempertimbangkan free space loss adalah:

Path Loss = 40 + 20log(5000) = 113 dB

Mengurangi kerugian path dari penguatan total

40 dB - 113 dB = -73 dB

Karena -73 dB lebih besar daripada sensitifitas penerima minimum dari klien radio (-82 dBm), level sinyal cukup untuk klien radio agar dapat mendengar akses point. Hanya ada margin 9 dB (82 dB - 73 dB) yang cukup untuk bekerja dengan baik dalam cuaca cerah, tetapi mungkin tidak cukup proteksi untuk menghadapi kondisi cuaca ekstrim.

Selanjutnya kita menghitung sambungan dari klien kembali ke akses point:

```
 15 dBm    (TX Power Radio 2)
+ 14 dBi   (Antenna Gain Radio 2)
-  2 dB    (Cable Losses Radio 2)
+ 10 dBi   (Antenna Gain Radio 1)
-  2 dB    (Cable Losses Radio 1)
-------------------------------------------
 35 dB = Total Gain
```

Tentunya, path loss akan sama pada perjalanan sebaliknya. Jadi level penerimaan sinyal pada sisi akses point adalah:

35 dB - 113 dB = -78 dB

Karena sensitifitas penerima AP adalah -89dBm, menyisakan kita 11dB untuk margin (89dB - 78dB). Secara keseluruhan, sambungan ini mungkin akan bekerja tetapi dapat menggunakan

penguatan sedikit lebih. Dengan menggunakan parabola 24dBi pada sisi klien lebih baik daripada antenna sektoral 14dBi, Anda akan mendapatkan tambahan 10dBi atas penguatan pada kedua arah sambungan (ingat, efek antena adalah timbal balik). Pilihan yang lebih mahal adalah menggunakan daya pancar radio yang lebih tinggipada kedua ujung sambungan, tetapi dicatat bahwa menambahkan amplifier atau daya yang lebih tinggi untuk sebuah sisi umumnya tidak membantu keseluruhan kualitas sambungan.

Software online dapat digunakan untuk menghitung link budget. Misalnya, analisis jaringan nirkabel dari Green Bay profesional paket radio (*http://my.athenet.net/~multiplx/cgi-bin/wireless.main.cgi*) merupakan software yang baik. Super Edisi menghasilkan file PDF berisi zona Fresnel dan grafik radio path. Perhitungan skrip bahkan dapat di-download dari situs web dan diinstal lokal.

Situs Web Terabeam uga menyediakan secara online kalkulator yang sangat baik (*http://www.terabeam.com/support/calculations/index.php*).

Tabel untuk menghitung link budget

Untuk menghitung link budget, hanya perkiraan jarak sambungan anda, kemudian mengisi tabel berikut:

Free Space Path Loss di 2.4 GHz

Jarak (m)	100	500	1.000	3.000	5.000	10.000
Loss (dB)	80	94	100	110	113	120

For more path loss distances, see **Appendix C.**

Penguatan Antenna:

Radio 1 Antenna	**+ Radio 2 Antenna**	**= Total Penguatan Antenna**

Losses:

Radio 1 + Cable Loss (dB)	**Radio 2 + Cable Loss (dB)**	**Free Space Path Loss (dB)**	**'= Total Loss (dB)**

Link Budget for Radio 1 --> Radio 2:

Radio 1 TX Power	+ Antenna Gain	- Total Loss	'= Signal	> Radio 2 Sensitivity

Link Budget for Radio 2 → Radio 1:

Radio 2 TX Power	+ Antenna Gain	- Total Loss	'= Signal	> Radio 1 Sensitivity

Jika sinyal yang diterima lebih besar daripada minimum kekuatan sinyal yang diterima di sambungan dua arah, serta noise di sepanjang sambungan, maka sambungan adalah mungkin.

Software perencanaan sambungan

Walaupun menghitung link budget menggunakan tangan sangat mudah, terdapat sejumlah tool yang tersedia untuk membantu mengotomatisasi proses. Selain itu untuk menghitung free space loss, alat ini akan mengambil banyak faktor lain yang terkait (seperti penyerapan oleh pohon, efek daerah, iklim, dan bahkan memperkirakan path loss di perkotaan). Pada bagian ini, kita akan membahas dua tool gratis / bebas yang berguna untuk perencanaan sambungan nirkabel: Green Bay Packet Radio Profesional online utilitas disain jatingan interaktif, dan RadioMobile.

CGI untuk disain secara interaktif.

Green Bay Packet Radio Profesional grup (GBPRR) telah membuat sekumpulan tool untuk perencanaan jaringan yang tersedia secara online dan gratis. Anda dapat mengakses tool ini secara online di *http://www.qsl.net/n9zia/wireless/page09.html.* Karena tool ini tersedia secara online, mereka dapat di akses menggunakan perangkat yang memiliki web browser dan akses Internet.

Kami akan melihat tool pertama, **Jaringan Wireless Link Analisis,** secara rinci. Anda dapat melihatnya secara online di *http://my.athenet.net/~multiplx/cgi-bin/wireless.main.cgi.*

Untuk memulai, masukkan kanal yang akan digunakan pada sambungan. Kanal dapat di set dalam MHz atau GHz. Jika anda tidak mengetahui frekuensinya, lihat tabel di **Appendix B.** Perlu di catat bahwa tabel hanya di perlihatkan frekwensi tengah kanal, sedangkan tool akan meminta untuk dimasukan frekuensi tertinggi. Perbedaan hasil akhir tidak berbeda jauh, jadi anda bebas menggunakan frekuensi tengah. Untuk menemukan tertinggi yang akan digunakan pada kanal, anda cukup menambahkan 11MHz ke frekuensi tengah.

Selanjutnya, memasukkan rincian untuk sisi pemancar, termasuk jenis saluran transmisi, penguatan antena, dan rincian lainnya. Cobalah untuk mengisi sebanyak mungkin data yang anda tahu atau dapat anda perkirakan. Anda juga dapat memasukkan ketinggian antena dan ketinggian tempat. Data ini akan digunakan untuk menghitung sudut miringnya antena. Untuk menghitung zona Fresnel clearance, anda perlu menggunakan GBPRR Zona Fresnel Kalkulator.

Bagian berikut sangat mirip, tetapi mencakup informasi tentang ujung sambungan lainnya. Masukkan semua data yang tersedia di tempat yang tersedia.

Akhirnya, bagian terakhir menjelaskan iklim, daerah, dan jarak sambungan. Masukkan sebanyak mungkin data yang anda tahu atau anda perkirakan. Jarak sambungan dapat dihitung dengan menentukan lintang dan bujur dari kedua tempat, atau dimasukkan dengan tangan.

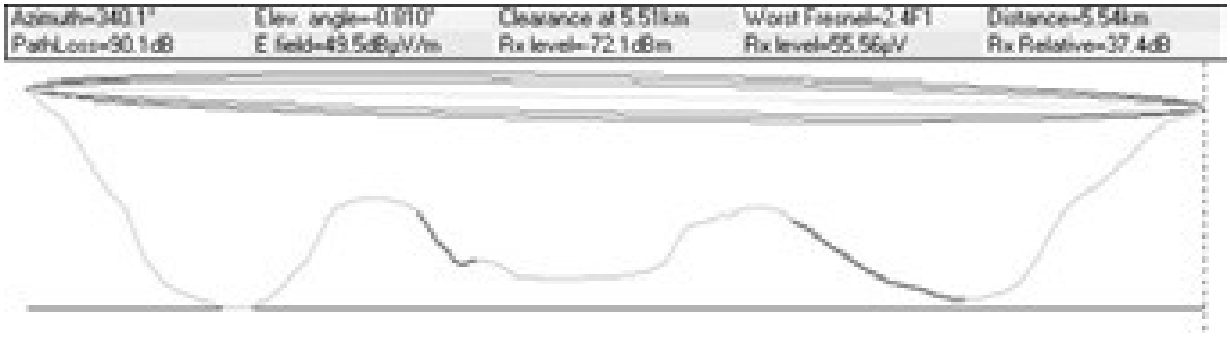
Sekarang, klik tombol Submit untuk memperoleh laporan lebih detil laporan mengenai sambungan yang diusulkan. Ini akan termasuk semua data yang dimasukkan, serta proyeksi path loss, banyaknya error, dan lama waktu sambungan dapat digunakan. Hasil tersebut sepenuhnya semua teori, tetapi cukup memberikan bayangan kasar kepada anda akan kelayakan sambungan. Dengan mengatur nilai pada form, anda dapat bermain "jika-maka?" Untuk melihat bagaimana perubahan berbagai parameter akan mempengaruhi sambungan.

Di samping tool analisis sambungan yang dasar, GBPRR menyediakan "edisi super" yang akan menghasilkan sebuah laporan PDF, serta sejumlah tool lain yang sangat berguna (termasuk diantaranya Kalkulator Zona Fresne, Kalkulayor Jarak & Arah, dan Kalkulator Konversi Decibel). Source code sebagian besar tool ini juga tersedia.

RadioMobile

Mobile radio merupakan tool untuk desain dan simulasi sistem nirkabel. Ia memperkirakan kinerja sambungan radio dengan menggunakan informasi tentang peralatan dan peta digital dari kawasan. Ini adalah perangkat lunak publik domain yang berjalan pada Windows, atau menggunakan Linux dan Wine emulator.

Mobile radio menggunakan ***model digital daerah ketinggian*** untuk perhitungan cakupan, menunjukkan kekuatan sinyal yang diterima di berbagai tempat di sepanjang path. Secara otomatis membangun profil antara dua titik di peta digital yang menunjukkan cakupan wilayah dan zona Fresnel yang pertama. Saat simulasi, ia akan memeriksa line of sight dan menghitung path loss, termasuk loss akibat gangguan. Sangat mungkin untuk membuat jaringan dari beberapa topologi yang berbeda, termasuk jaringan master/slave, point-to-point, dan point-to-multipoint. Software ini dapat digunakan untuk menghitung wilayah cakupan dari base stasiun dalam sebuah sistem point-to-multipoint. Ia bekerja untuk sistem yang memiliki frekuensi dari 100 kHz sampai 200 GHz. ***Peta digital ketinggian (Digital Elevation Map / DEM)*** tersedia secara gratis dari beberapa sumber, dan tersedia untuk sebagian besar wilayah di dunia. DEM tidak menunjukkan pantai atau tanda-tanda yang kita kenali, tetapi mereka dapat dengan mudah dapat dikombinasikan dengan jenis lain data (seperti foto udara atau grafik topografi) pada beberapa lapisan agar lebih berguna dan mudah dikenali. Anda dapat digitisasi peta anda sendiri dan menggabungkannya dengan DEM. Ketinggian peta digital dapat bergabung dengan peta hasil scan, foto satelit dan peta layanan internet (seperti Google Maps) untuk menghasilkan plot prediksi yang akurat.



Gambar 3.20: Kelayakan sambungan, termasuk zona Fresnel dan perkiraan line of sight, menggunakan RadioMobile.

Halaman Web utama Radio Mobile, dengan contoh dan tutorial, tersedia di: *http://www.cplus.org/rmw/english1.html*

RadioMobile menggunakan Linux

Radio Mobile juga akan bekerja menggunakan Wine di bawah Ubuntu Linux. Aplikasi berhasil di jalankan, sayang beberapa tombol label berjalan melebihi frame dari tombol dan akan sulit untuk dibaca.

Kami berhasil membuat Radio Mobile bekerja di Linux dengan menggunakan peralatan berikut:

- IBM Thinkpad x31
- Ubuntu Breezy (v5.10), *http://www.ubuntu.com/*

- Wine versi 20050725, dari repositori Ubuntu Universe

Petunjuk rinci untuk memasang RadioMobile pada Windows di *http://www.cplus.org/rmw/english1.html.* Anda harus mengikuti semua langkah-langkah kecuali untuk langkah 1 (karena sulit untuk extract DLL dari VBRUN60SP6.EXE di Linux). Anda lebih baik mengcopy file MSVBVM60.DLL dari mesin Windows yang sudah memiliki run-time environment Visual Basic 6 yang terinstall, atau Google untuk file MSVBVM60.DLL, dan men-download file.

Lanjutkan dengan langkah 2 dari URL di atas, pastikan unzip file yang di-download pada direktori yang sama dimana anda tempatkan file DLL yang di-download. Perlu diketahui bahwa Anda tidak perlu khawatir tentang hal setelah langkah 4; ini adalah langkah-langkah tambahan yang diperlukan hanya untuk pengguna Windows.

Akhirnya, anda dapat mulai menjalankan Wine dari terminal dengan perintah:

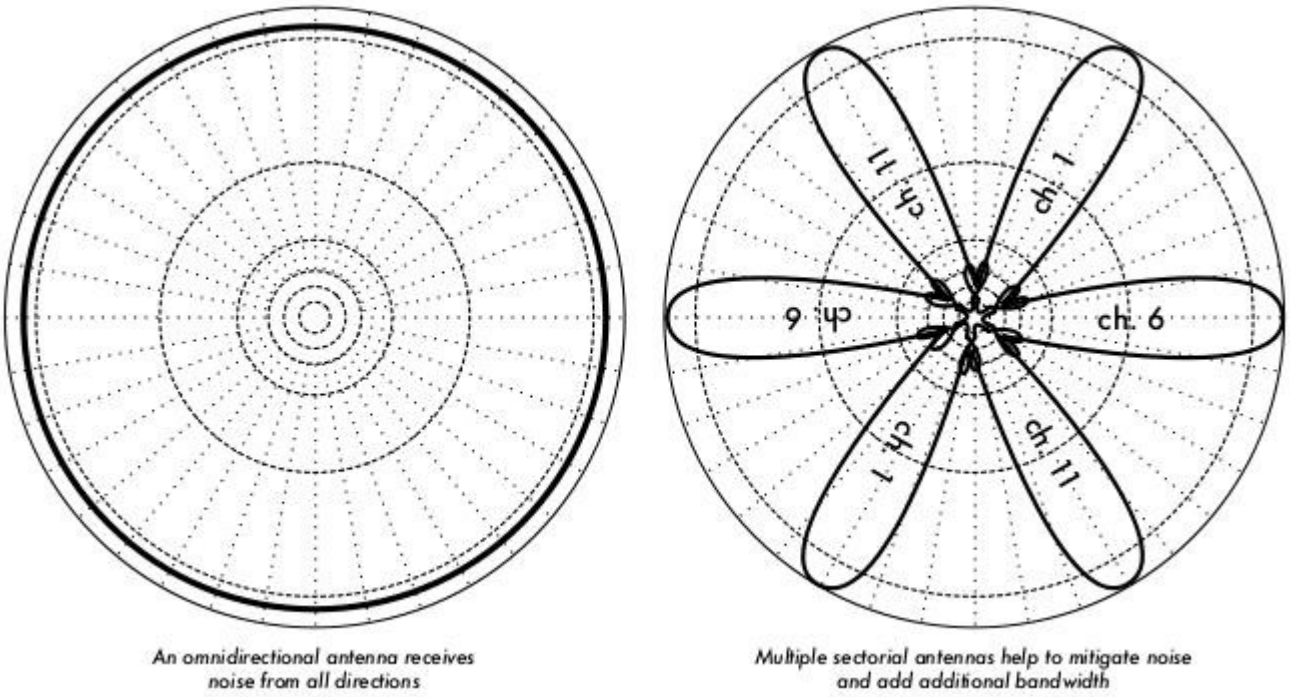
```
# wine RMWDLX.exe
```

Anda akan melihat RadioMobile dengan senang berjalan dalam sesi XWindows.

Menghindari noise

Band unlicensed ISM dan U-NII mewakili sepotongan kecil spektrum elektromagnetik. Karena wilayah band ini dapat digunakan tanpa membayar biaya lisensi, banyak konsumen menggunakan perangkat ini untuk berbagai aplikasi. Cordless telepon, pemancar video, Bluetooth, alat monitor bayi, dan bahkan microwave ovens bersaing dengan jaringan data nirkabel untuk penggunaan sangat terbatas 2,4 GHz band. Sinyal tersebut, serta jaringan nirkabel lokal lainnya, dapat menimbulkan masalah besar terutama untuk sambungan nirkabel link jarak jauh. Berikut ini adalah beberapa langkah yang dapat Anda gunakan untuk mengurangi penerimaan sinyal yang tidak diinginkan.

- **Meningkatkan penguatan antena pada kedua sisi dari sambungan point-to-point.** Antena tidak hanya untuk menambah penguatan sambungan, tetapi mereka cenderung meningkat arah penangkapan sinyal dan menolak noise yang ada sekitar sambungan. Dua parabola dengan penguatan tinggi yang diarahkan satu sama lain akan menolak noise dari arah yang berada di luar jalur sambungan. Menggunakan omnidirectional antena akan menerima noise dari semua arah.



Gambar 3.21: Satu omnidirectional antena vs beberapa sektoral.

- **Gunakan beberapa antenna sektoral jangan menggunakan omnidirectional.** Dengan menggunakan beberapa antenna sektoral, anda dapat mengurangi noise yang diterima di titik distribusi. Dengan membedakan kanal yang digunakan pada setiap sektoral, anda juga dapat meningkatkan bandwidth yang tersedia untuk klien anda.

- **Jangan menggunakan menggunakan amplifier.** Seperti yang kita lihat di **Bab 4,** amplifier dapat membuat masalah gangguan menjadi lebih buruk oleh penguatan tanpa pandang bulu sehingga semua sinyal yang di terima termasuk sumber gangguan di kuatkan. Amplifier juga menimbulkan gangguan bagi pengguna kanal tetangga kita di band.

- **Gunakan kanal terbaik yang ada.** Ingat bahwa kanal 802.11b/g lebarnya 22 MHz, tetapi hanya dipisahkan oleh 5MHz. Lakukan site survey, dan pilih saluran yang sedikit sekali gangguannya. Ingat bahwa penggunaan frekuensi nirkabel dapat berubah sewaktu-waktu karena orang menambahkan perangkat baru (cordless telepon, jaringan lain, dll). Jika sambungan anda tiba-tiba kesulitan mengirimkan paket, anda mungkin perlu melakukan sebuah site survey lagi dan memilih kanal yang lain.

- **Gunakan beberapa hop kecil dan repeater, daripada satu sambungan jarak jauh.** Pastikan sambungan point-to-point anda sependek mungkin. Meskipun sangat mungkin memmbuat sambungan 12 km untuk melintas sebuah kota, anda akan menghadapi banyak gangguan masalah. Jika anda dapat membagi sambungan jarak

jauh menjadi dua atau tiga hop, sambungan akan cenderung lebih stabil. Jelas ini akan sulit untuk membangun sambungan untuk pedesaan dimana listrik dan struktur untuk mendukung belum ada, di samping itu masalah noise juga belum parah di pedesaan.

- **Jika mungkin, gunakan frekuensi 5.8 GHz, atau band unlicensed lainnya.** Sementara hanya ini solusi jangka pendek yang ada, saat ini banyak peralatan konsumen yang terpasang di lapangan yang menggunakan 2,4 GHz. Menggunakan 802.11a atau mengupgrade peralatan 2,4 GHz ke 5,8 GHz untuk menghindari kemacetan di jaringan secara keseluruhan. Teknologi lain yang menarik adalah Ronja (http://ronja.twibright.com/) menggunakan teknologi optik untuk jarak dekat, untuk sambungan bebas noise.

- **Jika semua langkah gagal, gunakan spektrum berlisensi.** Ada beberapa tempat di mana semua spektrum unlicensed sangat aktif digunakan. Dalam kasus ini, mungkin masuk akal untuk menghabiskan uang tambahan untuk peralatan yang eksklusif untuk band yang tidak padat. Untuk sambungan jarak jauh point-to-point yang membutuhkan throughput sangat tinggi dan maksimum uptime, tentu ini adalah salah satu pilihan. Tentu saja, fitur ini mempunyai harga yang jauh lebih tinggi di bandingan peralatan yang menggunakan frekuensi unlicensed.

Untuk mengidentifikasi sumber kebisingan, anda perlu alat yang akan menunjukkan apa yang sedang terjadi di 2.4 GHz. Kami akan melihat beberapa contoh tool ini di Bab 6.

Repeater

Komponen yang paling penting untuk membangun sambungan jaringan jarak jauh adalah ***line of sight*** (sering disingkat sebagai ***LOS***). Sistem terrestrial microwave tidak bisa mentolerir bukit yang tinggi, pohon, atau kendala lain di sambungan jarak jauh. Anda harus mempunyai gambaran yang jelas dari topologi tanah antara dua titik sebelum anda dapat menentukan apakah sambungan tersebut mungkin.

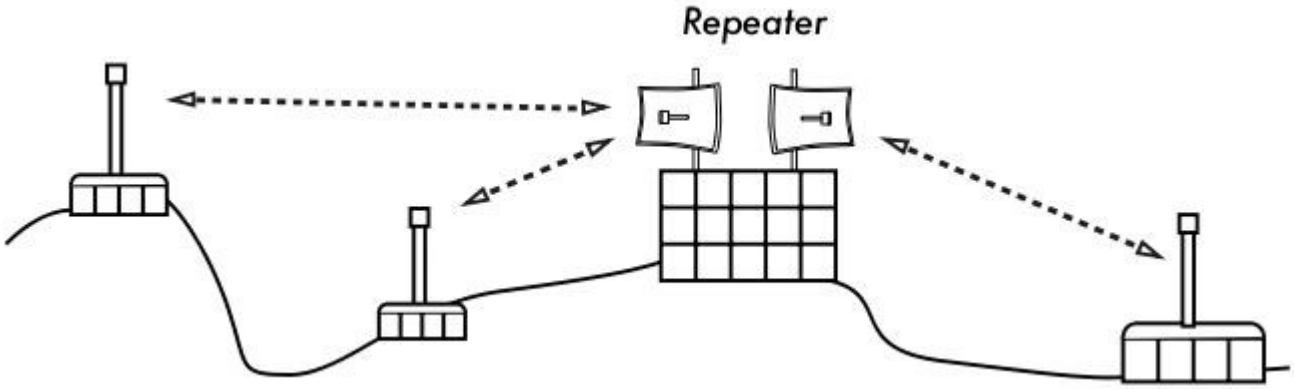
Namun bahkan jika ada gunung antara dua titik, ingat bahwa kendala tersebut kadang-kadang dapat berubah menjadi aset. Gunung mungkin akan memblokir sinyal anda, tetapi jika ada listrik di gunung tersebut akan menjadikan tempat ***repeater*** yang sangat baik.

Repeater adalah node yang dikonfigurasi untuk merelay trafik yang tidak diperuntukkan untuk node itu sendiri. Dalam sebuah jaringan mesh, setiap node adalah pengulang. Dalam jaringan infrastruktur tradisional, node harus dikonfigurasi untuk meneruskan trafik ke node lain.

Sebuah repeater / pengulang dapat menggunakan satu atau lebih perangkat nirkabel. Bila menggunakan sebuah radio (disebut ***repeater one-arm)***, keseluruhan efisiensi akan sedikit lebih rendah dari setengah bandwidth yang tersedia, karena radio dapat mengirim atau

menerima data, tetapi tidak keduanya sekaligus. Perangkat ini lebih murah, lebih sederhana, dan memiliki persyaratan daya lebih rendah. Sebuah repeater / pengulang dengan dua (atau lebih) card radio dapat beroperasi di semua radio dengan kapasitas penuh, sepanjang masing-masing dikonfigurasi untuk menggunakan saluran yang tidak tumpang tindih. Tentu saja, repeater dapat juga memberikan pasokan Ethernet untuk sambungan konektifitas lokal.

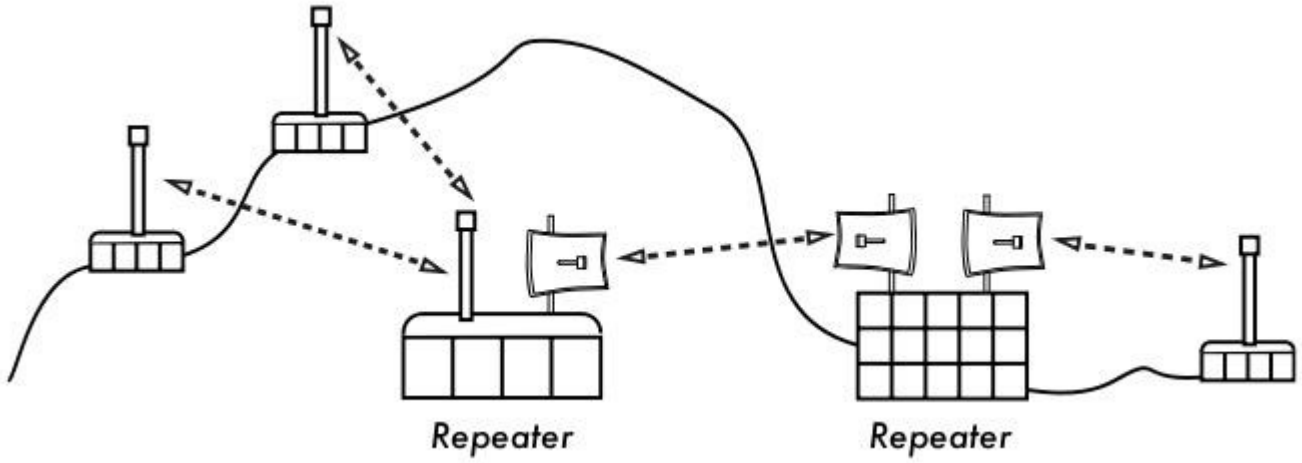
Repeater dapat dibeli sebagai solusi hardware yang lengkap, atau dengan mudah rakitan dengan menghubungkan dua atau lebih node nirkabel dengan dengan kabel Ethernet. Ketika berencana untuk menggunakan repeater dengan teknologi 802.11, ingat bahwa node harus dikonfigurasi untuk mode master, managed, atau ad-hoc. Biasanya, kedua radio repeater dikonfigurasikan untuk mode master, untuk mengijinkan beberapa klien untuk melakukan sambungan ke salah satu sisi pengulang. Tetapi tergantung pada tata letak jaringan anda, satu atau lebih perangkat mungkin perlu di set dalam mode ad-hoc atau mode klien.



Gambar 3.22: Pengulang memforward paket melalui udara antara node yang tidak memiliki line of sight secara langsung.

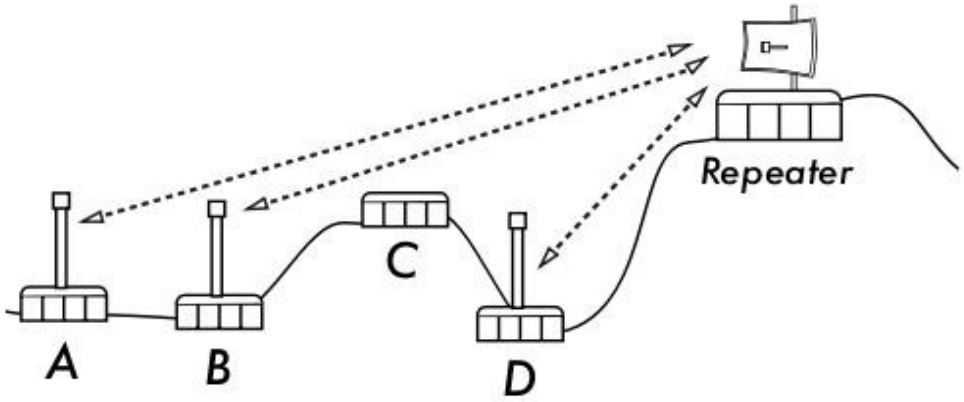
Biasanya, repeaters digunakan untuk mengatasi kendala di sambungan jarak jauh. Misalnya, mungkin ada bangunan di jalur sambungan, tetapi bangunan yang berisi orang. Perjanjian sering kali dapat dilakukan dengan pemilik bangunan untuk menyediakan bandwidth dalam pertukaran hak untuk menggunakan atap dan listrik. Jika pemilik bangunan tidak tertarik, penyewa di lantai tinggi mungkin dapat dibujuk untuk memasang peralatan pada sebuah jendela.

Jika Anda tidak dapat melalui sebuah kendala, anda dapat mengelilingi kendala tersebut. Daripada menggunakan sambungan langsung, coba menggunakan multi-hop untuk menghindari kendala.



Gambar 3.23: Tidak ada daya telah tersedia di bagian atas bukit, tetapi disiasati dengan menggunakan beberapa situs pengulang sekitar dasar bukit.

Terakhir, Anda mungkin perlu mempertimbangkan untuk mundur ke belakang untuk berjalan lurus. Jika ada yang tempat tinggi yang tersedia di arah yang berlawanan, dan tempat ini dapat melihat melewati kendala yang ada, sebuah sambungan yang stabil dapat dibuat melalui rute tidak langsung.



Gambar 3.24: Situs D tidak dapat membuat sambungan yang bersih ke situs A atau B, situs C berada di antaranya dan tidak di tempati sebuah node. Dengan menginstall sebuah pengulang yang tinggi, node A, B, dan D dapat berkomunikasi satu sama lain. Perlu di catat bahwa trafik dari node D sebetulnya berjalan ke seluruh jaringan sebelum pengulang mengulangi trafik tersebut.

Repeater di jaringan ingatkan saya pada prinsip "enam derajat pemisahan". Ide ini mengatakan bahwa siapapun yang anda cari, anda hanya perlu menghubungi lima perantara sebelum menemukan orang tersebut. Repeater di tempat tinggi dapat "melihat" banyak perantara, dan selama Anda berada dalam jangkauan node dari pengulang, anda dapat

berkomunikasi dengan setiap node yang dapat dicapai pengulang.

Optimasi Trafik

Bandwidth diukur dari jumlah bit dikirim dalam sebuah interval waktu. Ini berarti bahwa sepanjang waktu, bandwidth yang tersedia pada semua link mendekati angka tak terhingga. Sayangnya, untuk suatu jangka waktu tertentu, bandwidth yang diberikan oleh suatu jaringan sambungan terbatas. Anda selalu dapat men-download (atau upload) sebanyak yang anda inginkan; anda hanya perlu menunggu cukup lama saja. Tentu saja, manusia sebagai pengguna tidak sabar seperti komputer, dan tidak bersedia untuk menunggu dalam waktu lama sampai informasi yang diinginkan melintasi jaringan. Untuk alasan ini, bandwidth harus dikelola dan diprioritaskan seperti sumber daya terbatas lainnya.

Anda akan dapat secara signifikan meningkatkan waktu respon dan memaksimalkan throughput dengan mengurangi lalu lintas yang tidak diinginkan dari jaringan anda. Bagian ini menjelaskan beberapa teknik umum untuk memastikan bahwa jaringan hanya membawa lalu lintas yang harus melintasi. Untuk diskusi yang lebih dalam dari subjek yang sangat kompleks tentang optimasi bandwidth, lihat buku yang dapat diambil gratisan *“How To Accelerate Your Internet” (http://bwmo.net/).*

Web caching

A web proxy server adalah server pada jaringan lokal yang menyimpan copy dari web, atau halaman web, yang baru atau sering di ambil. Ketika orang selanjutnya mengambil halaman tersebut, mereka akan memperolehnya oleh server proxy lokal, bukan dari Internet. Hal ini membuat akses web menjadi lebih sangat cepat dalam banyak kasus, sekaligus mengurangi penggunaan bandwidth internet secara keseluruhan. Ketika server proxy diimplementasikan, administrator juga harus menyadari bahwa beberapa halaman tidak dapat di cache / di simpan - misalnya, halaman yang output dari script di sisi server, atau konten lainnya yang dihasilkan secara dinamis.

Loading halaman web juga terpengaruh. Dengan lambat sambungan Internet, pemuatan halaman akan lambat, pertama menampilkan beberapa teks dan kemudian menampilkan gambar satu per satu. Dalam sebuah jaringan dengan server proxy, mungkin terdapat penundaan yang tampaknya tidak terjadi apa-apa, kemudian halaman akan dimuat hampir sekaligus. Hal ini terjadi karena informasi yang dikirim ke komputer dengan cepat sehingga yang tampak menghabiskan hanya waktu render halaman. Keseluruhan waktu yang diperlukan untuk memuat seluruh halaman mungkin mengambil hanya sepuluh detik (sedangkan tanpa proxy server, mungkin butuh waktu 30 detik untuk memuat halaman secara bertahap). Kita perlu menjelaskan kepada pengguna yang tidak sabar, mereka cenderung mengatakan proxy membuat segala sesuatu menjadi lebih lambat. Biasanya tugas dari administrator jaringan untuk menangani masalah persepsi pengguna seperti ini.

Produk proxy server

Ada beberapa Web server proxy yang tersedia. Berikut adalah paket perangkat lunak yang banyak digunakan:

- **Squid.** Open source Squid adalah secara standard de facto di perguruan tinggi. Squid adalah gratis, handal, mudah digunakan dan dapat ditingkatkan (misalnya, menambahkan filter konten dan memblokir iklan). Squid menghasilkan catatan yang dapat di analisa menggunakan perangkat lunak seperti Awstats, atau Webalizer, keduanya open source dan menghasilkan laporan grafis yang baik. Dalam kebanyakan kasus, lebih mudah untuk meng-install sebagai bagian dari distribusi daripada men-download-nya dari *http://www.squid-cache.org/* (sebagian besar distribusi Linux seperti Debian, sebagai baik sebagai versi Unix lainnya seperti NetBSD dan FreeBSD telah menyediakan Squid). Panduan konfigurasi Squid yang baik dapat ditemukan pada Wiki Panduan Pengguna Squid di *http://www.deckle.co.za/squid-users-guide/.*

- **Microsoft proxy server 2.0.** Tidak tersedia untuk instalasi baru karena telah digantikan oleh Microsoft ISA server dan tidak lagi didukung. Walaupun demikian digunakan oleh beberapa lembaga, meskipun mungkin tidak harus dipertimbangkan untuk pemasangan baru.

- **Microsoft ISA server.** ISA server merupakan proxy server program yang baik, tetapi terlalu mahal untuk apa yang dia lakukan. Namun, dengan diskon akademik mungkin terjangkau untuk beberapa lembaga. Dia dapat membuat sendiri laporan grafis, namun log file juga dapat dianalisa dengan perangkat lunak analisa populer seperti Sawmill (*http://www.sawmill.net/*). Administrator di situs dengan MS ISA Server harus menghabiskan waktu cukup banyak untuk mengkonfigurasi ijin; karena MS ISA Server sendiri adalah pengkonsumsi bandwidth yang sangat besar. Misalnya, instalasi default dapat dengan mudah mengkonsumsi bandwidth lebih dari situs telah digunakan sebelumnya, karena halaman populer dengan masa kadaluwarsa singkat (seperti situs berita) yang terus di refresh. Oleh karena itu, sangat penting untuk mengatur ijin pre-fetching (pra-mengambilan), dan mengkonfigurasi pra-mengambilan terutama dilakukan di malam hari. ISA Server juga dapat terikat untuk produk konten penyaringan seperti WebSense. Untuk informasi lebih lanjut, lihat: *http://www.microsoft.com/isaserver/* dan *http://www.isaserver.org/.*

Mencegah pengguna untuk mem-bypass server proxy

sementara kebijakan melakukan penyensoran Internet dan membatasi akses informasi merupakan usaha politis yang terpuji, proxy dan firewall adalah tool yang diperlukan di daerah-daerah dengan bandwidth sangat terbatas. Tanpa mereka, stabilitas dan kegunaan dari jaringan yang baik terancam oleh pengguna itu sendiri. Teknik untuk melangkahi server proxy dapat dilihat di *http://www.antiproxy.com/.* Situs ini berguna bagi administrator untuk melihat bagaimana mereka harus mengatur jaringan untuk menghadapi tindakan tersebut.

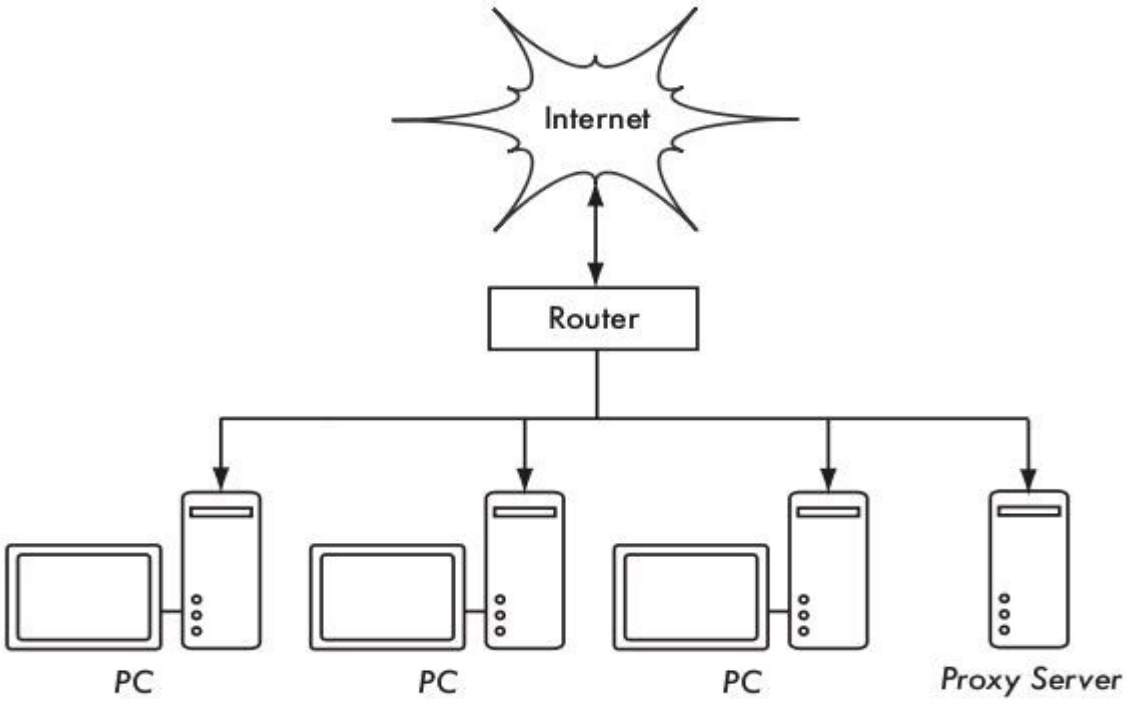
Untuk menerapkan penggunaan caching proxy, anda bisa mempertimbangkan hanya menyiapkan kebijakan akses jaringan akses dan kepercayaan bagi pengguna anda. Dalam tata letak di bawah ini, administrator harus percaya bahwa pengguna tidak akan melewati proxy server.

Dalam hal ini administrator biasanya menggunakan salah satu teknik berikut:

- **Tidak memberikan default gateway melalui alamat DCHP.** Ini mungkin berfungsi untuk sementara waktu, tetapi beberapa pengguna yang ahli jaringan yang ingin mem-bypass proxy mungkin menemukan atau menebak alamat default gateway. Setelah itu terjadi, cerita cenderung tersebar tentang bagaimana untuk memotong proxy.

- **Menggunakan domain atau kebijakan grup.** Hal ini sangat berguna untuk mengkonfigurasi benar pengaturan server proxy untuk Internet Explorer pada semua komputer dalam domain, namun tidak sangat berguna untuk mencegah orang yang akan mem-bypass proxy, karena tergantung pada pengguna login ke NT domain. Pengguna dengan Windows 95/98/ME komputer dapat membatalkan login-nya pada dan kemudian mengabaikan proxy, dan seseorang yang mengetahui password lokal pada Windows NT/2000/XP komputer dapat login secara lokal dan melakukan hal yang sama.

- **Mengemis dan berkelahi dengan pengguna.** Pendekatan ini, sementara umum digunakan, bukan merupakan solusi yang baik untuk administrator jaringan.



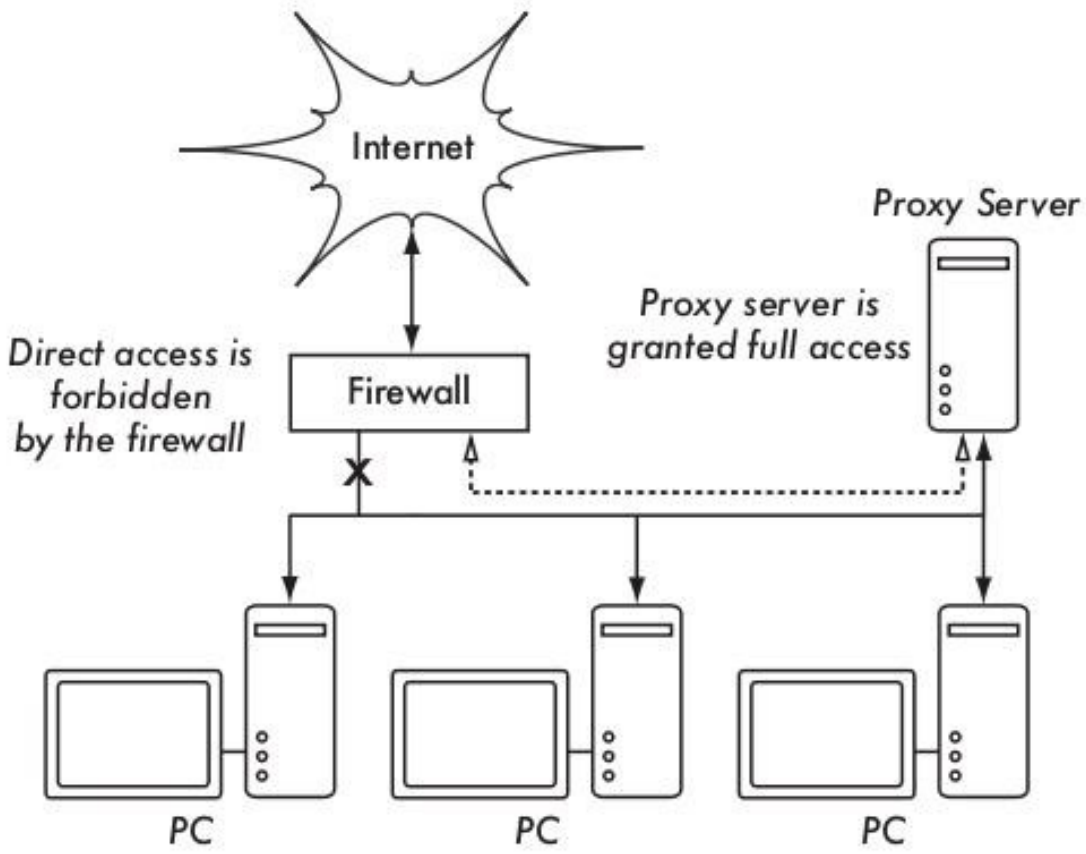
Gambar 3.25: Jaringan ini bergantung pada pengguna terpercaya untuk mengkonfigurasi dengan benar PC mereka untuk menggunakan server proxy.

Satu-satunya cara untuk memastikan bahwa proxy tidak dapat bypassed adalah dengan menggunakan tata letak jaringan yang benar, dengan menggunakan salah satu dari tiga teknik yang dijelaskan di bawah ini.

Firewall

Cara yang lebih dapat diandalkan untuk memastikan bahwa PC tidak melewati proxy dapat menggunakan firewall. Firewall dapat dikonfigurasi agar hanya memperbolehkan server proxy HTTP untuk membuat permintaan ke Internet. Semua PC lain yang diblokir, seperti yang ditunjukkan dalam **Gambar 3.26.**

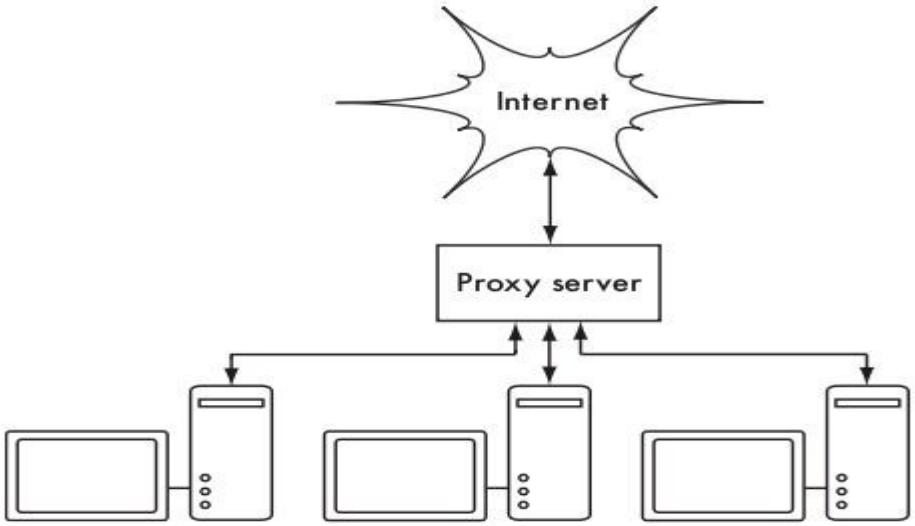
Mengandalkan firewall mungkin cukup mungkin tidak, tergantung bagaimana konfigurasi firewall. Jika hanya memblok akses dari LAN port 80 pada web server, akan ada cara untuk pengguna pandai untuk mengatasinya. Selain itu, mereka akan dapat menggunakan protokol lain yang lapar bandwidth seperti BitTorrent atau Kazaa.



Gambar 3.26: Firewall mencegah PC untuk mengakses Internet secara langsung, namun memungkinkan akses melalui proxy server.

Dua card jaringan

Mungkin metode yang paling dapat diandalkan adalah memasang dua card jaringan di proxy server dan menghubungkan jaringan LAN kampus ke Internet seperti yang ditunjukkan di bawah ini. Dengan cara ini, tata letak jaringan menjadikannya secara fisik tidak mungkin untuk mencapai Internet tanpa melalui proxy server.



Gambar 3.27: Satu-satunya rute ke Internet melalui proxy.

Proxy server dalam diagram ini seharusnya tidak mengaktifkan IP forwarding, kecuali administrator mengetahui apa yang mereka ingin membiarkan lewat.

Satu keuntungan besar pada desain ini adalah sebuah teknik yang dikenal sebagai *transparan proxy* dapat digunakan. Menggunakan transparent proxy berarti bahwa permintaan pengguna web secara otomatis akan diteruskan ke proxy server, tanpa perlu mengkonfigurasi web browser secara manual untuk menggunakannya. Ini secara efektif memaksa semua lalu lintas yang akan web cache, menghilangkan banyak kemungkinan pengguna membuat kesalahan, dan bahkan akan bekerja dengan perangkat yang tidak mendukung penggunaan manual proxy. Untuk informasi lebih rinci tentang konfigurasi transparent proxy dengan Squid, lihat:

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

Routing berbasis kebijakan

Salah satu cara untuk mencegah mem-bypass proxy menggunakan peralatan Cisco adalah dengan kebijakan routing. Router Cisco akan secara transparan meminta permohonan akses web ke server proxy. Teknik ini digunakan di Universitas Makerere. Keuntungan metode ini adalah bahwa, jika proxy server down, kebijakan rute dapat sementara dihapus, memungkinkan pelanggan untuk koneksi langsung ke internet.

Miror Situs Web

Dengan izin dari pemilik atau webmaster dari sebuah situs, seluruh situs dapat dimirror ke server lokal dimalam hari, jika tidak terlalu besar. Ini adalah sesuatu yang mungkin perlu dipertimbangkan untuk website yang penting untuk sebuah organisasi atau yang sangat populer dikalangan pengguna web. Ini mungkin ada beberapa kegunaan, tetapi memiliki beberapa potensi berbahaya. Misalnya, jika situs yang dimirror berisi CGI script atau konten yang dinamis interaktif yang memerlukan masukan dari pengguna, ini akan menimbulkan masalah. Salah satu contoh adalah situs yang membutuhkan orang untuk mendaftar secara online untuk konferensi. Jika seseorang mendaftarkan diri ke server mirror (dan script yang di mirror berjalan), maka operator situs yang asli-nya tidak akan memiliki informasi tentang orang yang mendaftar.

Karena situs mirror dapat melanggar hak cipta, teknik ini hanya dapat digunakan dengan izin dari situs yang bersangkutan. Jika situs menjalankan ***rsync***, situs dapat menggunakan mirror rsync. Ini mungkin yang tercepat dan paling efisien untuk menjaga isi situs mirror tetap sinkron. Jika remote web server rsync tidak berjalan, yang disarankan untuk menggunakan perangkat lunak adalah program ***wget.*** Ini adalah bagian dari sebagian besar versi Unix / Linux. Sebuah versi Windows dapat dilihat di *http://xoomer.virgilio.it/hherold/,* atau tool paket Unix bebas Cygwin (*http://www.cygwin.com/)*.

Sebuah skrip dapat mengatur untuk menjalankan setiap malam pada sebuah lokal web server dan lakukan berikut:

- Ubah direktori ke web server root dokumen web server: misalnya, **/var/www/** pada Unix, atau **C:\Inetpub\wwwroot** pada Windows.
- Mirror situs web menggunakan perintah:

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

Situs web yang di mirror akan ada di direktori **www.python.org**. Web server sebaiknya

sekarang dikonfigurasi untuk melayani isi direktori sebagai virtual host berbasis nama. Mengatur lokal ke server DNS untuk entri palsu dari situs ini. Agar ini dapat bekerja, PC klien harus dikonfigurasi untuk menggunakan server DNS lokal sebagai DNS primer. (Hal ini dianjurkan dalam setiap kasus, karena lokal caching server DNS akan mempercepat waktu respon web).

Pre-populate cache menggunakan wget

Daripada menyiapkan sebuah situs web mirror seperti yang dijelaskan di bagian sebelumnya, pendekatan yang lebih baik untuk mengisi proxy cache menggunakan proses otomatis. Metode ini telah dijelaskan oleh J.J. Eksteen dan J.P.L. Cloete dari CSIR di Pretoria, Afrika Selatan, di sebuah kertas berjudul "**Enhancing International World Wide Web Access in Mozambique Through the Use of Mirroring and Caching Proxies"**. Dalam makalah ini (tersedia di *http://www.isoc.org/inet97/ans97/cloet.htm)* mereka menjelaskan bagaimana proses tersebut bekerja:

> *"Sebuah proses otomatis yang mengambil situs home page dan yang ditentukan jumlah halaman tambahan (secara rekursif mengikuti link HTML pada halaman diambil) melalui penggunaan proxy. Daripada menulis halaman yang di ambil ke disk lokal, proses mirror membuang halaman yang diambil. Hal ini dilakukan dalam rangka untuk menghemat sumber daya sistem serta menghindari kemungkinan konflik hak cipta. Dengan menggunakan proxy sebagai perantara, halaman yang di ambil dijamin akan di cache oleh proxy seperti klien jika mengakses halaman. Bila klien mengakses halaman yang diambil, ia disajikan dari cache dan tidak melalui sambungan internasional yang padat. Proses ini dapat dijalankan di waktu off-peak untuk memaksimalkan pemanfaatan bandwidth dan tidak untuk bersaing dengan aktifitas akses lainnya."*

Perintah berikut (dijadwalkan untuk berjalan di malam hari atau sekali setiap minggu) adalah yang diperlukan (berulang lagi untuk setiap situs yang memerlukan pra-populasi).

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

Pilihan berikut mengaktifkan hal:

- **-m**: Mirror seluruh situs. wget dimulai di *www.python.org* dan mengikuti semua hyperlink, sehingga semua sub-halaman didownload.
- **--proxy-on**: memastikan bahwa wget menggunakan server proxy. Hal ini dapat tidak diabaikan jika digunakan transparent proxy.
- **--cache=off**: memastikan konten yang segar akan diambil dari Internet, dan tidak lokal dari server proxy.
- **--delete after**: Menghapus yang copy di mirror. Konten yang dimirror tetap di proxy cache jika ada cukup ruang disk, dan parameter server proxy-caching ditetapkan

dengan benar.

Selain itu, wget memiliki banyak pilihan lain; misalnya, untuk memberikan password untuk website yang memerlukan password. Ketika menggunakan tool ini, squid harus dikonfigurasi dengan ruang disk cukup untuk menampung semua situs pra-populasi dan lainnya (untuk penggunaan normal Squid melibatkan halaman selain yang pra-populasi). Untungnya, harddisk saat ini menjadi semakin murah dan ukuran disk yang jauh lebih besar dari sebelumnya. Namun, teknik ini hanya dapat digunakan dengan beberapa situs yang dipilih. Situs ini tidak boleh terlalu besar untuk proses selesai sebelum hari kerja dimulai, dan harus memperhatikan baik-baik sisa ruang harddisk.

Hirarki cache

Ketika suatu organisasi memiliki lebih dari satu proxy server, proxy cache dapat berbagi informasi di antara mereka. Misalnya, jika halaman web server yang ada di cache A, tetapi tidak dalam cache dari server B, pengguna terhubung melalui server B mungkin mendapatkan obyek cache dari server A melalui server B. ***Inter-Cache Protocol (ICP)*** dan ***Cache Array Routing Protocol (CARP)*** dapat berbagi informasi cache. CARP dianggap protokol yang lebih baik. Squid mendukung kedua protokol, dan MS ISA Server mendukung CARP. Untuk informasi lebih lanjut, lihat *http://squid-docs.sourceforge.net/latest/html/c2075.html.* Ini berbagi informasi dari cache mengurangi penggunaan bandwidth di organisasi di mana lebih dari satu proxy digunakan.

Spesifikasi proxy

Pada jaringan kampus universitas, seharusnya ada lebih dari satu server proxy, baik untuk kinerja dan juga untuk alasan cadangan. Pada hari ini dengan harddisk lebih murah dan lebih besar, server proxy yang ampuh dapat dibangun, dengan 50 GB atau lebih ruang harddisk yang dialokasikan untuk cache. Kinerja harddisk adalah penting, sehingga harddisk SCSI yang cepat akan melakukan yang terbaik (meskipun sebuah IDE berbasis Cache adalah lebih baik daripada tidak ada sama sekali). RAID atau mirroring tidak dianjurkan. Juga disarankan untuk menggunakan harddisk yang terpisah untuk cache yang terdedikasi. Misalnya, satu harddisk untuk cache, dan yang harddisk kedua untuk sistem operasi dan pencatatan cache. Squid dirancang untuk menggunakan RAM sebanyak yang dia dapat, karena bila data yang diambil dari RAM ini lebih cepat daripada jika berasal dari hard disk. Untuk jaringan kampus, gunakan memori RAM 1GB harus atau lebih:

- Selain dari memori yang dibutuhkan untuk sistem operasi dan aplikasi lain, Squid memerlukan 10 MB RAM untuk setiap 1 GB dari disk cache. Oleh karena itu, jika ada 50 GB yang dialokasikan untuk ruang disk caching, Squid akan memerlukan tambahan memori 500 MB.
- Mesin juga membutuhkan 128 MB untuk Linux dan 128 MB untuk Xwindows.

- 256 MB lain harus ditambahkan untuk aplikasi lain dan agar semuanya dapat berjalan dengan mudah. Kinerja mesin akan meningkat dengan pesat dengan menginstall memori yang besar, karena ini mengurangi kebutuhan untuk menggunakan hard disk. Memori ribuan kali lebih cepat dari hard disk. Sistem operasi modern sering menyimpan data yang sering di akses dalam memori jika ada cukup tersedia RAM. Tetapi mereka menggunakan halaman file sebagai memori tambahan ketika mereka tidak memiliki cukup RAM.

DNS caching dan optimalisasi

Caching-server DNS hanya mempunyai authoritas untuk semua domain, tetapi hanya cache dari hasil pencarian yang ditanyakan oleh klien mereka. Sama seperti proxy server yang mengcache halaman web yang populer untuk waktu tertentu, Alamat DNS akan di cache sampai Time To Live (TTL) mereka berakhir. Ini akan mengurangi jumlah lalu lintas DNS pada sambungan Internet Anda, sebagai DNS cache mungkin dapat memenuhi banyak permintaan dari jaringan lokal. Tentu saja, komputer klien harus dikonfigurasi untuk menggunakan caching-server sebagai DNS server mereka. Bila semua klien menggunakan server ini sebagai server DNS primer, ia akan dengan cepat mengisi cache dari alamat IP ke nama mesin, sehingga nama mesin yan sebelumnya pernah diminta akan dapat direspons dengan cepat. DNS server yang mempunyai authoritas untuk sebuah domain dapat juga bertindak sebagai cache DNS untuk pemetaan dari host di resolve oleh mereka.

Bind (named)

Bind adalah program standard yang secara de facto digunakan untuk layanan DNS di Internet. Ketika Bind terinstal dan dijalankan, akan bertindak sebagai caching server (tidak perlu melakukan konfigurasi tambahan). Bind dapat diinstal dari sebuah paket seperti Debian atau sebuah paket RPM. Instalasi dari sebuah paket biasanya merupakan cara termudah. Dalam Debian, tulis

```
apt-get install bind9
```

Selain itu untuk menjalankan cache, Bind juga dapat menjadi mesin authoritas sebuah zona, bertindak sebagai hamba / slave untuk authoritas zona, melaksanakan split horizon, dan melakukan semua yang mungkin dengan DNS.

dnsmasq

Salah satu alternatif caching DNS server ***dnsmasq***. Tersedia untuk BSD dan sebagian besar distribusi Linux, atau dari *http://www.thekelleys.org.uk/dnsmasq/*. Keuntungan terbesar dari dnsmasq adalah fleksibilitas: dengan mudah bertindak sebagai sebuah caching DNS proxy dan sumber authoritas dari host dan domain, tanpa konfigurasi file zona yang rumit. Update zona data bahkan dapat dilakukan tanpa me-restart layanan. Dia juga dapat berfungsi sebagai DHCP server, dan akan mengintegrasikan permintaan layanan DNS dengan DHCP

host. Sangat ringan, stabil, dan sangat fleksibel. Bind adalah pilihan yang lebih baik untuk jaringan sangat besar (lebih dari beberapa ratus node), tetapi kemudahan dan fleksibilitas dnsmasq menjadikannya menarik untuk jaringan ukuran kecil sampai medium.

Windows NT

Untuk memasang servis DNS pada Windows NT4: pilih Control Panel -> Jaringan -> Layanan Tambahkan Microsoft DNS server. Masukkan CD Windows NT4 ketika diminta. Mengkonfigurasi caching-server hanya dalam NT adalah dijelaskan dalam Knowledge Base artikel 167.234. Dari artikel:

> *"Cukup instal DNS dan menjalankan Sistem Nama Domain Manager. Klik DNS di dalam menu, pilih New Server, dan ketik alamat IP Anda di mana komputer Anda telah terinstal DNS. Anda sekarang memiliki caching-only DNS server."*

Windows 2000

Instalasi servis DNS: Start -> Settings -> Control Panel -> Add/Remove Software. Dalam Add/ Remove Windows Components, pilih Components -> Network Services -> Details -> Domain Name System (DNS). Kemudian mulai DNS MMC (Start -> Program -> Administrative Tools -> DNS) Dari menu Action pilih "Connect To Computer ..." Pada jendela Select Target Computer, aktifkan "The following computer:" dan masukkan nama server DNS ingin anda cache. Jika ada . [dot] di DNS manager (ini akan muncul secara default), ini berarti bahwa server DNS berfikir itu adalah root server DNS dari Internet. Hal ini tentu tidak. Hapus . [dot] agar semua dapat bekerja.

Split DNS dan mirror server

Tujuan split DNS (juga dikenal sebagai ***split horizon***) adalah untuk memberikan tampilan yang berbeda dari domain anda ke dalam dan jaringan di luar. Ada banyak cara untuk melakukan split DNS, tetapi untuk alasan keamanan, direkomendasikan bahwa anda memiliki dua DNS server internal dan eksternal yang terpisah (masing-masing dengan database yang berbeda).

Split DNS memungkinkan klien dari jaringan kampus untuk me-resolve alamat IP untuk domain kampus untuk alamat IP lokal RFC1918, sementara sisanya dari Internet yang akan me-resolve nama ke alamat IP yang berbeda. Hal ini dicapai dengan dua zona berbeda pada dua server DNS untuk domain yang sama.

Salah satu zona digunakan oleh klien jaringan internal dan oleh pengguna lain di Internet. Misalnya, dalam jaringan berikut pengguna pada kampus Makerere untuk h*ttp://www.makerere.ac.ug/* akan di-resolve menjadi 172.16.16.21, sedangkan pengguna lain di Internet untuk mendapatkan di-resolve menjadi 195.171.16.13.

DNS server di kampus dalam diagram di atas memiliki zona file untuk makerere.ac.ug dan dikonfigurasi seperti apabila otoritatif untuk domain tersebut. Selain itu, ia bertindak sebagai DNS caching server untuk Makerere kampus, dan semua komputer di kampus dikonfigurasikan untuk menggunakannya sebagai server DNS. DNS record untuk kampus server DNS akan terlihat seperti ini:

```
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
```

Tetapi pada server DNS di Internet yang benar-benar authoritif untuk domain makerere.ac.ug. DNS record untuk zona eksternal ini akan terlihat seperti ini:

```
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
```

Split DNS tidak tergantung pada menggunakan alamat RFC 1918. ISP di Afrika, misalnya, meng-hosting sebuah situs web atas nama sebuah universitas tetapi juga mirror situs web yang sama di Eropa. Apabila klien dari ISP yang mengakses situs web, ia mendapatkan alamat IP di Afrika ISP, sehingga lalu lintas dan tetap dalam negara yang sama. Bila pengunjung dari negara-negara lain yang mengakses situs web, mereka mendapatkan alamat IP dari server mirror web di Eropa. Dengan cara ini, pengunjung internasional tidak membuat macet sambungan VSAT ISP saat mengunjungi situs web universitas. Hal ini menjadi solusi yang menarik, karena jasa hosting web yang dekat dengan backbone Internet sangat murah.

Optimasi sambungan Internet

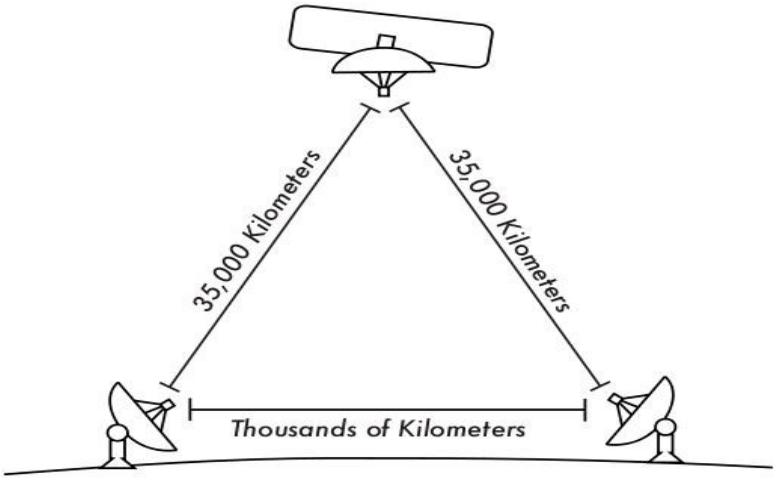
Seperti yang disebutkan sebelumnya, throughput jaringan sampai dengan 22 Mbps dapat dicapai dengan menggunakan peralatan standar nirkabel 802.11g. Throughput ini kemungkinan sepuluh kali lebih tinggi daripada sambungan Internet yang diberikan oleh provider anda, dan harusnya dapat nyaman untuk mendukung banyak pengguna internet secara serentak.

Tetapi jika sambungan utama Internet anda adalah melalui sambungan VSAT, anda akan menemukan beberapa masalah performa jika Anda mengandalkan parameter standar

TCP/IP. Dengan mengoptimalkan sambungann VSAT anda, anda dapat secara signifikan meningkatkan waktu respon ketika mengakses Internet.

Faktor TCP/IP pada sambungan satelit

VSAT yang sering disebut sebagai jaringan ***pipa panjang yang berlemak.*** Istilah ini merujuk kepada faktor-faktor yang mempengaruhi kinerja TCP/IP pada setiap jaringan yang berbandwidth yang relatif besar, tetapi latensi tinggi. Sebagian besar sambungan Internet di Afrika dan bagian lain dari negara berkembang adalah melalui VSAT. Oleh karena itu, meskipun sebuah universitas yang mendapat koneksi melalui sebuah ISP, bagian ini mungkin berlaku jika ISP melalui sambungan VSAT. Latensi yang tinggi dalam jaringan satelit adalah disebabkan oleh jarak yang sangat jauh ke satelit dan kecepatan cahaya yang konstan. Ini menambah jarak sekitar 520 ms untuk waktu Round Trip Time (RTT) paket, dibandingkan dengan RTT antara Eropa dan Amerika Serikat yang hanya sekitar 140 ms.



Gambar 3.28:
Karena kecepatan cahaya dan jarak yang jauh, sebuah paket ping dapat mengambil lebih dari 520 ms untuk memperoleh jawaban dari sambungan VSAT.

Faktor yang paling signifikan berdampak pada kinerja TCP/IP kinerja adalah **RTT yang panjang**, **perkalian bandwidth dan delay yang besar**, dan **kesalahan transmisi.**

Secara umum, sistem operasi yang mendukung implementasi TCP/IP modem harus digunakan pada jaringan satelit. Implementasi ini mendukung ekstensi RFC 1323:

- Pilihan ***skala jendela*** untuk mendukung TCP window dengan ukuran besar (lebih besar dari 64KB).
- ***Acknowledge yang selektif (SACK)*** untuk mengaktifkan lebih cepat dari pemulihan kesalahan transmisi.
- Pencatatan waktu yang tepat untuk menghitung nilai RTT dan retransmission timeout untuk sambungan yang digunakan.

Round-Trip Time (RTT) yang panjang

Sambungan satelit rata-rata memiliki RTT sekitar 520ms untuk satu hop. TCP menggunakan mekanisme slow-start pada awal sambungan untuk menemukan parameter TCP/IP untuk sambungan. Waktu yang di perlukan pada tahapan slow-start adalah proporsional dengan RTT, dan untuk sambungan satelit berarti TCP akan tetap di mode slow-start untuk waktu yang sedikit lebih lama daripada yang seharusnya. Hal ini menurun drastis throughput dalam waktu pendek di awal sambungan TCP. Hal ini dapat dilihat saat mengakses sebuah situs situs web kecil yang mungkin mengambil waktu muat yang lama sekali, tetapi ketika sebuah file besar ditransfer sepertinya kecepatan yang di peroleh cukup baik.

Selain itu, ketika ada paket yang hilang, TCP memasuki fase kontrol kemacetan, dan berkat RTT yang lebih tinggi, akan berada pada fase tersebut untuk waktu yang lebih panjang, sehingga mengurangi throughput baik, untuk sambungan TCP durasi pendek maupun durasi panjang.

Perkalian Bandiwdth-Delay yang besar

Jumlah data yang melewati sebuah sambungan pada suatu saat adalah perkalian dari bandwidth dan RTT. Karena tingginya latensi pada sambungan satelit, perkalian bandwidth-delay menjadi sangat besar. TCP/IP memungkinkan sebuah mesin remote untuk mengirim sejumlah data di muka tanpa acknowledgement. Acknowledgement biasanya diperlukan untuk semua data yang dikirim pada sambungan TCP/IP. Namun, host remote selalu diizinkan untuk mengirim sejumlah data tanpa acknowledgement, yang menjadi penting untuk mencapai kecepatan transfer yang baik pada sambungan yang memiliki perkalian bandwidth-delay yang besar. Besarnya data yang dikirim tanpa acknowledge disebut ***ukuran TCP windows.*** Besarnya TCP windows biasanya 64KB di implementasi TCP/IP modern.

Pada jaringan satelit, nilai perkalian bandwidth-delay sangat penting. Untuk memanfaatkan sepenuhnya sambungan, ukuran TCP Windows di sambungan harus sama dengan perkalian bandwidth-delay. Jika ukuran TCP windows terbesar yang di perbolehkan adalah 64KB, maksimum throughput secara teori yang dicapai melalui satelit adalah (ukuran jendela) / RTT, atau 64KB / 520 ms. Hal ini memberi kecepatan data maksimum 123 KB/s, atau 984 kbps, tanpa memperhitungkan fakta bahwa kapasitas sambungan mungkin jauh lebih besar.
Setiap segmen TCP header berisi parameter yang disebut ***advertised windows,*** yang menentukan berapa banyak tambahan byte data yang siap di terima oleh penerima. Jendela yang diiklankan adalah ketersediaan buffer / penyangga di penerima saat itu. Pengirim tidak diperbolehkan untuk mengirim lebih banyak byte dari jendela yang diiklankan. Untuk memaksimalkan kinerja, pengirim harus mengatur ukuran penyangga mengirim dan penerima harus mengatur ukuran buffer untuk menerima tidak kurang dari perkalian bandwidth-delay. Penyangga ini memiliki ukuran maksimum nilai 64KB di implementasi TCP/IP paling modern.

Untuk mengatasi masalah TCP/IP dari sistem operasi yang tidak meningkatkan ukuran

jendela luar 64KB, yang dikenal sebagai teknik ***TCP acknowledgement spoofing*** dapat digunakan (lihat Peningkatan Kinerja proxy, di bawah).

Kesalahan transmisi

Dalam implementasi TCP/IP yang lama, paket loss selalu dianggap disebabkan oleh tabrakan (bukan karena kesalahan sambungan). Bila ini terjadi, TCP melakukan menghindari kemacetan, yang memerlukan tiga duplikat ACKs atau slow start dalam kasus timeout. Karena dari nilai RTT yang panjang, jika fasa control-congestion ini di mulai, TCP/IP pada sambungan satelit akan memakan waktu lebih lama untuk kembali ke tingkat throughput sebelumnya. Oleh karena itu kesalahan pada sambungan satelit akan berdampak lebih serius terhadap kinerja TCP dibandingkan dengan sambungan dengan latensi rendah. Untuk mengatasi keterbatasan ini, mekanisme seperti ***Selective Acknowledgement (SACK)*** telah dikembangkan. SACK menetapkan paket mana yang telah diterima, memungkinkan pengirim untuk mengirim ulang hanya segmen / paket yang karena kesalahan link.

White paper Implementasi detail TCP/IP dari Microsoft Windows 2000 menyatakan

> *"Windows 2000 memperkenalkan dukungan fitur kinerja yang penting yang dikenal sebagai Selective Acknowledgement (SACK). SACK sangat penting untuk sambungan dengan ukuran jendela TCP yang besar."*

SACK telah menjadi fitur standar di Linux dan BSD kernel cukup lama. Pastikan bahwa router Internet dan ISP anda mendukung SACK di kedua sisi.

Implikasi untuk Universitas

Jika sebuah situs memiliki sambungan 512 kbps ke Internet, standar pengaturan TCP/IP kemungkinan cukup, karena ukuran jendela 64 KB dapat mengisi hingga 984 kbps. Tetapi jika universitas memiliki lebih dari 984 kbps, mungkin dalam beberapa kasus tidak mendapatkan penuh bandwidth yang tersedia karena sambungan ke faktor "jaringan pipa panjang dan berlemak" yang dibahas di atas. Faktor-faktor tersebut menyiratkan bahwa mereka mencegah satu mesin mengisi seluruh bandwidth. Ini bukan hal yang buruk pada siang hari, karena banyak orang yang menggunakan bandwidth. Tetapi jika, misalnya, ada download besar dijadwalkan pada malam hari, administrator mungkin ingin mereka download untuk membuat penuh penggunaan bandwidth, dan faktor "jaringan pipa panjang dan berlemak" mungkin merupakan salah satu kendala. Ini mungkin juga menjadi penting jika sejumlah besar jaringan anda melalui satu jalur satu terowongan atau koneksi VPN yang berujung pada sambungan VSAT.

Administrator mungkin mempertimbangkan mengambil langkah-langkah untuk memastikan bahwa penggunaan bandwidth secara maksimal dapat dicapai dengan menset TCP/IP mereka. Jika suatu universitas telah menerapkan jaringan dimana semua lalu lintas harus

melalui proxy (diperkuat dengan tata letak jaringan), maka mesin yang membuat sambungan ke Internet hanya proxy dan mail server.

Untuk informasi lebih lanjut, lihat *http://www.psc.edu/networking/perf_tune.html.*

Meningkatkan kinerja proxy (PEP)

Ide untuk meningkatkan Kinerja-proxy dijelaskan di RFC 3135 (lihat *http://www.ietf.org/rfc/rfc3135)*, dan membutuhkan proxy server dengan cache disk besar yang memiliki ekstensi RFC 1323, diantara fitur yang dibutuhkan. Sebuah laptop memiliki TCP sesi dengan PEP di ISP. PEP tersebut, dan lawannya di provier satelit, berkomunikasi menggunakan sesi TCP yang berbeda atau bahkan menggunakan protokol mereka sendiri. PEP yang di provider satelit mendapat file dari web server. Dengan cara ini, sesi TCP dibagi, dan dengan demikian karakteristik sambungan yang mempengaruhi kinerja protokol (faktor panjang pipa yang berlemak) akan mengatasi (dengan TCP acknowledge spoofing, misalnya). Selain itu, PEP menggunakan proxy dan pre-fetching untuk mempercepat akses ke web lebih lanjut.

Sistem seperti itu dapat dibangun dari nol menggunakan Squid, misalnya, atau dibeli "off the shelf" dari sejumlah vendor.

Informasi lebih lanjut

Sementara optimasi bandwidth adalah kompleks dan merupakan subjek yang sulit, teknik dalam bab ini harus membantu mengurangi sumber yang menyia-nyiakan bandwidth. Untuk menggunakan maksimal bandwidth yang tersedia, anda perlu menentukan kebijakan akses yang baik, mensetup tool untuk pemantauan dan analisa yang komprehensif, dan menerapkan arsitektur jaringan yang memaksa terjadinya penggunaan yang terbatas.

Untuk informasi lebih lanjut mengenai optimasi bandwidth, lihat buku gratis "*How to Accelerate Your Internet" (http://bwmo.net/)*.

Bab 4 Antena & Jalur Transmisi

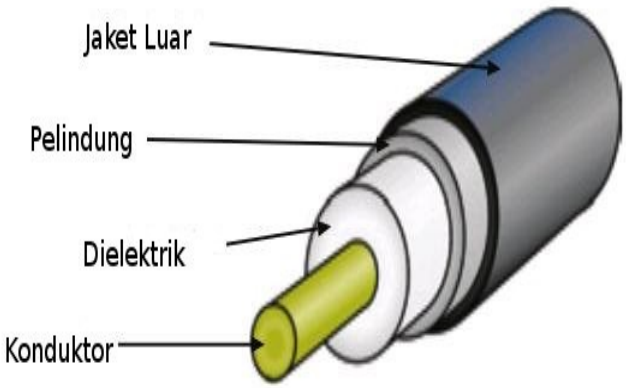
Transmiter yang membangkitkan daya RF[4] untuk mendorong antena yang biasanya terletak pada jarak tertentu dari teminal antena. Sambungan antara keduanya disebut ***jalur transmisi RF***. Tujuannya adalah membawa daya RF dari satu tempat ke tempat lain, dan melakukan ini seefisien mungkin. Di sisi penerima, antena bertanggung jawab untuk menangkap sinyal radio di udara dan meneruskannya ke penerima dengan gangguan sesedikit mungkin, sehingga radio dapat men-dekode sinyal dengan baik. Atas alasan-alasan ini, kabel RF memiliki peran yang sangat penting dalam sistem-sistem radio: ia harus menjaga integritas sinyal dalam dua arah.

Ada dua kategori umum jalur transmisi: kabel dan bumbung gelombang (Waveguide). Keduanya bekerja sangat baik untuk secara efisien membawa daya RF di frekuensi 2.4 GHz.

Kabel

Kabel RF, untuk frekuensi lebih tinggi daripada HF, adalah kabel coaxial (atau ***coax*** pendeknya, berasal dari kata-kata “common axis”). Kabel coax memiliki kawat ***konduktor*** ditengahnya yang dikelilingi oleh material non-konduktif yang dinamakan ***dielektrik,*** atau ***insulator***. Dielektrik ini kemudian dikelilingi oleh pembungkus yang sering kali terbuat dari kabel lilitan. Dielektrik mencegah konektor di tengah dan kabel pembungkusl. Akhirnya, coax dilindungi oleh sebuah penutup luar yang pada umumnya terbuat dari bahan PVC. Konduktor bagian dalam membawa sinyal RF, and pelindung luar mencegah sinyal RF untuk meradiasi ke atmosfer, and juga mencegah sinyal luar dari mengganggu sinyal yang dibawa oleh pusat. Sebuah fakta menarik lainnya adalah sinyal frekuensi tinggi selalu berjalan pada lapisan luar konduktor: semakin besar konduktor di tengah, semakin baik sinyal akan mengalir. Hal ini dinamakan”efek kulit” atau “skin effect”.

4 Radio Frekuensi (RF). Lihat bab dua untuk diskusi tentang gelombang elektromagnetik.



Gambar 4.1: Kabel coax dengan jaket, pelindung, dielektrik, dan konduktor inti / tengah.

Walaupun konstruksi coaxial sangat baik untuk menyimpan sinyal pada kawat utama, terdapat hambatan terhadap aliran listrik: sepanjang sinyal berjalan menuju intinya, sinyal tersebut akan memudar. Pemudaran ini dikenal sebagai ***atenuasi***, dan untuk jalur pemancaran, ini diukur dalam decibel per meter (***dB/m***). Laju atenuasi adalah fungsi frekuensi sinyal dan konstruksi fisik dari kabel itu sendiri. Ketika frekensi sinyal bertambah, bertambah pula atenuasinya. Jjelas, kita harus mengurangi atenuasi kabel serendah mungkin, dengan cara membuatnya sependek mungkin dan menggunakan kabel berpiringantas tinggi.

Berikut adalah beberapa hal penting yang patut dipertimbangkan pada saat memilih kabel yang akan digunakan dengan peralatan gelombang mikro:

1. “Semakin pendek semakin baik!” Aturan pertama pada saat anda memasang sebuah kabel adalah mencoba untuk membuatnya sependek mungkin. Kehilangan daya tidaklah linear, sehingga menggandakan panjang kabel berarti anda akan kehilangan jauh lebih banyak daripada dua kali daya. Dalam cara yang sama, mengurangi panjang kabel sampai setengah memberikan anda daya yang dua kali lebih kuat dari daya antena. Solusi terbaik adalah meletakan pemancar sedekat mungkin ke antena, walaupun ini berarti meletakkannya diatas menara.

2. “Semakin murah semakin buruk!” Aturan kedua adalah uang yang anda gunakan dalam membeli sebuah **kabel berpiringantas baik** adalah sebuah keuntungan. Kabel murah ditujukan pada penggunaan di frekuensi rendah, seperti VHF. Sedangkan gelombang mikro membutuhkan kabel berpiringantas yang tinggi. Semua pilihan lainnya merupakan “dummy load”[5].

5 Dummy load adalah sebuah alat yang menghilangkan energi RF tanpa meradiasikannya. Bayangkan dummy load sebagai heat sink yang bekerja pada frekuensi-frekuensi radio.

3. Selalu hindari RG-58. Ini ditujukan untuk jaringan coax untuk Ethernetl, radio CB atau radio VHF, bukan gelombang mikro.

4. Juga selalu hindari RG-213. Ini ditujukan untuk radio CB dan radio HF. Dalam kasus ini, diameter kabel bukan berarti piringantas tinggi, atau atenuasi rendah.

5. Sebisa mungkin, gunakan kabel Heliax (atau biasa disebut kabel “Foam” atau dalam bahasa pasar di Indonesia disebut kabel “Teflon”) untuk menyambungkan pemancar ke antena. Ketika Heliax tidak tersedia, gunakan kabel LMR yang terbaik yang anda dapat temukan. Kabel Heliax memiliki sebuah pusat konduktor yang padat atau berbentuk tabung dengan konduktor luar padat yang berkerut untuk memungkinkan mereka untuk lentur. Heliax dapat dibuat dalam dua cara, menggunakan udara maupun foam sebagai dielektrik. Heliax dengan dielektrik udara merupakan yang termahal dan menjamin tingkat kehilangan atau loss yang rendah, namun ini lebih sulit untuk ditangani. Heliax dengan dielektrik foam lebih rentan terhadap loss, namun lebih murah dan mudah untuk dipasang. Sebuah prosedur special dibutuhkan pada saat menyolder konektor untuk menjaga dielektrik foam agar tetap kering dan tidak rusak. LMR adalah sebuah merek kabel coax yang tersedia dalam berbagai diameter yang dapat bekerja di frekuensi-frekuensi gelombang mikro. LMR-400 dan MLR-600 merupakan alternatif yang secara umum digunakan selain Heliax.

6. Sebisa kapanpun, gunakan kabel-kabel yang sudah dikrimping dan dites di sebuah lab. Memasang konektor kabel sangatlah rumit, dan sulit untuk dilakukan secara benar bahkan dengan alat yang pas. Kecuali anda mempunyai peralatan yang dapat menguji sebuah kabel yang anda buat sendiri (seperti spectrum analyzer dan signal generator atau time domain reflectometer), penyelesaian masalah jaringan yang menggunakan kabel buatan sendiri dapat menjadi sulit.

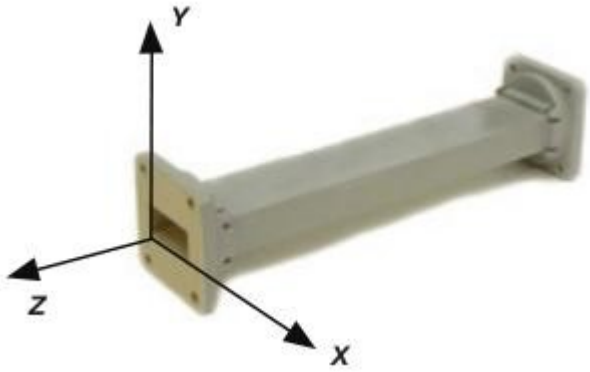
7. Jangan merusak jalur pemancar anda. Jangan pernah menginjak kabel, terlalu banyak membengkokan, atau mencoba untuk mencabut sebuah konektor dengan cara langsung menarik kabel tersebut. Semuanya ini dapat merubah karakteristik mekanis kabel dan impedansinya, memperpendek konduktor dalam hingga lapisan pelindung, atau bahkan memutuskan jalur. Semua masalah-masalah ini sangat sulit dilacak dan dapat menjurus pada ketidakstabilan pada sambungan radio.

Pemandung atau Bumbung Gelombang

Diatas 2 GHz, pandu gelombang cukup pendek untuk memperbolehkan pemindahkan energi yang praktis dan efisien dengan cara-cara yang berbeda. Sebuah pandu gelombang adalah sebuah tabung konduksi dimana energi dipancarkan dalam bentuk gelombang elektromagnetik. Tabung tersebut beraksi sebagai batas yang mengurung gelombang-gelombang tersebut dalam sebuah ruangan tertutup. Efek sangkar Faraday mencegah efek-efek elektromagnetik agar tidak muncul diluar pandu. medan elektromagnetik dipropagasikan melalui pandu gelombang dengan refleksi terhadap dinding bagian dalamnya, yang dianggap

sebagai konduktor sempurna. Intensitas medan sangat besar di pusat sepanjang dimensi X, dan harus berkurang sampai nol di akhir dinding karena keberadaan medan apapun yang paralel dengan dinding di permukaan dapat menimbulkan arus tak terbatas yang mengalir dalam sebuah konduktor sempurna. Pandu gelombang tentunya tidak dapat mengangkut RF dalam cara ini.

Dimensi X, Y, dan Z sebuah pandu gelombang persegi dapat dilihat dalam gambar seperti berikut:



Gambar 4.2: Dimensi X, Y, dan Z dari sebuah pandu gelombang rectangular.

Ada banyak cara bagi medan listrik dan medan magnet untuk mengatur diri mereka sendiri dalam sebuah pandu gelombang untuk frekuensi diatas frekuensi cutoff rendah. Setiap konfigurasi medan disebut sebuah ***mode.*** Mode-mode ini dapat dipisahkan menjadi dua kelompok. Yang pertama, disebut ***TM*** (Transverse Magnetic), memiliki medan magnetik yang seluruhnya melintang terhadap arah propagasi, namun memiliki komponen medan listrik searah dengan arah propagasi. Tipe yang lainnya, disebut ***TE*** (Transverse Electric), memiliki medan listrik yang seluruhnya melintang, namun memiliki komponen medan magnet searah dengan arah propagasi.

Mode propagasi diidentifikasikan dengan kelompok huruf-huruf yang diikuti oleh dua nomor terletak dibawah garis. Sebagai contoh, TE 10, TM 11, dsb. Jumlah mode yang dimungkinkan bertambah dengan frekuensi untuk ukuran bumbung gelombang yang diberikan, dan hanya ada satu cara yang mungkin, yang dinamakan ***mode dominan,*** untuk frekuensi yang paling rendah yang bisa diteruskan. Di bumbung gelombang persegi empat, dimensi kritis ialah X. Dimensi ini harus lebih dari 0,5 λ di frekuensi yang paling rendah yang akan diteruskan. Dalam prakteknya, dimensi Y biasanya dibuat hampir setara dengan 0,5 X untuk menghindari kemungkinan beroperasi di freuensi lain selain mode dominan. Bentuk cross-section selain segi empat dapat dipakai, yang paling penting adalah bentuk pipa bundar. Banyak pertimbangan yang sama berlaku seperti dalam kasus persegi empat. Dimensi panjang gelombang bagi pemandu persegi empat dan bundar tersedia di tabel berikut, di mana X adalah lebar pemandu persegi empat dan r adalah radius pemandu bundar. Semua bilangan berlaku untuk mode dominan.

Tipe Bumbung Gelombang	Persegi Empat	Lingkaran / Bundar
Panjang Gelombang Cutoff	2 X	3.41 r
Panjang Gelombang terpanjang yang dapat di teruskan dengan sedikit redaman	1.6 X	3.2 r
Panjang gelomban terpendek sebelum mode selanjutnya memungkinkan	1.1 X	2.8 r

Energi mungkin dapat dimasukan ke dalam atau diambil dari bumbung gelombang melalui medan listrik ataupun medan magnet. Transfer energi biasanya terjadi lewat kabel koaksial. Dua metode mungkin untuk penghubungan ke kabel koaksial adalah memakai konduktor bagian dalam kabel koaksial, atau melalui loop. Sebuah probe yang hanya merupakan perpanjangan konduktur yang pendek dari konduktor bagian dalam kabel koaksial dapat di orientasikan agar sejajar dengan garis gaya listrik. Sebuah loop dapat diatur agar menutup beberapa garis gaya magnetik. Titik dimana sambungan maksimum didapatkan bergantung pada cara propagasi di bumbung gelombang atau di rongga. Sambungan maksimum terjadi kalau alat penyambung berada di wilayah yang medannya paling kuat.

Jika waveguide dibiarkan terbuka di satu ujung, waveguide tersebut akan memancarkan energi (artinya, waveguie dapat dipakai sebagai antena bukan sebagai jalur pengiriman). Radiasi ini bisa ditingkatkan dengan membentuk waveguide untuk membentuk antena horn yang berbentuk piramida. Kita akan melihat contoh praktis antena waveguide untuk WiFi nanti di bab ini.

Tipe Kabel	Inti	Dielektrik	Pelindung	Jaket
RG-58	0.9 mm	2.94 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

Ini adalah tabel yang membandingkan ukuran berbagai kabel coax yang biasa digunakan. Pilih kabel terbaik yang anda dapat beli dengan tingkat atenuasi serendah di frekuensi untuk sambungan nirkabel anda.

Konektor dan Adapter

Konektor memungkinkan sebuah kabel dihubungkan dengan kabel lain atau ke peralatan radio. Ada berbagai jenis alat dan konektor yang didesain sesuai dengan berbagai ukuran

dan tipe jalur koaksial. Kami akan menggambarkan beberapa yang paling populer.

Konektor BNC dikembangkan di akhir tahun 40an. BNC adalah singkatan dari Bayonet Neill Concelman, yang dinamai seperti nama orang-orang yang menciptakannya, yaitu Paul Neill dan Carl Concelman. Lini produk BNC adalah konektor miniatur untuk menghubungkan/melepaskan secara cepat. Konektor ini tampak seperti dua bayonet memutar pada konektor perempuan, dan sambungan terbentuk hanya dengan seperempat pemutaran mata sambungan. BNC secara ideal cocok untuk terminasi kabel untuk kabel coax miniatur ke sub-miniaturl (RG-58 ke RG-179, RG-316, dll). Mereka mempunyai kinerja yang dapat diterima sampai pada sedikitnya GHz. Pada umumnya, mereka ditemukan pada perlengkapan tes dan kabel coaxial ethernet 10base2.

Konektor TNC juga diciptakan oleh Neill dan Concelman, dan adalah variasi BNC. Dikarenakan intekoneksi yang lebih baik yang disediakan oleh konektor berkumparan, konektor TNC berkerja baik lewat frekuensi sekitar 12 GHz. TNC adalah singkatan dari Threaded Neill Concelman.

Konektor Type N (sekali lagi bagi Neill, walaupun kadang-kadang dihubungkan dengan “Navy”) semula dibangun selama Perang Dunia ke dua. Mereka dapat dipakai sampai 18 Ghz, dan sangat umum dipakai untuk aplikasi gelombang mikro. Mereka tersedia untuk hampir semua macam kabel. Baik steker/kabel maupun steker/soket stop kontak semua kedap air, dan memberikan kelem kabel efektif.

SMA adalah singkatan dari SubMiniature versi A, dan dikembangkan di tahun 60-an. Konektor-konektor SMA adalah unit yang sangat presis, kecil / miniatur yang memberikan kinerja listrik yang baik sampai dengan 18 GHz. Konektor berkinersja tinggi ini mempunyai ukuran yang kompak dan mekanis mempunyai daya tahan luar biasa.

SMB berasal dari SubMiniature B, dan merupakan disain sub-miniatur kedua. SMB ini merupakan versi SMA yang lebih kecil dengan sambungan snap-on. SMB ini menyediakan kemampuan pita lebar sampai 4 GHz dengan pola konektor snap-on.

Konektor MCX diperkenalkan di tahun 80-an. Walaupun MCX memakai kontak dalam dan dimensi penyekat yang identik dengan SMB, garis tengah luar steker 30% lebih kecil daripada SMB. Seri ini memberikan pilihan bagi perancang jika berat dan ruang terbatas. MCX menyediakan kemampuan pita lebar sampai frekuensi 6 GHz dengan desain konektor snap-on.

Disamping konektor-konektor standar ini, kebanyakan alat WiFi memakai berbagai jenis konektor proprietary. Sering kali, semua ini merupakan konektor-konektor standar gelombang mikro dengan bagian-bagian tengah konduktor yang terbalik, atau ulir yang dipotong berlawanan arah. Bagian-bagian ini sering diintegrasikan ke dalam sistem gelombang mikro sebagai kabel pendek yang dinamakan ***pigtail*** yang mengubah yang konektor nonstandar menjadi sesuatu yang lebih kuat dan stabil dari pada yang biasanya. Beberapa dari konektor-konektor ini meliputi:

RP-TNC. Ini adalah konektor TNC dengan jenis kelamin terbalik. Konektor semacam ini sangat umum ditemukan pada peralatan Linksys, seperti WRT54G.

U.FL (juga dikenal sebagai ***MHF)***. U.FL adalah konektor berpaten dibuat oleh Hi-Rose, sedangkan MHF adalah konektor yang secara mekanis sepadan. Ini mungkin adalah konektor gelombang mikro yang paling kecil yang sekarang sedang digunakan secara luas. U.FL/MHF biasanya dipakai untuk menghubungkan card radio mini-PCI ke antena atau konektor yang lebih besar (seperti N atau TNC).

Seri ***MMCX,*** yang juga disebut MicroMate, adalah salah satu konektor RF yang paling kecil dan dikembangkan di tahun 90an. MMCX adalah seri konektor miniatur mikro dengan mekanisme lock-snap yang memungkinkan adanya kemampuan rotasi 360 derajat yang fleksibel. Konektor-konektor MMCX secara umum ditemukan pada kartu radio PCMCIA, seperti yang dibuat oleh Senao dan Cisco.

Konektor-konektor ***MC-Card*** bahkan lebih kecil lagi dan lebih ringkih daripada MMCX. Mereka mempunyai konektor luar terpisah yang dapat rusak secara mudah setelah beberapa interkoneksi saja. Mereka ini secara umum ditemukan pada peralatan Lucent/Orinoco/Avaya.

Adaptor, yang juga disebut sebagai adaptor koaksial, adalah konektor pendek bermuka dua yang digunakan untuk menghubungkan dua kabel atau bagian yang tidak bisa disambungkan secara langsung. Adaptor juga bisa dipakai untuk menginterkoneksikan alat atau kabel yang berbeda jenis. Misalnya, adaptor bisa dipergunakan untuk menyambung konetor SMA ke BNC. Adaptor juga mungkin digunakan untuk mencocokan konektor yang jenisnya sama, tetapi yang tidak bisa secara langsung dihubungkan karena jenis kelamin mereka.

Gambar 4.3: Sebuah Adapter barrel tipe N perempuan

Misalnya, sebuah adapter yang sangat berguna adalah yang memungkinkan untuk menggabungkan dua konektor Type N, mempunyai soket konektor (perempuan) di kedua pihak.

Memilih konektor yang tepat

1. “Pertanyaan jenis kelamin. ” Hampir semua konektor memiliki jenis kelamin yang terdefinisikan secara baik yang terdiri dari baik pin (“laki-laki”) atau soket (“perempuan”). Biasanya kabel mempunyai konektor laki-laki pada kedua ujungnya, sedangkan alat RF (misalnya pemancar dan antena) mempunyai konektor betina. Alat seperti directional coupler dan alat pengukur line-through mungkin mempunyai konektor baik jantan maupun betina. Pastikan setiap konektor jantan di sistem anda berpasangan dengan konektor betina.

2. “Sedikit itu terbaik!” Cobalah untuk memperkecil jumlah konektor dan adaptor di rantai sambungan RF. Masing-masing konektor menyebabkan tambahan loss (sampai beberapa dB untuk masing-masing koneksi, tergantung konektornya!)

3. “Beli, jangan membuat!” Seperti yang telah diutarakan lebih awal, beli kabel yang sudah diterminasi dengan konektor yang anda butuhkan kapanpun. Menyolder konektor bukanlah tugas yang mudah, dan untuk mengerjakan pekerjaan ini dengan semestinya hampir mustahil untuk konektor-konektor kecil seperti U.FL dan MMCX. Bahkan mengterminasikan kabel “Foam” bukanlah tugas yang mudah.

4. Jangan memberli BNC untuk frekuensi 2.4 GHz atau lebih tinggi. Gunakan konektor tipe N (atau SMA, SMB, TNC dll).

5. Konektor gelombang mikro merupakan peralatan yang dibuat presis, dan dapat secara mudah rusak karena kecerobohan dalam penanganannya. Sebagai kaidah umum, anda sebaiknya merotasikan pembungkus luar untuk mengencangkan konektor tersebut, sehingga bagian sisa dari konektor (dan kabel) tidak bergerak. Jika bagian-bagian konektor lain terbelit pada saat mengetatkan atau melonggarkan, maka kerusakan dapat dengan mudah terjadi.

6. Jangan pernah menginjak konektor, ataupun menjatuhkan konektor ke lantar ketika melepaskan kabel (ini lebih sering terjadi daripada apa yang mungkin anda bayangkan, khususnya ketika bekerja di tiang di atas atap).

7. Jangan pernah menggunakan alat seperti tang untuk mengencangkan konektor. Selalu gunakan tangan anda. Ketika bekerja di luar, ingat bahwa besi memuai pada temperatur tinggi dan mengurangi ukuran mereka di temperatur rendah: sebuah konektor yang sangat ketat pada musim panas bisa mengkerut atau malah rusak pada musim dingin.

Antena dan pola radiasi

Antena adalah bagian sistem komunikasi yang sangat penting. Sesuai definisinya, antena

adalah alat yang dulu digunakan untuk mengubah sinyal RF yang berjalan pada konduktor menjadi gelombang elektromagnetik di ruang bebas. Antena mempertunjukkan sebuah karakteristik yang biasa dikenal sebagai ***ketimbal-balikan***, yang berarti bahwa antena akan memelihara sifat yang sama terlepas apakah antena tersebut memancarkan atau menerima. Kebanyakan antena adalah alat yang beresonansi, yang beroperasi secara efisien sebuah pita frekuensi yang relatif sempit. Antena harus di-tune kepada pita frekuensi sama dari sistem radio yang tersambung ke antena itu, jika tidak maka penerimaan dan pemancaran akan terhalangi. Ketika sebuah sinyal masuk ke antena, antena akan memancarkan radiasi yang disebarkan di ruang dalam cara tertentu. Sebuah gambaran distribusi relatif daya yang dipancarkan di ruang dinamakan ***pola radiasi.***

Daftar istilah-istilah antena

Sebelum kita berbicara tentang antena tertentu, ada beberapa istilah-istilah umum yang harus didefinisikan dan diterangkan:

Input Impedance

Untuk pemindahan energi yang efisien, ***impedansi*** radio, antena, dan kabel pengiriman yang menyambung mereka harus sama. Transceivers dan kabel penghubung mereka biasanya didesain untuk impedenasi 50Ω. Jika antena mempunyai impedance berbeda dari 50Ω, maka akan ada ketidakcocokan dan sebuah rangkaian pencocok impedansi akan diperlukan. Ketika impedance tidak cocok, efisiensi pengiriman menurun.

Return Loss

Return Loss adalah cara lain mengungkapkan ketidakcocokan. Return Loss adalah rasio logaritmik yang diukur dalam dB yang membandingkan daya yang dipantulkan oleh antena dengan daya yang dimasukan ke dalam antena dari jalur pengiriman. Hubungan antara SWR dan Return Loss adalah sebagai berikut:

$$\text{Return Loss (dalam dB)} = 20\log_{10}\frac{SWR}{SWR-1}$$

Pada saat sebagian energi selalu akan dipantulkan kembali ke dalam sistem, return Loss yang tinggi akan menghasilkan kinerja antena yang tak dapat diterima.

Bandwidth

Lebar pita antena merujuk pada frekuensi dimana antena bisa beroperasi secara baik. Pita lebar antena menggunakan satuan Hz dimana antena akan menunjukkan SWR kurang dari 2:1.
Bandwidth juga bisa dideskripsikan dalam bentuk persentase frekuensi pusat pita.

$$\text{Bandwidth} = 100 \times \frac{F_H - F_L}{F_C}$$

... di mana F_H adalah frekuensi yang paling tinggi di pita, F_L adalah frekuensi yang paling rendah di pita, dan F_C adalah frekuensi tengah di pita.

Dengan begitu, lebar pita adalah konstanta relatif terhadap frekuensi. Jika lebar pita diungkapkan di satuan-satuan mutlak frekuensi, lebar pita akan berbeda bergantung pada frekuensi tengah. Macam antena yang berbeda mempunyai keterbatasan lebar pita yang berbeda.

Directivity dan Gain

Directivity adalah kemampuan antena untuk memusatkan energy di arah yang tertentu sewaktu memancarkan, atau untuk menerima energi dari arah yang tertentu sewaktu menerima. Jika sebuah sambungan nirkabel menggunakan lokasi tetap untuk kedua sisi, maka sangat memungkinkan untuk menggunakan antena directivity untuk memusatkan sorotan radiasi di arah yang diinginkan. Di aplikasi mobile yang bisa berpindah-pindah di mana transceiver tidak tetap, mungkin mustahil untuk meramalkan di mana transceiver akan berada, dan oleh sebab itu antena secara ideal sebaiknya menyebar secara sebaik-baiknya ke segala arah. Antena Omnidirectional dipakai dalam aplikasi ini.

Gain (Penguatan) bukanlah kuantitas yang bisa didefinisikan dalam bentuk fisik seperti Watt atau Ohm, tetapi Gain adalah rasio yang tidak berdimensi. Gain diberikan sesuai dengan rujukan kepada antena standar. Dua antena yang biasanya digunakan sebagai rujukan adalah ***antena isotropic*** dan ***antena dipole setengah gelombang.*** Antena Isotropic memancar sama baiknya ke segala arah. Antena isotropic yang sesungguhnya tidak pernah ada, tetapi antena ini menyediakan pola antena teoretis yang berguna dan sederhana yang dapat dibandingkan yang dengan antena sesungguhnya. Antena mana pun yang sesungguhnya akan memancarkan lebih banyak energi di beberapa arah daripada yang lainnya. Karena antena tidak bisa menciptakan energi, total data yang di pancarkan adalah sama dengan antena isotropic. Energi tambahan apapun yang terpancar dalam arah yang dipilih akan diimbangi oleh pengurangan energi yang sama atau kurang di arah yang lain.

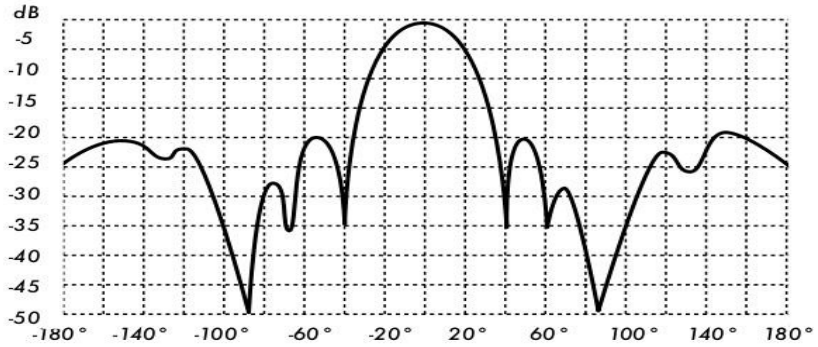
Gain sebuah antena pada sebuah arah adalah banyaknya energi yang dipancarkan dalam

arah itu sebanding dengan energi yang diradiasikan oleh antena isotropic dalam arah yang sama ketika didorong dengan daya masukan yang sama. Biasanya kita hanya tertarik pada gain maksimum, yang merupakan gain dalam arah dimana antena memancarkan sebagian besar dayanya. Gain antena sebanyak 3 dB dibandingkan dengan antena isotropic akan ditulis sebagai **3 dBi.** Sebuah dipole separuh-gelombang yang beresonansi akan menjadi standar yang berguna untuk dibandingkan dengan antena lain di satu frekuensi atau di lebar pita frekuensi yang sangat sempit. Untuk membandingkan dipole ke sebuah antena pada lebar frekuensi memerlukan sejumlah dipole dengan panjang yang berbeda. Gain antena sebanyak 3 dB dibandingkan dengan antena dipole akan ditulis sebagai **3 dBd.**

Metode mengukur gain dengan membandingkan antena yang sedang diuji terhadap antena standar yang ada, yang mempunyai gain yang terkalibrasi, secara teknis dikenal sebagai teknik ***gain transfer.*** Metode lain untuk mengukur gain adalah metode 3 antena, di mana daya yang dipancarkan dan diterima di terminal antena diukur di antara tiga antena di jarak tertentu.

Pola Radiasi

Pola radiasi atau ***pola antena*** menggambarkan kekuatan relatif medan yang dipancarkan di berbagai arah dari antena, pada jarak yang konstan. Pola radiasi adalah pola penerimaan juga, karena pola radiasi tersebut juga menggambarkan karakteristik menerima antena. Pola radiasi adalah tiga- dimensi, tetapi biasanya pola radiasi yang terukur merupakan irisan dua dimensi dari pola tiga dimensi, di bidang planar horisontal atau vertikal. Pengukuran pola ini ditampil kandalam format ***rectangular*** ataupun ***polar.*** Angka-angka berikut menunjukkan tampilan alur rectangular khusus untuk Yagi sepuluh-elemen. Detail ini baik tetapi sangatlah sulit untuk menggambarkan perilaku antena di arah yang berbeda.

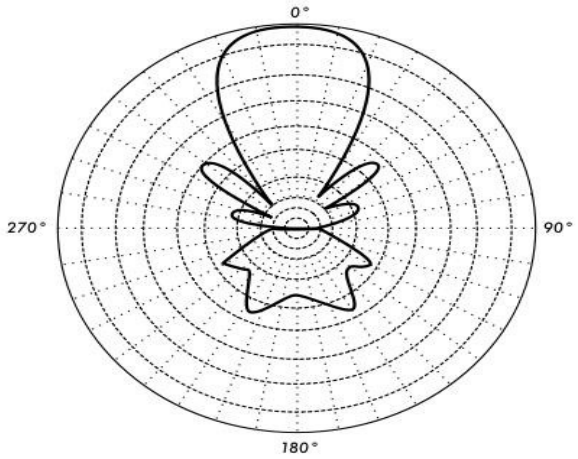


Gambar 4.4:

Sebuah plot rectangular pola radiasi Yagi

Sistem koordinat kutub dipakai hampir universal. Di grafik dengan koordinat polar, titik-titik ditemukan berdasarkan proyeksi sepanjang poros berputar (radius) terhadap persimpangan dengan satu di antara beberapa lingkaran konsentris. Yang berikut adalah plot polar dari antena Yagi 10 elemen yang sama

Sistem koordinat polar mungkin dapat dipisahkan secara umum menjadi dua kelas: ***linear*** dan ***logaritmis.*** Di sistem koordinat linear, lingkaran konsentris berjarak sama, atau berjarak gradual. Grid / kisi-kisi seperti ini mungkin dipergunakan untuk menampilan daya yang tersimpan pada sinyal secara linier. Untuk mempermudah perbandingan, lingkaran konsentris dengan jarak yang sama dapat diganti dengan lingkaran yang ditempatkan secara pas yang melambangkan respons dalam desibel, direferensikan sampai 0 dB di pinggir luar alur. Di plot seperti ini sidelobe kecil akan ditekan. sidelobe dengan puncak lebih dari sekitar 15 dB atau di bawahnya akan tidak terlihat dari lobe utama karena kecil-nya ukuran mereka. Kisi-kisi ini meningkatkan plot dimana antena tersebut mempunyai directivity yang tinggi dan sidelobe minor yang kecil. Tegangan sinyal, bukan daya, juga bisa diplot diatas sistem koordinat linear. Di kasus ini, directivity akan di ditingkatkan dan sidelobe kecil akan ditekan, tetapi tidak pada tingkat yangs ama jika kita menggunakan kisi-kisi daya linear.

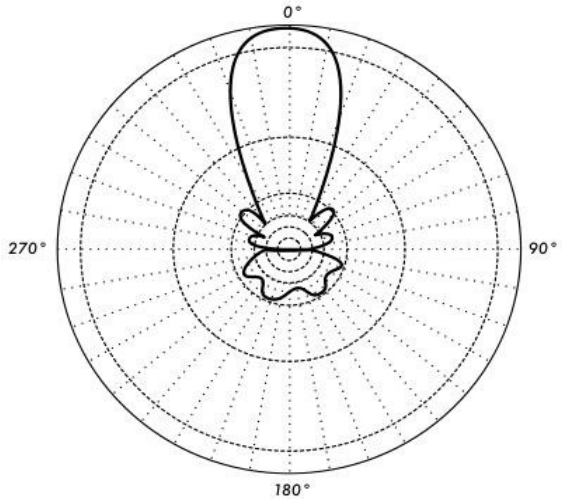


Gambar 4.5: Sebuah plot kutub dari antenna yagi yang sama.

Dalam sistem koordinat polar yang logaritmis, garis kisi-kisi konsentris diletakkan secara berkala logaritmis untuk tegangan dalam sinyalnya. Nilai yang berbeda dapat digunakan untuk konstanta dalam spasi logaritmik, dan pilihan ini akan berpengaruh pada penampilan pola yang ditampilkan. Secara umum referensi 0 dB untuk pinggir luar grafik digunakan. Dengan kisi-kisi jenis ini, sidelobe yang 30 atau 40 dB lebih rendah dari lobe utama masih dapat dibedakan. Jarak di antara ujung 0 dB dan -3 dB lebih panjang daripada jarak antara -20 dB dan -23 dB, yang lebih besar daripada jarak antara -50 dB dan -53 dB. Pemberian jarak berhubungan dengan kepentingan relatif pada kinerja antena.

Skala logaritmik yang dimodifikasi akan menegaskan bentuk bean utama dan mengkompresi sidelobe samping pada tingkat yang sangat rendah (>30 dB) terhadap pusat pola. Ini dapat dilihat di **Gambar 4.6.**

Ada dua jenis pola radiasi, yaitu ***mutlak*** dan ***relatif.*** Pola radiasi mutlak ditampilkan dalam satuan-satuan mutlak kekuatan atau daya medan. Pola radiasi relatifmerujuk pada satuan-satuan relatif kekuatan atau daya medan. Kebanyakan ukuran pola radiasi relatif kepada antena isotropic, dan metode transfer gain kemudian dipergunakan untuk menentukan gain mutlak antena.



Gambar 4.6: Gambar plot logaritmik

Pola radiasi di daerah dekat antena tidaklah sama seperti pola radiasi pada jarak jauh. Istilah medan dekat merujuk pada pola medan yang berada dekat antena, sedangkan istilah medan jauh merujuk pada pola medan yang berada di jarak jauh. Medan jauh juga disebut sebagai medan radiasi, dan merupakan hal yang diinginkan. Biasanya, daya yang dipancarkan adalah yang kita inginkan, dan oleh karena itu pola antena biasanya diukur di daerah medan jauh. Untuk pengukuran pola sangatlah penting untuk memilih jarak yang cukup besar untuk berada di medan jauh, jauh di luar medan dekat. Jarak dekat minimum yang diperbolehkan bergantung pada dimensi antena berkaitan dengan panjang gelombang. Rumusan yang biasa digunakan untuk jarak ini ialah:

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

Di mana r_{min} adalah jarak minimum dari antena, D adalah dimensi antena yang paling besar, dan λ adalah panjang gelombang.

Beamwidth

Beamwidth antenna biasanya dipahami sebagai lebar beam saat daya setengah. Puncak

intensitas radiasi ditemukan, dan lalu ujung kedua puncak yang melambangkan setengah daya intensitas puncak ditemukan. Jarak bersiku di antara ke dua ujung daya setengah di definisikan sebagai beamwidth. Setengah daya yang diekspresikan dalam decible adalah -3dB, sehingga beamwidth setengah daya beamwidth kadang-kadang dirujuk sebagai beamwidth 3dB. Beamwidth horisontal maupun vertikal biasanya dipertimbangkan.

Dengan asumsi bahwa sebagian besar daya yang dipancarkan tidak dibagi-bagi ke dalam sidelobe, gain kedepan akan berbanding terbalik dengan beamwidth: pada saat beamwidth berkurang, gain ke depan bertambah.

Sidelobes

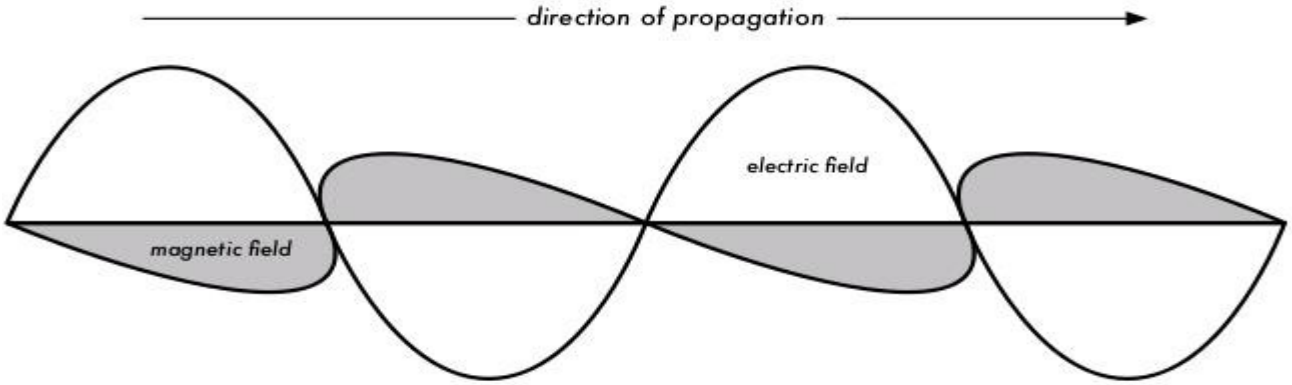
Tak ada antena yang dapat memancarkan seluruh energi di satu arah yang dipilih. Sebagian energi yang pasti dipancarkan di jurusan lain. Puncak-puncak yang lebih kecil ini dinamakan sebagai ***sidelobe,*** yang biasanya ditetapkan dalam dB lebih kecil dari lobe utama.

Nulls

Di pola radiasi antena, ***null*** adalah zona dimana daya efektif yang dipancarkan minimum. Null sering mempunyai sudut directivity yang sempit dibandingkan dengan yang dipunyai beam utama. Dengan begitu, null berguna untuk beberapa tujuan, seperti meminimalisir gangguan sinyal pada sebuah arah.

Polarisasi

Polarisasi didefinisikan sebagai orientasi medan listrik gelombang elektromagnetik. Polarisasi pada umumnya digambarkan seperti elips. Dua kasus istimewa polarisasi elips adalah ***polarisasi linear*** dan ***polarisasi sirkular.*** Awal polarisasi gelombang radio ditentukan oleh antena.



Gambar 4.7: gelombang listrik tegak lurus terhadap gelombang magnet, yang kedua diantaranya tegak lurus terhadap arah propagasi.

Dengan polarisasi linear, vektor medan listrik tetap berada di bidang yang sama terus menerus. Medan listrik mungkin meninggalkan antena dalam orientasi vertikal, horisontal, atau suatu sudut di antara keduanya. ***Radiasi dengan polarisasi vertikal*** lebih sedikit dipengaruhi oleh pantulan pada jalur perambatannya. Antena Omnidirectional selalu memiliki polarisasi vertikal. Dengan ***radiasi dengan polarisasi horisontal***, pantulan seperti itu menyebabkan variasi dalam kekuatan signal yang diterima. Antena horisontal lebih sedikit kemungkinannya untuk mendapat gangguan buatan manuasia, yang biasanya dipolarisasikan secara vertikal.

Dalam polarisasi sirkular, vektor medan listrik kelihatannya berotasi dengan gerakan berputar searah arah propagasi, membuat satu putaran penuh untuk setiap siklus RF. Rotasi ini mungkin berada di sebelah kanan atau sebelah kiri. Pilihan polarisasi adalah salah satu pilihan bentuk yang tersedia kepada sistem perancang RF.

Polarization Mismatch

Untuk mentransfer daya maksimum antara antena pemancar dan antena penerima, kedua antena harus mempunyai orientasi ruang yang sama, pengertian polarisasi yang sama, maupun rasio aksial yang sama.

Kalau antena tidak diluruskan atau tidak mempunyai polarisasi sama, akan ada penurunan di pemindahan energi antara kedua antena. Penurunan dalam pemindahan energi ini akan mengurangi efisiensi sistem dan kinerja keseluruhan. Ketika antena pemancar dan penerima secara linear terpolarisasi, ketidakcocokan fisik antena akan menghasilkan kehilangan ketidakseimbangan polarisasi, yang bisa ditentukan memakai rumusan berikut:

```
Loss (dB) = 20 log (cos □)
```

... di mana □ adalah perbedaan di sudut antara kedua antena. Untuk 15° kehilangan kira-kira 0.3dB, untuk 30° kehilangan 1.25dB, untuk 45° kehilangan 3dB dan untuk 90° kehilangan menjadi tidak terhingga.

Pendek kata, semakin besar ketidakseimbangan dalam polarisasi antara antena pemancar dan penerima, semakin besar kehilangan tersebut. Dalam dunia sesungguhnya, ketidakcocokan 90° di polarisasi cukup besar tetapi tidak infinite. Beberapa antena, seperti yagi atau antena kaleng, dapat diputar 90° secara sederhana untuk menyamai polarisasi akhir ujung lain hubungan tersebut. Anda bisa menggunakan efek polarisasi untuk keuntungan anda dalam hubungan dari titik yang satu ke yang lainnya. Gunakan alat monitoring untuk mengamati gangguan dari jaringan tetangga, dan putar satu antena sampai anda melihat sinyal paling rendah yang diterima. Kemudian operasikan sambungan anda dan arahkan ujung yang lain untuk menyamai polarisasi. Teknik ini kadang-kadang bisa dipergunakan untuk membuat hubungan stabil, bahkan di lingkungan radio yang banyak gangguan.

Front-to-back ratio

Akan sangat berguna untuk membandingkan ***front-to-back ratio*** dari antena directional. Ini adalah rasio penguatan maksimum pada arah antena terhadap penguatan ke arah yang berlawanan. Misalnya, kalau pola radiasinya digambarkan di atas skala dB yang relatif, maka rasio depan-belakang adalah perbedaan dalam dB antara radiasi maksimum di arah muka dan radiasi di 180 derajat. Angka ini tak berarti untuk antena omnidirectional, tetapi angka tersebut memberi gambaran kepada anda tentang banyaknya daya yang ditujukan ke muka dari antena pengarah.

Tipe antena

Klasifikasi antena dapat didasarkan pada:

- **Frekuensi dan ukuran.** Antena yang dipakai di HF berbeda dengan antena yang dipakai bagi VHF, dan juga berbeda dengan antena untuk gelombang mikro. Panjang gelombang berbeda di frekuensi yang berbeda, oleh sebab itu antena harus berbeda dalam ukurannya untuk memancarkan sinyal pada panjang gelombang yang tepat. Kita khususnya tertarik pada antena yang bekerja pada jangkauan gelombang mikro, khususnya di frekuensi 2,4 GHz dan 5 GHz. Di 2,4 GHz panjang gelombang adalah 12,5 cm, sedangkan di 5 GHz adalah 6 cm.

- **Directivity.** Antena bisa omnidirectional, sectorial atau directive. ***Antena Omni-directional*** memancarkan pola yang kurang lebih sama di sekitar antena dalam pola

360° yang sempurna. Tipe antena omnidirectional yang paling populer adalah ***dipole*** dan ***ground plane. Antena sektoral*** menyebar medan terutama ke arah tertentu. Beam antenna sektoral dapat selebar 180 derajat, atau sesempit 60 derajat. ***Antenna pengarah*** atau ***antenna directional*** adalah antena dimana beamwidth jauh lebih sempit daripada jika di sectorial antena. Mereka mempunyai gain yang paling tinggi dan oleh karena itu digunakan untuk hubungan jarak jauh. Beberapa tipe antena pengarah adalah Yagi, biquad, horn, helicoidal, antena patch, parabolic dish, dan banyak yang lainnya.

- **Pembuatan fisik.** Antena dapat dibuat dalam banyak cara yang berbeda, mulai dari kawat sederhana, ke parabola, hingga kaleng kopi.

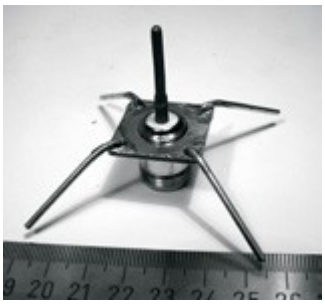
Ketika mempertimbangkan antena yang cocok untuk penggunaan WLAN 2,4 GHz, klasifikasi lain bisa dipakai:

- **Penggunaan.** Akses point cenderung membuat jaringan point-to-multipoint, sedangkan sambungan jarak jauh adalah point-to-point. Masing-masing menggunakan tipe antenna yang berbeda yang sesuai dengan tujuannya. Node yang digunakan untuk akses multi-titik lebih baik menggunakan antena omni yang menyebar secara merata ke segala arah, atau antena sectoral yang fokus pada area yang kecil. Dalam kasus point-to-point, antena dipergunakan untuk menyambung dua lokasi agar tersambung. Antena pengarah adalah pilihan terbaik untuk aplikasi ini.

Daftar ringkas macam antena untuk frekuensi 2,4 GHz, dengan deskripsi pendek dan informasi dasar tentang sifat mereka.

Antene Ground plane 1/4 panjang gelombang

Ground plane panjang gelombang 1⁄4 sangat sederhana dalam pembuatannya dan berguna untuk komunikasi pada saat ukuran, biaya dan kemudahan pembuatan menjadi penting. Antena ini didesain untuk meneruskan sinyal yang dipolarisasikan secara vertikal. Antenna ini terdiri dari ¼ elemen gelombang sebagai separuh-dipole dan tiga atau empat elemen ¼ panjang gelombang sebagai ground yang dibengkokan 30 sampai 45 derajat. Set elemen ini dinamakan radial, dikenal sebagai ground plane.



Gambar 4.8: Antenna ground plane seperempat panjang gelombang

Antenna ini sederhana dan efektif untuk menangkap sinyal secara sama rata dari semua arah. Untuk menambah penguatan, sinyal bisa diratakan untuk mengambil fokus secara langsung dari atas dan bawah, dan menyediakan lebih banyak fokus di horizon. Beamwidth vertikal melambangkan tingkat kerataan dalam fokus. Ini berguna dalam situasi point-to-multipoint, jika semua antena lainnya juga berada pada ketinggian yang sama. Gain dari antena ini sekitar 2-4 dBi.

Antena Yagi

Antenna Yagi pada dasarnya terdiri dari sejumlah elemen, yang masing-masing berukuran sekitar separuh panjang gelombang. Driven elemen atau elemen aktif pada Yagi sepadan dengan antena dipole dengan input di tengah, seperti antenna dipole separuh gelombang. Paralel dengan driven elemen, dan yang berkisar dari 0,2 ke 0,5 panjang gelombang pada kedua sisinya, adalah tangkai atau kawat lurus yang dianggap reflektor dan director (pengarah), atau elemen pasif. Seuah reflektor ditempatkan di belakang driven elemen dan agak lebih panjang daripada separuh panjang gelombang; director ditempatkan di muka driven elemen dan agak lebih pendek daripada separuh panjang gelombang. Sebuah Yagi biasanya mempunyai satu reflektor dan satu atau lebih director. Antena mempropagasikan energi medan elektromagnetik ke arah dari driven elemen sampai ke director, dan paling peka terhadap energi medan elektromagnetik yang datang dalam arah ini. Semakin banyak director yang dimiliki oleh sebuah Yagi, semakin besar gain-nya. Sewaktu lebih banyak director ditambahkan pada sebuah Yagi, maka Yagi menjadi lebih panjang. Berikut ini adalah foto antena Yagi dengan 6 director dan satu reflektor.

Gambar 4.9: Sebuah Antenna Yagi.

Antena Yagi dipakai terutama untuk sambungan point-to-point, mempunyai penguatan dari 10 sampai 20 dBi dan beamwidth horisontal 10 sampai 20 derajat.

Antena Horn

Nama antena horn berasal dari penampilannya yang khas. Bagian horn dapat segi empat, rectangular, silindris atau mengerucut. Arah radiasi maksimum sesuai dengan poros horn. Horndapat dengan mudah diberikan input dengan waveguide, tetapi juga bisa diberikan input dengan kabel coax dan peralihan yang benar.

Gambar 4.10: Feed horn yang terbuat dari sebuah kaleng makanan

Antena horn secara umum dipakai sebagai elemen aktif dalam antena parabola. Horn tersebut mengarah pada pusat reflektor parabola. Penggunaan horn, daripada antena dipole atau antena mana pun, di fokus parabola meminimalisir kehilangan energi di sekitar pinggiran reflektor parabola. Pada frekuensi 2,4 GHz, antena horn sederhana yang terbuat dari kaleng mempunyai gain sebesar 10 - 15 dBi.

Antena parabola

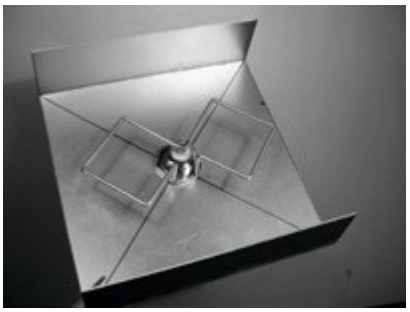
Antena yang berdasarkan reflektor parabola adalah jenis tipe antena pengarah jika diperlukan penguatan tinggi. Keuntungan utama adalah bahwa mereka dapat dibuat untuk mempunyai gain dan directivity sebesar yang diperlukan. Kekurangan utama adalah bahwa besarnya piringan sehingga sulit di pasang dan lebih rentan terhadap angin.

Gambar 4.11: sebuah piringan antenna parabola yang solid

Piringan berukuran sampai satu meter biasanya terbuat dari bahan padat. Aluminium sering dipakai karena ringan, daya tahan dan sifat listriknya yang baik. Kerentanan terhadap angin bertambah secara drastis sesuai dengan ukuran piringan dan akan menjadi masalah berat. Piringan yang mempunyai permukaan yang memantulkan dapat menggunakan jaring juga sering digunakan. Memang yang ini mempunyai front-to-back ratio lebih buruk, tetapi lebih aman untuk digunakan dan lebih mudah untuk dibuat. Tembaga, aluminium, kuningan, baja berlapis seng dan besi adalah bahan jaring baik.

Antena BiQuad

Antena BiQuad sederhana mudah dibuat dan menawarkan directivity dan gain yang baik untuk komunikasi point-to-point. Antena tersebut terdiri dari dua bujur sangkar berukuran sama dari ¼ panjang gelombang sebagai elemen pemancar dan pelat metal atau kisi-kisi metalik sebagai reflektor. Antena ini mempunyai beamwidth sekitar 70 derajat dan penguatan sekitar 10-12 dBi. Antena tersebut bisa digunakan sebagai antena berdiri sendiri atau sebagai tempat masukan untuk piringan parabola. Polarisasinya adalah vertikal jika kita lihat dari muka dan bentuk bujur sangkar berdampingan.



Gambar 4.12: BiQuad.

Antena lainnya

Banyak tipe antenna lain yang tersedia dan yang terbaru diciptakan mengikuti kemajuan dalam teknologi.

- Antena Sektoral: mereka pada umumnya digunakan di infrastruktur teleponi seluler dan biasanya dibuat dengann menambahkan pelat pemantul ke satu atau lebih dipole. Beamwidth horizontal mereka bisa selebar 180 derajat, atau sesempit 60 derajat, sedangkan beamwidth vertikalnya biasanya jauh lebih kecil. Antena kombinasi bisa dibuat dengan banyak Sektor untuk menutupi wilayah horisontal yang lebar (antena multisectoral).

- Antena Panel atau Patch: mereka adalah panel datar yang padat yang digunakan untuk liputan dalam gedung, dengan gain sampai 20 dB.

Teori Reflektor

Karakteristik dasar sebuah reflektor parabola sempurna adalah reflektor tersebut mengubah gelombang yang berbentuk bola menyinari dari sumber titik ditempatkan di fokus menjadi gelombang planar. Sebaliknya, seluruh energi yang diterima oleh piringan parabola dari sumber yang jauh dipantulkan sampai ke satu titik pada fokus parabola. Posisi fokus, atau pusat panjang, dapat ditemukan dengan rumus:

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

... di mana D adalah diameter piringan dan C adalah kedalaman parabola pada pusatnya.

Ukuran piringan adalah faktor yang paling penting karena faktor tersebut menentukan gain maksimum yang dapat dicapai pada sebuah frekuensi dan beamwidth yang dihasilkannya.

Gain dan beamwidth yang didapatkan dapat dicari dengan rumus:

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

$$\text{Beamwidth} = \frac{70\ \lambda}{D}$$

... di mana D adalah diameter piringan dan n adalah efisiensi. Efisiensi ini ditentukan sebagian besar oleh keefektifan penerangan piringan berdasarkan input, tetapi juga oleh faktor lain. Setiap saat diameter piringan digandakan, gain menjadi empat kali lipat, atau 6 dB, lebih besar. Jika kedua stasiun menggandakan ukuran piringan mereka, kekuatan sinyal bisa bertambah 12 dB, sebuah perolehan yang sangat besar. Efisiensi sebanyak 50% bisa diraih sewaktu membuat antena.

Perbandingan f/D (fokus/diameter piringan) adalah faktor yang mendasari disain dari feed untuk piringan. Rasionya secara langsung terkait dengan beamwidth input yang diperlukan untuk menerangi piringan secara efektif. Dua piringan dengan diameter yang sama tetapi berbeda panjang fokus membutuhkan disain feed yang berbeda, jika keduanya harus diterangi secara efisien. Nilai sebanyak 0,25 sesuai dengan piringan dengan focal-plane yang sama dimana fokus berada pada bidang yang sama dengan dasar piringan.

Amplifier

Seperti yang dikatakan lebih awal, antena tidak menciptakan daya. Mereka secara sederhana mengarahkan semua daya yang ada ke dalam pola yang khusus. Dengan memakai ***penguat daya,*** anda dapat mempergunakan daya DC untuk menambah sinyal anda yang ada. Penguat menghubungkan pemancar radio dan antena, dan mempunyai tambahan kabel yang tersambung ke sumber daya. Penguat dapat bekerja di frekuensi 2,4 GHz, dan dapat menambahkan beberapa Watt daya kepada pancaran anda. Alat ini mengetahui bahwa radio yang tersambung sedang memancar, dan secara cepat akan nyala dan menguatkan sinyal. Mereka kemudian mati lagi ketika transmisi berakhir. Ketika menerima, mereka juga menambahkan penguatan sinyal sebelum mengirimkannya ke radio.

Sayangnya, menambahkan penguat tidak akan memecahkan semua masalah jaringan anda. Kami tidak akan membicarakan Amplifier dibuku ini karena sudah ada sejumlah kekurangan dalam penggunaan mereka:

- **Amplifier mahall.** Amplifier harus dapat bekerja di pita lebar di frekuensi 2,4 GHz, dan harus bisa berfungsi dengan cukup cepat untuk memfasilitasi aplikasi Wi-Fi. Amplifier ini memang tersedia, namun dengan harga beberapa ratus dolar setiap unitnya.
- **Anda akan memerlukan sedikitnya dua.** Sementara antena menyediakan penguatan timbal balik yang menguntungkan kedua sisi sambungan, Amplifier bekerja paling baik untuk memperkuat sinyal yang dipancarkan. Jika anda hanya menambahkan amplifier kepada satu sisi hubungan dengan gain antena yang tidak cukup, kemungkinan sinyal akan sampai ke ujung yang lain, tapi kita tidak dapat mendengarkan inyal dari ujung tersebut..
- **Amplifier tidak mengarahkan sinyal.** Menambahkan gain antena memberikan keuntungan gain maupun keuntungan pengarahan kepada kedua ujung sambungan. Mereka tak hanya meningkatkan kekuatan sinyal, tetapi juga menolak gangguan sinyal dari arah lainnya. Amplifier akan memperkuat sinyal secara membabi buta baik sinyal yang baik maupun sinyal pengganggu, dan bisa membuat masalah gangguan menjadi lebih buruk.
- **Amplifiers menghasilkan noise bagi pengguna lainnya di pita yang sama.** Dengan menambah daya output anda, anda menciptakan sebuah sumber noise yang lebih keras bagi pengguna lain di pita unlicensed ini. Ini mungkin bukan masalah di daerah pedesaan, tetapi bisa menyebabkan masalah besar di area dengan populasi yang padat. Sebaliknya, menambahkan gain antena akan meningkatkan sambungan anda dan juga mengurangi derajat gangguan bagi tetangga anda.
- **Penggunaan amplifier mungkin tidak legal.** Setiap negara memberlakukan batas penggunaan spektrum tak berlisensi. Menambahkan antena pada sinyal yang sudah tinggi mungkin akan menyebabkan sambungan melebihi batas legal yang ada. Di Indonesia, amplifier tidak legal.

Penggunaan amplifier sering diibaratkan dengan tetangga yang tidak sopan yang ingin mendengarkan radio di luar rumah mereka, dan oleh sebab itu mengeraskan volume radionya. Mereka mungkin bahkan dapat “meningkatkan” penerimaan dengan mengarahkan speaker mereka ke luar jendela. Sementara mereka sekarang mungkin dapat mendengar radionya, begitu pula orang lain di lingkungan yang sama. Cara ini mungkin dapat berlaku hanya kepada satu orang pengguna, tetapi apa terjadi kalau tetangga lainnya memutuskan melakukan hal sama dengan radio mereka? Memakai amplifier untuk sebuah sambungan nirkabel menyebabkan efek yang hampir sama di frekuensi 2,4 GHz. Sambungan anda mungkin “bekerja lebih baik” untuk sementara waktu, tetapi anda akan mempunyai masalah kalau pengguna lain di pita yang sama memutuskan untuk menggunakan amplifier mereka sendiri.

Dengan memakai antena gain tinggi daripada amplifier, anda dapat menghindari semua masalah ini. Antena harganya jauh lebih murah dari amplifier, dan dapat meningkatkan sambungan dengan sederhana dengan mengganti antena pada sebuah ujung sambungan. Menggunakan radio yang peka dan kabel berkualitas baik juga secara signifikan membantu tembakan jarak jauh. Teknik ini lebih tidak bermasalah bagi pengguna lainnya di pita yang sama, dan oleh sebab itu kami menganjurkan anda untuk menggunaka mereka sebelum

menambahkan amplifier.

Disain praktis antenna

Biaya antena frekuensi 2,4 GHz sudah jatuh secara dramatis semenjak adanya 802.11b. Disain inovatif menggunakan komponen yang sederhana dan bahan yang lebih sedikit untuk meraih gain yang tinggi dengan pengerjaan teknis yang relatif sedikit. Sayangnya, ketersediaan antena yang baik masih terbatas di banyak daerah di dunia, dan pengimporan antena tersebut bisa sangat mahal. Walaupun mendesain antena bisa rumit dan prosesnya rentan terhadap kesalahan, membuat antena dari bahan yang tersedia lokal sangat dibutuhkan, dan bisa menyenangkan. Kami berikan empat bentuk antena praktis yang bisa dibuat dengan pengeluaran uang yang sangat sedikit.

USB wireless sebagai feed pada pirinan parabola

Mungkin bentuk antena yang paling sederhana adalah penggunaan parabola untuk mengarahkan output dari ***USB wireless*** (atau biasa disebut ***USB dongle***). Dengan menempatkan bagian antena dipole yang ada di USB wireless pada fokus piringan parabola, anda bisa menyediakan gain yang signifikan tanpa harus menyolder ataupun membongkar alat nirkabel tersebut. Bermacam-macam piringan parabola dapat berfungsi, termasuk diantaranya adalah piringan satelit, antena televisi, dan alat masak logam (seperti wajan, tutup panci yang bundar, atau saringan). Sebagai bonus, kabel USB yang murah dan yang rentan terhadap kehilangan gain kemudian digunakan sebagai input ke antena, menghilangkan keperluan untuk kabel coax yang mahal atau Heliax.

Untuk membuat USB wireless parabola, anda perlu menemukan orientasi dan lokasi dipole di dalam dongle. Kebanyakan alat mengorientasikan dipole untuk sejajar dengan pinggiran pendek dongle, tetapi sebagian meletakkan dipole tegaklurus terhadap pinggiran pendek tersebut. Anda bisa membuka dongle dan mencari sendiri, atau dengan sederhana berusaha mencoba dongle di kedua posisi untuk melihat yang mana yang menyediakan lebih banyak gain. Untuk menguji antena, arahkan antena tersebut ke akses point beberapa meter jauhnya, dan menyambung USB wireless ke laptop. Dengan menggunakan client driver laptop atau software seperti Netstumbler (lihat **Bab 6)**, coba anda amati kekuatan sinyal akses point yang diterima. Sekarang, pindahkan secara perlahan USB wireless relatif terhadap antenna parabola, sekaligus memperhatikan kekuatan signal. Anda akan melihat adanya peningkatan yang signifikan dalam gain (20 dB atau lebih) ketika anda mencari posisi yang baik. Posisi yang benar akan bervariasi menurut bentuk parabola dan konstruksi USB wirless. Cobalah berbagai posisi pada saat mengawasi kekuatan sinyal anda sampai anda menemukan lokasi optimal.

Setelah lokasi terbaik ditemukan, matikan USB wireless pada tempatnya. Anda perlu untuk membuat USB wireless dan kabel-nya kedap air jika antena digunakan di luar. Gunakan silicone compound atau sepotong pipa PVC untuk melindungi perangkat elektronik dari

cuaca. Banyak bentuk disain dan ide parabola dengan USB terdokumentasi secara online di http://www.usbwifi.orcon.net.nz/.

Collinear omni

Antena ini sangat sederhana untuk dibuat, memerlukan hanya sepotong kawat, sebuah soket N dan pelat metal segi empat. Antena ini bisa digunakan baik dalam gedung atau di luar untuk sambungan jarak pendek point-to-multipoint. Pelat dibuatkan lubang yang dibor di tengah untuk tempat soket casis tipe N yang diletakan di tengah pelat. Kawat disolder ke pin pusat soket N dan mempunyai lilitan untuk memisahkan elemen tahapan yang aktif. Dua versi antena memungkinkan: sesuatu dengan dua tahapan elemen dan dua buah lilitan dan satu lagi dengan empat tahapan elemen dan empat lilitan. Untuk antenna yang pendek gain akan kecil sekitar 5 dBi, sedangkan antenna yang panjang dengan empat elemen akan mempunyai gain 7 sampai 9 dBi. Kami akan menggambarkan bagaimana caranya membuat antena panjang.

Daftar komponen dan alat yang diperlukan:

- Satu konektor tipe N perempuan.
- Kawat tembaga 50 cm atau kuningan berdiameter 2 mm.
- Sebuah pelat metalik segi empat berukuran 10x10 cm atau lebih besar.

Gambar 4.13: pelat aluminium 10 cm x 10 cm.

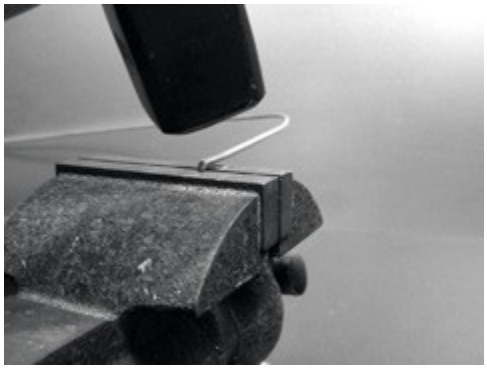
- Penggaris
- Tang
- Amplas
- Timah solder dan solder
- Bor dengan set mata bor untuk logam (termasuk diantaranya sebuah mata bor berdiameter 1.5 cm)
- Sepotong pipa atau mata bor dengan diameter 1 cm
- Vice atau penjepit
- Palu
- Spanner atau kunci inggris

Pembuatan

1. Luruskan kawat dengan menggunakan vice.

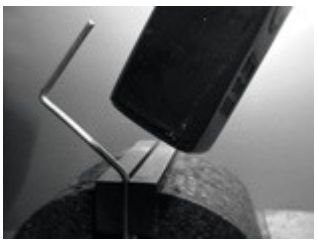
Gambar 4.14: membuat kawat selurus mungkin.

2. Dengan bolpen, gambar sebuah garis pada 2,5 cm dari ujung kawat. Pada garis ini, bengkokan kawat sampai 90 derajat dengan menggunakan vice dan palu.



Gambar 4.15: dengan hati-hati mengetuk kawat untuk membuat lengkungan tajam.

3. Gambar garis lainnya 3,6 cm dari lengkungan. Dengan memakai penjepit dan palu, bengkokan sekali lagi kawat di balik garis kedua ini sampai 90 derajat, di arah yang berlawanan terhadap bengkokan pertama tetapi di bidang yang sama. Kawat nampak seperti huruf Z.



Gambar 4.16: bengkokan kawat ke dalam bentuk "Z".

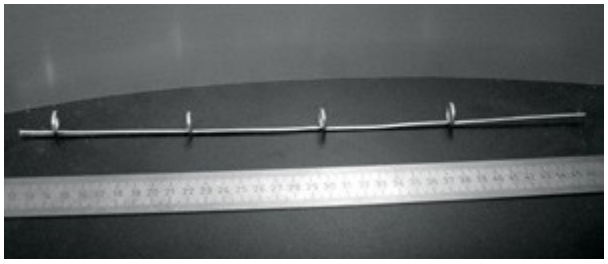
4. Kita memilin bagian Z dari kawat untuk membuat sebuah lilitan dengan diameter 1 cm. Untuk melakukan ini, kita akan menggunakan pipa atau mata bor dan melengkungkan kawat sehingga memutarinya, dengan bantuan penjepit dan tang.

Gambar 4.17: Bengkokan kawat sehingga memutari mata bor untuk membuat sebuah lilitan.

Lilitan akan tampak seperti ini:

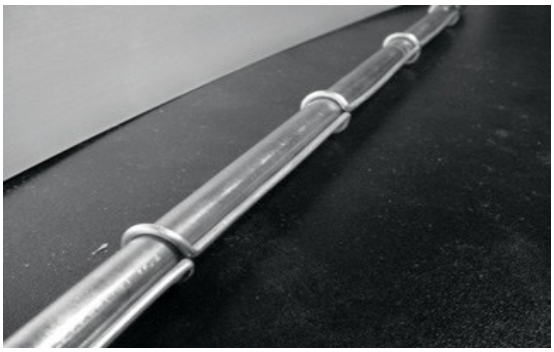
Gambar 4.18: Lilitan yang sudah selesai.

5. Anda sebaiknya membuat lilitan kedua dengan jarak 7,8 cm dari yang pertama. Kedua lilitan sebaiknya mempunyai arah balik yang sama dan sebaiknya ditempatkan di sisi kawat yang sama. Buatlah lilitan ketiga dan lilitan keempat dengan mengikuti prosedur yang sama, di jarak yang sama yaitu 7,8 cm dari satu dengan yang lainnya. Potong bagian elemen tahapan terakhir dengan jarak 8,0 cm dari lilitan keempat.



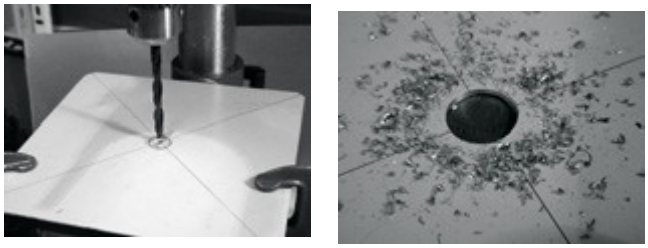
Gambar 4.19: Cobalah untuk menjaganya agar tetap selurus mungkin.

Jika lilitan-lilitan tersebut sudah dibuat dengan benar, sekarang sangat mungkin untuk memasukkan pipa lewat semua lilitan seperti yang sedang diperlihatkan.



Gambar 4.20: memasukkan pipa bisa membantu meluruskan kawat.

6. Dengan bolpen dan penggaris, buat garis diagonal di atas pelat metal, dan tentukan pusatnya. Dengan mata bor berdiameter kecil, buatlah sebuah lubang penunjuk di tengah pelat. Lebarkan diameter lubang menggunakan mata bor dengan diameter yang lebih besar.



Gambar 4.21: membor luang di piring logam.

Lubang sebaiknya sesuai dengan N connector persis. Pakai berkas jika diperlukan.

Gambar 4.22: Konektor N sebaiknya cocok dengan lubang.

7. Agar antena mempunyai impedansi 50 Ohm, sangat penting agar permukaan insulator konektor yang kelihatan (bagian putih sekitar pin pusat) berada di derajat yang sama dengan permukaan pelat. Untuk tujuan ini, potonglah 0,5 cm pipa tembaga dengan

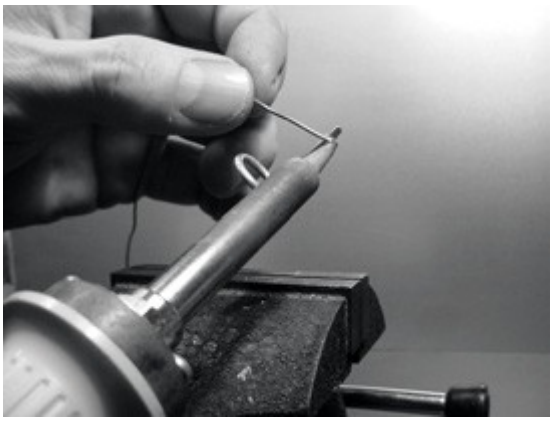
diameter eksternal sepanjang 2 cm, dan letakkan potongan tersebut di antara konektor dan pelat.

Gambar 4.23: menambahkan pipa tembaga membantu untuk mencocokkan impedansi antena agar 50 Ohm.

8. Sekrupkan mur ke konektor untuk menempatkannya secara kukuh di atas pelat dengan menggunakan kunci inggris.

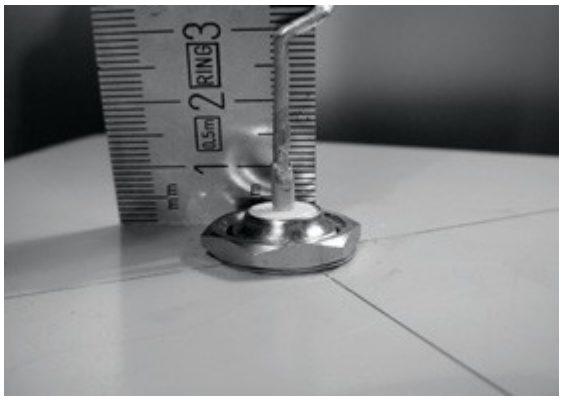
Gambar 4.24: Kencangkan konektor N ke pelat.

9. Haluskan dengan amplas sisi kawat yang panjangnya 2,5 cm, dari lilitan pertama. Berikan timah pada kawat di sekitar 0,5 cm di bagian yang sudah dihaluskan, gunakan penjepit untuk membantu anda.



Gambar 4.25: Berikan timah sedikit pada bagian akhir kawat untuk menimahkannya sebelum penyolderan.

10. Dengan besi solder, berikan timah pada pin pusat konektor. Sambil menjaga kawat agar tetap vertikal dengan tang, solderlah bagian kawat yang sudah bertimah di lubang pin pusat. Lilitan pertama sebaiknya berada 3,0 cm dari pelat.

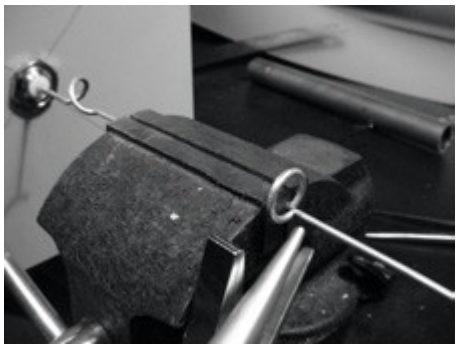


Gambar 4.26: lilitan pertama sebaiknya berawal 3,0 cm dari permukaan piring.

11. Kita sekarang akan merentangkan lilitan, memperpanjang panjang vertikal kawat. Dengan menggunakan penjepit dan tang, anda dapat menarik kabel agar panjang terakhir lilitan menjadi 2,0 cm.

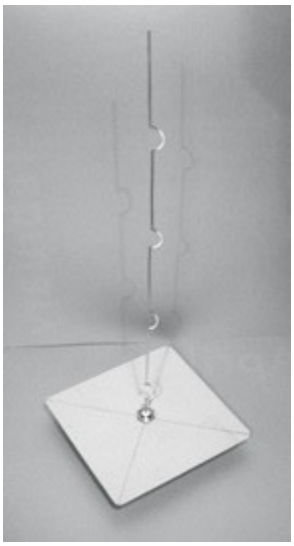
Gambar 4.27: merentangkan lilitan. Cobalah untuk secara hati-hati dan tidak untuk menggores permukaan kawat dengan tang.

12. Ulangi prosedur yang sama untuk tiga lilitan lainnya, rentangkan panjang mereka sampai 2,0 cm.



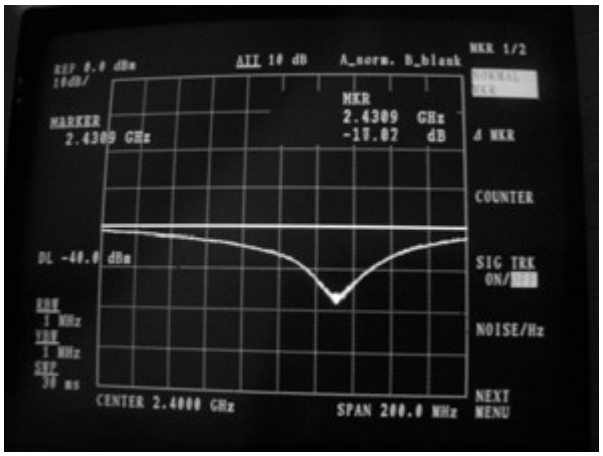
Gambar 4.28: Ulangi prosedur merentang untuk semua lilitan yang tersisa.

13. Selesai sudah konstruksi fisik antenna, antenna berukuran 42,5 cm dari pelat ke atas.



Gambar 4.29: antena yang sudah selesai berukuran 42,5 cm dari pelat hingga akhir kawat.

14. Jika anda mempunyai spektrum analyzer dengan tracking generator dan directional coupler, anda dapat memeriksa kurva dari daya yang di pantulkan oleh antenna. Gambar di bawah menunjukkan sebuah gambaran spektrum analyzer.



Gambar 4.30: Plot dari daya yang di pantulkan oleh antenna collinear omni.

Jika anda bermaksud memakai antena ini di luar ruangan, anda akan perlu membuatnya tahan cuaca. Metode yang paling sederhana adalah menutup seluruh bagian dengan sepotong pipa PVC besar yang tertutup dengan penutupnya. Lubangi bagian bawah untuk coa, dan sekatlah antena tersebut secara rapat dengan silikon atau lem PVC.

Antena Kaleng

Antena bumbung gelombang, yang kadang-kadang disebut Cantenna dari asal “can antenna” atau antenna kaleng, menggunakan kaleng sebagai bumbung gelombang dan sebuah kawat pendek yang disolder di konektor N sebagai probe untuk peralihan dari kabel koaksial ke bumbung gelombang. Pembuatan antena ini sangat murah karena hanya menggunakan konektor, kaleng bekas makanan, jus dan sebagainya. Antena ini adalah antena pengarah, yang berguna untuk sambungan point-to-point dengan jarak pendek ke sedang. Antena ini juga dapat digunakan sebagai input untuk piringan atau kisi-kisi parabolik.

Tidak semua kaleng dapat digunakan untuk dibuat sebagai antena karena harus memenuhi ukuran tertentu..

1. Nilai diameter D input yang dapat di terima adalah antara 0,60 dan 0,75 panjang gelombang di udara pada frekuensi yang diinginkan. Panjang gelombang frekuensi 2.44 GHz adalah 12,2 cm, oleh sebab itu diameter kaleng sebaiknya dalam wilayah 7,3 - 9,2 cm.

2. Panjang kaleng L sebaiknya sedikitnya 0,75 λ_G, di mana λ_G adalah panjang gelombang pemandu dan diberi oleh:

$$\lambda$$

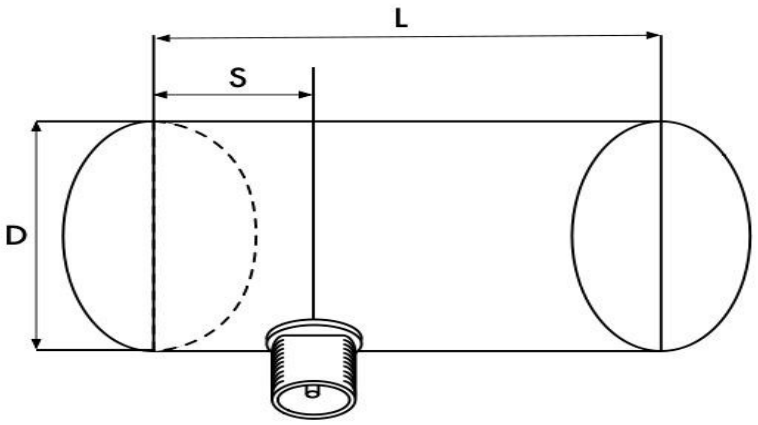
$$\lambda_G = \frac{}{\text{sqrt}(1 - (\lambda / 1.706D)^2)}$$

Untuk D = 7,3 cm, kita membutuhkan sebuah kaleng berukuran sedikitnya 56,4 cm, sedangkan untuk D = 9,2 cm kita membutuhkan kaleng berukuran sedikitnya 14,8 cm. Secara umum semakin kecil diameternya, semakin panjang kaleng yang dibutuhkan. Untuk contoh yang kami berikan, kami akan memakai kaleng minyak berdiameter 8,3 cm dan mempunyai panjang sekitar 21 cm.

3. Probe untuk kabel koaksial untuk injeksi ke bumbung gelombang sebaiknya ditempatkan dengan jarak S dari dasar kaleng, dengan rumus yang diberi oleh:

$$S = 0{,}25\ \lambda_G$$

Panjangnya harus 0,25 λ, yang pada 2,44 GHz adalah 3,05 cm.



Gambar 4.31: Dimensi yang harus di penuhi cantenna

Gain untuk antena akan sekitar 10 sampai 14 dBi, dengan beamwidth sekitar 60 derajat.

Gambar 4.32: Cantenna yang telah selesai dibuat.

Daftar komponen

- Ssatu konektor perempuan tipe N.
- Kawat tembaga atau kuningan 4 cm berdiameter 2 mm
- Kaleng minyak dengan diameter 8,3 cm dan tinggi 21 cm

Gambar 4,33: Komponen yang diperlukan untuk membuat sebuah antena kaleng.

Alat yang di perlukan

- Pembuka kaleng
- Penggaris
- Tang
- Amplas
- Timah solder
- Solder

- Bor dengan set mata bor untuk logam (dengan mata bor berdiameter 1,5 cm)
- Vice atau mengepit
- Spanner atau kunci inggris
- Palu
- Paku

Pembuatan

1. Dengan pembuka kaleng, buka dengan hati-hati tutup atas kaleng.

Gambar 4.34: hati-hati terhadap pinggir tajam ketika membuka kaleng.

Piringan tutup kaleng mempunyai pinggiran yang sangat tajam. Hati-hati ketika menanganinya! Kosongkan kaleng dan cucilah dengan sabun. Jika kaleng berisi nanas, biskuit, atau makanan lezat lain, hidangkan makanan tersebut dahulu kepada orang lain.

2. Dengan penggaris, ukurlah 6,2 cm dari dasar kaleng dan tandai dengan paku. Hati-hati dalam mengukur dari dasar. Pakai pemukul (atau mata bor yang kecil atau sebuah Obeng bintang) dan palu untuk menandakan titik. Ini membuatnya lebih mudah membor lubang secara tepat. Hati-hati untuk tidak mengubah bentuk kaleng. Lakukan ini dengan memasukkan balok kecil kayu atau objek lain di kaleng sebelum mengetuk-ngetuknya.

Gambar 4.35: Berikan tanda pada lubang sebelum membor.

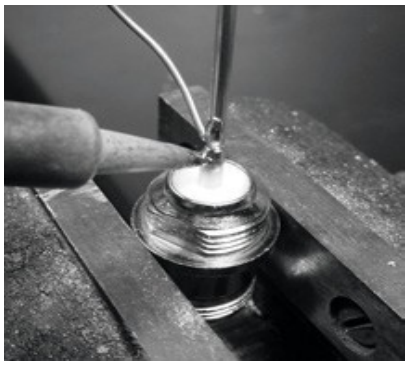
3. Dengan bor ber diameter kecil, buatlah lubang di pusat kaleng yang sudah di tandai. Tambahkan diameter lubang dengan menggunakan mata bor berdiameter lebih besar. Lubang harus cocok dengan diameter konektor N. Pergunakan amplas untuk melicinkan batas lubang dan untuk menyingkirkan sisa ukiran di sekitarnya untuk menjamin kontak listrik yang lebih baik dengan konektor.

Gambar 4.36: Secara teliti borlah lubang penunjuk, kemudian gunakan mata bor yang sedikit lebih besar untuk menyelesaikan pekerjaan.

4. Haluskan ujung kawat dengan menggunakan amplas. Berikan timah pada kawat untuk sekitar 0,5 cm dari ujung tersebut.

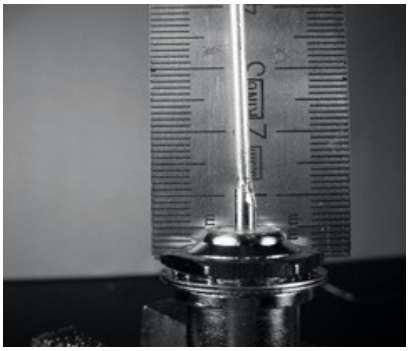
Gambar 4.37: Berikan timah pada ujung kawat sebelum disolder.

5. Dengan solder besi, berikan timah pada pin pusat konektor. Sambil menjaga kawat agar tetap vertikal dengan tang, solderlah sisi yang penuh timah di dalam lubang pin pusat konektor N.



Gambar 4.38: solderlah kawat ke pin emas di atas konektor N..

6. Masukkan ring dan sekrup mur ke konektor secara perlahan. Potong kawat sepanjang 3,05 cm yang diukur dari bagian dasar mur.



Gambar 4.39: panjang kawat sangatlah penting.

7. Lepaskan mur dari konektor, tinggalkan ring di tempatnya. Masukkan konektor ke dalam lubang kaleng. Sekrup mur di konektor dari dalam kaleng.

Gambar 4.40: memasang antena.

8. Pergunakan tang atau kunci inggris untuk mengencangkan mur pada konektor. Anda sudah selesai!

Gambar 4.41: Antena Kaleng Anda yang sudah selesai.

Seperti disain antenna lainnya, anda sebaiknya membuat penutup yang tahan cuaca untuk antena jika anda menginginkan untuk menggunakannya di luar ruangan. PVC sangat cocok untuk antena kaleng. Masukkan kaleng seluruhnya ke dalam sisi PVC yang besar, dan tutup menggunakan dop pralon di ujung-nya dan lem. Anda akan perlu membor sebuah lubang di sisi tabung untuk tempat konektor N di sisi kaleng.

Cantenna sebagai piringan input

Seperti USB wireless parabola, anda dapat menggunakan desain cantenna sebagai feeder untuk memperoleh gain yang lebih tinggi. Pasang kaleng di fokus parabola dengan lubang kaleng tertuju ke pusat piringan parabola. Gunakan teknik yang sudah dijelaskan pada contoh antena USB wireless (memperhatikan perubahan kekuatan sinyal sepanjang waktu) untuk

menemukan lokasi terbaik kaleng untuk parabola yang anda sedang menggunakan.

Dengan menggunakan cantenna yang terbuat baik dengan bentuk parabola yang sudah dituning secara benar, anda bisa mendapatkan gain antena keseluruhan 30dBi atau lebih. Pada saat ukuran parabola bertambah, bertambah pula gain dan potensi pengarahan antena. Dengan parabola yang sangat besar, anda dapat meraih gain yang tinggi secara signifikan. Misalnya, pada 2005, sebuah tim mahasiswa berhasil memasang sambungan dari Nevada ke Utah di Amerika Serikat. Sambungan melintasi jarak lebih dari 200 kilometer! Mereka menggunakan piringan parabola satelit berukuran 3,5 meter untuk memasang sambungan 802.11b yang beroperasi di 11 Mbps, tanpa amplifier. Detail tentang prestasi ini bisa ditemukan di http://www.wifi-shootout.com/

NEC2

NEC2 adalah singkatan dari ***Numerical Electromagnetics Code*** (versi 2) dan adalah free software untuk pemodelan antenna. NEC2 membantu anda membuat model antena dalam tiga dimensi, dan mensimulasi respon elektromagnetik antena. NEC2 dikembangkan lebih dari sepuluh tahun yang lalu dan sudah di-compile agar dapat berjalan di banyak sistem komputer yang berbeda. NEC2 benar-benar efektif untuk menganalisa model wiregrid, tetapi juga mempunyai suatu kemampuan permodelan patch permukaan.

Disain antena di tulis / di jelaskan dalam sebuah file teks, dan model dibangun menggunakan deskripsi teks ini. Antena yang dijelaskan dalam NEC2 diberi dalam dua bagian: ***struktur*** dan urutan ***kontrol.*** Struktur secara sederhana adalah deskripsi numerik mengenai dimana bagian-bagian antena yang berbeda ditemukan, dan bagaimana kawat disambung. Kontrol memberi tahu NEC di mana sumber RF dihubungkan. Setelah semuanya jelas, antena yang memancarkan kemudian dijadikan model. Karena teori ketimbal-balikan, pola gain pemancaran sama seperti yang penerimaan, sehingga memodelkan sifat pengiriman sudah cukup untuk memahami perlilaku antena secara lengkap.

Frekuensi atau wilayah frekuensi dari sinyal RF harus ditentukan. Elemen penting berikutnya adalah karakteristik tanah. Kondutivitas tanah berubah-ubah dari satu tempat ke tempat lain, tetapi dalam banyak kasus konduktivitas itu memainkan peran yang sangat penting dalam menentukan pola radiasi antena.

Untuk menjalankan NEC2 di Linux, pasanglah paket NEC2 dari URL yang tersedia di bawah. Untuk menjalankannya, ketik **nec2** dan masukan nama file input dan ourput. Hal lain yang juga penting adalah memasang paket **xnecview** untuk verifikasi struktur dan plot pola radiasi. Jika semua yang berhasil anda akan mempunyai file berisi output perhitungan. File ini dibagi ke dalam berbagai bagian, tetapi untuk dapat memahami secara cepat pola radiasi dapat dilihat menggunakan xnecview. Anda akan melihat pola radiasi yang diharapkan, secara horisontal omnidirectional, dengan puncak di sudut take off. Versi Windows dan Mac juga

tersedia.

Keuntungan NEC2 adalah bahwa kita dapat mendapatkan pemahaman mengenai bagaimana antena bekerja terlebih dahulu sebelum membuatnya, dan bagaimana kita dapat mengubah bentuk untuk mendapat gain maksimum. NEC2 adalah software yang kompleks dan memerlukan suatu penelitian untuk memperlajari bagaimana caranya untuk menggunakannya secara efektif, tetapi NEC2 adalah alat yang sangat berharga bagi perancang antena.

NEC2 tersedia di *http://www.nec2.org/*

Dokumentasi online bisa didapatkan dari "Unofficial NEC Home Page" di *http://www.nittany-scientific.com/nec/.*

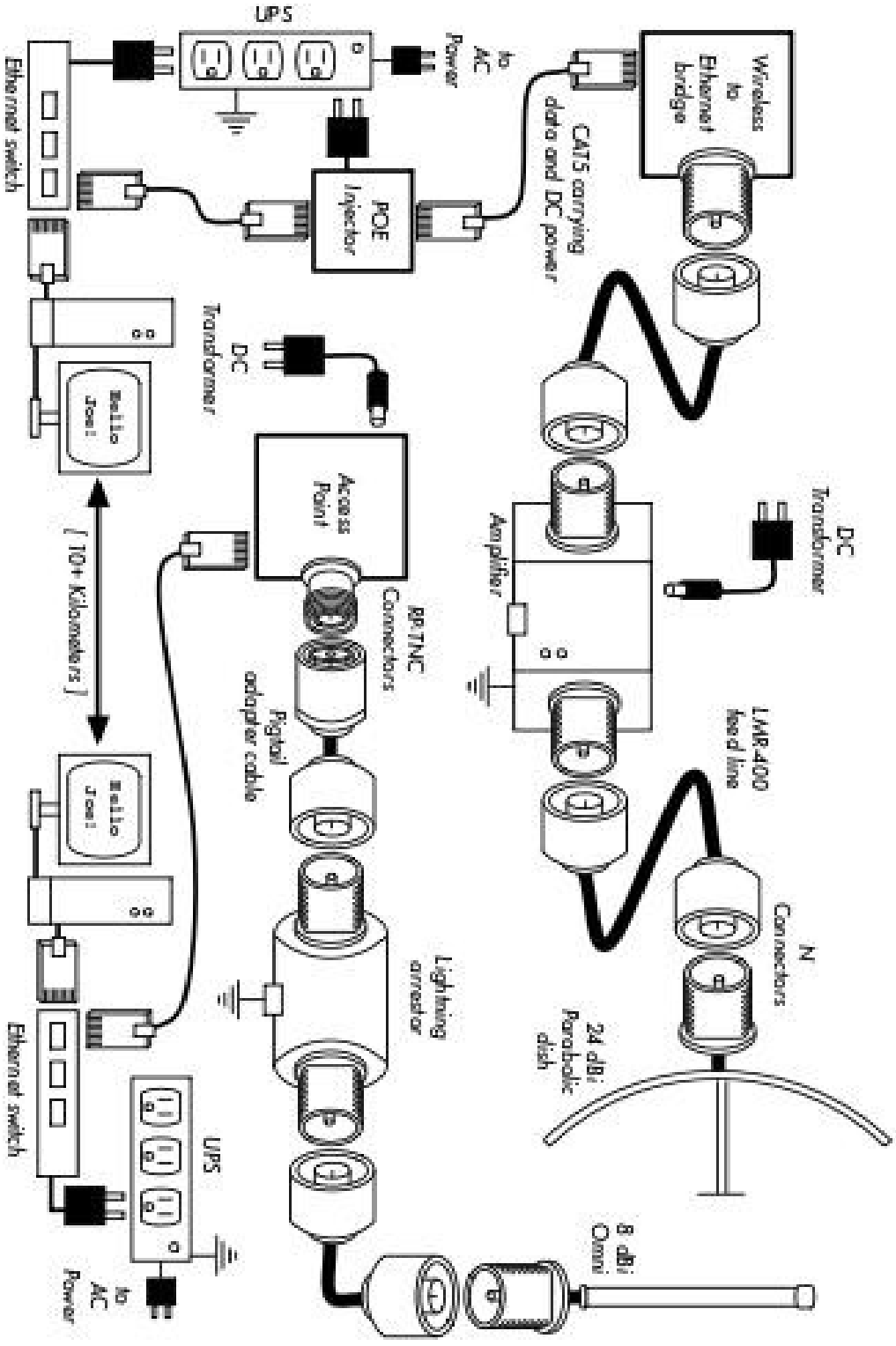
Bab 5 Perangkat Keras Jaringan

Dalam beberapa tahun belakangan, terjadi perkembangan luar biasa perangkat keras nirkabel sehingga membanjirkan banyak peralatan nirkabel murah di pasar. Jenisnya begitu, sehingga mustahil untuk membuat katalog semua komponen yang ada. Dalam bab ini, kita akan melihat beberapa fitur dan sifat yang diinginkan pada komponen nirkabel, dan memahami beberapa contoh peralatan komersial dan DIY yang sudah berkerja dengan baik di masa lalu.

Nirkabel yang tersambung

Dengan istilah seperti “wireless”, anda mungkin terkejut dengan berapa banyak kawat dilibatkan dalam membuat sambungan point-to-point sederhana. Sebuah node nirkabel terdiri dari banyak bagian, yang harus dihubungkan satu sama lain dengan kabel yang sesuai. Anda tentunya memerlukan sedikitnya satu komputer yang dihubungkan dengan jaringan Ethernet, dan router atau bridge nirkabel yang dipasang di jaringan yang sama. Bagian radio perlu dihubungkan dengan antena, tetapi suatu waktu mereka mungkin perlu berhubungan dengan amplifier, penangkal petir, atau alat lainnya. Banyak bagian memerlukan daya, baik melalui listrik AC atau memakai trafo DC. Semua bagian ini menggunakan berbagai macam konektor, tidak terlepas dari berbagai jenis tipe kabel dan ketebalannya.

Coba kalikan kabel dan konektor tersebut dengan jumlah node yang anda akan gunakan untuk online, dan anda mungkin bertanya-tanya mengapa barang ini dikatakan “wireless”. Diagram berikut akan memberi anda gambaran mengenai jumlah dan tipe kabel yang diperlukan untuk sambungan satu titik ke yang lainnya. Perhatikan bahwa diagram ini tidak berdasarkan skala, juga bukan merupakan pilihan terbaik bentuk jaringan. Namun diagram ini akan memperkenalkan anda banyaknya interkoneksi yang mungkin anda akan temukan di dunia sesungguhnya.



Gambar 5.1: Interkoneksi sambungan.

Sementara komponen yang digunakan sesungguhnya dapat berbeda dari satu node ke node lain, setiap instalasi akan menyertakan komponen berikut:

1. Komputer atau jaringan yang sudah ada yang tersambung ke Ethernet switch.
2. Alat yang menyambungakan jaringan ke peralatan nirkabel (radio router, bridge, atau repeater).
3. Antena yang tersambung melalui feed line, atau diintegrasikan ke dalam alat nirkabel itu sendiri.
4. komponen listrik yang terdiri dari power supply, regulator, dan penangkal petir.

Pemilihan perangkat keras sebaiknya ditentukan dengan membuat persyaratan untuk proyek, menentukan anggaran, dan mengecek bahwa proyek ini sangat mungkin menggunakan sumber daya yang ada (termasuk menyediakan cadangan dan biaya pemeliharaan). Seperti yang dibicarakan di **Bab 1**, menentukan scope proyek anda sangat penting sebelum mengambil keputusan untuk membeli perlengkapan.

Memilih komponen nirkabel

Sayangnya, dalam dunia dimana banyak pembuatan perangkat keras yang kompetitif dan anggaran yang terbatas, harga adalah faktor tunggal yang biasanya menerima perhatian paling banyak. Pepatah mengatakan “anda mendapat apa yang anda bayar” seringkali benar ketika membeli peralatan berteknologi tinggi, tetapi sebaiknya tidak dianggap sebagai kebenaran mutlak. Sementara harga adalah bagian penting dari pengambilan keputusan, adalah vital untuk mengerti secara persis apa yang anda dapat untuk uang anda sehingga anda bisa membuat pilihan yang sesuai dengan keperluan anda. Ketika membandingkan perlengkapan nirkabel untuk penggunaan di jaringan anda, pastikan anda mempertimbangkan variabel berikut:

- **Interoperability.** Apakah peralatan yang anda sedang pertimbangkan dapat bekerja dengan peralatan dari pabrik lain? Jika tidak, apakah ini adalah faktor penting untuk bagian jaringan anda tersebut? Jika alat yang sedang dipertanyakan mendukung protokol terbuka (seperti 802.11b/g), maka alat tersebut mungkin dapat interoperate dengan peralatan dari sumber lain.

- **Jarak.** Seperti yang kita lihat di **Bab 4**, jarak adalah sesuatu yang tak terpisahkan dari sebuah alat. Jarak jangkau sebuah alat bergantung pada antena yang tersambung dengannya, keadaan tanah sekitarnya, sifat alat di ujung sambungan yang lain, dan faktor lainnya. Daripada bergantung pada penilaian jarak yang disediakan oleh pabrik, lebih baik untuk mengetahui ***daya pancar radio*** serta ***gain antena*** (jika antena termasuk). Dengan informasi ini, anda bisa memperhitungkan jarak jangkau teoritis seperti yang telah dijabarkan di **Bab 3.**

- **Kepekaan radio.** Seberapa peka alat radio tersebut pada suatu kecepatan pengiriman data? Vendor sebaiknya menyediakan informasi ini, minimal di kecepatan yang paling cepat dan paling lambat. Ini dapat dipakai sebagai ukuran kualitas perangkat keras, sekaligus memungkinkan anda untuk menyelesaikan perhitungan link budget. Seperti yang kita telah lihat di **Bab 3**, angka yang lebih rendah lebih baik untuk kepekaan radio.

- **Throughput.** Vendor biasanya mencantumkan kecepatan yang paling tinggi sebagai "speed" alat mereka. Ingat bahwa kecepatan radio (misalnya 54 Mbps) bukan merupakan throughput alat yang sebenarnya (misalnya sekitar 22 Mbps untuk 802.11g). Jika laju informasi throughput tidak tersedia untuk alat yang anda sedang evaluasi, perkiraan yang baik adalah membagi "kecepatan" alat menjadi dua, dan kurangi 20% atau lebih. Kalau ragu-ragu, lakukan tes throughput pada sebuah unit terlebih dahulu sebelum berkomitmen untuk membeli peralatan yang sangat banyak namun tidak mempunyai penilaian throughput yang baik.

- **Aksesori yang diperlukan.** Untuk menjaga harga agar tetap rendah, vendor sering tidak menyediakan informasi mengenai aksesori yang diperlukan untuk penggunaan biasa. Apakah label harga termasuk semua adaptor daya? (power supply DC biasanya termasuk; daya melalui injektor Ethernet biasanya tidak. Juga teliti kembali tegangan listrik-nya, karena peralatan sering kali disediakan dengan sumber listrik Amerika Serikat). Bagaimana dengan pigtail, adapter, kabel, antena, dan card radio? Jika anda bermaksud menggunakannya di luar, apakah alat sudah memiliki kotak weatherproof?

- **Ketersediaan.** Apakah anda akan secara mudah mengganti komponen yang rusak atau tidak jalan? Apakah anda dapat memesan komponen tersebut dalam kuantitas berjumlah besar, jika proyek anda membutuhkannya? Kira-kira berapa lama umur produk ini, baik lama waktu kegunaan di lapangan maupun ketersediaannya dari vendor?

- **Faktor lain.** Pastikan bahwa fitur lain yang diperlukan tersedia untuk memenuhi kebutuhan khusus anda. Misalnya, apakah alat tersebut memiliki konektor antena eksternal? Jika iya, apakah tipenya? Apakah ada keterbatasan dalam jumlah pengguna atau throughput yang disebabkan oleh perangkat lunak, dan jika iya, berapa biaya yang harus ditanggung untuk menambah batas ini? Berapa besarkah alat tersebut? Berapa besar daya yang digunakannya? Apakah alat itu mendukung POE sebagai sumber daya? Apakah alat tersebut menyediakan enkripsi, NAT, software monitor bandwidth, atau fitur lainnya yang penting untuk desain jaringan yang diinginkan?

Dengan menjawab pertanyaan-pertanyaan ini terlebih dahulu, anda akan dapat membuat keputusan membeli yang baik saat memilih jaringan perangkat keras. Tak mungkin anda akan dapat menjawab setiap pertanyaan yang ada terlebih dahulu sebelum membeli perlengkapan, tetapi jika anda memprioritaskan pertanyaan dan meminta vendor untuk menjawab

pertanyaan-pertanyaan tersebut sebelum membuat komitmen pembelian, anda akan memakai anggaran secara baik dan membuat jaringan komponen yang sesuai dengan kebutuhan anda.

Solusi Komersial vs. DIY

Proyek jaringan anda pastinya akan terdiri dari komponen yang dibeli dari vendor serta komponen yang didapatkan atau malah dibuat secara lokal. Ini adalah kenyataan ekonomi yang mendasar di banyak daerah di dunia. Di tahap ini dari teknologi manusia, distribusi informasi secara global lebih jelas dibandingkan dengan distribusi global barang-barang. Di banyak daerah, impor komponen yang diperlukan untuk membuat jaringan sangatlah mahal bagi kebanyakan orang kecuali yang mempunyai anggaran paling besar. Anda dapat menghemat dengan mencari sumber lokal untuk komponen yang di perlukan dan tenaga kerja, dan hanya mengimpor komponen yang harus dibeli.

Tentu saja, ada batas sampai sejauh apa kerjaan yang dapat dilakukan oleh individu atau kelompok yang mana pun dalam jumlah waktu yang diberikan. Dalam kata lain, dengan mengimpor teknologi, anda dapat menukar uang untuk perlengkapan yang bisa memecahkan masalah tertentu dalam waktu yang relatif pendek. Seni membuat prasarana telekomunikasi lokal adalah mencari keseimbangan yang tepat antara uang terhadap usaha yang perlu dikeluarkan untuk memecahkan masalah yang ada.

Beberapa komponen, seperti card radio dan feed line antena, mungkin jauh terlalu kompleks untuk dipertimbangkan sebagai sesuatu dapat diproduksi secara lokal. Komponen lainnya, seperti antena dan menara, relatif sederhana dan bisa dibuat secara lokal dengan biaya yang kecil dibandingkan dengan biaya pengimporan. Antara kedua ekstrem ini terletak alat komunikasi itu sendiri.

Dengan menggunakan card radio, motherboard, dan komponen lain yang ada di pasaran, anda dapat membuat alat yang menyediakan fitur hampir sama (atau bahkan lebih baik dari) dengan kebanyakan implementasi komersial. Menggabungkan platform perangkat keras terbuka dengan perangkat halus open source bisa menghasilkan dampak yang luar biasa dengan menghasilkan solusi yang dapat di kustomisasi, kuat untuk biaya yang sangat rendah.

Ini tidak bermaksud mengatakan bahwa peralatan komersial tidak baik dibandingkan solusi yang anda buat sendiri. Dengan menyediakan apa yang dinamakan “turn-key-solution”, vendor tak hanya menghemat waktu pengembangan, tetapi mereka juga bisa memungkinkan orang yang relatif tak berketrampilan untuk memasang dan memelihara peralatan. Kekuatan utama solusi komersial adalah bahwa mereka menyediakan ***bantuan*** dan ***garansi peralatan*** (yang biasanya terbatas). Mereka juga menyediakan platform yang konsisten yang cenderung mengarah pada instalasi jaringan yang stabil, dan dapat dengan mudah di pertukarkan.

Jika sebuah peralatan idak bekerja atau sulit dikonfigurasi atau di-troubleshoot, vendor yang baik akan membantu anda. Jika peralatan tidak berfungsi dalam keadaan normal (kecuali kerusakan ekstrim, seperti tersambar petir), maka vendor biasanya akan menggantinya. Kebanyakan yang akan menyediakan jasa ini untuk waktu terbatas sebagai bagian dari harga beli, dan banyak yang menawarkan bantuan dan garansi selama periode panjang dengan biaya bulanan. Dengan menyediakan platform yang konsisten, sangat mudah untuk menyimpan cadangan dan dengan sederhana "menukar" peralatan yang gagal, tanpa diperlukannya seorang teknisi untuk menkonfigurasi peralatan di tempat. Tentu saja, semuanya ini datang dengan biaya awal yang relatif lebih tinggi dibandingkan komponen peralatan yang tidak tersedia di pasaran.

Dari sudut pandang seorang arsitek jaringan, tiga risiko terbesar yang tersembunyi ketika memilih pemecahan komersial adalah **ketergantungan vendor, produk yang tidak diproduksi lagi**, dan **biaya lisensi yang terus-menerus bertambah.**

Bisa sangat mahal untuk membiarkan "fitur" baru yang tidak jelas mengendalikan pengembangan jaringan anda. Vendor sering kali akan menyediakan fitur yang bertentangan dengan kompetisi mereka berdasarkan desain, dan kemudian mengeluarkan sebagai bahan promosi untuk meyakinkan anda bahwa anda tidak bisa hidup tanpa mereka (terlepas apakah fitur tersebut sebenarnya berkontribusi ke solusi untuk problem komunikasi anda). Sewaktu anda mulai bergantung pada fitur-fitur ini, anda mungkin akan memutuskan terus membeli peralatan dari vendor yang sama di masa mendatang. Ini adalah intisari ketergantungan vendor. Jika lembaga besar menggunakan peralatan berpaten dalam jumlah besar, tak mungkin mereka dengan mudah meninggalkannya untuk memakai vendor yang berbeda. Tim penjualan memahami ini (dan memang, beberapa mengandalkannya) dan menggunakan ketergantungan vendor ini sebagai strategi untuk perundingan harga.

Kalau dikombinasikan dengan ketergantungan vendor, sebuah vendor akhirnya mungkin memutuskan menghentikan lini produk, walaupun produk tersebut populer. Ini menjamin bahwa pelanggan, yang sudah tergantung pada fitur proprietary vendor, akan membeli model yang paling baru (dan hampir yang selalu lebih mahal). Efek jangka panjang ketergantungan vendor pada produk yang dihentikan sulit diperkirakan pada saat merencanakan proyek jaringan, tetapi sebaiknya diingat.

Akhirnya, jika sebuah bagian khusus peralatan menggunakan software proprietary, anda mungkin perlu membayar lisensi penggunaan kode tersebut secara terus-menerus. Biaya lisensi ini mungkin berubah-ubah menurut fitur yang disediakan, jumlah pengguna, kecepatan sambungan, atau faktor lainnya. Jika biaya lisensi tidak dibayar, beberapa peralatan didesain untuk berhenti berfungsi sampai sebuah lisensi yang sah dan sudah dibayar! Pastikan bahwa anda memahami syarat-syarat penggunaan peralatan yang anda beli, termasuk diantaranya adalah biaya lisensi yang muncul.

Dengan memakai peralatan yang mendukung standar terbuka dan perangkat lunak open source, anda dapat menghindari beberapa perangkap ini. Misalnya, sangatlah sulit untuk tergantung pada vendor yang menggunakan protokol terbuka (seperti TCP/IP melalui 802.11a/b/g). Jika anda menemukan masalah dengan peralatan atau vendornya, anda selalu dapat membeli peralatan dari vendor yang berbeda tapi tetap dapat beroperasi dengan

peralatan yang sudah ada. Karena alasan ini kami anjurkan menggunakan protokol proprietari dan spektrum berlisensi hanya dalam kasus di mana penggunaan peralatan terbuka (seperti 802.11a/b/g) secara teknis tidak mungkin.

Demikian juga, sementara produk selalu bisa dihentikan produksinya kapan saja, anda bisa membatasi dampak yang ditimbulkan terhadap jaringan anda dengan menggunakan komponen generik. Misalnya, sebuah motherboard tertentu mungkin menjadi tak yang ada lagi di pasar, tetapi anda mungkin mempunyai sejumlah motherboard PC yang tersedia yang dapat berfungi secara efektif untuk keperluan yang sama. Kita akan melihat beberapa contoh bagaimana caranya mempergunakan komponen umum ini untuk membuat node nirkabel yang lengkap nanti di bab ini.

Tentu saja, tidak ada biaya lisensi yang terkait dengan perangkat lunak open source (dengan pengecualian vendor yang menyediakan bantuan lebih atau suatu jasa lain, tanpa adanya biaya untuk penggunaan perangkat lunak itu sendiri). Sekali-sekali memang ada vendor yang mengkapitalisasi sumber gratis yang sudah diberikan kepada dunia oleh pemrogram open source untuk penjualan berlisensi secara terus menerus, sehingga melanggar syarat-syarat distribusi yang sudah diatur oleh pencipta aslinya. Lebih bijaksana untuk menghindari vendor seperti itu, dan untuk waspada terhadap klaim “free software” yang tersedia dengan biaya lisensi.

Kerugian dari menggunakan software open source dan hardware generik adalah masalah dukungan / support. Sewaktu timbul masalah di jaringan, anda perlu memecahkan masalah itu sendiri. Ini sering diselesaikan dengan berkonsultasi pada sumber online dan mesin pencari yang gratis, dan mengaplikasikan patch untuk software secara langsung. Jika anda tidak mempunyai anggota tim yang kompeten dan berdedikasi untuk mendesain solusi atas masalah komunikasi anda, maka bisa diperlukan cukup banyak waktu untuk memulai proyek jaringan. Tentu saja, tidak pernah ada jaminan bahwa dengan “melempar uang kepada masalah” akan memecahkan masalah. Sementara kami menyediakan banyak contoh bagaimana cara untuk mengerjakan sebagian besar kerjaan sendiri, anda mungkin merasa pekerjaan ini sangat menantang. Anda akan perlu menemukan keseimbangan antara solusi komersial dan apa yang anda bisa lakukan sendiri untuk proyek.

Pendek kata, selalu cari tahu scope jaringan anda terlebih dulu, kenali sumber yang anda dapat gunakan untuk memecahkan masalah, dan biarkan seleksi peralatan secara alami muncul sebagai hasilnya. Pertimbangkan solusi komersial serta komponen terbuka, sekaligus mengingat biaya jangka panjang untuk keduanya.

Saat mempertimbangkan perlengkapan mana yang akan digunakan, selalu ingat untuk membandingkan jarak jangkau yang diharapkan, ketahanan, dan throughput, disamping harganya. Pastikan untuk memperhitungkan biaya lisensi apapun pada saat memperhitungkan biaya keseluruhan peralatan. Dan akhirnya, pastikan bahwa radio yang anda beli beroperasi di pita yang tak berlisensi di mana anda memasang radio tersebut, atau jika anda harus menggunakan spektrum berlisensi, bahwa anda mempunyai anggaran dan izin untuk membayar lisensi yang sesuai.

Perlindungan petir profesional

Petir adalah predator alami peralatan nirkabel. Ada dua cara berbeda petir bisa menyambar atau merusak peralatan: sambaran langsung atau induksi. Sambaran langsung terjadi saat petir mengenai menara atau antena. Induksi disebabkan kalau petir yang menyambar di dekat menara. Bayangkan petir yang membawa banyak muatan listrik negatif. Karena muatan listrik yang sama akan saling tolak menolak, petir akan membuat elektron di kabel berpindah saat terjadi sambaran, hal ini menciptakan arus listrik di atas kawat. Arus listrik sangat mungkin cukup besar di luar kapasitas peralatan radio tersebut. Salah satu dari kedua jenis sambaran ini biasanya akan menghancurkan perlengkapan yang tak terlindungi.

Gambar 5.2: menara dengan sebuah kawat tembaga besar yang menghubungkan ke tanah

Melindungi jaringan nirkabel dari petir bukan ilmu pasti, dan tidak ada jaminan bahwa sambaran petir tidak akan terjadi, sekalipun setiap tindakan pencegahan telah diambil. Banyak metode yang sudah digunakan akan membantu mencegah baik sambaran langsung maupun induksi. Memang kita tidak perlu mengimplementasikan semua metode perlindungan petir, semakin banyak metode perlindungan yang digunakan semakin baik peralatan terlindungi. Perkiraan banyaknya petir yang ada di suatu daerah akan menjadi pemandu seberapa banyak pekerjaan yang perlu dilakukan.

Mulai dari bagian terbawah menara. Ingat, dasar menara berada di bawah tanah. Sesudah fondasi menara terpasang, namun sebelum lubang diisi, sebuah lingkaran kawat besar berulir penghubung tanah sebaiknya dipasang dengan timbal memanjang di atas permukaan tanah berhadapan dengan dekat kaki menara. Kawat yang digunakan sebaiknya adalah American Wire Gauge (AWG) #4 atau lebih tebal. Sebagai tambahan, penghubung tanah atau tangkai cadangan sebaiknya dimasukan ke dalam tanah, dan sebuah kawat penghubung tanah tersambung dari tangkai ke timbal pada tungkai ulir yang dipendam.

Penting untuk diperhatikan adalah bahwa tidak semua baja mengkonduksikan listrik dengan cara yang sama. Beberapa baja bertindak sebagai konduktor listrik yang lebih baik daripada yang lainnya, dan lapisan permukaan yang berbeda juga bisa mempengaruhi bagaimana baja menara menangani listrik. Baja tahan karat adalah salah satu di antara konduktor yang

paling jelek, dan lapisan tahan karat seperti penguat atau cat mengurangi kondutivitas baja. Atas alasan ini, sehelai kawat penghubung tanah berulit dipasang dari dasar menara hingga ke atas. Bagian dasar perlu disambungkan dengan baik ke timbal ada di ulir maupun dari tangkai cadangan penghubung tanah. Puncak menara sebaiknya tersambung tangkai petir, dan puncak penangkal petir harus tajam. Semakin runcing dan tajam puncaknya, semakin efektif tangkai tersebut. Kawat ulir penghubung tanah dari dasar perlu diakhiri di tangkai penghubung tanah. Sangat penting untuk memastikan bahwa kawat penghubung tanah dihubungkan dengan logam sebenarnya. Lapisan apapun, seperti cat, harus disingkirkan sebelum kawat disambungkan. Ketika hubungan sudah dibuat, bagian terbuka bisa dicat ulang, menutupi kawat dan konektor jika perlu untuk melindungi menara dari karat dan korosi lainnya.

Solusi di atas memperinci instalasi sistem grounding yang mendasar. Solusi ini menyediakan perlindungan untuk menara itu sendiri dari sambaran langsung, dan memasang sistem dasar yang berhubungan dengan peralatan apapun.

Perlindungan ideal untuk induksi dari sambaran petir adalah arrestor tabung gas di kedua akhir kabel. Arrestors ini perlu dihubungkan langsung ke kawat penghubung tanah yang terpasang di menara jika arrestor itu berada di ujung yang tinggi. Bagian dasar harus dihubungkan ke sesuatu yang aman untuk listrik, seperti pelat ground atau sebuah pipa tembaga yang secara konsisten berisi penuh air. Penting untuk memastikan bahwa arrestor petir dibuat tahan cuaca. Banyak arresters untuk kabel coax dibuat tahan cuaca, sedangkan banyak arresters untuk CAT5 kabel tidak.

Saat arrestor gas tidak digunakan, dan pengkabelan berbasis coax, maka menyambungkan ujung dari pelindung kabel coax ke instalasi kabel ground di tower akan menyediakan perlindungan. Ini dapat menyediakan jalan untuk arus induksi, dan jika charge cukup lemah, charge tersebut tidak akan mempengaruhi kawat konduktor kabel. Metode ini tidak sebaik perlindungan gas arrestors, tetapi metode ini lebih baik daripada tidak ada sama sekali.

Membuat sebuah Akses Point dari PC

Tidak seperti sistem operasi konsumen (seperti Microsoft Windows), sistem operasi GNU/Linux memberi seorang administrator ke potensi untuk mengakses penuh kemampuan jaringan. Seseorang dapat mengakses dan memanipulasikan paket jaringan di tingkat mana pun dari lapisan data-link hingga lapisan aplikasi. Keputusan Routing dapat diambil berdasarkan informasi apapun yang terdapat di paket jaringan, dari alamat routing dan port sampai ke isi bagian data. Akses point yang berbasis Linux dapat bertindak sebagai router, bridge, firewall, VPN concentrator, server application, monitor jaringan, atau hampir semua peran jaringan lain yang dapat anda pikirkan. OS tersebut tersedia secara gratis dan tidak memerlukan biaya lisensi. GNU/Linux adalah alat yang sangat kuat yang bisa mengisi berbagai jenis peran pada sebuah prasarana jaringan.

Menambahkan card nirkabel dan alat Ethernet ke PC yang menjalankan Linux akan memberi anda sebuah alat yang sangat fleksibel yang bisa membantu anda memberi bandwidth dan mengelola jaringan anda dengan biaya yang sedikit. Perangkat keras bisa dari apa saja dari laptop atau desktop bekas sampai ke embedded komputer, seperti Linksys WRT54G atau kit

jaringan Metrix.

Di bagian ini kita akan melihat bagaimana caranya mengkonfigurasi Linux dalam konfigurasi berikut:

- Sebagai akses point nirkabel dengan masquerading/NAT dan sambungan kabel ke Internet (biasanya di kenal sebagai wireless gateway).
- Sebagai akses point nirkabel yang bertindak sebagai bridge transparan. Jembatan dapat digunakan sebagai akses point sederhana, atau sebagai pengulang dengan 2 radio.

Pertimbangkan resep ini sebagai titik awal. Dengan menggunakan contoh sederhana ini, anda bisa membuat server yang bisa secara yang sangat sesuai dengan prasarana jaringan anda.

Persyaratan

Sebelum melanjutkan, anda sudah sebaiknya mengenal baik Linux dari perspektif pengguna, dan dapat menginstal distribusi Gnu/distribusi pilihan anda. Pengertian dasar perintah teks (terminal) dalam Linux juga diperlukan.

Anda akan memerlukan sebuah komputer dengan satu atau lebih card nirkabel yang sudah terpasang, dan juga interface Ethernet. Contoh ini menggunakan card dan driver tertentu, tetapi ada sejumlah kartu yang berbeda yang juga berfungsi sama baiknya. Kartu nirkabel berbasis chipset Atheros dan Prisma berfungsi secara baik. Contoh ini didasarkan di Ubuntu Linux versi 5.10 (Breezy Badger), dengan card nirkabel yang didukung oleh driver HostAP atau MADWiFi. Untuk informasi lebih banyak mengenai driver ini, lihatlah *http://hostap.epitest.fi/*dan *http://madwifi.org/.*

Perangkat lunak berikut diperlukan untuk menyelesaikan instalasi ini. Perangkat lunak ini biasanya disediakan di distribusi Linux anda:

- Tool untuk nirkabel (perintah iwconfig, iwlist)
- firewall iptables
- dnsmasq (caching DNS server dan DHCP server)

Daya CPU yang diperlukan bergantung pada seberapa banyak pekerjaan yang harus dilakukan diluar routing sederhana dan NAT. Untuk banyak aplikasi, sebuah mesin 486 133MHz dengan sempurna dapat melakukan routing paket pada kecepatan nirkabel. Jika anda bermaksud menggunakan banyak enkripsi (seperti WEP atau server VPN), maka anda akan memerlukan sesuatu yang lebih cepat. Jika anda juga ingin menjalankan caching server (seperti Squid) maka anda akan memerlukan komputer dengan harddisk dan RAM yang besar dan cepat. Sebuah router yang khusus hanya melakukan NAT akan beroperasi secara baik dengan hanya 64MB RAM dan harddisk.

Ketika membuat mesin yang dimaksudkan untuk menjadi bagian prasarana jaringan anda,

selalu ingat bahwa harddisk mempunyai umur yang terbatas dibandingkan dengan kebanyakan bagian lainnya. Anda dapat sering menggunakan bentuk penyimpanan yang solid, seperti flash disk, sebagai pengganti harddisk. Ini bisa berupa USB flash drive (mengasumsikan PC anda akan di-boot dari USB), atau kartu Compact Flash yang di pasang menggunakan CF ke IDE adapter. Adapter ini cukup murah, dan akan membuat kartu CF tampil berfungsi seperti IDE harddisk yang standar. Mereka bisa digunakan di PC apapun yang mendukung harddisk IDE. Karena mereka tidak mempunyai bagian yang bergerak, mereka akan beroperasi selama beberapa tahun tahun pada suhu operasi yang jauh lebih lebar daripada yang bisa ditolerir oleh hard disk.

Skenario 1: Akses point dengan Masquerading

Ini adalah yang paling sederhana di antara semua skenario, dan amat berguna di situasi di mana anda ingin sebuah akses point untuk kantor. Ini paling mudah di situasi di mana:

1. Ada Firewall khusus dan gateway yang menjalankan Linux, dan anda hanya ingin menambahkan wireless interface.
2. Anda mempunyai komputer bekas yang tua atau laptop yang ada, dan lebih suka untuk menggunakannya sebagai akses point.
3. Anda ingin lebih banyak kemampuan dalam mengamati, mencatatkan dan/atau keamanan daripada apa yang disediakan oleh kebanyakan akses point komersial, tetapi tidak mau berroyal-royal dengan akses point perusahaan.
4. Anda ingin sebuah mesin untuk bertindak sebagai 2 akses point (dan firewall) agar anda bisa memberikan akses jaringan yang aman ke ke intranet, maupun tamu dengan akses terbuka.

Setup awal

Mulailah dengan komputer yang sudah terkonfigurasi yang menjalankan GNU/Linux. Ini bisa berupa instalasi Ubuntu Server, atau Fedora Core. Komputer harus mempunyai sedikitnya 2 interface agar dapat berfungsi, dan sedikitnya salah satunya harus nirkabel. Sisa deskripsi ini mengasumsikan bahwa port Ethernet (eth0) yang tersambung kabel dihubungkan ke Internet, dan bahwa ada interface nirkabel (wlan0) yang akan menyediakan fungsi akses point. Untuk mencari tahu apakah chipset anda mendukung cara master, coba perintah berikut dengan user root:

```
# iwconfig wlan0 mode Master
```

... ganti wlan0 dengan nama interface nirkabel anda.

Jika anda mendapat error, maka kartu nirkabel anda tidak mendukung mode akses point. Anda masih bisa menguji susunan yang sama untuk mode Ad-hoc, yang didukung oleh semua chipsets. Ini memerlukan anda untuk menyetel semua laptop yang sedang bersambungan dengan “akses point” ke mode Ad-hoc juga, dan mungkin tidak berjalan sesuai dengan apa yang anda harapkan. Biasanya lebih baik menemukan kartu nirkabel yang akan mendukung mode AP. Lihat situs web HostAP dan MADWiFi untuk memperoleh daftar card yang didukung.

Sebelum meneruskan lebih lanjut, pastikanlah dnsmasq terinstal di mesin anda. Anda dapat menggunakan manajer paket grafis dari distribusi anda untuk menginstal dnsmasq. Dalam Ubuntu anda dengan sederhana dapat menjalankan perintah berikut sebagai root:

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

Mengkonfigurasi interface

Atur server anda agar eth0 terhubung ke Internet. Gunakan alat konfigurasi grafis yang datang dengan distribusi anda. Jika jaringan Ethernet anda memakai DHCP, anda bisa menggunakan perintah berikut sebagai root:

```
# dhclient eth0
```

Anda seharusnya menerima IP address dan default gateway. Selanjutnya, konfigurasi interface nirkabel anda ke mode Master dan beri nama pilihan anda:

```
# iwconfig wlan0 essid “jaringan saya” mode Master enc off
```

Switch **enc off** mematikan enkripsi WEP. Untuk mengaktifkan WEP, tambahkan string hexkey dengan panjang yang benar:

```
# iwconfig wlan0 essid “jaringan saya” mode Master enc 1A2B3C4D5E
```

Atau anda dapat menggunakan string teks yang dapat dibaca dengan memulai dengan “s:”

```
# iwconfig wlan0 essid “jaringan saya” mode Master enc “s:apple”
```

Sekarang berilah interface nirkabel anda IP address dalam sebuah subnet privat, namun pastikan subnet tersebut tidaklah sama dengan subnet Ethernet adapter anda:

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

Mengkonfigurasi masquerading di kernel

Supaya kita dapat menerjemahkan address antara kedua interface pada komputer, kita perlu untuk mengaktifkan masquerading (NAT) di kernel linux. Pertama kita muat modul kernel yang relevan:

```
# modprobe ipt MASQUERADE
```

Sekarang kita akan hapus semua peraturan firewall yang sudah ada untuk memastikan bahwa firewall tidak menghalangi kita dari meneruskan paket di antara kedua interface. Jika firewall yang sudah ada sedang berjalan, pastikan anda tahu bagaimana caranya nanti untuk memulihkan peraturan yang sudah ada sebelum melanjutkan.

```
# iptables -F
```

Aktifkan fungsi NAT di antara kedua interface

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

Akhirnya kita perlu memungkinkan kernel untuk dapat meneruskan paket di antara interface:

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

Pada Linux berbasis distribusi Debian seperti Ubuntu, pergantian ini juga bisa dibuat dengan mengedit file/etc/network/options, dan pastikan bahwa ip_forward diset ke yes:

```
ip_forward=yes
```

dan me-restart interface jaringan dengan:

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

atau

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

Mengkonfigurasi server DHCP

Pada tahapan ini kita harusnya sudah mempunyai akses point yang beroperasi. Hal ini dapat diuji dengan menyambungkan dengan jaringan nirkabel “jaringan saya” dari mesin lain dan memberi mesin itu sebuah alamat IP dalam wilayah alamat IP yang sama dengan interface nirkabel pada server (pada contoh digunakan 10.0.0.0/24). Jika anda sudah mengaktifkan WEP, pastikan supaya memakai kunci yang sama dengan yang anda tetapkan di akses point.

Untuk membuat lebih mudah bagi orang untuk menyambung ke server tanpa mengetahui wilayah alamat IP jaringan, kita akan membuat server DHCP untuk secara otomatis membagi-bagikan address kepada klien nirkabel.

Kita menggunakan program dnsmasq untuk tujuan ini. Seperti yang ditunjukkan oleh namanya, program ini menyediakan caching DNS server serta server DHCP. Program ini dikembangkan khususnya untuk penggunaan dengan firewall yang melakukan NAT. Kemampuan caching DNS server terutama berguna jika hubungan Internet anda mempunyai latensi sambungan yang tinggi dan/atau sambungan bandwidth rendah, seperti VSAT atau dial-up. Ini berarti bahwa banyak pencarian DNS yang harus di resolve secara lokal, menghemat banyak trafik di sambungan Internet, dan juga membuat koneksi terasa lebih cepat bagi mereka yang tersambung.

Install dnsmasq menggunakan manajer paket distribusi anda. Jika dnsmasq tidak tersedia sebagai paket, download source kode dan install secara manual. Ini tersedia di http://www.thekelleys.org.uk/dnsmasq/doc.html.

Apa yang kita butuhkan untuk menjalankan dnsmasq hanya mengedit beberapa baris pada file konfigurasi dnsmasq, /etc/dnsmasq.conf.

File konfigurasi sudah dikomentari secara baik, dan mempunyai banyak pilihan untuk berbagai macam konfigurasi. Untuk mengaktifkan server dasar DHCP dan membuatnya berfungsi, kita hanya perlu untuk menghapus komentar dan/atau menyunting dua garis.

Temukan garis yang dimulai dengan:

```
interface=
```

... pastikan kita mengeditnya menjadi:

```
interface=wlan0
```

... ubah wlan0 agar sesuai dengan nama interface wireless anda. Kemudian cari baris yang dimulai dengan:

```
#dhcp-range=
```

Hapus garis komentar dan sunting agar sesuai dengan alamat yang digunakan, misalnya:

```
dhcp-range=10.0.0.10.10.0.0.110.255.255.255.0.6h
```

Kemudian simpan file dan jalankan dnsmasq melalui perintah:

```
#/etc/init.d/dnsmasq start
```

Itu saja, sekarang anda dapat bersambungan dengan server sebagai akses point, dan mendapatkan alamat IP menggunakan DHCP. Ini akan memungkinkan anda untuk bersambungan dengan Internet melalui server.

Menambahkan keamanan ekstra: mengkonfigurasi Firewall

Ketika ini selesai dan telah di uji, anda dapat menambahkan tambahan peraturan firewall dengan menggunakan tool firewall yang tersedia di distribusi anda. Beberapa front-end / tool administrator untuk mengkonfigurasi firewall antara lain adalah:

- **firestarter** – klien grafis untuk Gnome, yang memerlukan server anda menjalankan Gnome
- **knetfilter** – klien grafis untuk KDE, yang memerlukan server anda menjalankan KDE
- **Shorewall** – sekumpulan script dan file konfigurasi yang akan membuatnya lebih mudah untuk menyusun iptables firewall. Ada juga front-end untuk shorewall, seperti webmin-shorewall.
- **fwbuilder** – sangat powerful, tapi merupakan tool grafik yang agak rumit dan memungkinkan anda untuk menciptakan script iptables pada mesin yang terpisah dari server anda, lalu mentransfer-nya ke server kemudian. Ini tidak mengharuskan anda untuk menjalankan desktop grafik pada server, dan merupakan pilihan terbaik bagi mereka yang sangat perhatian pada masalah keamanan.

Ketika semua sudah terkonfigurasi dengan baik, pastikan semua setting tersirat di script di sistem startup. Dengan cara ini, perubahan yang anda buat akan terus berjalan jika mesin harus di-boot ulang.

Skenario 2: Akses Point Dengan Kemampuan Bridging yang Transparan

Skenario ini dapat digunakan untuk repeater dua-radio, ataupun untuk akses point yang bersambungan dengan Ethernet. Kita menggunakan sebuah bridge bukan routing jika kita ingin kedua interface akses point menggunakan subnet yang sama. Ini dapat benar-benar berguna di jaringan-jaringan dengan beberapa akses point di mana kita ingin mempunyai

firewall yang terpusat, dan mungkin server authentication. Karena semua klien menggunakan subnet yang sama, mereka dapat dengan mudah dikelola dengan sebuah server DHCP dan firewall tanpa memerlukan relay DHCP.

Misalnya, anda dapat menyusun sebuah server menggunakan skenario pertama, tetapi menggunakan dua interface Ethernet, satu di sambungkan ke kabel dan satu nirkabel. Satu interface akan menjadi hubungan Internet anda, dan yang lain akan tersambung ke switch. Lalu, sambungkan akses point sebanyak yang anda perlukan ke swith yang sama, set akses point tersebut sebagai bridge transparan, dan setiap orang akan melewati firewall yang sama dan menggunakan server DHCP yang sama.

Kesederhanaan bridge menyebabkan efisiensi biaya. Karena semua klien menggunakan subnet yang sama, trafik broadcast akan diulangi di keseluruhan jaringan. Ini biasanya tidak masalah untuk jaringan kecil, tetapi dengan semakin banyak-nya client, banyak bandwidth nirkabel yang terbuang untuk trafik broadcast.

Konfigurasi awal

Konfigurasi awal untuk akses point bridging sangat mirip dengan akses point masquerading, tanpa persyaratan dnsmasq. Ikuti instruksi konfigurasi awal dari contoh sebelumnya.

Sebagai tambahan, paket **bridge-utils** diperlukan untuk bridging. Paket ini ada untuk distribusi Ubuntu dan distribusi lainnya yang berbasis Debian, serta untuk Fedora Core. Pastikan paket tersebut terinstal dan perintah **brctl** tersedia sebelum melanjutkan.

Mengkonfigurasi Interface

Pada Ubuntu atau Debian interface jaringan dikonfigurasi dengan mengedit file **/etc/network/interfaces.**

Tambahkan sebuah bagian sebagai berikut, tapi ganti nama interfacenya dan IP address-nya sesuai dengan jaringan anda. IP address dan netmask harus sesuai dengan yang ada pada jaringan anda. Contoh ini mengasumsikan anda sedang membuat repeater wireless dengan interface nirkabel, wlan0 dan wlan1. Interface wlan0 akan menjadi klien ke jaringan “office” , dan wlan1 akan membuat jaringan yang dinamakan “repeater”.

Tambahkan yang berikut ke **/etc/network/interfaces**:

```
auto br0
iface br0 inet static
   address 192.168.1.2
   network 192.168.1.0
   netmask 255.255.255.0
```

```
   broadcast 192.168.1.255
   gateway 192.168.1.1
   pre-up ifconfig wlan 0 0.0.0.0 up
   pre-up ifconfig wlan1 0.0.0.0 up
   pre-up iwconfig wlan0 essid "office" mode Managed
   pre-up iwconfig wlan1 essid "repeater" mode Master
   bridge_ports wlan0 wlan1
   post-down ifconfig wlan1 down
   post-down ifconfig wlan0 down
```

Komentari bagian lain mana pun di file yang merujuk pada wlan0 atau wlan1 untuk memastikan bahwa mereka tidak mengganggu konfigurasi kita.

Sintaks untuk mengkonfigurasi bridge melalui file **interfaces** adalah khusus untuk distribusi berbasis Debian, dan detil untuk mengkonfigurasi bridge ditangani oleh beberapa script: **/etc/ network/if-pre-up.d/bridge** dan **/etc/network/if-post-down.d/bridge**. Dokumentasi untuk skrip ini ditemukan di **/usr/share/doc/bridge-utils/**.

Jika script tersebut tidak ada pada distribusi anda (seperti Fedora Core), berikut adalah alternatif setup untuk **/etc/network/interfaces** yang akan menghasilkan hasil yang sama tapi dengan pekerjaan yang lebih banyak:

```
iface br0 inet static
   pre-up ifconfig wlan 0 0.0.0.0 up
   pre-up ifconfig wlan1 0.0.0.0 up
   pre-up iwconfig wlan0 essid "office" mode Managed
   pre-up iwconfig wlan1 essid "repeater" mode Master
   pre-up brctl addbr br0
   pre-up brctl addif br0 wlan0
   pre-up brctl addif br0 wlan1
   post-down ifconfig wlan1 down
   post-down ifconfig wlan0 down
   post-down brctl delif br0 wlan0
   post-down brctl delif br0 wlan1
   post-down brctl delbr br0
```

Mengaktifkan bridge

Setelah bridge ditetapkan sebagai interface, mengaktifkan bridge sangat sederhana melalui perintah:

```
# ifup -v br0
```

"-v" bermaksud memberikan keluaran detil dan akan memberi anda informasi mengenai apa

yang sedang berlangsung.

Di Fedora Core (distribusi non-debian) anda masih perlu memberi interface bridge anda IP address dan menambahkan rute default ke jaringan:

```
#ifconfig br0 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255
#route add default gw 192.168.1.1
```

Anda sekarang dapat menyambung laptop nirkabel ke akses point yang baru ini, dan tersambung dengan Internet (atau setidaknya dengan jaringan LAN anda) melalui PC ini.

Gunakan perintah **brctl** untuk melihat apa yang dilakukan oleh bridge anda:

```
# brctl show br0
```

Skenario 1 & 2 cara yang mudah

Daripada mengkonfigurasi komputer anda sebagai akses point dari nol, anda mungkin ingin untuk menggunakan distribusi Linux yang didedikasikan yang secara khusus didesain untuk tujuan ini. Distribusi ini dapat membuat pekerjaan sesederhana membooting dari CD khusus pada komputer dengan interface nirkabel. Lihat bagian berikut, “Sistem operasi yang cocok dengan nirkabel” untuk informasi lebih lanjut.

Seperti yang anda lihat, sangatlah jelas untuk memberikan layanan akses point dari standar router Linux. Menggunakan Linux memberi anda kemampuan kontrol yang lebih baik pada bagaimana paket diarahkan melalui jaringan anda, dan memiliki fitur yang jauh lebih kompleks daripada akses point komersial biasa.

Sebagai gambaran, anda dapat mulai dengan salah satu dari kedua contoh di atas untuk mengimplementasikan jaringan nirkabel pribadi di mana pengguna diautentikasi dengan menggunakan web browser standar. Memakai captive portal seperti Chillispot, pengguna nirkabel dapat di cek kebenarannya menggunakan database yang sudah ada (misalnya, server domain Windows yang dapat diakses melalui RADIUS). Pengaturan ini dapat memberikan akses istimewa kepada pengguna dalam database, sekaligus menyediakan derajat akses yang sangat terbatas untuk publik.

Aplikasi populer lainnya adalah model komersial pra-bayar. Dalam model ini, pengguna harus membeli voucher sebelum mengakses jaringan. Voucher ini menyediakan password yang berlaku untuk waktu yang terbatas (biasanya satu hari). Ketika voucher berakhir, pengguna harus membeli lagi. Fitur voucher ini hanya tersedia pada peralatan pembuatan jaringan komersial yang relatif mahal, tetapi juga bisa diimplementasikan menggunakan perangkat lunak gratis seperti Chillispot dan phpMyPrePaid. Kita akan melihat lebih banyak lagi tentang teknologi captive portal dan sistem tiket di bagian **Autentikasi** di **Bab 6.**

Sistem operasi yang cocok dengan nirkabel

Ada sejumlah sistem operasi open source yang menyediakan tool yang berguna untuk bekerja dengan jaringan nirkabel. Semua ini ditujukan agar dapat dipakai di PC bekas atau perangkat keras jaringan lainnya (daripada di laptop atau server) dan tune untuk membuat jaringan nirkabel. Beberapa proyek ini termasuk:

- **Freifunk**. Berbasis proyek OpenWRT (*http://openwrt.org/*), Freifunk firmware memungkinkan OLSR berjalan di akses point berbasis MIPS, seperti Linksys WRT54G/WRT54GS/WAP54G, Siemens SE505, dan lainnya. Dengan secara sederhana mem-flash salah satu dari AP dengan Freifunkfirmware, anda dapat secara cepat membuat OLSR mesh yang membentuk diri sendiri. Freifunk sekarang tidak tersedia untuk mesin arsitektur x86. Freifunk diurusi oleh Sven Ola dari kelompok nirkabel Freifunk di Berlin. Anda dapat mendownload firmware dari *http://www.freifunk.net/wiki/FreifunkFirmware.*

- **Pyramid Linux.** Pyramid adalah distribusi Linux untuk penggunaan embedded platform yang berevolusi dari Pebble Linux yang sangat diminati. Linux ini mendukung beberapa card nirkabel yang berbeda, dan mempunyai interface web serderhana untuk mengkonfigurasi interface jaringan, port forwarding, WifiDog, dan OLSR. Pyramid disebarkan dan dikelola oleh Metrix Communication LLC, dan tersedia di *http://pyramid.metrix.net/*.

- **m0n0wall.** Berdasarkan FreeBSD, m0n0wall adalah paket firewall yang lengkat namun sangat kecil yang menyediakan layanan AP. Paket ini dikonfigurasi dari interface web dan keseluruhan konfigurasi sistem disimpan dalam satu file XML. Ukurannya yang sangat kecil (kurang dari 6MB) membuatnya menarik untuk penggunaan di embedded sistem yang sangat kecil. Tujuannya adalah menyediakan firewall yang aman, dan untuk ini itu tidak termasuk tool userspace (Bahkan tidak mungkin untuk masuk ke dalam mesin melalui jaringan). Meskipun ada keterbatasan ini, paket ini adalah pilihan populer untuk pembuat jaringan nirkabel, khusunya mereka dengan latar belakang di FreeBSD. Anda dapat mendownload m0n0wall dari *http://www.m0n0.ch/.*

Semua distribusi ini didesain untuk sesuai dengan mesin dengan penyimpanan terbatas. Jika anda menggunakan flash disk atau hard drive yang sangat besar, anda tentu bisa menginstal OS yang lebih lengkap (seperti Ubuntu atau Debian) dan menggunakan mesin tersebut sebagai router atau akses point. Akan membutuhkan waktu pengembangan yang cukup lama untuk memastikan bahwa semua alat yang diperlukan sudah ada, tanpa menginstal paket yang tidak perlu. Dengan memakai salah satu proyek ini sebagai titik awal untuk membuat node radio, anda akan menyelamatkan cukup banyak waktu dan usaha.

Linksys WRT54G

Salah satu akses point konsumen yang sekarang ini sangat populer di pasaran adalah Linksys WRT54G. Akses point ini memiliki dua konektor antena RP-TNC eksternal, Ethernet switch dengan empat port, dan radio 802.11b/g. Akses point ini dikonfigurasikan lewat interface Web yang sederhana. Walaupun tidak didesain sebagai solusi di luar, titik akses dapat dimasukan dalam kotak plastik dengan harga yang relatif rendah. Pada saat tulisan ini dibuat, WRT54G berharga sekitar $60.

Pada tahun 2003, hacker jaringan menyadari bahwa firmware yang dipaketkan dengan WRT54G adalah sebetulnya versi Linux. Ini menyebabkan perhatian luar biasa di pembuatan firmware yang memperluas kemampuan router Linksys secara signifikan. Beberapa fitur baru ini termasuk dukungan cara radio pelanggan, captive portal, dan jaringan mesh. Beberapa paket firmware alternatif yang populer untuk WRT54G adalah DD-Wrt (*http://www.dd-wrt.com/*), OpenWRT (*http://openwrt.org/)*, Tomat (*http://www.polarcloud.com/tomat*) dan Freifunk (*http://www.freifunk.net/*).

Sayangnya, di akhir musim gugur tahun 2005, Linksys meluncurkan versi 5 WRT54G. Revisi perangkat keras ini menghapuskan beberapa RAM dan flash storage di motherboard, membuatnya sangat sulit untuk menjalankan Linux (dipaketkan dengan VxWorks, sistem yang jauh lebih kecil yang tidak mudah untuk di kustomisasi). Linksys juga meluncurkan WRT54GL, yang pada hakekatnya adalah WRT54G v4 (yang dapat menjalankan Linux) dengan label harga yang lebih besar.

Sejumlah akses point Linksys lainnya juga berjalan di Linux, termasuk WRT54GS dan WAP54G. Sementara yang ini juga mempunyai label harga yang relatif rendah, spesifikasi perangkat keras mungkin berganti kapan saja. Sulit untuk mengetahui perangkat keras mana yang digunakan tanpa membuka kemasan, membuatnya riskan untuk membeli mereka di toko pengecer dan mustahil untuk membelinya online. Walaupun WRT54GL dijamin dapat menjalankan Linux, Linksys sudah menginformasikan bahwa mereka tidak berekspetasi untuk menjual model ini dalam jumlah besar, dan tak jelas berapa lama alat ini dijual.

Untungnya, hackers nirkabel sekarang sudah dapat memasang firmware kustom di WRT54G versi 5 dan 6, dan revisi terakhir juga (v7 dan v8), yang terkenal sulit. Untuk detil dalam mendapatkan firmware alternatif yang terpasang di v5 atau v6 titik akses, lihatlah: *http://www.scorpiontek.org/portal/content/view/27/36/.*

Untuk informasi lebih lanjut mengenai kondisi terkahir hacking router nirkabel Linksys, lihatlah *http://linksysinfo.org/ .*

DD-WRT

Sebuah firmware alternatif yang populer bagi perangkat keras akses point keluarga Linksys

adalah DD-WRT (*http://www.dd-wrt.com/*). Firmware ini memasukkan beberapa fitur berguna, termasuk radio client mode, pengaturan daya pancar, berbagai captive portal, dukungan QoS, dan lebih banyak lagi. Firmware ini memakai konfigurasi berbasis web yang intuitif (tidak terenkrip atau via HTTPS), dan juga menyediakan akses SSH dan akses telnet.

Beberapa versi firmware tersedia dari situs web DD-WRT. Prosedur umum untuk mengupgrade adalah mendownload versi firmware sesuai untuk perangkat keras anda, dan meng-upload-nya via fitur "firmware update" pada router. Detail instalasi spesifik berubah-ubah menurut versi perangkat keras router anda. Disamping perangkat keras Linksys, DD-WRT akan berfungsi di Buffalo, ASUS, La Fonera, dan akses point lainnya.

Untuk instruksi spesifik untuk perangkat keras anda, bacalah pemandu instalasi di wiki DD-WRT di *http://www.dd-wrt.com/wiki/index.php/Instalasi.* Login default untuk instalasi murni DD-WRT adalah "root" dengan password "admin".

Gambar 5.3: Panel kontrol DD-WRT (v23).

Bab 6 Keamanan & Pengawasan

Di jaringan berkabel tradisional, kontrol akses sangat sederhana: Jika seseorang punya akses langsung (secara jasmani) ke komputer atau hub jaringan, mereka bisa memakai (atau menyalahgunakan) sumber daya jaringan itu. Sementara mekanisme software adalah komponen penting dari keamanan jaringan, membatasi akses langsung ke alat-alat jaringan adalah mekanisme kontrol akses yang terbaik. Dengan sederhana, jika semua terminal dan komponen jaringan hanya bisa diakses oleh individu yang terpercaya, jaringan itu mungkin bisa dipercaya.

Peraturan berubah secara signifikan untuk jaringan nirkabel. Sementara jangkauan dari akses point kelihatannya hanya beberapa ratus meter, seorang user dengan antena dengan pengguatan tinggi mungkin dapat memakai jaringan dari jangkauan beberapa blok. Jika seorang user yang tidak sah ketahuan, tidak mungkin bisa secara sederhana “mengikuti jejak kabel” kembali ke lokasi user. Tanpa mentransmit sebuah paket, seorang user bahkan bisa mengambil semua data jaringan ke disk. Data ini nantinya bisa untuk meluncurkan serangan yang lebih hebat terhadap jaringan itu.

Jangan pernah berpikiran kalau gelombang radio secara sederhana “berhenti” di ujung batas rumah anda. Biasanya tak masuk akal untuk percaya pada semua user di jaringan, bahkan di jaringan berkabel. Karyawan yang kesal, user jaringan tidak terdidik, dan kesalahan sederhana dari para user jujur bisa membawa kerusakan yang signifikan ke operasi jaringan. Sebagai arsitek jaringan, sasaran kamu adalah menyediakan komunikasi pribadi di antara user-user sah dari jaringan. Sementara beberapa bagian dari kontrol akses dan pembuktian keaslian diperlukan di jaringan manapun, kamu sudah gagal dalam pekerjaanmu jika user-user sah menemukan bahwa sulit untuk memakai jaringan itu untuk berkomunikasi. Ada perkataan lama bahwa cara satu-satunya untuk benar-benar mengamankan sebuah komputer adalah cabut kabelnya, masukkan ke dalam kotak besi, hancurkan kuncinya, dan kubur semuanya di dalam beton. Biarpun sistem seperti itu bisa betul-betul “aman”, itu tidak berguna untuk tujuan komunikasi. Ketika anda memilih pilihan keamanan untuk jaringan anda, ingatlah bahwa di atas semuanya, jaringan itu ada agar para user bisa berkomunikasi satu sama lain. Keamanan itu penting, tetapi seharusnya tidak menghalangi pemakaian user jaringan.

Keamanan secara Fisik

Ketika sedang menginstalasi sebuah jaringan, kamu sedang membuat sebuah infrastruktur yang diandalkan masyarakat. Tindakan keamanan dilakukan untuk menjamin bahwa jaringan itu bisa dipercaya. Untuk banyak instalasi, kekurangan sering terjadi karena gangguan manusia, biarpun sengaja atau tidak. Jaringan mempunyai komponen fisik, seperti kabel dan

kotak-kotak, yang mudah untuk diganggu. Pada banyak instalasi, masyarakat tidak akan mengerti apa tujuan dari peralatan yang di install, atau keingintahuan membuat mereka melakukan experimen. Mereka mungkin tidak sadar pentingnya sebuah kabel yang tersambung ke sebuah port. Seseorang mungkin mencabut kabel Ethernet sehingga mereka bisa menyambungkan laptop mereka selama 5 menit, atau memindahkan sebuah switch karena menghalangi mereka. Sebuah steker mungkin bisa di lepas dari sebuah power bar karena seseorang membutuhkan wadah itu. Menjamin keamanan langsung dari sebuah instalasi adalah yang terpenting. Tanda-tanda & label-label hanya akan berguna untuk mereka yang bisa mengerti bahasa anda. Menaruh barang-barang di luar jangkauan dan membatasi akses adalah cara terbaik untuk menjamin kesalahan dan perubahan dari luar itu tidak terjadi.

Di negara berkembang, pengikat yang benar atau kotak yang memadai tidak akan gampang dicari. Kamu harusnya bisa mencari listrik yang berfungsi baik. Penutup / kotak mudah dibuat dan penting untuk instalasi. Biasanya lebih ekonomis untuk membayar tukang batu untuk membuat lubang dan install pipa penyalur. Dimana ini akan menjadi pilihan yang mahal di negara berkembang, hal-hal seperti ini bisa terjangkau harganya di negara-negara selatan. PVC bisa dipasang di tembok semen untuk menyalurkan kabel antar ruangan. Ini menghindari keperluan untuk membuat lubang baru setiap kali sebuah kabel perlu di salurkan. Kantong plastik bisa dimasukkan ke pipa penyalur di sekitar kabel untuk isolasi.

Peralatan kecil harus selalu dipasang di dinding dan peralatan besar harus selalu diletakan di atas lemari.

Switch

Switch, hub atau akses point bisa di pasang langsung ke dinding dengan colokan listrik ke dinding. Sangat bagus untuk meletakan peralatan ini setinggi mungkin untuk mengurangi kemungkinan seseorang menyentuh alatnya atau kabelnya.

Kabel

Setidaknya, kabel harus di sembunyikan dan diikatkan. Anda bisa mencari pipa saluran kabel plastik yang bisa dipakai untuk bangunan. Jika anda tidak bisa mencarinya, alat pelengkap kabel bisa dipakukan di dinding untuk mengamankan kabelnya. Ini membuat kabelnya tidak menggantung sehingga gampang di tarik atau dipotong.

Lebih baik lagi untuk mengubur kabelnya, daripada membiarkannya tergantung di lapangan. Kabel yang menggantung bisa dipakai untuk menjemur pakaian, atau diambil dengan tangga, dll. Untuk mencegah hama dan serangga, pakai saluran kabel elektrik plastik. Bayaran tambahan ini akan lebih berguna dibanding dengan usaha yang kita jalankan. Saluran kabel itu harusnya di kubur sedalam 30 cm , atau di bawah titik beku di iklim dingin. Cukup

berharga untuk membeli saluran kabel yang lebih besar daripada yang diperlukan sekarang, agar kabel yang dipakai nanti bisa memakai tempat yang sama. Pikirkan untuk membuat label di kabel yang sudah dikubur dengan tanda ”telepon sebelum menggali” untuk mencegah terputusnya jaringan.

Listrik

Sangat baik untuk mempunyai power bar yang terkunci di lemari. Jika itu tidak mungkin, pasang power bar di bawah meja, atau di dinding dan pakai duct tape (atau gaffer tape, sebuah tape perekat yang kuat) untuk mengamankan plug ke steker, jadi buatlah hal-hal penting ini sulit diubah orang. Jika anda tidak melakukannya, anda mungkin menemukan bahwa kipas atau lampu dicolokkan ke UPS anda; biarpun bagus ada lampu, akan lebih bagus lagi jika server anda tetap berjalan!

Air

Lindungi peralatan anda dari air dan cairan. Ceklah peralatan anda, termasuk UPS anda setidaknya 30 cm di atas tanah, untuk mencegah kerusakan dan kebanjiran. Coba juga untuk memasang atap di atas peralatan anda, jadi air dan cairan tidak jatuh di atasnya. Di iklim basah, penting untuk memberi ventilasi yang memadai pada peralatan anda untuk meyakinkan bahwa cairan bisa dikeringkan. Lemari kecil perlu ventilasi, atau vairan dan panas akan menhancurkan alat-alat anda

Tiang

Peralatan yang dipasang di tiang biasanya aman dari pencuri. Tetapi untuk menjaga peralatan anda aman dari angin sebaiknya anda meyakinkan bahwa teknik pemasangan di atas tower-nya cukup baik.. Mencat peralatan anda dengan warna putih polos atau abu-abu memantulkan sinar matahari dan membuatnya kelihatan membosankan dan tidak menarik. Antena panel biasanya disukai karena mereka halus dan tidak semenarik parabola. Semua instalasi di dinding harus cukup tinggi sehingga perlu tangga untuk mencapainya. Coba cari tempat terang tetapi tidak menyolok untuk meletakan peralatan. Coba hindari antena yang kelihatannya seperti antena televisi, karena benda-benda seperti itu biasanya menarik perhatian pencuri, sedangkan antena wifi akan tidak berguna untuk pencuri biasa.

Ancaman Terhadap Jaringan

Satu perbedaan besar antara Ethernet dan nirkabel bahwa jaringan nirkabel di sebuah ***medium yang dipakai bersama.*** Mereka lebih terlihat seperti hub jaringan lama daripada switch modern, di mana setiap komputer yang terdapat di jaringan bisa “melihat” trafik semua user lain. Untuk mengawasi semua trafik jaringan di sebuah akses point, seseorang tinggal

mengatur ke channel yang sedang dipakai, pasang network card ke monitor mode, dan log semua frame. Data ini mungkin penting untuk pencuri dengar (termasuk data seperti email, voice data, atau log chat online). Ini mungkin juga memberikan password dan data sensitif lainnya, membuatnya mungkin untuk memasuki jaringan itu lebih jauh lagi. Seperti yang akan kita lihat nanti di bab ini, masalah ini bisa di selesaikan dengan enkripsi.

Masalah serius yang lainnya pada jaringan nirkabel adalah bahwa user cukup tidak diketahui (anonim). Biarpun benar bahwa setiap alat wireless memasukkan sebuah alamat MAC unik yang di berikan oleh pembuatnya, alamat ini dapat dirubah dengan software. Bahkan ketika alamat MAC ini diketahui, bisa sangat sulit untuk mengetahui dimana letak user nirkabel berada secara fisik. Efek multi-path, antena penguatan tinggi, dan banyaknya perbedaan karakteristik transmitter radio bisa membuatnya tidak mungkin untuk mengetahui jika user nirkabel jahat sedang duduk di ruangan sebelah atau sedang di apartemen sejauh satu mil.

Biarpun spektrum tidak terlisensi memberikan penghematan biaya yang besar kepada user, dia mempunyai efek samping yang buruk yaitu serangan ***denial of service (DoS)*** yang sederhana. Hanya dengan menyalakan sebuah akses point berkekuatan tinggi, telepon cordless, transmitter video, atau alat-alat 2.4 GHz lainnya, seseorang yang jahat bisa membuat kerusakan besar pada jaringan. Banyak juga alat-alat jaringan yang mudah diserang oleh bentuk-bentuk lain dari serangan denial of service, seperti disassociation flooding dan ARP table overflows.

Berikut adalah beberapa kategori dari individu yang mungkin bisa membuat masalah di jaringan nirkabel:

- ***User yang tidak sengaja:*** Karena makin banyak jaringan nirkabel yang diinstalli di tempat yang padat penduduk, sangat mungkin seorang pengguna laptop tidak sengaja masuk ke jaringan yang salah. Kebanyakan client nirkabel akan dengan mudah memilih jaringan nirkabel manapun ketika jaringan mereka tidak bisa dipakai. User lalu mungkin memakai jaringan seperti biasanya, sama sekali tidak sadar kalau mereka mengirim data sensitif melalui jaringan orang lain. Orang jahat akan mengambil kesempatan seperti ini dengan cara membuat akses point di lokasi strategis, untuk mencoba menarik user dan menangkap data mereka.

  Hal pertama yang dilakukan untuk mencegah masalah ini adalah dengan memberi pengetahuan pada user anda, dan memberitahu pentingnya menyambung hanya pada jaringan yang diketahui dan dipercaya.Kebanyakan client nirkabel bisa di atur untuk hanya menyambung pada jaringan yang dipercaya, atau untuk meminta izin sebelum bergabung dengan network baru. Seperti yang akan kita lihat nanti di bab ini, user bisa menyambung dengan aman ke jaringan publik yang terbuka dengan memakai enkripsi yang kuat.

- ***War driver.*** Fenomena “war driving” mengambil namanya dari film hacker 1983 yang populer, “War Games”. War driver tertarik dengan mencari lokasi fisik dari jaringan nirkabel. Mereka biasanya bepergian dengan membawa laptop, GPS, dan antena

omnidirectional, mereka log nama dan lokasi dari semua jaringan yang mereka temukan. Log-log ini lalu disatukan dengan log dari para war driver lain, lalu dirubah menjadi peta grafis yang menggambarkan “peta” nirkabel di suatu kota.

Kebanyakan war driver biasanya tidak membahayakan jaringan, tetapi data yang mereka koleksi mungkin menarik untuk cracker jaringan. Sebagai contoh, jelas kalau akses point yang tidak dilindungi yang terdeteksi oleh war driver terdapat di dalam bangunan sensitif, seperti kantor pemerintah atau perusahaan. Orang jahat bisa menggunakan informasi ini mengakses jaringan disana secara ilegal. AP seperti itu harusnya memang tidak pernah dipasang, tetapi war driver membuat masalah ini menjadi lebih mendesak. Seperti yang nanti akan kita lihat di bab ini, war driver yang memakai program populer NetStumbler bisa di deteksi dengan memakai program seperti Kismet. Untuk lebih jelas tentang war driver, lihat site seperti *http://www.wifimaps.com/, http://www.nodedb.com/,* atau *http://www.netstumbler.com/* .

- ***Rogue akses point.*** Ada dua kelas umum rogue akses points: yang di install secara salah oleh user yang sah, dan yang di install oleh orang jahat yang bermaksud untuk mengkoleksi data atau merusak jaringan. Di kasus yang paling sederhana, user yang sah mungkin ingin mempunyai cakupan nirkabel yang lebih baik di kantor mereka, atau mereka mungkin menemukan restriksi keamanan di jaringan nirkabel perusahaan terlalu sulit untuk diikuti. Dengan menginstall sebuah akses point konsumen yang murah tanpa izin, user itu membuka seluruh jaringan itu untuk serangan dari dalam. Biarpun bisa melakukan scan untuk mengetahui akses point tidak sah, membuat peraturan yang jelas yang melarang mereka sangat penting.

  Kelas kedua dari rogue akses point bisa sangat sulit untuk diurus. Dengan menginstall AP berkekuatan tinggi yang memakai ESSID yang sama dengan jaringan yang ada, orang yang jahat bisa menipu orang untuk memakai peralatan mereka, dan menyimpan atau bahkan memanipulasi semua data yang melewatinya. Jika user anda terlatih untuk memakai enkripsi kuat, masalah ini berkurang secara signifikan.

- ***Eavesdropper.*** Seperti yang dibicarakan sebelumnya Eavesdropper (pencuri dengar) adalah masalah yang sangat susah dihadapi di jaringan nirkabel. Dengan memakai alat pengawas pasif (seperti Kismet), seorang eavesdropper bisa menyimpan semua data jaringan dari jarak yang jauh, tanpa harus membuat kehadiran mereka diketahui. Data yang di enkripsi dengan buruk dengan sederhana bisa di simpan lalu di crack kemudian, sedangkan data yang tak di enkripsi dengan mudah bisa langsung dibaca secara realtime.

  Jika anda mempunyai kesuitan meyakinkan orang lain tentang masalah ini, anda mungkin mau mempertunjukkan alat seperti Etherpeg (http://www.etherpeg.org/) atau Driftnet (http://www.ex-parrot.com/~chris/driftnet/). Alat ini memperlihatkan jaringan nirkabel dalam bentuk data grafis, seperti GIF dan JPEG. Sementara user lain sedang melihat-lihat Internet, alat ini dengan sederhana menunjukkan semua graphics yang ditemukan di graphical collage. Saya sering memakai alat seperti ini sebagai

demonstrasi kalau memberi kuliah tentang keamanan nirkabel. Biarpun anda bisa memberi tahu seorang user bahwa email mereka rentan tanpa enkripsi, tidak ada yang memberikan pesan setegas memperlihatkan kepada mereka gambar yang sedang mereka lihat di web browser mereka. Lagi pula, biarpun ini tidak bisa dicegah sepenuhnya, penggunaan aplikasi memadai yang enkripsinya kuat akan menghalangi Eavesdropper.

Perkenalan ini dimaksudkan untuk memberi gambaran kepada anda masalah yang akan anda hadapi ketika mendesain jaringan nirkabel. Nanti di bab ini, kami akan meperlihatkan alat dan teknik yang akan menolong anda untuk mengurangi masalah-masalah ini

Authentikasi

Sebelum diberi akses untuk ke sumber daya jaringan, user sebaiknya ***diauthentikasi*** terlebih dahulu. Di dunia ideal, setiap user nirkabel akan mempunyai identifier yang unik, tak bisa diubah, dan tidak bisa ditirukan oleh user lain. Ini ternyata masalah yang sangat sulit untuk diselesaikan di dunia nyata.

Fitur yang terdekat dengan identifier unik adalah alamat MAC. Ini adalah angka 48-bit yang diberikan pada setiap alat nirkabel dan Ethernet oleh pembuat alat. Dengan menjalankan ***mac filtering*** di akses point kami, kami bisa mengauthentikasi user berdasarkan dari alamat MAC mereka. Dengan fitur ini, akses point menyimpan internal table berisi alamat MAC yang sudah diakui. Kalau seorang user nirkabel berusaha untuk berrelasi ke akses point, alamat MAC klien harus ada di daftar yang diakui, atau relasi akan ditolak. Sebagai alternatif, AP mungkin menyimpan table berisi alamat MAC yang dikenal “buruk”, dan mengizinkan semua alat yang tidak ada di daftar untuk berelasi.

Sayangnya, ini bukan mekanisme keamanan yang ideal. Mempertahankan table MAC di setiap alat sangat tidak praktis, perlu mencatat semua alamat MAC client dan di upload ke AP. Lebih parah lagi, alamat MAC sering bisa diganti dengan software. Dengan memperhatikan alamat MAC di penggunaan pada jaringan nirkabel, seorang penyerang gigih bisa ***spoof / menipu (menirukan)*** alamat MAC yang diakui dan berhasil relasi kepada AP. Biarpun MAC filter akan mencegah user yang tak sengaja dan kebanyakan pengguna untuk mengakses jaringan, MAC filtering sendiri tidak bisa mencegah serangan dari penyerang yang gigih.

MAC filter berguna untuk membatasi akses untuk sementara dari client nakal. Misalnya, jika sebuah laptop mempunyai virus yang mengirim banyak spam atau trafik lain, alamat MAC-nya dapat ditambahkan ke table saringan untuk menghentikan trafik. Ini akan memberikan anda waktu untuk menemukan user itu dan membetulkan masalahnya.

Fitur authentikasi populer lain dari nirkabel adalah yang dinamakan ***jaringan tertutup.*** Di jaringan umum, AP akan membroadcast ESSID mereka banyak kali perdetik, membolehkan klien nirkabel (dan juga alat seperti NetStumbler) untuk menemukan jaringan dan

menunjukan keberadaannya ke user. Di jaringan tertutup, AP tidak memberitahu ESSID, dan user harus mengetahui nama lengkap jaringan terlebih dahulu sebelum AP akan membolehkan relasi. Ini mencegah pemakai biasa untuk menemukan jaringan dan memilihnya di client nirkabel mereka.

Ada sejumlah kekurangan dari fitur ini. Memaksa pemakai untuk mengetik ESSID penuh sebelum bersambungan dengan jaringan biasanya banyak kesalahan dan sering menyebabkan menelpon bantuan dan pengaduan. Karena jaringan tidak jelas hadir di tool site survey seperti NetStumbler, ini bisa mencegah jaringan-jaringan anda terlihat di peta Wardriver. Tetapi menyatakan juga bahwa pembuat jaringan lainnya tidak bisa dengan mudah menemukan jaringan, dan mereka tidak tahu bahwa anda sudah memakai suatu kanal. Tetangga yang bersungguh-sungguh mungkin melakukan site survey, memastikan tidak ada jaringan didekatnya, dan memasang jaringan mereka sendiri di atas saluran sama dengan yang sedang anda gunakan. Ini akan menyebabkan masalah gangguan bagi baik anda maupun tetangga anda.

Menggunakan jaringan tertutup pada akhirnya akan menambah sedikit keamanan jaringan secara keseluruhan. Dengan memakai alat mengamat pasif (seperti Kismet), seorang user trampil bisa mengetahui frame yang dikirim dari klien sah anda ke AP. Frame ini perlu berisi nama jaringan itu. Seorang pemakai jahat kemudian bisa memakai nama ini untuk berelasi ke akses point, seperti seorang pemakai normal.

Enkripsi mungkin adalah alat terbaik kita yang ada untuk mengauthentikasi user nirkabel. Melalui enkripsi kuat, kita secara unik bisa mengenali seorang user dengan cara yang sangat sulit untuk di spoof, dan mempergunakan identitas itu untuk menentukan akses jaringan lebih lanjut. Enkripsi juga mempunyai keuntungan menambahkan selapis privasi dengan mencegah Eavesdropper melihat dengan mudah trafik jaringan.

Metode enkripsi yang paling banyak dipakai adalah enkripsi ***WEP.*** WEP adalah singkatan dari ***Wired Equivalent Privacy***, dan disokong oleh semua peralatan 802.11a/b/g. WEP mempergunakan kunci shared 40 bit untuk enkripsi data antara akses point dan klien. Kunci harus dimasukkan di AP dan pada masing-masing klien. Dengan memakai WEP, klien nirkabel tidak bisa menghubungkan dengan AP sampai mereka memakai kunci yang benar. Seorang Eavesdropper yang mendengarkan jaringan yang sudah memakai WEP masih akan melihat trafik dan alamat MAC, tetapi muatan data masing-masing paket di enkripsi. Ini menyediakan mekanisme authetikasi yang cukup baik sedangkan juga menambahkan sedikit privasi ke jaringan.

WEP pasti bukan solusi enkripsi terkuat yang ada. Untuk satu hal, kunci WEP di pakai bersama-sama oleh semua pemakai. Jika kunci ketahuan (seperti, jika seorang user memberitahu kepada seorang teman apa passwordnya, atau jika seorang pegawai dilepaskan) lalu mengganti password bisa sulit, karena semua AP dan alat client perlu diganti. Ini juga berarti pemakai sah jaringan masih bisa menguping pada trafik masing-masing , karena semuanya mengetahui kunci yang dipakai bersama-sama.

Kuncinya itu sendiri sering dipilih secara buruk, membuat penge-crack-an offline bisa dilakukan. Lebih buruknya lagi, implementasiWEP dipecah ke banyak akses point, membuatnya lebih mudah lagi untuk meng-crack beberapa jaringan. Biarpun pembuat sudah melaksanakan sejumlah extensi pada WEP (seperti kunci yang lebih panjang dan fast rotation scheme), extensi ini bukan bagian dari standar, dan secara umum tidak akan interoperate di antara perlengkapan dari pembuat yang berbeda. Dengan upgrade ke firmware yang paling baru untuk semua alat nirkabel, anda bisa mencegah beberapa serangan awal yang ditemukan di WEP.

WEP masih bisa menjadi alat authentikasi yang berguna. Mengasumsikan user anda bisa dipercaya untuk tidak menyerahkan password, anda bisa cukup yakin bahwa klien nirkabel anda sah. Biarpun menge-crack WEP itu mungkin, itu bukan ketrampilan kebanyakan user. WEP cukup berguna untuk mengamankan sambungan point-to-point jarak jauh, bahkan di jaringan-jaringan yang umumnya terbuka. Dengan memakai WEP di sambungan tersebut, anda mengurangi niat orang untuk berasosiasi dengan sambungan anda, dan mereka akan cenderung menggunakan AP yang lain. Pikirkan WEP sebagai tanda “jangan masuk” untuk jaringan anda. Siapa saja yang mendeteksi jaringan akan melihat bahwa jaringan tersebut menggunakan kunci, membuatnya jelas bahwa sambungan tersebut bukan untuk mereka.

Kekuatan paling hebat dari WEP adalah interoperability. Untuk mengikuti standar 802.11, semua alat nirkabel harus mendukung WEP yang paling dasar. Biarpun bukan metode paling kuat yang ada, tentu dia adalah fitur enkripsi yang paling umum untuk digunakan. Kita akan melihat teknik enkripsi tingkat lanjut lainnya nanti di bab ini.

Untuk lebih detil tentang enkripsi WEP, silahkan lihat alamat berikut ini:

- 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

Protokol authentikasi lapisan data-link lain adalah ***Wi-Fi Protected Access***, atau ***WPA***. WPA diciptakan khusus untuk mengatasi masalah / kekurangan WEP. WPA menyediakan pola enkripsi yang lebih kuat secara signifikan, dan bisa memakai kunci private yang dipakai bersama, kunci unik yang dialokasikan pada masing-masing user, atau bahkan sertifikat SSL untuk authentikasi baik klien maupun akses point. Keabsahan authentikasi diperiksa menggunakan protokol 802.1X, yang bisa berunding dengan database pihak ketiga seperti RADIUS. Melalui penggunaan ***Temporal Key Integrity Protocol (TKIP),*** kunci bisa dirotasi dengan cepat setelah selang waktu tertentu, sehingga sangat mengurangi kemungkinan sebuah sesi di crack. Secara keseluruhan, WPA menyediakan authentikasi dan privasi lebih baik secara signifikan daripada WEP standar.

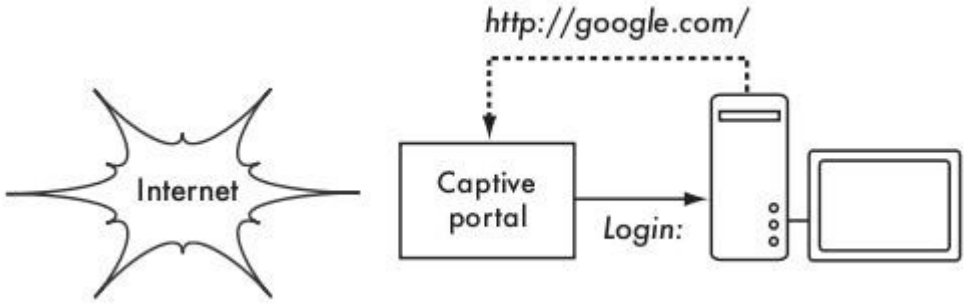
WPA memerlukan hardware akses point yang cukup baru dan firmware terbaru pada semua klien nirkabel, serta sejumlah besar konfigurasi. Jika anda sedang memasang jaringan di tempat di mana anda menguasai seluruh hardware, WPA menjadi sangat ideal. Dengan mengauthentikasi baik klien maupun AP, dia memecahkan masalah rogue akses point dan

menyediakan banyak keuntungan dibandingkan WEP. Tapi di kebanyakan jaringan yang menggunakan campuran hardware tua dan pengetahuan pengguna yang terbatas, pemasangan WPA bisa menjadi mimpi buruk. Oleh karenanya banyak lokasi tetap memakai WEP, jika ingin menggunakan enkripsi.

Captive portal

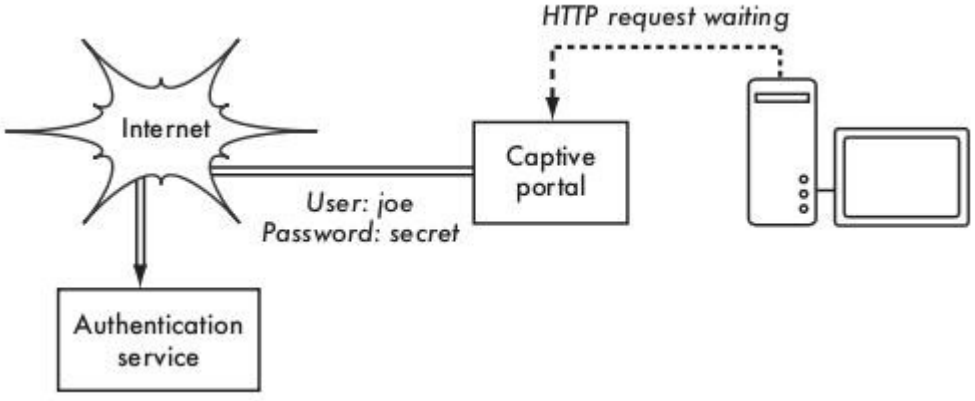
Alat authentikasi yang biasa dipakai di jaringan nirkabel adalah ***captive portal.*** Captive portal memakai standar web browser untuk memberi seorang user nirkabel kesempatan untuk mengauthentikasi dirinya, biasanya berupa username & password. Captive portal juga dapat memberi informasi (seperti Kebijakan Penggunaan Jaringan yang Dapat di Terima / Acceptable Use Policy) kepada pemakai sebelum memberi akses lebih lanjut. Dengan memakai web browser, captive portal dapat bekerja dengan semua laptop dan sistem operasi. Captive portal biasanya dipakai di jaringan terbuka yang tak punya metode authentikasi lain (seperti WEP atau MAC filter).

Untuk memulai, seorang user nirkabel membuka laptop mereka dan memilih jaringan. Komputer mereka akan meminta sewa DHCP, yang kemudian akan diberi. Mereka kemudian memakai web browser untuk pergi ke situs mana pun di Internet.



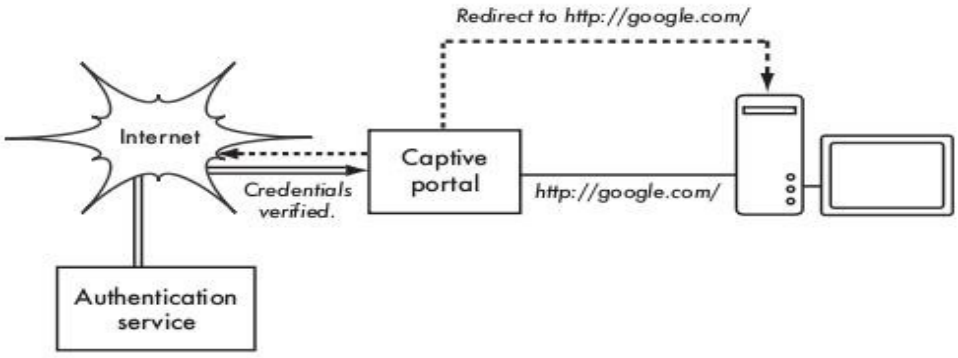
Gambar 6.1: User meminta sebuah halaman web dan diarahkan.

Daripada menerima halaman yang diminta, user diperlihatkan layar login. Halaman ini bisa mengharuskan user untuk memasukkan username dan password, kemudian klik tombol “login”, ketik nomor voucher yang sudah dibayar lebih dulu, atau masukkan surat kepercayaan lain diperlukan oleh administrator jaringan. User memasukan keabsahan mereka, yang diperiksa oleh akses point atau server lain di jaringan. Semua akses jaringan lain di blok sampai authentikasi telah dicek.



Gambar 6.2: Keabsahan user dicek sebelum akses jaringan lebih lanjut diberikan. Server authentikasi bisa dilakukan di akses point, atau mesin lain di jaringan lokal, atau server di mana pun di Internet.

Setelah di authentikasi, user diizinkan untuk mengakses sumber daya jaringan, dan biasanya dialihkan penggunaannya ke situs yang semula mereka minta.



Gambar 6.3: Sesudah diauthentikasi, user diizinkan akses ke seluruh jaringan.

Captive portal tidak menyediakan enkripsi untuk user nirkabel, malahan mengandalkan alamat MAC dan IP dari klien sebagai identifier unik. Karena ini tidak perlu terlalu aman, banyak implementasi akan memerlukan user untuk mengauthentikasi kembali secara periodik. Ini sering dilakukan secara otomatis dengan minimizing pop-up window pada browser ketika user pertama kali login.

Karena mereka tidak menyediakan enkripsi kuat, captive portal bukan pilihan bagus untuk jaringan-jaringan yang perlu diamankan yang hanya dapat di akses oleh user yang dapat di percaya. Teknik ini lebih cocok untuk kafe, hotel, dan lokasi akses umum lain di mana user umum akan berdatangan dan akan menggunakan jaringan.

Di jaringan publik atau semi-publik, teknik enkripsi seperti WEP dan WPA tidak berguna. Tidak ada cara untuk menyebarkan publik atau kunci yang dipakai bersama kepada masyarakat tanpa membahayakan keamanan dari kunci tersebut. Pada konfigurasi ini, aplikasi sederhana seperti captive portal menyediakan tingkat layanan antara betul-betul terbuka dan betul-betul tertutup.

Projek hotspot yang populer

- Chillispot (*http://www.chillispot.info/*). Chillispot adalah captive portal yang didesain untuk authentikasi terhadap database keabsahan user yang sudah ada, seperti RADUIS. Digabung dengan aplikasi phpMyPrePaid, authentikasi berdasarkan voucher yang sudah dibayar lebih dulu bisa dilaksanakan dengan sangat mudah. Anda bisa mendownload phpMyPrePaid dari *http://sourceforge.net/projects/phpmyprepaid/.*

- WiFi Dog (*http://www.wifidog.org/*). WiFi Dog menyediakan paket authentikasi captive portal yang sangat lengkap untuk ruang yang sempit (biasanya di bawah 30kb). Dari perspektif user, dia tidak memerlukan pop-up atau sokongan javascript, memperbolehkannya mengerjakan jenis alat nirkabel yang lebih luas.

- m0n0wall (*http://m0n0.ch/wall/*). M0n0wall adalah sebuah sistem operasi embedded yang berbasis pada FreeBSD. Termasuk di dalamnya adalah captive portal dengan dukungan untuk RADIUS, serta web server PHP.

- NoCatSplash (*http://nocat.net/download/NoCatSplash/*) memberikan splash page yang dapat diubah-ubah kepada user anda, mengharuskan mereka untuk klik tombol “login” sebelum memakai jaringan. Ini berguna untuk mengenali operator jaringan dan menampilkan peraturan untuk akses jaringan. Dia menyediakan solusi yang sangat mudah di situasi di mana anda perlu memberi user jaringan terbuka dengan informasi dan Acceptable Use Policy.

Privasi

Kebanyakan user dengan tak sadar bahwa email pribadi mereka, percakapan chat, dan malah password sering dikirim “dengan sangat jelas” ke puluhan jaringan yang tak dipercaya sebelum tiba di tujuan akhir mereka di Internet. Tetapi sesalah apapun mereka, user biasanya masih berharap adanya privasi di jaringan.

Privasi bisa tercapai, bahkan pada jaringan yang tak dipercaya seperti akses point umum dan Internet. Satu-satunya metode efektif yang terbukti dapat melindungi privasi adalah penggunaan enkripsi kuat.

Teknik enkripsi seperti WEP dan WPA mencoba mengatasi persoalan privasi di lapisan dua, lapisan data-link. Ini melindungi melawan Eavesdropper yang menguping sambungan nirkabel, tetapi perlindungan ini berakhir di akses point. Jika pelanggan pengguna nirkabel memakai protokol yang tidak aman (seperti POP atau SMTP sederhana untuk menerima dan mengirim email), lalu user diluar AP masih bisa log sesi itu dan melihat data peka. Seperti yang dikatakan sebelumnya, WEP juga menderita dari fakta bahwa dia memakai kunci private yang dipakai bersama. Ini berarti user nirkabel yang sah bisa menguping satu sama lain, karena semuanya mengetahui kuncinya.

Dengan memakai enkripsi sampai akhir sambungan yang jauh, user bisa mengelak seluruh

masalah ini. Teknik ini bekerja baik bahkan di jaringan-jaringan umum yang tak dipercaya, di mana Eavesdropper sedang mendengarkan dan mungkin memanipulasi data yang datang dari akses point.

Untuk menjamin privasi data, enkripsi end-to-end yang baik sebaiknya menyediakan fitur berikut:

- ***Verifikasi authentikasi dari remote end.*** User sebaiknya dapat tahu tanpa ragu-ragu kepada siapa dia berbicara di ujung lain. Tanpa authentikasi, seorang user bisa dapat data sensitif kepada siapa saja yang menyebutkan bahwa dia adalah layanan yang sah.
- ***Metode enkripsi kuat.*** Algoritma enkripsi sebaiknya kuat terhadap serangan di masyarakat, dan tidak dengan mudah di pecahkan oleh pihak ketiga. Tidak ada keamanan di ketidakjelasan, dan enkripsi akan lebih kuat lagi jika algoritma dikenal secara luas dan sudah di review oleh banyak orang. Algoritma yang baik dengan kunci yang panjang dan terlindungi dapat menyediakan enkripsi yang tak mungkin di bongkar oleh siapapun pada generasi kita dengan memakai teknologi sekarang.
- ***Public key cryptography.***. Biarpun bukan syarat mutlak untuk enkripsi end-to-end, penggunaan public key cryptography bukan shared key (kunci bersama) dapat menjamin bahwa data seorang individu tetap pribadi (aman), sekalipun kunci dari pemakai lain telah jebol. Hal ini memecahkan masalah penyebaran kunci kepada pemakai melalui jaringan yang tidak dipercayai.
- ***Data encapsulation.*** Mekanisme enkripsi end-to-end yang baik akan berusaha melindungi sebanyak mungkin data. Mulai dari meng-enkripsi satu transaksi email sampai encapsulation seluruh trafik IP, termasuk DNS lookups dan protokol pendukung lain. Beberapa tool enkripsi yang sederhana hanya menyediakan saluran aman yang bisa dipakai oleh aplikasi lain. Ini memungkinkan user memakai program apapun yang mereka suka dan masih memperoleh perlindungan enkripsi yang kuat, sekalipun program itu sendiri tidak menyokongnya.

Undang-undang tentang penggunaan enkripsi berbeda-beda dari suatu negara ke negara lain. Beberapa negara menganggap enkripsi sebagai senjata, dan mungkin memerlukan surat izin, dibutuhkan penjaga kunci private, bahkan atau malah melarang penggunaannya secara keseluruhan. Sebelum mengoperasikan apapun yang melibatkan enkripsi, pastikan bahwa penggunaan teknologi ini diizinkan di negara anda.

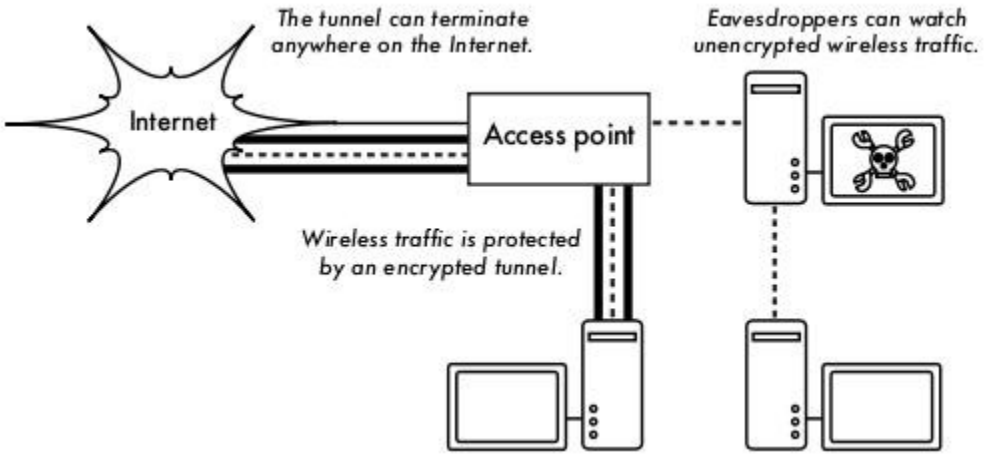
Di bagian-bagian berikut, kita akan melihat beberapa tool khusus yang bisa menyediakan perlindungan yang baik untuk data user anda.

SSL

Teknologi enkripsi yang banyak digunakan adalah ***Secure Sockets Layer***, biasanya dikenal sebagai ***SSL***. Dipakai di semua web browser, SSL memakai public key cryptography dan

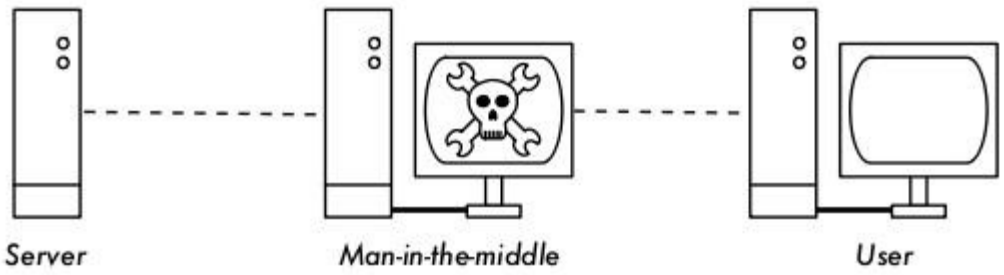
public key infrastructure (PKI) yang dipercaya untuk menjamin komunikasi data di web. Setiap kali anda berkunjung jaringan URL yang mulai dengan http, anda sedang memakai SSL.

Implementasi SSL di dalam web browser termasuk sekumpulan sertifikat dari sumber yang dipercaya, yang dikenal sebagai ***certificate authorities (CA)***. Sertifikat ini adalah kunci cryptographic yang dipergunakan untuk mencek keaslian situs web. Kalau anda melihat-lihat ke situs web yang memakai SSL, browser dan server terlebih dulu bertukaran sertifikat. Browser mencek bahwa sertifikat yang disediakan oleh server sama dengan hostname DNS-nya, bahwa dia belum expire, dan bahwa ditandatangani oleh certificate authorities terpercaya. Server dapat juga mencek identitas sertifikat browser. Jika surat keterangan diakui, browser dan server akan menegosiasikan kunci sesi master menggunakan sertifikat yang sudah dipertukarkan sebelumnya untuk melindunginya. Kunci itu kemudian dipergunakan untuk meng-enkripsi semua komunikasi sampai browser selesai berkomunikasi. Enkapsulasi data seperti ini dikenal sebagai ***tunnel.***



Gambar 6.4: Eavesdropper harus membuka enkripsi yang kuat untuk mengamati trafik di tunnel yang sudah di enkripsi. Percakapan di tunnel identik dengan percakapan yang tidak dienkripsi.

Penggunaan sertifikat dengan PKI tak hanya melindungi komunikasi dari Eavesdropper, tetapi juga mencegah apa yang dinamakan serangan ***man-in-the-middle (MITM).*** Di serangan man-in-the-middle, seorang user jahat intersep / menangkap semua komunikasi di antara browser dan server. Dengan memberikan sertifikat palsu baik ke browser maupun server, pemakai jahat bisa melakukan dua sesi yang dienkripsi sekaligus. Karena user jahat mengetahui rahasia kedua sambungan, sengat mudah untuk mengamati dan manipulasi data yang diberikan di antara server dan browser.



Gambar 6.5: Man-in-the-middle secara efektif menguasai segalanya yang di lihat user, dan dapat merekam dan memanipulasi semua trafik. Tanpa infrastruktur kunci publik untuk mencek keaslian kunci, enkripsi kuat saja tidak bisa melindungi terhadap serangan seperti ini.

Penggunaan PKI sangat baik untuk mencegah serangan seperti ini. Agar serangan berhasil, user jahat harus memberikan sertifikat kepada klien yang ditandatangani oleh certificate authorities terpercaya. Kecuali kalau CA sudah dijebol (walaupun sangat tak mungkin) atau user ditipu agar mau menerima sertifikat palsu, maka serangan seperti itu tidak mungkin. Oleh karenanya penting bagi user untuk tahu bahwa mengabaikan peringatan mengenai sertifikat yang sudah expire atau tidak layak sangat berbahaya, khususnya jika memakai jaringan nirkabel. Dengan mengklik tombol “ignore” saat di minta oleh browser mereka, user membuka diri mereka terhadap banyak kemungkinan serangan.

SSL tak hanya dipakai untuk web browsing. Protokol email yang tidak aman seperti IMAP, POP, dan SMTP dapat di amankan dengan membungkus mereka dengan tunnel SSL. Kebanyakan klien email modern mendukung IMAPS dan POPS (IMAP dan POP aman) dan juga SMTP yang dilindungi SSL/TLS. Jika server email anda tidak menyediakan bantuan SSL, anda masih bisa mendapatkannya dengan SSL memakai paket seperti Stunnel (http://www.stunnel.org/). SSL bisa dipergunakan untuk secara efektif untuk menjamin hampir semua servis mana pun yang jalan di TCP.

SSH

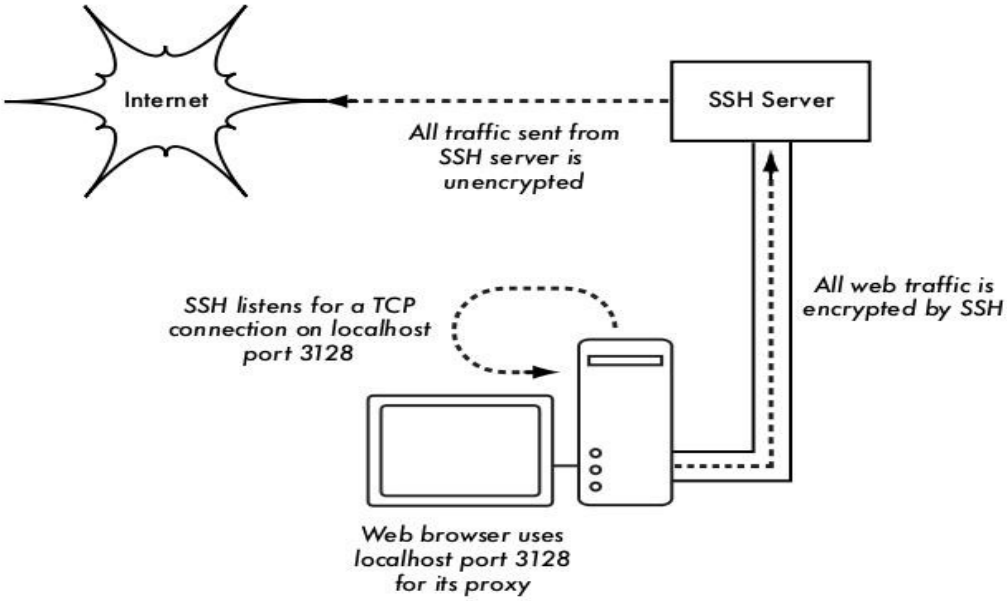
Kebanyakan orang berpikir SSH adalah pengganti **telnet** yang aman, seperti **scp** dan **sftp** adalah aplikasi yang sama dengan **rcp** dan **ftp** tapi lebih aman. SSH melakukan lebih dari hanya sekedar meng-enkripsi remote shell. Seperti SSL, dia menggunakan public key cryptography yang kuat untuk mencek server dan meng-enkripsi data. Daripada menggunakan PKI, SSH memakai cache dari key fingerprint yang diperiksa sebelum koneksi diizinkan. SSH dapat memakai password, public key, atau metode lain untuk authentikasi pemakai.

Kebanyakan orang tidak tahu bahwa SSH juga bisa bertindak sebagai tunnel pengenkripsi, bahkan proxy web yang berenkripsi. Dengan terlebih dulu membuat koneksi SSH ke lokasi terpercaya di dekat (atau langsung ke) remote server , protokol yang tidak aman dapat

dilindungi dari eavesdropper dan penyerangan.

Biarpun teknik ini mungkin sedikit lebih maju untuk kebanyakan user, arsitek jaringan dapat mempergunakan SSH untuk meng-enkripsi trafik melalui sambungan yang tak terpercaya, seperti sambungan nirkabel point-to-point. Karena tool tersedia secara leluasa dan berjalan di atas TCP standar, user yang mengetahui tekniknya dapat menjalankan SSH sendiri, menyediakan enkripsi end-to-end mereka tanpa intervensi administrator.

OpenSSH (*http://openssh.org/*) mungkin adalah implementasi yang paling populer di platform seperti UNIX. Implementasi gratis seperti Putty (*http://www.putty.nl/*) dan WinSCP (*http://winscp.net/*) tersedia di Windows. OpenSSH juga bisa dipakai di Windows di bawah paket Cygwin (*http://www.cygwin.com/*). Contoh berikut ini berasumsi bahwa anda memakai versi OpenSSH yang terbaru.



Gambar 6.6: Tunnel SSH melindungi trafik web sampai kepada server SSH.

Untuk membangin tunnel yang ter-enkripsi dari sebuah port di mesin lokal ke port di mesin remote, gunakan switch -L. Misalnya, jika anda mau menyampaikan trafik web proxy melalui sambungan yang sudah ter-enkripsi ke server squid di squid.example.net. Forward port 3128 (port proxy standar) memakai perintah berikut:

```
ssh -fN -g -L3128:squid.example.net:3128 squid.example.net
```

Switch -fN memerintahkan ssh untuk masuk ke background sesudah tersambung. Switch -g mengijinkan user lain di segmen lokal anda untuk menyambung dengan mesin lokal dan memakainya untuk untuk enkripsi melalui sambungan yang tak terpercaya. OpenSSH akan memakai public key untuk authentikasi jika anda mensetupnya, atau dia akan meminta untuk memasukan password anda di remote side. Anda kemudian bisa mengatur web browser

anda untuk menyambung ke localhost port 3128 sebagai layanan web proxy nya. Semua trafik web kemudian akan di enkripsi sebelum dikirim ke remote side.

SSH juga dapat bertindak sebagai proxy SOCKS4 atau SOCKS5 dinamis. Ini memungkinkan anda membuat web browser yang mengenkripsi, tanpa perlu menggunakan squid. Perhatikan bahwa ini bukan proxy caching; dia hanya meng-enkripsi semua trafik.

```
ssh -fN -D 8080 remote.example.net
```

Atur web browser anda untuk memakai SOCKS4 or SOCKS5 di local port 8080,
dan anda dapat langsung memakainya.

SSH bisa meng-enkripsi data di TCP port manapun, termasuk port yang dipakai untuk email. Ia bahkan bisa meng-kompres data sepanjang jalan, yang bisa mengurangi latensi di sambungan yang berkapasitas rendah.

```
ssh -fNCg -L110:localhost:110 -L25:localhost:25 mailhost.example.net
```

Switch -C mengaktifkan kompresi. Anda bisa menambahkan banyak aturan port forwarding yang anda mau dengan menggunakan switch -L berkali-kali. Perhatikan bahwa untuk mengikat ke port lokal dibawah 1024, anda harus mempunyai hak root di mesin lokal.

Itu hanya sedikit contoh fleksibilitas SSH. Dengan mengimplementasikan public key dan menggunakan agen ssh forwarding, anda dapat mengautomatisasi pembuatan tunnel yang terenkripsi sepanjang jaringan nirkabel anda, dan melindungi komunikasi anda dengan enkripsi dan authentikasi yang kuat.

OpenVPN

OpenVPN adalah sebuah implementasi VPN open source yang menggunakan enkripsi SSL. Implementasi klien OpenVPN tersedia untuk banyak sistem operasi, termasuk Linux, Windows 2000/XP atau yang lebih tinggi, OpenBSD, FreeBSD, NetBSD, Mac OS X, dan Solaris. Pada sebuah VPN, dia akan meng-enkapsulasi semua trafik (termasuk protokol DNS dan protokol-protokol lain) di tunnel yang terenkripsi, jadi bukan hanya satu port TCP saja. Kebanyakan orang merasa hal itu sangat memudahkan untuk dimengerti dan diatur daripada IPSEC.

OpenVPN juga mempunyai beberapa kerugian, seperti latensi yang cukup tinggi. Beberapa latensi tak terelakan karena semua enkripsi/dekripsi dilakukan di aplikasi user, dengan memakai komputer yang relatif baru kedua ujung tunnel dapat mengurangi latensi ini. Biarpun bisa memakai shared key yang tradisional, OpenVPN akan lebih bercahaya jika digunakan bersama sertifikat SSL dan certificate authority. OpenVPN mempunyai banyak keuntungan yang membuatkannya pilihan yang baik untuk menyediakan keamanan end-to-end.

Beberapa alasan tersebut adalah:

- Dia didasarkan pada protokol enkripsi yang handal dan sudah terbukti (SSL dan RSA).
- Dia relatif mudah untuk di konfigurasi..
- Dia bekerja di banyak platform yang berbeda.
- Dia didokumentasikan dengan baik.
- Dia gratis dan open source.

OpenVPN perlu menyambung sebuah port TCP atau UDP di remote side. Setelah tersambungkan, dia akan mengenkapsulasi semua data ke Networking layer, atau bahkan sampai ke lapisan Data-Link, jika anda membutuhkan solusi yang demikian. Anda bisa menggunakannya untuk membuat sambungan VPN yang handal di antara mesin-mesin, atau dengan sederhana gunakan itu untuk menghubungkan router jaringan melalui jaringan-jaringan nirkabel yang tidak terpercaya.

Teknologi VPN adalah bidang kompleks, dan diluar scope bagian ini untuk merincinya. Penting untuk mengerti bagaimana VPN bisa masuk ke struktur jaringan anda untuk memberikan perlindungan yang terbaik tanpa membuka organisasi anda pada masalah yang tak disengaja. Ada banyak sumber online mengenai cara install OpenVPN di server dan klien, kami merekomendasikan artikel ini dari Linux Journal: *http://www.linuxjournal.com/article/7949* dan juga HOWTO resmi: *http://openvpn.net/howto.html*

Tor & Anonymizers

Internet pada dasarnya adalah jaringan terbuka yang berbasis pada kepercayaan. Kalau anda menyambung ke web server di Internet, trafik anda melewati banyak router berbeda, lembaga, perusahaan dan individu yang berbeda. Secara prinsip, masing-masing router ini mempunyai kemampuan untuk mengamati secara seksama data anda, melihat alamat sumber dan tujuan, dan sering juga isi data sebenarnya. Sekalipun data anda di enkripsi memakai protokol aman, Internet provider anda sangat mungkin untuk memonitor data yang di transfer, termasuk sumber dan tujuan data itu. Biasanya ini cukup untuk memberikan gambaran yang cukup lengkap tentang aktivitas online anda.

Privasi dan keanoniman penting, dan amat dihubungkan kepada satu sama lain. Ada banyak sebab untuk mempertimbangkan melindungi privasi anda dengan cara ***meng-anonimkan*** trafik jaringan anda. Misalnya anda ingin menawarkan sambungan Internet ke komunitas lokal anda dengan mendirikan sejumlah akses point untuk tempat orang-orang menyambung. Entah anda meminta mereka membayar akses mereka atau tidak, selalu ada risiko bahwa orang akan memakai jaringan untuk sesuatu yang tidak legal di negara atau daerah anda. Anda bisa memohon pada pengadilan bahwa tindakan ilegal ini tidak dilakukan oleh anda, tetapi bisa dilakukan siapa saja yang menyambung dengan jaringan anda. Masalah ini bisa dielakkan jika secara teknis tidak mungkin mengetahui kemana trafik mengarah. Dan

bagaimana tentang sensor on-line? Mempublikasi halaman web tanpa nama mungkin juga perlu untuk menghindari sensor pemerintah.

Ada tool yang memungkinkan anda untuk meng-anonymize trafik anda dengan cara yang relatif mudah. Kombinasi dari ***Tor*** (*http://www.torproject.org/*) dan ***Privoxy*** (*http://www.privoxy.org/)* adalah cara yang powerful untuk menjalankan proxy server lokal yang akan melewatkan trafik Internet anda melewati sejumlah server di seluruh net, membuatnya sangat sulit mengikuti jejak informasi. Tor bisa dijalankan di PC lokal, di bawah Microsoft Windows, Mac OSX, Linux dan beberapa jenis BSD, di mana dia akan meng-anonymize trafik dari browser di mesin itu. Tor dan Privoxy juga bisa di install di atas gateway server, atau bahkan akses point kecil yang terpasang (seperti Linksys WRT54G) di mana mereka memberikan keanoniman kepada semua user jaringan secara otomatis.

Tor bekerja dengan berulang kali melambungkan koneksi TCP anda melewati sejumlah server yang menyebar di seluruh Internet, dan dengan membungkus informasi routing di sejumlah lapisan yang terenkripsi (oleh karena itu dinamakan ***onion routing / routing bawang***), yang dikupas sewaktu paket berpindah dari network. Ini berarti, di titik mana pun di jaringan, alamat sumber dan tujuan tidak bisa dihubungkan. Ini membuat analisa trafik menjadi sangat sulit.

Keperluan bagi privacy proxy Privoxy dalam hubungannya dengann Tor disebabkan karena name server queries (DNS queries) di kebanyakan kasus tidak melewati server proxy, dan seseorang yang menganalisa trafik anda dengan mudah bisa melihat bahwa anda sedang mencoba masuk ke sebuah site (contohnya google.com) dengan fakta bahwa anda dikirimi DNS query untuk menterjemahkan google.com ke alamat sesuai IP. Privoxy bersambungan dengan Tor sebagai proxy SOCKS4, yang menggunakan host-name (bukan alamat IP) untuk mengantarkan paket anda ke tujuan yang dimaksudkan.

Di kata lain, memakai Privoxy dengan Tor adalah cara sederhana dan efektif untuk mencegah analisa trafik yang berusaha menghubungkan alamat IP anda dengan layanan online yang anda gunakan. Digabungkan dengan protokol yang terenkripsi dan aman (seperti yang itu sudah kami lihat di bab ini), Tor dan Privoxy menyediakan level keanoniman tinggi di Internet.

Network Monitoring

Network Monitoring penggunaan tool pencatatan dan analisis yang secara akurat menentukan arus trafik, penggunaan, dan indikator kinerja di jaringan lainnya. Tool monitoring yang baik memberi anda baik angka maupun representasi grafik dari kondisi jaringan. Ini menolong anda untuk menvisualisasikan secara akurat apa yang terjadi, agar anda tahu di mana perlu dilakukan penyesuaian. Tool ini dapat menolong anda untuk menjawab pertanyaan penting, seperti:

- Servis apa yang paling populer digunakan di jaringan?
- Siapa yang paling banyak menggunakan jaringan?
- Kanal nirkabel mana yang digunakan di wilayah saya?
- Apakah user meng install akses point nirkabel di jaringan kabel pribadi saya?
- Kapankah jaringan paling banyak dipakai?
- Situs apa yang paling sering dikunjungi user?
- Apakah jumlah trafik inbound atau outbound mendekati kapasitas jaringan kita?
- Apakah ada indikasi tentang situasi jaringan yang aneh dan memakai bandwith atau masalah lain?
- Apakah Internet Service Provider (ISP) kita menyediakan level layanan yang sesuai dengan yang kita bayar? Ini seharusnya dijawab berdasarkan bandwith yang tersedia, kehilangan paket, latensi, dan ketersediaan keseleruhan.

Dan mungkin adalah pertanyaan yang paling penting:

- Apakah pola trafik yang dilihat sesuai dengan harapan kita?

Mari lihat bagaimana seorang system administrator memakai alat monitoring dengan baik.

Contoh network monitoring yang efektif

Untuk contoh, asumsikan bahwa kita menguasai jaringan yang sudah jalan selama tiga bulan. Terdiri atas 50 komputer dan tiga server: email, jaringan, dan server proxy. Biarpun awalnya berjalan baik, user mulai mengadu kecepatan jaringan lambat dan spam email bertambah. Kinerja komputer melambat hingga sangat lamban (bahkan ketika tidak ada yang memakai jaringan), menyebabkan frustrasi di user anda.

Dengan banyak aduan dan penggunaan komputer sangat rendah, Dewan mempertanyakan keperluan untuk begitu banyak hardware jaringan. Dewan juga ingin bukti bahwa bandwidth yang mereka bayar betul-betul dipakai. Sebagai administrator jaringan, anda di posisi yang menerima pengaduan ini. Bagaimana anda bisa mendiagnosa penurunan mendadak di kinerja jaringan dan komputer dan juga menjustifikasi hardware jaringan dan biaya bandwidth?

Monitoring the LAN (local traffic)

Untuk mendapat gambaran secara akurat apa yang menyebabkan kelambatan, anda sebaiknya memulai dengan melihat trafik di LAN lokal. Ada beberapa keuntungan monitoring trafik lokal:

- Penyelesaian masalah menjadi sangat disederhanakan.
- Virus bisa di deteksi dan di musnahkan.
- User jahat bisa dideteksi dan di urus.
- Hardware jaringan dan sumber daya bisa ukur dengan statistik nyata.

Asumsi bahwa semua switch mendukung ***Simple Network Management Protocol (SNMP).*** SNMP adalah protokol lapisan aplikasi yang di disain untuk memudahkan pertukaran informasi manajemen di antara alat-alat jaringan. Dengan memberikan alamat IP pada masing-masing switch, anda dapat memonitor semua interface di switch itu, mengawasi seluruh jaringan dari satu titik. Ini jauh lebih mudah daripada memakai SNMP di semua komputer di jaringan.

Dengan memakai tool gratisan seperti MRTG (lihat **Halaman 190)**, anda bisa memonitor masing-masing port di switch dan memberi data secara grafis, sebagai rata-rata agregasi trafik terhadap waktu. Grafik ini dapat diakses melalui web, jadi anda dapat melihat grafik dari mesin yang mana pun dan kapanpun.

Dengan adanya monitoring MRTG, menjadi jelas bahwa internal LAN dibanjiri dengan jauh lebih banyak trafik dari yang bisa disokong koneksi Internet nya, bahkan ketika lab sedang kosong. Ini adalah tanda yang sangat jelas bahwa beberapa komputer di infestasi oleh virus jaringan. Sesudah meng install software anti-virus dan anti-spyware yang baik di semua mesin, trafik internal LAN turun sampai level yang diharapkan. Mesin berjalan jauh lebih cepat, spam email berkurang, dan semangat user bertambah baik.

Monitor WAN (trafik keluar)

Disamping memperhatikan trafik di LAN internal, anda perlu memperlihatkan bahwa bandwidth yang dibayar organisasi sesuai dengan apa yang mereka dapat dari ISP. Anda dapat memperoleh ini dengan mengamati t***rafik eksternal.***

Trafik eksternal secara umum adalah apa saja yang dikirim di ***Wide Area Network (WAN)***. Apa saja yang diterima dari (atau mengirim ke) jaringan selain LAN internal anda juga memenuhi syarat sebagai trafik eksternal. Keuntungan memonitor trafik eksternal adalah:

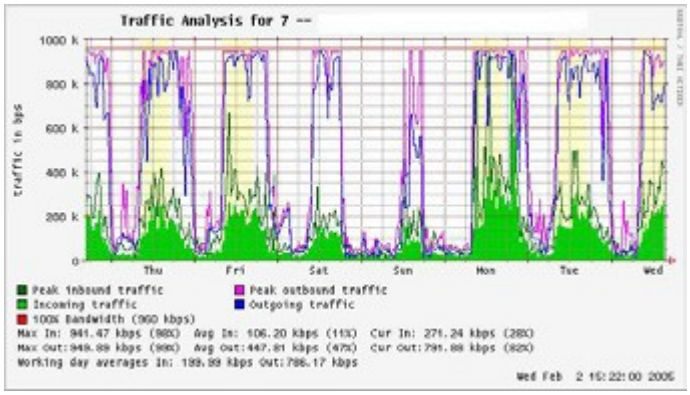
- Biaya bandwidth Internet dijustifikasi dengan memperlihatkan penggunaan sebenarnya, dan apakah penggunaan sesuai dengan biaya bandwidth yang diminta ISP anda.
- Kebutuhan kapasitas di masa depan dapat diperkirakan dengan cara memperhatikan pola penggunaan dan memperkirakan pola pertumbuhan.
- Penyusup dari Internet dideteksi dan disaring sebelum mereka bisa menyebabkan masalah.

Monitoring trafik ini dengan mudah dilakukan dengan penggunaan MRTG di alat yang dilengkapi SNMP, seperti router. Jika router anda tidak menyokong SNMP, anda bisa menambahkan switch di antara router anda dan koneksi ISP anda, dan memonitor port traffic dengan cara seperti LAN internal.

Mendeteksi Padamnya Jaringan

Dengan instalasi tool monitoring, anda dapat mengukur dengan akurat berapa banyak bandwidth yang digunakan organisasi. Hasil pengukuran harus sesuai dengan bandwidth ISP anda. Dia juga bisa menunjukkan throughput koneksi anda yang sebenarnya jika anda mendekati batas kapasitas anda di waktu-waktu puncak. Grafik "flat top" adalah tanda yang cukup jelas bahwa anda sedang beroperasi di kapasitas penuh. **Gambar 6.7** memperlihatkan flat top di puncak trafik outbound tertinggi di pertengahan setiap hari kecuali Minggu.

Jelas bahwa hubungan Internet anda sekarang terlalu banyak digunakan di waktu puncak, menyebabkan lag jaringan. Sesudah memberikan informasi ini kepada Dewan, anda bisa membuat rencana untuk lebih lanjut mengoptimisasi koneksi anda yang sudah ada (dengan mengupgrade server proxy anda dan memakai teknik lain di buku ini) dan memperkirakan kapan anda akan perlu mengupgrade koneksi anda untuk mengikuti permintaan. Ini adalah juga waktu yang bagus untuk memeriksa kebijakan anda dengan Dewan, dan mendiskusikan cara untuk membawa masuk penggunaan sebenarnya sesuai dengan kebijakan itu.



Gambar 6.7: Grafik dengan "flat top" adalah indikasi penggunaan berlebih.

Kemudian, anda mendapat telepon mendadak di malam harinya. Rupanya, tak seorang pun di lab yang dapat browsing ke Internet atau mengirim email. Anda tergesa-gesa ke lab dan dengan tergesa-gesa mereboot server proxy, tanpa hasil. Browsing dan email masih gagal. Anda lalu mereboot router, tetapi masih tidak berhasil. Anda terus mencoba kemungkinan kesalahan satu per satu sampai anda menyadari bahwa switch dari jaringan mati – penyebabnya adalah kabel listrik yang longgar. Sesudah memperbaiki listriknya, jaringan hidup lagi.

Bagaimanakah anda memperbaiki gangguan listrik seperti itu tanpa mencoba-coba yang memakan waktu seperti itu? Apakah mungkin diberitahukan mengenai gangguan listrik saat mereka terjadi, daripada menunggu seorang user untuk mengadu? Satu cara untuk melakukan ini adalah memakai program seperti Nagios yang secara terus-menerus mengawasi alat jaringan dan memberitahukan anda jika ada gangguan listrik. Nagios akan melaporkan ketersediaan berbagai mesin dan layanan, dan akan menyiagakan anda ke

mesin yang mati. Disamping memberitahu status jaringan secara grafis di sebuah halaman web, dia akan mengirim pemberitahuan melalui SMS atau email, segera menyiagakan anda kalau masalah timbul.

Dengan menggunakan tool monitor yang baik, anda akan dapat menentukan biaya perlengkapan dan bandwidth dengan secara efektif mempertunjukkan bagaimana itu dipakai oleh organisasi. Anda diberitahu secara otomatis kalau masalah timbul, dan anda mempunyai sejarah dalam statistik bagaimana alat jaringan sedang berjalan. Anda bisa membandingkan kinerja sekarang dan sejarah statistik ini untuk menemukan perilaku yang tidak biasa, dan mencegah masalah sebelum mereka menjadi kritis. Kalau masalah muncul, sangat sederhana untuk menentukan sumber dan sifat masalah. Pekerjaan anda lebih mudah, Dewan puas, dan user anda lebih bahagia.

Monitoring your network

Mengelola jaringan tanpa memonitor mirip mengemudi kendaraan tanpa sebuah speedometer atau pengukur bahan bakar, dengan mata tertutup. Bagaimana anda tahu bagaimana cepat anda sekarang? Apakah mobil memakan bahan bakar seefisien seperti yang dijanjikan oleh penjual? Jika anda melakukan permeriksaan mesin sesudah beberapa bulan, apakah mobil lebih cepat atau lebih efisien daripada sebelumnya?

Demikian pula, bagaimana anda bisa membayar tagihan listrik atau air dengan tanpa melihat penggunaan bulanan anda dari meteran? Anda harus mempunyai catatan penggunaan bandwidth jaringan anda untuk menentukan biaya servis dan pembelian hardware, dan untuk mencatat pola penggunaan
.
Ada beberapa keuntungan melakukan sistem monitor yang baik untuk jaringan anda:

1. **Anggaran jaringan dan sumber daya di justifikasi.** Tool monitor yang baik bisa memperlihatkan tanpa ragu-ragu bahwa infrastruktur jaringan (bandwidth, hardware, dan software) cocok dan bisa menangani kebutuhan pengguna jaringan.

2. **Penyusup jaringan dideteksi dan disaring.** Dengan menonton trafik jaringan anda, anda bisa mendeteksi penyerang dan mencegah akses ke server dan layanan yang penting.

3. **Virus jaringan dengan mudah dideteksi.** Anda akan diberitahu akan adanya virus jaringan, dan melakukan tindakan sebelum mereka memakan bandwidth Internet dan mendestabilisasi jaringan anda.

4. **Troubleshooting masalah jaringan sangat disederhanakan.** Daripada mencoba untuk men-debug masalah jaringan, anda dengan segera bisa diberitahukan mengenai masalah spesifik. Beberapa masalah bahkan bisa diperbaiki secara otomatis.

5. **Kinerja jaringan bisa sangat di optimisasi.** Tanpa monitoring efektif, mustahil untuk mengkonfigurasi alat dan protokol anda untuk mencapai kinerja yang terbaik.

6. **Perencanaan kapasitas lebih mudah.** Dengan catatan kinerja sejarah, anda tidak harus "mengira-ngira" berapa banyak bandwidth yang anda perlukan sewaktu jaringan anda bertambah besar.

7. **Penggunaan jaringan secara layak bisa ditekankan.** Ketika bandwidth adalah sumber daya yang susah didapat, satu-satunya cara untuk menjadi adil kepada semua user adalah menjamin kalau jaringan dipakai sesuai dengan maksudnya.

Untungnya, monitoring jaringan tidak perlu mahal. Ada banyak tool open source yang gratis yang akan menunjukkan pada anda apa yang sedang terjadi di jaringan anda dengan cukup rinci. Bagian ini akan menolong anda mengenali banyak tool yang tak ternilai harganya dan cara untuk memakai mereka.

Server dedicated untuk monitoring

Biarpun layanan monitoring dapat ditambahkan ke server jaringan yang sudah ada, sering diinginkan untuk mendedikasikan satu mesin (atau lebih banyak, jika perlu) untuk monitoring jaringan. Beberapa aplikasi (seperti **ntop**) membutuhkan sumber daya yang banyak untuk dijalankan, terutama pada jaringan sibuk. Tetapi kebanyakan program logging dan monitoring memerlukan syarat RAM dan storage sedang, biasanya dengan sedikit tenaga CPU diperlukan. Sejak operating sistem open source (seperti Linux atau BSD) memakai sumber daya hardware dengan sangat efisien, ini membuatnya mungkin untuk membangun server monitoring yang baik dari PC bekas. Biasanya tidak perlu membeli server baru hanya untuk keperluan monitoring.

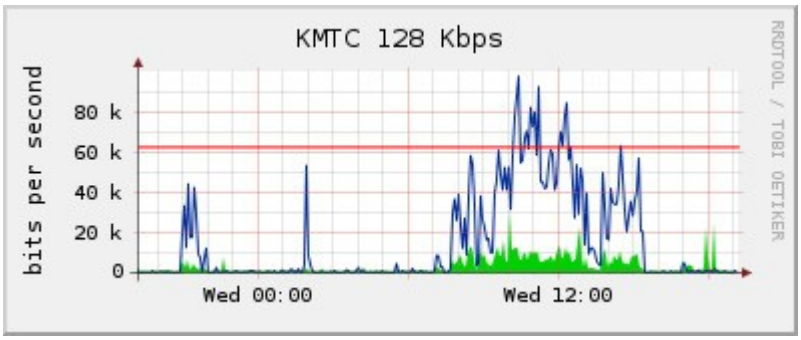
Pengecualian dari cara ini adalah pada instalasi yang sangat besar. Jika jaringan anda lebih dari beberapa ratus nodes, atau jika anda menggunakan lebih dari 50 Mbps bandwidth Internet, anda mungkin akan perlu memecah keperluan monitoring di antara beberapa mesin yang didedikasikan. Ini sangat tergantung pada apa yang ingin anda amati. Jika anda sedang mencoba mencatat semua alamat layanan yang di akses per MAC, ini akan memakan jauh lebih banyak sumber daya daripada sekedar mengukur aliran jaringan di sebuah switch port. Tetapi untuk kebanyakan instalasi, satu mesin yang didedikasikan untuk monitoring biasanya cukup.

Dengan mengkonsolidasi layanan monitoring ke satu mesin akan memudahkan administrasi dan mengupgrade, selain itu juga menjamin monitoring 24 jam yang lebih baik. Misalnya, jika anda menginstall layanan monitoring di sebuah web server , dan web server mengalami masalah, maka jaringan anda mungkin tidak dapat di monitor sampai masalah di Web server terselesaikan.

Untuk seorang administrator jaringan, data yang dikoleksi mengenai kinerja jaringan hampir sama penting dengan jaringan itu sendiri. Fasilitas monitoring anda sebaiknya cukup kuat dan dilindungi dari gangguan listrik. Tanpa statistik jaringan, anda buta akan masalah di jaringan anda.

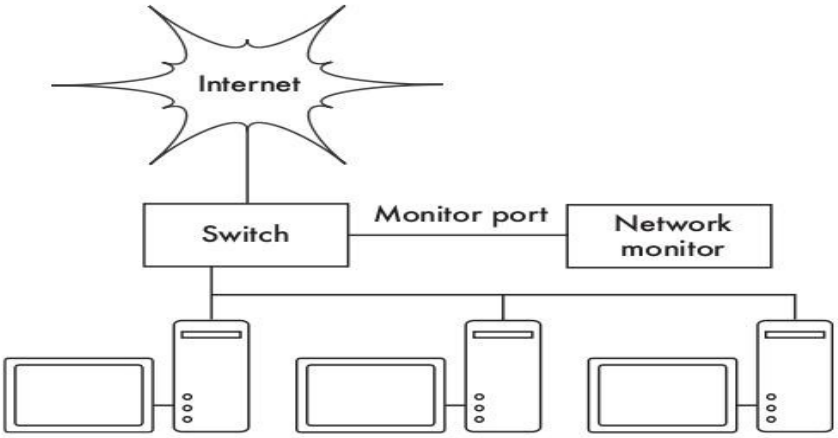
Dimanakah letak server ke jaringan saya?

Jika anda hanya tertarik dalam mengumpulkan statistik aliran data di jaringan dari router, anda bisa melakukan ini dari hampir semua lokasi di LAN. Ini memberikan feedback sederhana tentang penggunaan, tetapi tidak bisa memberi anda detail menyeluruh mengenai pola penggunaan. **Gambar 6.8** menampilkan grafik umum MRTG yang ditimbulkan dari Internet router. Biarpun penggunaan inbound dan outbound jelas, tidak ada detail tentang komputer, pemakai, atau protokol yang mana yang sedang menggunakan bandwidth.



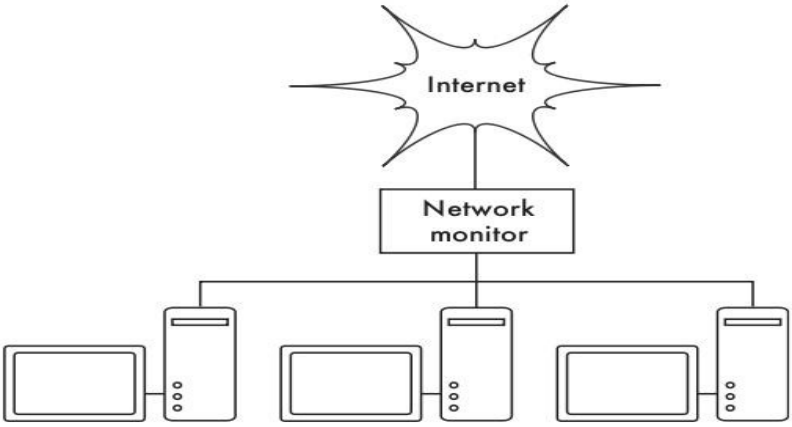
Gambar 6.8: Hasil polling router edge memperlihatkan kepada anda penggunaan jaringan keseluruhan, tetapi anda tidak bisa menyimak data lebih jauh ke dalam mesin, layanan, dan user.

Untuk lebih rinci, server monitoring terdedikasi harus mempunyai akses ke semua yang perlu di perhatikan. Biasanya, ini berarti harus mempunyai akses ke seluruh jaringan. Untuk mengamati hubungan WAN, seperti hubungan Internet kepada ISP anda, server monitor harus dapat melihat trafik yang melewati router pinggir. Untuk memonitor LAN, server monitor biasanya dihubungkan dengan ***monitor port*** di switch. Jika banyak switch dipakai di instalasi, server monitor mungkin memerlukan koneksi kepada semuanya. Sambungan dapat berupa sebuah kabel fisik, atau jika switch jaringan mendukungnya, VLAN yang diatur khusus untuk monitoring trafik.



Gambar 6.9:
Menggunakan monitor port di switch anda untuk mengamati trafik yang melewati port jaringan.

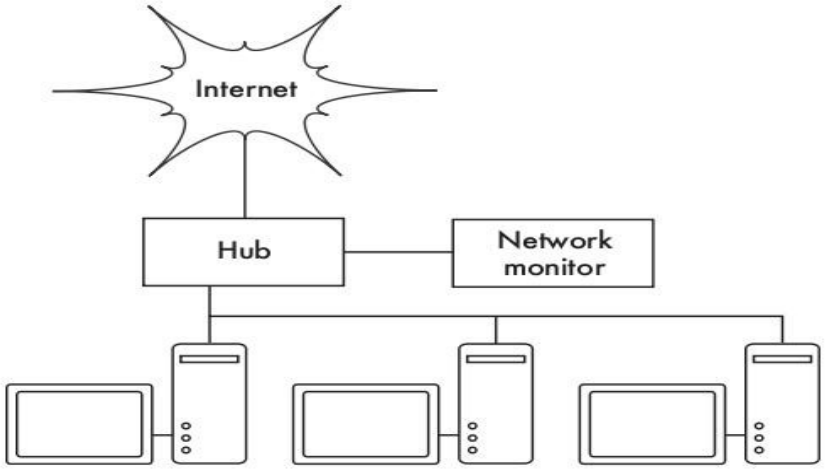
Jika fungsi monitor port tidak ada di switch anda, server monitor mungkin dipasang di antara internal LAN anda dan Internet. Walaupun ini akan bekerja, ini akan memasukan satu titik kelemahan pada jaringan, karena jaringan akan gagal jika server monitor mengalami masalah. Ini juga berpotensi menjadi kinerja bottleneck, jika server tidak bisa mengikuti tuntutan jaringan.



Gambar 6.10:
Dengan memasukkan sebuah server monitor jaringan di antara LAN dan koneksi Internet anda, anda bisa mengamati semua trafik jaringan.

.
Pemecahan yang lebih baik adalah memakai hub jaringan sederhana (bukan sebuah switch) yang menyambungkan mesin monitor ke LAN internal, eksternal router, dan mesin monitor.

Biarpun ini masih mempunyai titik kegagalan tambahan kepada jaringan (karena seluruh jaringan tak dapat dicapai jika hub mati), hub secara umum dianggap lebih dapat diandalkan daripada router. Mereka juga sangat mudah diganti jika mereka gagal.



Gambar 6.11:
Jika switch anda tidak menyediakan fungsi monitor port , anda dapat menggunakan sebuah hub jaringan diantara router Internet dan LAN, dan menyambungkan server monitor ke hub.

Setelah monitoring server anda siap, anda siap untuk mulai menumpulkan data

Apa yang di monitor

Sangat mungkin untuk menampilkan hampir semua kejadian jaringan dan melihat nilainya di grafik sejalan dengan waktu. Karena setiap jaringan agak berbeda, anda harus memilih informasi apa yang penting agar bisa mengukur kinerja jaringan anda.

Berikut Ini adalah beberapa indikator yang biasanya akan dicari administrator jaringan.

Statistik Wireless

- Sinyal yang didapat dan semua gangguan dari backbone nodes
- Jumlah dari stations yang terasosiasi.
- Mendeteksi jaringan dan kanal tetangga.
- Adanya pengiriman ulang yang terlalu banyak.
- Kecepatan data di radio, jika memakai automatic rate scaling

Statistik Switch

- Pemakaian Bandwidth per switch port

- Pemakaian Bandwidth per protokol
- Pemakaian Bandwidth per alamat MAC
- Trafik broadcast sebagai persentase dari total paket
- Kehilangan Packet dan rate error

Statistik Internet

- Internet bandwidth yang di pakai per host dan protocol
- Cache hits pada jaringan proxy
- 100 site yang paling sering diakses
- Permohonan DNS
- Jumlah dari email inbound / email spam / email bounce
- Besarnya antrian e-mail yang keluar
- Ketersediaan dari servis penting (jaringan web, jaringan email, etc.).
- Waktu Ping dan rate kehilangan paket ke ISP
- Status dari backup

Statistik kesehatan system

- Penggunaan memory
- Penggunaan swap file
- Process count / zombie process
- System load
- Voltase dan load dari Uninterruptible Power Supply (UPS)
- Temperatur, kecepatan kipas, dan voltase sistem
- Status Disk SMART
- Status RAID array

Anda sebaiknya menggunakan ini sebagai saran untuk memulai. Bersamaan dengan tumbuhnya jaringan anda, anda biasanya akan menemukan kunci indikator baru dari kinerja jaringan, dan anda seharusnya dapat mengamati itu pula. Ada banyak tool gratis yang dapat memperlihatkan kepada anda perincian sebanyak yang anda suka mengenai apa yang sedang terjadi di jaringan anda. Anda sebaiknya mempertimbangkan memonitor ketersediaan sumber daya yang ada dan mencari titik / alat yang paling kritis jika tidak ada terhadap pengguna jaringan anda.

Misalnya, user anda mungkin menggunakan modem telepon untuk mengakses situs anda untuk mendapat remote access ke jaringan anda. Jika semua modem dipakai, atau jika ada yang rusak, maka pemakai akan ditolak aksesnya dan mungkin akan komplain. Anda bisa memprediksi dan menghindari masalah seperti itu dengan mengamati jumlah modem yang ada, dan menyiapkan kapasitas ekstra sebelum anda kehabisan.

Jangan lupa memonitor mesin monitor itu sendiri, misalnya penggunaan CPU dan disk space, untuk mendapat peringatan yang lebih dahulu jika itu menjadi terlalu penuh atau rusak. Mesin

monitor yang bersumber daya rendah bisa mempengaruhi kemampuan anda untuk memonitor jaringan secara efektif.

Tipe tool monitoring

Kita sekarang akan melihat beberapa kelas tool monitoring. Tool ***pendeteksi jaringan*** memperhatikan beacon yang dikirim oleh akses point nirkabel, dan menampilkan informasi seperti nama jaringan, kekuatan signal yang didapat, dan channel. Tool ***spot check*** di disain untuk troubleshooting dan biasanya dikelola secara interaktif selama periode waktu yang singkat. Program seperti **ping** mungkin dianggap sebagai tool spot check aktif, karena dia mengeluarkan trafik dan melakukan polling ke mesin tertentu. Tool spot check pasif termasuk ***protokol analyzer***, yang memeriksa setiap paket di jaringan dan menyediakan perincian secara detail mengenai percakapan jaringan (termasuk alamat sumber dan tujuan, informasi protokol, dan bahkan data aplikasi). Tool ***trending*** menjalankan monitor tanpa operator dalam periode lama, dan biasanya menyiapkan hasil menjadi grafik. Tool ***monitor realtime*** menjalankan monitor yang sama, tetapi segera memberitahu administrator jika mereka mengetahui masalah. Tool ***penguji throughput*** memberitahu anda bandwidth sebenarnya yang ada di antara dua ujung di jaringan. Tool ***Intrusion detection*** mengamati trafik jaringan yang tidak diinginkan, dan mengambil keputusan yang tepat (biasanya menolak akses dan/atau memberitahu seorang network administrator). Akhirnya, tool ***benchmarking*** memperkirakan kinerja maksimum dari sebuah layanan atau sambungan jaringan.

Mendeteksi Jaringan

Tool monitor nirkabel yang paling sederhana hnya memberikan daftar jaringan yang tersedia, di dampingi oleh informasi dasar (seperti kekuatan sinyal dan kanal). Mereka memungkinkan anda mendeteksi jaringan yang dekat dengan cepat dan menentukan bila mereka ada dalam jangkauan atau mengakibatkan gangguan.

- **Built-in client.** Semua sistem operasi modern mempunyai built-in support untuk jaringan nirkabel. Ini biasanya termasuk kemampuan untuk scan jaringan yang tersedia, membantu user untuk memilih sebuah jaringan dari daftar. Hampir semua alat nirkabel biasanya mempunyai alat scan sederhana, fungsi bisa berbeda di setiap implementasi. Alat-alat ini biasanya hanya berguna untuk mengatur sebuah komputer di konfigurasi rumah atau kantor. Mereka biasanya hanya menyediakan sedikit informasi selain dari nama jaringan dan sinyal yang tersedia sampai dengan akses point yang sedang dipakai.

- **Netstumbler (***http://www.netstumbler.com/***)**. Ini adalah tool yang paling populer karena mendeteksi jaringan nirkabel menggunakan Microsoft Windows. Dia mendukung beberapa jenis wireless card, dan sangat mudah digunakan. Dia akan mendeteksi jaringan-jaringan yang terenkripsi dan yang terbuka, tetapi tidak bisa mendeteksi jaringan-jaringan nirkabel “tertutup”. Dia juga menampilkan kekuatan sinyal / noise dan

menggambarkan sinyal yang di terima sebagai fungsi waktu. Dia juga dapat berintegrasi dengan beberapa jenis GPS, untuk mencatatkan informasi lokasi dan kekuatan sinyal secara tepat. Ini membuat Netstumbler menjadi sebuah alat berguna untuk site survey informal.

- **Ministumbler** (*http://www.netstumbler.com/*). Dari pembuat Netstumbler, Ministumbler memberikan fungsi yang sama dengan versi Windows nya, tapi bekerja di Pocket PC Ministumbler nyaman digunakan di handheld PDA dengan sebuah wireless card untuk mendeteksi akses point.

- **Macstumbler** (*http://www.macstumbler.com/*). Biarpun tidak terkait langsung dengan Netstumbler, Macstumbler memberi banyak fungsi yang sama tetapi untuk platform Mac OSX. Dia bekerja dengan semua Apple Airport cards.

- **Wellenreiter** (*http://www.wellenreiter.net/*). Wellenreiter adalah sebuah pendeteksi jaringan nirkabel grafik untuk Linux. Dia membutuhkan Perl dan GTK, dan menyokong port Prism2, Lucent, dan Cisco wireless cards.

Tool Spot check

Apa yang anda lakukan ketika jaringan rusak? Jika anda tidak bisa mengakses web page atau server email, dan mengklik tombol reload tidak membereskan masalah, maka anda perlu mengisolasi lokasi masalah yang tepat. Alat ini akan menolong anda untuk memutuskan di mana ada masalah koneksi. Bagian ini adalah perkenalan saja ke alat troubleshooting yang biasa dipakai. Untuk memperoleh gambaran masalah jaringan yang umum terjadi dan bagaimana caranya untuk mendiagnosa mereka, lihat **Bab 9, Troubleshooting.**

Ping

Hampir semua sistem operasi (termasuk Windows, Mac OS X, dan tentu saja Linux dan BSD) memasukkan sebuah versi dari tool **ping.** Ping menggunakan paket ICMP untuk mencoba menghubungi sebuah host, dan memberitahu berapa lama waktu yang diperlukan untuk mendapat respon.

Mengetahui apa yang di ping sama pentingnya dengan mengetahui bagaimana cara ping. Jika anda mengetahui bahwa anda tidak bisa menyambung dengan suatu servis di web browser anda (misalnya, *http://yahoo.com/*), anda bisa mencoba mem ping nya:

```
$ 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
```

Tekan control-C jika anda selesai mengumpulkan data. Jika paket perlu waktu lama untuk kembali, mungkin ada kepadatan di jaringan. Jika paket ping memperoleh waktu ***Time To Live (TTL)*** yang tidak normal, anda mungkin mempunyai masalah routing di antara mesin anda dan remote end. Tetapi bagaimana jika ping tidak mengembalikan data sama sekali? Jika anda sedang ping sebuah nama dan bukan alamat IP, anda mungkin menemui masalah DNS.

Coba ping sebuah alamat IP di Internet. Jika anda tidak bisa mencapainya, cobalah ping router default anda:

```
$ ping 69.90.235.230
PING 69.90.235.230 (69.90.235.230): 56 data bytes
64 bytes from 69.90.235.230: icmp_seq=0 ttl=126 time=12.991 ms
64 bytes from 69.90.235.230: icmp_seq=1 ttl=126 time=14.869 ms
64 bytes from 69.90.235.230: 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
```

Jika anda tidak dapat ping router default anda, maka kemungkinan anda tidak bisa ke internet juga. Jika anda bahkan tidak bisa alamat IP lain di LAN lokal anda, maka anda perlu mencek koneksi anda. Jika anda menggunakan Ethernet, apakah sudah dicolok? Jika anda menggunakan nirkabel, apakah anda tersambung ke jaringan nirkabel yang betul, dan apakah ada dalam jangkauan?

Network debugging dengan ping sedikit berseni, tetapi dia sangat berguna untuk dipelajari. Karena anda biasanya menemukan ping di hampir semua mesin yang akan anda pakai, sangat baik jika anda dapat mempelajari bagaimana menggunakannya dengan baik.

Traceroute and mtr

http://www.bitwizard.nl/mtr/. Seperti ping, traceroute ditemukan pada kebanyakan sistem operasi (di Windows biasanya di sebut tracert). Dengan menjalankan traceroute, anda bisa mencari lokasi masalah anda di antara komputer anda dan semua node di internet:

```
$ traceroute -n google.com
```

```
traceroute to google.com (72.14.207.99), 64 hops max, 40 byte packets
traceroute and mtr
  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 * * *
```

Switch -n memberitahu traceroute agar tidak perlu me-resolve nama-nama di DNS, dan membuat proses trace makin cepat. Anda dapat melihat bahwa pada hop ke tujuh, waktu round trip naik lebih dari dua detik, paket tampaknya seperti dibuang pada hop ke delapan. Ini mengindikasikan bahwa ada sbeuah masalah jaringan di titik tersebut. Jika bagian dari jaringan ini ada di dalam kendali anda, mungkin akan berguna untuk memulai troubleshooting di node tersebut.

My TraceRoute (mtr) adalah sebuah program yang berguna yang menggabungkan ping dan traceroute menjadi satu tool. Dengan menjalankan mtr, anda bisa sebuah ongoing average of latency dan packet loss ke sebuah host, daripada snapshot sementara yang disediakan ping dan 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
```

Data akan terus di update dan di rata-ratakan seiring dengan waktu. Seperti ping, anda harus menekan tombol control-C ketika anda sudah selesai melihat data itu. Perhatikan bahwa anda harus menjadi root untuk menjalankan mtr.

Biarpun tool-tool ini tidak akan memberitahu secara tepat kesalahan apa yang terjadi pada jaringan anad, mereka akan memberi anda cukup informasi untuk mengetahui dimana akan melannjutkan troubleshooting.

Protocol analyzers

Protocol analyzer jaringan memberikan detail yang banyak tentang informasi yang mengalir di jaringan, dengan memungkinkan anda menginspeksi paket individual. Untuk jaringan berkabel, anda bisa menginspeksi paket di lapisan data-link atau diatasnya. Untuk jaringan nirkabel, anda bisa menginspeksi informasi sampai kepada frame 802.11 secara individual. Ini adalah beberapa protocol analyzer jaringan yang populer (dan gratis):

Kismet

http://www.kismetwireless.net/. Kismet adalah sebuah sebuah protocol analyzer jaringan yang powerful untuk berbagai platform termasuk Linux, Mac OS X, bahkan distribusi Linux embedded OpenWRT. Ia bekerja dengan semua wireless card yang menyokong mode monitoring pasif. Selain dari deteksi jaringan dasar, Kismet akan secara pasif mencatat semua frame 802.11 ke disk atau ke jaringan dalam format standar PCAP, untuk analisa selanjutnya menggunakan tool seperti Ethereal. Kismet juga menampilkan informasi klien yang berasosiasi, mengetahui hardware AP, mendeteksi adanya Netstumbler, dan integrasi dengan GPS.

Karena ia adalah sebuah monitor jaringan pasif, ia bahkan bisa mendeteksi jaringan nirkabel "tertutup" dengan menganalisa trafik yang dikirim oleh client nirkabel. Anda bisa menjalankan Kismet di beberapa mesin sekaligus, dan membuat mereka melapor dari jaringan ke sebuah central user interface. Ini memungkinkan monitoring nirkabel di area yang luas, seperti sebuah universitas atau campus corporate.

Figure 6.12: Kismet dijalankan di sebuah Nokia 770 Internet Tablet

Karena Kismet memakai mode monitor pasif dari radio card, ia melakukan semua ini tanpa mengirimkan data apapun. Kismet adalah sebuah alat penting untuk mendiagnosa masalah jaringan nirkabel.

KisMAC

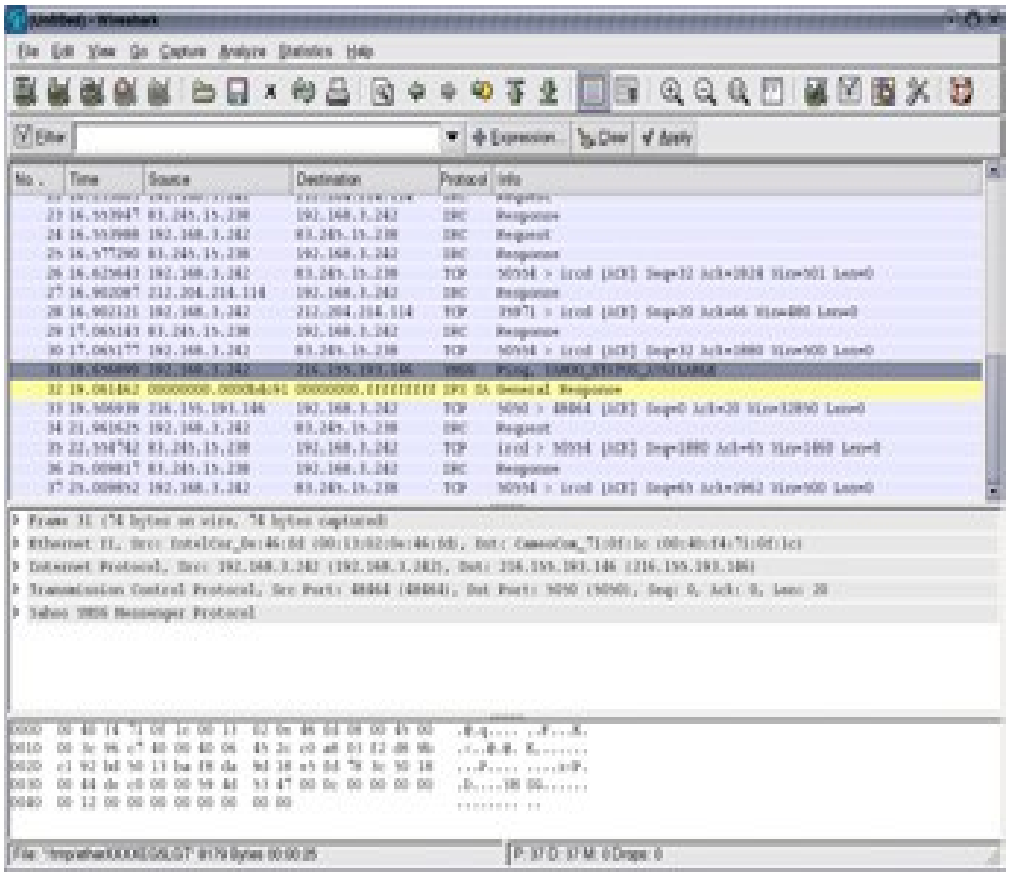
http://kismac.macpirate.ch/. Hanya untuk platform Mac OS X, KisMAC melakukan apa yang Kismet bisa lakukan, tetapi dengan interface grafik Mac OS X. Ia adalah sebuah scanner pasif yang akan mencatat data ke disk dalam format PCAP yang cocok dengan Wireshark. Ia menyokong scanning pasif dengan AirportExtreme card dan juga beberapa varietas dari USB wireless adapters.

tcpdump

http://www.tcpdump.org/. **tcpdump** adalah sebuah tool command-line untuk monitoring trafik jaringan. Tidak mempunyai semua fitur wireshark tetapi memakai lebih sedikit sumber daya. Tcpdump bisa menangkap dan menunjukkan semua informasi protokol jaringan sampai ke link layer. Ia bisa memperlihatkan semua headers paket dan data yang diterima, atau hanya paket yang memenuhi kriteria khusus. Paket yang tertangkap dengan tcpdump dapat dimasukkan ke dalam wireshark untuk analisa visual dan diagnostik lebih jauh. Ini sangat berguna jika anda menginginkan untuk mengamati interface di sebuah remote system dan mengambil kembali filenya ke mesin lokal anda untuk analisa. Tool tcpdump tersedia sebagai tool standar dalam derivatif Unix (Linux, BSD, dan Mac OS X). Ada juga port Windows bernama **WinDump** yang tersedia di *http://www.winpcap.org/windump/.*

Wireshark

http://www.wireshark.org/. Sebelumnya dikenal sebagai Ethereal, Wireshark adalah sebuah network protocol analyzer untuk Unix dan Windows. Ia ditulis sebagai "The World's Most Popular Network Protocol Analyzer."



Gambar 6.13: Wireshark (sebelumnya Ethereal) adalah sebuah network protocol analyzer yang powerful yang dapat memperlihatkan secara detail tentang sebuah paket apapun.

Wireshark memungkinkan anda mengamati data dari jaringan yang sedang beroperasi atau dari data yang ada di disk, dan langsung melihat dan mensortir data yang tertangkap. Informasi singkat dan detail tersedia bagi masing-masing paket, termasuk full header dan porsi data. Wireshark punya beberapa fitur powerful termasuk display filter language yang kaya dan kemampuan untuk merekonstruksi kembali sebuah aliran pada sesi TCP.

Wireshark dapat menakutkan bagi para pemula atau mereka yang tidak kenal dengan lapisan OSI. Ia biasanya dipakai untuk mengisolasi dan menganalisa sebuah trafik tertentu untuk/dari sebuah alamat IP, tapi bisanya juga untuk alat pencari masalah secara umum. Misalnya, sebuah mesin diinfeksi dengan sebuah worm atau virus bisa diidentifikasi dengan melihat ke mesin yang mengirim paket TCPIP yang sama ke banyak alamat IP.

Trending tools

Tool trending dipergunakan untuk melihat bagaimana jaringan anda dipakai dalam jangka waktu yang lama. Mereka bekerja dengan memonitor aktivitas jaringan anda secara periodik,

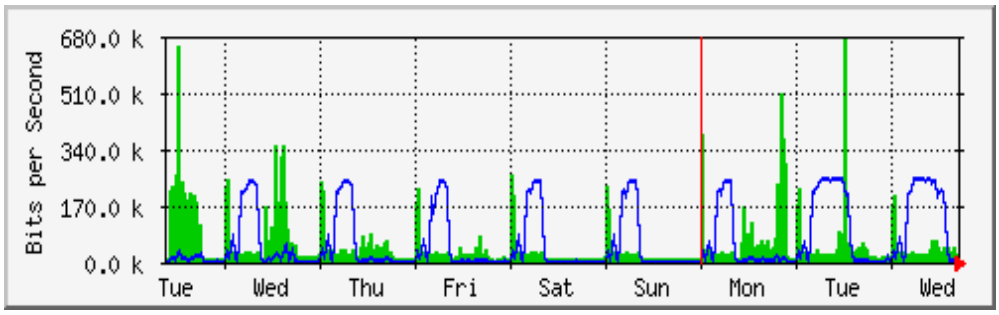
dan menampilkan dalam sebuah ringkasan ang bisa dibaca manusia (seperti grafik).Tool trending mengumpulakan data dan juga menganalisa dan melaporkannya.

Di bawah ini adalah beberapa contoh tool trending. Beberapa dari mereka perlu dipakai bersama dengan yang lain, karena mereka bukan program stand-alone.

MRTG

http://oss.oetiker.ch/mrtg/. ***Multi Router Traffic Grapher (MRTG)*** memonitor load trafik di sambungan-sambungan jaringan yang memakai SNMP. MRTG menghasilkan grafik yang menyediakan gambaran visual dari trafik inbound dan outbound. Ini biasanya di tampilkan di sebuah halaman web.

MRTG bisa agak membingungkan untuk dipasang, khususnya jika anda tidak kenal baik dengan SNMP. Tetapi begitu terpasang, MRTG tidak memerlukan maintenance, kecuali kalau anda mengganti sesuatu di sistem yang dimonitor (seperti alamat IPnya).



Gambar 6.14: MRTG mungkin adalah pembuat grafik jaringan yang paling banyak di install.

RRDtool

http://oss.oetiker.ch/rrdtool/. ***RRD*** adalah singkatan untuk ***Round Robin Database.*** RRD adalah sebuah database yang menyimpan informasi dengan cara yang sangat compact yang tidak berkembang seiring waktu. ***RRDtool*** merujuk pada sesederetan tool yang memungkinkan anda menciptakan dan mengubah database RRD, dan juga menghasilkan grafik untuk merepresentasikan data. Ia dipakai untuk mencatat data terhadap waktu (seperti jaringan bandwith, temperatur ruang mesin, atau load server rata-rata) dan bisa menampilkan data itu sebagai rata-rata dalam selang waktu tertentu.

Perhatikan bahwa RRDtool itu sendiri tidak berhubungan dengan peralatan jaringan untuk mendapatkan data. Ia hanya alat manipulasi database belaka. Anda bisa memakai wrapper script sederhana (biasanya di shell atau Perl) untuk melakukan pekerjaan itu untuk anda. RRDtool juga dipakai oleh banyak front-ends yang mempunyai banyak fitur yang memberi anda interface jaringan yang lebih bersahabat untuk konfigurasi dan menampilkan. Grafik

RRD memberi anda lebih banyak kontrol pada pilihan display dan jumlah data yang akan di tampilkan pada sebuah grafik dibandingkan kepada MRTG.

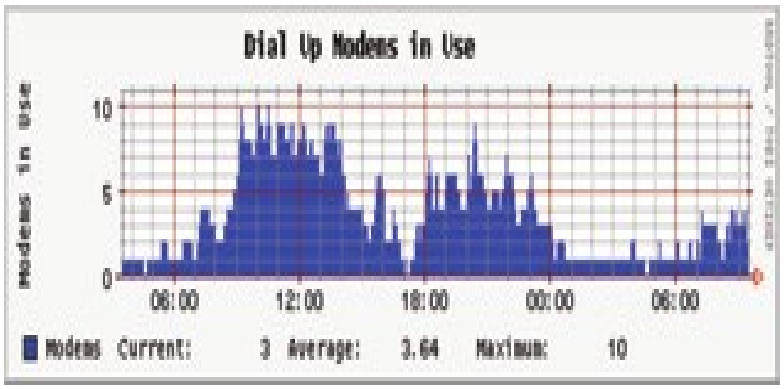


Figure 6,15: RRDtool memberi anda banyak fleksibelitas tentang bagaimana data jaringan dikumpulkan dan diperlihatkan.

RRDtool dimasukkan di semua distribusi modern Linux, dan bisa didownload dari *http://oss.oetiker.ch/rrdtool/.*

ntop

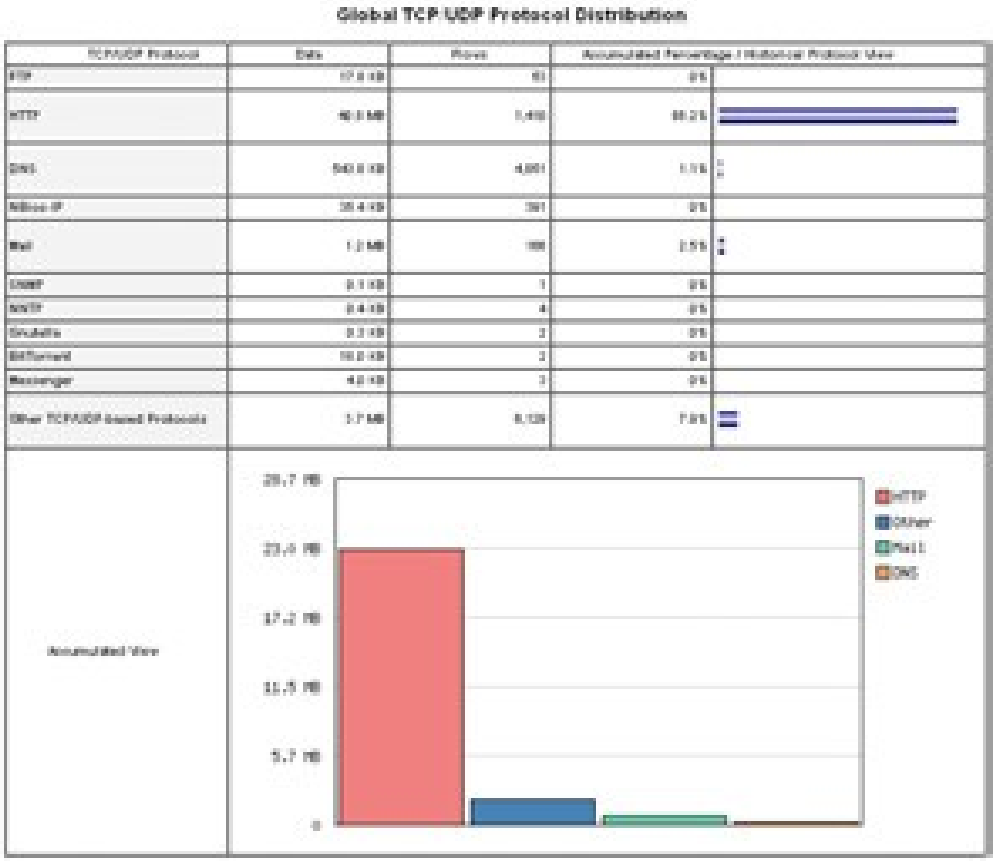
http://www.ntop.org/. Untuk melakukan analisis sejarah trafik dan penggunaan, anda tentu akan ingin mencoba **ntop.** Program ini membuat sebuah laporan real-time yang terperinci pada trafik jaringan yang diamati, yang ditunjukkan di web browser anda. Ia berintegrasi dengan rrdtool, dan membuat grafik yang secara visual menggambarkan bagaimana jaringan dipakai. Di jaringan-jaringan yang sangat sibuk, ntop akan menggunakan sebagian besar CPU dan harddisk, tetapi ia memberi anda gambaran yang luas akan bagaimana jaringan anda dipakai. Ia jalan di Linux, BSD, Mac OS X, dan Windows.

Beberapa fiturnya yang berguna termasuk:

- Penampilan trafik bisa diatur dengan berbagai kriteria (sumber, tujuan, protokol, alamat MAC, dll).
- Statistik trafik dikelompokkan oleh protokol dan port number
- Sebuah IP trafik matrix yang menunjukkan koneksi diantara mesin.
- Aliran jaringan untuk router dan switch yang menyokong protokol NetFlow
- Mengidentifikasi sistem operasi Host
- Mengidentifikasi trafik P2P
- Berbagai jenis grafik
- Perl, PHP, dan Python API

Ntop tersedia dari *http://www.ntop.org/* dan dapat digunakan di banyak sistem operasi. Ia

biasanya termasuk dalam banyak distribusi populer Linux, termasuk RedHat, Debian, dan Ubuntu. Pada saat ntop berjalan sendiri untuk mengumpulkan data, ntop dapat sangat mengkonsumsi CPU, tergantung pada banyaknya trafik yang diamati. Jika anda sedang memakainya selama periode yang lama anda sebaiknya mengamati penggunaan CPU dari mesin monitor.



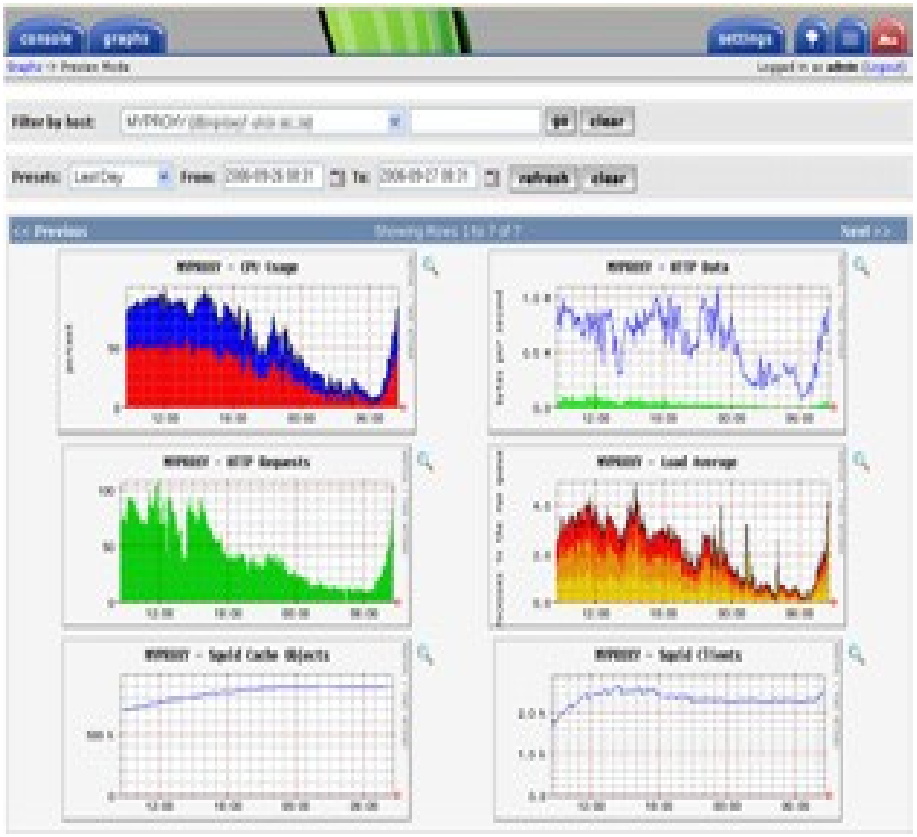
Gambar 6.16: ntop menampilkan banyak informasi tentang bagaimana jaringan dipakai oleh berbagai klien dan server.

Kekurangan utama dari ntop adalah ia tidak memberi informasi instan, hanya total dan rata-rata jangka panjang. Ini bisa menyusahkan untuk menggunakanya mengdiagnosa masalah yang muncul tiba-tiba.

Cacti

http://www.cacti.net/. Cacti adalah sebuah front-end untuk RRDtool. Ia menyimpan seluruh informasi yang diperlukan untuk membuat grafik di sebuah database MySQL. Front-end ditulis di PHP. Cacti yang memelihara grafik, sumber data, dan mengatur pengumpulan data

sebenarnya. Ada dukungann untuk tool SNMP, dan script yang di kustomisasi dengan mudah bisa ditulis untuk poll peristiwa jaringan apapun pun.



Gambar 6.17: Cacti dapat mengatur pengambil data dari peralatan jaringan, dan membuat visualisasi dari perilaku jaringan yang sangat informatif dan kompleks.

Cacti bisa agak membingungkan untuk dikonfigurasi, tetapi setelah anda menyelesaikan membaca dokumentasi dan contoh, ia bisa memberikan grafik yang sangat mengesankan. Ada ratusan template untuk berbagai sistem yang ada di website cacti, dan program Cacti sedang di kembangkan dengan pesat.

NetFlow

NetFlow adalah sebuah protokol untuk mengumpulkan informasi trafik IP yang dibuat oleh Cisco. Dari website Cisco:

> *Cisco IOS NetFlow secara efisien menyediakan layanan untuk aplikasi IP, termasuk penghitungan trafik jaringan, billing jaringan berdasarkan penggunaan, perencanaan jaringan, keamanan, kemampuan monitor Denial of Service, dan network monitoring. NetFlow memberikan informasi berharga mengenai user jaringan dan aplikasi, waktu*

penggunaan tertinggi, dan routing trafik.

Router Cisco akan menghasilkan informasi NetFlow yang tersedia dari router dalam bentuk paket UDP. NetFlow juga tidak memakan CPU di router Cisco dibanding menggunakan SNMP. Ia juga memberikan memberikan informasi granular lebih banyak dari SMNP, memperbolehkan untuk mendapatkan gambaran yang lebih rinci untuk penggunaan port dan protokol.

Informasi ini dikumpulkan oleh sebuah kolektor NetFlow yang menyimpan dan mempresentasian data sebagai akumulasi jumlah seiring waktu. Dengan menganalisa aliran data, seseorang dapat memperoleh gambaran tentang arus trafik dan volume trafik di jaringan atau di sebuah sambungan. Ada beberapa pengumpul NetFlow komersial dan gratis. Ntop adalah satu tool gratis yang bisa bertindak sebagai kolektor NetFlow dan probe. Yang lain adalah Flowc (lihat di bawah).

Netflow dapat digunakan sebagai tool spot check, dengan hanya memandang cuplikan cepat data selama krisis jaringan. Bayangkan NetFlow sebagai pilihan alternatif terhadap SNMP untuk alat Cisco. Untuk informasi lebih lanjut tetang NetFlow, lihat http://en.wikipedia.org/wiki/Netflow.

Flowc

http://netacad.kiev.ua/flowc/. **Flowc** adalah sebuah kolektor NetFlow open source (lihat NetFlow di atas). Ia ringan dan mudah untuk diatur. Flowc menggunakan sebuah database MySQL untuk menyimpan informasi trafik yang terkumpul. Oleh karena itu, mungkin untuk membuat laporan untuk anda sendiri dari data menggunakan SQL, atau menggunakan pembuat laporan yang tersedia di Flowc. Pembuat laporan yang tersedia di Flowc menghasilkan laporan dalam bentuk HTML, teks polos atau format grafik.

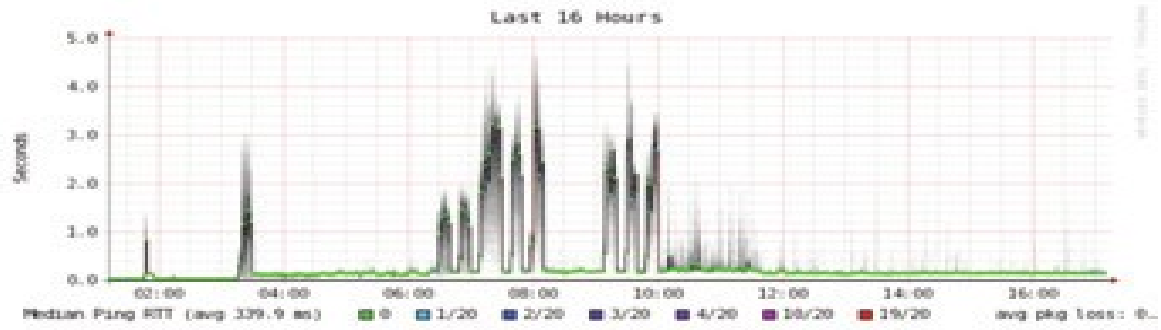
Gambar 6.18: Sebuah grafik arus umum oleh Flowc.

Celah besar di data mungkin menunjukkan sebuah gangguan listrik di jaringan. Trending tools biasanya tidak akan memberitahukan anda tentang gangguan listrik, tetapi hanya sekedar

mencata kejadian itu. Untuk diberitahu kalau masalah jaringan terjadi, gunakan sebuah alat monitor realtime seperti Nagios (lihat **Halaman 200**).

SmokePing

http://oss.oetiker.ch/smokeping/. ***SmokePing*** adalah sebuah alat pengukur latency mewah ditulis di Perl. Ia dapat mengukur, menyimpan dan menampilkan latensi, distribusi latensi dan paket loss semua dalam satu grafik. SmokePing menggunakan RRDtool untuk penyimpanan data, dan bisa menggambar grafik yang sangat informatif yang ditampilkan sampai informasi sangat rinci mengenai status koneksi jaringan anda. Sangat berguna jika menjalankan SmokePing pada host dengan konektivitas baik ke seluruh jaringan anda. Seiring waktu, trends yang dikeluarkan dapat menunjukkan ke berbagai macam masalah jaringan. Digabung dengan MRTG (lihat **Halaman 190**) atau Cacti (lihat **Halaman 192**), anda dapat mengawasi efek kepadatan jaringan pada packet loss dan latensi. SmokePing mempunyai opsi untuk enyiagakan anda kalau syarat tertentu terpenuhi, seperti kalau packet loss berlebihan dilihat di sebuah link untuk waktu yang lama. Contoh SmokePing dalam aksinya ditunjukkan di **Gambar 6.19.**



Gambar 6.19: SmokePing bisa menampilkan packet loss dan penyebaran latensi dalam satu grafik.

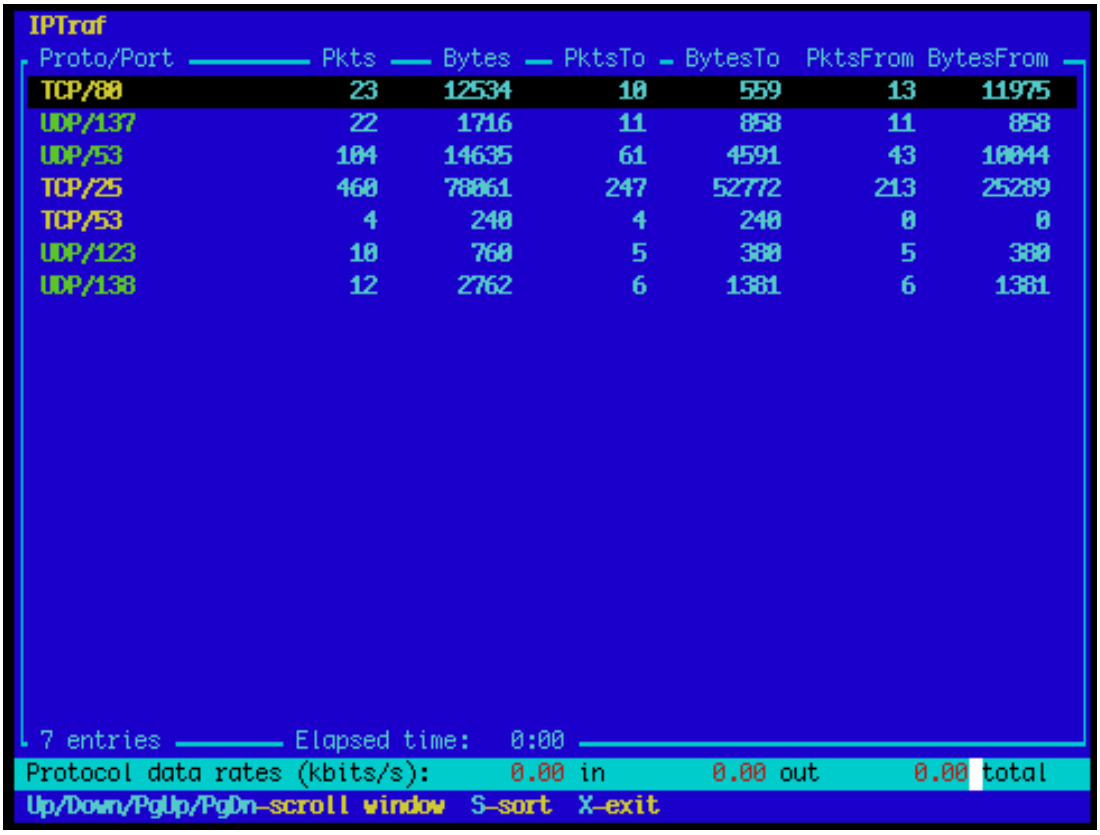
EtherApe

http://etherape.sourceforge.net/. **EtherApe** menampilkan sebuah representasi grafik dari trafik jaringan. Host dan sambungan akan berubah ukuran tergantung dari besarnya trafik yang terkirim dan diterima. Warna berganti untuk melambangkan protokol paling banyak digunakan. Seperti dengan wireshark dan tcpdump, data bisa diambil "off the wire" dari koneksi jaringan hidup atau membaca dari file tangkapan tcpdump.

EtherApe tidak memberikan sebanyak perincian seperti ntop, tetapi syarat sumber dayanya lebih ringan.

iptraf

http://iptraf.seul.org/. **IPTraf** adalah monitor LAN yang ringan tetapi powerful. Ia mempunyai interface ncurses dan jalan di sebuah command shell. IPTraf memerlukan waktu untuk mengukur trafik yang diamati, dan lalu menampilkan berbagai statistik jaringan termasuk koneksi TCP dan UDP, ICMP dan informasi OSPF, arus trafik, IP checksum kesalahan, dan lebih banyak lagi. Sederhana untuk menggunakan program yang memakai sumber daya sistem minimal. Biarpun tidak menyimpan data sejarah, ia sangat berguna karena menampilkan laporan penggunaan seketika itu juga.



Gambar 6.20: iptraf mengelompokkan trafik sesuai .

Argus

http://qosient.com/argus/. ***Argus*** adalah singkatan dari ***Audit Record Generation and Utilization System.*** Argus adalah nama dari salah satu dewa mitologi Yunani yang memiliki beratus-ratus mata.

Dari website argus:

> *Argus menghasilkan statistik aliran seperti seperti konektifitas, kapasitas, permintaan, loss, delay, dan jitter per basis transaksi. Argus digunakan untuk menganalisa dan melaporkan isi dari file paket yang di tangkap atau bisa dijalankan untuk terus menerus memonitor, memeriksa data dari interface yang hidup; mengeluarkan catatan audit untuk semua aktivitas jaringan yang dilihat di packet stream. Argus dapat dipasang untuk memonitor masing-masing sistem, atau seluruh aktivitas jaringan sebuah perusahaan. Saat memonitor terus-menerus, Argus menyediakan data handling model push dan pull, yang memungkinkan strategi yang fleksibel untuk mengumpulkan audit data jaringan. Klien data Argus mendukung banyak operasi, seperti pengelompokkan, penjumlahan, pengarsipan dan pelaporan.*

Argus terdiri dari dua bagian: sebuah kolektor master yang membaca paket dari sebuah alat jaringan, dan sebuah klien yang berhubungan dengan master dan menampilkan statistik penggunaan. Argus beroperasi di BSD, Linux, dan kebanyakan sistem UNIX lain.

NeTraMet

http://freshmeat.net/projects/netramet/. ***NeTraMet*** adalah alat analisa aliran yang populer. Seperti Argus, NeTraMet terdiri atas dua bagian: sebuah kolektor yang mengumpulkan statistik via SNMP, dan sebuah manajer yang menetapkan aliran mana yang sebaiknya diamati. Aliran ditetapkan menggunakan bahasa progamming yang sederhana yang menetapkan alamat yang dipakai di kedua akhiran, dan bisa memasukkan Ethernet, IP, informasi protokol, atau identifier lain. NeTraMet jalan di DOS dan kebanyakan sistem UNIX, termasuk Linux dan BSD.

Pengujian throughput

Secepat apakah jaringan bisa berjalan? Berapakah kapasitas sebenarnya yang dapat digunakan di sebuah sambungan jaringan? Anda bisa mendapat perkiraan kapasitas throughput anda dengan cara membanjiri sambungan anda dengan trafik dan mengukur berapa lama waktu yang diperlukan untuk mentransfer data.

Gambar 6.21: Tool seperti SpeedTest.net sangat bagus, tetapi tidak selalu memberi anda gambaran tepat dari kinerja jaringan.

Biarpun ada halaman web yang tersedia yang akan melakukan “speed test” di browser anda (seperti *http://www.dslreports.com/stest* atau *http://speedtest.net/*), tes ini semakin tak tepat jika jaringan anda semakin jauh dari sumber tes. Lebih jelek lagi, mereka tidak mengijinkan anda menguji kecepatan pada sambungan tertentu, tetapi hanya kecepatan link anda ke tempat tertentu di Internet. Berikut adalah sedikit tool yang memungkinkan anda melakukan tes throughput atas jaringan anda sendiri.

ttcp

http://ftp.arl.mil/ftp/pub/ttcp/. Merupakan software standard di banyak sistem Unix, ttcp adalah sebuah tool sederhana untuk pengujian kinerja jaringan. Untuk melakukan tes kita harus menjalankan ttcp di ke dua sisi sambungan yang ingin anda uji. Node yang pertama berjalan di mode receive, dan yang lain akan transmit:

```
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
```

Sesudah mengambil data di satu arah, anda sebaiknya mengganti mesin yang transmit dengan yang receive untuk menguji hubungan di arah yang lain. Ia dapat menguji stream UDP serta TCP, dan bisa mengubah berbagai parameter TCP dan panjang buffer untuk memberi jaringan sebuah latihan yang baik. Ia bahkan bisa menggunakan data stream dari user daripada mengirim data acak. Ingat bahwa kecepatan readout ada dalam kilobyte, bukan kilobit. Kalikan hasilnya dengan 8 untuk menemukan kecepatan di kilobit per detik. Satu-satunya kerugian untuk ttcp adalah bahwa ia tidak dikembangkan selama bertahun-tahun. Untungnya, kodenya sudah dikeluarkan ke public domain dan bisa diambil dengan leluasa. Seperti ping dan traceroute, ttcp adalah alat standar di banyak sistem.

iperf

http://dast.nlanr.net/Projects/Iperf/. Seperti ttcp, **iperf** adalah sebuah tool command line untuk memperkirakan throughput sebuah sambungan jaringan. Ia mendukung banyak fitur yang sama seperti ttcp, tetapi menggunakan model“client” dan “server” daripada pasangan “receive” dan “transmit”. Untuk menjalankan iperf, jalankan sebuah server di satu sisi dan sebuah klien di sisi yang lain:

```
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
```

Sisi server akan terus mendengarkan dan menerima sambungan klien di port 5001 sampai anda menekan control-C untuk menghentikannya. Ini bisa membuatnya berguna ketika menjalankan beberapa test sekaligus dari berbagai jenis lokasi.

Perbedaan terbesar antara ttcp dan iperf adalah iperf masih dikembangkan, dan punya banyak fitur baru (termasuk sokongan IPv6). Ini membuatnya sebuah pilihan yang bagus untuk dipakai sebagai tool kinerja ketika membuat jaringan baru.

bing

http://fgouget.free.fr/bing/index-en.shtml. Daripada membanjiri koneksi dengan data dan melihat berapa lama transfer dilakukan, **Bing** mencoba menaksir throughput yang tersedia dari koneksi point-to-point dengan menganalisa round trip times untuk berbagai ukuran paket ICMP. Biarpun tidak selalu tepat seperti sebuah tes yang membanjiri sambungan, ia bisa menyediakan perkiraan baik tanpa harus mentransmit banyak byte.

Karena bing menggunakan ICMP echo request yang standar, ia bisa menaksir bandwidth yang tersedia tanpa harus menjalankan sebuah klien istimewa di akhir yang lain, dan bahkan bisa mencoba untuk menaksir throughput dari sebuah link di luar jaringan anda. Karena ia menggunakan bandwidth yang relatif kecil, bing bisa memberi anda gambaran kasar dari kinerja jaringan tanpa harus membajnjiri jaringan.

Tool realtime

Adalah sangat penting untuk mengetahui kapan orang mencoba masuk jaringan anda, atau ketika suatu bagian jaringan sudah gagal. Karena tak ada administrator sistem yang bisa memonitor jaringan terus-menerus, ada program dapat terus memonitor status jaringan dan bisa menyiagakan kalau peristiwa penting terjadi. Berikut adalah beberapa tool open source yang bisa menolong melakukan tugas ini.

Snort

Snort (http://www.snort.org/) adalah sniffer paket dan pencatat yang bisa dipakai sebagai sistem pendeteksi gangguan jaringan yang ringan. Ia mempunyai fitur pencatatan berdasarkan peraturan dan bisa melakukan analisa protokol, pencarian isi, dan pencocokkan paket. Ia bisa dipergunakan untuk mendeteksi berbagai jenis serangan dan probe, seperti stealth port scan, serangan CGI, probe SMB, percobaan fingerprinting OS, dan banyak jenis lain dari pola trafik yang wajar. Snort punya kemampuan penyiagaan realtime yang bisa memberitahu administrator tentang masalah selagi mereka terjadi dengan berbagai jenis metode.

Menginstalasi dan menjalankan Snort tidak sulit, dan bergantung pada banyaknya trafik jaringan, mungkin akan memerlukan mesin yang didedikasikan untuk monitor dengan sumber daya besar. Untungnya, dokumentasi Snort sangat baik dan mempunyai komunitas user yang kuat. Dengan melaksanakan set peraturan Snort menyeluruh, anda bisa mengenali perilaku yang tak diharapkan yang secara misterius akan menghabiskan bandwidth Internet anda.

Lihat *http://snort.org/docs/* untuk daftar lengkap untuk instalasi dan sumber daya konfigurasi.

Apache: mod_security

ModSecurity (*http://www.modsecurity.org/)* adalah sebuah tool open source untuk membuat mesin pendeteksi intrusi dan pencegahan untuk aplikasi web. Jenis alat keamanan ini juga dikenal sebagai sebuah ***web application firewall.*** ModSecurity menambah keamanan aplikasi web dengan melindungi aplikasi web dari serangan yang sudah dan belum dikenal. Ia bisa digunakan sendirian, atau sebagai sebuah modul di Apache web server (*http://www.apache.org/*).

Ada beberapa sumber untuk memperoleh aturan / data mod_security yang terbaru yang akan membantu melindungi dari eksploitasi keamanan terkini. Salah satu sumber daya yang paling bagus adalah GotRoot, yang punya daftar peraturan yang besar dan terus diperbaharui:

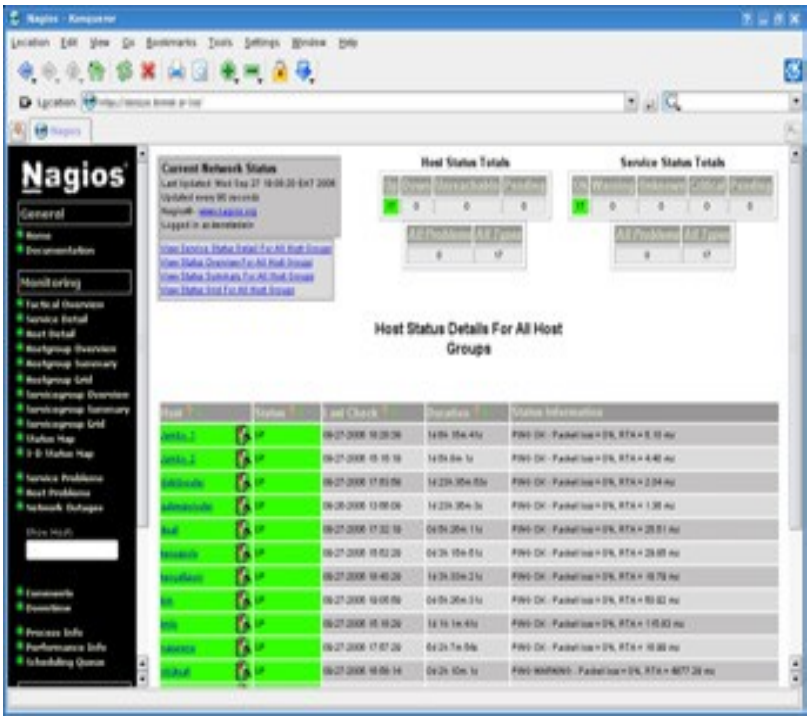
http://gotroot.com/tiki-index.php?page=mod_security+rules

Keamanan aplikasi web penting dalam perlindungan dari serangan di web server, yang bisa menyebabkan pencurian dari data penting atau data pribadi, atau server dipakai untuk menyerang atau mengirim spam ke user Internet lain. Dan juga merusak Internet secara keseluruhan, intrusi seperti ini bisa mengurangi bandwith anda secara drastis.

Nagios

Nagios (*http://nagios.org/*) adalah sebuah program yang memonitor host dan layanan di jaringan anda, memberitahu anda ketika masalah sedang berlangsung. Ia bisa mengirim notifikasi via email, SMS, atau menjalankan sebuah script, dan akan mengirim notifikasi pada seseorang atau suatu grup tergantung pada sifat dari masalah. Nagios berjalan di Linux atau BSD, dan memberikan sebuah interface web untuk menampilkan status sistem terkini.

Nagios dapat dikembangkan, dan dapat memonitor status dari semua peristiwa jaringan. Ia melakukan cek dengan menjalankan sebuah script kecil dengan interval reguler, dan membandingkan hasilnya dengan hasil yang seharusnya di peroleh. Ini dapat memberikan cek yang lebih canggih daripada sebuah probe jaringan sederhana. Misalnya, ping (**halaman 185**) mungkin akan memberitahu anda bahwa mesin sedang berjalan, dan nmap mungkin melaporkan bahwa sebuah port TCP merespon pada sebuah permintaan, tetapi Nagios dapat mengambil halaman web atau membuat sebuah query / permintaan database, dan memverifikasi bahwa respon tersebut bukan sebuah kesalahan.



Gambar 6.22: Nagios langsung memberitahu anda ketika sebuah kesalahan di jaringan atau gangguan layanan jaringan terjadi.

Nagios bahkan bisa memberitahu ketika penggunaan bandwidth, packet loss, suhu ruang, atau indikator kesehatan jaringan lainnya melewati batas tertentu. Ini bisa memberi anda sebuah peringatan awal tentang suatu masalah jaringan, seringkali memperbolehkan anda untuk merespon kepada masalah sebelum user punya kesempatan untuk mengadu.

Zabbix

Zabbix (*http://www.zabbix.org/*) adalah sebuah alat monitor realtime open source yang merupakan suatu gabungan dari Cacti dan Nagios. Ia memakai SQL database untuk penyimpanan data, mempunyai paket pembuat grafik sendiri, dan melakukan semua fungsi yang anda harapkan tool untuk monitor modern secara realtime (seperti polling SNMP dan notifikasi seketika ketika ada masalah). Zabbix menggunakan GNU General Public License.

Alat berguna lainnya

Ada ribuan tool monitor jaringan gratis yang memenuhi suatu kebutuhan khusus. Ini beberapa dari favorit kami yang kurang cocok dimasukkan di kategori diatas.

Driftnet dan Etherpeg.

Alat-alat ini bisa membuka data grafik (seperti file GIF dan JPEG) dan menampilkan mereka sebagai kolase. Seperti disebutkan sebelumnya, alat seperti ini tidak banyak berguna dalam masalah troubleshooting, tetapi sangat penting untuk mendemonstrasikan kelemahan protokol yang tidak terenkripsi. **Etherpeg** tersedia dari *http://www.etherpeg.org/,* dan **Driftnet** bisa di download di *http://www.ex-parrot.com/~chris/driftnet/.*

Gambar 6.23: Sebuah kolase web dibuat oleh Etherpeg.

ngrep

Ngrep menyediakan sebagian besar fitur pencocokan pola GNU grep, tetapi untuk pada trafik jaringan. Sekarang ini ia mengenali IPv4 dan IPv6, TCP, UDP, ICMP, IGMP, PPP, SLIP, FDDI, Token Ring, dan lebih banyak lagi. Karena mereka banyak memakai persamaan ekpresi reguler, ia adalah alat yang cocok untuk user tingkat lanjut atau mereka yang mempunyai pengetahuan baik untuk ekspresi reguler. Tetapi anda tidak perlu menjadi seorang ahli regex untuk bisa menggunakan fungsi dasar ngrep. Misalnya, untuk melihat semua paket yang berisi string GET (diperkirakan permintaan HTTP), coba ini:

```
# ngrep -q GET
```

Pencocokan pola bisa dipaksa mencocokan protokol tertentu, nomor port, atau kriteria lain memakai filter BPF. Ini adalah bahasa filter yang dipakai oleh alat sniffing paket biasa, seperti

tcpdump dan snoop. Untuk melihat GET atau string POST yang terkirim ke port 80, gunakan command line ini:

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

Dengan memakai ngrep secara kreatif, anda bisa mendeteksi apa pun dari aktivitas virus sampai spam email. Anda bisa download ngrep di http://ngrep.sourceforge.net/.

Trafik Normal?

Jika anda sedang mencari jawaban pasti untuk bagaimana pola trafik seharusnya terbentuk, anda akan kecewa. Tidak ada jawaban pasti untuk pertanyaan ini, tetapi dengan mengamati jaringan beberapa lama anda dapat mengetahui apa yang normal untuk jaringan anda. Biarpun semua lingkungan itu berbeda, beberapa faktor yang mempengaruhi pola trafik anda adalah:

- Kapasitas koneksi Internet anda
- Jumlah user yang punya akses ke jaringan anda
- Kebijaksanaan sosial (byte charging, quotas, honor system, dll.).
- Jumlah, jenis, dan level dari layanan yang ditawarkan
- Kesehatan dari jaringan (keberadaan virus, broadcast yang terlalu banyak, routing loops, open email relays, serangan denial of service, dll.).
- Tingkat kepandaian user komputer anda
- Lokasi dan konfigurasi dari struktur pengontrol (firewall, server proxy, caches, dan lainnya)

Ini bukan sebuah daftar yang pasti, tetapi bisa memberi anda gambaran bagaimana banyak faktor bisa mempengaruhi pola bandwidth anda. Dengan memikirkan ini, mari lihat ke topik baselines.

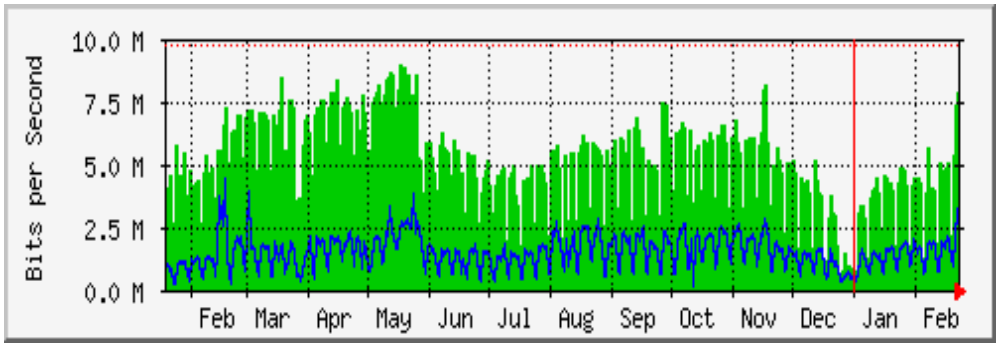
Membangun baseline

Karena semua lingkungan berbeda, anda perlu menentukan sendiri bagaimana bentuk pola trafik anda di situasi normal. Ini berguna karena memungkinkan anda untuk merubah perubahan seiiring waktu, antara tiba-tiba atau bertahap. Perubahan-perubahan ini mungkin akan mengindikasikan sebuah masalah, atau sebuah potensi masalah di masa depan, dengan jaringan anda.

Misalnya, jaringan anda bengong hingga akhirnya berhenti beroperasi,dan anda tidak yakin apa penyebabnya. Untungnya, anda sudah menyimpan sebuah grafik dari broadcast sebagai persentase dari trafik jaringan anda secara keseluruhan. Jika grafik ini menunjukkan tiba-tiba ada pertambahan dari trafik broadcast, ini mungkin berarti jaringan anda terkena virus. Tanpa

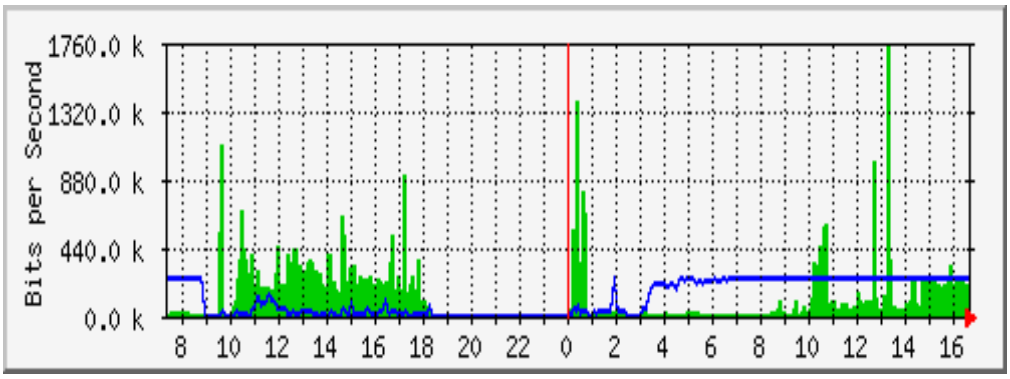
gambaran apa itu "normal" di jaringan anda (sebuah baseline), anda tidak akan bisa melihat kalau jumlah broadcasts sudah menambah, hanya bahwa ia relatif tinggi, yang mungkin tidak akan mengindikasikan masalah.

Grafik baseline dan gambar juga berguna waktu menganalisa efek dari perubahan yang terjadi di jaringan. Seringkali berguna untuk bereksperimen dengan berbagai perubahan tersebut dengan cara mencoba berbagai nilai yang mungkin. Mengetahui bagaimana bentuk baseline akan memperlihatkan anda apakah perubahan anda telah memperbaiki masalah, atau membuat mereka lebih jelek.



Gambar 6.24: Dengan mengumpulkan data dalam jangka waktu yang lama, anda dapat memperkirakan perkembangan dari jaringan anda dan membuat perubahan sebelum masalah berkembang.

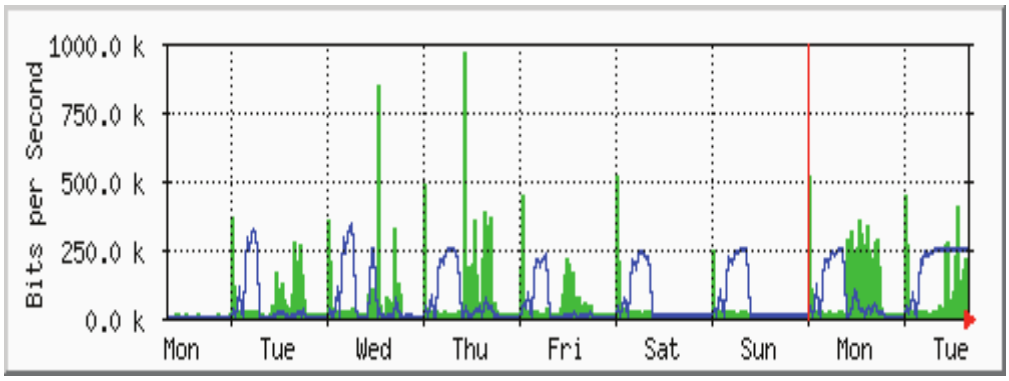
Di **Gambar 6.24**, kita melihat efek dari implementasi delay pool pada penggunaan Internet di sekitar bulan Mei. Jika kita tidak menyimpan grafik dari pengguanaan, kita tidak akan pernah tahu apa efek dari perubahan dalam jangka waktu yang lama. Ketika melihat sebuah grafik dari trafik total setelah melakukan perubahan, Jangan berasumsi kalau usahamu sia-sia jika grafiknya tidak berubah secara radikal. Anda mungkin sudah menghilangkan penggunaan tidak karuan dari saluran anda untuk digantikan dengan trafik sah yang baik. Anda kemudian bisa menggabungkan baseline ini dengan yang lain, misalnya 100 top site yang diakses atau penggunaan rata-rata oleh dua puluh user teratas anda, untuk melihat bahwa kebiasaan mereka berubah. Seperti yang akan kita lihat nanti, MRTG, RRDtool, dan Cacti adalah alat bagus yang bisa anda gunakan untuk menyimpan baseline.



Gambar 6.25: Trend trafik di Aidworld di catat selama satu hari.

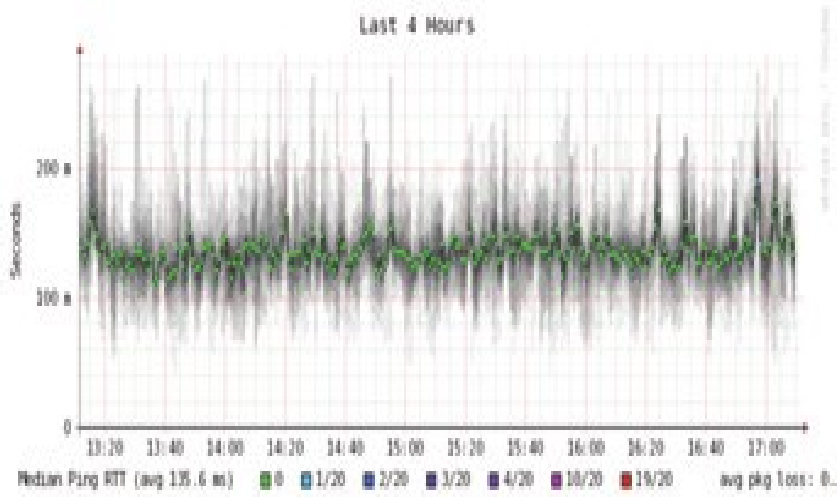
Gambar 6.25 memperlihatkan trafik di sebuah firewall Aidworld dalam sebuah periode 24 jam. Tidak ada yang kelihatan aneh di grafik ini, tetapi para user komplain akses internet lambat.

Gambar 6.26 memperlihatkan bahwa penggunaan bandwidth upload (area gelap) lebih tinggi pada jam kerja di hari terakhir dibanding hari-hari sebelumnya. Sebuah periode penggunaan upload berat dimulai setiap pagi pada 03:00, dan biasanya selesai pada 09:00, tetapi pada hari terakhir ia masih berjalan sampai 16:30. Investigasi lebih lanjut memperlihatkan masalah pada software backup, yang berjalan pada 03:00 setiap hari.



Gambar 6.26: Jaringan yang sama dicatat selama seminggu penuh memperlihatkan masalah dengan backup, yang membuat kepadatan jaringan tidak diharapkan oleh user jaringan.

Gambar 6.27 menampilkan pengukuran dari latensi pada sambungan yang sama yang diukur oleh program SmokePing. Posisi dari titik menampilkan latensi rata-rata, sementara asap abu-abu menampilkan distribusi latensi (jitter). Warna dari titik mengindikasikan jumlah dari paket yang hilang. Grafik ini pada sebuah periode empat jam tidak membantu mengidentifikasi adanya masalah di jaringan.

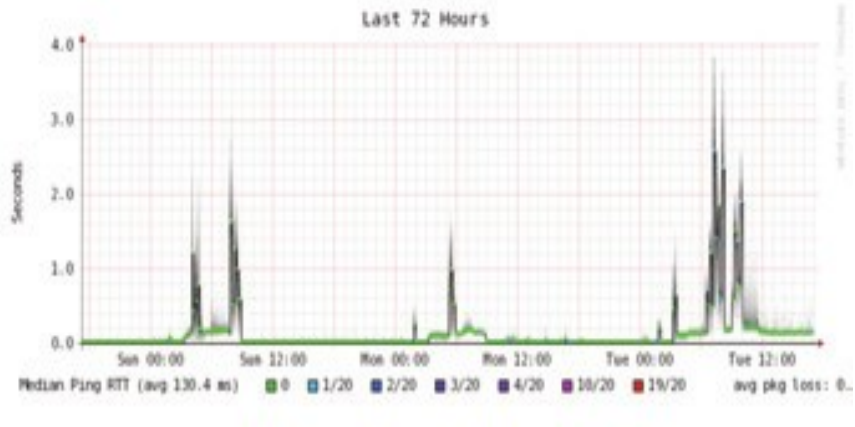


Gambar 6.27: Empat jam jitter dan packet loss.

Grafik berikutnya (**Gambar 6.28**) menampilkan data yang sama dalam sebuah periode 16 jam. Ini mengindikasikan bahwa nilai di grafik di atas dekat dengan level normal (baseline), tetapi bahwa ada pertambahan signifikan di latensi pada beberapa waktu ketika pagi, sampai 30 kali nilai baseline. Ini mengindikasikan bahwa monitoring tambahan seharusnya dilakukan pada periode awal pagi untuk mengetahui penyebab dari latensi tinggi, yang mungkin adalah suatu macam trafik besar.

Gambar 6.28: Sebuah penyebaran tinggi jitter dibuka pada pencatatan 16 jam.

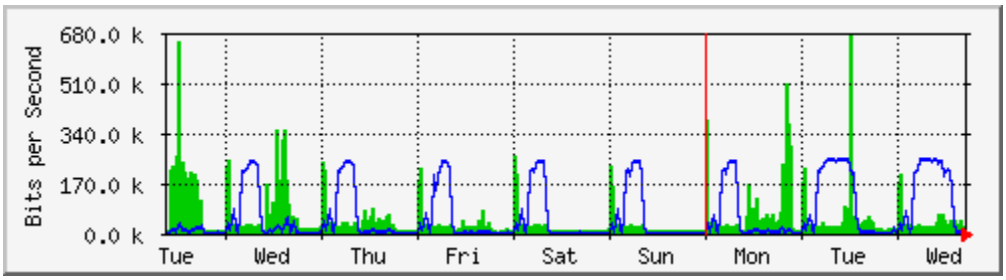
Gambar 6.29 menampilkan bahwa Selasa lebih parah daripada Minggu atau Senin untuk latensi, khususnya pada saat periode awal pagi. Ini mungkin mengindikasikan bahwa sesuatu telah berubah di jaringan.



Gambar 6.29: Zoom pada catatan satu minggu menunjukkan repitisi penambahan latensi dan packet loss di pagi hari.

Bagaimana saya menginterpretasi grafik trafik?

Pada grafik aliran jaringan sederhana (seperti yang dikeluarkan oleh monitor jaringan MRTG), area hijau mengindikasikan ***trafik inbound,*** sementara garis biru mengindikasikan ***trafik outbound.*** Trafik inbound adalah trafik yang berasal dari jaringan lain (biasanya Internet) dan dialamatkan ke komputer di dalam jaringan anda.Trafik outbound adalah trafik yang berasal dari jaringan anda, dan dialamatkan ke komputer disuatu tempat di Internet. Tergantung pada lingkungan jaringan seperti apa yang anda punya, grafik ini akan membantu anda untuk mengerti bagaimana sebuah jaringan benar-benar dipakai. Misalnya, monitoring dari server biasanya menampilkan lebih banyak trafik outbound ketika server merespon pada permintaan (seperti mengirim surat atau melayani halaman web), sementara monitoring
mesin klien mungkin akan menampilkan trafik inbound yang lebih banyak pada mesin ketika mereka mendapat data dari server.



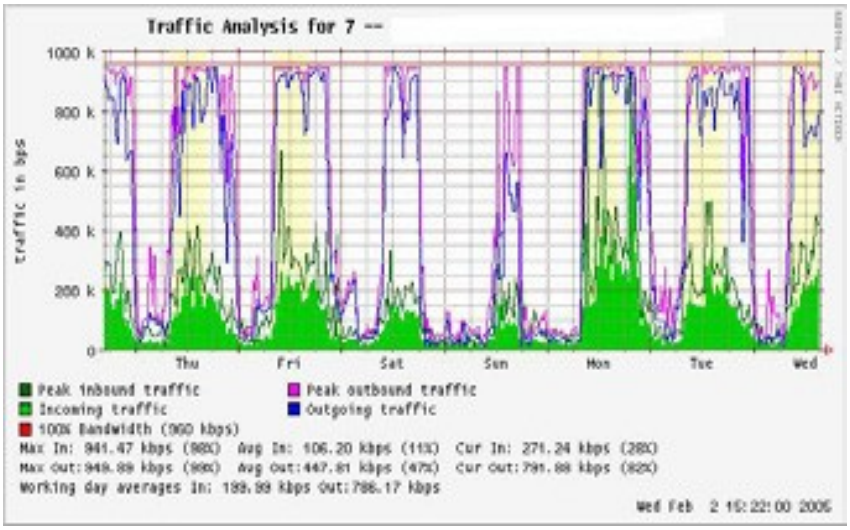
Gambar 6.30: Grafik aliran trafik di jaringan. Area gelap merepresentasikan trafik inbound, sementara garis merepresentasikan trafik outbound. Kurva berulang pada trafik outbound

terjadi ketika backup tiap malam berjalan.

Pola trafik akan bervariasi dengan apa yang sedang anda monitor. Sebuah router biasanya akan menampilkan lebih banyak trafik datang daripada trafik keluar ketika user mendownload data dari Internet. Bandwidth outbound yang berlebihan yang tidak di transmit oleh server jaringan anda bisa mengindikasikan sebuah klien peer-to-peer, server tidak sah, atau bahkan sebuah virus di satu atau lebih klien anda. Tidak ada set acuan yang mengindikasikan bentuk seharusnya dari trafik keluar dan trafik masuk. Tergantung anda untuk membuat sebuah baseline untuk mengerti bagaimana bentuk dari pola trafik jaringan normal di jaringan anda.

Mendeteksi overload di jaringan

Gambar 6.31 menampilkan trafik di sebuah sambunganInternet yang terlalu penuh.

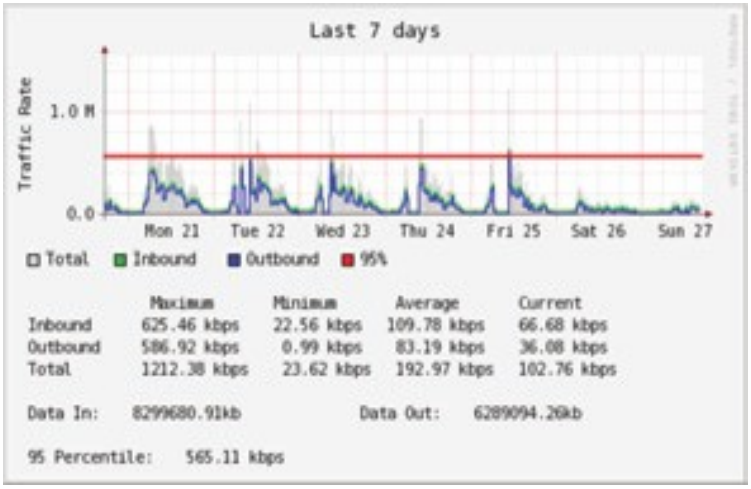


Gambar 6.31: Grafik dengan trafik yang flat-topped mengindikasikan bahwa sebuah saluran sedang menggunakan bandwith maksimum yang tersedia, dan terlalu banyak dipakai pada waktu tersebut.

Tanda yang paling terlihat dari overloading adalah flat top pada trafik outbound di tengah hari setiap hari. Flat top bisa mengindikasikan overloading, bahkan jika mereka masih berada dibawah dari kapasitas maksimum dari sambungan menurut teori. Dalam kasus ini ia mungkin mengindikasikan bahwa anda tidak mendapat bandwith dari service provider sebanyak yang mereka janjikan.

Mengukur 95 persen

95 persen adalah sebuah kalkulasi matematik yang banyak dipakai untuk mengevaluasi penggunaan biasa dari pipa jaringan. Nilainya menampilkan konsumsi trafik paling tinggi dari suatu periode. Mengkalkulasi 95 persen berarti 95% dari penggunaan ada dibawah suatu nilai, dan 5% dari waktu penggunaan ada di atas nilai itu. 95 persen adalah sebuah nilai baik untuk digunakan untuk menampilkan bandwith sebenarnya dipakai setidaknya 95%.



Gambar 6.32: Garis horizontal menampilkan nilai 95 persen.

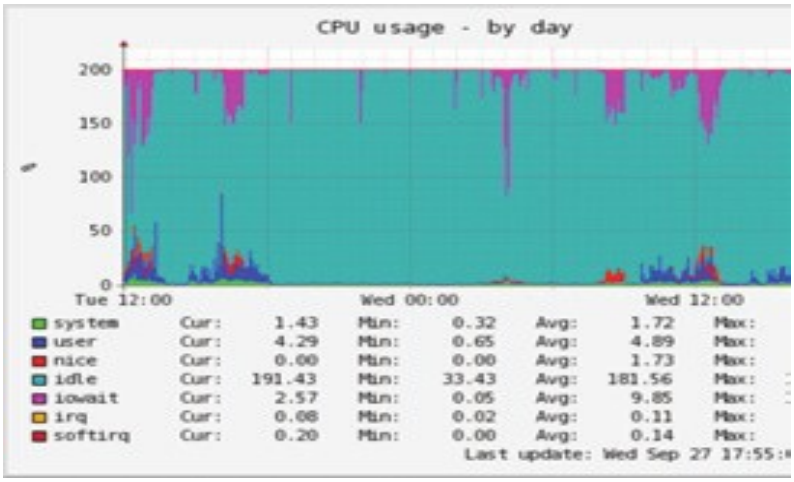
MRTG dan Cacti akan mengkalkulasi 95 persen untuk anda. Ini adalah contoh grafik dari koneksi 960 kbps. 95 persen berada pada 945 kbps setelah membuang 5% trafik tertinggi.

Monitoring Penggunaan RAM dan CPU

Menurut definisi, server menyediakan layanan penting yang seharusnya selalu tersedia. Server menerima dan merespon pada permintaan mesin klien, memberi akses pada servis yang merupakan tujuan utama mempunyai sebuah jaringan. Maka, server harus punya kemampuan hardware yang cukup untuk mengakomodasi beban kerja. Ini berarti mereka harus punya RAM, storage, dan kemampuan processing yang sesuai untuk mengakomodasi permintaan klien. Kalau tidak, server akan merespon terlalu lama, atau di kasus yang paling buruk, tidak bisa merespon sama sekali. Karena sumber daya hardware terbatas, penting untuk mencatat bagaimana sumber daya sistem sedang dipakai. Jika sebuah core server (Seperti sebuah server proxy atau server email) sedang terbanjiri oleh permintaan, waktu akses menjadi lambat. Ini biasanya dianggap sebagai sebuah masalah jaringan oleh user.

Ada beberapa program yang bisa dipakai untuk memonitor sumber daya di sebuah server. Metode paling sederhana di sebuah mesin Window adalah melihat Task Manager

menggunakan **Ctrl Alt + Del**, lalu klik tab Performance. Di sebuah Linux atau BSD box, anda mengetik top di sebuah terminal. Untuk menyimpan catatan sejarah dari kinerja itu, MRTG atau RRDtool (di **Halaman 190**) bisa juga dipakai.



Gambar 6.33: RRDtool bisa menampilkan data sembarang, seperti penggunaan memory dan CPU, diekspresikan sebagai sebuah rata-rata seiring waktu.

Mail server memerlukan space yang sesuai, karena beberapa orang lebih suka meninggalkan email mereka di server untuk waktu yang lama. Surat-surat ini bisa terakumulasi dan memenuhi hard disk, khususnya jika quotas tidak diaktifkan. Jika disk atau partisi yang terpakai untuk penyimpanan surat terpenuhi, mail server tidak bisa menerima surat. Jika disk itu juga dipakai oleh sistem, semua jenis masalah sistem bisa terjadi karena sistem operasi kehabisan swap space dan temporary storage.

File server perlu di monitor, bahkan jika mereka punya disk yang besar. User akan mencari cara untuk memenuhi disk ukuran apapun lebih cepat dari yang anda pikir. Penggunaan disk bisa dipaksakan melalui pengunaan quota, atau secara sederhana memonitor penggunaan dan memberitahu orang-orang ketika mereka menggunakan terlalu banyak. Nagios (lihat **Halaman 200**) bisa memberitahu anda ketika penggunaan disk, utilisasi CPU, atau sumber daya sistem lainnya melewati batas kritis.

Jika sebuah mesin menjadi tidak merespon dan lambat, dan pengukuran menunjukkan bahwa sebuah sumber daya sistem sering sekali dipakai, ini mungkin sebuah indikasi bahwa sebuah upgrade dibutuhkan. Jika penggunaan processor sering melewati 60% dari total, ini mungkin waktu untuk mengupgrade processor. Kecepatan menjadi lambat bisa juga karenai RAM yang tidak cukup. Ceklah penggunaan keseluruhan dari CPU, RAM, dan disk space sebelum memutuskan untuk mengupgrade sebuah komponen tertentu.

Cara sederhana untuk mengecek apakah sebuah mesin punya RAM yang cukup adalah melihat ke lampu hard disk. Ketika lampunya sering menyala, ini biasanya berarti mesinnya sering menukar sejumlah data yang besar dari dan ke disk. Ini dikenal sebagai ***thrashing,***

dan sangat buruk untuk kinerja. Ini biasanya bisa dibetulkan dengan menginvestigasi proses mana yang paling banyak memakai RAM, dan mematikan atau mengkonfigurasi ulang proses itu. Jika gagal juga, berarti sistem butuh RAM yang lebih banyak.

Anda seharusnya selalu menentukan apakah lebih bagus menupgrade sebuah komponen atau membeli sebuah mesin baru. Beberapa komputer susah atau tidak mungkin di upgrade, dan biasanya membutuhkan biaya lebih untuk mengganti komponen indivual daripada mengganti sistem keseluruhan. Karena ketersediaan bagian-bagian dan sistem berbeda-beda di seluruh dunia, selalu bandingkan harga komponen vs. seluruh sistem, termasuk ongkos pengantaran dan pajak, ketika menentukan harga mengupgrade.

Bab 7 Pembangkit Listrik Tenaga Surya

Bab ini memperkenalkan komponen dari photovoltaic sistem yang mandiri (***stand-alone photovoltaic system***). Kata mandiri merujuk pada kenyataan bahwa sistem tersebut berfungsi tanpa ada sambungan jaringan daya manapun yang sudah ada. Di bab ini, kami akan memberikan konsep dasar pembangkitan dan penyimpanan daya surya photovoltaic. Kami juga akan menyediakan metode untuk mendesain sistem surya fungsionil dengan akses terbatas terhadap informasi dan sumber daya.

Bab ini hanya membicarakan penggunaan daya surya untuk produksi langsung listrik (***energi surya photovoltaic*** atau ***solar energy photovoltaic***). Daya surya juga bisa digunakan untuk memanaskan cairan (***energi panas surya*** atau ***thermal solar energy***) yang kemudian dapat digunakan sebagai sumber panas atau untuk memutar turbin untuk membangkitkan listrik. Sistem daya surya termal diluar pembahasan bab ini.

Energi surya

Sistem Photovoltaic berbasis pada kemampuan bahan tertentu untuk mengubah energi cahaya matahari menjadi daya listrik. Jumlah daya surya yang menyalakan suatu area tertentu diketahui sebagai penyinaran atau ***irradiance (G)*** dan diukur dalam ***watt per meter persegi (W/m2).*** Nilai seketika itu biasanya dirata-rata dalam suatu periode waktu, sehingga biasa disebut total penyinaran per jam, hari atau bulan.

Tentunya, jumlah radiasi yang akurat yang tiba di permukaan bumi tidak bisa diperkirakan dengan keakuratan yang tinggi, karena variasi cuaca alami. Oleh karena itu perlu untuk bekerja dengan data statistik berdasarkan "sejarah surya" pada suatu tempat. Data ini dikumpulkan oleh kantor pengamat cuaca dalam jangka waktu yang lama dan tersedia dari sejumlah sumber, berupa tabel atau database. Di kebanyakan kasus, bisa sulit menemukan informasi terperinci mengenai suatu daerah tertentu, dan anda harus bekerja dengan nilai perkiraan.

Beberapa organisasi sudah menghasilkan peta yang meliputi nilai rata-rata penyinaran global sehari-hari untuk daerah yang berbeda. Nilai ini diketahui sebagai Waktu Puncak Matahari atau ***Peak Sun Hours*** atau ***PSH***. Anda bisa mempergunakan nilai PSH untuk daerah anda untuk menyederhanakan perhitungan anda. Satu kesatuan "tertinggi matahari" berhubungan dengan radiasi sebanyak 1000 Watt semeter persegi. Jika kita menemukan daerah tertentu itu mempunyai 4 PSH yang terburuk di antara bulan-bulan, itu berarti bahwa pada bulan itu kita sebaiknya tidak mengharapkan penyinaran harian lebih besar daripada 4000 W/m2 (hari). Penggunaan waktu matahari tertinggi adalah cara mudah untuk melambangkan rata-rata kasus penyinaran sehari yang paling buruk.

Peta PSH beresolusi rendah tersedia dari sejumlah sumber online, seperti *http://www.solar4power.com/solar-power-global-maps.html.* Untuk informasi yang lebih terperinci, konsultasikan dengan vendor lokal energi surya atau pengamat cuaca lokal.

Bagaimana dengan tenaga angin?

Adalah mungkin untuk menggunakan pembangkit listrik daya angin sebagai pengganti panel surya ketika sistem mandiri sedang didesain untuk instalasi di bukit atau gunung. Untuk menjadi efektif, kecepatan angin rata-rata dalam setahun sebaiknya sedikitnya 3 sampai 4 meter per detik, dan pembangkit listrik daya angin sebaiknya 6 meter lebih tinggi daripada benda lain dalam jarak 100 meter. Lokasi yang jauh dari pantai biasanya kurang cukup daya angin untuk mendukung sistem berdaya angin.

Secara umum, sistem photovoltaic lebih dapat diandalkan daripada pembangkit listrik daya angin, karena sinar matahari lebih tersedia daripada angin yang konsisten di kebanyakan tempat. Di sisi lain, pembangkit listrik berdaya angin dapat meng-charge baterai bahkan pada malam hari, selama ada angin yang cukup. Tentu saja mungkin untuk menggunakan angin bersama daya surya untuk membantu pada saat ada keadaan yang berawan, atau pada saat angin tidak cukup.

Untuk kebanyakan lokasi, biaya pembangkit listrik daya angin yang baik tidak dijustifikasi dengan sedikitnya daya yang ditambahkannya ke keseluruhan sistem. Bab ini maka akan fokus pada penggunaan panel surya untuk membangkitkan listrik.

Komponen sistem Photovoltaic

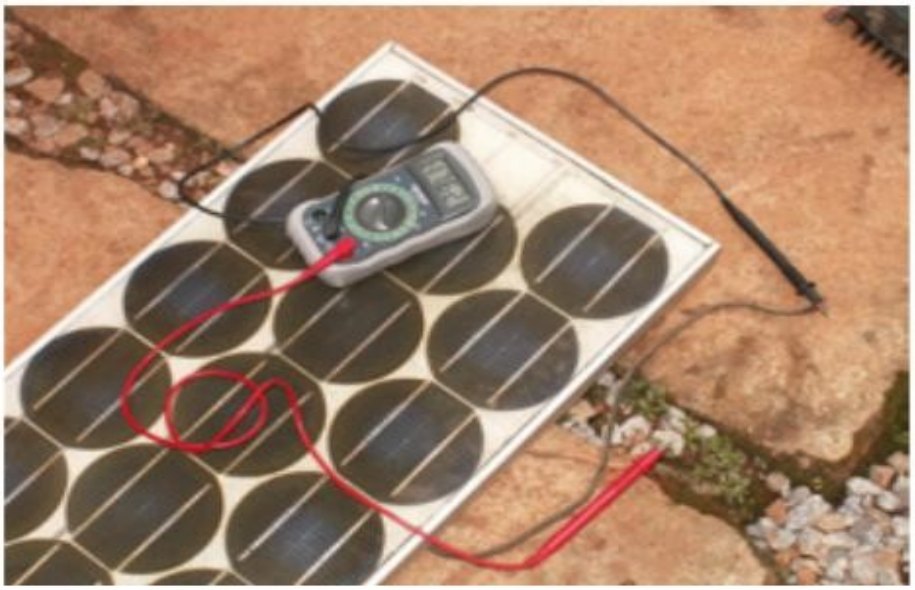
Dasar sistem photovoltaic terdiri dari empat komponen utama: ***panel surya (solar panel), baterai (batteries)***, ***regulator***, dan ***beban (load)***. Panel bertanggung jawab untuk mengumpulkan daya matahari dan membangkitkan listrik. Baterai menyimpan daya listrik untuk penggunaannya nanti. Regulator menjamin panel dan baterai bekerja sama dalam model optimal. Beban merujuk pada alat apapun yang memerlukan daya listrik, dan merupakan jumlah konsumsi listrik dari semua peralatan listrik yang dihubungkan dengan sistem. Penting untuk diingat bahwa panel surya dan baterai menggunakan ***arus searah*** atau ***direct current (DC).***

Jika jangkauan tegangan operasional peralatan anda tidak cocok dengan tegangan yang disediakan oleh baterai anda, anda perlu menggunakan ***converter*** untuk menyesuaikan tegangan. Jika peralatan anda menggunakan tegangan yang berbeda dengan tegangan baterai, anda perlu mengunakan ***konverter DC/DC (DC/DC converter).*** Jika sebagian dari peralatan anda memerlukan tegangan AC, maka anda perlu menggunakan ***konverter DC/AC (DC/AC converter)***, yang juga dikenal sebagai ***inverter***.

Setiap sistem daya listrik sebaiknya memasukkan berbagai alat keamanan untuk mengantisipasi kekacauan. Alat ini meliputi perkabelan yang baik, sekering, proteksi perubahan tegangan (surge protector), sekering, pentanahan, penangkal petir, dll.

Panel surya

Panel surya (solar panel) terdiri dari sel surya yang mengumpulkan radiasi surya dan mengubahnya menjadi daya listrik. Bagian sistem ini kadang-kadang dinamakan ***modul surya (solar module)*** atau ***pembangkit listrik daya photovoltaic (photovoltaic generator)***. ***Sekumpulan panel surya*** dapat dibuat dengan menyambung sekumpulan panel dalam serial dan/atau paralel untuk menyediakan daya yang diperlukan untuk beban yang ada. Arus listrik yang disediakan oleh panel surya bervariasi secara proporsional terhadap radiasi surya. Ini akan bervariasi menurut kondisi iklim, jam, dan waktu pada suatu tahun.



Gambar 7.1: Panel surya (Solar panel)

Beberapa teknologi dapat digunakan dalam pembuatan sel surya. Yang paling banyak digunakan adalah kristal silicon, dan dapat berupa baik monocrystalline atau polycrystalline. Silikon amorphous (Amorphous silicon) bisa lebih murah tetapi lebih tidak efisien untuk mengubah daya surya ke listrik. Dengan waktu hidup yang berkurang dan efisiensi transformasi 6 sampai 8%, amorphous silicon biasanya digunakan untuk peralatan berdaya rendah, seperti kalkulator yang mudah dibawa. Teknologi surya baru, seperti silicon ribbon dan photovoltaics film tipis, sekarang ini dalam perkembangan. Teknologi ini menjanjikan efisiensi yang lebih tinggi tetapi belum tersedia secara luas.

Baterai

Baterai menyimpan daya yang dihasilkan oleh panel surya yang tidak segera digunakan oleh beban. Daya yang disimpan dapat digunakan saat periode radiasi matahari rendah. Komponen baterai kadang-kadang dinamakan ***akumulator (accumulator).*** Baterai menyimpan listrik dalam bentuk daya kimia. Baterai yang paling biasa digunakan dalam aplikasi surya adalah ***baterai yang bebas pemeliharaan bertimbal asam (maintenance-free lead-acid batteries)***, yang juga dinamakan baterai ***recombinant*** atau ***VRLA (klep pengatur asam timbal*** atau ***valve regulated lead acid).***

Gambar 7.2: Sebuah baterai bertimbal asam Ah 200. Terminal negatif rusak karena berat pada terminal selama transportasi.

Disamping menyimpan daya, baterai-baterai bertimbal asam yang disekat juga melayani dua fungsi penting:

- Mereka dapat menyediakan daya seketika yang lebih kuat dibandingkan dengan apa yang dihasilkan oleh sekumpulan panel. Daya seketika ini diperlukan untuk memulai beberapa peralatan, seperti mesin kulkas atau pompa.
- Mereka menentukan tegangan operasi instalasi anda

Untuk instalasi daya kecil dan dimana keterbatasan ruang penting, jenis baterai lainnya (seperti NiCd, NiMh, atau Li-ion) dapat digunakan. Baterai seperti ini memerlukan

charger/regulator yang khusus dan tidak dapat secara langsung digunakan untuk menggantikan baterai bertimbal asam.

Regulator

Pengatur / Regulator (atau lebih formalnya ***pengatur penyimpanan daya surya*** atau ***Solar power charge regulator***) memastikan bahwa baterai berkerja dalam kondisi yang seharusnya. Pengatur ini menghindari penyimpanan (charge) atau pengeluaran (discharge) baterai yang berlebihan, yang keduanya sangat merusak umur baterai. Untuk menjamin charging dan discharging baterai yang baik, pengatur tersebut menjaga informasi ***kondisi penyimpanan daya*** (***State of Charge*** atau ***SoC***) baterai. SoC diukur berdasarkan pada tegangan sebenarnya dari baterai. Dengan mengukur tegangan baterai dan diprogram dengan tipe teknologi penyimpanan yang digunakan oleh baterai, pengatur bisa mengetahui titik tepat di mana baterai akan mengalami charge atau discharge yang berlebihan.

Gambar 7.3: Pengontrol penyimpanan daya surya 30 Ampere

Pengatur dapat meliputi fitur lain yang menambahkan informasi berharga dan keamanan kontrol kepada peralatan. Fitur ini termasuk amperemeter, voltmeter, pengukuran ampere-jam, pengatur waktu, alaram, dll. Walaupun terkesan nyaman, tidak satupun dari fitur ini diperlukan untuk photovoltaic sistem yang berfungsi.

Konverter

Listrik yang disediakan oleh sekumpulan panel dan baterai adalah DC pada tegangan yang tetap. Tegangan yang disediakan mungkin tidak sesuai dengan apa yang diperlukan oleh beban anda. Sebuah ***konverter DC/AC***, yang juga dikenal sebagai ***inverter***, mengubah arus DC dari baterai anda menjadi AC. Ini diikuti dengan kehilangan suatu daya selama konversi.

Jika perlu, anda juga dapat menggunakan konverter untuk mendapatkan DC di tingkat tegangan yang berbeda dengan apa yang disediakan oleh baterai. Konverter DC/DC juga kehilangan suatu daya selama konversi. Untuk pelaksanaan optimal, anda sebaiknya mendesain sistem anda yang berdaya surya agar sesuai dengan tegangan DC yang dihasilkan agar sesuai dengan beban.

Gambar 7.4: Sebuah konverter DC/AC 800 Watt (inverter daya)

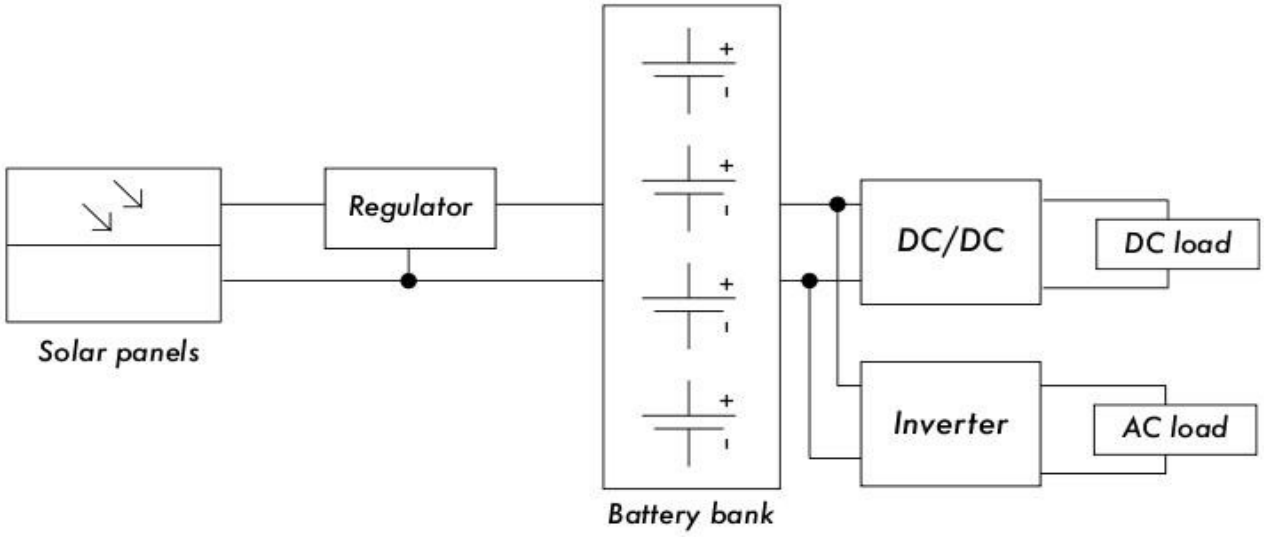
Load

Load adalah peralatan yang mengkonsumsi daya yang dihasilkan oleh sistem daya anda. Beban mungkin termasuk peralatan komunikasi nirkabel, router, meja bekerja, lampu, set TV, modem VSAT, dll. Walaupun tidak mungkin secara persis memperhitungkan jumlah persis konsumsi peralatan anda, sangat penting untuk membuat perkiraan yang baik. Dalam sistem sejenis ini, sangatlah penting untuk mempergunakan peralatan yang efisien dan berdaya rendah untuk menghindari daya yang terbuang.

Menyatukan semua menjadi satu kesatuan

Sistem photovoltaic yang lengkap memasukkan semua dari bagian-bagian ini. Panel-panel surya membangkitkan daya kalau daya surya tersedia. Pengatur memastikan operasi panel-panel yang paling efisien dan mencegah kerusakan terhadap baterai. Bank baterai

mengumpulkan daya untuk penggunaan kemudian. Konverter dan inverter menyesuaikan daya yang disimpan agar sama dengan keperluan beban anda. Akhirnya, beban memakan daya yang disimpan untuk melakukan pekerjaan. Sewaktu semua bagian dalam keseimbangan dan terjaga secara baik, sistem akan dapat mendukung dirinya sendiri bertahun-tahun.



Gambar 7.5: Sebuah instalasi solar dengan beban DC dan AC

Kita sekarang akan melihat lebih dekat setiap komponen photovoltaic secara seksama

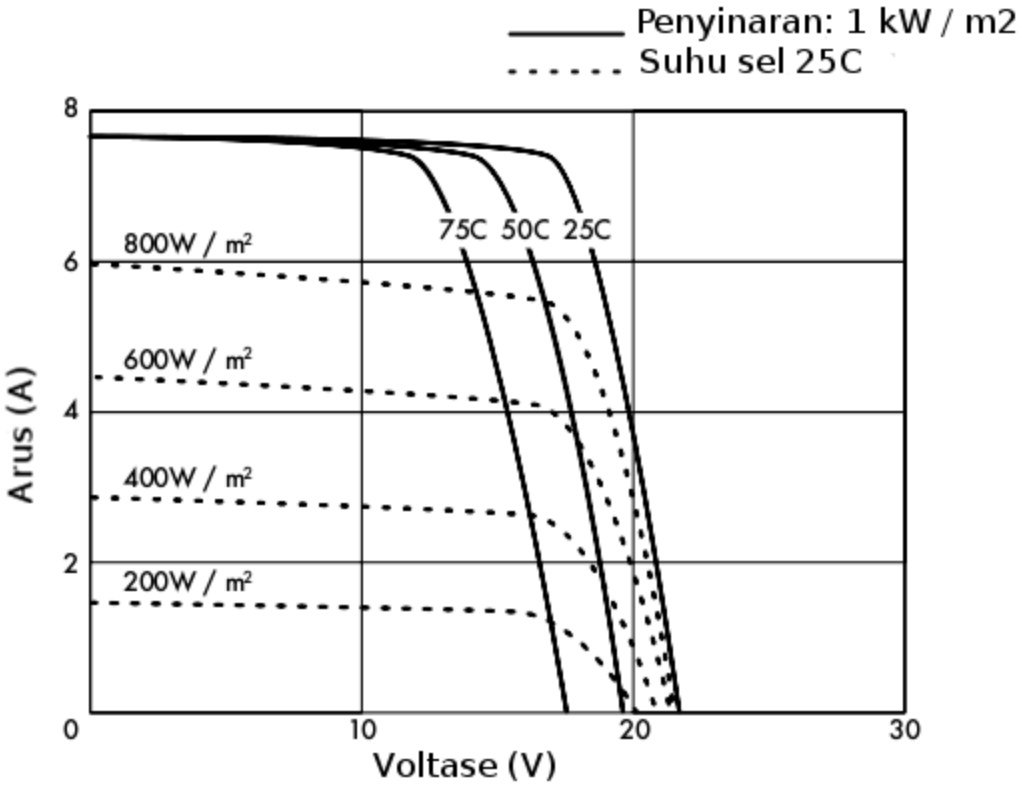
Panel surya

Sebuah panel surya terbuat dari banyak sel surya. Sel tersambung secara elektrik untuk memberikan arus dan tegangan tertentu. Masing-masing sel di enkapsulasi untuk mengisolasi dan melindungi dari kelembaban dan korosi.

Gambar 7.6: akibat dari air dan karat pada panel surya

Ada beda tipe modul yang tersedia di pasaran, tergantung pada kebutuhan daya aplikasi anda. Modul yang paling umum digunakan terbuat dari 32 atau 36 crystalline silicon sel surya. Sel-sel ini berukuran sama, tersambung secara seri, dan terbungkus diantara bahan kaca dan plastik, menggunakan polymer resin (EVA) sebagai insulator termal (thermal insulator). Bagian muka modul biasanya antara 0,1 dan 0,5 m2. Panel surya biasanya memiliki dua kontak listrik, satu positif dan satu negatif.

Beberapa panel menyertakan kontak ekstra yang memungkinkan instalasi ***dioda penyingkat*** atau ***bypass diode*** di antara masing-masing sel. Dioda ini melindungi panel dari gejala yang dikenal sebagai “hot-spots”. Sebuah hot spot terjadi ketika beberapa sel berada dalam bayangan sedangkan sisa panel berada di bawah matahari penuh. Daripada menghasilkan daya, sel yang terteduh bertingkah laku sebagai beban yang membuang daya. Dalam situasi ini, sel yang terteduh dapat mengalami peningkatan suhu yang luar biasa (sekitar 85 sampai 100 derajat Celsius.) Dioda penyingkat akan mencegah hot spot di sel yang terteduh, tetapi mengurangi tegangan maksimum panel. Mereka sebaiknya hanya digunakan kalau peneduhan tak dapat dielakkan. Adalah solusi yang jauh lebih baik untuk menggelar seluruh panel di bawah matahari penuh sebisa mungkin.



Gambar 7.7: Kurva IV yang berbeda. Arus (A) berubah dengan penyinaran, dan voltase (V) berubah dengan suhu

Kinerja modul surya yang direpresentasikan oleh ***kurva karakteristik IV*** atau ***IV characteristic curve***, yang merepresentasikan arus yang disediakan berdasarkan tegangan yang ditimbulkan oleh tingkat radiasi surya tertentu.

Kurva merepresentasikan semua nilai tegangan-arus yang mungkin. Kurva bergantung pada dua faktor utama: suhu dan radiasi surya yang diterima oleh sel. Untuk sebuah area sel surya, arus yang dihasilkan secara langsung sebanding dengan penyinaran surya (G), sedangkan tegangan berkurang dengan kenaikan suhu. Sebuah pengatur yang baik akan berusaha memaksimalkan jumlah daya yang disediakan oleh panel dengan mengikuti titik yang menyediakan daya maksimum (V x I). Daya maksimum berkaitan dengan lutut kurva IV

Parameter panel surya

Parameter utama yang mengkarakterisasi panel photovoltaic adalah:

1. **ARUS SIRKUIT PENDEK** atau **SHORT CIRCUIT CURRENT** (I_{SC}): arus maksimum yang disediakan oleh panel waktu konektor mengalami sirkuit pendek.

2. **TEGANGAN SIRKUIT TERBUKA** atau **OPEN CIRCUIT VOLTAGE** (V_{OC}): tegangan maksimum yang disediakan oleh panel ketika terminal tidak dihubungkan pada beban sama sekali (kontak terbuka). Nilai ini biasanya 22 V untuk panel-panel yang bekerja di sistem 12 V, dan secara langsung proporsional dengan sejumlah sel yang tersambung dalam serial.

3. **TITIK DAYA MAKSIMUM** atau **MAKSIMUM POWER POINT** (P_{max}): titik dimana daya yang disediakan oleh panel berada di titik maksimum, dimana $P_{max} = I_{max} \times V_{max}$. Titik daya maksimum panel diukur dalam Watt (W) atau Watt tertinggi (W_p). Penting untuk tidak lupa bahwa dalam kondisi normal, panel akan tidak dapat bekerja pada kondisi tertinggi, karena tegangan operasi ditetapkan oleh beban atau pengatur. Nilai umum Vmax dan Imax sebaiknya sedikit lebih rendah daripada I_{SC} dan V_{OC}.

4. **FAKTOR PENGISI** atau **FILL FACTOR** (FF): hubungan antara daya maksimum sesungguhnya yang dapat disediakan oleh panel dengan perkalian $I_{SC} \times V_{OC}$. Ini memberikan anda gambaran kualitas panel karena ini adalah indikasi tipe kurva karakteristik IV. Semakin dekat FF kepada 1, semakin banyak daya yang dapat diberikan oleh panel. Nilai umum biasanya berkisar antara 0,7 dan 0,8.

5. **EFISIENSI** atau **EFFICIENCY** (h): rasio antara daya listrik maksimum yang dapat diberikan oleh panel kepada beban dan daya dari radiasi surya ($P_{L)}$ yang masuk ke panel. Ini biasanya sekitar 10-12%, tergantung pada tipe sel (monocrystalline, polycrystalline, amorphous atau film tipis).

Mempertimbangkan definisi titik daya maksimum dan faktor pengisi, kita dapat melihat

bahwa:

$$h = P_{max} / P_L = FF . I_{SC} . V_{OC} / P_L$$

Nilai I_{SC}, V_{OC}, I_{Pmax} dan V_{Pmax} disediakan oleh pabrik dan merujuk pada kondisi standar pengukuran dengan penyinaran G = 1000 W/m^2, pada ketinggian permukaan laut, untuk suhu sel $T_c = 25°C$.

Nilai parameter panel berubah jika penyinaran dan suhu berbeda. Vendor kadang-kadang akan memasukkan grafik atau tabel dengan nilai untuk kondisi yang berbeda dari yang standar. Anda sebaiknya memeriksa nilai kinerja di suhu panel yang mungkin akan sesuai dengan instalasi anda.

Perhatikan bahwa dua panel bisa mempunyai W_p yang sama tetapi berbeda tingkah laku dalam kondisi operasi yang berbeda. Ketika memperoleh panel, adalah penting untuk mengecek, jika memungkinkan, bahwa parameter mereka (setidaknya, I_{SC} dan V_{OC}) sesuai dengan nilai yang dijanjikan oleh vendor.

Parameter panel untuk menentukan ukuran sistem

Untuk menghitung jumlah panel-panel yang diperlukan untuk mengcover beban yang ada, anda hanya perlu mengetahui arus dan tegangan di titik daya maksimum: I_{Pmax} dan V_{Pmax}.

Anda sebaiknya waspada bahwa panel tidak akan beroperasi dalam kondisi sempurna karena beban atau pengaturan tidak selalu berfungsi pada titik daya maksimum panel. Anda sebaiknya mengasumsikan kehilangan efisiensi sebanyak 5% dalam perhitungan anda untuk mengkompensasi ini.

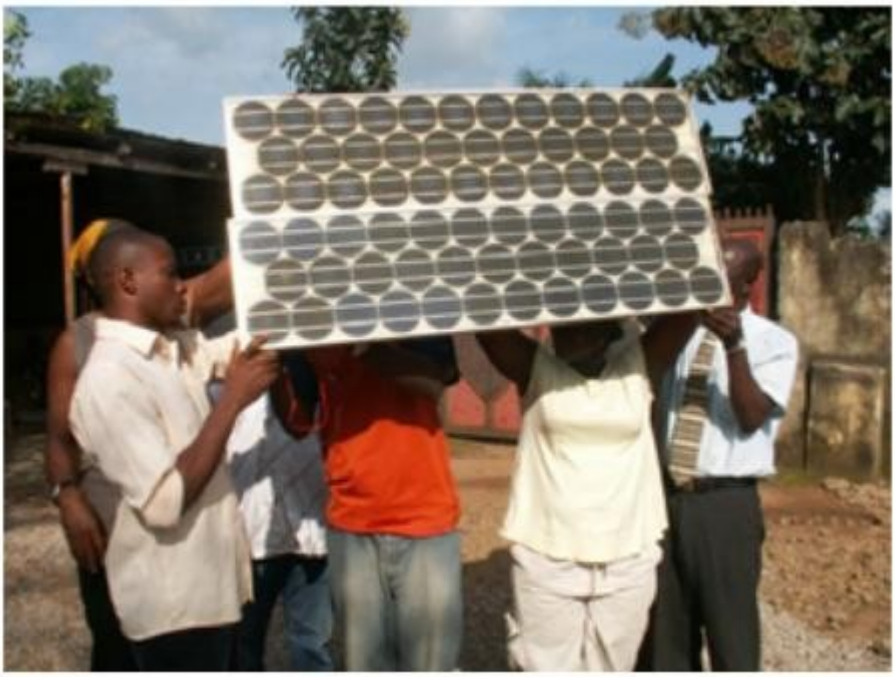
Penyambungan panel-panel surya

Sekumpulan panel surya atau ***solar panel array*** adalah sekumpulan panel-panel surya yang secara elektrik saling tersambung dan terpasang pada semacam struktur penopang. Menggunakan sekumpulan panel surya memungkinkan anda untuk membangkitkan tegangan dan arus yang lebih besar daripada apa yang mungkin dibangkitkan oleh satu panel surya. Panel-panel saling tersambung sedemikian rupa bahwa tegangan yang dihasilkan berdekatan dengan (namun lebih besar daripada) tegangan baterai, dan bahwa arus yang dihasilkan cukup untuk menghidupkan peralatan dan untuk mengisi baterai.

Menyambung panel-panel surya dalam konfigurasi seri akan meningkatkan tegangan yang dihasilkan. Menyambung panel-panel dalam konfigurasi paralel akan meningkatkan arus. Jumlah panel-panel yang digunakan sebaiknya ditambah sampai banyaknya daya yang dibangkitkan sedikit melebihi kebutuhan beban anda.

Adalah sangat penting bahwa semua panel dalam array anda seidentik mungkin. Dalam array, anda sebaiknya menggunakan panel-panel bermerek dan berkarakteristik yang sama karena perbedaan sedikit dalam kondisi operasi mereka akan mempunyai dampak besar pada kesehatan dan kinerja sistem anda. Bahkan panel-panel yang mempunyai penilaian kinerja yang sama biasanya akan menunjukkan suatu varian dalam sifat mereka karena proses pembuatan. Sifat operasi sesungguhnya dari dua panel dari vendor yang sama dapat bervariasi sampai ±10%.

Jika dimungkinkan, adalah gagasan yang baik untuk menguji kinerja nyata panel-panel individu untuk mengecek karakteristik operasi mereka sebelum mengumpulkan mereka ke dalam array.



Gambar 7.8: Sambungan panel-panel yang paralel. Tegangan tetap konstan sedangkan arus berduplikasi. (Foto: Fantsuam Foundation, Nigeria)

Bagaimana caranya untuk memilih panel yang baik

Salah satu ukuran yang digunakan pada saat berbelanja panel-panel surya adalah membandingkan rasio nominal daya tertinggi (W_p) terhadap harganya. Ini akan memberi anda ide secara garis besar biaya per Watt untuk panel-panel yang berbeda. Akan tetapi ada sejumlah pertimbangan lain yang juga harus diingat.

Jika anda berniat untuk menginstal panel-panel surya di daerah geografis dimana kotoran (dari debu, pasir, atau kerikil halus) akan mungkin menjadi masalah, pertimbangkanlah

pembelian panel-panel dimana tanah tidak terlalu suka menempel. Panel-panel ini terbuat dari bahan yang dapat membersihkan panel secara otomatis oleh angin dan hujan.

Periksa konstruksi mekanis masing-masing panel. Cek bahwa kaca dikeraskan dan bingkai aluminium kuat dan terbuat secara kokoh. Sel surya di dalam panel dapat bertahan selama lebih dari 20 tahun, tetapi mereka sangat mudah pecah dan panel harus dapat melindungi diri mereka sendiri dari bahaya mekanis. Cari garansi pabrik terutama untuk daya keluaran panel dan konstruksi mekanik panel.

Akhirnya, pastikanlah bahwa pabrik menyediakan tidak hanya daya tertinggi nominal panel (W_p) tetapi juga variasi daya dengan penyinaran dan suhu. Ini benar-benar penting kalau panel-panel digunakan dalam array, sebab variasi dalam parameter operasi dapat berdampak besar pada kualitas daya yang ditimbulkan dan umur kegunaan panel-panel.

Baterai

Baterai “menyimpan” reaksi kimia yang dapat dibalikkan yang menyimpan daya listrik yang nantinya dapat dipulihkan pada saat diperlukan. Daya listrik berubah menjadi daya kimia ketika baterai diisi, dan proses kebalikkannya terjadi pada saat baterai mengeluarkan daya.

Baterai terbentuk oleh sekelompok elemen atau ***sel*** yang diletakan secara seri. Baterai timbal-asam terdiri dari dua elektroda timbal yang berada dalam larutan elektrolit air dan asam sulfat. Perbedaan potensial sekitar 2 volt terjadi di antara elektroda, tergantung pada nilai seketika kondisi penyimpanan baterai. Baterai yang paling umum dalam aplikasi surya fotovoltaik mempunyai tegangan nominal sebanyak 12 atau 24 volt. Maka sebuah baterai 12 V berisi 6 sel secara seri.

Baterai memenuhi dua tujuan penting dalam sistem fotovoltaik: untuk memberikan daya listrik kepada sistem ketika daya tidak disediakan oleh array panel-panel surya, dan untuk menyimpan kelebihan daya yang ditimbulkan oleh panel-panel setiap kali daya itu melebihi beban. Baterai tersebut mengalami proses siklis menyimpan dan mengeluarkan, tergantung pada ada atau tidak adanya sinar matahari. Selama waktu adanya matahari, array panel menghasilkan daya listrik. Daya yang tidak digunakan dengan segera dipergunakan untuk mengisi baterai. Selama waktu tidak adanya matahari, permintaan daya listrik disediakan oleh baterai, yang oleh karena itu akan mengeluarkannya.

Siklus menyimpan dan mengeluarkan ini terjadi setiap kali daya yang dihasilkan oleh panel tidak sama dengan daya yang dibutuhkan untuk mendukung beban. Kalau ada cukup matahari dan bebannya ringan, baterai akan menyimpan daya. Tentunya, baterai akan mengeluarkan daya pada malam hari setiap kali sejumlah daya diperlukan. Baterai juga akan mengeluarkan daya ketika penyinaran tidak cukup untuk menutupi kebutuhan beban (karena variasi alami kondisi keikliman, awan, debu, dll.)

Jika baterai tidak menyimpan cukup daya untuk memenuhi permintaan selama periode tidak adanya matahari, sistem akan kehabisan daya dan tidak siap memenuhi konsumsi. Di sisi lainnya, memperbesar sistem (dengan menambahkan terlalu banyak panel dan baterai) mahal dan tidak efisien. Ketika mendesain sistem yang mandiri, kita perlu mengkompromikan antara biaya komponen dengan ketersediaan daya dari sistem. Satu cara untuk melakukan ini adalah memperkirakan ***jumlah hari dimana sistem beroperasi secara mandiri*** atau ***number of days of autonomy.*** Dalam kasus sistem telekomunikasi, jumlah hari-hari otonomi bergantung pada fungsi kritisnya dalam bentuk jaringan anda. Jika peralatan akan berfungsi sebagai repeater dan merupakan bagian tulang punggung jaringan anda, anda mungkin harus mendesain sistem fotovoltaik anda dengan otonomi sampai 5-7 hari.

Sebaliknya, jika sistem surya bertanggung jawab atas daya yang menyediakan ke peralatan pelanggan anda mungkin dapat mengurangi jumlah hari otonomi sampai dua atau tiga. Di daerah dengan penyinaran yang rendah, nilai ini mungkin perlu ditambah semakin banyak. Dalam kasus apapun, anda harus selalu menemukan keseimbangan yang baik antara biaya dan kehandalan.

Macam baterai

Banyak teknologi baterai yang tersedia, dan dimaksudkan untuk penggunaan dalam berbagai jenis aplikasi yang berbeda. Jenis yang paling cocok untuk aplikasi fotovoltaik adalah ***baterai yang tak bergerak*** (***stationary battery***), yang didesain untuk mempunyai lokasi tetap dan untuk skenario dimana pemakaian daya tidak teratur. Baterai yang "tidak bergerak" dapat mengakomodasi siklus pengeluaran yang dalam, tetapi mereka tidak didesain untuk menghasilkan arus tinggi dalam periode waktu yang singkat.

Baterai yang tidak bergerak dapat menggunakan elektrolit seperti alkali (seperti Nickel-Cadmium) atau asam (seperti Lead-Acid). Baterai yang tidak bergerak berdasarkan Nickel-Cadmium sebisa mungkin direkomendasikan menurut kehandalan dan ketahanan mereka yang tinggi. Sayangnya, mereka cenderung menjadi jauh lebih mahal dan sulit untuk diperoleh daripada baterai timbal-asam yang disegel.

Di banyak kasus ketika sulit menemukan baterai yang tidak bergerak lokal yang baik dan murah (mengimpor baterai tidak murah), anda dikondisikan untuk memakai baterai (aki) yang dirancang untuk mobil.

Memakai baterai mobil

Baterai mobil tidak cocok untuk aplikasi fotovoltaik karena mereka didesain untuk memberikan arus besar hanya selama beberapa detik saja (ketika menyalakan mesin) daripada memberikan arus rendah untuk periode waktu yang lama. Karakteristik aki mobil ini (juga dinamakan ***baterai daya cengkeram*** atau ***traction batteries***) menghasilkan sebuah kehidupan efektif yang pendek kalau dipakai di sistem fotovoltaik.

Baterai mobil dapat digunakan dalam aplikasi kecil dimana biaya rendah adalah pertimbangan yang paling penting, atau ketika baterai jenis lain tidak ada. Baterai mobil didesain untuk kendaraan dan gerobak tangan listrik. Mereka lebih murah daripada baterai yang tidak bergerak dan dapat melayani dalam sebuah instalasi fotovoltaik, walaupun mereka sering kali memerlukan pemeliharaan. Baterai ini tidak boleh terlalu banyak mengeluarkan dayanya, karena ini akan sangat secara luar biasa mengurangi kemampuan mereka untuk menyimpan daya. Sebuah baterai truk sebaiknya tidak mengeluarkan lebih dari 70% dari kapasitas totalnya. Ini berarti anda hanya bisa memakai maksimum 30% dari kapasitas nominal aki lead-acid sebelum aki tersebut harus diisi kembali.

Anda dapat memperpanjang umur baterai asam-timbal dengan menggunakan air sulingan. Dengan menggunakan densimeter atau hydrometer, anda dapat mengukur kepadatan elektrolit baterai tersebut. Sebuah aki pada umumnya mempunyai berat jenis 1,28. Menambahkan air sulingan dan merendahkan kepadatan ke 1,2 dapat membantu mengurangi korosi anoda, dengan biaya mengurangi kapasitas keseluruhan baterai. Jika anda menyesuaikan kepadatan baterai elektrolit, anda **harus** menggunakan air sulingan, karena air keran atau air tanah akan secara permanen merusak baterai.

Kondisi penyimpanan (State of Charge)

Ada dua kondisi istimewa penyimpanan yang dapat terjadi selama siklus penyimpanan dan pengeluaran daya dari baterai. Keduanya sebaiknya dihindari guna memperpanjang umur kegunaan baterai.

Penyimpanan yang berlebihan (Overcharge)

Penyimpanan yang berlebihan atau overcharge terjadi pada saat baterai berada pada kondisi keterbatasan kapasitasnya. Jika daya yang dimasukan di luar batas titik penyimpanan maksimum, elektrolit mulai hancur. Ini menghasilkan gelembung oksigen dan hidrogen, dalam proses yang diketahui sebagai ***pembuatan gas*** atau ***gasification***. Ini berakibat hilangnya air, oksidasi di elektroda positif, dan dalam kasus ekstrim, terjadi bahaya ledakan.

Di sisi lainnya, keberadaan gas menghindari stratifikasi asam. Setelah beberapa siklus penyimpanan dan pengeluaran yang terus menerus, asam cenderung terpusat di bagian bawah baterai, sehingga mengurangi kapasitas efektifnya. Proses gasifikasi menggerakan elektrolit dan menghindari stratifikasi. Sekali lagi, adalah perlu untuk menemukan kompromi antara keuntungan (menghindari stratifikasi elektrolit) dan keadaan merugikan (kehilangan air dan produksi hidrogen). Satu pemecahannya adalah lebih sering membiarkan penyimpanan yang sedikit berlebihan. Satu metode yang umum adalah membiarkan tegangan sebanyak 2,35 sampai 2,4 Volt untuk masing-masing elemen baterai sekali dalam beberapa hari, di suhu 25^{o} C. Regulator sebaiknya menjamin penyimpanan berlebihan yang berkala dan terkontrol.

Pengeluaran daya yang berlebihan (Overdischarge)

Dengan cara yang sama dimana ada batas atas, ada juga batas bawah dari kondisi penyimpanan baterai. Mengeluarkan melebihi batas itu akan menimbulkan pengrusakan pada baterai. Ketika persediaan baterai yang efektif habis, pengatur mencegah daya yang tersisa agar tidak diambil dari baterai. Kalau tegangan baterai mencapai batas minimum 1,85 Volt setiap selnya di suhu 25° C, pengatur memutuskan beban dari baterai.

Jika pengeluaran baterai sangat mendalam dan baterai tetap dalam kondisi pengeluaran untuk jangka waktu yang lama, akan terjadi tiga efek: pembentukan sulfat yang terkristal pada pelat baterai, bahan aktif pada pelat baterai akan lepas / berguguran, dan pelat baterai akan melengkung. Proses membentuk kristal sulfat yang stabil dinamakan sulfasi keras. Ini benar-benar tidak baik karena akan membentuk kristal besar yang tidak turut serta dalam reaksi kimia dan dapat membuat baterai anda tidak dapat digunakan.

Parameter baterai

Parameter utama sebuah baterai adalah:

- ***Tegangan Nominal*** atau ***Nominal voltage,*** V_{NBat}. Nilai yang paling umum adalah 12 V.
- ***Kapasitas Nominal*** atau ***Nominal Capacity***, $C_{NBat:}$ jumlah daya maksimum yang dapat diambil dari sebuah baterai yang terisi penuh. Ini diekspresikan dalam Ampere-jam (Ah) atau Watt-jam (Wh). Banyaknya daya yang bisa didapatkan dari baterai bergantung pada waktu dimana proses ekstraksi terjadi. Mengeluarkan daya baterai dalam jangka waktu lama akan menghasilkan lebih banyak daya dibandingkan dengan mengeluarkan daya baterai dalam jangka waktu yang singkat. Kapasitas baterai oleh sebab itu dispesifikasi di waktu pengeluaran daya yang berbeda. Untuk aplikasi fotovoltaik, waktu ini sebaiknya lebih lama daripada 100 jam (C100).
- ***Maximum Depth of Discharge***, DoD_{max}: Kedalaman pengeluaran daya adalah banyaknya daya yang diambil dari baterai dalam satu siklus pengeluaran daya, yang diekspresikan sebagai persentase. Umur baterai bergantung pada seberapa dalam pengeluaran daya itu terjadi dalam masing-masing siklus. Pabrik sebaiknya menyediakan grafik yang mengkaitkan jumlah siklus penyimpanan-pengeluaran daya dengan umur baterai. Sebagai kadiah umum anda sebaiknya menghindari pengeluaran daya baterai siklus yang dalam yang melebihi 50%. Baterai mobil sebaiknya hanya dikeluarkan dayanya sebanyak sekecil-kecilnya 30%.
- ***Kapasitas Berguna*** atau ***Useful Capacity***, C_{UBat}: adalah yang kapasitas baterai sesungguhnya (yang dapat digunakan). C_{UBat} setara dengan perkalian kapasitas nominal dan DoD maksimum. Misalnya, kapasitas nominal baterai yang tak bergerak (C100) 120 Ah dan kedalaman pengeluaran daya sebanyak 70% mempunyai kapasitas berguna (120 x 0,7) 84 Ah.

Mengukur kondisi penyimpanan daya baterai

Baterai timbal-asam 12 V yang disekat menyediakan tegangan yang berbeda tergantung pada kondisi penyimpanan dayanya. Ketika baterai penuh dengan daya dalam sebuah sirkuit terbuka, tegangan output adalah sekitar 12,8 V. Tegangan output turun dengan cepat sampai 12,6 V ketika terdapat beban. Pada saat baterai menyediakan arus yang konstan selama operasi, tegangan baterai berkurang secara linear dari 12,6 ke 11,6 V tergantung pada kondisi penyimpanan daya. Baterai timbal-asam yang disekat memberikan 95% dari dayanya dalam tegangan ini. Jika kita membuat asumsi yang lebih luas bahwa baterai yang sepenuhnya terisi mempunyai tegangan 12,6 V pada saat "penuh" dan 11,6 V pada saat "kosong", kita dapat memperkirakan bahwa baterai sudah mengeluarkan 70% ketika baterai mencapai tegangan 11,9 V. Nilai ini hanyalah perkiraan kasar karena mereka bergantung pada umur dan kualitas baterai, suhu, dll.

Kondisi penyimpanan	12 V Battery Voltage	Volts per Cell
100%	12,7	2,12
90%	12,5	2,08
80%	12,42	2,07
70%	12,32	2,05
60%	12,2	2,03
50%	12,06	2,01
40%	11,9	1,98
30%	11,75	1,96
20%	11,58	1,93
10%	11,31	1,89
0%	10,5	1,75

Menurut tabel ini, dan mempertimbangkan bahwa baterai truk sebaiknya tidak dikeluarkan dayanya lebih dari 20% sampai 30%, kita dapat menentukan bahwa kapasitas berguna baterai truk 170 Ah adalah 34 Ah (20%) ke 51 Ah (30%). Dengan menggunakan tabel yang sama, kita menyadari bahwa kita sebaiknya memprogram pengatur untuk mencegah baterai dari mengeluarkan daya di bawah 12,3 V.

Perlindungan baterai dan pengatur

Pemutus sambungan Thermomagnetic atau sekering sekali pakai harus digunakan untuk melindungi baterai dan instalasi dari arus sirkuit pendek dan kerusakan. Ada dua macam sekering: ***slow blow***, dan ***quick blow***. Sekering slow blow sebaiknya digunakan dengan muatan induktif atau kapasitif dimana arus tinggi dapat terjadi pada start / penyalaan pertama

kali. Slow blow akan mengijinkan arus yang lebih tinggi daripada nilai ideal mereka untuk berlalu dalam waktu singkat. Sekering quick blow akan langsung hangus jika arus yang mengalir lewat mereka lebih tinggi daripada nilai ideal mereka.

Pengatur dihubungkan dengan baterai dan beban, sehingga dua jenis perlindungan yang berbeda perlu dipertimbangkan. Sebuah sekering sebaiknya ditempatkan di antara baterai dan pengatur, untuk melindungi baterai dari korsleting jika terjadi kegagalan regulator. Sekering kedua diperlukan untuk melindungi regulator dari arus beban yang berlebihan. Sekering kedua ini biasanya diintegrasikan ke dalam pengatur itu sendiri.

Gambar 7.9: bank baterai 3600 Ah, arus mencapai tingkat 45 A selama penyimpanan daya

Setiap sekering dinilai dengan arus maksimum dan tegangan maksimum yang dapat digunakan. Arus maksimum sekering sebaiknya 20% lebih besar daripada arus maksimum yang diperkirakan. Sekalipun baterai membawa tegangan rendah, arus sirkuit pendek dapat menimbulkan arus yang sangat tinggi yang dengan mudah dapat mencapai beberapa ratus ampere. Arus besar dapat menimbulkan kebakaran, merusak peralatan dan baterai, dan mungkin mengejutkan badan manusia.

Jika sekering rusak, jangan pernah mengganti sekering dengan sehelai kawat atau sekering yang lebih baik. Tentukan terlebih dulu sebabnya, lalu ganti sekering dengan yang sama.

Efek temperatur

Suhu ambien mempunyai beberapa efek penting pada sifat baterai:

- Kapasitas nominal baterai (yang biasanya diberikan oleh pabrik untuk 25°C) meningkat dengan suhu pada laju di sekitar 1%/°C. Namun jika suhu terlalu tinggi, reaksi kimia yang terjadi dalam baterai melaju, yang dapat menimbulkan tipe oksidasi yang sama yang terjadi selama penyimpanan daya yang berlebihan. Ini secara nyata akan mengurangi perkiraan umur baterai. Masalah ini dapat dikompensasi sebagian dalam baterai mobil dengan menggunakan disolusi berkepadatan rendah (berat jenis 1,25

ketika baterai terisi penuh).

- Pada saat suhu berkurang, umur kegunaan baterai bertambah. Namun jika suhu terlalu rendah, anda menghadapi resiko pembekuan elektrolit. Suhu yang sangat dingin bergantung pada kepadatan solusi, yang juga berhubungan dengan kondisi penyimpanan daya baterai. Semakin rendah kepadatan, semakin besar resiko pembekuan. Di daerah bersuhu rendah, anda sebaiknya menghindari mengeluarkan daya baterai secara mendalam (yaitu, DoD_{max} dikurangi secara efektif.)
- Suhu juga mengubah hubungan antara tegangan dan penyimpanan daya. Adalah lebih baik untuk menggunakan regulator yang mengatur parameter penyambungan dan pemutusan tegangan rendah menurut suhu. Sensor suhu regulator sebaiknya dipasang pada baterai menggunakan selotip atau suatu metode sederhana lainnya.
- Pada daerah panas adalah sangat penting untuk menjaga baterai agar tetap sesejuk mungkin. Baterai harus disimpan di tempat teduh dan tidak pernah mendapat sinar matahari langsung. Sebaiknya baterai diletakkan pada penyanggah kecil untuk membiarkan udara mengalir di bawah mereka, dengan begitu meningkatkan pendinginan.

Bagaimana caranya untuk memilih baterai yang baik

Memilih baterai yang baik dapat menjadi tantangan di negara berkembang. Baterai berkapasitas tinggi biasanya berat, besar dan mahal untuk diimpor. Sebuah baterai 200 Ah memiliki berat sekitar 50 kg (120 pon) dan tidak bisa diangkut sebagai bagasi tangan. Jika anda ingin baterai berumur panjang (misalnya > 5 tahun) dan pemeliharaan baterai gratis, bersiaplah untuk membayar harganya.

Baterai yang baik selalu tersedia dengan spesifikasi teknisnya, termasuk kapasitas laju pengeluaran daya yang berbeda (C20, C100), suhu operasi, batas titik tegangan, dan syarat untuk alat pengisi ulang.

Baterai harus terbebas dari keretakan, kebocoran cairan atau tanda kerusakan apapun, dan sambungan baterai sebaiknya terbebas dari korosi. Karena tes laboratorium dibutuhkan untuk melengkapi data mengenai kapasitas dan penuaan yang sesungguhnya, bersiaplah untuk menerima kenyataan bahwa banyak bateria bermutu rendah di pasar lokal. Harga biasanya (tidak termasuk pajak angkutan dan barang impor) $3-4 USD per Ah untuk baterai timbal-asam 12 V.

Ekspetasi umur versus banyaknya siklus

Baterai merupakan satu-satunya bagian sistem surya yang sebaiknya dibeli secara berkala dalam jangka waktu singkat dan secara teratur diganti. Anda dapat menambah umur kegunaan baterai dengan mengurangi kedalaman pengeluaran daya per siklus. Baterai

bersiklus dalam pun akan mempunyai umur baterai yang bertambah jika jumlah siklus pengeluaran daya yang dalam (>30%) dikurangi.

Jika anda mengeluarkan daya baterai secara penuh setiap hari, anda biasanya akan perlu menggantinya setelah kurang dari satu tahun. Jika anda menggunakan hanya 1/3 kapasitas baterai, baterai tersebut dapat bertahan lebih dari 3 tahun. Akan menjadi lebih murah untuk membeli baterai dengan 3 kali kapasitasnya daripada mengganti baterai tersebut setiap tahun.

Regulator penyimpanan daya

Regulator penyimpanan daya juga dikenal sebagai pengontrol penyimpanan daya, pengatur tegangan, pengontrol penyimpanan-pengeluaran atau pengontrol penyimpanan-pengeluaran dan muatan.
Regulator berada di antara array panel-panel, baterai, dan peralatan atau beban anda.

Ingatlah bahwa tegangan baterai, walaupun selalu dekat 2 V setiap selnya, bervariasi menurut kondisi penyimpanan dayanya. Dengan mengamati tegangan baterai, pengatur mencegah penyimpanan atau pengeluaran daya yang berlebihan.

Pengatur yang digunakan di aplikasi surya sebaiknya disambung dalam serial: mereka memutuskan array panel-panel dari baterai untuk menghindari penyimpanan daya yang berlebihan, dan mereka memutuskan baterai dari beban untuk menghindari pengeluaran daya yang berlebihan. Penyambungan dan pemutusan dilakukan oleh switch yang jenisnya bisa dua macam: electromechanical (relay) atau solid state (transistor bipolar, MOSFET). Pengatur tidak boleh sekali-sekali disambungkan secara paralel.

Guna melindungi baterai dari pembuatan gas, switch membuka sirkuit penyimpanan daya ketika tegangan dalam baterai mencapai pemutusan tegangan tingginya atau high voltage disconnect (HVD) atau titik batas yang ditentukan. Pemutusan tegangan rendah atau low voltage disconnect (LVD) mencegah baterai dari pengeluaran energi yang berlebihan dengan memutuskan atau menahan beban. Untuk mencegah hubungan penyambungan dan pemutusan yang terus-menerus, pengatur tidak akan menghubungkan beban kembali sampai baterai mencapai tegangan penyambungan kembali yang rendah atau low reconnect voltage (LRV).

Nilai umum untuk sebuah baterai timbal-asam 12 V adalah:

Titik tegangan	tegangan
LVD	11,5
LRV	12,6
tegangan konstan teregulasi	14,3
Penyamaan	14,6
HVD	15,5

Pengatur yang paling modern juga dapat secara otomatis memutuskan panel selama malam hari untuk menghindari pengeluaran daya baterai. Mereka juga dapat secara berkala menyimpan daya baterai yang berlebihan untuk meningkatkan umur mereka, dan mereka mungkin menggunakan mekanisme yang dikenal sebagai modulasi lebar nadi atau pulse width modulation (PWM) untuk mencegah gassing yang berlebihan.

Karena titik operasi daya puncak array panel akan bervariasi dengan suhu dan penerangan surya, pengatur yang baru mampu secara konstan melacak titik maksimum daya array surya. Fitur ini dikenal sebagai pelacakan titik daya maksimum atau maximum power point tracking (MPPT).

Parameter pengatur

Ketika memilih pengatur untuk sistem anda, anda sebaiknya setidaknya mengetahui ***tegangan operasi*** atau ***operating voltage*** dan ***arus maksimum*** atau ***maximum current*** yang bisa ditangani oleh pengatur. Tegangan operasi adalah 12, 24, atau 48 V. Arus maksimum harus 20% lebih besar daripada arus yang disediakan oleh array panel-panel yang tersambung dengan regulator

Fitur dan data yang menarik lainnya termasuk:

- Nilai spesifik bagi LVD, LRV dan HVD.
- Dukungan untuk kompensasi suhu. Tegangan yang menunjukkan kondisi penyimpanan daya baterai bervariasi dengan suhu. Atas alasan ini beberapa pengatur dapat mengukur suhu baterai dan mengkoreksi nilai batas dan penyambungan kembali yang berbeda.
- Instrumentasi dan pengukur. Alat yang paling umum mengukur tegangan panel dan baterai, kondisi penyimpanan daya (SoC) atau kedalaman pengeluaran daya (DoD). Beberapa pengatur memasukkan alaram istimewa untuk menunjukkan bahwa panel-panel atau beban-beban sudah diputuskan, LVD atau HVD sudah dicapai, dll.

Konverter

Pengatur menyediakan daya DC di tegangan spesifik. Konverter dan inverter dipergunakan untuk mengatur tegangan agar sama dengan kebutuhan beban anda.

Konverter DC/DC

Konverter DC/DC mengubah tegangan DC menjadi tegangan DC lainnya dengan nilai yang berbeda. Ada dua metode konversi yang dapat dipergunakan untuk mengubah tegangan dari

baterai: ***konversi linear*** atau ***linear conversion*** dan ***konversi peralihan*** atau ***switching conversion.***

Konversi linear menurunkan tegangan dari baterai dengan mengubah kelebihan daya menjadi panas. Metode ini sangat sederhana namun pada kenyataannya tidak efisien. Konversi peralihan pada umumnya menggunakan komponen magnetik untuk menyimpan daya secara sementara dan mengubahnya menjadi tegangan lainnya. Tegangan yang dihasilkan bisa lebih besar, lebih rendah, atau kebalikan (negatif) daripada tegangan input.

Efisiensi pengatur linear berkurang dengan semakin banyaknya perbedaan antara tegangan input dan tegangan output. Misalnya, jika kita ingin mengubah dari 12 V ke 6 V, pengatur linear akan mempunyai efisiensi sebanyak hanya 50%. Pengatur peralihan standar mempunyai efisiensi sedikitnya 80%.

Konverter DC/AC atau Inverter

Inverter digunakan ketika peralatan anda memerlukan daya AC. Inverter memotong dan membalikkan arus DC untuk membangkitkan gelombang segi empat yang nantinya disaring menjadi gelombang sinus yang disesuaikan dan menghapus harmonik yang tidak diinginkan. Sangat sedikit inverter yang sebetulnya menyediakan gelombang sinus yang murni sebagai output. Kebanyakan model yang tersedia di pasar menciptakan apa yang diketahui sebagai "gelombang sinus yang termodifikasi", karena output tegangan mereka bukanlah sinusoid yang murni. Ketika kita memikirkan efisiensi, gelombang sinus yang termodifikasi berkinerja lebih baik daripada inverter sinusoidal yang murni.

Ketahuilah bahwa tidak semua peralatan akan menerima gelombang sinus yang termodifikasi sebagai tegangan input. Secara umum, beberapa printer laser tidak akan berkerja dengan gelombang sinus inverter yang termodifikasi. Mesin akan tetap berfungsi, tetapi mereka mungkin memakan lebih banyak daya daripada jika mereka diberi input dengan gelombang sinus murni. Selain itu, power supply DC cenderung semakin memanas, dan pengeras audio dapat mengeluarkan bunyi berdengung.

Disamping tipe bentuk gelombang, beberapa fitur penting inverter juga termasuk:

- **Kehandalan saat adanya sentakan.** Inverter mempunyai dua penilaian daya: satu untuk daya yang terus-menerus, dan yang lebih tinggi untuk daya tertinggi. Mereka dapat menyediakan daya tertinggi untuk waktu yang sangat singkat, seperti ketika menghidupkan mesin. Inverter juga sebaiknya dapat secara aman menginterupsi dirinya sendiri (dengan sakelar pemutus (circuit breaker) atau sekering) seandainya terjadi arus sirkuti pendek, atau jika daya yang diminta terlalu tinggi.
- **Efisiensi konversi.** Inverter paling efisien ketika memberikan 50% sampai 90% dari

rating daya terus-menerus mereka. Anda sebaiknya memilih inverter yang hampir sesuai dengan syarat beban anda. Pabrik biasanya menyediakan kinerja inverter di 70% dari daya nominalnya.

- **Pengisian daya baterai.** Banyak inverter juga memasukkan fungsi terbalik: kemungkinan mengisi daya baterai dari sebuah sumber arus AC (jaringan listrik, genset dll). Inverter tipe ini dikenal sebagai charger/inverter.
- **Automati fail-over.** Beberapa inverter dapat berpindah secara otomatis di antara sumber daya yang berbeda (jaringan listrik PLN, pembangkit daya listrik, surya) tergantung pada apa yang tersedia.

Ketika menggunakan peralatan telekomunikasi, sebaiknya menghindari penggunaan konverter DC/AC dan memberi daya kepada mereka secara langsung dari sebuah sumber DC. Kebanyakan peralatan komunikasi dapat menerima tingkatan input tegangan yang cukup lebar.

Peralatan atau beban

Sangatlah nyata bahwa pada saat keperluan daya bertambah, bertambah pula pengeluaran biaya sistem fotovoltaik. Maka sangatlah penting untuk menyamakan ukuran sistem sesama mungkin dengan beban yang ada. Ketika mendesain sistem, anda terlebih dulu harus membuatkan perkiraan realistis konsumsi maksimum. Ketika instalasi sudah terpasang, tingkat konsumsi maksimum yang sudah ditentukan harus dipatuhi untuk menghindari sering terjadinya pemadaman listrik.

Peralatan rumah

Penggunaan daya surya fotovoltaik tidak dianjurkan untuk aplikasi penukaran panas (pemanas listrik, kulkas, pemanggang roti, dll.) Sebisa mungkin, daya sebaiknya digunakan dengan hemat memakai peralatan berdaya rendah. Ini beberapa hal yang perlu diingat ketika memilih peralatan yang pas untuk penggunaan dengan sistem surya:

- Daya surya fotovoltaik cocok untuk penerangan. Dalam kasus ini, penggunaan bola lampu halogen atau lampu berpendar (fluorescent) adalah suatu keharusan. Walaupun lampu ini lebih mahal, mereka mempunyai efisiensi daya yang lebih baik daripada bola lampu ringan yang pijar (incandescent). Lampu LED juga merupakan pilihan yang baik karena mereka sangat efisien dan diberi input daya DC.

- Adalah mungkin untuk menggunakan daya fotovoltaik untuk peralatan yang memerlukan konsumsi rendah dan terus-menerus (seperti dalam kasus yang umum, televisi). Televisi kecil akan menggunakan daya yang lebih sedikit daripada televisi besar. Juga pertimbangkan bahwa televisi hitam putih mengkonsumsi sekitar setengah daya televisi berwarna.

- Daya surya fotovoltaik tidak dianjurkan untuk aplikasi apapun yang mengubah daya menjadi panas (daya termal). Gunakanlah pemanasan surya atau LPG sebagai alternatif.

- Mesin cuci otomatis yang biasa dapat digunakan, tetapi anda sebaiknya menghindari penggunaan program mencuci apapun yang terdapat pemanasan air terpusat.

- Jika anda harus menggunakan kulkas, kulkas tersebut sebaiknya mengkonsumsi daya sesedikit mungkin. Ada kulkas yang khusus yang bekerja di DC, walaupun konsumsi mereka bisa cukup tinggi (sekitar 1000 Wh/hari).

Estimasi konsumsi total adalah langkah pokok dalam menentukan besaran ukuran sistem surya anda. Berikut ini adalah tabel yang memberi anda gagasan umum pemakaian daya yang bisa anda perkirakan dari peralatan yang berbeda.

Peralatan	Konsumsi (Watt)
Portable computer	30-50
Low power lamp	6-10
WRAP router (one radio)	4-10
VSAT modem	15-30
PC (tanpaLCD)	20-30
PC (dengan LCD)	200-300
Network Switch (16 port)	6-8

Peralatan telekomunikasi nirkabel

Menghemat daya dengan memilih peralatan yang sesuai menekan pengeluaran dan mengurangi kesulitan. Misalnya, hubungan jarak jauh tidak terlalu memerlukan amplifier yang kuat yang menggunakan banyak daya. Sebuah kartu Wi-Fi dengan kepekaan receiver yang baik dan zona fresnel sedikitnya 60% jelas akan berfungsi lebih baik daripada amplifier, dan juga menghemat penggunaan daya. Pepatah tenar amatir radio juga berlaku di sini: amplifier terbaik adalah antena yang baik. Tindakan lebih lanjut untuk mengurangi pemakaian daya termasuk menambah kecepatan CPU, mengurangi daya pancar sampai ke nilai minimum yang cukup untuk memberikan hubungan yang stabil, menambah panjang interval beacon, dan mematikan sistem selama sistem tersebut tidak diperlukan.

Kebanyakan sistem pembangkit tenaga surya mandiri bekerja di 12 atau 24 volt. Lebih baik, alat nirkabel yang menggunakan tegangan DC sebaiknya digunakan, yang beroperasi di tegangan 12 Volt yang disediakan oleh kebanyakan baterai asam timbal. Mengubah tegangan yang disediakan oleh baterai menjadi AC atau memakai tegangan di input titik akses yang berbeda dari tegangan baterai akan menyebabkan kehilangan daya yang tidak perlu. Sangat baik jika kita menggunakan router atau titik akses yang menerima 8-20 Volt DC.

Kebanyakan titik akses yang murah mempunyai pengatur tegangan switching di dalamnya dan akan berkerja pada kisaran tegangan tersebut tanpa modifikasi atau menjadi panas (sekalipun alat dipaketkan dengan sumber listrik 5 atau 12 Volt).

PERINGATAN: mengoperasikan titik akses anda dengan sumber listrik lain daripada yang disediakan oleh pabrik tentunya akan membatalkan garansi apapun, dan mungkin menyebabkan kerusakan pada peralatan anda. Teknik berikut akan bekerja seperti yang dijelaskan, tapi ingat jika anda mencobanya, anda melakukannya dengan resiko anda sendiri.

Buka titik akses anda dan perhatikan bagian dekat input DC untuk dua kapasitor yang relatif besar dan sebuah induktor (ferrite toroid dengan kawat tembaga yang dibelitkan padanya). Jika mereka ada, maka alat tersebut mempunyai input switch, dan tegangan input maksimum sebaiknya agak di bawah tegangan yang tertulis pada kapasitor. Biasanya penilaian kapasitor ini adalah 16 atau 25 volt. Perhatikan bahwa sumber listrik yang tidak teratur mempunyai gelombang dan mungkin memberikan input tegangan yang jauh lebih tinggi kepada titik akses anda daripada tegangan umum yang disarankan oleh apa yang tertulis. Oleh sebab itu, menyambung sumber listrik yang tidak teratur dengan tegangan 24 Volt ke alat dengan kapasitor bertegangan 25 Volt bukanlah hal yang baik. Tentunya, membuka alat anda akan membatalkan garansi apapun yang ada. Jangan coba-coba menjalankan titik akses di tegangan yang lebih tinggi jika titik akses itu tidak mempunyai regulator switching. Titik akses akan menjadi panas, rusak, atau terbakar.

Peralatan berdasarkan CPU tradisional Intel x86 adalah peralatan yang boros daya dibandingkan dengan arsitektur berbasis pada RISC seperti ARM atau MIPS. Satu dari banyak motherboard dengan konsumsi daya terendah adalah platform Soekris yang menggunakan prosesor AMD ElanSC520. Pilihan yang berbeda dari AMD (ElanSC atau Geode SC1100) adalah penggunaan peralatan dengan prosesor MIPS. Prosesor MIPS mempunyai kinerja yang lebih baik daripada AMD Geode, sesuatu yang harus dibayar dengan konsumsi daya antara 20-30% lebih banyak.

Linksys WRT54G yang populer berfungsi di tegangan antara 5 dan 20 volt DC dan menggunakan daya sekitar 6 Watt, tetapi alat ini memiliki Ethernet switch didalamnya. Mempunyai sebuah switch tentu saja baik dan berguna - tetapi switch ini menggunakan daya ekstra. Linksys juga menyediakan titk akses Wi-Fi yang dinamakan WAP54G yang menggunakan daya hanya sebesar 3 Watt dan dapat menjalankan OpenWRT dan Freifunk firmware. Sistem 4G Accesscube menggunakan daya sekitar 6 Watt ketika diperlengkapi dengan sebuah antarmuka WiFi. Jika 802.11b cukup, maka kartu mini PCI dengan chipset Orinoco berkinerja dengan baik saat menggunakan daya minimum.

Peralatan	Konsumsi (Watt)
Linksys WRT54G (BCM2050 radio)	6
Linksys WAP54G	3

(BCM2050 radio)	
Orinoco WavePoint II ROR (30mW radio)	15
Peralatan	Konsumsi (Watt)
Soekris net4511 (no radio)	1.8
PC Engines WRAP.1E-1 (no radio)	2.04
Mikrotik Routerboard 532 (no radio)	2.3
Inhand ELF3 (no radio)	1.53
Senao 250mW radio	3
Ubiquiti 400mW radio	6

Banyaknya daya yang diperlukan oleh peralatan nirkabel bergantung tidak hanya pada arsitektur tetapi juga pada jumlah jaringan antarmuka, radio, macam memori/penyimpanan dan lalu-lintas. Sebagai kadiah umum, motherborad nirkabel konsumsi rendah mengkonsumsi 2 sampai 3 W, dan kartu radio 200 mW mengkonsumsi sampai 3 W. Kartu berdaya tinggi (seperti 400 mW Ubiquity) mengkonsumsi sekitar 6 W. Stasion pengulang dengan dua radio dapat berkisar antara 8 sampai 10 W.

Walaupun standar IEEE 802.11 meliputi mekanisme cara penghematan daya atau power saving mode (PS), keuntungannya tidak sebaik seperti yang anda harapkan. Mekanisme utama untuk penghematan daya adalah memungkinkan stasiun untuk secara periodik me-non-aktifkan kartu nirkabel mereka dengan sirkuit pengatur waktu. Ketika kartu nirkabel aktif, kartu tersebut akan mengecek apakah beacon tersedia, yang menunjukkan adanya trafik yang menunggu. Penghematan daya oleh karena itu hanya terjadi di sisi klien, karena titik akses harus tetap aktif untuk memancarkan beacon dan menyimpan trafik bagi klien.

Mode penghematan daya mungkin tidak kompatibel antar pabrik, yang dapat menyebabkan tidak stabilnya hubungan nirkabel. Adalah hampir selalu yang terbaik untuk membiarkan mode penghematan daya agar tetap tidak aktif pada semua peralatan, karena kesukaran yang ditimbulkan mungkin akan melebihi jumlah penghematan daya yang sedikit.

Memilih tegangan

Kebanyakan sistem mandiri yang berdaya rendah menggunakan baterai berdaya 12 V, karena daya baterai tersebut adalah tegangan operasional yang umum dipergunakan dalam baterai asam-timbal yang disekat. Ketika mendesain sebuah sistem komunikasi nirkabel, anda harus mempertimbangkan tegangan yang sangat efisien operasi peralatan anda. Sementara tegangan input dapat menerima wilayah tegangan yang lebar, anda perlu

memastikan bahwa konsumsi daya keseluruhan sistem adalah minimal.

Memasang kabel

Bagian penting instalasi adalah pengawatan, karena pengawatan yang baik akan menjamin pemindahan daya yang efisien. Beberapa praktek yang baik yang sebaiknya anda pertimbangkan termasuk:

- Gunakan sekrup untuk untuk mengencangkan kabel pada sambungan baterai. Hubungan yang longgar akan memboroskan daya.
- Oleskan Vaseline atau selai mineral pada sambungan baterai. Sambungan yang rusak mempunyai hambatan tambahan, yang menimbulkan kehilangan.
- Untuk arus rendah (<10), pertimbangkanlah penggunaan konektor powerpole Faston atau Anderson. Untuk arus yang lebih besar, gunakanlah metalik ring berulir.

Ukuran kawat biasanya tersedia dalam American Wire Gauge (AWG). Selama perhitungan anda, anda perlu melakukan konversi antara AWG dan mm2 untuk memperkirakan hambatan kabel. Misalnya, kabel AWG #6 mempunyai diameter 4,11 mm dan dapat bekerja dengan baik sampai 55 A. Sebuah grafik koversi, yang didalamnya termasuk perkiraan hambatan dan kapasitas mengangkut arus, tersedia dalam **Appendix D.** Selalu ingat bahwa kapasitas mengangkut arus juga dapat bervariasi tergantung pada macam isolasi dan aplikasi. Jika anda ragu-ragu, konsultasikan dengan pabrik untuk lebih banyak informasi.

Orientasi panel surya

Sebagian besar daya yang datang dari matahari tiba dalam bentuk garis lurus. Modul surya akan menangkap lebih banyak daya jika modul tersebut “menghadap” matahari, tegaklurus terhadap garis lurus antara posisi instalasi dan matahari. Tentunya, posisi matahari terus-menerus berubah relatif terhadap tanah, oleh sebab itu kita perlu menemukan posisi optimal bagi panel-panel kita. Orientasi panel-panel ditentukan oleh dua sudut, ***azimut a*** dan ***kemiringan*** atau ***ketinggian ß.*** Azimut adalah sudut ke arah selatan bagi mereka yang berada di belahan bumi utara, atau sudut ke arah utara bagi mereka di belahan bumi selatan. Kemiringan adalah sudut yang terbentuk oleh permukaan modul dan bidang horisontal.

Azimuth

Anda sebaiknya membuat modul mengarah ke arah khatulistiwa (menghadap ke selatan di belahan bumi utara, dan utara di yang selatan) agar selama siang hari panel tersebut dapat menangkap jumlah radiasi sebanyak mungkin (a = 0).

Adalah sangat penting untuk memastikan bahwa tidak ada bagian panel-panel yang berada

di bawah tempat yang teduh!. Pelajari elemen di sekitar array panel (pohon, gedung, tembok, panel lain, dll.) untuk memastikan bahwa mereka tidak akan pernah membentuk bayangan di atas panel-panel. Adalah dapat diterima untuk memutar panel ±20° ke arah timur atau barat jika diperlukan (= ±20°).

Kemiringan

Ketika anda sudah menetapkan azimut, parameter yang pokok dalam perhitungan kita adalah kemiringan panel, yang akan kita ungkapkan sebagai sudut beta (ß). Tinggi maksimum yang dicapai oleh matahari setiap hari akan bervariasi, dengan maksimum pada hari pertengahan musim panas dan minimum pada pertengahan musim dingin. Idealnya, panel-panel sebaiknya mengikuti variasi ini, tetapi ini biasanya tidak mungkin karena alasan biaya.

Dalam instalasi dengan peralatan telekomunikasi adalah normal untuk memasang panel pada kemiringan tertentu. Dalam kebanyakan skenario telekomunikasi, permintaan daya sistem adalah konstan sepanjang tahun. Penyediaan daya yang cukup selama "bulan terburuk" akan terjadi paling baik untuk sisa tahun.

Nilai ß sebaiknya memaksimalisir rasio antara tawaran dan permintaan daya.

- Untuk instalasi dengan konsumsi yang konsisten (atau hampir konsisten) sepanjang tahun, sangat diinginkan untuk mengoptimalkan instalasi untuk menangkap radiasi maksimum selama bulan "musim dingin". Anda sebaiknya menggunakan nilai mutlak garis lintang dari tempat (sudut F) yang bertambah sebanyak 10° (ß = | F | + 10 °).
- Untuk instalasi dengan konsumsi yang kurang selama musim dingin, nilai garis lintang dari tempat dapat digunakan sebagai kemiringan panel surya. Dengan cara ini, sistem dioptimisasi untuk bulan-bulan musim semi dan musim gugur (ß = | F |).
- Untuk instalasi yang hanya digunakan selama musim panas, anda sebaiknya menggunakan nilai mutlak garis lintang tempat (sudut F) yang dikurangi sebanyak 10° (ß = | F | - 10°).

Kemiringan panel tidak boleh kurang dari 15° untuk menghindari penumpukan debu dan/atau kelembaban pada panel. Dalam daerah dimana terdapat salju dan es, sangatlah penting untuk melindungi panel-panel dan menambah kemiringan mereka sebesar 65° atau lebih.

Jika ada pertambahan yang besar dalam konsumsi selama musim panas, anda mungkin perlu mempertimbangkan untuk mengatur dua sudut kemiringan yang tetap, satu posisi untuk bulan musim panas dan lain untuk bulan musim dingin. Ini akan memerlukan struktur penopang yang khusus dan jadwal yang teratur untuk mengubah posisi panel-panel.

Bagaimana caranya untuk menentukan ukuran sistem fotovoltaik anda

Ketika memilih peralatan untuk memenuhi kebutuhan daya anda, anda perlu menentukan setidaknya yang berikut ini:

- Jumlah dan macam panel surya yang diperlukan untuk menangkap daya surya yang cukup untuk mendukung beban anda.
- Kapasitas minimum baterai. Baterai perlu menyimpan cukup daya untuk menyediakan daya pada malam hari dan hari-hari dengan penyinaran matahari yang sedikit, dan akan menentukan jumlah hari-hari otonomi anda.
- Karakteristik semua bagian lainnya (regulator, perkabelan, dll.) yang diperlukan untuk mendukung banyaknya daya yang dihasilkan dan disimpan.

Perhitungan besaran ukuran sistem penting, karena kecuali jika komponen sistem seimbang, daya (dan juga, uang) akan terbuang percuma. Misalnya, jika kita memasang lebih banyak panel surya untuk menghasilkan lebih banyak daya, baterai sebaiknya mempunyai kapasitas yang cukup untuk menyimpan daya tambahan yang dihasilkan. Jika kumpulan baterai terlalu kecil dan beban tidak menggunakan daya maka ketika daya tersebut dihasilkan, maka daya harus dibuang. Sebuah regulator amperage yang lebih kecil daripada yang diperlukan, atau satu kabel yang terlalu kecil, dapat menjadi sebab kegagalan (atau bahkan kebakaran) dan membuat instalasi tidak berguna.

Jangan pernah lupa bahwa kemampuan daya fotovoltaik untuk menghasilkan dan menyimpan daya listrik terbatas. Dengan tidak sengaja meninggalkan sebuah bola lampu ringan tetap menyala pada siang hari dapat dengan mudah menghabiskan cadangan daya anda sebelum malam hari, ketika tidak ada daya tambahan yang tersedia. Ketersediaan "bahan bakar" untuk sistem fotovoltaik (yaitu, radiasi matahari) bisa sulit untuk diramalkan. Sebenarnya, tidak pernah mungkin untuk benar-benar memastikan bahwa sistem yang mandiri dapat memberikan daya yang diperlukan pada saat tertentu kapanpun. Sistem pembangkit tenaga surya didesain untuk konsumsi tertentu, dan jika pengguna melanggar batas yang sudah direncanakan, maka penyediaan daya akan gagal.

Metode desain yang kami usulkan termasuk pertimbangan keperluan daya, dan berdasarkan keperluan tersebut memperhitungkan sistem yang berfungsi untuk sejumlah waktu maksimum sehingga sistem itu dapat diandalkan sebisa mungkin. Tentunya, jika lebih banyak panel dan baterai terpasang, akan lebih banyak daya yang dapat dikumpulkan dan disimpan. Peningkatan kehandalan ini juga akan mempunyai pertambahan dalam biaya.

Dalam beberapa instalasi fotovoltaik (seperti penyediaan daya untuk peralatan telekomunikasi pada tulang punggung jaringan), faktor kehandalan lebih penting daripada biaya. Pada instalasi pelanggan, biaya rendah mungkin merupakan faktor yang paling penting. Menemukan keseimbangan antara biaya dan kehandalan bukanlah tugas yang mudah, tetapi apapun situasinya, anda sebaiknya dapat menentukan apa yang diharapkan dari pilihan desain anda, dan pada biaya berapa.

Metode yang kita akan gunakan untuk menentukan besaran ukuran sistem dikenal sebagai ***metode bulan terburuk*** atau ***method of the worst month.*** Secara sederhana, kita hitung

dimensi sistem mandiri tersebut, agar sistem itu dapat berfungsi dalam bulan dimana permintaan daya terbesar terkait dengan ketersediaan daya surya. Bulan tersebut merupakan yang teburuk dalam setahun, karena bulan ini mempunyai rasio terbesar antara daya yang diperlukan dan daya yang tersedia.

Dengan menggunakan metode ini, ***kehandalan / reliability*** dimasukan sebagai pertimbangan dengan menetapkan jumlah maksimum hari dimana sistem dapat beroperasi tanpa menerima radiasi surya (yaitu, ketika semua konsumsi dibuat hanya dengan mengorbankan daya yang disimpan dalam baterai). Ini dikenal sebagai ***jumlah maksimum hari otonomi*** atau ***maximum number of days of autonomy*** (N), dan dapat dibayangkan sebagai jumlah hari berawan yang berurutan jika panel tidak mengumpulkan jumlah daya apapun yang berarti.

Ketika memilih N, kita harus mengetahui kondisi iklim setempat, serta keterkaitan ekonomi dan sosial terhadap instalasi tersebut. Apakah instalasi tersebut akan digunakan untuk menerangi rumah, rumah sakit, pabrik, untuk hubungan radio, atau untuk suatu aplikasi lainnya? Ingatlah bahwa pada saat N bertambah, bertambah pula investasi dalam peralatan dan pemeliharaan. Juga penting untuk mengevaluasi semua kemungkinan biaya logistik penggantian peralatan. Tidaklah sama antara mengganti baterai yang dayanya sudah habis dari sebuah instalasi di tengah kota dengan mengganti baterai di atas menara telekomunikasi yang berlokasi beberapa jam lebih jauh untuk ditempuh dengan berjalan kaki.

Menetapkan nilai N bukanlah tugas yang mudah, karena ada banyak faktor yang terlibat, dan banyak di antara mereka tidak bisa dievaluasi secara mudah. Pengalaman anda akan memainkan peranan penting dalam menentukan ukuran sistem ini. Satu nilai yang biasanya digunakan untuk peralatan telekomunikasi yang penting adalah N = 5, sedangkan untuk peralatan pelanggan berbiaya rendah sangatlah mungkin untuk mengurangi otonomi sampai N = 3.

Dalam **Appendix E**, kami sudah memasukkan beberapa tabel yang akan memudahkan pengumpulan data yang diperlukan untuk menentukan ukuran sistem. Sisa bab ini akan menjelaskan secara terperinci informasi apa yang anda perlu kumpulkan atau perkirakan dan bagaimana caranya untuk menggunakan metode "bulan terburuk".

Data yang perlu dikumpulkan

- **Lintang instalasi / latitude of the installation.** Ingatlah untuk menggunakan tanda positif untuk belahan bumi utara dan negatif untuk sebelah selatan.
- **Data radiasi surya / solar radiation data.** Untuk metode "bulan terburuk" cukup diketahui hanya dua belas nilai, satu untuk setiap bulannya. Kedua belas angka ini adalah nilai rata-rata bulanan penyinaran global harian di bidang horisontal ($G_{dm}(0)$, dalam kWh/m2 per hari). Nilai bulanan adalah jumlah nilai penyinaran global untuk setiap harinya dalam sebulan, yang dibagi dengan jumlah hari dalam bulan tersebut.

Jika anda mempunyai data dalam Joule (J), anda dapat mempergunakan konversi berikut:

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

Data penyinaran $G_{dm}(0)$ dari banyak tempat di dunia dikumpulkan dalam tabel dan database. Anda sebaiknya memeriksa informasi ini dari kantor pengamat cuaca yang berdekatan dengan lokasi implementasi anda, namun janganlah kaget jika anda tidak menemukan data dalam format elektronik. Adalah gagasan yang baik untuk bertanya pada perusahaan yang memasang sistem fotovoltaik di daerah tersebut, karena pengalaman mereka bisa sangat berguna.

Jangan anggap "jam matahari" sama dengan "jam puncak matahari". Jumlah jam puncak matahari tidak ada hubungannya dengan jumlah jam tanpa awan, tetapi merujuk pada banyaknya penyinaran harian. 5 jam matahari dalam sehari tanpa awan belum tentu merupakan jam itu ketika matahari berada zenithnya.

Jam puncak matahari adalah nilai radiasi matahari yang dinormalisasikan 1000 W/m2 pada 25^{o} C. Jadi ketika kita merujuk pada 5 jam puncak matahari, ini berarti radiasi matahari harian 5000 W/m2.

Karakteristik kelistrikan komponen sistem

Karakteristik kelistrikan komponen sistem anda sebaiknya disediakan oleh pabrik. Adalah dianjurkan untuk membuat pengukuran anda sendiri untuk memeriksa deviasi dari nilai nominal. Sayangnya, deviasi dari nilai yang dijanjikan bisa besar dan sebaiknya dinantikan.

Berikut ini adalah nilai minimum yang harus anda kumpulkan sebelum menentukan ukuran sistem anda:

Panel

Anda perlu mengetahui tegangan V_{Pmax} dan arus I_{Pmax} di titik daya maksimum dalam kondisi standar.

Baterai

Kapasitas nominal (untuk 100 jam pengeluaran daya) C_{NBat}, tegangan operasional V_{NBat}, dan kedalaman maksimum pengeluaran daya DoD_{max} atau kapasitas berguna C_{UBat}. Anda juga perlu mengetahui macam baterai yang anda berencana untuk gunakan, baik apakah itu timbal-asam tersekat, AGM, baterai mobil yang sudah dimodifikasi dll. Macam baterai penting ketika menentukan batas dalam pengatur.

Regulator

Anda perlu mengetahui nominal tegangan V_{NReg}, dan arus maksimum yang bisa beroperasi I_{maxReg}.

Konverter/ Inverter DC/AC

Jika anda akan menggunakan konverter, anda perlu mengetahui tegangan nominal V_{NConv}, daya seketika P_{IConv} dan kinerja pada 70% beban maksimum H_{70}.

Peralatan atau beban

Kita perlu mengetahui tegangan nominal V_{NC} dan daya nominal operasi P_C untuk setiap bagian peralatan yang dihidupkan oleh sistem. Guna mengetahui jumlah daya yang akan dikonsumsi oleh instalasi kita, sangatlah penting untuk mempertimbangkan waktu rata-rata setiap beban yang akan dipakai. Apakah terus-menerus? Atau apakah akan dipakai tiap hari, tiap minggu, setiap bulan atau tahun? Pertimbangkan pergantian apapun dalam penggunaan yang mungkin berdampak pada banyaknya daya yang diperlukan (penggunaan musiman, periode latihan atau sekolah, dll.)
Variabel lainnya

Terlepas dari sifat-sifat kelistrikan komponen dan beban, adalah perlu untuk mengambil keputusan pada dua informasi tambahan sebelum kita dapat menentukan besaran ukuran sebuah sistem fotovoltaik. Dua keputusan ini adalah jumlah hari otonomi yang diperlukan dan tegangan operasional sistem.

N, jumlah hari-hari otonomi

Anda perlu menentukan nilai untuk N yang akan menyeimbangkan kondisi meteorologi dengan tipe instalasi dan biaya keseluruhan. Adalah mustahil untuk memberikan nilai konkrit N yang berlaku untuk setiap instalasi, tetapi tabel berikut ini memberi beberapa nilai yang dianjurkan. Gunakan nilai ini sebagai perkiraan kasar, dan konsultasikan dengan seorang perancang berpengalaman untuk mencapai keputusan akhir.

Ketersediaan Matahari	Instalasi Rumah	Instalasi Kritis
Sangat berawan	5	10
Bervariasi	4	8
Terang	3	6

V_N, tegangan nominal instalasi

Komponen sistem anda perlu dipilih agar dapat berfungsi pada tegangan nominal V_N. Tegangan ini biasanya 12 atau 24 Volt untuk sistem kecil, dan jika konsumsi daya total melebihi 3 kW, tegangan akan menjadi 48 V. Seleksi VN tidak sembarangan, dan bergantung pada ketersediaan peralatan.

- Jika peralatan mengijinkannya, cobalah menetapkan tegangan nominal ke 12 atau 24 V. Banyak peralatan komunikasi nirkabel menerima tegangan input yang lebar dan dapat digunakan tanpa konverter.
- Jika anda perlu menghidupkan beberapa macam peralatan yang berkerja pada tegangan nominal yang berbeda, perhitungkan tegangan yang meminimalkan pemakaian daya secara keseluruhan, termasuk kehilangan pada konversi daya menggunakan konverter DC/DC dan DC/AC.

Prosedur perhitungan Sistem Photovoltaic

Ada tiga langkah utama yang perlu diikuti untuk menghitung ukuran sistem yang sesuai:

1. **Perhitungkan daya surya yang ada (sebagai tawaran).** Berdasarkan data statistik radiasi surya, dan orientasi dan kemiringan optimal panel-panel surya, kita menghitung daya surya yang ada. Penilaian daya surya yang ada dilakukan dalam interval bulanan, mengurangi data statistik sampai 12 nilai. Perkiraan ini adalah kompromi yang baik antara ketepatan dan kesederhanaan.
2. **Perkirakan daya listrik yang diperlukan (sebagai permintaan).** Catat sifat pemakaian daya peralatan yang dipilih serta perkiraan lama penggunaannya. Lalu perhitungkan daya listrik yang diperlukan dalam setiap bulannya. Anda sebaiknya mempertimbangkan fluktuasi penggunaan yang diharapkan karena variasi antara musim dingin dan musim panas, periode musim hujan/kering, periode sekolah/liburan, dll. Hasil berupa 12 nilai permintaan daya, masing-masing untuk setiap bulan dalam setahun.
3. **Perhitungkan ukuran sistem ideal (hasilnya).** Dengan data dari “bulan terburuk”, ketika hubungan antara daya surya yang dibutuhkan dan daya yang tersedia sangat erat, maka kita menghitung:

    - Arus yang harus disediakan oleh array panel, yang akan menentukan jumlah minimum panel.
    - Kapasitas penyimpanan daya yang diperlukan untuk menutupi jumlah minimum hari-hari otonomi, yang akan menentukan jumlah baterai yang diperlukan.
    - Karakteristik kelistrikan regulator yang diperlukan.

- Panjang dan bagian-bagian yang diperlukan dari kabel itu untuk hubungan listrik.

Arus yang diperlukan dalam bulan terburuk

Untuk setiap bulan, anda perlu memperhitungkan nilai I_m, yang merupakan arus maksimum sehari-hari yang harus disediakan oleh array panel yang beroperasi pada tegangan nominal V_N, dalam suatu hari dengan penyinaran G_{dm} untuk bulan ”m”, bagi panel-panel dengan kemiringan ß derajat.

I_m(BULAN TERBURUK) akan menjadi nilai Im yang paling besar, dan penentuan besaran ukuran sistem didasarkan pada data bulan terburuk itu. Perhitungan G_{dm} (ß) untuk tempat tertentu dapat dibuat berdasarkan G_{dm}(0) dengan menggunakan software komputer seperti PVSYST (http://www.pvsyst.com/) atau PVSOL (http://www.solardesign.co.uk/).

Karena loss di pengatur dan baterai, dan karena fakta bahwa panel-panel tidak selalu berfungsi di titik daya maksimum, arus yang diperlukan I_{mMAX} dihitung sebagai berikut:

$$I_{mMAX} = 1{,}21\ I_m\ (\text{BULAN TERBURUK})$$

Ketika anda sudah menentukan bulan terburuk, nilai I_{mMAX}, dan total daya yang anda perlukan E_{TOTAL} (BULAN TERBURUK), anda dapat melanjutkan ke perhitungan terakhir. E_{TOTAL} adalah jumlah seluruh beban DC dan AC, dalam Watt. Untuk menghitung E_{TOTAL}, lihatlah **Appendix E**.

Jumlah panel

Dengan mengkombinasikan panel-panel surya dalam serial dan paralel, kita dapat mendapatkan tegangan dan arus yang diinginkan. Ketika panel-panel tersambung dalam serial, jumlah tegangan total setara dengan jumlah tegangan individual masing-masing modul, sedangkan arus tidak berubah. Ketika menyambungkan panel-panel secara paralel, arus dijumlahkan sedangkan tegangan tidak berubah. Sangatlah penting untuk memakai panel-panel yang sifatnya yang hampir identik ketika membuat array.

Anda sebaiknya mencoba untuk memperoleh panel-panel dengan V_{Pmax} yang sedikit lebih besar daripada tegangan nominal sistem (12, 24 atau 48 V). Ingatlah bahwa anda perlu menyediakan sedikit tegangan dari tegangan nominal baterai untuk mengisinya. Jika tidak mungkin untuk menemukan satu panel yang memenuhi keperluan anda, anda perlu menyambung beberapa panel dalam serial untuk mencapai tegangan yang anda inginkan. Jumlah panel yang di seri N_{ps} adalah sama dengan tegangan nominal sistem dibagi tegangan sebuah panel, yang dibulatkan ke atas ke bilangan bulat terdekat.

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

Untuk memperhitungkan jumlah panel yang paralel (N_{pp}), anda perlu membagi I_{mMAX} dengan arus sebuah panel di titik daya maksimum I_{pmax}, yang dibulatkan ke atas ke integer terdekat.

$$Npp = ImMAX/IPmax$$

Jumlah total panel adalah hasil perkalian jumlah panel yang di seri (untuk menentukan tegangan) oleh jumlah panel yang di paralel (untuk menentukan arus).

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

Kapasitas baterai atau akumulator

Baterai menentukan tegangan keseluruhan sistem dan memerlukan kapasitas yang cukup untuk menyediakan daya kepada beban pada saat tidak terdapat radiasi surya yang cukup. Untuk memperkirakan kapasitas baterai kita, kita terlebih dulu menghitung kapasitas daya sistem kita yang diperlukan (kapasitas yang diperlukan atau necessary capacity, C_{NEC}). Kapasitas yang diperlukan ini bergantung pada daya yang ada selama "bulan terburuk" dan jumlah hari-hari otonomi yang diinginkan (N).

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

Kapasitas nominal baterai C_{NOM} harus lebih besar daripada C_{NEC} karena kita tidak bisa sepenuhnya mengeluarkan daya baterai. Untuk menghitung ukuran baterai kita perlu mempertimbangkan kedalaman maksimum pengeluaran daya (DoD) yang dimungkinkan oleh baterai:

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

Untuk memperhitungkan jumlah baterai dalam seri (N_{bs}), kita bagi tegangan nominal instalasi kita (V_N) dengan tegangan nominal satu baterai (V_{NBat}):

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

Regulator

Sebuah peringatan penting: selalu gunakan regulator dalam seri, tidak paralel. Jika pengatur anda tidak mampu mendukug arus yang diperlukan oleh sistem anda, anda perlu membeli sebuah pengatur baru dengan arus yang lebih besar.

Untuk alasan keamanan, sebuah pengatur baru harus mampu beroperasi dengan arus I_{maxReg} sedikitnya 20% lebih besar daripada intensitas maksimum yang disediakan oleh array panel-

panel:

$I_{maxReg} = 1,2\ N_{pp}\ I_{PMax}$

Inverter DC/AC

Jumlah daya yang diperlukan untuk peralatan AC dihitung dengan memasukkan semua loss yang disebabkan oleh konverter DC/AC atau inverter DC/AC. Ketika memilih inverter, selalu ingat bahwa kinerja inverter bervariasi berdasarkan banyaknya daya yang dibutuhkan. Sebuah inverter mempunyai karakteristik kinerja yang lebih baik ketika beroperasi dekat kemampuan dayanya. Menggunakan inverter 1500 Watt untuk menghidupkan beban 25 Watt sangatlah tidak efisien. Untuk menghindari daya yang terbuang ini, sangatlah penting untuk menganggap bukan daya tertinggi seluruh peralatan anda, tetapi puncak daya peralatan yang diharapkan untuk beroperasi secara bersamaan.

Kabel

Pada saat anda sudah mengetahui jumlah panel surya dan baterai, dan macam regulator dan inverter yang anda ingin gunakan, adalah perlu untuk memperhitungkan panjang dan ketebalan kabel yang diperlukan untuk menyambung berbagai bagian tersebut menjadi satu.

Panjang kabel bergantung pada lokasi instalasi anda. Anda sebaiknya berusaha meminimalkan panjang kabel antara pengatur, panel surya, dan baterai. Memakai kabel pendek akan mengurangi kehilangan daya dan biaya kabel.

Ketebalan kabel dipilih berdasarkan panjang kabel dan arus maksimum yang harus diteruskannya. Tujuannya adalah meminimalisir penurunan tegangan. Untuk dapat menghitung ketebalan S kabel, perlu untuk mengetahui:

- Arus maksimum I_{MC} yang akan melalui kabel. Dalam kasus sub-sistem baterai-panel, adalah I_{mMAX} yang diperhitungkan untuk setiap bulan. Dalam sub-sistem beban-baterai I_{mMax} bergantung pada bagaimana caranya beban disambung.
- Penurunan tegangan (V_a-V_b) yang kita anggap dapat diterima dalam kabel. Penurunan tegangan yang merupakan hasil dari penambahan semua penurunan yang mungkin diungkapkan sebagai persen tegangan nominal instalasi. Nilai umum maksimum ialah:

Komponen	Penurunan tegangan (% V_N)
Panel Array -> Battery	1%
Battery -> Converter	1%
Main Line	3%
Main Line (Illumination)	3%
Main Line (Equipment)	5%

Penurunan Tegangan Yang Dapat di Terima di Kabel

Bagian kabel ditentukan oleh hukum Ohm:

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

Di mana S adalah bagian kabel, r ialah resistivitas (karakteristik internal bahan: untuk tembaga, 0,01286 $\Omega mm^2/m$), dan L adalah panjang kabel.

S dipilih dengan mempertimbangkan kabel yang ada di pasar. Anda sebaiknya memilih bagian yang jauh lebih baik daripada apa yang didapatkan dari rumus. Karena alasan keamanan ada nilai minimum, untuk kabel yang menyambung panel dan baterai, nilai minimum adalah 6 mm^2. Untuk bagian lain, minimumnya ialah 4 mm^2.

Biaya instalasi pembangkit listrik tenaga surya

Sementara daya surya sendiri gratis, namun tidak untuk peralatan yang diperlukan untuk mengubahnya menjadi daya listrik. Anda tidak hanya perlu membeli peralatan untuk mengubah daya surya menjadi listrik dan menyimpannya untuk penggunaan, tetapi anda juga harus mengganti dan memelihara berbagai bagian sistem. Masalah penggantian peralatan sering kali diabaikan, akhirnya sistem pembangkit listrik tenaga surya dijalankan tanpa rencana pemeliharaan yang baik.

Untuk memperhitungkan biaya sesungguhnya dari instalasi anda, kami berikan sebuah contoh ilustratif. Hal pertama yang harus dilakukan adalah memperhitungkan biaya investasi awal.

Deskripsi	Jumlah	Biaya satuan	Subtotal
Panel surya 60W (sekitar $4/W)	4	$300	$1,200
Regulator 30A	1	$100	$100
Kabel (meter)	25	$1/ meter	$25
Baterai 50Ah (deep cycle)	6	$150	$900
Total			$2,225

Perhitungan biaya investasi kita relatif mudah ketika sistem sudah didimensikan. Anda hanya perlu menambahkan harga untuk masing-masing bagian peralatan dan biaya tenaga kerja untuk memasang dan menyambungkan peralatan menjadi satu. Untuk kesederhanaan, kita tidak memasukkan biaya angkut dan instalasi tetapi anda sebaiknya tidak mengabaikan mereka.

Untuk memahami berapa biaya sistem agar dapat beroperasi, kita harus memperkirakan seberapa lama tiap bagian akan berfungsi dan seberapa sering anda harus menggantinya.

Dalam istilah akuntansi, ini dikenal sebagai ***amortisasi.*** Tabel baru kita terlihat seperti berikut ini:

Deskripsi	#	Biaya satuan	Subtotal	Umur (tahun)	Biaya Tahunan
Panel surya 60W	4	$300	$1,200	20	$60
Regulator 30A	1	$100	$100	5	$20
Kabel (meter) dengan ketebalan 50 Ah	25	$1/ meter	$25	10	$2.50
Baterai 50 Ah (deep cycle)	6	$150	$900	5	$180
		Total:	$2,225	Biaya tahunan:	$262.50

Seperti yang anda lihat, ketika investasi pertama sudah dilakukan, akan ada biaya tahunan sebesar $262,50. Biaya tahunan adalah perkiraan kapital yang dibutuhkan setiap tahun untuk mengganti bagian sistem begitu umur kegunaan mereka berakhir.

Bab 8 Membangun sebuah Node Luar Ruang

Ada banyak pertimbangan praktis ketika memasang peralatan elektronik di luar ruangan. Secara nyata, peralatan tersebut harus terlindungi dari hujan, angin, matahari, dan elemen berbahaya lainnya. Daya harus disediakan, dan antena harus dipasang cukup tinggi. Tanpa penyambungan ke tanah yang baik, petir yang dekat, daya yang berfluktuasi, dan bahkan angin yang ringan walaupun dalam keadaan cuaca normal dapat menghancurkan sambungan nirkabel anda. Bab ini akan memberikan anda gagasan mengenai masalah-masalah praktis yang akan anda hadapi ketika memasang peralatan nirkabel luar ruang.

Penutup kedap air

Penutup kedap air tersedia dalam berbagai banyak jenis. Logam atau plastik dapat digunakan untuk membuat sebuah kontainer kedap air untuk peralatan luar ruang. Tentu saja, peralatan memerlukan daya agar dapat berkerja, dan sepertinya harus terhubung dengan antena dan kabel Ethernet. Setiap kali anda melubangi penutup kedap air, anda menciptakan potensi masuknya air ke dalam peralatan tersebut.

Asosasi Pengusaha Pabrik Listrik Nasional atau National Electrical Manufacturers Association (NEMA) menyediakan petunjuk untuk perlindungan peralatan listrik dari hujan, es, debu, dan kontaminan lainnya. Sebuah penutup dengan penilaian **NEMA 3** atau lebih baik cocok untuk penggunaan luar ruang dalam kondisi iklim yang cukup baik. Sebuah **NEMA 4X** atau **NEMA 6** memberikan perlindungan yang sempurna, bahkan dari semprotan air selang dan es. Untuk sesuatu yang permanen yang melubangi tubuh penutup (seperti kabel gland dan konektor berkepala besar), Komisi Teknik-eletronika Internasional atau International Electrotechnical Comission (IEC) memberikan penilaian perlindungan penetrasi (ingress).

Sebuah penilaian perlindungan penetrasi ***IP66*** atau ***IP67*** akan melindungi lubang-lubang ini dari semburan air yang sangat kuat. Sebuah penutup luar ruang yang baik juga harus menyediakan perlindungan UV untuk mencegah kehancuran penyekat dari kontak matahari, serta untuk melindungi peralatan yang ada di dalam.

Tentunya, mencari penutup berperingkat NEMA atau IEC bisa akan sangat sulit di daerah lokal anda. Sering kali, bagian-bagian yang tersedia secara lokal dapat didaur ulang untuk digunakan sebagai penutup. Plastik kasar atau kotak logam penyembur air, kotak saluran listrik, atau bahkan kontainer makanan plastik dapat digunakan jika memang diperlukan. Ketika melubangi penutup, gunakan cincin karet atau o-ring yang berkualitas bersamaan dengan kabel gland untuk menyekat bagian yang terbuka. Salep silikon yang stabil terhadap UV atau penyekat lainnya dapat digunakan untuk instalasi sementara, namun ingatlah bahwa kabel melentur dalam angin, dan sendi-sendi yang dilem akhirnya akan melemah dan menyebabkan embun untuk merembes masuk.

Anda dapat memperpanjang umur penutup plastik dengan menyediakan suatu perlindungan dari matahari. Meletakan kotak di tempat teduh, baik di bawah peralatan yang ada, panel solar, atau lembaran tipis logam yang diperuntukan untuk tujuan ini, akan memperpanjang umur kotak serta peralatan yang tersimpan di dalamnya.

Sebelum meletakan bagian eletronika apapun ke dalam kotak yang disekat, pastikan adanya keperluan pembuangan panas yang minimal. Jika motherboard anda memerlukan sebuah fan atau pembuangan panas yang besar, ingatlah bahwa tidak akan ada aliran udara, dan peralatan eletronika anda akan terpanggang hingga tidak berfungsi pada menara. Hanya gunakan komponen eletronika yang di desain untuk digunakan dalam lingkungan tertutup.

Menyediakan daya

Secara nyata, daya DC dapat disediakan dengan secara sederhana melubangi penutup anda dan memasukan kabel. Jika penutup anda cukup besar (katakanlah, sebuah kotak listrik luar ruang) anda bahkan dapat menyambungkan outlet AC di dalam kotak. Saat ini pabrik mulai semakin mendukung fitur yang sangat membantu untuk menghilangkan lubang tambahan di kotak dengan menggunakan: ***Daya melalui Ethernet*** atau ***Power over Ethernet*** (***POE***).

Standar 802.3af mendefinisikan sebuah metode untuk menyediakan daya ke alat yang menggunakan pasangan kabel yang tak terpakai pada kabel Ethernet standar. Daya hampir sebanyak 13 Watt dapat disediakan secara aman pada kabel CAT5 tanpa mengganggu pengiriman data melalui kawat yang sama. Switch Ethernet yang sesuai dengan 802.3af yang lebih baru (dinamakan ***penyuntik jengkal akhir*** atau ***end span injectors***) menyediakan daya secara langsung ke alat yang dihubungkan. Switch dengan penyuntik jengkal akhir dapat menyediakan daya pada kawat yang sama yang dipakai untuk data (pasangan 1- 2 dan 3-6) atau pada kawat yang tak terpakai (pasangan 4-5 dan 7-8). Peralatan lain, dinamakan penyuntik jengkal tengah, dimasukkan antara switch Ethernet dan alat yang dihidupkan. Penyuntik ini menyediakan daya pada pasangan kabel yang tak terpakai.

Jika router nirkabel anda atau CPE termasuk dukungan untuk 802.3af, anda secara teoritis dapat secara langsung menghubungkannya ke penyuntik. Sayangnya, beberapa pabrik (khususnya Cisco) memiliki polaritas daya yang tidak sama, dan menghubungkannya dapat merusak penyuntik dan peralatan yang ingin dihidupkan. Bacalah petunjuk yang ada dan pastikan bahwa penyuntik dan peralatan nirkabel anda sesuai dengan pin dan polaritas yang dapat digunakan untuk daya.

Jika peralatan nirkabel anda tidak menyangga daya melalui Ethernet, anda masih dapat menggunakan pasangan yang tak terpakai dalam kabel CAT5 untuk meneruskan daya. Anda dapat menggunakan baik ***penyuntik POE pasif*** (***passive POE injector***) atau secara sederhana membuat satu sendiri. Alat-alat ini secara manual menghubungkan daya DC ke kawat yang tak terpakai pada satu akhir kabel, dan menghubungkan akhir yang lain secara langsung ke konektor barrel yang dimasukkan ke dalam mata daya alatnya. Pasangan alat

POE pasif biasanya bisa dibeli di bawah $20.

Untuk membuat alat anda sendiri, anda perlu mengetahui seberapa banyak daya yang diperlukan alat tersebut agar dapat beroperasi dan menyediakan sedikitnya arus dan tegangan yang cukup, ditambah tegangan secukupnya untuk menutupi kehilangan pada berjalannya Ethernet. Anda tidak ingin menyediakan terlalu banyak daya, karena hambatan kabel kecil dapat menimbulkan bahaya api. Berikut ini adalah kalkulator online yang akan membantu anda memperhitungkan penurunan tegangan untuk sebuah CAT5: http://www.gweep.net/~sfoskett/tech/poecalc.html.

Setelah anda mengetahui polaritas listrik dan daya yang pas yang dibutuhkan untuk menjalankan peralatan nirkabel anda, crimp-lah kabel CAT5 yang hanya menggunakan kawat data (pasangan 1-2 dan 3-6). Lalu secara mudah sambungkan transformer ke pasangan 4-5 (biasanya biru/ biru-keputihan) dan 7-8 (coklat/ coklat-keputihan) pada satu ujung, dan sebuah konektor barrel yang cocok pada ujung yang satunya.

Pertimbangan peletakan

Dalam banyak kasus, peralatan dapat diletakan di dalam gedung, dengan syarat ada jendela dengan kaca biasa yang bisa dilalui oleh cahaya. Kaca normal akan menyebabkan sedikit atenuasi, tetapi kaca berwarna akan menyebabkan atenuasi yang tidak dapat ditoleransikan. Ini sangat menyederhanakan permasalahan peletakan, daya, dan tahan cuaca, tetapi secara nyata hanya berguna di daerah yang didiami penduduk.

Ketika meletakkan antena pada menara, sangat penting untuk menggunakan stand-off bracket (penopang siku yang dapat berdiri sendiri), dan tidak meletakkan antena secara langsung pada menara. Penopang siku ini membantu dengan banyak fungsi termasuk pemisahan antena, pemosisian antena dan perlindungan antena.

Stand-off bracket harus cukup kuat untuk menopang bobot antena, dan juga menjaga agar antena tetap pada letaknya ketika ada angin. Ingatlah, antena dapat beraksi seperti layar kecil, dan dapat menimbulkan gaya yang kuat pada sandaran mereka ketika ada angin kuat. Ketika memperkirakan hambatan angin, luas total permukaan struktur antena harus dipertimbangkan, serta jarak dari pusat antena sampai titik sambungan ke gedung. Antena besar seperti parabola utuh atau panel sektoral dengan gain yang tinggi dapat mempunyai beban angin yang cukup besar. Menggunakan sebuah parabola slotted atau mesh, daripada parabola utuh, akan membantu mengurangi beban angin tanpa banyak mempengaruhi gain antena. Pastikan bahwa siku-siku sandaran dan struktur pendukung terpasang secara kokoh, atau posisi/arah antena anda akan berubah seiring berjalannya waktu (atau lebih parah lagi, semuanya jatuh dari menara!)

Bracket sandaran antenna harus cukup jauh dari tower untuk memudahkan pembidikan antenna, tapi tidak terlalu jauh sehingga antenna sukar untuk di jangkau jika dibutuhkan perbaikan atau pemeliharaan.

Gambar 8.1: Sebuah antena dengan stand-off bracket sedang diangkat ke atas menara

Pipa pada stand-off bracket dimana antena akan dipasang harus berbentuk silinder. Dengan cara ini, antena dapat diputar pada pipa untuk pembidikan. Kedua, pipa juga harus vertikal. Jika diletakkan pada menara yang meruncing, siku-siku tersebut harus didesain agar dapat bisa dipasang pada menara ini. Ini bisa dilakukan dengan memakai baja dengan panjang berbeda, atau dengan menggunakan kombinasi tangkai berulir dan pelat baja.

Karena peralatan tersebut akan berada diluar selama umur kegunaannya, adalah penting untuk memastikan bahwa baja yang digunakan tahan cuaca. Baja tahan karat seringkali terlalu mahal untuk instalasi menara. Penguatan yang sangat baik (Hot galvanizing) akan lebih baik, tetapi mungkin tidak tersedia di beberapa daerah. Pengecatan semua baja dengan cat anti-karat yang baik juga bisa. Jika menggunakan cat, maka penting untuk merencanakan pemeriksaan tahunan bracket dan melakukan pengecatan ulang jika perlu.

Menara dengan penyangga kabel

Guyed Tower (menara dengan penyangga kabel) yang dapat dipanjat adalah pilihan sempurna untuk banyak instalasi, tetapi untuk struktur yang sangat tinggi, menara self-support yang menyanggah dirinya sendiri akan lebih baik.

Ketika memasang guyed tower, sebuah kerekan yang tersambung pada bagian atas tiang akan memudahkan instalasi menara. Tiang tersebut dipasangkan pada stek / bagian tower yang lebih rendah yang sudah ada di tempatnya, sementara kedua bagian / stek tower terhubung dengan sambungan sementara. Sebuah tali melalui kerekan akan memudahkan pengangkatan stek / bagian berikutnya. Setelah bagian penopang menjadi vertikal, bautkan penopang tersebut pada bagian lebih rendah tiang. Tiang dapat dipindahkan, dan instalasi stek tower dapat diulangi, jika diperlukan. Kencangkan kawat-kawat itu secara hati-hati, memastikan bahwa anda memberikan ketegangan yang sama di semua titik penancapan yang sesuai. Pilihlah titik agar sudut-sudut, seperti yang terlihat dari pusat menara, berada pada jarak yang sama.

Gambar 8.2: menara dengan penyangga kabel yang dapat dipanjat

Tower self-support

Menara self-support atau yang dapat menyanggah dirinya sendiri mahal tetapi kadang-kadang diperlukan, khususnya jika dibutuhkan ketinggian yang sangat tinggi. Ini bisa sebuah tiang yang berat yang tertanam dalam beton, atau serumit menara radio profesional.

Gambar 8.3: menara self-support yang sederhana

Menara yang sudah ada kadang-kadang dapat digunakan, walaupun antena stasiun pemancar AM sebaiknya dihindari karena seluruh strukturnya aktif. Antena stasiun FM dapat diterima, dengan syarat ada jarak sedikitnya beberapa meter di antara antena. Perhatikan bahwa sementara antena pemancar yang berdampingan mungkin tidak mengganggu hubungan nirkabel anda, FM berdaya tinggi dapat mengganggu kabel Ethernet anda. Setiap kali menggunakan menara antena yang penuh dengan antena, cermatilah penghubungan ke tanah yang baik dan pertimbangkan penggunaan kabel yang terlindung.

Gambar 8.4: Sebuah menara yang sangat rumit

Bubungan atap

Antenna pada bubungan atap yang tidak penetratif dapat digunakan pada atap yang datar. Ini termasuk sebuah tripod yang dipasang pada sebuah dasar logam atau kayu. Dasar kemudian diganjal dengan bata, karung pasir, kendi air, atau apapun yang sama beratnya. Menggunakan pengganjal pada bubungan atap menghilangkan keperluan untuk membuat lubang pada atap dengan pemasangan baut, sehingga menghindari potensi kebocoran.

Gambar 8.5: Dasar logam ini dapat diganjal dengan karung pasir, batu, atau botol air untuk membuat panggung stabil tanpa membolongi atap

Sandaran tembok atau pengikat logam dapat digunakan pada struktur yang sudah ada seperti cerobong asap atau sisi samping bangunan. Jika antena harus diletakkan sekitar 4 meter lebih tinggi dari bubungan atap, menara yang dapat dipanjat mungkin menjadi pemecahan yang lebih baik untuk memungkinkan akses yang lebih mudah ke peralatan dan untuk mencegah pergerakan antena selama adanya angin kuat.

Logam yang tidak sama

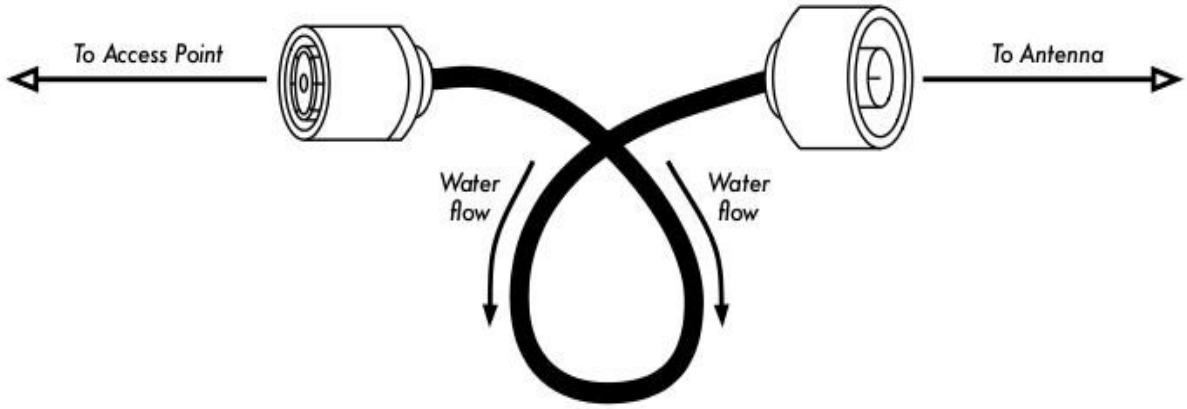
Untuk meminimalisir korosi elektrolit ketika dua metal yang berbeda berada dalam kontak yang lembab, potensi elektrolit mereka sebaiknya sedekat mungkin. Gunakanlah pelumas dielektrik pada sambungan antara dua metal yang berbeda jenis untuk mencegah efek elektrolisa apapun.

Tembaga sebaiknya tidak pernah menyentuh bahan yang berlapis secara langsung tanpa adanya perlindungan sendi yang baik. Tetesan air dari tembaga berisi ion yang akan membersihkan lapisan (seng) menara. Baja tahan karat dapat digunakan sebagai bahan penetral, tetapi anda sebaiknya tahu bahwa baja tahan karat bukanlah konduktor yang sangat

baik. Jika baja tersebut dipakai sebagai penetral di antara tembaga dan logam berlapis, bidang permukaan kontak sebaiknya besar dan baja tahan karat sebaiknya tipis. Olesan sendi juga sebaiknya digunakan untuk menutup sambungan sehingga air tidak dapat menjembatani logam yang tidak sama itu.

Melindungi konektor mikrowave

Kebocoran embun dalam konektor adalah sesuatu yang mungkin seringkali diamati sebagai penyebab kegagalan hubungan radio. Pastikanlah untuk mengencangkan konektor secara kuat, namun jangan pernah mempergunakan kunci inggris atau alat lain untuk melakukannya. Ingat bahwa logam memuai dan menyusut seiring dengan perubahan suhu, dan konektor yang terlalu kencang bisa rusak dalam pergantian cuaca yang ekstrim.



Gambar 8.6: Sebuah loop untuk membuang tetesan air hujan dari konektor anda.

Ketika sudah kencang, konektor sebaiknya dilindungi dengan memberikan selapis selotip listrik, kemudian selapis selotip penyekat, and kemudian satu lapis selotip listrik lagi di bagian atas. Penyekat melindungi konektor dari rembesan air, dan lapisan selotip melindungi penyekat dari pengrusakan ultraviolet (UV). Kabel sebaiknya memiliki sebuah loop tetesan tambahan untuk mencegah air untuk masuk ke dalam transceiver.

Pengamanan

Selalu gunakan sebuah harness yang terpasang secara aman pada menara ketika bekerja pada ketinggian. Jika anda belum pernah bekerja pada sebuah menara, sewa seorang profesional untuk melakukannya untuk anda. Banyak negara mengharuskan latihan khusus agar seseorang dapat bekerja pada menara pada ketinggian tertentu.

Hindari bekerja pada menara ketika ada angin kencang atau badai. Selalu memanjat dengan seorang rekan, dan hanya ketika ada banyak sekali penerangan cahaya. Pekerjaan menara akan membutuhkan waktu yang lebih lama daripada yang anda perkirakan. Ingat bahwa ***sangat*** berbahaya untuk bekerja dalam kegelapan. Berikan anda sendiri banyak waktu untuk

menyelesaikan pekerjaan jauh sebelum matahari terbenam. Jika anda kehabisan waktu, ingat bahwa menara akan tetap ada di pagi hari, ketika anda dapat mulai menyelesaikan masalahnya lagi setelah anda sudah cukup beristirahat.

Mengarahkan antena pada hubungan jarak jauh

Agar dapat secara baik mengarahkan antena pada jarak yang jauh, anda akan memerlukan semacam umpan balik visual yang memperlihatkan kepada anda daya yang diterima seketika itu pada input antena. Ini memungkinkan anda untuk melakukan perubahan kecil pada posisi antena sekaligus memperhatikan alat umpan balik, yang pada intinya berhenti ketika daya maksimum yang diterima sudah ditemukan.

Toolkit pengatur posisi antenna yang ideal terdiri dari ***signal generator*** dan ***spectrum analyzer***, satu untuk masing-masing ujung sambungan. Dengan menghubungkan signal generator ke ujung sambungan dan spectrum analyzer ke ujung yang lainnya, anda dapat memantau daya yang diterima dan memperhatikan efek memindahkan antena ke berbagai posisi dalam waktu yang nyata. Ketika titik maksimum sudah ditemukan pada satu ujung sambungun point-to-point, generator dan analyzer dapat ditukar, dan ulangi proses untuk ujung lainnya.

Penggunaan signal generator lebih diminati daripada menggunakan kartu radio itu sendiri, sebab signal generator dapat membangkitkan sinyal carrier terus menerus. Kartu WiFi memancarkan banyak paket pendek, yang secara cepat menghidupkan dan mematikan pemancar. Ini bisa sangat sulit untuk ditemukan dengan spectrum analyzer, khususnya ketika beroperasi di daerah yang banyak noise / interferensi.

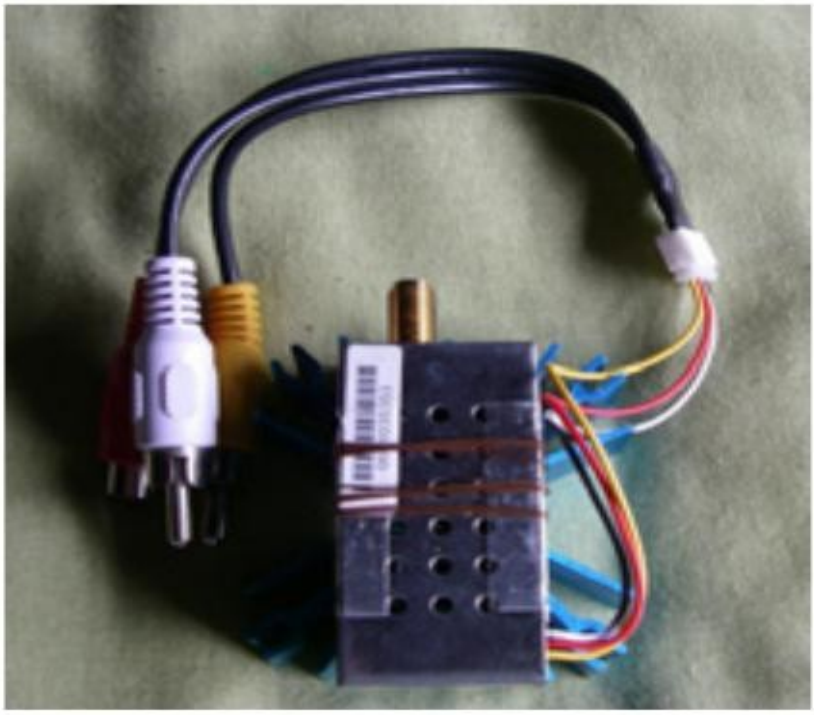
Harga signal generator dan spectrum analyzer yang terkalibrasi dan yang bekerja di 2,4 GHz (atau malah 5 GHz jika menggunakan 802.11a) jauh di luar anggaran kebanyakan proyek. Untungnya, ada sejumlah alat murah yang bisa dipakai sebagai gantinya.

Signal generator murah

Ada banyak pemancar murah yang menggunakan pita ISM 2,4 GHz. Misalnya, telepon cordless, pemantau bayi, dan pemancar televisi miniatur semuanya membangkitkan sinyal yang terus-menerus di 2,4 GHz. Pemancar televisi (kadang-kadang disebut ***pengirim video*** atau ***video senders***) benar-benar berguna, karena mereka seringkali memasukkan konektor antena SMA eksternal dan dapat dihidupkan oleh baterai kecil.
Pengirim video biasanya termasuk dukungan untuk tiga atau empat saluran. Sementara yang ini tidak secara langsung berkaitan dengan saluran WiFi, mereka memungkinkan anda untuk menguji pancaran pada band bawah, tengah, atau atas.

Untuk pekerjaan 5 GHz, anda dapat menggunakan pengirim video dalam kombinasi dengan konverter 2,4 GHz sampai 5 GHz. Alat-alat ini menerima sinyal berdaya rendah 2,4 GHz dan memancarkan sinyal berdaya tinggi 5 GHz . Mereka biasanya cukup mahal (masing-masing

$300-$500), tetapi mungkin akan tetap lebih murah daripada signal generator dan spectrum analyzer 5 GHz.



Gambar 8.7: Pengirim video 2,4 GHz dengan konektor antena SMA

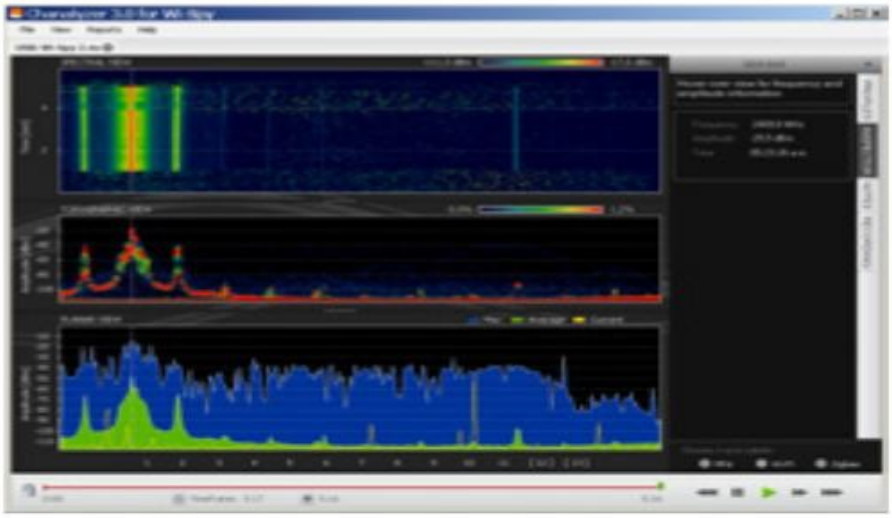
Apapun yang anda pilih sebagai sumber sinyal, anda akan memerlukan sebuah cara untuk menayangkan tingkat daya yang diterima pada ujung lainnya. Sementara biaya spectrum analyzer 2,4 GHz lambat laun menurun, mereka biasanya masih berharga beberapa ribu dolar, bahkan untuk peralatan bekas.

Wi-Spy

Wi-Spy adalah alat analisa spektrum USB yang dibuat oleh MetaGeek (http://www.metageek.net/). Alat ini mempunyai fitur penerima yang sangat sensitif dalam ukuran yang kecil (berukuran sebesar USB ibu jari).

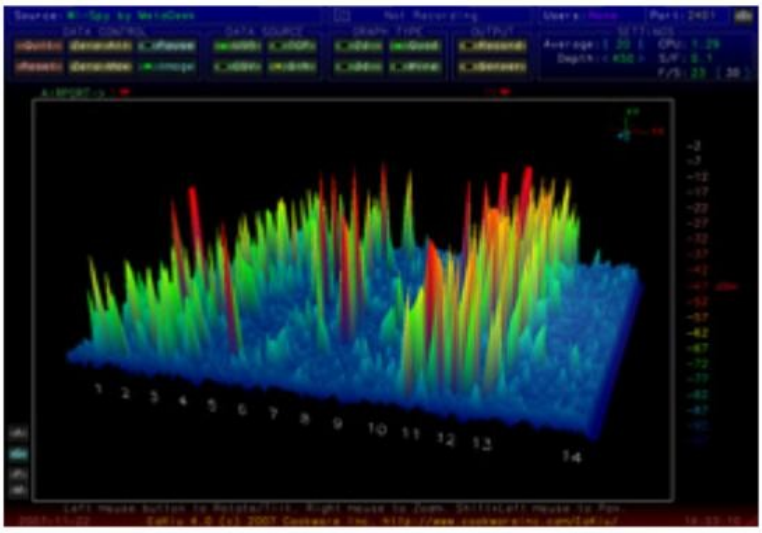
Gambar 8.8: Spectrum Analyzer USB Wi-Spy

Versi terakhir Wi-Spy meliputi jangkauan dinamis yang lebih baik dan konektor antena eksternal. Pada versi ini juga tersedia perangkat lunak spectrum analyzer yang sangat baik untuk Windows yang dinamakan Chanalyzer. Perangkat lunak ini menyediakan sudut pandang seketika, rata-rata, maksimum, topografis, dan spektral.



Gambar 8.9: Pola tajam yang nyata di sebelah kiri gambar disebabkan oleh pemancar televisi 2,4 GHz berdaya tinggi

Ada paket perangkat lunak gratis yang sempurna untuk sistem operasi Mac yang dinamakan EaKiu (http://www.cookwareinc.com/EaKiu). Disamping sudut pandang standar, perangkat lunak ini juga menyediakan sudut pandang 3D, dan menambahkan dukungan untuk beberapa alat Wi-Spy.



Gambar 8.10: Sudut pandang EaKiu memungkinkan anda untuk memutar grafik dan memperjelas bagian grafik yang mana pun di waktu nyata. Mungkin ada jaringan WiFi di saluran 11, dengan sumber bunyi lain yang berada di bagian lebih bawah pita.

Bagi pengguna Linux, Wi-Spy didukung oleh proyek Kismet Spectrum-Tools (http://kismetwireless.net/spectools/). Paket ini termasuk tool command line serta GUI yang dibangun berdasarkan GTK.

Metode lain

Beberapa router nirkabel (seperti Mikrotik) menyediakan "tool pengarah antena" yang memperlihatkan kepada anda sebuah bar yang bergerak yang melambangkan daya yang diterima. Ketika bar adalah maksimum, antena sudah terarah dengan benar. Dengan beberapa router, anda juga dapat mengaktifkan mode umpan balik audio. Ini menyebabkan router akan memancarkan nada tinggi, mengubah volume nada sesuai dengan daya yang diterima.

Jika anda tidak mempunyai spectrum analyzer, Wi-Spy, atau alat yang mendukung mode pengarah antena, anda perlu mempergunakan sistem operasi untuk menyediakan umpan balik mengenai kualitas hubungan nirkabel. Satu metode sederhana untuk melakukan ini dalam Linux adalah dengan loop yang secara terus-menerus memanggil **iwconfig**. Misalnya:

```
wildnet:~# while :; do clear; iwconfig; sleep 1; done
```

Ini akan memperlihatkan keadaan semua kartu radio dalam sistem, memperbarui sekali setiap detik. Perhatikan bahwa ini hanya akan bekerja pada sisi klien sebuah hubungan. Di sisiakses point (master mode), anda sebaiknya menggunakan perintah **iwspy** untuk mengumpulkan data statistik untuk alamat MAC klien:

```
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
```

Anda kemudian dapat menggunakan loop **while** (seperti dalam contoh sebelumnya) untuk secara terus-menerus memperbarui keadaan hubungan.

```
wildnet:~# while :; do clear; iwspy; sleep 1; done
```

Prosedur Mengarahkan antena

Kunci agar dapat secara sukses mengarahkan antena pada sambungan jarak jauh adalah komunikasi. Jika anda merubah terlalu banyak variabel sekaligus (misalnya, satu tim mulai menggoyang-goyangkan antena sedangkan yang lain mencoba mengambil pengukuran kekuatan sinyal), maka proses akan membutuhkan waktu seharian dan mungkin akan berakhir dengan antena yang tidak terarah.

Anda akan mempunyai dua tim. Idealnya, setiap tim sebaiknya mempunyai sedikitnya dua orang: satu untuk mengambil pengukuran sinyal dan berkomunikasi dengan ujung yang sangat jauh, orang yang satunya lagi untuk menggerakkan antena. Ingatlah hal-hal ini selama mengerjakan sambungan jarak jauh.

1. **Uji semua perlengkapan terlebih dahulu**. Anda tidak ingin bermain-main dengan setting ketika anda sudah berada di lapangan. Sebelum memisahkan peralatan, hidupkan segalanya, sambungkan setiap antena dan pigtail, dan pastikan anda dapat menciptakan hubungan di antara alat-alat tersebut. Anda seharusnya dapat kembali ke keadaan yang sudah diketahui ini dengan secara sederhana menghidupkan alat tersebut, tanpa harus log in atau merubah setting apapun. Sekarang adalah waktu yang tepat untuk menyesuaikan polarisasi antena (lihat **Bab 2** jika anda tidak mengerti apa artinya polarisasi).

2. **Bawa perlengkapan komunikasi cadangan**. Walaupun ponsel biasanya cukup baik untuk digunakan di kota, sinyal penerimaan ponsel bisa buruk atau tidak ada di daerah pedesaan. Bawalah radio FRS atau GMRS berdaya tinggi, atau jika tim-tim anda mempunyai ijin radio amatir, gunakan sebuah rig amatir radio. Bekerja di tempat yang jauh bisa membuat frustrasi jika anda selalu bertanya kepada tim lainnya ”apakah kamu bisa mendengarkan saya sekarang?” Pilih saluran komunikasi anda dan tes radio anda (termasuk baterainya) sebelum berpisah.

3. **Bawa sebuah kamera**. Luangkan waktu untuk mendokumentasikan lokasi setiap

tempat, termasuk tanda-tanda penting dan halangan di sekitarnya. Ini dapat menjadi sangat berguna nantinya untuk menentukan kemungkinan hubungan lain ke lokasi tanpa harus mengunjungi tempat itu. Jika ini merupakan perjalanan pertama anda ke tempat tersebut, masukan koordinat GPS beserta ketinggiannya.

4. **Mulai dengan memperkirakan arah dan ketinggian yang benar**. Untuk memulai, kedua tim sebaiknya menggunakan triangulasi (menggunakan koordinat GPS atau sebuah peta) untuk mendapat gambaran arah yang dituju. Gunakan kompas untuk meluruskan antena ke arah yang diinginkan. Tanda-tanda alam atau bangunan besar dapat berguna untuk pengarahan. Jika anda dapat menggunakan teropong untuk melihat ujung yang satunya, maka akan lebih baik. Ketika anda sudah membuat perkiraan anda, lakukan pengukuran kekuatan sinyal. Jika anda cukup dekat dan sudah membuat perkiraan yang baik, anda mungkin sudah mendapatkan sebuah sinyal.

5. **Jika semuanya gagal, buatlah tanda anda sendiri**. Beberapa bentuk kondisi lapangan membuat sulit untuk memperkirakan posisi ujung sambungan yang lainnya. Jika anda sedang membangun sebuah sambungan di daerah dengan sedikit tanpa alam, gunakan / buatlah sendiri tanda tersebut seperti layang-layang, balon, cahaya senter, nyala api, atau bahkan sinyal asap mungkin dapat membantu. Anda tidak terlalu memerlukan sebuah GPS untuk mendapatkan gambaran kemana anda harus mengarahkan antena anda.

6. **Uji sinyal di kedua tempat, tetapi hanya satu setiap saat**. Ketika kedua ujung sudah memiliki perkiraan terbaik, antena ujung dengan gain terendah harus ditetapkan pada posisi-nya. Menggunakan alat pemantau yang baik (seperti Kismet, Netstumbler, atau built-in klien nirkabel yang baik), tim dengan gain antena tertinggi secara perlahan-lahan menyapunya secara horisontal sekaligus mengamati meteran sinyal. Ketika posisi terbaik sudah ditemukan, coba ubah ketinggian antena. Setelah posisi yang mungkin terbaik ditemukan, kuncilah antena secara kukuh pada tempatnya dan beri tanda kepada tim yang lain untuk mulai secara perlahan menyapu tempat sekitar. Ulangi proses ini beberapa kali sampai diperoleh posisi yang terbaik untuk kedua antena.

7. **Jangan sentuh antena ketika mengukur.** Badan anda akan mempengaruhi pola radiasi antena. Jangan sentuh antena, dan jangan berada di garis edar tembakan, ketika mengambil pengukuran kekuatan sinyal. Ini juga berlaku untuk tim yang berada di sisi lain sambungan.

8. **Jangan takut untuk melewati sinyal penerimaan terbaik**. Seperti yang sudah kita lihat di bab empat, pola radiasi antenna terdiri dari beberapa sidelobe yang lebih kecil, disamping sidelobe utama yang jauh lebih besar. Jika sinyal anda yang diterima kecil, anda mungkin sudah menemukan sidelobe. Teruskan melakukan sweeping secara perlahan-lahan melewati sidelobe itu agar dapat menemukan lobe utama.

9. **Sudut antena mungkin tampak salah**. Lobe utama antena kadang hanya berada di satu sisi atau pusat antena sepertinya salah arah. Parabola dengan offset feed akan terlihat mengarah terlalu ke bawah, atau bahkan ke tanah. Jangan khawatir mengenai bagaimana antena terlihat; anda hanya perlu memperhatikan bagaimana mencari posisi terbaik untuk mendapatkan sinyal terbesar yang diterima.

10. **Teliti kembali polarisasi**. Anda dapat menjadi frustrasi untuk mencoba mengarahkan antena hanya karena ternyata tim yang lain menggunakan polarisasi yang berlawanan. Sekali lagi, ini sebaiknya disesuaikan sebelum meninggalkan pangkalan, namun jika sambungan tetap lemah, melakukan pengecekan ulang tidak ada salahnya.

- **Jika tidak ada yang berjalan, periksa semua bagian satu per satu**. Apakah alat pada kedua ujung sambungan telah dihidupkan? Apakah semua pigtail dan konektor sudah dengan semestinya tersambung, dengan tidak ada bagian yang rusak atau ganjil? Seperti yang diuraikan secara garis besar di bab delapan, teknik troubleshooting yang baik akan menghemat waktu dan mencegah frustrasi. Bekerjalah secara perlahan-lahan dan komunikasikan status anda dengan baik dengan tim yang lain.

Dengan bekerja secara terstruktur dan berkomunikasi dengan baik, anda dapat menyelesaikan pekerjaan pengarahan antena dengan gain yang tinggi dalam waktu yang singkat saja. Jika dilakukan dengan semestinya, ini seharusnya menjadi sesuatu yang menyenangkan!

Perlindungan sentakan dan kilat

Penyediaan daya adalah tantangan terbesar bagi kebanyakan instalasi di dunia berkembang. Di mana ada jaringan listrik, jaringan tersebut seringkali tidak terkontrol secara baik, berfluktuasi secara dramatis, dan rentan terhadap kilat. Perlindungan sentakan yang baik adalah kritis tidak hanya untuk melindungi peralatan nirkabel anda, tetapi juga seluruh peralatan yang tersambung dengannya.

Sekering dan sakelar pemutus sirkuit

Di daerah pedesaan, dan bahkan di banyak daerah perkotaan negara berkembang, sekering sulit ditemukan. Meskipun ada biaya tambahan, sangat bijak untuk memakai sakelar pemutus sebagai alternatif. Yang ini mungkin perlu diimpor, tetapi sebaiknya tidak diabaikan. Seringkali, sekering yang dapat diganti disingkirkan dan uang koin malahan digunakan. Dalam kasus terbaru, seluruh peralatan elektronik di stasiun pemancar radio pedesaan hancur ketika sambaran kilat menembus sirkuit, tanpa adanya sakelar pemutus sirkuit atau bahkan sekering untuk melindunginya.

Cara menghubungkan ke tanah

Grounding atau penghubungan ke tanah yang baik tidak harus rumit. Ketika meng-ground-kan, anda berusaha untuk menyelesaikan dua hal: menyediakan sebuah rangkaian arus pendek untuk sambaran petir, dan menyediakan sebuah sirkuit untuk kelebihan daya yang akan dibuang.

Langkah pertama adalah melindungi peralatan dari sambaran kilat langsung atau dekat, sedangkan yang kedua adalah menyediakan jalur untuk membuang kelebihan daya yang akan menyebabkan pengumpulan listrik statis. Listrik statis ini dapat menyebabkan degradasi yang luar biasa pada kualitas sinyal, khususnya pada kepekaan penerima (misalnya, VSAT). Menyediakan rangkaian arus pendek sederhana. Tukang hanya perlu membuat jalur terpendek menggunakan kabel / permukaan yang sangat konduktif (tangkai kilat) ke tanah. Ketika petir menyambar tangkai, energi akan melewati jalur terpendek dan oleh sebab itu melompati peralatan. Ground ini sebaiknya dapat menangani tegangan tinggi (seperti ketika anda memerlukan kawat tebal, seperti tembaga lilitan ukuran 8-gauge).

Untuk menghubungkan peralatan ke tanah, letakkan sebuah tangkai petir diatas peralatan yang terpasang pada sebuah menara atau struktur lainnya. Lalu gunakan kawat konduktif gauge yang tebal untuk menghubungkan tangkai ke sesuatu yang juga terhubung ke tanah secara baik. Pipa tembaga bawah tanah dapat terhubung ke tanah secara baik (tergantung pada kedalaman mereka, kelembaban, salinitas, jumlah logam dan kandungan organik tanah). Di banyak tempat di Afrika Barat, pipa belum berada dalam tanah, dan peralatan penghubungan ke tanah sebelumnya seringkali tidak cukup dikarenakan tanah yang tidak konduktif (khas tanah tropis yang gersang secara musiman). Ada tiga cara mudah untuk mengukur efisiensi hubungan ke tanah anda:

Cara yang sangat tidak akurat adalah secara sederhana menancapkan UPS berkualitas baik atau kabel listrik ke rangkaian yang mempunyai indikator deteksi hubungan tanah (lampu LED). LED ini dinyalakan oleh listrik yang mengalir ke sirkuit penghubungan ke tanah. Penghubungan ke tanah yang efektif akan menghilangkan sedikit tenaga ke tanah. Beberapa orang sebetulnya mempergunakan ini untuk mencuri sedikit penerangan gratis, karena tenaga ini tidak memutar meteran listrik!

Ambil soket listrik dan bola lampu ber-Watt rendah (30 Watt), hubungkan satu kawat ke kawat tanah dan yang kedua ke kawat yang lain. Jika hubungan ke tanah berhasil, maka bola lampu akan menyala sedikit.

Cara yang lebih canggih adalah secara sederhana mengukur impedansi antara kontak positif dan tanah.

Jika tanah anda tidak efisien, anda akan perlu mengubur tangkai yang tertancap lebih dalam lagi (dimana tanahnya lebih lembab, mempunyai lebih banyak zat organik dan logam) atau anda perlu membuat tanah agar lebih konduktif. Sebuah pendekatan yang umum dimana ada

sedikit tanah adalah menggali lubang berdiameter 1 meter dan berkedalaman 2 meter. Letakkan lempengan logam yang sangat konduktif yang berat. Ini seringkali dinamakan sebuah ***plomb***, yang secara literal artinya timbal namun bisa berupa logam berat apapun seberat 50 kg atau lebih, seperti misalnya paron besi atau roda baja. Lalu isi lubang dengan arang dan campurkan garam, lalu timbun bagian atas dengan tanah. Basahkan bagian tersebut, dan arang dan garam akan menyebar di sekitar lubang dan membuat bagian konduktif mengelilingi plomb anda, meningkatkan efisiensi tanah.

Jika kabel radio digunakan, kabel tersebut juga dapat dipergunakan untuk menghubungkan menara ke tanah, meskipun disain yang lebih kuat adalah untuk memisahkan penghubungan ke tanah untuk menara dari kabel. Untuk menghubungkan kabel ke tanah, secara sederhana kupas sedikit kulit kabel di titik terdekat ke tanah sebelum kabel tersebut memasuki bangunan, lalu sambungkan kabel penghubung ke tanah dari titik itu, baik dengan menyolder ataupun menggunakan konektor yang sangat konduktif. Ini kemudian perlu dibuat kedap air.

Stabilizer & regulator daya

Ada banyak merek stabiliator daya, tetapi kebanyakan adalah digital atau mekanis-elektro. Yang terakhir jauh lebih murah dan lebih biasa. Stabiliator mekanis-elektro menerima daya di 220V, 240V, atau 110V dan menggunakan energi itu untuk menjalankan motor, yang selalu menghasilkan tegangan yang diinginkan (biasanya 220V). Ini biasanya efektif, namun satuan-satuan ini menawarkan perlindungan yang sedikit dari kilat ataupun sentakan listrik lainnya. Mereka seringkali terbakar setelah satu sambaran saja. Setelah terbakar, mereka sebetulnya terpatri pada tegangan output tertentu (yang biasanya salah).

Regulator digital mengatur daya menggunakan hambatan dan komponen elektronik lainnya. Mereka lebih mahal, tetapi tidak terlalu rentan terhadap kebakaran.

Sebisa mungkin, gunakan regulator digital. Mereka sepadan nilainya dengan biaya tambahan, dan akan memberikan perlindungan yang lebih baik untuk sisa peralatan anda. Pastikan untuk memeriksa semua komponen sistem daya anda (termasuk stabiliator) setelah terjadinya kilat.

Bab 9 Troubleshooting

Bagaimana anda membuat infrastruktur penyangga untuk jaringan sama pentingnya dengan peralatan jenis apa yang anda gunakan. Tidak seperti sambungan berkawat, permasalahan dengan jaringan nirkabel seringkali tidak kelihatan, dan memerlukan kemampuan yang lebih dan lebih banyak waktu untuk meng-diagnosa dan memperbaiki. Gangguan, angin, dan hambatan fisik yang baru dapat menyebabkan sebuah jaringan yang sudah lama berfungsi untuk gagal. Bab ini menjelaskan secara detil beberapa strategi untuk membantu anda untuk membentuk sebuah tim yang dapat secara efektif mendukung jaringan anda.

Membentuk tim

Di setiap desa, perusahaan atau keluarga terdapat orang-orang yang tertarik pada teknologi. Mereka adalah yang memotong kabel televisi, memperbaiki televisi yang rusak atau melas bagian sepeda. Orang-orang ini akan tertarik pada jaringan anda dan ingin mempelajarinya sebanyak mungkin. Meski orang-orang ini adalah sumber yang berharga, anda harus menghindari membebankan semua ilmu khusus jaringan nirkabel hanya pada satu orang. Jika ahli anda satu-satunya kehilangan minat atau menemukan pekerjaan dengan gaji yang lebih baik di tempat lain, mereka akan membawa ilmu tersebut bersama mereka kemana saja mereka pergi.

Mungkin juga ada remaja muda dan ambisius atau orang dewasa muda yang akan tertarik dan yang memiliki waktu baik untuk mempelajari jaringan tersebut maupun membantu memasangnya. Sekali lagi, mereka sangat berguna dan akan belajar dengan cepat, namun tim proyek harus memfokuskan perhatian mereka pada mereka yang sebaiknya ditempatkan untuk mendukung jaringan tersebut dalam bulan dan tahun yang akan datang. Orang dewasa dan remaja akan pergi ke universitas atau mencari lowongan kerja, khususnya mereka yang muda dan ambisius yang ingin terlibat. Anak-anak muda ini juga memiliki pengaruh kecil dalam komunitas, dimana orang yang lebih tua mungkin akan lebih mampu untuk membuat keputusan yang secara positif berdampak pada jaringan secara keseluruhan. Walaupun orang-orang yang lebih tua ini mungkin memiliki waktu yang lebih sedikit untuk belajar dan mungkin sepertinya kurang tertarik, peran serta mereka dan pendidikan mereka yang baik mengenai sistem bisa kritis.

Maka, sebuah strategi utama dalam membentuk tim pendukung adalah menyeimbangkan dan membagi pengetahuan di antara mereka yang dapat mendukung jaringan untuk jangka waktu yang lama. Anda sebaiknya melibatkan yang muda, tetapi biarkan mereka mengkapitalisasi kegunaan atau pengetahuan sistem ini. Carilah mereka yang memiliki komitmen terhadap komunitas, yang berakar dalam komunitas, yang dapat dimotivasi, dan ajari mereka. Sebuah strategi pelengkap adalah membagi-bagi fungsi dan tugas, dan mengdokumentasikan semua metodologi dan prosedur. Dengan cara ini, masyarakat dapat

dilatih secara mudah, dan diganti dengan jerih payah yang sedikit.

Sebagai contoh, dalam sebuah proyek tim pelatihan memilih seorang lulusan universitas yang cerdas yang telah kembali ke desanya. Ia sangat termotivasi dan belajar dengan cepat. Karena dia belajar begitu cepat, ia diajarkan lebih daripada apa yang ia pernah lihat, dan ia dapat mengatasi berbagai masalah, dari memperbaiki sebuah komputer sampai memasang kabel Ethernet. Sayangnya, dua bulan setelah peluncuran proyek ia ditawari sebuah pekerjaan di pemerintahan dan meninggalkan komunitas tersebut. Gaji tinggi pun tidak dapat menahannya, karena prospek pekerjaan pemerintah yang stabil sangat menggiurkan. Semua pengetahuan mengenai jaringan dan bagaimana mendukungnya hilang bersamanya. Tim pelatihan harus kembali lagi dan memulai pelatihan lagi. Strategi yang berikutnya adalah membagi fungsi, dan melatih mereka yang selamanya tinggal dalam komunitas: mereka yang memiliki rumah dan anak, dan sudah bekerja. Ini membutuhkan waktu tiga kali lebih lama untuk melatih tiga orang daripada melatih lulusan universitas tersebut, namun komunitas itu akan menyimpan ilmu ini untuk waktu yang lebih lama.

Walau ini sepertinya menyarankan bahwa anda harus memilih siapa yang akan terlibat, seringkali pendekatan ini bukanlah yang terbaik. Adalah seringkali terbaik untuk mencari partner organisasi lokal atau manajer lokal, dan bekerja sama dengan mereka untuk mencari tim teknis yang tepat. Nilai, sejarah, politik lokal, dan banyak faktor lainnya akan menjadi penting untuk mereka, sementara tetap tidak dapat dimengerti oleh mereka yang bukan dari komunitas itu. Cara yang terbaik adalah melatih partner lokal anda, memberikan mereka kriteria yang jelas, memastikan bahwa mereka memahami kriteria itu, dan menentukan ketentuan-ketentuan yang tegas. Ketentuan-ketentuan seperti ini sebaiknya meliputi peraturan-peraturan mengenai nepotisme dan pembagian tugas, meskipun peraturan-peraturan ini juga harus mempertimbangkan kondisi lokal. Adalah mustahil untuk mengatakan bahwa anda tidak dapat memperkerjakan teman atau relasi, tetapi akan menjadi sangat baik untuk menyediakan cara check and balance. Dimana seorang kandidat adalah relasi, haruslah ada kriteria yang jelas dan otoritas kedua dalam memutuskan kekandidatan mereka. Adalah penting juga bahwa partner lokal diberikan otoritas ini dan tidak disisihkan oleh organisator proyek tersebut, sehingga mengganggu kemampuan mereka untuk mengatur. Mereka akan sangat baik untuk menilai siapa yang sebaiknya bekerja dengan mereka. Jika mereka sangat mengerti proses ini, maka kebutuhan anda akan terpenuhi.

Troubleshooting dan dukungan teknologi adalah seni yang abstrak. Pertama kali anda melihat lukisan abstrak, ini mungkin terlihat oleh anda seperti kumpulan bercak cat asal-asalan. Setelah merefleksikan komposisinya untuk beberapa lama, anda mungkin menghargai karya tersebut secara keseluruhan, dan koherensinya yang sebelumnya “tidak kelihatan” menjadi sangat nyata. Para orang awam/pemula yang melihat jaringan nirkabel mungkin akan melihat antena, kabel dan komputernya, namun akan membutuhkan waktu yang lama bagi mereka untuk dapat memahami maksud jaringan yang “tidak kelihatan”. Di daerah pedesaan, ini kadang membutuhkan sebuah lompatan besar pengertian sebelum masyarakat lokal dapat memahami jaringan yang tidak kelihatan yang dengan mudahnya disediakan di desa mereka. Oleh karena itu, sebuah pendekatan bertahap diperlukan untuk memudahkan orang untuk mendukung sistem teknologi. Metode yang terbaik adalah

keterlibatan. Ketika peserta sudah dipilih dan berkomitmen pada proyek, libatkan mereka sebisa mungkin. Biarkan mereka menjalankan. Berikan mereka crimper kabel atau keyboard dan tunjukan kepada mereka bagaimana melakukan pekerjaannya. Meski anda tidak mempunyai waktu untuk menjelaskan setiap detil dan walaupun dibutuhkan lebih banyak waktu, mereka harus dilibatkan secara fisik dan melihat tidak hanya apa yang sudah dikerjakan namun juga seberapa banyak pekerjaan yang sudah dilakukan.

Metode ilimiah diajari di hampir semua sekolah Barat. Banyak orang belajar mengenainya pada saat mereka masuk kelas ilmiah sekolah menengah atas. Dengan kata lain, anda mengambil sekelompok variabel, lalu secara perlahan-lahan mengeliminir variabel-variabel itu melalui tes binary sampai anda tersisa hanya satu atau beberapa kemungkinan. Dengan kemungkinan-kemungkinan ini di benak anda, anda menyelesaikan eksperimen tersebut. Anda lalu menguji untuk melihat apakah eksperimen itu menghasilkan sesuatu yang sama dengan hasil yang diharapkan. Jika tidak sama, anda hitung ulang hasil yang anda harapkan dan cobalah sekali lagi. Orang pedesaan yang biasa mungkin dapat diperkenalkan kepada konsep tersebut, tetapi tidak akan memiliki kesempatan untuk memperbaiki permasalahan yang rumit. Walaupun mereka mengenali metode ilmiah itu, mereka mungkin tidak terpikir untuk menerapkannya terhadap pemecahan masalah yang nyata.

Metode ini sangat efektif, walaupun memakan waktu yang banyak. Metode ini dapat dipercepat dengan membuat asumsi logis. Misalnya, jika sebuah titik akses yang sudah cukup lama berfungsi tiba-tiba berhenti berfungsi setelah adanya badai, anda dapat menebaknya sebagai sebuah masalah terkait sumber daya dan oleh sebab itu meloncati sebagian besar prosedur. Orang yang bertanggung jawab untuk mendukung teknologi harus diajarkan bagaimana memecahkan masalah menggunakan metode ini, karena akan ada waktu ketika permasalahan ini tidak dikenali ataupun kelihatan. Diagram pohon keputusan yang sederhana atau flow chart dapat dibuat untuk menguji variabel-variabel ini, dan cobalah untuk mengeliminir variabel untuk mengisolasi permasalahan. Tentunya, diagram ini sebaiknya tidak diikuti secara membabi buta.

Adalah seringkali lebih mudah untuk mengajarkan metode ini pertama-tama menggunakan permasalahan non-teknologi. Sebagai contoh, buatlah murid anda membangun sebuah prosedur pemecahan masalah pada sesuatu yang sederhana dan dikenali, seperti televisi yang dihidupkan oleh baterai. Mulailah dengan menyabotase televisi tersebut. Berikan mereka baterai yang tidak terisi. Lepaskan antenanya. Masukan sekering yang rusak. Uji sang murid, dengan membuat jelas bahwa setiap permasalahan akan menunjukan gejala yang spesifik, dan tunjukkan jalannya bagaimana untuk melanjutkan.

Ketika mereka sudah memperbaiki televisinya, instruksikan mereka untuk menerapkan prosedur ini pada permasalahan yang lebih rumit. Dalam sebuah jaringan, anda dapat merubah sebuah alamat IP, mengganti atau merusak kabel, menggunakan SSID yang salah, atau mengarahkan antena ke arah yang salah. Adalah penting bahwa mereka membangun sebuah metodologi dan prosedur untuk mengatasi masalah-masalah ini.

Teknik pemecahan masalah yang baik

Tidak ada metodologi troubleshooting yang dapat secara keseluruhan mengatasi semua masalah yang anda temukan ketika bekerja dengan jaringan-jaringan nirkabel. Namun seringkali, masalah biasanya berupa satu dari beberapa kesalahan yang umum. Berikut ini adalah beberapa petunjuk yang sebaiknya diingat agar usaha pemecahan masalah anda berada di jalur yang benar.

Jangan panik. Jika anda meng-troubleshoot sebuah sistem, ini berarti bahwa alat itu pernah berfungsi, bahkan mungkin baru-baru saja. Sebelum bergerak dan membuat perubahan, surveilah situasi dan teliti secara seksama apa yang rusak. Jika anda memiliki log historis atau data statistik yang anda bisa acu, semakin baik. Pastikan untuk pertama-tama mengumpulkan informasi, sehingga anda dapat mengambil keputusan berinformasi sebelum membuat perubahan.

Apakah sudah tercolok? Langkah ini seringkali diabaikan sampai semua pilihan tereksplorasi. Colokan dapat baik secara sengaja ataupun tidak sengaja terlepas secara mudah. Apakah tembaga tersambung pada sumber daya yang baik? Apakah ujung yang lain tersambung ke alat anda? Apakah lampu sumber daya menyala? Ini mungkin terkesan bodoh, tetapi anda akan merasa lebih bodoh jika anda meluangkan banyak waktu mengecek sebuah jalur input antena hanya untuk menyadari bahwa colokan titik akses ternyata terlepas. Percayalah, ini lebih sering terjadi daripada kebanyakan dari kita yang mau mengaku.

Apa yang terakhir kali dirubah? Jika anda merupakan satu-satunya orang dengan akses ke sistem, apakah yang paling terakhir anda rubah? Jika orang lain memiliki akses, apakah perubahan terakhir yang mereka buat dan kapan? Kapan terakhir kali sistem bekerja? Seringkali, perubahan-perubahan sistem memiliki konsekuensi yang tidak diinginkan yang mungkin tidak dapat secara langsung ditemukan. Kembalikan ke konfigurasi semula dan perhatikan efek apa yang dilakukannya terhadap permasalahan.

Buatlah backup. Ini berlaku sebelum anda menemukan masalah, serta setelahnya. Jika anda membuat perubahan perangkat lunak yang rumit pada sebuah sistem, memiliki sebuah backup berarti anda dapat secara cepat mengembalikannya ke konfigurasi sebelumnya dan memulai kembali. Ketika memecahkan masalah yang sangat rumit, memiliki sebuah konfigurasi yang “kira-kira” dapat bekerja jauh lebih baik daripada menghadapi kerumitan yang tidak dapat bekerja sama sekali (dan ini bukanlah sesuatu yang anda dapat kembalikan secara mudah dari memori).

Sesuatu yang baik yang diketahui. Gagasan ini berlaku pada perangkat keras, serta lunak. **Sesuatu yang baik yang diketahui** adalah komponen apapun yang anda dapat tukar dalam sebuah sistem yang kompleks untuk mengecek bahwa komponen yang sama yang terpasang berada dalam kondisi yang baik dan berfungsi. Misalnya, anda mungkin membawa sebuah kabel Ethernet yang sudah diuji dalam kotak perlengkapan anda. Jika anda menduga ada masalah dengan kabel di lapangan, anda dapat secara mudah mengganti kabel yang

bermasalah tersebut dengan kabel yang sudah diuji tersebut dan melihat apakah kondisinya membaik. Ini jauh lebih cepat dan memiliki kerentanan kesalahan yang lebih sedikit dibandingkan dengan meng-crimping sebuah kabel, dan secara langsung memberitahu anda apakah perubahan tersebut menyelesaikan masalah. Begitu pula, anda juga dapat memasukan sebuah baterai, kabel antena, atau CD-ROM cadangan dengan konfigurasi yang sudah dianggap baik untuk sistem tersebut. Ketika memperbaiki masalah yang rumit, menyimpan pekerjaan anda pada suatu tahap memungkinkan anda untuk kembali ke sesuatu yang baik yang diketahui, walaupun masalah tersebut belum sepenuhnya teratasi.

Rubahlah variabel satu per satu. Ketika dalam tekanan untuk menghidupkan sistem yang rusak kembali online, sangatlah menggiurkan untuk langsung bergerak dan merubah beberapa variabel sekaligus. Jika anda tetap melakukan ini, dan perubahan anda sepertinya memperbaiki permasalahannya, maka anda tidak akan mengerti secara persis apa yang sebenarnya menimbulkan masalah tersebut pada awalnya. Lebih buruk lagi, perubahan anda mungkin memperbaiki permasalahan utama, namun menimbulkan konsekuensi yang tidak diinginkan yang merusak bagian lain sistem. Dengan merubah variabel anda satu per satu, anda dapat secara persis memahami apa yang mula-mula salah, dan dapat melihat efek langsung dari perubahan yang anda buat.

Jangan merusak. Jika anda tidak sepenuhnya mengerti bagaimana sebuah sistem berfungsi, janganlah ragu-ragu untuk memanggil seseorang yang ahli. Jika anda tidak yakin apakah sebuah perubahan akan merusak bagian sistem, maka carilah seorang yang ahli dengan banyak pengalaman atau buat sebuah cara untuk menguji perubahan anda tanpa merusak. Meletakan sebuah koin logam sebagai pengganti sekering mungkin akan menyelesaikan masalah secara langsung, namun mungkin juga akan menyebabkan kebakaran.

Sepertinya tidak mungkin orang yang mendesain jaringan anda akan tersedia 24 jam setiap hari untuk memperbaiki kesalahan ketika mereka muncul. Tim troubleshooting anda akan memerlukan keahlian troubleshooting yang baik, tetapi mungkin tidak cukup kompeten untuk mengkonfigurasi router dari nol atau untuk meng-crimp sebuah bagian dari LMR-400. Adalah seringkali lebih efisien untuk membuat beberapa komponen backup selalu tersedia, dan melatih tim anda untuk dapat mengganti seluruh bagian yang rusak. Ini dapat berarti memiliki sebuah titik akses yang sudah dikonfigurasikan dan tersedia di lemari yang terkunci, dilabel secara sederhana, dan disimpan dengan kabel dan sumber daya cadangan.

Tim anda dapat menukar komponen yang gagal, dan entah mengirim bagian yang rusak ke yang ahli untuk diperbaiki, atau mengatur agar cadangan dikirim. Mengasumsikan cadangan tersebut tersimpan dengan aman dan diganti ketika digunakan, ini akan menghemat banyak waktu untuk siapa saja.

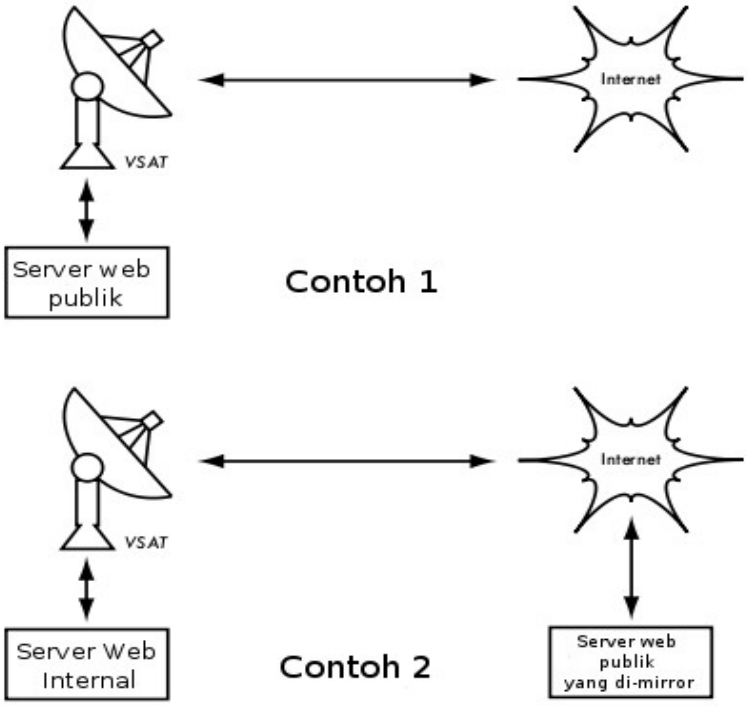
Permasalahan umum jaringan

Seringkali, permasalahan sambungan ditimbulkan oleh komponen yang gagal, cuaca yang

tidak baik, atau kesalahan konfigurasi yang sederhana. Ketika jaringan anda sudah tersambung ke Internet atau terbuka kepada publik, ancaman yang besar akan datang dari pengguna jaringan itu sendiri. Ancaman ini mulai dari yang paling ringan sampai yang paling berat, namun semuanya mempunyai dampak pada jaringan anda jika tidak dikonfigurasikan secara benar. Bagian ini melihat pada beberapa masalah umum yang ditemukan ketika jaringan anda digunakan oleh manusia sesungguhnya.

Situs web yang disimpan secara lokal

Jika sebuah universitas menyimpan situs web-nya secara lokal, pengunjung situs dari luar kampus dan dunia lainnya akan bersaing dengan staf universitas untuk lebar pita Internet. Ini termasuk akses otomatis dari mesin pencari yang secara berkala mengunjungi seluruh situs anda. Satu pemecahan untuk masalah ini adalah menggunakan DNS terpisah dan mirroring. Universitas me-mirror sebuah kopi websitenya ke sebuah server, katakanlah, di sebuah perusahaan hosting di Eropa, dan menggunakan DNS terpisah untuk mengarahkan semua pengguna dari luar jaringan universitas ke situs mirror, sedangkan pengguna di universitas mengakses situs yang sama secara lokal. Detil mengenai bagaimana mempersiapkan ini tersedia di bab tiga.



Gambar 9.1: Dalam contoh 1, semua lalu lintas situs web yang datang dari Internet harus berjalan melalui VSAT. Dalam contoh 2, situs web publik disimpan di jasa cepat Eropa, sedangkan sebuah kopi disimpan di server internal untuk akses lokal yang sangat cepat. Ini meningkatkan koneksi VSAT dan mengurangi waktu muat untuk pengguna situs web.

Proxy terbuka

Sebuah server proxy sebaiknya dikonfigurasikan agar hanya menerima sambungan dari jaringan universitas, bukan dari Internet. Ini karena orang-orang di tempat lain akan menyambung ke dan menggunakan proxy terbuka karena berbagai macam alasan, seperti menghindari membayar bandwidth internasional. Cara untuk mengkonfigurasikan ini bergantung pada server proxy yang anda sedang gunakan. Misalnya, anda dapat memspesifikasi alamat IP jaringan kampus dalam file **squid.conf** anda sebagai satu-satunya jaringan yang dapat menggunakan Squid. Alternatif lainnya, jika server proxy anda berada di belakang sebuah firewall pagar, anda dapat mengkonfigurasikan firewall itu agar hanya mengijinkan host internal untuk menyambung ke port proxy.

Host relay terbuka

Sebuah mail server yang terkonfigurasi secara tidak benar akan ditemukan oleh oknum di Internet, dan digunakan sebagai host relay untuk mengirim email dan spam bervolume besar. Mereka melakukan ini untuk menyembunyikan sumber asli spam, dan menghindar agar tidak tertangkap. Untuk mengetes host relay terbuka, tes yang berikut ini sebaiknya dijalankan pada mail server anda (atau pada server SMTP yang berfungsi sebagai host relay pada perimeter jaringan kampus). Gunakan ***telnet*** untuk membuka sebuah sambungan ke port 25 dari server yang sedang digunakan (dengan beberapa versi telnet Windows, kita mungkin perlu untuk mengetik 'set local_echo' sebelum text-nya dapat terlihat):

```
telnet mail.uzz.ac.zz 25
```

Kemudian, jika sebuah baris perintah percakapan interaktif dapat terjadi (sebagai contoh, seperti yang berikut ini), server tersebut merupakan host relay terbuka:

```
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
```

Malahan, balasan setelah MAIL FROM yang pertama kira-kira seperti ini:

```
550 Relaying is prohibited.
```

Sebuah tester online tersedia di situs seperti *http://www.ordb.org/*. Ada juga informasi tentang masalah tersebut di situs ini. Karena pengirim email bervolume besar mempunyai metode otomatis untuk mencari host relay terbuka seperti ini, sebuah institusi yang tidak melindungi sistem suratnya sudah pasti dijamin akan ditemukan dan diganggu. Mengkonfigurasikan server surat agar tidak menjadi relay terbuka meliputi memspesifikasikan jaringan dan host

yang diijinkan untuk me-relay surat melalui mereka dalam MTA (misalnya, Sendmail, Postfix, Exim, atau Exchange). Ini mungkin akan menjadi alamat IP jaringan kampus.

Jaringan peer-to-peer

Gangguan pita lebar melalui program berbagi-file peer-to-peer (P2P) seperti Kazaa, Mospheus, BitTorrent, WinMX dan BearShare dapat dicegah dengan cara berikut:

- **Buatlah mustahil untuk meng-instal program baru pada komputer kampus**. Dengan tidak memberikan pengguna biasa akses administratif ke workstation PC, sangatlah mungkin untuk mencegah instalasi program seperti Kazaa. Banyak lembaga juga berstandar pada sebuah rakitan desktop, dimana mereka menginstal sistem operasi yang dibutuhkan pada satu PC. Mereka kemudian menginstal semua aplikasi yang dibutuhkan pada PC ini, dan mengkonfigurasi aplikasi-aplikasi ini secara optimal. PC juga dikonfigurasikan dalam cara yang mencegah agar pengguna tidak dapat menginstal aplikasi-aplikasi baru. Kopi disk PC ini kemudian di-duplikasikan ke semua PC lainnya menggunakan software seperti Partition Image (lihat *http://www.partimage.org/*) atau Drive Image Pro (lihat *http://www.powerquest.com/*).

  Dari waktu ke waktu, pengguna mungkin berhasil dalam menginstal perangkat lunak baru atau sebaliknya merusak perangkat lunak pada komputer (membuatnya terlalu sering hang, misalnya). Ketika ini terjadi, seorang administrator dapat secara mudah mengembalikan kopi disk, membuat sistem operasi dan semua software para komputer itu menjadi sama seperti yang dispesifikasikan.

- **Memblok protokol-protokol ini bukanlah sebuah solusi**. Ini karena Kazaa dan protokol lainnya cukup canggih untuk memotong jalur port yang diblok. Kazaa meng-default pada port 1214 untuk sambungan awal, namun jika ini tidak tersedia, Kazaa akan mencoba untuk menggunakan port 1000 sampai 4000. Jika ini diblok, Kazaa menggunakan port 80, membuatnya seperti lalu lintas web. Karena alasan ini, ISPs tidak membloknya, tetapi mempercepatnya menggunakan alat manajemen bandwidth.

- **Jika pembatasan laju bukanlah sebuah pilihan, gantilah layout jaringan**. Jika server proxy dan server surat dikonfigurasikan dengan dua kartu jaringan (seperti yang dideskripsikan dalam bab tiga) dan server-server ini tidak terkonfigurasi untuk meneruskan paket apapun, ini akan memblok semua lalu lintas P2P. Ini juga akan memblok semua jenis lalu lintas lainnya, seperti Microsoft NetMeeting, SSH, VPN software, dan semua jasa lainnya yang tidak secara spesifik diperbolehkan oleh server proxy. Dalam jaringan bandwidth rendah, mungkin dapat diputuskan bahwa kesederhanaan desain ini akan melebihi kerugiannya. Keputusan seperti ini mungkin diperlukan, namun jangan dianggap remeh. Administrator jaringan tidak dapat secara sederhana meramalkan bagaimana pengguna akan menggunakan jaringan secara inovatif. Dengan memblok semua akses terlebih dahulu, anda akan mencegah pengguna dari memanfaatkan kegunaan layanan apapun (bandwidth rendah sekalipun) yang tidak

didukung oleh proxy anda. Sementara ini mungkin diharapkan dalam keadaan bandwidth yang sangat rendah, ini tidak boleh pernah dianggap sebagai kebijakan akses yang baik dalam kasus yang umum.

Program yang menginstal dirinya sendiri (dari internet)

Ada program-program yang secara otomatis menginstal dirinya sendiri dan kemudian tetap menggunakan bandwidth – sebagai contoh, Bonzi-Buddy yang terkenal, Microsoft Network, dan beberapa jenis worm lainnya. Beberapa program merupakan spyware, yang tetap mengirim informasi mengenai kebiasaan browsing seorang pengguna kepada sebuah perusahaan yang berlokasi di suatu tempat di Internet. Program-program ini dapat dicegah sampai batas tertentu dengan pendidikan untuk pengguna dan mengunci PC untuk mencegah akses administratif untuk pengguna normal. Dalam kasus-kasus lainnya, ada solusi perangkat lunak untuk mencari dan membuang program-program bermasalah ini, seperti Sphychecker (*http://www.spychecker.com/*) atau Ad-Aware (*http://www.lavasoft.de/*).

Update Windows

Sistem operasi Microsoft Windows yang terbaru mengasumsikan bahwa sebuah komputer dengan sambungan LAN mempunyai sambungan yang baik ke Internet, dan secara otomatis meng-download patch-patch keamanan, perbaikan bug, dan peningkatan fitur dari situs web Microsoft. Ini dapat menghabiskan bandwidth dalam jumlah besar pada sambungan Internet yang mahal. Dua pendekatan yang mungkin untuk masalah ini adalah:

- **Non-aktifkan update Windows pada semua workstation PC.** Update keamanan sangatlah penting untuk server, tetapi apakah workstation dalam jaringan pribadi yang terlindungi seperti jaringan kampus membutuhkan mereka adalah sesuatu yang dapat diperdebatkan.

- **Menginstal Update Server Perangkat Lunak.** Ini adalah program gratis dari Microsoft yang memungkinkan anda untuk meng-download semua update dari Microsoft dalam waktu singkat ke sebuah server lokal dan mengdistribusikan update tersebut ke workstation pengguna dari situ. Dalam cara ini, update Windows tidak perlu menggunakan bandwidth pada sambungan Internet pada siang hari. Sayangnya, semua PC pengguna harus dikonfigurasikan agar dapat menggunakan server update perangkat lunak agar ini dapat berdampak. Jika anda memiliki server DNS yang fleksibel, anda juga dapat mengkonfigurasikannya untuk menjawab permintaan untuk *windowsupdate.microsoft.com* dan mengalihkan updater ke server update anda. Ini hanya merupakan pilihan yang baik untuk jaringan yang sangat besar, namun dapat menghemat bandwidth Internet yang tak terbilang jumlahnya.

Memblok situs update Windows pada server proxy bukanlah sebuah solusi yang baik karena layanan update Windows (update otomatis) tetap mencoba berulang-ulang secara agresif,

dan jika semua workstation melakukan itu, ini akan memberikan beban yang besar pada server proxy. Cuplikan dibawah ini adalah dari log proxy (log akses Squid) dimana ini dilakukan dengan memblok kabinet Microsoft (.cab) files.

Kebanyakan dari log Squid tampil seperti ini:

```
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
```

Meski ini mungkin dapat ditoleransikan untuk beberapa klien PC, permasalahan berkembang secara luar biasa sewaktu host ditambahkan ke jaringan. Daripada memaksakan server proxy untuk melayani permintaan yang akan selalu gagal, adalah lebih masuk akal untuk mengalihkan klien perangkat lunak update ke sebuah server update lokal.

Program yang mengasumsikan sambungan bandwidth tinggi

Disamping update Windows, beberapa program dan layanan lainnya berasumsi bahwa bandwidth bukanlah masalah, dan oleh karena itu menggunakan bandwidth untuk alasan yang mungkin tidak dimengerti oleh si pengguna. Sebagai contoh, paket anti-virus (seperti AntiVirus Norton) secara berkala meng-update dirinya sendiri secara otomatis dan secara langsung dari Internet. Adalah lebih baik jika update-update ini didistribusikan dari server lokal.

Program lain, seperti RealNetworks video player, secara otomatis meng-download update dan pengumuman, serta meng-upload pola penggunaan kembali ke situs pada Internet. Applet yang sepertinya tidak berbahaya (seperti Konfabulator dan widget Dashboard) secara terus-menerus mencari informasi yang sudah di-update pada Internet host. Ini bisa berupa permintaan ber-bandwidth rendah (seperti update berita atau cuaca), atau permintaan ber-bandwidth yang sangat tinggi (seperti webcam). Aplikasi-aplikasi ini mungkin harus dipercepat atau bahkan diblok secara keseluruhan. Versi terbaru Windows dan Mac OS X

juga mempunyai layanan sinkronisasi waktu.

Ini membuat jam komputer akurat dengan menyambung ke server waktu di Internet. Adalah lebih efisien untuk menginstal sebuah server waktu lokal dan mengdistribusi waktu yang akurat dari sana, daripada terikat pada sambungan Internet dengan permintaan-permintaan ini.

Lalu lintas Windows pada sambungan internet

Komputer-komputer Windows saling berkomunikasi satu sama lainnya melalui ***NetBIOS*** dan ***Server Message Block*** (***SMB***). Protokol-protokol ini berkerja diatas TCP/IP atau protokol-protokol pengangkut lainnya. Ini merupakan protokol yang berkerja dengan mengadakan ***pemilihan*** untuk menentukan komputer mana yang akan menjadi ***browser utama***. Browser utama adalah sebuah komputer yang menyimpan daftar semua komputer, file yang digunakan bersama atau di-share, dan printer yang dapat anda lihat dalam ***Network Neighborhood*** atau ***My Network Places***. Informasi mengenai bagian yang tersedia juga ditayangkan pada interval yang reguler.

Protokol SMB didesain untuk LAN dan menimbulkan masalah ketika komputer Windows disambungkan ke Internet. Kecuali lalu lintas SMB di-filter, protokol ini juga cenderung untuk menyebar ke sambungan Internet, menghabiskan bandwidth secara cuma-cuma. Langkah-langkah berikut mungkin dapat diambil untuk menghindari ini:

- **Bloklah lalu lintas SMB/NetBIOS yang keluar pada perimeter router atau firewall.** Lalulintas ini akan menghabiskan bandwidth Internet, dan lebih parah lagi, dapat menimbulkan potensi resiko keamanan. Banyak worm Internet dan alat penetrasi yang secara aktif mencari bagian SMB yang terbuka, dan akan mengeksploitasi sambungan-sambungan ini untuk memperoleh akses yang lebih besar ke jaringan anda.

- **Instal ZoneAlarm pada semua workstation (tidak pada servernya).** Sebuah versi gratis dapat ditemukan di *http://www.zonelabs.com/*. Program ini memungkinkan si pengguna untuk menentukan aplikasi mana yang bisa membuat sambungan dengan Internet dan yang mana yang tidak bisa. Sebagai contoh, Internet Explorer harus tersambung dengan Internet, namun Windows Explorer tidak perlu. ZoneAlarm dapat memblok Windows Explorer dari melakukan ini.

- **Kurangi file-sharing jaringan.** Idealnya, hanya server file yang dapat mempunyai file-sharing. Anda dapat menggunakan alat seperti SoftPerfect Network Scanner (dari *http://www.softperfect.com/*) untuk secara mudah mengidentifikasi semua file-sharing dalam jaringan anda.

Worm dan Virus

Worm dan virus dapat menimbulkan kemacetan lalu lintas. Worm W32/Opaserv, misalnya, masih unggul, walaupun worm ini adalah worm yang tua. Worm ini menyebar lewat pembagian file Windows dan dideteksi oleh orang lain di Internet karena worm ini mencoba untuk menyebar lebih jauh. Oleh karena itu, adalah penting agar perlindungan antivirus dipasang pada semua PC. Disamping itu, pendidikan pengguna mengenai membuka lampiran dan merespon ke email yang tidak dikenal adalah penting. Pada kenyataannya, ini harus menjadi kebijakan bahwa tidak satupun workstation atau server sebaiknya menjalankan layanan yang tidak digunakan. Sebuah PC sebaiknya tidak memiliki pembagian file kecuali PC tersebut adalah file server; dan sebuah server sebaiknya juga tidak menjalankan layanan yang tidak diperlukan. Sebagai contoh, server Windows dan Unix pada umumnya menjalankan layanan server web secara default. Ini sebaiknya dimatikan jika server itu memiliki fungsi yang berbeda; semakin sedikit layanan yang dijalankan sebuah komputer; semakin sedikit yang bisa dieksploitasikan.

Loop forward email

Pada waktu tertentu, seorang pengguna yang membuat kesalahan dapat menimbulkan masalah. Sebagai contoh, seorang pengguna yang akun universitasnya terkonfigurasi untuk meneruskan semua surat ke akun Yahoonya. Si pengguna pergi berlibur. Semua email yang terkirim kepadanya ketika ia tidak ada diteruskan ke akun Yahoonya, yang hanya berkapasitas 2 MB. Ketika akun yahoo menjadi penuh, akun ini mulai mengirimkan email-email itu kembali ke akun universitas, yang langsung meneruskannya ke akun Yahoo. Sebuah loop email terbentuk yang dapat mengirim ratusan ribu email bolak-balik, menimbulkan lalulintas yang besar dan membuat server crash.

Ada fitur-fitur program server surat yang dapat mengenali loop. Ini sebaiknya diaktifkan secara default. Administrator juga harus berhati-hati agar mereka tidak mematikan fitur ini secara tidak sengaja, atau menginstal sebuah penerus SMTP yang memodifikasi header surat dalam sebuah cara dimana server surat tidak mengenali loop surat.

Download besar-besaran

Seorang user dapat melakukan beberapa download sekaligus, atau meng-download file besar seperti imej ISO 650MB. Dalam cara ini, seorang pengguna dapat menggunakan hampir semua bandwidth-nya. Pemecahan untuk masalah seperti ini terletak pada pelatihan, peng-download-an secara offline, dan pemantauan (termasuk pemantauan waktu-nyata, seperti yang digambarkan dalam bab enam). Peng-download-an secara offline dapat dilaksanakan setidaknya dalam dua cara:

1. Di Universitas Moratuwa, sebuah sistem diimplementasikan menggunakan pengarahan ulang URL. Pengguna yang mengakses URL **ftp://** dilayani dengan sebuah daftar direktori dimana setiap file memiliki dua sambungan: satu untuk peng-download-an normal, dan

satunya lagi untuk peng-download-an offline. Jika sambungan offline yang dipilih, file yang dispesifikasi akan diantrikan untuk download pada nantinya dan si pengguna diberitahu melalui email ketika download sudah selesai. Sistem tersebut menyimpan setumpuk file yang baru-baru saja di-download, dan mengambil file-file seperti ini secara langsung ketika diminta kembali. Antrian download diatur berdasarkan ukuran file. Oleh sebab itu, file yang kecil di-download terlebih dahulu. Karena sejumlah bandwidth dialokasikan ke sistem ini bahkan selama waktu sibuk, pengguna yang meminta file-file yang kecil mungkin menerimanya dalam waktu menit, bahkan seringkali lebih cepat daripada download online.

1. Pendekatan yang satunya adalah membuat sebuah antarmuka web dimana pengguna memasukkan URL file yang mereka ingin download. Ini kemudian di-download dalam waktu singkat menggunakan sebuah pekerjaan cron atau pekerjaan yang sudah dijadwalkan. Sistem ini hanya akan berkerja untuk pengguna yang tidak sabar, dan yang sudah mengenal ukuran file seperti apa yang akan bermasalah untuk peng-download-an selama hari-hari sibuk.

Mengirim file besar

Ketika pengguna harus mengirim file-file besar kepada penerima lainnya dimanapun mereka berada di Internet, mereka sebaiknya diberitahu bagaimana menjadwalkan upload tersebut. Dalam Windows, sebuah upload ke server FTP yang terletak jauh dapat dilakukan menggunakan skrip file FTP, yang merupakan file text berisi perintah-perintah FTP, yang sama dengan yang berikut ini (disimpan sebagai **c:\ftpscript.txt**):

```
open ftp.ed.ac.uk
gventer
mysecretword
delete data.zip
binary
put data.zip
quit
```

Untuk melaksanakan, ketik ini dari command prompt:

```
ftp -s:c:\ftpscript.txt
```

Pada komputer Windows NT, 2000 dan XP, perintah tersebut dapat disimpan ke dalam sebuah file seperti **transfer.cmd**, dan dijadwalkan untuk berfungsi pada malam hari menggunakan Pekerjaan yang Terjadwalkan atau Scheduled Tasks (Start → Settings → Control Panel → Scheduled Tasks). Dalam Unix, cara yang sama dapat dicapai dengan menggunakan ***at*** atau ***cron***.

Pengguna yang saling mengirimkan file

Pengguna seringkali perlu untuk saling mengirim file besar satu sama lainnya. Ini adalah pemborosan bandwidth untuk mengirim file-file ini melalui Internet jika penerimanya adalah lokal. Sebuah pembagian file sebaiknya dibuat pada server Windows/Samba/web Novell lokal, dimana pengguna dapat menyimpan file besar tersebut agar dapat diakses oleh orang lain.

Secara alternatif, sebuah ujung-depan web dapat ditulis untuk sebuah server web lokal untuk menerima sebuah file besar dan meletakkannya di tempat download. Setelah meng-upload-kannya ke server web, si pengguna menerima sebuah URL untuk file itu. Orang tersebut kemudian dapat mengirim URL itu kepada penerima lokal atau internasional, dan ketika mereka mengakses URL itu mereka dapat meng-download-nya. Ini adalah apa yang sudah dilakukan oleh Universitas Bristol terhadap sistem FLUFF mereka. Universitas tersebut menawarkan fasilitas untuk upload file besar (FLUFF) yang tersedia di *http://www.bristol.ac.uk/fluff/*. File-file ini kemudian dapat diakses oleh siapapun yang sudah diberikan lokasinya. Keuntungan pendekatan ini adalah bahwa pengguna-pengguna dapat memberikan pengguna-pengguna luar akses ke file mereka, sedangkan sebaliknya metode pembagian file berguna hanya bagi mereka yang berada dalam jaringan kampus. Sistem seperti ini dapat secara mudah diimplementasikan sebagai skrip CGI menggunakan Python dan Apache.

Bab 10 Keberlanjutan Ekonomi

Memperoleh kesinambungan jangka panjang kemungkinan adalah hal yang paling sulit ketika mendisain dan mengoperasikan jaringan wireless dan telecenter di negara berkembang. Biaya penghalang dari sambungan internet di banyak negara berkembang adalah biaya operasional yang besar yang membuat model ini sensitivitas terhadap fluktuasi ekonomi dan inovasi yang diperlukan untuk kelangsungan hidupnya. Kemajuan yang besar dalam penggunaan jaringan wireless untuk komunikasi pedesaan telah disempurnakan beberapa tahun yang lalu, sebahagian besar karena banyaknya penemuan baru dalam bidang teknologi. Sambungan jarak jauh dapat dibangun, disain bandwith tinggi dan membuka ketersediaan akses jaringan. Sayangnya, sangat sedikit keberhasilan dalam mengembangkan model bisnis berkesinambungan untuk jaringan wireless dan telecenter, khususnya untuk daerah yang terpencil. Berdasarkan pengalaman dan observasi penulis pada jaringan yang sudah berhasil, juga pengetahuan dari pengalaman praktis yang baik dari wiraswastawan pembangunan, bagian ini akan memfokuskan pada metoda untuk membangun kesinambungan jaringan wireles dan telecenter.

Pada dekade yang dulu, terjadi pertumbuhan luar biasa dalam akses Internet di antara dunia berkembang. Hampir semua kota di negara berkembang mempunyai wireless atau jaringan ADSL dan fiber optic untuk sambungan ke internet, merupakan sebuah peningkatan yang substansial. Meskipun di luar daerah perkotaan, akses internet masih merupakan tantangan yang berat. Hanya ada sedikit infrastruktur kabel diluar kota besar. Oleh karena itu, jaringan wireless, merupakan salah satu dari sedikit pilihan yang dapat menyediakan akses internet yang terjangkau. Di Macedonia , Proyek Macedonia Connects, saat ini telah menyambungkan sebagian besar sekolah-sekolah pemerintah ke Internet. Buku ini di tulis bagi mereka yang berharap untuk menyambungkan komunitas mereka. Model yang dikembangkan disini berskala kecil dan menggunakan desain yang terjangkau. Tujuan kami adalah menyediakan contoh bagaimana jaringan wireles dapat di desain untuk memungkinkan akses yang kesinambungan dimana operator telekomunikasi besar belum memasang jaringan-jaringan mereka ke dalam wilayah yang secara ekonomis tidak memungkinkan berdasarkan model tradisional

Dua kesalahpahaman yang harus dihindari. Pertama, banyak orang berasumsi bahwa ada satu model bisnis yang baik yang dapat digunakan oleh setiap komunitas di dunia berkembang, kunci sukesnya adalah menemukan satu solusi “eureka” . Pada kenyataan praktisnya, hal ini tidak berlaku. Setiap komunitas, setiap kota dan setiap desa ternyata berbeda. Tidak ada satu model yang pasti yang akan memenuhi semua wilayah di dunia berkembang. Memang beberapa daerah mungkin mempunya pola ekonomi yang sama, karakteristik dari model bisnis yang berkesinambungan akan berbeda-beda dari satu komunitas ke komunitas lainnya. Walaupun sebuah model bisa bekerja di suatu desa, desa terdekat lainnya bisa jadi kualitas kebutuhannya terhadap model ini tidak sama untuk bisa berkesinambungan. Dalam lingkup ini, model-model inovasi harus bisa di buat sesuai

kebutuhan masyarakat itu sendiri.

Kesalahan konsepsi lainnya adalah bahwa berkesinambungan mempunyai definisi sama untuk semua orang. Walaupun kesinambungan biasanya berarti bahwa sistem di bangun untuk dapat bertahan selamanya, bab ini fokus pada diskusi tentang kondisi ekonomi (finansial dana manajerial) dari pada aspek keberlanjutan. Juga sebagai ganti selamanya, keberanjutan akan lebi pada perioda lima tahun – perioda dimana infrastruktur IT dan Teknologi wireless diharapkan berguna. Istilah keberlanjutan digunakan untuk mengenkapsulasi disain system yang cocok untuk kira-kira lima tahun atau lebih.

Ketika menentukan dan mengimplementasikan model yang baik untuk jaringan wireless atau telecenter, ada beberapa faktor kunci yang membantu kesuksesan, Bab ini tidak bermaksud untuk menjadi panduan dalam mengelola jaringan wireless yang berkelanjutan, “How-to” ini dapat dijadikan petunjuk untuk mencari pendekatan yang cocok untuk situasi anda. Tool dan informasi yang ada di bab ini akan menolong orang untuk memulai jaringan wireless di dunia berkembang dan mencari jawaban dari pertanyaan dan mengumpulkan data-data agar bisa mendefinisikan komponen yang cocok bagi model mereka. Perlu di pahami bahwa mencari modem yang terbaik bukan proses yang berurut dimana setiap langkah harus diikuti sampai selesai. Kenyataannya, proses mencari model terbaik bersifat terus menerus dan rutin. Semua langkah-langkah terintegrasi dan terhubung satu sama lain, dan seringkali anda akan mengulang langkah-langkah tsb beberapa kali sampai ada kemajuan.

Membuat sebuah Misi tertulis.

Apa yang anda ingin capai dengan membangun aringan anda ? Sepertinya sebuah pertanyaan yang sederhana. Bagaimanapun, banyak jaringan wireless sudah terpasang tanpa visi yang jelas akan apa yang mereka kerjakan dan apa yang akan di capai di kemudian hari.. Langkah pertama, adalah pendokumentasian visi dengan masukan dari seluruh team atau staff. Apa yang di maksud dengan jaringan wireless ? Untuk siapa layanan jaringan ini ? Apa yang dilakukan jaringan untuk kebutuhan komunitas dan nilai apa yang dikembangkan? Apa prinsip yang memandu jaringan? Sebuah misi tertulis yang baik dapat menggambarkan maksud dari jaringan anda secara singkat, cara yang berarti untuk meng-artikulasikan nilai dan layanan anda. Di atas semuanya, misi anda memberikan sebuah visi dari aspirasi untuk jaringan wireless anda.

Sangat penting bahwa setiap anggota team bekerja untuk membangun jaringan wireless termasuk proses didalam pengembangan misi nya, yang mempunyai nilai jual. Itu akan menjadi dukungan dan komitmen tidak hanya dari staf anda, tetapi juga dari pelanggan, rekan dan donor, yang akan menjadi tujuan keseluruhan. Dalam dunia teknologi yang dinamis, kebutuhan dari pelanggan dan cara terbaik untuk memuaskan kebutuhan itu dapat berubah sangat cepat, oleh karenanya, pengembangan misi anda adalah proses yang berjalan terus menerus. Setelah pendefinisian misi awal dengan team, anda harus melakukan riset untuk melihat apakah konsepsi pertama sesuai dengan realita di lingkungan anda.

Berdasar pada analisis lingkungan luar dan kompetensi internal, anda harus terus menerus menyesuaikan misi selama siklus kehidupan dari jaringan wireless.

Evaluasi setiap permintaan yang potensial.

Tahap selanjutnya dalam mengembangkan model bisnis libatkan masukan dari permintaan masyarakat untuk produk dan layanan jaringan. Pertama, identifikasikan, perorangan, group dan organisasi di masyarakat yang mempunyai kebutuhan akan informasi dan akan mendapatkan manfaat dari jaringan wireles yang anda tawarkan. Pemakai yang potensial dapat terdiri dari berbagai macam individu atau perorangan maupun organisasi yang sangat besar, tapi tidak terbatas seperti :

- Asosiasi petani, dan koperasi
- Kelompok-kelompok Perempuan
- Sekolah dan Universitas
- Bisnis dan wiraswasta
- Kelompok keagamaan
- Lembaga Swadaya Masyarakat ataupun International
- Agen Lokal dan Pemerintah
- Stasiun Radio
- Organisasi di Industri Wisata

Setelah membuat daftar kelompok pemakai jaringan yang potensial, anda harus menentukan kebutuhan mereka akan akses Informasi dan komunikasi, seringkali orang bingung dengan apa yang dibutuhkan. Seorang petani butuh mengumpulkan informasi tentang harga pasar dan situasi cuaca untuk memperbaiki panen dan penjualan mereka. Informasi ini bisa mereka dapatkan melalui internet, namun petani juga dapat informasi melalui SMS lewat Handphone atau lewat ***VOIP (telepon internet)***. Penting juga untuk membedakan antara kebutuhan dan layanan karena ada beragam cara yang dapat digunakan memenuhi kebutuhan petani itu. Jaringan wireless anda harus melihat mana yang terbaik agar dapat memenuhi kebutuhan petani, menciptakan suatu cara yang murah bagi pelanggan.

Pada saat kita melakukan penelitian akan kebutuhan masyarakat, dan penting untuk bagaimana jaringan dapat membawa manfaat kepada penggunanya. Contoh : di kota kecil Douentza, Mali, seorang manajer telecenter mengevaluasi manfaat potensial dari membangun jaringan wireless melalui diskusi dengan beberapa organisasi lokal. Dia menginterview sebuah LSM Lokal dan mendiskusikan kebutuhan mereka untuk mengirim laporan ke kantor pusat di Bamako. Saat itu, tidak ada akses internet di Douentza, untuk mengirim salinan laporan saja mereka mengirim seorang staf nya ke Mopti sebulan sekali, hasilnya biaya transportasi dan penginapan yang dikeluarkan selama beberapa hari dalam

sebulan dapat mengurangi pendapatan mereka. Ketika manajer telecenter menghitung-hitung, total biaya bulanan yang dikeluarkan per bulan oleh LSM tsb, dia dapat memperlihatkan betapa Internet sangat membantu dan mendatang manfaat, sehingga mereka dapat menekan biaya yang dikeluarkan organisasi.

Bantuan dari mitra kunci mungkin juga di perlukan untuk memastikan keberlanjutan untuk jaringan wireless anda. Dalam tahap ini, anda perlu berhubungan dengan mitra potensial dan menggali kerjasama yang saling menguntungkan.

Anda dapat mengevaluasi permintaan di masyarakat anda dengan berhubungan dengan pelanggan yang potensial dan menanyakan secaralangsung melalui survey, group diskusi, interview atau pertemuan-pertemuan dalam kota. Melakukan riset melalui review dokumentasi statistik, laporan industri, sensus, majalah, koran dan data sekunder lainnya sangat membantu dalam memberikan gambaran yang lebih jelas dan baik tentang lingkungan anda. Tujuan dari pengumpulan data ini adalah untuk memperoleh pengertian yang menyeluruh akan kebutuhan untuk informasi dan komunikasi di komunitas anda sehingga jaringan yang dibangun dapat memenuhi kebutuhan itu. Seringkali, jaringan wireless tidak berhasil di dunia berkembang karena melupakan tahap-tahap ini. Jaringan wireless anda harus berbasis pada kebutuhan dalam masyarakat. Jika anda membangun jaringan wireless dimana komunitas tidak menemukan manfaat atau tidak mampu membeli layannya, jaringan anda akan pada akhirnya gagal.

Membentuk Insentif yang Sesuai

Seringkali, sangat sedikit insentif ekonomis bagi pengguna yang masih sekedar hidup untuk mengakses Internet. Sebagai tambahan, biaya untuk mendapatkan sebuah komputer, belajar untuk menggunakannya, dan mendapatkan akses internet jauh lebih besar daripada perolehan kembalinya. Baru-baru ini telah ada ada perkembangan aplikasi untuk mengatasi kekurangan insentif tersebut, seperti system informasi pasar, standar kualitas ditentukan oleh negara pengimpor dan pertukaran komoditi. Akses internet menjadi suatu manfaat nyata dalam situasi dimana pengetahuan akan harga sehari ke hari dari produk dapat membuat perbedaan yang signifikan dalam pendapatan.

Membangun insentif ekonomi yang sesuai sangat penting untuk suksesnya jaringan. Jaringan harus menyediakan nilai ekonomis bagi penggunanya sehingga lebih besar dari biaya yang di keluarkan, atau cukup murah sehingga sangat kecil dan sesuai kemampuan penggunanya. Sangat penting sekali untuk mendesain sebuah jaringan dengan penggunaan ekonomis dan biaya yang dikeluarkan lebih kecil dari nilai ekonomis yang tersedia. Untuk membuat struktur insentif yang sesuai, anda harus terlibat di masyarakat dalam menciptakan jaringan dari awal proyek, pastikan bahwa inisiatif ini bersifat lokal dan tidak ada unsur luar. Untuk memulai, anda harus mencoba menjawab beberapa pertanyaan:

1. Nilai ekonomis apa yang dapat dihasilkan jaringan untuk ekonomi lokal dan untuk

siapa?

2. Berapa banyak nilai ekonomis yang dapat dihasilkan dan dapat terlihat ?
3. Dapatkah halangan yang ada diatasi dengan memungkinkan prestasi dalam pengembalian ekonomi?

Dengan menjawab pertanyaan ini, jaringan akan dapat dituliskan dengan jelas nilai proposional bagi tiap user (pengguna). Contoh : “Dengan menggunakan jaringan ini maka anda dapat meningkatkan margin keuntungan penjualan menjadi 2 %”, atau “Internet dapat menghemat uang dari biaya telephone dan biaya transportasi per bulan”. Anda harus bisa memperhitungkan bagaimana jaringan dapat meningkatkan efisiensi, mengurangi biaya, atau mningkatkan pendapatan pada pelanggan.

Sebagai contoh : jika menyediakan informasi pasar pada industri jagung lokal, jaringan juga harus dilokasikan dekat dengan petani membawa hasil panen untuk di jual ke pembeli. Jaringan akan dapat memenuhi keterikatan sistem informasi pasar, menyediakan lembar harga pasar (Rp 10.000 per buah), atau tempat untuk penjual dan pembeli (Rp 20.000 / hari). Jaringan anda dapat juga menyediakan sarana untuk petani untuk membaca tentang teknik baru dan membeli produk baru. Anda juga dapat menyediakan jaringan wireless pada pembeli dan menyewakan mereka terminal kecil untuk akses internet. Jika pasar sangat kecil, anda dapat mengurangi biaya dengan membatasi akses pada gambar-gambar dan berbagai layanan yang mengkonsumsi bandwith. Sekali lagi, mengetahui berapa banyak manfaat jaringan anda untuk para pedagang akan memungkinkan anda menaksir biaya yang dapat mereka bayar untuk layanan anda.

Riset tentang Regulasi Wireless

Regulasi pada Wireless juga tergantung pada model bisnis yang dapat diimplementasikan. Pertama, telitilah apakah semua organisasi dapat menggunakan frekwensi 2,4 GHz tanpa izin. Dalam banyak situasi, 2.4 GHz bebas digunakan di seluruh dunia, namun beberapa negara membatasi siapa yang dapat mengoperasikan jaringan atau memberi ijin yang sangat mahal pada mereka yang membutuhkan.

Meskipun Jaringan Wireless di Ukraina adalah legal, pemerintah meminta lisensi yang mahal untuk penggunaan 2.4GHz, hal ini menyebabkan pemakaian bersama menjadi sulit. Biasanya hanya Internet Service Provider yang mapan di negara itu yang mempunyai uang yang cukup untuk membayar lisensi yang mahal tersebut. Pembatasan ini membuat susah bagi masyarakat kecil untuk membagi jaringan wireless mereka kepada organisasi maupun mitra-mitra yang potensial. Di negara lain, seperti Repulik Mali, lebih mengijinkan, karena tidak ada larangan atau batasan pada jaringan wireless mereka. Kemungkinan untuk membagi sambungan Internet ke komunitas kecil menjadi solusi yang memungkinkan. Pelajaran ini menggaris bawahi perlunya riset yang mendalam, yakinkan jaringan anda susah sesuai

dengan hukum di negara itu dan di masyarakat lokalnya. Beberapa manajer proyek telah dipaksa untuk mematikan jaringan wireless mereka karena mereka tidak mengetahui tentang hukum yang berlaku di sana.

Anda juga harus mencek legalitas dari layanan VOIP (Voice over Internet Protocol). Beberapa negara di negara berkembang belum mndefinisikan apakah VOIP di izinkan. Bagaimanapun di beberapa negara ada aturan yang sangat rumit seputar VOIP. Misal di Syria, VOIP di larang untuk semua jaringan tidak hanya wireless, di Ukraina, VOIP legal hanya untuk panggilan Internasional.

Analisa Kompetisi

Tahap selanjutnya adalah mengevaluasi komunitas dalam hal analisa kompetisi jaringan wireless di tempat anda. Kompetitor termasuk organisasi yang menyediakan produk dan layanan yang sama (misal, Wireless Internet Service Provider atau WISP yang lain), organisasi yang berfungsi sebagai pengganti atau alternatif kepada produk dan layanan dari jaringan anda (contoh : WARNET), dan organisasi yang merupakan pendatang bari di pasar wireless. Sekali anda mengidentifikasi kompetitor, anda harus meneliti mereka lebih jauh. Anda dapat memperoleh informasi tentang kompetitor dari Internet, telephone, iklan maupun materi pemasaran mereka, survey pelanggannya dan kunjungi sitenya. Buat sebuah file tentang setiap kompetitor. Informasi kompetitif yang anda kumpulkan dapat termasuk daftar layanan (termasuk kualitas informasi dan harga), target klien mereka, reputasi, marketing, dll. Pastikan kumpulkan segala sesuatu yang akan membantu anda dalam menentukan bagaimana memposisikan jaringan anda di komunitas.

Sangat penting untuk mengevaluasi kompetisi anda untuk berbagai alasan. Pertama, membantu anda menentukan tingkat kejenuhan pasar. Ada beberapa instansi yang mensubsidi telecenter yang sudah dibangun oleh organisasi donor di desa kecil dengan permintaan terbatas, padahal disitu sudah ada WARNET. Bayangkan sebuah situasi, WARNET bersubsidi memberikan harga murah karena mereka tidak harus menutupi biaya operasi. Skenario ini membuat WARNET lokal menjadi bangkrut. Setelah dana berhenti, WARNET bersubsidi juga menghentikan usahanya, karena rendahnya pendapatan dan tingginya biaya. Dengan mengetahui apa yang telah ada di komunitas akan memudahkan anda untuk menentukan bagaimana jaringan anda dapat berkontribusi pada masyarakat. Analisa kompetisi dapat menstimulasi ide inovasi pada layanan yang anda tawarkan. Apa ada yang lebih baik dilakukan dari kompetitor agar servise anda lebih efektif suai dengan kebutuhan komunitas? Akhirnya, dengan menganalisa kompetitor dari pandangan pelanggan dan mengerti bagaimana kekuatan dan kelemahannya, anda dapat menentukan kompetitif advantage di komunitas. Kompetitif advantage adalah sesuatu yang tidak akan dapat dengan mudah di replikasi oleh kompetitor. Sebagai contoh, sebuah jaringan Wireless dapat menawarkan secara eksklusif sebuah koneksi internet yang tercepat dari pada kompetitor

merupakan kompetitif advantage yang dapat memfasilitasi kebutuhan kliennya.

Menentukan Biaya dan Harga Awal maupun rutin.

Ketika anda merencanakan membentuk dan mengoperasikan jaringan wireleess anda, anda harus menentukan sumber-sumber yang diperlukan untuk memulai proyek dan biaya -baya operasional yang akan timbul. Biaya permulaan termasuk segala sesuatu yang harus di beli untuk memulai jaringan wireless anda. Pengeluaran ini akan dapat ditentukan dari awal anda berinvestasi berupa peralatan, instalasi, dan peralatan untuk akses point, hubs, switch, kabel, UPS, dll juga biaya untuk mendaftarkan izinnya. Biaya yang timbul dan harus dibayarkan untuk melanjutkan operasi jaringan wireless, termasuk biaya akses internet, telephone, pinjaman, listrik, gaji, sewa kantor, pemeliharaan dan perbaikan peralatan dan biaya lain untuk investasi untuk penggantian peralatan yang sudah tidak berfungsi dengan baik.

Setiap buah alat akan mengalami kerusakan atau kadaluarsa pada saatnya, dan anda harus menyiapakan ekstra dana untuk penggantiannya, caranya adalah dengan melakukan perhitungan biaya ***penyusutan.*** Contoh : sebuah komputer pemakaian rata-rata 2-5 tahun, pertama dibeli harganya USD 1.000 dan anda dapat memakainya hingga 5 tahun. Maka nilai penyusutannya adalah USD 200 per tahun, atau USD 16,67 per bulan, maka ketika masanya selesai anda dapat membeli komputer yang baru. Untuk membuat proyek berkesinambungan, sangat penting untuk menyimpan uang untuk kompensasi penyusutan barang setiap bulannya. Simpan uang tersebut sampai akhirnya bisa mengganti peralatan tersebut. Beberapa negara mempunyai aturan pajak tentang penentuan nilai penyusutan yang berbeda setiap barangnya. Dalam satu hal, anda harus mencoba utuk realistis tentang siklus hidup seluruh peralatan dan merencanakan nilai penyusutan secara hati-hati.

Coba untuk menemukan dulu berapa biayanya dan estimasi pengeluarannya. Tahap berikut (di halaman berikut) tunjukkan cara anda mengklasifikasi dan daftar biayanya. Ini cara terbaik untuk menstruktur biaya yang berbeda-beda, juga akan membantu anda untuk membedakan untuk membedakan antara biaya awal dengan biaya beulang.

Penting untuk meneliti biaya awal yang dikeluarkan lebih dulu, dan membuat estimasi yang realistis pada biaya Rutin yang timbul. Lebih baik untuk melebihkan budget dari pada kekurangan. Setiap proyek wireless selalu ada biaya tak terduga, khususnya di tahun pertama pengoperasian karena anda baru belajar untuk mengelola jaringan anda dengan baik.

Kategori Biaya

	Biaya Awal	Biaya Rutin
Biaya Buruh	• Anlisa dan konsultansi • Biaya pengembangan untuk pemrogramman, testing, integrasi dll. • Biaya Instalasi. • Biaya perekrutan. • Biaya training (pengenalan).	• Biaya penanganan / gaji untuk pegawai atau freelancer, termasuk kita sendiri. • Biaya pemeliharaan dan dukungan untuk software, hardware, dan peralatan tambahan. • Penjaga keamanan. • Biaya training (lanjutan).

	Biaya Awal	Biaya Rutin
Biaya Material (non buruh)	• Pembelian dan biaya produksi (untuk hardware seperti PC, VSAT, sambungan radio dan software). • Peralatan tambahan (seperti switch, kabel dan perkabelan, generator, UPS dll). • Proteksi data dan keamanan jaringan. • Inventori awal (kursi, meja, lampu, korden dan karpet). • Biaya bangunan (bangunan baru, modifikasi, AC, kabel listrik, teralis). • Biaya lisensi (VSAT). • Biaya marketing awal (selebaran, stiker, poster, pesta pembukaan).	• Biaya operasi untuk hardware dan pengoperasian system (akses Internet, telepon, dll). • Biasa sewa. • Depresiasi dari hardware dan peralatan. • Biaya lisensi. • ATK (seperti kertas, klip, disket). • Biaya operasi untuk memelihara keamanan data. • Asuransi. • Biaya untuk listrik untuk menjamin supply daya. • Biaya iklan. • Biaya lokal. • Jasa hukum dan akuntan.

Untuk meningkatkan kesempatan keberlanjutan, umumnya yang terbaik adalah memelihara struktur biaya rendah pada jaringan. Dengan kata lainnya, kecilkan pengeluaran sebisa mungkin. Ambil waktu untuk melakukan riset ke semua suplier, khususnya ISP-ISP dan toko sekitar agar dapat memberikan pelayanan terbaik. Sekali lagi, pastikan apa yang ingin di beli dari suplier sesuai permintaan komunitas. Sebelum pemasangan VSAT yang mahal, pastikan

bahwa berapa jumlah organisasi atau perorangan di masyarakat anda yang akan menggunakan dan membayarnya. Tergantung permintaan akses informasi dan kemampuan membayar, metode sambungan alternatif mungkin lebih cocok. Jangan takut untuk berfikir beda dan kreatiflah untuk menentukan cara terbaik.

Menekan biaya menjadi rendah tidak harus mengorbankan kualitas. Karena peralatan berkualitas rendah lebih gampang rusak, anda dapat menghabiskan lebih banyak untuk pemeliharaan jangka panjang. Jumlah uang yang anda habiskan untuk pemeliharaan infrastruktur IT susah diperkirakan. Dengan infrastruktur yang makin besar dan kompleks, makin banyak sumber daya dan keuangan yang harus dialokasikan untuk pemeliharaannya.

Pada banyak kesempatan hubungan ini tidak linier tapi exponensial. Jjika anda mempunyai masalah besar dengan peralatan yang di bangun, maka dapat menghabis dana yang sangat besar untuk memperbaikinya. Bersamaan dengan itu, penjualan anda akan berkurang karena peralatan kita tidak dapat berjalan. Ada contoh menarik dalam WISP (wireless internet service provider) yang besar, mereka mempunyai lebih dari 3000 akses point yang beroperasi, mereka tidak pernah mencapai break event (untung) karena dihabiskan terlalu banyak untuk pemeliharaan akses pointnya. Di samping itu, mereka menganggap enteng jangka waktu hidup yang pendek dari peralatan. Hardware ICT cenderung menjadi murah dan semakin baik bersama waktu. Sesaat setelah perusahaan investasi waktu dan uang untuk memasang akses point generasi pertama dan mahal type 802.11b, produk baru standard “g” keluar. Kompetitor baru akan mendisain akses pont lebih bagus dan lebih murah dan menawarkan Akses internet lebih cepat dengan biaya murah. Akhirnya WISP pertama harus menutup perusahaannya, meskipun mereka pernah memimpin pasar. Lihat tabel berikut untuk mendapatkan gambaran bagaimana cepatnya berkembang standar peralatan wireless :

Protokol	Tanggal Release	Kecepatan Data
802.11	1997	< 1Mbps
802.11b	1999	5 Mbps
802.11g	2003	20 Mbps
802.11a	1999, tapi langka sampai 2005.	23 Mbps
802.11y	Juni 2008 (estimasi)	23 Mbps
802.11n	Juni 2009 (estimasi)	75 Mbps

Pahami akan adanya kemajuan dan perubahan yang cepat dari teknologi dan pikiran bagaimana dan kapan waktu yang baik untuk investasiulang menggunakan peralatan yang lebih baru dan lebih murah untuk membuat infrastruktur anda kompetitif dan up-to-date. Seperti disebut sebelumnya, sangat penting sekali anda menyimpan dana cukup untuk melakukannya bila diperlukan.

Saat anda telah mengenali dan memetakan biaya anda, anda juga sebaiknya memutuskan apa dan bagaimana cara mengenakan biaya untuk layanan anda. Ini adalah proses rumit dan memakan waktu untuk melakukan dengan benar. Ini Tip-tip kunci untuk menentukan harga:

- Hitung harga yang anda kenakan dan apakah sudah menutupi semua biaya untuk menyediakan service itu, termasuk semua pengeluaran rutin.
- Pelajari harga dari kompetitor anda.
- Evaluasi apa yang pelanggan anda inginkan dan mereka bayar pada layanan anda, dan yakinkan bahwa harga anda sesuai dengan itu.

Sangat penting untuk membuat rencana keuangan sebelum memulai. Anda perlu daftar seluruh biaya awal dan biaya rutin dan membuat perhitungan untuk menentukan apakah proyek ini dapat berkelanjutan.

Mengamankan Keuangan

Setelah anda menentukan biaya awal dan biaya rutin serta sudah membuat rencana keuangan, anda tahu berapa banyak dana yang anda butuhkan untuk menjalankan jaringan wireless dengan sukses. Langkah selanjutnya adalah untuk melakukan riset tentang berapa jumlah dana yang aman untuk memulai dan menjalankan bisnis ini.

Metode yang sederhana adalah menerima dana untuk jaringan wireless di negara berkembang dengan mendapatkan dana hibah dari donor-donor. Donor adalah sebuah organisasi yang mengkontribusikan dana maupun donasi lainnya kepada organisasi atau konsorsium organisasi untuk menolong mereka mengelola proyek atau mendukung proyek bagi yag membutuhkan. Karena dana ini diberikan dalam bentuk hibah atau donasi lainnya, tidak perlu dikembalikan oleh organisasi yang menjalankan proyek wireless atau penerima proyek. Donor-donor termasuk organisasi internasional besar misal United Nations (UN) dan berbagai UN Agensi seperti United Nations Development Program (UNDP) dan United Nations Educational, Scientific and Cultural Organization (UNESCO). Badan pemerintah spesialisasi dalam Perkembangan Internasional, seperti United States Agency for International Development (USAID), United Kingdom s Department for International Development (DFID), dan Canadian International Development Agency (CIDA), merupakan donor yang perlu diperhitungkan. Beberapa yayasan besar Gates Foundation dan Soros Foundation Network dan banyak perusahan swasta adalah jenis donor yang lain.

Penerimaan dana melibatkan proses kompetisi dan mungkin juga non kompetisi. Proses non kompetitif lebih jarang. Dalam bab ini kita akan fokus pada proses kompetitif pada level sangat tinggi. Hampir semua donor mempunyai prosedur yang rumit sekitar pendistribusian dananya. Penulis dalam buku ini tidak ada maksud mencoba menyederhanakan system kebiasaan maupun peraturan-peraturan. Penulis hanya menyampaikan sebuah pengertian umum dari proses pada usaha masyarakat untuk memangun jaringan network di negara berkembang. Selama proses tender berlangsung, donor membuat sebuah ***permintaan***

proposal / Reuqest For Proposal (RFP) atau ***permintaan untuk Aplikasi / Request For Application (RFA),*** yang mengumpulkan organisasi non pemerintah, perusahaan swasta dan rekan-rekan lainnya untuk mengirim proposal yang berisi tentang rencana mereka pada proyek ini dengan batasan-batasan dari petunjuk serta tujuan donor. Dalam merespon RFP dan RFA, LSM-LSM dan organisasi-organisasi bertarung dengan mengirim proposal mereka. Lalu Donor akan mengevaluasi berdasarkan kriteria spesifik yang dibuat. Akhirnya, Organisasi Donor akan menseleksi proposal yang paling layak dengan ranking tertinggi untuk didanai proyek nya. Kadang-kadang Donor juga mensuplai dana untuk operasional organisasi, tetapi dana jenis ini lebih tidak umum dibanding proses tender ini.

Cara lain untuk mengakses dana yang diperlukan untuk memulai dan merawat jaringan network melalui ***keuangan skala mikro / microfinances,*** atau pinjaman, tabungan dan bentuk pelayanan keuangan lainnya bagi masyarakat miskin di dunia. Beberapa pionir di tahun 1970-an, organisasi seperti ACCION International dan Grameen Bank, mikro kredit, salah satu jenis keuangan mikro. Individu yang miskin dan pengusaha kecil menerima pinjaman dalam nilai kecil untuk memulai usaha mereka. Walaupun kenyataannya bahwa individu tidak memiliki banyak kualifikasi tradisional untuk memperoleh pinjaman seperti verifikasi kredit yang mudah didapat. Jaminan atau pekerjaan tetap. Program mikro kredit sangat sukses di banyak negara berkembang. Umumnya proses ini melibatkan individu maupun group yang mengajukan permohonan pinjaman dengan harapan mendapatkan pinjaman, dan si pemberi pinjaman, baik individu maupun organisasi memberi pinjangan dengan harapan dapat dibayar kembali berikut dengan bunganya.

Kegunaan mikro kredit untuk mendanai jaringan wireless menghadapi sebuah hambatan, biasanya mikro kredit memberikan jumlah uang yang sedikit. Sayangnya, karena besarnya jumlah modal awal yang dibutuhkan untuk membeli peralatan untuk membangun jaringan wireless, kadang-kadang pinjaman mikro kredit ini tidak cocok. Bagaimanapun juga, banyak aplikasi mikro kredit yang sukses dan telah membawa teknologi dan manfaat bagi dunia berkembang. Sebagai contoh cerita tentang operator telephone di desa. Pengusaha ini menggunakan pinjaman mikro kredit untuk membeli kredit handphone dan biaya telephone, lalu dia sewakan kepada anggota masyarakat berdasarkan hitungan per panggilan dan mendapatkan cukup uang untuk mengembalikan hutang mereka dan mendapatkan keuntungan untuk dia sendiri maupun keluarganya.

Mekanisme lain adalah mendapatkan dana untuk memulai jaringan wireless dari orang yang dermawan memberi pinjaman. Investor dermawan biasanya individu kaya yang menyediakan modal untuk memulai bisnis dengan pertukaran untuk mendapatkan nilai tinggi pengembalian investasi mereka. Karena pola ini mengandung resiko tinggi pada apa yang mereka investasikan dari permulaan dan sering beresiko tinggi, maka investor dermawan ini cenderung mengharapkan sesuatu yang berbeda sebagai nilai tambahan dalam pengembalian investasinya.Banyaknya harapan seperti angota dewan komisaris atau jabatan dalam organisasi. Beberapa dermawan ingin menjadi pemegang saham di perusahaan, sementara yang lainnya cukup memperoleh saham di perusahaan yang dapat dengan mudah di tebus dengan nilai terkemuka, lalu menyediakan jalan keluar yang bersih bagi investor. Untuk melindungi investasinya, si dermawan sering meminta kepada para usahawan untuk

tidak mengambil keputusan kunci tanpa persetujuan mereka. Karena ingginya risiko di pasar dunia berkembang, sangat sulit untuk mencari investor dermawan untuk membantu membangun jaringan nirkabel, tetapi tidak mustahil. Cara terbaik untuk menemukan investor potensial adalah melalui jaringan sosial anda dan melalui penelitian on-line.

Mengevaluasi Kekuatan dan Kelemahan dari Situasi Internal

Sebuah jaringan hanya akan sebaik-baiknya orang yang bekerja dan mengoperasikannya. Tim yang anda bentuk akan menentukan keberhasilan dan kegagalan. Oleh karenanya sangat penting untuk melihat pada kualifikasi dan keterampilan tim, termasuk staf dan relawan, dibandingkan dengan kompetensi diperlukan untuk proyek nirkabel. Pertama, membuat daftar semua kompetensi diperlukan untuk agar proyek nirkabel berhasil. Diantara wilayah kemampuan yang harus dicakup adalah teknologi, sumber daya manusia, akuntansi, pemasaran, penjualan, negosiasi, hukum, dan operasi, Setelah itu, identifikasi sumber manusia daya lokal yang mampu memenuhi keterampilan ini. Petakan keterampilan tim anda untuk memenuhi kompetensi yang dibutuhkan, identifikasi kesenjangan yang fatal.

Salah satu tool yang sering digunakan untuk membantu dengan evaluasi diri ini merupakan analisis kekuatan (strength), kelemahan (weakness), peluang (opportunity) dan ancaman (threats), disebut SWOT. Untuk melakukan analisis ini, anda perlu menentukan kekuatan dan kelemahan internal, dan melihat kesempatan di luar maupun ancaman di komunitas anda. Penting untuk realistis dan jujur tentang apa yang anda lakukan dengan baik dan apa yang kurang. Pastikan untuk dapat membedakan dimana organisasi anda berawal dan dimana di masa depan. Kkuatan dan lemahan anda memungkinkan anda untuk mengevaluasi kapasitas anda secara internal dan lebih memahami apa yang dapat dilakukan oleh organisasi, serta keterbatasannya. Dengan pemahaman kekuatan dan kelemahan anda dan membandingkannya dengan pesaing Anda, Anda dapat menentukan keunggulan kompetitif di pasar. Anda juga dapat mencatat bidang dimana anda dapat tingkatkan. Peluang dan ancaman yang external, memungkinkan anda untuk menganalisa kondisi dunia nyata dan bagaimana kondisi ini mempengaruhi jaringan Anda.

Diagram di bawah ini akan membantu Anda dalam membuat SWOT anda sendiri untuk menganalisis
organisasi Anda. Jangan lupa untuk menanggapi pertanyaan yang diajukan dan buatlah daftar kekuatan, kelemahan, peluang dan ancaman di tempat yang dituju.

Kekuatan	**Kelemahan**
• Apa yang anda lakukan dengan baik? • Apkah sumber daya unik yang dapat	• Apakah anda menjadi lebih baik? • Dimana anda memiliki sumber daya

anda lakukan? • Apakah yang akan dilihat orang lain sebagai kekuatan?	lebih sedikit dibandingkan yang lain? • Apakah yang akan dilihat orang lain sebagai kelemahan?
Peluang	**Ancaman**
• Apakah peluang yang baik terbuka untuk anda? • Trend apa yang dapat anda ambil manfaatnya? • Bagaimana anda dapat mengubah kekuatan anda menjadi peluang?	• Trend apa yang akan merugikan anda? • Apa yang dilakukan oleh pesaing anda? • Ancaman apa yang mengancam kelemahan ada?

Menjadikan semua menjadi satu kesatuan

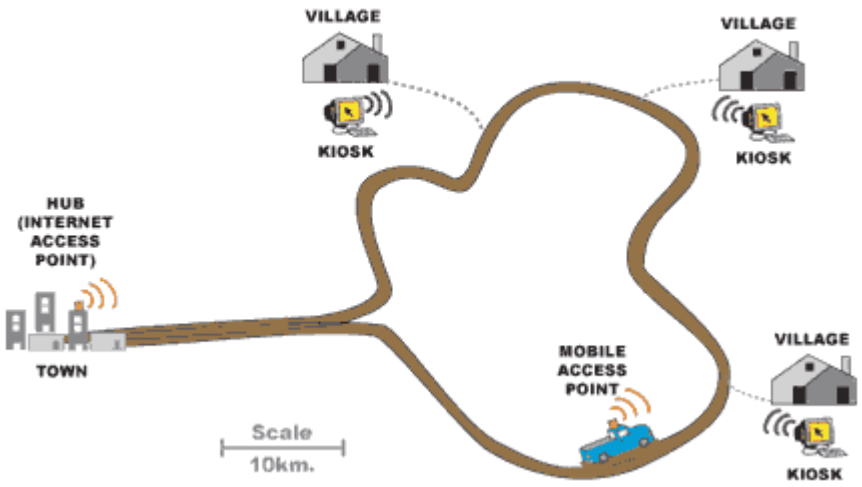
Setelah anda mengumpulkan semua informasi, anda siap untuk menyatukan semuanya dan memutuskan model terbaik untuk jaringan nirkabel komunitas anda. Berdasarkan hasil dari analisa internal dan eksternal, anda harus memperyajam misi dan layanan kepada pelanggan. Semua faktor yang anda teliti di langkah sebelumnya semua memainkan peran yang penting untuk menentukan strategi secara keseluruhan. Sangat penting untuk menggunakan model yang merealisasi peluang dan bekerja adalam batasan lingkungan setempat. Untuk melakukan ini, anda harus menemukan solusi inovatif untuk mencapai kesinambungan. Dengan mempelajari beberapa contoh dan mendiskusikan komponen dari model yang diimplementasikan pada contoh tersebut, sebaiknya anda memahami bagaimana untuk mencapai pada suatu model yang tepat.

Di hutan Republik Demokratik Kongo, terdapat rumah sakit pedesaan di sebuah desa bernama Vanga di provinsi Bandundu. Rumah sakit ini demikian jauh sehingga pasien harus berjalan beberapa minggu menuju ke sana melalui kombinasi perjalanan kaki dan sungai. Desa ini, yang didirikan oleh misionaris Baptis di tahun 1904, yang membaktikan diri sebagai rumah sakit selama bertahun-tahun. Walaupun sangat jauh, rumah sakit tersebut terkenal sebagai sebuah fasilitas yang sangat baik dan telah memiliki dukungan misionaris Jerman dan Amerika yang telah memastikan fasilitas ini agar dapat beroperasi. Pada tahun 2004, proyek yang disponsori oleh USAID didirikan sebuah telecenter di desa ini untuk membantu meningkatkan pendidikan di masyarakat terisolasi ini; fasilitas Internet ini banyak digunakan oleh kalangan berpendidikan di komunitas – staff rumah sakit. WARNET telah memberikan keuntungan besar kepada masyarakat, menawarkan akses ke dunia pengetahuan dan bahkan memungkinkan konsultasi dengan rekan jauh di Swiss, Prancis dan Kanada. WARNET memerlukan subsidi hampir total untuk beroperasi dan menutup biaya, dan pendanaan akan berakhir di tahun 2006.
Walaupun WARNET mempunyai banyak manfaat untuk komunitas, mereka memiliki

beberapa
kekurangan, terutama kemampuan teknis, ekonomi, dan isu politik yang membatasi kesinambungannya. Sebuah studi dilakukan untuk mempertimbangkan pilihan untuk masa depan. Setelah meninjau struktur biaya WARNET, maka ditetapkan bahwa diperlukan untuk memotong biaya dan mencari cara baru untuk meningkatkan pendapatan. Pengeluaran terbesar adalah listrik dan akses Internet; karena itu, dibutuhkan membuat model kreatif untuk mengurangi biaya WARNET dan menyediakan akses Internet melalui cara yang lebih berkesinambungan.

Gambar 10.1: Berbagi Internet Melalui nirkabel

Dalam contoh ini, VSAT tradisional yang digunakan untuk sambungan ke Internet. Namun, model ini memberikan cara yang unik untuk menampung group komunitas lokal yang mempunyai kemampuan terbatas dalam membayar layanan Internet. Berbagai organisasi di komunitas berbagi berbagi akses Internet melalui jaringan nirkabel; mereka juga berbagi biaya yang terkait dengan sambungan ke Internet. Model ini bekerja dengan baik karena kondisi yang spesifik - yaitu adanya kesadaran dan pemahaman nilai dari Internet pada anggota kunci komunitas, sebuah sumber daya yang penting untuk mendukung akses Internet, dan sistem peraturan yang mengijinkan berbagi menggunakan nirkabel. Di Vanga, beberapa organisasi, termasuk rumah sakit, apotik, beberapa kelompok misionari, pusat sumber daya komunitas, dan beberapa organisasi nirlaba, memiliki kebutuhan untuk akses Internet dan mau membayarnya. Kondisi ini memungkinkan jaringan antar organisasi untuk memiliki kualitas yang lebih baik dengan biaya yang lebih rendah. Selain itu, salah satu organisasi di desa mempunyai kemampuan dan keinginan untuk mengelola beberapa aspek operasi jaringan, termasuk billing dan pemungutan pembayaran, teknis pemeliharaan dan operasi bisnis dari seluruh jaringan. Oleh karena itu, model ini berfungsi baik dalam Vanga karena telah disesuaikan untuk memenuhi kebutuhan masyarakat dan penggunaan sumber daya ekonomi lokal.



Gambar 10.2: Akses Point DakNet yang berjalan / mobile

Contoh lain dari model diadaptasi agar sesuai dengan konteks lokal adalah Solusi Kilometer Pertama dari DakNet. Model ini telah dioperasikan di desa-desa di India, Kamboja, Rwanda, dan Paraguay. Dengan mempertimbangkan daya beli yang terbatas dari penduduk desa, model ini memenuhi kebutuhan komunikasi mereka dengan cara yang innovatif. Dalam model DakNet, ada sebuah franchise yang telah ada di negara tersebut, dan pengusaha lokal direkrut dan dilatih untuk beroperasi kios dilengkapi dengan antena Wi-Fi. Menggunakan kartu pra-bayar, penduduk desa dapat secara asinkron mengirim dan menerima email, teks, dan voice mail, melakukan pencarian Web, dan berpartisipasi dalam e-commerce. Setelah itu, komunikasi ini di simpan di server lokal di kios. Ketika sebuah bis atau sepeda motor dengan akses point melalui kios, kendaraan tersebut secara otomatis menerima data yang di simpan di kios dan memberikan kepada kios semua data yang masuk. Setelah kendaraan mencapai sebuah hub dengan sambungan internet, dia akan memproses semua permintaan, relay email, pesan, dan berbagi file.

DakNet mengintegrasikanakses mobile internet dan model franchise untuk memberikan manfaat kepada desa terpencil. Agar model tersebut dapat berkelanjutan, harus ada beberapa kondisi kunci. Pertama, harus ada organisasi yang membeli franchise untuk memberikan dukungan keuangan dan kelembagaan, termasuk investasi awal, modal kerja untuk biaya rutin, nasihat pada perusahaan baru, pelatihan manajemen, standarisasi proses, mekanisme pelaporan, dan tool pemasaran. Di samping itu, , model ini memerlukan orang desa yang bermotivasi tinggi dan dinamis, dengan ketrampilan yang cocok untuk memanage bisnis dan kemauan untuk menerima beberapa persyaratan dari organisasi franchise. Karena pengusaha biasanya akan diminta untuk mengalokasikan sumber daya mereka untuk biaya awal, mereka harus memiliki akses yang memadai ke sumber daya keuangan. Terakhir, untuk memastikan model ini akan berkesinambungan, seharusnya ada cukup permintaan untuk informasi dan komunikasi dan beberapa pesaing di komunitas.

Kesimpulan

Tidak ada satu model bisnis akan memungkinkan jaringan nirkabel berkelanjutan di semua lingkungan dari negara berkembang; berbagai model harus digunakan dan disesuaikan dengan keadaan. Setiap masyarakat memiliki karakteristik yang unik, dan analisis yang cukup harus dilakukan pada permulaan dari sebuah proyek untuk menentukan model yang paling sesuai. Analisis ini harus mempertimbangkan beberapa faktor dalam lingkungan lokal, termasuk permintaan masyarakat, persaingan, biaya, sumber daya ekonomi, dll Meskipun perencanaan yang baik dan pelaksanaannya akan memaksimalkan kemungkinan membuat jaringan anda berkesinambungan, tidak ada jaminan bahwa jaringan kita akan berhasil. Namun, dengan menggunakan metode yang detail seperti di jelaskan dalam bab ini, anda akan membantu untuk memastikan bahwa jaringan anda akan memberikan manfaat kepada masyrakat yang sesuai dengan kebutuhan pengguna.

Bab 11 Studi Kasus

Tidak peduli berapa banyak perencanaan yang dilakukan pada saatnya anda harus membangun sebuah sambungan atau node, anda harus terjun dan menginstalasi sesuatu. Ini merupakan momen pembuktian untuk melihat berapa akurat perkiraan dan prediksi yang anda lakukan.

Sangat langka jika semuanya berjalan persis seperti yang direncanakan. Bahkan setelah anda menginstal node yang pertama, 10, atau 100, anda masih akan menemukan hal-hal yang tidak selalu bekerja seperti yang telah anda rancang. Bab ini menjelaskan beberapa kenangan proyek jaringan kami. Apakah anda akan mengambil bagian pada proyek nirkabel pertama anda atau anda adalah seorang ahli di ini, sangat menenangkan untuk diingat bahwa selalu ada sesuatu untuk dipelajari.

Nasihat umum

Ekonomi di negara-negara berkembang sangat berbeda dari negara maju, sehingga proses atau solusi yang dirancang untuk negara maju mungkin tidak cocok di Afrika Barat, atau Asia Selatan. Khususnya, biaya produksi bahan lokal dan biaya tenaga kerja akan diabaikan, sedangkan impor barang dapat lebih mahal dibandingkan dengan biaya di negara maju. Misalnya, salah satu produsen dan dapat memasang menara dengan biaya seperseputih dari sebuah menara di Amerika Serikat, tetapi harga antena mungkin dobel. Solusi yang mempergunakan keunggulan kompetitif lokal, yaitu tenaga kerja murah dan bahan-bahan lokal, akan termudah untuk ditiru / di replikasi.

Mencari peralatan yang tepat adalah salah satu tugas yang paling sulit dalam pengembangan pasar. Karena transportasi, komunikasi dan sistem ekonomi belum berkembang, materalatau peralatan yang cocok sangat sulit dan sering mustahil untuk dinemukan. Sebuah sekering, misalnya, sulit untuk dinemukan, sehingga mencari kawat yang telah terbakar pada arus tertentu dapat digunakan sebagai pengganti merupakan keuntungan yang besar. Mencari pengganti bahan-bahan lokal akan mendorong kewirausahaan, kepemilikan, dan dapat untuk menambung.

Rumah Penutup Peralatan

Plastik yang murah ada di mana-mana di negara berkembang, tetapi mereka terbuat dari bahan-bahan yang jelek dan tipis, sehingga tidak cocok untuk rumah penutup peralatan. Sistem pipa-pipa PVC adalah jauh lebih kuat dan dibuat untuk tahan air. Di Afrika Barat, pipa PVC yang paling sering ditemukan adalah untuk saluran air, dari ukuran 90mm sampai 220mm. Akses point seperti Routerboard 500 dan 200 yang dapat disimpan ke dalam pipa-

pipa tersebut, dan dengan ujungnya di tutup, PVC dapat dibuat menjadi rumah kedap air yang sangat kuat. Mereka juga memiliki tambahan manfaat yang aerodinamis dan tidak menarik bagi orang yang lalu lalang. Ruang sisa yang ada di sekitar peralatan menjamin adanya sirkulasi udara yang memadai. Selain itu, sebaiknya dibuatkan sebuah lubang di bagian bawah rumah PVC. Penulis tidak menemukan bahwa membuka lubang pada PVC dapat menjadi masalah. Dalam sebuah kasus, kelompok semut memutuskan untuk sarang 25 meter di atas tanah di dalam PVC tempat akses point. Menggunakan kawat penutup yang terbuat dari bahan lokal untuk mengamankan lubang dari serangan serangga.

Tiang Antena

Menggunakan material bekas menjadi penting untuk industri di negara termiskin. Dari mobil tua hingga televisi, material yang memiliki nilai akan dipreteli, dijual, atau digunakan kembali. Misalnya, anda akan melihat sebuah mobil di preteli satu persatu komponen-nya dari hari ke hari. Besi yang dihasilkan akan di simpan kemudian di masukan ke truk untuk di jual. Pekerja logam lokal sudah terbiasa untuk membuat kerangka televisi dari besi tua. Beberapa adaptasi cepat untuk membuat kerangka ini untuk jaringan nirkabel.

Tiang yang banyak digunakan adalah tiang 5 meter, yang terdiri dari satu tiang dengan diameter 30 mm yang ditanam ke dalam semen. Sebaiknya membangun tiang dalam dua bagian, bagian tiang yang dapat di lepas yang dimasukan ke dasar tiang yang lebih besar diameternya. Alternatif lain, tiang yang dapat dibuat dengan tangan kecil yang dapat di semen dengan aman ke dinding. Proyek ini mudah, namun memerlukan penggunaan tangga untuk menyelesaikan dan sangat di sarankan untuk berhati-hati.

Tiang jenis ini dapat diperpanjang beberapa meter dengan penggunaan beberapa tali pengikat. Untuk tiang yang kuat, tanam tiga tali pengikat dalam sudut 120 derajat, membentuk sebuah sudut minimal 33 derajat dengan menara.

Di atas semua: libatkan masyarakat setempat

Keterlibatan masyarakat snagat penting dalam memastikan keberhasilan dan keberlangsungan proyek. Melibatkan masyarakat dalam proyek dapat menjadi tantangan terbesar, tetapi jika masyarakat tidak terlibat teknologi tidak akan melayani kebutuhan mereka, dan tidak akan diterima. Selain itu, masyarakat yang takut dan mungkin dapat merusak inisiatif. Apapun kompleksitas yang dilakukan, kesuksesan proyek membutuhkan dukungan dari orang-orang yang akan dilayani.

Strategi yang efektif dalam mendapatkan dukungan adalah untuk mencari pemimpin yang dihormati dengan tujuan yang benar. Menemukan orang, atau orang-orang yang tertarik dengan proyek. Seringkali, anda perlu melibatkan pemimpin tersebut sebagai penasehat, atau sebagai seorang anggota steering komitea. Orang-orang ini sudah memperoleh

kepercayaan dari masyarakat, akan tahu siapa yang harus didekati, dan dapat berbicara bahasa masyarakat setempat. Luangkan waktu anda agar dapat secara selektif dalam mencari orang yang tepat untuk proyek anda. Adalah sebuah keputusan yang sangat strategis untuk memperoleh orang lokal yang effektif dan di percaya dari masyarakat setempat. Selain itu, perhatikan pemain kunci dalam sebuah lembaga, atau masyarakat. Mengidentifikasi orang-orang yang kemungkinan besar akan lawan dan proyek proponent proyek Anda. Sedini mungkin, berusaha untuk mendapatkan dukungan lawan dan membaur dengan lawan-lawan. Ini merupakan hal yang sulit memerlukan keintiman dengan lembaga atau masyarakat. Jika proyek tidak memiliki sekutu lokal, proyek harus meluangkan banyak waktu untuk memperoleh pengetahuan dan kepercayaan dari masyarakat.

Hati-hati dalam memilih sekutu anda. Sebuah pertemuan di "balai kota" sering berguna untuk melihat politik lokal, dan aliansi yang terjadi. Selanjutnya, akan lebih mudah untuk memutuskan siapa yang dijadikan sekutu, dan siapa pemimpun dan siapa yang perlu untuk membaur. Coba untuk tidak mengendurkan semangat. Penting untuk berlaku jujur, terus terang, dan tidak membuat janji-janji yang tidak dapat anda tepati.

Pada masyarakat yang sebagian besar buta huruf, fokus pada layanan Internet dari digital ke analog seperti untuk stasiun radio, pencetakan artikel dan foto on-line, dan aplikasi non-tekstual lainnya. Jangan mencoba untuk memperkenalkan teknologi kepada masyarakat tanpa pemahaman aplikasi yang akan benar-benar akan melayani masyarakat. Seringkali masyarakat akan memiliki sedikit ide bagaimana teknologi baru akan membantu masalah mereka. Cukup menyediakan fitur baru yang berguna tanpa pemahaman tentang bagaimana masyarakat akan manfaat.

Saat mengumpulkan informasi, verifikasi fakta yang diberikan. Jika Anda ingin mengetahui status keuangan perusahaan / organisasi, meminta untuk melihat rekening listrik, telepon atau tagihan. Apakah mereka telah membayar tagihan mereka? Pada saat ini, calon penerima donor suka membohongi nilai-nilai mereka sendiri berharap memenangkan dana atau peralatan. Seringkali, mitra lokal yang anda percaya akan sangat terus terang, jujur, dan suka menolong.

Kesalahan umum adalah yang saya sebut sindrom "orang tua bercerai", dimana LSM, donor, dan mitra tidak saling memberitahu keterlibatan masing-masing dengan si penerima dana / manfaat. Penerima yang mahir akan memperoleh hadiah yang menarik dengan membiarkan LSM dan donor memberi mereka dengan peralatan, pelatihan dan dana. Adalah penting untuk mengetahui organisasi lain yang terlibat sehingga anda dapat memahami dampak kegiatan mereka pada anda sendiri. Misalnya, saya pernah merancang proyek untuk sekolah di pedesaan Mali. Tim saya menginstalasi open source dengan komputer bekas dan menghabiskan beberapa hari melatih masyarakat bagaimana untuk menggunakannya. Proyek ini dianggap berhasil, tetapi segera setelah instalasi, donor lain tiba dengan komputer Pentium 4 baru menjalankan Windows XP. Siswa dengan cepat ditinggalkan komputer lama dan menggunakan komputer baru. Akan lebih baik untuk melakukan negosiasi dengan sekolah di awal, untuk mengetahui komitmen mereka untuk proyek. Jika mereka berterus terang, komputer bekas yang sekarang duduk tidak digunakan dapat dikirim ke sekolah lain

yang lebih membutuhkan.

Dalam banyak masyarakat di pedesaan di negara berkembang, hukum dan kebijakan sangat lemah, dan kontrak dapat menjadi sia-sia. Seringkali, jaminan lainnya harus ditemukan. Di sinilah layanan pra-bayar yang ideal, karena mereka tidak memerlukan hukum kontrak. Komitmen dijjamin oleh dana investasi sebelum layanan diberikan.

Buy-in diperlukan bagi mereka yang terlibat investasi dalam proyek itu sendiri. Sebuah proyek harus meminta keterlibatan timbal balik dari masyarakat. Di atas semua, pilihan "batal" harus selalu dievaluasi. Jika masyarakat lokal dan komunitas pengguna tidak ada, proyek harus mempertimbangkan memilih komunitas atau masyarakat penerima manfaat yang berbeda. Harus ada negosiasi; peralatan, uang, dan pelatihan tidak dapat dihadiahkan. Masyarakat harus dilibatkan dan mereka juga harus berkontribusi.
-- Ian Howard

Studi kasus: Menyeberangi keterpisahan dengan jembatan sederhana di Timbuktu

Jaringan akhirnya menghubungkan manusia menjadi satu kesatuan, dan oleh karenanya selalu melibatkan komponen politik. Biaya Internet di negara kurang berkembang sangat tinggi dan kemampuan untuk membayar rendah, ditambah dengan tantangan politik. Mencoba untuk membangun jaringan di atas jaringan manusia yang tidak sepenuhnya berfungsi adalah hampir mustahil untuk jangka panjang. Mencoba untuk melakukannya dapat meninggalkan sebuah proyek di situasi sosial yang tidak stabil, mengancam keberadaannya. Di sinilah biaya rendah dan mobilitas dari jaringan nirkabel dapat menguntungkan.

Tim penulis diminta oleh penyandang dana untuk menentukan cara untuk menghubungkan desa dengan stasiun radio ke telecenter yang sangat kecil (2 komputer) ke Internet di Timbuktu, padang gurun ibukota Mali. Timbuktu ini lebih banyak dikenal sebagai daerah terpencil di dunia. Pada situs ini, tim memutuskan untuk menerapkan model yang telah disebut ***model parasit nirkabel***. Model ini mengambil sambungan dari jaringan nirkabel yang sudah ada, dan memperpanjang jaringan ke sisi klien menggunakan jaringan bidge sederhana. Model ini dipilih karena tidak memerlukan investasi yang besar dari organisasi pendukung. Meskipun menambahkan sumber pendapatan bagi telecentre, tapi tidak menambah biaya operasional yang besar. Solusi ini dimaksudkan bahwa klien bisa mendapatkan situs internet murah, walaupun tidak cepat atau sebagai dapat diandalkan sebagai solusi berdedikasi. Karena pola penggunaan berlawanan antara kantor dan telecentre tidak ada tampak perlambatan dari jaringan untuk masing-masing pihak.

Walaupun dalam situasi yang ideal akan lebih baik untuk mendorong pembangunan telecentre kecil ke sebuah ISP, sayangnya baik telecentre maupun pasar tidak siap. Seperti yang sering terjadi, ada keprihatinan serius tentang apakah telecentre ini dapat menjadi berdiri sendiri saat nanti pemberi dana meninggalkannya. Dengan demikian, solusi yang ada

berusaha meminimalkan investasi awal sementara mencapai dua tujuan: pertama, memberikan Internet untuk penerima manfaat yang di targetkan, sebuah stasiun radio, dengan biaya yang terjangkau. Kedua, ia menambahkan sedikit tambahan sumber pendapatan telecentre untuk sementara tanpa meningkatkan biaya operasional maupun tanpa menambahkan kompleksitas sistem.

Orang

Timbuktu sangat remote, tetapi memiliki nama terkenal dunia. Menjadi simbol keterpencilan, banyak proyek-proyek telah ingin "tiang bendera" di pasir gurun kota ini. Dengan demikian, ada beberapa aktifitas teknologi informasi dan komunikasi (ICT) di daerah ini. Pada perhitungan terakhir ada delapan (8) sambungan satelit ke Timbuktu, yang sebagian besar berupa layanan khusus kecuali dua operator, SOTELMA dan Ikatel. Mereka saat ini menggunakan sambungan VSAT ke jaringan telepon mereka ke daerah-daerah lainnya. Telecentre ini menggunakan sambungan X.25 ke salah satu Telkom ini, yang kemudian direlay kembali ke Bamako. Berbeda relatif jauh dengan kota-kota lain di negara ini, Timbuktu memiliki jumlah staf TI terlatih, yang ada di tiga telecentre, ditambah yang baru diinstal telecentre di stasiun radio. Kota ini pada beberapa tahap mempunyai sambungan Internet yang cukup jenuh, menjangkau kepentingan swasta dan komersial yang berkelanjutan.

Pilihan disain

Dalam instalasi ini situs klien hanya 1 km secara line of sight. Dua buah akses point Linksys yang sudah di modifikasi, di isi dengan OpenWRT dan di set pada mode bridge, terpasang. Satu dipasang pada dinding bangunan telecentre, dan lainnya yang telah terpasang 5 meter di atas tiang stasiun radio. Satu-satunya parameter konfigurasi yang diperlukan pada kedua perangkat adalah ssid dan kanal. Antenna panel sederhana 14 dBi (dari *http://hyperlinktech.com/*) yang digunakan. Di sisi internet, akses point dan antena yang terpasang menggunakan sekrup untuk semen ke bagian samping bangunan, menghadap ke situs klien. Di situs klien, tiang antenna yang ada digunakan. Akses point dan antena dipasang menggunakan cincin pipa.

Untuk memutuskan klien, telecentre cukup mematikan bridge di sisi mereka. Tambahan node / situs nantinya akan diinstal, dan masing-masing akan akan memiliki bridge di telecentre sehingga staf dapat secara fisik mematikan sambungan klien jika mereka tidak membayar. Walaupun kasar, ini adalah solusi efektif dan mengurangi resiko bahwa staf akan membuat kesalahan saat membuat perubahan pada konfigurasi sistem. Mempunyai bridge yang dikhususkan untuk satu sambungan membuat sederhana instalasi di pusat. Sehingga tim instalasi dapat memilih tempat terbaik untuk menghubungkan situs klien. Meskipun tidak optimal menjembatani jaringan (daripada menggunakan router untuk lalu lintas jaringan), ketika pengetahuan tentang teknologi rendah adalah kita ingin menginstali sebuah sistem sangat sederhana maka solusi ini sangat cocok untuk jaringan kecil. Bridge membuat sistem yang terpasang di situs remote (stasiun radio) muncul seolah-olah mereka terhubung ke

jaringan lokal.

Model keuangan

Model keuangan di sini sangat sederhana. Telecentre menarik biaya bulanan, sekitar $30 per komputer yang terhubung ke stasiun radio. Hal ini jauh lebih murah dibandingkan dengan alternatif lainnya. Telecentre yang terletak di pengadilan dekat kantor Walikota, sehingga klien utama dari telecentre adalah staf Walikota. Hal ini penting karena stasiun radio tidak ingin bersaing dengan telecentre dan sistem stasiun radio yang terutama ditujukan untuk staf stasiun radio. Cara cepat ini dikurangi biaya, ini berarti bahwa klien yang sangat selektif dapat mendukung biaya Internet tanpa harus bersaing dengan telecentre maupun para pemasok. Telecentre juga memiliki kemampuan untuk dengan mudah putuskan stasiun radio jika mereka tidak membayar. Model ini juga mengijinkan berbagi sumber daya jaringan. Misalnya, stasiun radio baru memiliki printer laser, sedangkan telecentre memiliki warna printer. Karena sistem klien berada pada jaringan yang sama, pelanggan dapat mencetak di kedua jaringan tersebut.

Pelatihan

Untuk mendukung jaringan ini, sangat sedikit pelatihan yang diperlukan. Staf telecentre hanya perlu di perlihatkan bagaimana cara memasang peralatan dan dasar troubleshooting, seperti reboot akses point, dan bagaimana untuk menggantikan unit yang rusak. Hal ini memungkinkan tim penulis untuk mengirimkan penggantian dan menghindari dua hari perjalanan ke Timbuktu.

Ringkasan

Instalasi dianggap sebuah ukuran. Hal ini dimaksudkan sebagai langkah sementara sebelum memperoleh solusi lengkap untuk maju. Meskipun dapat dianggap sebagai keberhasilan, itu belum memimpin untuk pembangunan infrastruktur fisik lebih jauh. Ini telah membawa ICT dekat dengan solusi radio, dan mempererat hubungan klien - pemasok lokal.

Karena itu, akses Internet masih mahal di Timbuktu. Politik lokal dan persaingan inisiatif subsidi sedang berjalan, namun solusi yang sederhana ini telah terbukti sangat ideal untuk digunakan. Memerlukan waktu beberapa bulan bagi tim untuk melakukan analisis dan berpikir kritis untuk tiba di sini, tetapi tampaknya ini merupakan solusi yang paling sederhana yang paling memberikan manfaat.

--Ian Howard

Studi kasus: Mencari pijakan yang keras di Gao

Satu hari berkendara ke timur Timbuktu, di Mali Timur, adalah Gao. Kota pedesaan ini,

tampaknya seperti desa yang besar, yang duduk di atas sungai Niger sebelum terus ke selatan ke persimpangan ke Niger dan masuk ke Nigeria. Kota di lereng yang masuk menuju sungai, dan memiliki beberapa bangunan tinggi dengan maksimum dua tingkat. Pada tahun 2004, sebuah telecentre dipasang di Gao. Tujuan proyek ini adalah untuk memberikan informasi kepada masyarakat dengan harapan membuat masyarakat kebih sehat dan lebih berpendidikan.

Pusat tersebut menyediakan informasi melalui CD-ROM, film dan radio, tetapi sumber informasi utama dari pusat tersebut adalah Internet. Ini merupakan standar telecentre, dengan 8 komputer, yang all-in-one printer, scanner, fax, telepon dan kamera digital. Sebuah bangunan kecil dengan dua kamar dibangun untuk telecentre. Terletak sedikit di luar kota, yang bukan merupakan lokasi yang ideal untuk menarik pelanggan, tetapi situs ini dipilih karena pemiliknya yang sangat simpatik. Pusat tersebut menerima bantuan dana untuk semua konstruksi diperlukan, dan peralatan dan termasuk pelatihan awal. Telecentre diharapkan dapat mandiri setelah satu tahun.

Beberapa bulan setelah dibuka, telecentre telah menarik beberapa pelanggan. Telecentre menggunakan modem dial-up untuk koneksi ke internet melalui provider di ibukota. Koneksi ini terlalu lambat dan tidak dapat diandalkan, dan sehingga lembaga donor mendanai instalasi sebuah sistem VSAT. Ada sejumlah sistem VSAT sekarang tersedia untuk daerah; kebanyakan dari layanan ini hanya baru-baru ini saja tersedia. Sebelumnya hanya sistem C-band (yang mencakup wilayah yang lebih besar dari Ku-band) yang tersedia. Baru-baru ini, serat optik telah meletakkan hampir di setiap terowongan kereta bawah tanah dan kanal di seluruh Eropa, dan dengan demikian ia telah menggantikan layanan satelit yang lebih mahal. Akibatnya, penyedia layanan mengarahkan sistem VSAT mereka ke pasar baru, termasuk Afrika Tengah dan Barat, dan Asia Selatan. Ini telah menyebabkan sejumlah proyek yang menggunakan sistem satelit untuk sambungan Internet.

Setelah VSAT terpasang, sambungan yang disediakan 128 kbps down dan 64 kbps up, dengan biaya sekitar $400 per bulan. Telecentre ini kesulitan untuk mendapatkan penghasilan cukup untuk membayar biaya bulanan yang tinggi ini, sehingga telecentre mencari bantuan. Sebuah kontraktor swasta telah disewa, yang telah dilatih oleh penulis untuk memasang sistem nirkabel. Sistem ini akan memecah sambungan yang ada ke tiga klien: dua klien lain, sebuah stasiun radio, dan telecentre, masing-masing membayar $140. Pembayaran secara kolektif ini cukup untuk membiayai VSAT, dan tambahan pendapatan dari telecentre dan stasiun radio cukup dukungan dan administrasi sistem.

Orang

Walaupun mampu dan bersedia, tim penulis tidak melakukan instalasi yang sebenarnya. Sebagai gantinya, kami mendorong telecentre untuk menyewa kontraktor lokal untuk melakukannya. Kami mampu meyakinkan klien dengan setuju untuk melatih dan mendukung kontraktor dalam penyelesaian instalasi ini. Dasar dari keputusan ini adalah melepaskan

ketergantungan pada LSM jangka pendek, dan bukan untuk membangun kepercayaan dan hubungan antara penyedia layanan domestik dengan pelanggan mereka. Hal ini terbukti bahwa pendekatan tersebut berhasil. Mengambil pendekatan ini membuat tim penulis harus meluangkan lebih banyak waktu, mungkin dua kali lebih banyak, namun investasi ini mulai terbayarkan. Jaringan masih terpasang dan tim penulis sekarang kembali ke rumah masing-masing di Eropa dan Amerika Utara.

Pilihan disain

Pada awalnya, sangat penting untuk menyambungkan tulang punggung sambungan ke stasiun radio, yang telah memiliki menara 25 meter. Menara akan digunakan untuk relay ke klien lain, menghindari kebutuhan untuk memasang menara di situs klien, karena menara jauh lebih tinggi dari halangan yang ada dalam kota. Untuk melakukan ini, tiga pendekatan yang dibahas: memasang akses point dalam mode pengulang, menggunakan protokol WDS, atau menggunakan protokol routing mesh. Mode pengulang / repeater tidak diingini karena akan memasukan latensi (karena yang masalah one-armed repeater) pada sambungan yang sudah lambat. Sambungan VSAT perlu mengirim paket sampai ke satelit dan kembali ke bawah, sering memasukan delay sampai 3.000 ms di sepanjang perjalanan. Untuk menghindari masalah ini, telah diputuskan untuk menggunakan satu radio untuk koneksi ke klien, dan radio kedua untuk khusus untuk sambungan ke backbone. Untuk penyederhanaan diputuskan untuk membuat sebuah sambungan bridge sederhana, sehingga akses point di stasiun radio akan terlihat pada fisik yang sama pada LAN telecentre.

Dalam uji apakah pendekatan ini berfungsi, meskipun dalam dunia nyata, kinerjanya cukup suram. Setelah berbagai perubahan, termasuk menggantikan akses point, teknisi memutuskan bahwa tampaknya ada software atau hardware bug yang mempengaruhi desain. Installer kemudian memutuskan untuk meletakkan akses point di telecentre secara langsung menggunakan tiang pendek 3 meter, dan tidak menggunakan stasiun radio sebagai situs untuk relay. Situs klien menggunakan pipa pendek dalam desain ini. Semua situs berhasil terhubung, walaupun sambungan sangat lemah, dan mempunyai banyak paket loss.
Kemudian, selama musim debu, sambungan ini menjadi lebih aneh dan bahkan kurang stabil. Situs klien berada pada jarak 2 sampai 5 km, menggunakan 802.11b. Tim berteori bahwa menara di kedua sisinya terlalu pendek, memotong terlalu banyak dari zona Fresnel. Setelah membahas banyak teori, tim juga menyadari ada masalah dengan kinerja stasiun radio: radio frekuensi 90,0 MHz hampir sama dengan frekuensi dari sambungann Ethernet kecepatan tinggi (100BT). Sementara transmisi, sinyal FM (pada 500 watt) telah sepenuhnya masuk pada kabel Ethernet. Dengan demikian, diperlukan kabel Ethernet yang mempunyai shield / pelindung, atau frekuensi sambungan jaringan perlu diubah. Pipa disisi klien di naikan, dan di stasiun radio kecepatan dari Ethernet diubah menjadi 10 Mbps. Frekuensi ini berubah pada kawat menjadi 20 MHz, dan terhindar dari gangguan transmisi FM. Perubahan ini menyelesaikan kedua masalah, meningkatkan kekuatan dan keandalan dari jaringan. Keuntungan dari menggunakan mesh atau WDS di sini bahwa klien akan dapat terhubung ke salah satu akses point, baik secara langsung ke telecentre atau ke stasiun radio. Pada

akhirnya, mengeluarkan bergantung pada stasiun radio sebagai pengulang / repeater membuat instalasi lebih stabil dalam jangka waktu yang lebih panjang.

Model keuangan

Sistem satelit yang digunakan di situs memerlukan biaya sekitar $400 per bulan. Untuk banyak pembangunan proyek IT ini biaya bulanan yang mahal dan sulit untuk mengelola. Biasanya proyek ini dapat membeli peralatan dan membayar untuk instalasi jaringan nirkabel, tapi paling tidak mampu untuk membayar biaya dari jaringan setelah waktu singkat (termasuk biaya Internet dan biaya operasional). Penting untuk menemukan sebuah model dimana biaya bulanan untuk jaringan dapat dipenuhi oleh orang-orang yang menggunakan. Untuk sebagian besar masyarakat telecenter atau stasiun radio, ini adalah cukup terlalu mahal. Seringkali, satu-satunya adalah rencana yang baik adalah berbagi biaya dengan pengguna lain. Untuk membuat internet lebih terjangkau, situs ini digunakan untuk berbagi nirkabel internet untuk masyarakat, yang memungkinkan lebih banyak organisasi untuk mengakses Internet sekaligus mengurangi biaya per klien.

Biasanya di Mali, di komunitas pedesaan hanya ada beberapa organisasi atau perusahaan yang mampu tersambung ke Internet. Hanya ada beberapa klien, karena biaya koneksi internet yang tinggi, model yang dikembangkan oleh tim termasuk klien besar: klien yang kuat dan siapa yang berisiko rendah. Untuk daerah ini, LSM asing (Organisasi non pemerintah), Badan PBB yang besar dan perusahaan komersial termasuk di antara yang sangat sedikit yang memenuhi syarat. Di antara klien dipilih untuk proyek ini adalah tiga klien besar, yang membayar secara kolektif seluruh biaya bulanan dari sambungan satelit. Penerima manfaat kedua, sebuah stasiun radio komunitas, juga telah terhubung. Setiap penghasilan yang diperoleh memberikan kontribusi untuk biaya deposit untuk masa depan, tetapi tidak diperhitungkan karena margin kecil dimana layanan masyarakat ini dioperasikan. Klien mereka dapat melepaskan dan dapat melanjutkan layanan mereka jika mereka mampu lagi.

Pelatihan Yang Diperlukan: Siapa, Apa, Untuk Berapa Lama

Kontraktor mengajarkan teknisi telecentre teknisi dasar-dasar untuk mendukung jaringan, yang sangat sederhana. Setiap pekerjaan non-rutin, seperti menambahkan klien baru, dikontrakan keluar. Oleh karena itu, tidak terlalu penting mengajar staf telecentre bagaimana untuk mendukung sistem secara keseluruhan.

Pelajaran yang di peroleh

Dengan berbagi sambungan, telecentre menjadi mandiri dan berkesinambungan, dan di tambah, tiga situs lainnya memperoleh akses Internet. Walaupun hal tersebut akan memakan

lebih banyak waktu dan lebih banyak uang, akan sangat berharga jika kita dapat menemukan talen lokal dan mendorong mereka untuk membangun sambungan dengan klien. Seorang teknisi lokal akan mampu menyediakan dukungan selanjutnya yang dibutuhkan untuk mempertahankan dan memperluas jaringan. Kegiatan ini membangun keahlian lokal, dan permintaan lokal, yang akan memungkinkan proyek ICT selanjutnya untuk di bangun dengan dasar proyek ini.

-- Ian Howard

Studi Kasus: Komunitas jaringan nirkabel Fantsuam Foundation

Kafanchan adalah sebuah komunitas dengan 83.000 orang terletak 200 km timur laut Abuja, di Pusat Nigeria. Kafanchan dikenal sebagai kota yang sibuk dan berkembang, tuan rumah dari salah satu pertemuan utama dari jalur kereta api nasional. Pada masa industri kereta api booming, hampir 80% dari populasi Kafanchan mengandalkan dirinya para industri tersebut melalui satu atau cara lain. Setelah hancurnya sistem kereta api Nigeria, penduduk Kafanchan dipaksa untuk kembali ke sumber pendapatan aslinya, yaitu pertanian.

Kafanchan adalah daerah yang kurang terhubung dalam telepon dan sambungan Internet. Saat ini, tidak ada layanan telepon tetap (PSTN) yang tersedia di wilayah tersebut, dan GSM baru masuk di tahun 2005. Namun, cakupan jaringan GSM sangat jelek seperti juga kualitas layanannya. Saat ini, SMS adalah layanan yang paling dapat diandalkan karena layanan komunikasi suara percakapan cenderung terputus-putus dan sangat bising.

Ketiadaan listrik membuat tambangan tantangan bagi orang Kafanchan. Perusahaan listrik nasional Nigeria, dikenal sebagai NEPA (National Electric Power Authority), adalah banyak dikenal oleh orang Nigeria sebagai “Never Expect Power Always” (“Jangan Pernah Berharap Ada Listrik”). Pada tahun 2005, NEPA berubah nama menjadi Power Holding Company Nigeria (PHCN).

Kafanchan menerima listrik dari NEPA rata-rata 3 jam per hari. Untuk sisanya 21 jam, penduduk harus mengandalkan generator solar yang mahal atau minyak tanah untuk penerangan dan memasak. Ketika NEPA tersedia pada jaringan listrik, ia memberikan tegangan tidak stabil dalam kisaran antara 100-120 V pada sebuah sistem yang dirancang untuk tegangan 240 V. Seharusnya tegangan stabil pada 240 V sebelum ada beban yang terhubung. Hanya lampu dapat dicolok langsung ke listrik karena lampu dapat di operasikan pada tegangan rendah tanpa rusak.

Peserta Proyek

Mengingat latar belakang tantangan pada Kafanchan, bagaimana kita dapat

mengimplementasi ide membentuk Wireless ISP pedesaan di Nigeria?

Fantsuam Foundation melakukannya dan mereka membuat semua ini terjadi.
Fantsuam Foundation adalah organisasi non-pemerintah lokal yang telah bekerjasama dengan komunitas di Kafanchan sejak tahun 1996 untuk memerangi kemiskinan dan ketertinggalan melalui program pembangunan terpadu. Fantsuam fokus pada keuangan mikro, layanan ICT dan pembangunan sosial di komunitas pedesaan Nigeria. Menjadi ISP nirkabel pedesaan pertama di Nigeria adalah bagian dari misi mereka untuk menjadi pemimpin diakui dalam inisiatif pembangunan pedesaan, terutama pendorong pengetahuan ekonomi pedesaan di Nigeria.

ISP Wireless dari Fantsuam Foundation, dikenal sebagai Zittnet, didanai oleh IDRC, International Development Research Center Kanada. IT +46, sebuah perusahaan konsultan yang berbasis di Swedia yang fokus pada ICT untuk pembangunan, telah bekerja sama dengan tim Zittnet untuk memberikan dukungan teknis untuk komunikasi nirkabel, bandwidth manajemen, energi surya, daya cadangan dan implementasi sistem VoIP.

Tujuan

Tujuan utama dari Zittnet adalah untuk meningkatkan akses untuk komunikasi di kawasan Kafanchan melalui implementasi dari jaringan nirkabel komunitas. Jaringan tersebut menyediakan akses internet dan intranet untuk mitra lokal di komunitas. Masyarakat jaringan ini dibentuk oleh organisasi berbasis masyarakat seperti lembaga pendidikan, lembaga keagamaan, layanan kesehatan, usaha kecil dan individu.

Cadangan daya sistem

Untuk dapat memberikan pelayanan yang reliable kepada masyarakat, Zittnet perlu melengkapi dengan sistem cadangan daya yang stabil yang akan membuat jaringan berjalan secara mandiri terlepas dari NEPA. Sebuah sistem hibrid daya dirancang untuk Fantsuam, yang terdiri dari tempat penyimpanan batere dan panel surya 2 kW (puncak). Sistem memperoleh pasokan daya dari tiga sumber: generator solar, kumpulan panel surya, dan dari NEPA bila listrik tersedia. Network Operation Center (NOC) dari organisasi berjalan sepenuhnya dari tenaga surya. Sisa dari peralatan Fantsuam beroperasi dengan catu daya dari NEPA atau generator melalui tempat penyimpanan batere, yang memberikan tegangan yang stabil. Beban NOC dipisahkan dari beban lainnya dari Fantsuam untuk memastikan sumber daya yang handal ke infrastruktur yang sangat penting dalam NOC, meskipun saat tempat penyimpanan batere bekerja dengan sisa daya yang rendah.

Gambar 11.1: 24 panel surya dengan daya nominal 80 W telah terpasang di atap NOC untuk menyediakan daya untuk sistem 24 / 7.

Simulasi dengan data matahari terbaik yang ada memperlihatkan bahwa negara bagian Kaduna, dimana Kafanchan terletak, menerima paling tidak empat (4) jam puncak matahari saat bulan-bulan paling jelek antara bulan Juni sampai Agustus (musim hujan). Masing-masing panel surya (Suntech 80W peak) menyediakan maksimum arus 5 A (saat radiasi matahari tertinggi di siang hari). Dalam bulan terburuk dalam setahun, sistem ini diharapkan dapat menghasilkan tidak kurang dari 6 kWh/hari.

Sistem tenaga surya dirancang untuk menyediakan tegangan keluargan 12 dan 24 V DC agar sesuai dengan tegangan masukan server berdaya rendah dan workstation pada infrastruktur NOC maupun pada kelas untuk pelatihan.

Panel surya yang digunakan adalah **Suntech STP080S-12/Bb-1** dengan spesifikasi berikut:

- Tegangan sirkit terbuka (V_{OC}) : 21,6V
- Tegangan operasi optimal (V_{MP}) : 17.2V
- Arus hubung singkat (I_{SC}) : 5A
- Arus operasi optimum (I_{MP}) : 4,65A
- Maksimum daya di STC (P_{MAX}) : 80 W (Puncak)

Minimum 6 kWh/hari yang di alirkan ke NOC digunakan untuk memberikan daya bagi peralatan berikut:

Alat	Jam/Hari	Unit	Daya (W)	Wh
Akses Point	24	3	15	1080
Low Power Server	24	4	10	960
Layar LCD	2	4	20	160
Laptop	10	2	75	1500
Lampu	8	4	15	480
VSAR Modem	24	1	60	1440
Total				**5620**

Konsumsi daya untuk server dan layar LCD dihitung berdasarkan perhitungan Inveneo Low Power Station, *http://www.inveneo.org/?q=Computingstation.*

Jumlah estimasi konsumsi daya NOC adalah 5,6 kWh/hari yang kurang dari daya harian yang dihasilkan dari panel surya saat bulan terburuk.

Gambar 11.2: NOC yang dibangun dari batu bata laterite, diproduksi dan diletakkan oleh pemuda di Kafanchan.

Network Operating Center (NOC)

Sebuah Pusat Operasi Jaringan baru dibentuk menjadi tempat sistem cadangan daya dan fasilitas ruang server. NOC dirancang untuk menyediakan tempat aman dari debu, dengan pendinginan dengan baik dari batere dan inverter. NOC dibangun menggunakan metode alami dan dibuat dari bahan-bahan lokal yang tersedia. Bangunan terdiri dari empat kamar:

ruang penyimpanan batere, ruang server, ruang kerja dan ruang untuk penyimpanan peralatan.

Ruang penyimpanan batere menyimpan tujuh puluh batere 200 Ah, serta lima inverters (salah satu dari mereka dapat menghasilkan gelombang sinus murni), dua regulator matahari, penstabil daya / stabilizer dan disconnect DC dan AC. Batere ditumpuk vertikal pada struktur logam rak untuk pendinginan yang lebih baik.

Ruang server terdapat sebuah rak untuk server dan kipas angin. Ruangan tidak memiliki jendela biasa, untuk menghindari debu dan panas. Ruang server dan ruang batere menghadap selatan untuk meningkatkan pendinginan alam dan untuk membantu menjaga kamar pada suhu yang sesuai.

Ruang server dan ruang batere membutuhkan pendingin biaya rendah / rendah energi yang effektif karena mereka harus beroperasi 24x7. Untuk mencapai tujuan ini, teknik pendinginan alam diperkenalkan pada disain NOC: fan kecil dan extractors dan dinding tebal dari batu bata (lebar-nya double) di arah matahari terbenam.

Di sebelah selatan bangunan terletak 24 panel surya pada wilayah bebas bayangan dengan atap logam. Atap dirancang dengan inklinasi 20 derajat untuk menempatkan panel dan membatasi karat dan debu. Usaha tambahan dilakukan agar panel mudah dijangkau untuk pembersihan dan pemeliharaan. Bagian atap diperkuat untuk membawa beban tambahan 150-200 kg. NOC gedung dibangun dari batu bata lumpur laterite yang di hasilkan secara lokal. Bahan tersebut sangat murah karena sering digunakan dan berasal dari bagian atas lapisan tanah. Batu bata diproduksi secara lokal dengan menggunakan tangan dan teknologi tekan yang sederhana. NOC tersebut sangat unik dan satu-satunya di negara bagian Kaduna.

Gambar 11.3: Omolayo Samuel, salah seorang staf Zittnet, tidak takut pada ketinggian di menara 45m saat dia mengarahakan antenna yang terdapat di atap menara.

Infrastruktur fisik: Sebuah tiang komunikasi

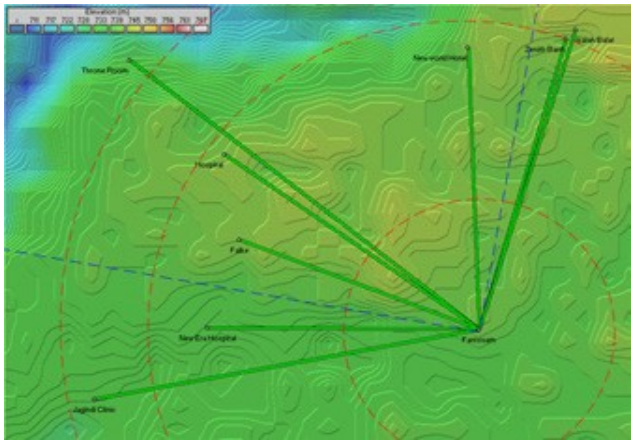
Kebanyakan klien potensial untuk Zittnet terletak antara 1 km sampai 10 km dari lokasi Fantsuam. Untuk mencapai klien ini, Fantsuam mendirikan tower komunikasi di tempat mereka. Pada bulan Oktober 2006, tower selfstanding setinggi 45m (150 kaki) tiang dipasang di Fantsuam Foundation. Tiang yang telah dilengkapi grounding dan perlindungan terhadap petir termasuk lampu isyarat yang di wajibkan.

Sebuah cincin logam telah dikuburkan di bagian bawah menara di kedalaman 4 kaki. Kesemua tiga kaki dari tiang tersebut kemudian terhubung ke sirkuit grounding. Sebuah pipa untuk anti petir telah terpasang di titik tertinggi dari tower untuk melindungi peralatan terhadap serangan petir. Pipa anti pentir terbuat dari tembaga murni dan terhubung ke cincin di tanah di bagian dasar dari tiang menggunakan pita tembaga.

Sinyal lampu terpasang di bagian atas tiang merupakan persyaratan dari Authoritas Penerbangan Sipil. Lampu akan dilengkapi dengan photocell yang memungkinkan penyalaan automatis jika hari gelap. Dengan cara ini, lampu akan nyala secara automatis saat malam hari dan mati di siang hari.

Infrastruktur Tulang Punggung Wireless

Infrastruktur tulang punggung wireless dibangun menggunakan akses point SmartBridges multi-band dan unit di klien dari Nexus seri PROTM TOTAL. Unit tersebut di rancang untuk penyedia layanan dan perusahaan untuk membangun sambungan nirkabel point-to-multipoint di luar ruangan dengan kinerja tinggi. Peralatan ini datang dengan antenna sektoral multi-band yang terpadi yang dapat beroperasi baik di frekuensi 2.4 GHz dan 5.1-5.8 GHz. Nexus seri PROTM TOTAL menawarkan QoS untuk prioritas lalu lintas dan manajemen bandwidth per klien yang sesuai dengan persyaratan IEEE 802.11e dengan extensi WMM (WiFi multimedia).



Gambar 11.4: Topologi Jaringan dari Zittnet pada Oktober 2007.

Saat ini, topologi dari jaringan adalah sebuah topologi bintang dengan dua akses point yang berada di tower komunikasi pada lokasi Fantsuam. Sebuah akses point di pasang antenna sektoral 90 derajat (garis biru titik-titik) dan akses point lainnya menggunakan antenna omnidirectional yang menyediakan cakupan ke daerah-daerah sekitarnya (lingkaran merah titik-titik). Klien yang berada dalam kawasan antara garis titik-titik terhubung ke antena sektoral, sedangkan sisanya klien tersambung ke antenna omnidirectional.

Rencana dilakukan untuk memperluas tulang punggung wireless dengan menyiapkan dua repeater wireless. Satu repeater akan berlokasi di kota Kafanchan menggunakan tower NITEL untuk meningkatkan cakupan nirkabel di pusat kota. Repeater ke dua akan didirikan di bukit Kagoro, sebuah kelompok gunung dengan ketinggian relatif terhadap Kafanchan sekitar 500 meter, yang terletak sekitar 7 km dari Kafanchan. Repeater ini akan menyediakan cakupan untuk banyak kota disekitar Kafanchan dan bahkan memungkinkan sambungan jarak jauh ke Abuja. Zittnet menghubungkan klien pertama awal Agustus 2007. Dua bulan kemudian, tidak kurang dari delapan klien tersambung ke Zittnet. Klien ini termasuk:

- Rumah sakit umum.
- Rumah sakit New Era.
- Klinik kesehatan Jagindi.
- Bank Zenith Bank (untuk penggunaan sendiri
- Isaiah Balat (Internet café)
- Hotel New World
- Throne Room GuestHouse
- Fulke

Permasalahan yang dihadapi

Beberapa masalah yang timbul sepanjang proyek adalah sebagai berikut.

Bangunan Rendah

Sebagian besar lokasi klien adalah bangunan bertingkat satu dengan ketinggian tidak lebih dari 3 meter. Banyak rumah mempunyai struktur atap yang sangat lemah yang menyulitkan untuk memasang peralatan di atap, akses secara fisik tidak mungkin dilakukan. Rendahnya bangunan memaksa kami untuk memasang peralatan pada ketinggian yang cukup rendah, karena klien tidak mampu untuk investasi tower setinggi 10 meter untuk di tempatkan peralatan. Kebanyakan instalasi memanfaatkan tangki air atau pipa besi 3 meter yang

sederhana yang di pasangkan di dinding bangunan.

Karena peralatan di pasang rendah, zona Fresnel yang pertama biasanya tidak terlampaui sehingga akan memperoleh throughput yang rendah. Meskipun dataran di Kafanchan sangat datar, vegetasi dalam bentuk pohon mangga yang rapat dengan mudah blokir line-of-sight.

Serangan Petir

Hujan badai petir sangat sering terjadi selama musim hujan di Kafanchan. Pada bulan September 2007, petir merusak peralatan yang yang di pasang pada sebuah tower, beserta power supply-nya. Saat ini, akses point dan injektor PoE (Power over Ethernet) digrounding ke tower itu sendiri. Penyeledikan lebih lanjut perlu dilakukan untuk mencegah kerusakan peralatan yang disebabkan oleh petir yang dekat. Saat ini, tim Zittnet bekerja untuk meningkatkan perlindungan dengan menambahkan tambahan anti petir pada coaxial. Selain itu, shield dari kabel UTP yang menyambungkan akses point dengan jalur NOC akan di grounding menggunakan grounding blok dan fastener.

Rendahnya kualitas peralatan

Sayangnya, kurangnya produk berkualitas di pasar adalah masalah yang luas di seluruh benua Afrika. Karena sebagian besar negara-negara sub-sahara kurangnya kebijakan untuk menjamin kualitas barang impor, pasar kebanjiran barang "murah" berkualitas sangat rendah. Karena produk berkualitas sangat sulit untuk ditemukan, anda melihat barang lokal yang kita beli rusak padahal belum digunakan. Karena tidak ada jaminan untuk pembelian kecil-kecil ini, pada akhirnya semua menjadi sangat mahal. Permasalahan ini hampir selalu hadir di aksesori umum seperti soket-soket daya, power bar, konektor RJ45, kabel CAT5, dan peralatan low-tech lainnya.

Model Bisnis

Satu-satunya alternatif untuk akses Internet di Kafanchan adalah melalui satelit. Selama tahun 2006, Fantsuam telah berlangganan dari 128/64 kbps bandwidth dengan biaya $1800 USD / bulan. Besarnya biaya sambungan bulanan telah menjadi beban yang cukup besar untuk Fantsuam dan stres karena tidak dapat memenuhi tagihan bulanan.

Sebagai alternatif dari model “bayar bulanan” yang beresiko tinggi, Fantsuam telah dilaksanakan sebuah sistem yang disebut ***HookMeUP*** disediakan oleh Koochi Komunikasi. Menawarkan sistem fleksibel Pay-As-You-Go melalui sambungan Internet broadband VSAT ke seluruh negara sub-Sahara Afrika. Jenis model akses ini biasanya ditemukan di bandara, hotel atau mall di negara-negara barat dimana user membeli kupon online dan login menggunakan kode akses (username & password).

Sistem HookMeUP menawarkan 512/256 kbps didedikasikan untuk sambungan VSAT Fantsuam (dari ground station mereka di Inggris). Fantsuam membeli kupon dari Koochi Communications dan menjual kembali mereka untuk para klien lokal di Kafanchan. Dengan cara ini, Fantsuam tidak lagi terjebak dengan biaya bulanan tetap tetapi hanya untuk membayar Koochi untuk bandwidth mereka pakai. Risiko membeli bandwidth internasional yang mahal di pindahkan ke Internet provider, bukan user, dengan biaya yang lebih tinggi dari harga untuk user.

Fantsuam Foundation saat ini bertindak sebagai reseller kupon dari Koochi dan pemasok infrastruktur nirkabel ke user. Jaringan komunitas wireless masyarakat memberikan Fantsuam Foundation dengan lima sumber pendapatan:

1. Instalasi peralatan di lokasi klien (satu kali per klien)
2. Penyewaan dari peralatan nirkabel (biaya bulanan per klien)
3. Reselling peralatan nirkabel (satu kali per klien)
4. Pemasangan nirkabel di area hotspot klien (satu kali per klien)
5. Reselling kupon (terus menerus)

Voucher sistem yang didasarkan pada tiga parameter: ***waktu akses, limit data*** dan ***waktu valid.*** Parameter mana saja yang habis pertama kali yang akan membuat kupon mati.

Waktu akses	Limit Data (MB)	Waktu Valid	Harga (USD)	USD/jam	USD/700 Mbyte
30 min	5	1 hari	0.80	1.60	112.00
60 min	10	5 hari	1.28	1.28	89.60
12 jam	60	14 hari	10.40	0.87	121.33
24 jam	150	30 hari	26.00	1.08	121.33
1 bulan	500	1 bulan	71.50	0.10	100.10
3 bulan	1600	3 bulan	208.00	0.10	91.00
6 bulan	3600	6 bulan	416.00	0.10	83.20
12 bulan	7500	12 bulan	728.00	0.08	67.95

Keuntungan terbesar yang di peroleh Fantsuam Foundation dari sistem ini adalah tidak lagi harus menanggung beban tagihan bulanan yang besar untuk bandwidth internasional. Dengan model “bayar bulanan” anda dipaksa untuk menjual sejumlah bandwidth setiap bulan. Dengan model Pay-As-You-Go (PAYG), pendapatan Fantsuam dari reselling kupon

tergantung pada berapa banyak konsumsi bandwidth klien mereka. Klien membayar di muka (model pra-bayar), oleh karenanya Fantsuam tidak akan pernah membayar hutang yang besar kepada provider.

Model pra-bayar berfungsi baik di Afrika karena orang cukup familiar dengan model ini di operator selular. Model ini bahkan digunakan oleh perusahaan listrik di beberapa negara. Model pra-bayar disukai oleh banyak orang karena membantu mereka mengetahui pengeluaran mereka. Salah satu keterbatasan utama model PAYG adalah kurangnya fleksibilitas dan transparansi. Saat ini , sistem PAYG menyediakan sangat sedikit informasi ke pengguna tentang waktu atau volume yang digunakan. Hanya ketika pengguna akan log off dia memperoleh informasi tentang berapa menit yang tersisa untuk belanja.

Namun, tampaknya model bisnis tersebut sesuai dengan realitas lokal di Kafanchan dan banyak komunitas pedesaan di Afrika. Meskipun ada ruang untuk perbaikan, menghindari hutang ternyata sangat bermanfaat di bandingkan berbagai kekurangan yang ada. Dengan perjalanan waktu, ketika jumlah pelanggan telah meningkat dan mereka mempunyai pendapatan bulanan yang mencukupi untuk berlangganan jaringan nirkabel, mungkin akan bermanfaat untuk kembali ke model langganan bulanan.

Klien

Klien bebas menggunakan akses Internet untuk tujuan apapun. Misalnya, Isaiah Balat menjual kembali kupon (yang dibeli dari Fantsuam) kepada kliennya. Di WARNET -nya ada 10 komputer yang terhubung ke semua Zittnet. Klien membeli kupon dari pemilik dengan margin 25% di atas harga yang ditawarkan oleh Fantsuam. Sebagai gantinya, klien yang memiliki komputer yang terhubung ke Zittnet dapat mengakses jaringan walaupun melalui PC di WARNET Isaiah Balat.

Hotel New World adalah pelanggan lain yang juga melakukan model usaha sejenis tapi pada skala yang lebih besar. Mereka akan menyediakan akses internet nirkabel untuk semua kamar mereka dan menawarkan akses ke uplink Zittnet dengan cara menjual kembali kupon. Klien lainnya, seperti Rumah Sakit Umum dan Klinik Jagindi Street, yang menggunakan akses Internet untuk profesional dan pribadi tanpa menjual kembali akses kepada pelanggan mereka.

-- Louise Berthilson

Studi kasus: Usaha Memperoleh Internet murah di pedesaan Mali

Selama beberapa tahun komunitas pembangunan internasional mempromosikan ide untuk menutup kesenjangan digital. Jurang yang tidak terlihat ini terbentuk karena perbedaan akses ke kekayaan teknologi informasi dan komunikasi (ICT) antara negara maju dan berkembang.

Akses ke peralatan komunikasi dan informasi telah memperlihatkan akan adanya dampak yang dramatis pada kualitas hidup. Bagi banyak donor, lelah dengan puluhan tahun mendukung kegiatan pembangunan tradisional, instalasi telecentre di negara berkembang tampaknya lebih menjanjikan untuk dapat di capai dan memberikan manfaat. Karena infrastruktur tidak ada, hal ini jauh lebih mahal dan sulit untuk dilakukan di negara berkembang daripada di negara barat. Selain itu, beberapa model telah diperlihatkan bagaimana cara mempertahankan aktifitas ini. Untuk membantu mengurangi beberapa biaya dalam menarik Internet ke pedesaan dari negara maju, tim penulis mempromosikan penggunaan sistem nirkabel untuk berbagi biaya sambungan Internet. Pada bulan November 2004, proyek terkait meminta tim penulis untuk mencoba sistem nirkabel yang baru saja diinstal telecentre di pedesaan Mali, 8 jam kearah tenggara menggunakan kendaraan four-by-four dari ibukota Bamako.

Di kota pedesaan ini, yang terletak pada tepi waduk buatan yang menampung air untuk bendungan Manitali bendungan yang menghasilkan listrik untuk sepertiga dari Mali. Lokasi ini cukup beruntung karena dekat dengan pembangkit listrik tenaga air sehingga listrik lebih stabil dan tidak terlalu perlu mengandalkan generator solar. Memang listrik yang di hasilkan oleh generator solar daya kurang stabil, tapi bagi beberapa komunitas pedesaan cukup beruntung untuk memperoleh listrik darinya. Kota ini diakui merupakan wilayah yang paling subur di negara Mali, merupakan menghasil uang utama di Mali. Kami yakin bahwa tempat ini akan jauh lebih mudah membuat daerah pedesaan lain di Mali untuk dapat membuat telecentre yang mandiri. Seperti banyak percobaan, uji coba dilakukan dengan penuh tantangan. Secara teknologi sangat sederhana. Dalam 24 jam tim telah menginstalasi jaringan nirkabel 802.11b berbagi sambungan Internet VSAT di telecenter dengan 5 layanan lokal lainnya: Walikota, Gubernur, layanan kesehatan, Dewan Walikota Kabupaten (CC) dan layanan penasihat komunitas (CCC).

Klien ini dipilih setelah melalui evaluasi selama dua bulan. Pada masa tersebut tim mewawancarai klien yang potensial dan menentukan klien mana yang dapat di sambungkan tanpa instalasi yang rumit atau mahal. Telecentre sendiri adalah berlokasi di stasiun radio komunitas. Stasiun radio umumnya merupakan tempat yang ideal untuk menempatkan jaringan nirkabel di pedesaan Mali karena sering kali berada di tempat yang baik, memiliki listrik, aman dan orang-orang yang memahami di dasar-dasar radio. Mereka juga merupakan pusat yang netral untuk sebuah desa. Menyediakan internet untuk stasiun radio pada akhirnya akan menyediakan informasi yang lebih baik kepada para pendengarnya. Dan untuk budaya lisan, radio terjadi menjadi media penting untuk memberikan informasi.

Dari daftar klien di atas, anda akan melihat bahwa semua klien yang pemerintah atau semi-pemerintah. Hal ini terbukti merupakan campuran yang sulit, karena ternyata ada cukup banyak dendam dan kebencian antara berbagai tingkat pemerintah, dan sengketa berkelanjutan tentang pajak dan masalah fiskal. Untungnya direktur stasiun radio, pemimpin di jaringan, sangat dinamis dan mampu bekerja keras untuk mengatasi sebagian besar politik ini, meskipun tidak semua.

Pilihan Disain

Tim teknis menentukan peletakan akses point pada ketinggian 20 meter di menara stasiun radio, tepat di bawah antenna dipole radio FM, dan tidak terlalu tinggi agar mengganggu cakupan ke situs klien di lembah bawah seperti mangkuk dimana kebanyakan klien berada. Tim kemudian terfokus pada bagaimana untuk menghubungkan setiap klien ke situs ini. Sebuah antenna omni 8 dBi (dari Hyperlinktech, http://hyperlinktech.com/) akan cukup, menyediakan cakupan untuk semua klien. Antenna 8 dBi dipilih karena memiliki beamwidth vertikal 15 derajat, memastikan bahwa klien kurang dari dua kilometer jauhnya masih dapat menerima sinyal yang kuat. Beberapa antenna mempunyai beam yang sangat sempit sehingga "melampaui" situs yang dekat. Panel antenna diperhatikan, walaupun diperlukan paling tidak dua radio atau menggunakan pemecah / splitter kanal. Hal ini dianggap tidak perlu untuk instalasi ini. Berikut adalah bagaimana menghitung sudut antara antenna klien dan antenna di base station, menggunakan standar trigonometri.

```
tan (x) = perbedaan ketinggian
        + Tinggi stasiun pangkalan antena
        - Ketinggian antena CPE
        / Jarak antara lokasi

tan (x) = 5m + 20m - 3m / 400m
     x  = tan-1 (22m / 400m)
     x  = ~ 3 derajat
```

Selain peralatan di telecentre (4 komputer, sebuah printer laser, 16 port switch), stasiun radio mempunyai sebuah workstation Linux yang diinstal oleh penulis untuk mengedit audio. Sebuah switch kecil di install di stasiun radio, sebuah kabel Ethernet di instalasi melalui pipa plastik yang di tanam 5 cm melintasi telecentre, menyeberangi halaman.

Dari switch utama, dua kabel di larikan ke sebuah akses point Mikrotik RB220. RB220 mempunyai dua buah Ethernet port, satu terhubung ke VSAT melalui kabel cross, dan yang kedua terhubung ke switch pusat dari staiun radio. RB 220 dimasukan ke rumah PCV dari D-I-Y dan sebuah antenna omni 8 dBi (Hiperrangkai Technologies) diletakan langsung di atas tutup PVC.

RB220 menjalankan turunan dari Linux, Mikrotik versi 2.8.27. RB220 mengendalikan jaringan, menyediakan DHCP, firewall, dan layanan cache DNS, sambil merouting trafik ke VSAT melalui NAT. Di Mikrotik tersedia fasilitas perintah menggunakan command line maupun fasilitas antarmuka grafis yang ramah. RB220 sebuah komputer kecil berbasis x86, yang dirancang untuk digunakan sebagai akses point atau embedded komputer. Akses point ini mampu untuk PoE, memiliki dua buah port Ethernet, sebuah port mini-pci, dua slot PCMCIA,

sebuah pembaca CF (yang digunakan untuk NVRAM), mentolerasi suhu yang besar dan mendukung berbagai sistem operasi x86. Meskipun Mikrotik bahwa perangkat lunak memerlukan lisensi, sudah ada basis pengguna yang besar di Mali. Karena sistem memiliki antarmuka grafis yang handal dan ramah menjadikannya lebih unggul dari produk lainnya. Karena faktor di atas tim sepakat untuk menggunakan sistem ini, termasuk software Mikrotik untuk mengontrol jaringan. Total biaya dari RB220, dengan Lisensi Tingkat 5,
Atheros mini-pci a/b/g dan POE adalah $461. Anda dapat menemukan komponen ini di Mikrotik online di *http://www.mikrotik.com/routers.php#linx1part0.*

Jaringan ini dirancang untuk mengakomodasi perluasan dengan cara memisahkan berbagai sub-jaringan dari setiap klien; private subnet 24 bit digunakan. AP mempunyai antarmuka virtual pada setiap subnet dan melakukan routing antara subnet, juga firewall di lapisan IP. Perlu di catat: ini tidak menyediakan firewall di lapisan jaringan, sehingga, menggunakan sniffer jaringan seperti tcpdump seseorang dapat melihat semua lalu lintas paket yang lewat di sambungan wireless.

Untuk membatasi akses ke pelanggan, jaringan menggunakan akses kontrol tingkat MAC. Ada sedikit menimbulkan risiko keamanan untuk jaringan. Untuk tahap pertama ini, sistem keamanan yang lebih teliti akan di bangun di masa mendatang, ketika ada antarmuka yang lebih mudah untuk mengendalikan akses. Pengguna di sarankan untuk menggunakan protokol yang aman, seperti https, pops, imaps dll.

Proyek afiliasi telah menginstal sistem VSAT C-band (DVB-S). Sistem satelit ini biasanya sangat handal dan sering digunakan oleh ISP. Ini merupakan unit besar yang mempunyai besar piringan parabola antenna ber-diameter 2,2 meter dan mahal, biaya sekitar $ 12.000 termasuk instalasi. Selain itu juga mahal untuk di operasikan. Sebuah sambungan Internet dengan 128 kbps down dan 64 kbps up berharga sekitar $700 per bulan. Sistem ini memiliki beberapa keunggulan dibandingkan sistem Ku, termasuk: lebih tahan cuaca buruk, lebih rendah persaingan harga (persaingan jumlah pengguna pada layanan yang sama) dan transfer data yang lebih effisien.

Instalasi VSAT ini tidak ideal. Karena sistem menjalankan Windows, pengguna dapat dengan cepat mengubah beberapa konfigurasi, termasuk menambahkan password untuk account default. Sistem tidak mempunyai UPS atau batere cadangan, sehingga jika listrik mati maka sistem akan reboot dan diam menunggu seseorang untuk memasukan password, yang mungkin sudah di lupakan orang. Untuk membuat situasi ini lebih buruk lagi, karena software VSAT tidak dikonfigurasi untuk beroperasi sebagai layanan di latar belakang maka software VSAT tidak secara automatis beroperasi dan membuat sambungan. Walaupun sistem C-band biasanya dapat diandalkan, instalasi ini menyebabkan putusnya sambungan yang sebetulnya tidak perlu yang sebetulnya dapat di atasi dengan penggunaan UPS, konfigurasi yang tepat dari software VSAT sebagai layanan di belakang layar, dan dengan membatasi akses fisik ke modem. Seperti semua pemilik peralatan yang baru, stasiun radio ingin menampilkan peralatan VSAT-nya, maka peralatan ini sebaiknya di tampilkan jangan di sembunyikan. Tapi dengan sebuah ruang kaca akan menyimpan unit ini dengan aman walaupun dapat dilihat orang.

Sistem wireless cukup sederhana. Semua situs klien yang dipilih berada dalam radius 2 km dari stasiun radio. Setiap situs yang mempunyai bagian bangunan secara fisik dapat melihat stasiun radio. Di situs klien, tim memilih untuk menggunakan CPE klien kelas komersial; berdasarkan harga, Powernoc 802.11b CPE bridge, antenna SuperPass 7 dBi patch kecil dengan adaptor Pover Over Ethernet (PoE) buatan sendiri. Untuk memudahkan instalasi, CPE dan antenna patch di pasang pada sepotong kayu pendek yang dapat di instalasi di dinding bangunan yang menghadap ke stasiun radio.

Dalam beberapa kasus, potongan kayu dibuat menyudut untuk mengoptimalkan posisi antena. Di dalam, POE yang dibuat dari booster televisi (12V) yang di modifikasi digunakan sebagai power supply. Pada situs client biasanya tidak ada jaringan LAN lokal, oleh karenanya tim harus menginstalasi kabel dan hub untuk memberikan akses Internet ke setiap komputer. Dalam banyak kasus perlu di instalasi Ethernet card dan driver-nya (hal ini tidak terpikirkan pada saat assesment). Tim memutuskan, karena jaringan klien yang sederhana, akan lebih mudah untuk membuat bridge dari jaringan mereka. Jika diperlukan, arsitektur IP memungkinkan partisi lebih lanjut dimasa depan dan peralatan CPE didukung mode STA. Kami menggunakan PowerNOC CPE bridge yang biaya $ 249.

Staf lokal terlibat selama instalasi jaringan nirkabel. Mereka belajar semuamya mulai dari perkabelan sampai penempatan antena. Pelatihan intensif dilakukan setelah instalasi. Hal ini berlangsung beberapa minggu, dan dimaksudkan untuk mengajar staf tugas sehari-hari, serta dasar cara mengatasi permasalahan jaringan.

Seorang anak muda yang baru lulusan universitas yang kembali ke komunitas telah di pilih untuk menjadi support system, kecuali untuk instalasi kabel, karena teknisi stasiun radio cukup cepat mempelajarinya. Perkabelan jaringan Ethernet sangat mirip dengan perbaikan dan instalasi kabel coax yang biasa dilakukan oleh teknisi radio sehari-hari. Para pemuda yang baru lulus juga membutuhkan sedikit pelatihan. Tim memberikan banyak waktu untuk membantu dia mempelajari bagaimana untuk mendukung sistem dasar dan telecentre. Segera setelah telecentre dibuka, murid mengantri untuk pelatihan komputer, yang ditawarkan 20 jam pelatihan dan penggunaan Internet per bulan hanya $40, sangat murah dibandingkan dengan $2 per jam untuk akses Internet. Memberikan pelatihan ini membuka kesempatan memperoleh pemasukan dan sangat cocok bagi anak muda yang baru lulus dan mengerti komputer ini.

Sayangnya, dan sedikit mengagetkan, muda yang baru lulus tersebut meninggalkan semuanya untuk bekerja di ibu kota Bamako, setelah menerima tawaran pekerjaan dari pemerintah. Ini menyebabkan telecentre menjadi sengsara. Anggota mereka yang paling mengerti teknis, dan satu-satunya yang terlatih dalam cara untuk mendukung sistem, telah kiri. Sebagian besar pengetahuan yang diperlukan untuk mengoperasikan jaringan telecentre juga hilang bersamanya. Setelah melalui banyak pertimbangan, tim akhirnya memutuskan, untuk tidak melatih pemuda lain, tetapi akan fokus pada staf lokal, walaupun mereka mempunyai pengalaman teknis yang terbatas. Memang ini akan membutuhkan jauh lebih banyak waktu. Para trainer harus meluangkan total 150 jam pelatihan. Beberapa orang

diajarkan setiap fungsi, dan tugas untuk men-support telecentre dibagi di kalangan staf.

Pelatihan tidak berhenti disana. Setelah layanan masyarakat tersambung, ternyata masyarakat juga membutuhkan akses. Tampaknya meskipun masyarakat berpartisipasi, para petinggi, termasuk walikota, tidak menggunakan sistem itu sendiri. Tim menyadari pentingnya memastikan pengambil keputusan menggunakan sistem, dan memberikan pelatihan bagi mereka dan staf mereka. Hal ini berhasil menghilangkan beberapa mistik dari jaringan dan berhasil mengajak pengambil keputusan di kota untuk terlibat. Setelah pelatihan, program memonitor situs dan mulai memberikan masukan, mengevaluasi kemungkinan meningkatkan model ini. Pelajaran di sini telah diterapkan ke tempat-tempat lainnya.

Model Keuangan

Komunitas telecentre telah ditetapkan sebagai nirlaba, dan memperoleh amanat untuk menopang diri sendiri melalui penjualan layanannya. Sistem wireless dimasukan sebagai tambahan sumber pendapatan karena proyeksi keuangan awal dari telecentre menunjukan bahwa mereka tidak akan mampu untuk membayar sambungan VSAT.

Berdasarkan survei, dan konsultasi dengan stasiun radio yang mengelola telecentre, beberapa klien dipilih. Stasiun radio merundingkan beberapa kontrak dengan mitra penyandang dana. Untuk tahap pertama ini, klien dipilih berdasarkan kemudahan instalasi dan pernyataan kemampuan untuk membayar. Klien diminta untuk membayar biaya berlangganan, seperti yang dijelaskan berikut ini.

Menentukan berapa besar biaya langganan merupakan kegiatan besar yang membutuhkan konsultasi dan keahlian yang komunitas tidak memilikinya terutama dalam proyeksi keuangan. Peralatan dibayar oleh hibah, untuk membantu meringankan biaya masyarakat, tetapi klien masih diminta untuk membayar biaya berlangganan, untuk menjamin komitmen mereka. Hal ini setara dengan satu bulan dari biaya layanan. Untuk menentukan biaya langganan bulanan untuk bandwidth tertentu kami mulai dengan rumus sebagai berikut:

```
VSAT + gaji + biaya (listrik, alat tulis) =
pendapatan telecentre + pendapatan klien wireless
```

Kami telah diperkirakan bahwa telecentre harus memperoleh pendapatan $200 sampai $300 per bulan. Total pengeluaran diperkirakan $ 1.050 per bulan, yang terdiri dari: $700 untuk VSAT, $100 untuk gaji, $150 untuk listrik, dan sekitar $100 untuk alat tulis. Sekitar $750 pendapatan dari klien nirkabel diperlukan untuk menyeimbangkan persamaan ini. Jadi sekitar sekitar $150 dari setiap klien. Hal ini cukup lumayan bagi klien, dan tampaknya layak, tetapi diperlukan suasana yang baik, dan tidak ada ruang untuk komplikasi.

Karena ini telah menjadi rumit, kami memasukan teknik bisnis para geeks, yang memodifikasi formula seperti:

```
Biaya bulanan + amortisasi + dana cadangan = total pendapatan
```

Para ahli bisnis akan langsung menunjukkan kebutuhan akan amortisasi peralatan, atau "dana re-investasi" serta dana cadangan, untuk memastikan bahwa jaringan dapat melanjutkan jika client menunggak, atau jika beberapa peralatan rusak. Ini menambahkan sekitar $ 150 per bulan untuk amortisasi (peralatan bernilai sekitar $ 3000, amortisasi lebih dari 24 bulan) dan nilai sebuah klien untuk pembayaran standar, di $100. Tambahan 10% untuk devaluasi mata uang devaluasi ($80), yang sama dengan pengeluaran $1380 per bulan. Dalam mencoba untuk melaksanakan model ini, akhirnya diputuskan bahwa konsep amortisasi terlalu sulit untuk menyampaikan kepada masyarakat, dan bahwa mereka tidak mempertimbangkan klien yang menunggak pembayaran. Dengan demikian, kedua rumus digunakan, pertama oleh telecentre dan kedua untuk analisis internal kami.

Segera diketahui, pembayaran secara teratur bukan merupakan bagian dari budaya di pedesaan Mali. Dalam sebuah masyarakat agraris semuanya adalah musiman, dan termasuk pendapatan. Ini berarti bahwa pendapatan masyarakat berfluktuasi sangat lebar. Selain itu, banyak lembaga publik yang terlibat, mereka mempunyai siklus anggaran yang lama dan tidak fleksibel. Meskipun secara teoritis mereka mempunyai anggaran untuk membayar layanan mereka, diperlukan waktu beberapa bulan untuk melakukan pembayaran yang sebenarnya. Kesulitan keuangan juga timbul. Misalnya, walikota menanda tangani dan menggunakan “back tax” dari radio untuk membayar biaya langgannya. Hal ini tentu saja tidak memberikan kontribusi untuk cash flow telecentre. Sayangnya, penyedia layanan VSAT tidak memiliki fleksibelitas maupun kesabaran, karena mereka mempunyai bandwidth terbatas dan hanya ada ruang bagi mereka yang dapat membayar.

Manajemen cash flow menjadi perhatian utama. Pertama, pendapatan yang di perlihatkan pada proyeksi keuangan menunjukkan bahwa walaupun optimis, mereka mengalami kesulitan mendapatkan penghasilan pada waktu cukup untuk membayar biaya tepat waktu, bahkan mendapatkan uang dari bank di Bamako juga sulit. Jalan dekat desa dapat sangat berbahaya, karena banyaknya penyelundup dari Guinea dan pemberontak dari Pantai Gading. Seperti yang diproyeksikan, telecentre yang tidak mampu membayar untuk layanannya dan layanan ini akhirnya ditangguhkan, sehingga menangguhkan pembayaran dari pelanggan mereka juga.

Sebelum proyek ini dapat menemukan solusi dari permasalahan tersebut, biaya VSAT sudah mulai membuat hutang bagi telecentre. Setelah beberapa bulan, karena masalah teknis, serta keprihatinan dalam analisis di atas, VSAT C-band yang besar diganti sistem Ku band yang lebih murah. Meskipun lebih murah, cukup untuk membuat sebuah jaringan. Sistem ini hanya $450, dengan mengabaikan perlunya keselamatan dan amortisasi, cukup terjangkau untuk jaringan. Sayangnya, karena penunggakan pembayaran, jaringan tidak dapat membayar untuk sambungan VSAT setelah perioda awal yang di subsidi.

Kesimpulan

Membangun jaringan nirkabel relatif mudah, tetapi menjadikannya bekerja lebih merupakan masalah bisnis daripada masalah teknis. Model pembayaran yang memasukan re-investasi dan resiko sangat penting, atau jaringan akan gagal. Dalam hal ini, model pembayaran tersebut tidak sesuai karena tidak memenuhi siklus keuangan dari klien, maupun tidak memenuhi harapan sosial. Analisis risiko akan memperlihatkan bahwa pembayaran bulanan $700 (atau bahkan $450) menyediakan margin terlalu sempit antara pendapatan dan pengeluaran untuk kompensasi kekurangan keuangan. Kebutuhan hidup yang tinggi dan kebutuhan pendidikan membatasi pengembangan jaringan.

Setelah pelatihan, jaringan beroperasi selama 8 bulan tanpa masalah teknis yang berarti. Kemudian, kerusakan listrik karena serangan petir menghancurkan banyak peralatan di stasiun, termasuk akses point dan VSAT. Akibatnya, telecentre masih off-line yang pada saat buku ini ditulis. Pada saat itu rumus ini akhirnya dianggap sebagai solusi tidak sesuai.

-- Ian Howard

Studi kasus: Implementasi Komersial di Afrika Timur

Menjelaskan implementasi komersial jaringan nirkabel di Tanzania dan Kenya, bab ini menggaris bawahi solusi teknis yang memberikan 99,5% ketersediaan sambungan Internet dan data yang solid di negara berkembang. Berbeda dengan proyek-proyek yang dikhususkan untuk akses di mana-mana, kami berfokus pada memberikan pelayanan kepada organisasi, biasanya yang kritis dengan kebutuhan komunikasi internasional. Saya akan menjelaskan dua pendekatan komersial yang radikal untuk sambungan nirkabel, merangkum pelajaran lebih dari sepuluh tahun di Afrika Timur.

Tanzania

Pada tahun 1995, dengan Bill Sangiwa, saya mendirikan CyberTwiga, salah satu ISP pertama di Afrika. Layanan komersial, terbatas untuk lalu lintas e-mail dialup yang dijalankan melalui sambungan SITA 9,6 kbps (biaya lebih dari $4000/bulan!), yang dimulai pada pertengahan 1996. Kecewa dengan layanan PSTN yang tidak baik, dan terbuai oleh implementasi yang sukses dari jaringan 3-node point-multipoint (PMP) untuk Authoritas Pelabuhan Tanzania, kami melakukan negosiasi dengan perusahaan selular lokal untuk menempatkan base stasion PMP di tower pusat mereka. Menyambungkan segelintir perusahaan menggunakan sistem WiLan di 2,4 GHz pada akhir tahun 1998, kami memvalidasi pasar dan kemampuan teknis kami untuk menyediakan layanan nirkabel.

Para pesaing semena-mena menggelar jaringan 2,4 GHz, dua fakta muncul: ada pasar yang sehat untuk layanan nirkabel, tetapi kenaikan noise RF di 2,4 GHz menjadikan kualitas

jaringan berkurang. Merger kami dengan operator selular, pada pertengahan tahun 2000, termasuk rencana untuk membangun jaringan nirkabel nasional pada infrastruktur selular yang ada (menara dan sambungan transmisi) dan menggunaan alokasi spektrum RF proprietary.

Prasarana telah ada (menara selular, saluran transmisi, dll) sehingga disain jaringan data nirkabel maupun implementasinya menjadi mudah. Dar es Salaam sangat datar, dan karena mitra operator selular mengoperasikan jaringan analog, menara yang ada sangat tinggi. Sebuah perusahaan sejenis di Inggris, Tele2, telah mulai beroperasi dengan Breezecom (sekarang Alvarion) peralatan di 3.8/3.9 GHz, sehingga kami diikuti kepemimpinan mereka.

Dengan akhir 2000, kami telah cakupan di beberapa kota, menggunakan sirkuit transmisi dengan kapasitas sebagian E1 untuk backhaul. Dalam banyak kasus sebuah kota berukuran kecil cukup untuk sebuah base station dengan PMP omnidirectional; hanya di ibu kota komersial, Dar es Salaam, diinstalasi base station 3-sektor. Pembatas bandwidth dikonfigurasi langsung pada radio pelanggan; klien biasanya di berikan sebuah alamat IP publik. Router ujung di setiap base stasiun mengirim trafik ke alamat IP statis di lokasi klien, dan mencegah trafik broadcast yang akan mencekik trafik jaringan. Pasar menekan agar harga menjadi rendah ke sekitar $100/bulan untuk 64 kbps, tetapi pada waktu itu (pertengahan / akhir 2000) ISP dapat beroperasi dengan mengesankan, sangat menguntungkan, dengan rasio pertarungan yang ada.

Aplikasi lapar bandwidth seperti file sharing peer-to-peer, suara, dan ERP sama sekali tidak ada di Afrika Timur. Tingginya biaya PSTN internasional, membuat organisasi cepat berpindah dari fax ke trafik email, walaupun mereka membeli peralatan nirkabel biaya berkisar dari $2000-3000.

Kemampuan teknis dikembangkan di lokasi, membutuhkan pelatihan staf ke luar negeri dalam mata pelajaran seperti SNMP dan UNIX. Selain meningkatkan kemampuan perusahaan, kesempatan pelatihan meningkatkan loyalitas staf. Kami harus bersaing dalam pasar tenaga kerja TI yang sangat terbatas dengan perusahaan pertambangan emas internasional, PBB, dan lembaga internasional lainnya.

Untuk memastikan kualitas lokasi pelanggan, sebuah stasiun radio lokal dan kontraktor telekomunikasi terbaik di kontrak untuk melaksanakan instalasi, kemajuan di perhatikan secara ketat menggunakan kartu pekerjaan. Temperatur yang tinggi, sinar matahari khatulistiwa yang keras, hujan lebat, dan petir adalah sebagian dari serangan dari lingkungan yang akan membuat gosong peralatan di luar ruangan; integritas kabel RF adalah penting.

Pelanggan sering kekurangan staf TI yang kompeten, membebani karyawan kami dengan tugas mengkonfigurasi banyak hardware dan topologi jaringan. Infrastruktur dan kendala peraturan sering menyulitkan operasional. Kontrol menara perusahaan selular yang sangat ketat, sehingga jika ada masalah teknis di base station butuh berjam-jam atau berhari-hari sebelum kami bisa masuk. Meskipun ada cadangan generator dan sistem UPS di setiap lokasi, listrik selalu bermasalah. Untuk perusahaan selular, pasokan listrik utama di base

station tidak kritis. Bagi pelanggan seluler cukup mengkaitkan diri ke base station yang berbeda; sayangnya bagi pelanggan nirkabel data mau tidak mau harus putus sambungan / offline.

Di sisi peraturan, kekacauan terbesar terjadi saat authoritas telekom memutuskan bahwa jaringan kami yang bertanggung jawab kepada gangguan pada operasi satelit C-band untuk seluruh negara dan memerintahkan untuk mematikan jaringan kami.

Meskipun bukti menunjukkan bahwa kami tidak bersalah, regulator melakukan penyitaan peralatan kami dan dipublikasikan secara besar-besaran. Tentu saja gangguan tetap berlangsung, kemudian hari di temukan bahwa interferensi terjadi dari radar kapal rusia, yang terlibat dalam aktifitas pelacakan udara. Kami melakukan negosiasi secara diam-diam dengan regulator, dan akhirnya diberikan 2 x 42 MHz spektrum di band 3.4/3.5 GHz. Pelanggan perlu beralih ke dialup selama satu bulan lebih saat kami mengkonfigurasi ulang base station dan menginstalasi CPE baru.

Pada akhirnya jaringan tumbuh melayani sambungan bagi 100 node, meskipun tidak besar, menyambungkan 7 kota dengan sambungan lebih dari 3.000 km. Hanya dengan cara merger dengan operator seluler yang dibuat jaringann ini menjadi mungkin – untuk skala Internet / bisnis data tidak memungkinkan untuk menjustifikasi pembuatan jaringan data pada ukuran besar dan membuat investasi yang diperlukan untuk frekuensi proprietary. Sayangnya, operator selular mengambil keputusan untuk menutup bisnis internet di pertengahan 2002.

Nairobi

Pada awal 2003, saya di dekati oleh perusahaan Kenya, AccessKenya, dengan dukungan bisnis dan teknik dari Inggris yang kuat untuk mendisain dan menyebarkan sebuah jaringan nirkabel di Nairobi dan sekitarnya. Dengan nilai tambah sebagai profesional jaringan dan bisnis yang baik, perbaikan perangkat keras nirkabel, kemajuan di teknologi internet, dan pasar yang lebih besar kami merancang jaringan dengan ketersediaan tinggi sejalan dengan batasan peraturan.

Dua peraturan yang mendasari disain jaringan kami. Pada saat itu di Kenya, layanan Internet memperoleh lisensi yang berbeda dari operator jaringan public data, dan sebuah perusahaan tidak dapat mempunyai kedua lisensi sekaligus. Membawa trafik dari beberapa jaringan, baik ISP pesaing atau perusahaan pengguna, membuat jaringan beroperasi secara netral. Selain itu, frekuensi proprietary, yaitu 3.4/3.5 GHz, tidak secara eksklusif diberikan lisensi untuk satu operator, dan kami khawatir akan gangguan interferensi dan kemampuan teknis / political will dari regulator untuk melakukan penegakkan. Selain itu, spektrum 3.4/3.5 GHz adalah mahal, biaya sekitar USD1000 per MHz per tahun per base station. Oleh karenanya, sebuah base station menggunakan 2 x 12 MHz akan di tarik biaya lisensi lebih dari $10.000 per tahun. Karena Nairobi merupakan tempat yang berbukit-bukit dengan banyak pohon tinggi mauoun lembah, jaringan broadband nirkabel memerlukan banyak base station. Overhead perizinan

sangat tidak masuk akal. Sebaliknya, frekuensi 5.7/5.8 GHz hanya membutuhkan membayar ongkos tahunan sekitar USD 120 per radio yang di gelar.

Untuk memenuhi persyaratan peraturan pertama kami memilih untuk memberikan layanan menggunakan jalur-jalur VPN Tunnel, tidak melalui rute jaringan IP statis. Sebuah ISP akan memberikan sebuah alamat IP publik untuk jaringan kami di NOC mereka. Jaringan kami melakukan konversi IP publik ke IP private, dan trafik transit ke jaringan kami yang menggunakan IP private. Di lokasi pelanggan, konversi IP private ke IP publik dilakukan lagi untuk memberikan alamat IP yang dapat di routing secra global di jaringan pelanggan.

Keamanan dan enkripsi ditambahkan untuk menambahkan netralitas jaringan, dan fleksibilitas, sebagai cara penjualan yang unik dari jaringan kami. Bandwidth dibatasi di tingkat VPN tunnel. Berdasarkan pengalaman operasi saudara perusahaan Inggris, VirtualIT, kami dipilih Netscreen (sekarang berada di bawah Juniper Networks) sebagai vendor untuk VPN firewall router.

Kami kriteria untuk peralatan broadband nirkabel menghapuskan pipa besar dan kaya-fitur, lebih kepada peralatan berkinerja tinggi. Faktor bentuk, keandalan, dan kemudahan instalasi dan manajemen yang lebih penting daripada throughput. Semua sambungan Internet internasional ke Kenya pada tahun 2003, dan saat tulisan ini ditulis, dibawa oleh satelit. Dengan biaya 100X lebih besar dari serat optik global, sambungan satelit menset plafon keuangan pada jumlah bandwidth dapat dibeli oleh user. Kami menilai bahwa sebagian besar populasipengguna akan membutuhkan kapasitas sekitar 128 sampai 256 kbps. Kami dipilih platform Canopy yang baru-baru ini diperkenalkan oleh Motorola baru-baru ini dengan model bisnis dan model jaringan.

Perusahaan Broadband Access mulai hidup pada bulan July 2003, meluncurkan jaringan “Blue”. Kami mulai kecil, dengan sebuah base station. Kami ingin mendorong expansi jaringan kami, daripada menggunakan strategi membangun pipa besar dan berhadap agar kami dapat mengisinya.

Canopy, dan pengembangan perangkat pihak ketiga seperti base station omnidirectional, mengijinkan jaringan kami untuk tumbuh sebagaimana pertumbuhan trafik, hal ini memperingan pengeluaran modal awal. Kami tahu bahwa ada kesulitan perluasan jaringan, kami akan harus membuat sektor pada jaringan dan mengarahkan ulang radio klien. Kurva belajar yang perlahan dari sebuah jaringan kecil akan memberikan keuntungan yang besar di kemudian hari. Staf teknis menjadi nyaman untuk mensupport pelanggan dalam lingkungan jaringan yang sederhana, daripada harus berurusan dengan mereka di atas sebuah jaringan RF dengan keranga logis yang kompleks. Staf teknis mengikuti sesi training Motorola selama dua hari.

Sebuah desain khas PMP, dengan base station terhubung ke pusat melalui microwave backbone Canopy berkecepatan tinggi, jaringan digelar di atap bangunan, tidak pada menara. Semua sewa memungkinkan akses 24x7 untuk staf, listrik dan yang penting perlindungan eksklusif bagi frekuensi radio kami.

Kami tidak ingin membatasi pemilik untuk memberikan ruang di atap untuk kompetitor, kami hanya ingin memperoleh jaminan bahwa layanan kami tidak akan terputus. Instalasi di atap memberikan banyak keuntungan. Akses fisik tanpa batas, tidak di halangi oleh malam atau hujan, membantu memenuhi target dari 99,5% ketersediaan jaringan. Bangunan besar biasanya merupakan tempat tinggal banyak klien besar, dan memungkinkan untuk menghubungkan mereka langsung ke jaringan microwave utama kami. Lokasi atap juga memiliki kelemahan karena lebih banyak lalu lintas manusia - pekerja pemeliharaan peralatan (a/c) atau penambal kebocoran kadang-kadang merusak kabel. Akibatnya semua base station dibuat dengan dua set kabel jaringan untuk semua unsur jaringan, sebuah yang utama dan sebuah cadangan.

Site survey mengkonfirmasi ketersediakan jalur radio dan persyaratan klien. Survei staf akan mencatat posisi GPS untuk setiap klien, dan membawa range-finder laser untuk untuk menentukan ketinggian halangan. Setelah menerima pembayaran untuk hardware, kontraktor di bawah pengawasan staf teknis melakukan instalasi. Canopy memiliki keuntungan yaitu CPE dan base station yang ringan, sehingga kebanyakan instalasi tidak memerlukan pekerjaan sipil atau perkabelan. Perkabelan Canopy juga sederhana, dengan menyambungkan langsung UTP outdoor di radio ke jaringan pelanggan. Perencanaan yang baik memungkinkan penyelesaian banyak instalasi dalam waktu kurang dari satu jam, petugas kontraktor juga tidak perlu pelatihan maupun peralatan yang rumit.

Setelah kami mengumpulkan ratusan posisi GPS pelanggan kami mulai bekerja sama dengan perusahaan survey lokal untuk untuk melihat lokasi di atas peta topografi. Hal ini menjadi alat utama untuk perencanaan penempatan base station. Ingat bahwa kita menggunakan arsitektur VPN tunnel point-to-point, karena keterpisahan jaringan fisik maupun logik, klien perlu membeli sekaligus peralatan broadband nirkabel dan VPN hardware. Untuk mengontrol kualitas, kami menolak mengizinkan klien untuk menyediakan sendiri hardware - mereka harus membeli dari kami untuk memiliki jaminan kelayanan dan perangkat keras. Setiap klien mempunyai paket hardware yang sama. Biaya instalasi rata-rata sekitar USD 2500, bandingkan dengan tagihan $500-600 per bulan untuk bandwidth 64-128 kbps.

Sebuah keuntungan dari pendekatan VPN tunnel, kami dapat mencegah lalu lintas klien untuk menyeberangi jaringan logik (yaitu jika mereka jaringan mendapat serangan worm atau jika mereka tidak membayar tagihan) sementara lapisan radio tetap utuh dan terkendali.

Semasa dia tumbuh dari satu base station menjadi sepuluh, dan layanan diperluas ke Mombasa, disain jaringan RF berkembang dan sedapat mungkin elemen jaringan (router) dikonfigurasi dengan fallover atau redudansi hot swap. Investasi utama adalah di inverter dan peralatan dual konversi UPS di setiap base station yang diperlukan untuk menjaga kestabilan jaringan yang harus berhadapan dengan listrik yang sangat tidak stabil. Setelah jumlah pelanggan komplain (karena putusnya sambungan VPN) karena putusnya listrik, kami menambahkan UPS kecil sebagai bagian dari paket peralatan.

Menambahkan portabel spektrum analizer untuk modal awal kami adalah investasi yang

mahal, tetapi kami sangatlah mendukung karena kami mengoperasikan jaringan. Penelusuri operator yang tidak baik, membenarkan karakteristik operasi peralatan, dan memverifikasi cakupan RF meningkatkan kinerja kami.

Perhatian untuk memonitor secara terus menerus memungkinkan kami untuk mentuning kinerja jaringan, dan mengumpulkan data historis. Penggambaran grafis melalui MRTG atau Cacti (seperti yang dijelaskan dalam bab enam), parameter seperti jitter, RSSI, dan peringatan traffik akan adanya operator yang nakal, potensi kerusakan kabel / konektor, dan keberadaan worm pada jaringan klien. Tidak jarang klien mengklaim bahwa layanan ke lokasi mereka telah terputus untuk beberapa jam / hari meminta penggantian / kredit. Pemantauan historis memperlihatkan dan membatalkan klaim tersebut. Jaringan Blue menggabungan sejumlah pelajaran dari Tanzania dengan peningkatan teknologi RF dan jaringan.

Pelajaran Yang Diperoleh

Untuk beberapa tahun ke depan sirkuit satelit akan menyediakan semua sambungann Internet internasional di Afrika Timur. Beberapa kelompok telah menyodorkan proposal untuk sambungan serat optik bawah laut, yang akan memberikan semangat pada dunia telekomunikasi bila itu terjadi. Dibandingkan dengan daerah yang mempunyai sambungan serat optik, biaya bandwidth di Afrika Timur akan tetap sangat tinggi.

Jaringan broadband nirkabel untuk pemberian layanan Internet sehingga tidak perlu fokus pada throughput. Sebaliknya, penekanan harus ditempatkan pada kehandalan, redudansi, dan fleksibilitas. Kehandalan untuk jaringan nirkabel kami merupakan selling point utama. Pada sisi jaringan ini diterjemahkan pada investasi infrastruktur substitution yang cukup besar, seperti cadangan daya, dan perhatian ke detil kecil seperti crimping dan kabel yang baik. Alasan yang paling sering dari pelanggan yang putus sambungannya adalah masalah perkabelan dan crimping. Kegagalan radio hampir tidak pernah terdengar.

Kunci keuntungan kompetitif dari proses instalasi pelanggan adalah kami mendorong kontraktor untuk mematuhi spesifikasi yang ketat. Oleh karena sangat biasa pada sebuah lokasi customer yang di managed dengan baik untuk tetap tersambung selama ratusan hari dengan nol unscheduled downtime. Kami mengontrol sebagai besar infrastruktur kami (yaitu atap bangunan).

Walaupun sangat menarik kemungkin beraliansi dengan provider selular, pengalaman kami menunjukan lebih banyak masalah daripada memecahkan masalah. Di Afrika Timur, Internet bisnis menghasilkan pendapatan yang jauh lebih kecil dari telepon mobil, dan sangat tidak terasa bagi sebuah perusahaan selular. Mencoba untuk menjalankan di atas jaringan infrastruktur yang bukan milik anda, yang dari sudut pandang penyedia selular, hanya merupakan sikap baik saja, akan membuat tidak mungkin untuk memenuhi komitmen layanan.

Mengimplementasi sepenuhnya jaringan yang redundan, dengan fail-over dan hotswap

adalah proposisi yang mahal di Afrika. Namun demikian router inti dan hardware VPN kami di titik Point of Precence sepenuhnya redundan, dikonfigurasi untuk fail-over, dan diuji secara rutin. Untuk base stasion kami mengambil keputusan untuk tidak menginstal dual router, tapi menyimpan router dalam stok. Kami memutuskan bahwa downtime 2-3 jam adalah yang terburuk (sebuah kegagalan pada jam 1 dini hari di hari Minggu dalam keadaan hujan) akan diterima untuk klien.

Demikian anggota staf untuk akhir pekan mempunyai akses untuk keadaan darurat pada lemari berisi cadangan peralatan untuk di lokasi pelanggan, seperti radio dan power supply. Fleksibilitas direkayasa ke dalam disain jaringan logis dan RF. Arsitektur VPN tunnel point-to-point yang di gelar di Nairobi sangat luar biasa fleksibel dalam memberikan layanan bagi klien maupun kebutuhan jaringan. Sambungan klien dapat diset untuk memanfatkan maksimal pada jam tidak sibuk untuk mengaktifkan backup di offsite, sebagai satu contoh. Kami juga dapat menjual beberapa sambungan untuk tujuan yang berbeda, untuk meningkatkan laba atas investasi atas jaringan kami sambil membuka layanan baru (seperti pemantauan kamera CCTV) untuk klien.

Di samping sisi RF kami sudah memiliki spektrum yang cukup untuk perencanaan perluasan, serta mempersiapkan alternatif desain jaringan radio jika ada gangguan. Dengan meningkatnya jumlah base station, mungkin 80% dari pelanggan kami mempunyai kemungkinan untuk tersambung ke dua base station yang line of sight sehingga juga sebuah base station rusak kita dapat memulihkan pelayanan dengan cepat.

Pemisahan lapisan logis dan RF pada jaringan Blue menyebabkan tambahan tingkat kompleksitas dan biaya. Mempertimbangkan kenyataan jangka panjang bahwa teknologi radio akan naik lebih cepat dibandingkan teknik Internetwork. Pemisahan jaringan, secara teori, memberikan kami fleksibilitas untuk menggantikan jaringan RF yang ada tanpa membuat risak jaringan logik. Atau kita boleh memasang jaringan radio yang berbeda sejalan dengan perkembangan teknologi (Wimax) atau kebutuhan klien, sambil mempertahankan jaringan logis.

Akhirnya, kita harus menyerah pada sebuah titik yang sangat jelas bahwa jaringan yang kami gelar akan tidak berguna tanpa komitmen untuk layanan pelanggan. Sesudah semua yang kami lakukan.

Informasi lebih lanjut

- Akses Broadband, Ltd: *http://www.blue.co.ke/*
- AccessKenya, Ltd: *http://www.accesskenya.com/*
- VirtualIT: *http://www.virtualit.biz/*

-- Adam Messer, Ph.D

Studi kasus: Komunitas Dharamsala Jaringan Wireless Mesh

Jaringan Wireless Mesh Komunitas Dharamsala mulai hidup di Februari 2005, mengikuti deregulasi WiFi untuk penggunaan di luar ruangan di India. Pada akhir Februari 2005, jaringan mesh telah menghubungkan delapan (8) kampus. Ujicoba secara mendalam dilakukan selama bulan Februari 2005 menunjukkan bahwa wilayah bergunung-gunung sangat cocok untuk jaringan mesh, karena jaringan konvensional point-to-multipoint, tidak dapat mengatasi keterbatasan line-of-sight yang ada pada wilayah yang bergunung-gunung. Topologi mesh juga menawarkan wilayah cakupan yang lebih besar, dengan kemampuan "penyembuhan sendiri" dari routing mesh secara alamiah, terbukti menjadi penting pada tempat dimana pasokan listrik sangat tidak menentu.

Tulang punggung mesh mencakup lebih dari 30 node, semua berbagi pada satu kanal radio. Sambungan Internet broadband diberikan pada semua anggota mesh. Total bandwidth ke Internet yang tersedia adalah 6 Mbps. Terdapat lebih dari 2000 komputer terhubung ke mesh, sambungan internet broadband membuat beban mesh sangat besar. Saat ini, tampaknya sistem dapat menangani beban tanpa peningkatan latensi atau packet-loss. Jelas skalabilitas / pengembangan akan menjadi masalah jika kita terus menggunakan satu saluran radio. Untuk memecahkan masalah ini, router mesh baru dengan dukungan beberapa saluran radio sedang dikembangkan dan diuji di Dharamsala, dengan penekanan pada produk yang memenuhi persyaratan baik teknis maupun sisi ekonomis. Hasil awal yang ada sangat menjanjikan.

Menghubungkan jaringan mesh yang berbasis pada peralatan daur ulang, yang di rancang dan dibuat secara lokal - dikenal sebagai ***Himalayan-Mesh-Router*** (http://drupal.airjaldi.com/node/9). Router mesh di instalasi di setiap lokasi, berbeda hanya antenna saja, tergantung pada lokasi geografis dan kebutuhan. Kami menggunakan berbagai antena, dari 8 - 11 dBi omnidirectional, 12 - 24 dBi antena directional dan kadang-kadang antenna sektoral penguatan tinggi (dan biaya tinggi). Mesh terutama digunakan untuk:

- Akses Internet.
- Aplikasi file sharing.
- Off-situs backup.
- Memutar video berkualitas tinggi dari arsip yang jauh.

Sebuah pusat VoIP, PBX berbasis software (Asterisk) juga di install dan memberikan layanan jasa telepon untuk anggota. PBX Asterisk juga dihubungkan ke jaringan telepon PSTN. Namun, karena masalah hukum saat ini hanya digunakan untuk panggilan masuk ke dalam mesh. Pelanggan menggunakan berbagai software-phone, serta berbagai ATA (Analog Telepon Adaptor) maupun IP phone yang mempunyai fitur lengkap.

Gambar 11.5: Seorang installer Dharmsala bekerja pada sebuah menara

Pada tulang punggung mesh yang di enkripsi tidak di ijinkan akses bagi perangkat mobile (notebook dan PDA), jadi kami telah menempatkan beberapa akses point 802.11b di banyak lokasi yang sama dimana router mesh diinstal. Router mesh memberikan infrastruktur tulang punggung sedang AP memberikan akses untuk perangkat mobile, dimana diperlukan.
Akses ke tulang punggung mesh hanya di ijinkan bagi router mesh. Wireless klien yang sederhana yang tidak memiliki kepandaian untuk "berbicara" menggunakan routing protokol mesh akan menghadapi kebijakan akses yang ketat. Kanal mesh oleh karenanya di enkripsi (WPA), dan juga "disembunyikan" untuk mencegah peralatan mobile untuk menemukannya dan mencoba untuk mengaksesnya. Dengan hanya mengijinkan akses ke mesh pada router router memungkinkan untuk kebijakan kontrol akses yang ketat dan melakukan pembatasan pada CPE (Client Premises Equipment) yang merupakan elemen penting yang dibutuhkan untuk mencapai keamanan end-to-end, mengatur trafik, dan Quality-of-Service.

Konsumsi daya dari router mesh kurang dari 4 Watt. Hal ini membuat mereka ideal untuk penggunaan panel surya. Banyak dari router mesh Dharamsala hanya menggunakan panel surya kecil. Penggunaan tenaga surya di kombinasi dengan antena kecil dan router rendah daya sangat cocok untuk daerah bencana, karena sangat mungkin untuk bertahan ketika semua infrastruktur komunikasi lain sudah rusak.

-- AirJaldi, http://airjaldi.com/

Studi kasus: Jaringan Negara Bagian Mérida

Kota Mérida terletak di kaki gunung tertinggi di Venezuela, di dataran pada ketinggian 1.600 m. Ini adalah ibu kota negara bagian Mérida, dan rumah ke universitas berusia dua abad, dengan sekitar 35.000 mahasiswa. University of Los Andes (ULA) menggelar jaringan komputer akademik pertama pada tahun 1989, walaupun dengan keterbatasan ekonomi, telah berkembang meliputi 26 km kabel serat optik yang melalukan jaringan TDM dan ATM (asynchronous transfer mode). Pada tahun 2006, diatas kabel serat optik yang sama, jaringan Gigabit Ethernet sepanjang 50 km telah digelar.

Gambar 11.6: Mérida adalah salah satu dari tiga negara bagian yang bergunung-gunung dari Venezuela, dimana Andes mencapai 5.000 m.

Meskipun demikian, banyak tempat di kota dan desa-desa di sekitarnya jauh dari jangkauan cincin serat optik. Universitas mengoperasikan sebuah server komunikasi dengan kabel telepon untuk menyediakan akses remote ke dalam jaringan, tetapi panggilan lokal dikenakan biaya per menit dan banyak desa kekurangan saluran telepon.

Untuk alasan ini, upaya untuk membangun akses nirkabel ke jaringan universitas, disebut RedULA, dilakukan sejak awal. Usaha pertama mengambil keuntungan dari jaringan paket radio yang di operasikan oleh amatir radio. Sejak tahun 1987, amatir radio telah memiliki gateway dengan stasiun radio ***HF (High Frekuensi)*** yang bekerja pada 300 bps untuk hubungan luar negeri, di samping beberapa stasiun ***VHF (Frekuensi Sangat Tinggi)*** yang tersambung pada 1200 bps yang malang melintang di negeri ini.

Sementara daerah pegunungan merupakan kendala besar untuk peletakan kabel dan pembuatan jalan, gunung dapat sangat memudahkan dalam membangun jaringan radio. Pekerjaan ini di bantu oleh keberadaan sistem cable car, yang terkenal paling tinggi di dunia yang menyambungkan kota ke puncak 4765 m.

Gambar 11.7: Dalam perjalanan ke puncak, cable car melewati oleh stasiun antara yang disebut La Aguada, pada ketinggian 3.450 m dan memiliki pemandangan yang indah ke kota Mérida dan desa-desa lainnya pada jarak 50 km.

Packet radio

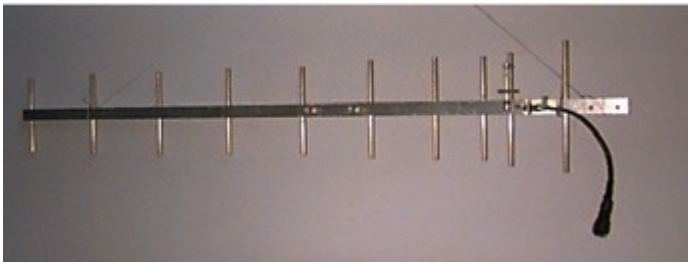
Amatir radio lokal mengoperasikan jaringan radio paket. Pada awalnya jaringan ini bekerja pada 1200 bps, menggunakan VHF amatir radio FM terhubung ke komputer pribadi melalui ***Terminal Node Controller (TNC).*** TNC adalah antarmuka antara radio yang bersifat analog dan sinyal digital yang ditangani oleh PC.

TNC mengontrol rangkaian “Push To Talk” di radio untuk men-switch radio untuk dapat transmit dan receive, melakukan modulasi / demodulation dan assembly / disassembly paket yang menggunakan variasi dari X.25 dikenal sebagai protokol ***AX.25.*** Gerbang antara VHF dan HF radio dibangun dengan menggunakan dua modem TNC dan komputer. Biasanya, sebuah gateway akan menghubungkan jaringan paket radio lokal VHF ke stasiun luar negeri dengan melalui stasiun HF hingga ribuan kilometer, walaupun pada kecepatan hanya 300 bps. Sebuah jaringan radio paket nasional juga dibangun, yang di relay melalui ***digipeater*** (digital repeater, intinya adalah TNC terhubung ke dua radio dengan antena mengarah pada arah yang berbeda), untuk memperluas jaringan dari Mérida ke Caracas dengan cara tersebut hanya membutuhkan dua stasiun pengulang / digipeater. Digipeater yang dioperasikan pada 1200 bps dan memungkinkan untuk sharing dari beberapa program dan file teks di antara para amatir radio.

Phil Karn, seorang radio amatir yang memiliki latar belakang jaringan komputer, menulis program KA9Q yang menerapkan TCP / IP di atas AX.25. Menggunakan program ini, yang menggunakan callsign pengembangnya, amatir radio di seluruh dunia dapat terhubung ke Internet menggunakan berbagai jenis radio. KA9Q tetap menggunakan fungsi TNC seminimal mungkin, memberikan hampir semua fungsi proses kepada PC. Pendekatan ini memungkinkan untuk lebih mudah melakukan upgrade dan fleksibilitas. Dalam Mérida, kami dapat segera meng-upgrade jaringan kami untuk 9600 bps dengan menggunakan modem yang lebih maju, dan beberapa amatir radio sekarang dapat mengakses Internet melalui

jaringan kabel RedULA. Keterbatasan bandwidth radio yang tersedia pada band VHF menjadikan batas atas kecepatan tertinggi yang dapat di capai. Untuk meningkatkan kecepatan, kita harus pindah ke frekuensi yang lebih tinggi.

Amatir radio diperbolehkan untuk menggunakan kanal dengan lebar 100 kHz di UHF (Ultra High-Frekuensi). Digital radio digabungkan dengan modem 19,2 kbps akan melipatgandakan bandwidth transmisi. Proyek ini dikembangkan menggunakan teknologi ini untuk menyambungkan House of Science di kota El Vigia, ke Mérida dan Internet. Antenna UHF dibuat di LabCom, laboratorium komunikasi dari ULA.



Gambar 11.8: Sebuah Antenna UHF untuk radio paket yang dikembangkan di ULA, LabCom.

Meskipun El Vigia hanya 100 km dari Mérida melalui jalan, wilayah yang bergunung-gunung membutuhkan penggunaan dua repeater. Satu terletak di La Aguada, pada ketinggian 3600 m, dan yang lainnya di Tusta, di 2000 m. Proyek ini dibiayai oleh FUNDACITE MERIDA, sebuah lembaga pemerintah yang mempromosikan ilmu pengetahuan dan teknologi di negara bagian. FUNDACITE juga mengoperasikan sekumpulan telepon modem 56 kbps untuk menyediakan akses Internet untuk perorangan dan lembaga.

Kebutuhan untuk dua stasiun pengulang menggaris bawahi keterbatasan yang dihadapi oleh operator yang menggunakan frekuensi tinggi, yang memerlukan line of sight untuk memperoleh transmisi yang handal. Pada band yang lebih rendah dari VHF, sinyal yang dengan mudah terpantul dan mencapai wilayah di belakang perbukitan.

Kadang-kadang kita dapat memantulkan sinyal menggunakan ***repeater pasif,*** yang dibuat dengan menghubungkan dua directional antenna back-to-back dengan kabel coaxial, tanpa radio. Cara ini telah diuji untuk menyambung ke tempat tinggal saya ke LabCom. Jarak hanya 11 km, tetapi ada bukit yang memblokir sinyal radio. Sambungan dilakukan dengan menggunakan pengulang pasif untuk memantulkan ke La Aguada, dengan dua antenna sebagai pengulang yang membentuk 40 derajat satu sama lain. Hal ini menjadi sangat menarik dan tentunya jauh lebih murah daripada menggunakan modem telepon, yang jelas merupakan media yang jauh lebih cepat daripada tulang punggung nirkabel untuk menghubungkan desa-desa terpencil.

Untuk itu, kami menjajaki penggunaan modem radio 56 kbps yang dikembangkan oleh Dale Heatherington. Modem tersebut dimasukan ke dibuah card PI2 yang dibuat oleh Amatir Radio

di Ottawa, dan terhubung langsung ke PC menggunakan Linux sebagai sistem operasi jaringan. Walaupun sistem ini berfungsi sangat baik, munculnya World Wide Web dengan kebanyakan gambar dan file-file yang sangat mengkonsumsi bandwidth sangat jelas bahwa jika kami ingin memenuhi kebutuhan sekolah dan rumah sakit kami harus menyebarkan solusi bandwidth yang lebih tinggi, di setidaknya pada tulang punggung. Ini berarti penggunaan frekuensi operasi yang lebih tinggi di microwave, yang berarti juga biaya tinggi.

Untungnya, teknologi alternatif yang banyak digunakan dalam aplikasi militer telah tersedia untuk keperluan sipil menggunakan harga terjangkau. Disebut ***Spread Spectrum***, teknologi ini pertama kali di temukan untuk penggunan sipil sebagai jaringan nirkabel area lokal jarak pendek, tetapi segera memberikan sumbangsih yang sangat berguna di tempat di mana spektrum elektromagnetik tidak terlalu sesak, yang memungkinkan menjembatani jarak beberapa kilometer.

Spread Spektrum

Spread spectrum menggunakan kekuatan sinyal rendah yang sengaja perluas memenuhi semua alokasi bandwidth, sementara pada saat yang sama memungkinkan sejumlah pengguna untuk berbagi media / kanal yang sama dengan menggunakan kode yang berbeda untuk setiap pelanggan. Ada dua cara untuk melakukannya: ***Direct Squence Spread Spectrum (DSSS)*** dan ***Frequency Hopping Spread Spectrum (FHSS).***

- Dalam DSSS informasi yang akan dikirim dikalikan secara digital yang urutan frekuensi yang lebih tinggi, sehingga memperlebar bandwidth pengiriman. Meskipun ini mungkin terlihat seperti membuang-buang bandwidth, pemulihan sistem sangat efisien sehingga dapat membaca sinyal yang sangat lemah, memungkinkan untuk serentak penggunaan spektrum yang sama dengan beberapa stasiun sekaligus.

- Pada FHSS, pemancar akan secara terus menerus mengubah frekuensi dalam alokasi bandwidth yang di ijinkan sesuai dengan kode tertentu. Penerima harus mengetahui kode ini untuk melacak frekuensi pemancar.

Kedua teknik mempertukarkan daya pancar dengan bandwidth, memungkinkan banyak stasiun untuk menggunakan secara bersama sebuah spektrum frekuensi. Pada Latin American Networking School yang pertama (EsLaRed'92), diadakan di Mérida pada tahun 1992, kami menunjukkan teknik ini. Kami membuat jaringan percobaan menggunakan antenna luar yang dibuat di LabCom, memungkinkan pengiriman data untuk beberapa kilometer. Pada tahun 1993, Departemen Telekomunikasi Venezuela membuka empat band untuk digunakan dengan DSSS:

- 400 - 512 MHz
- 806 - 960 MHz
- 2.4 - 2.4835 GHz

- 5.725 - 5.850 GHz

Pada salah satu band di atas, maksimum data pemancar dibatasi untuk 1 Watt dengan penguatan maksimum antena 6 dBi, untuk total EIRP (Effective Isotropic Radiated Power) sebesar 36dBm. Aturan ini membuka jalan untuk pengembangan jaringan DSSS dengan nominal bandwidth 2 Mbps pada band 900 MHz. Teknologi ini memuaskan kebutuhan akan aktifitas World Wide Web.

Jaringan dimulai di LabCom, di mana sambungan ke RedULA telah tersedia. LabCom membuat sebuah antenna Yagi yang di arhkan ke sebuah reflektor pojok di Aguada. Ini diberikan 90 derajat beamwidth, yang terlihat di sebagian besar kota Mérida. Beberapa lokasi pelanggan, semua berbagi bandwidth 2 Mbps, yang segera bertukar file, termasuk gambar dan video klip. Beberapa lokasi pelanggan memerlukan kabel yang panjang antenna antenna dengan radio spread spectrum yang di akomodasi oleh penggunaan amplifier dua arah.

Hasil sangat menarik ini di laporkan ke grup di International Center untuk Fisika Teoretis (ICTP) di Trieste, Italia, pada tahun 1995. Grup ini adalah bertujuan untuk menyediakan konektivitas antara Pusat Komputer, Ilmu Fisika Bangunan, dan Teknologi Bangunan di Universitas Ile-Ife di Nigeria. Tak ama kemudian di tahun yang sama, jaringan didirikan oleh staf ICTP dengan dana dari Perserikatan Bangsa-Bangsa dan Universitas telah berjalan sejak memuaskan, terbukti menjadi jauh lebih efektif dibandingkan dengan solusi jaringan serat optik awalnya direncanakan.

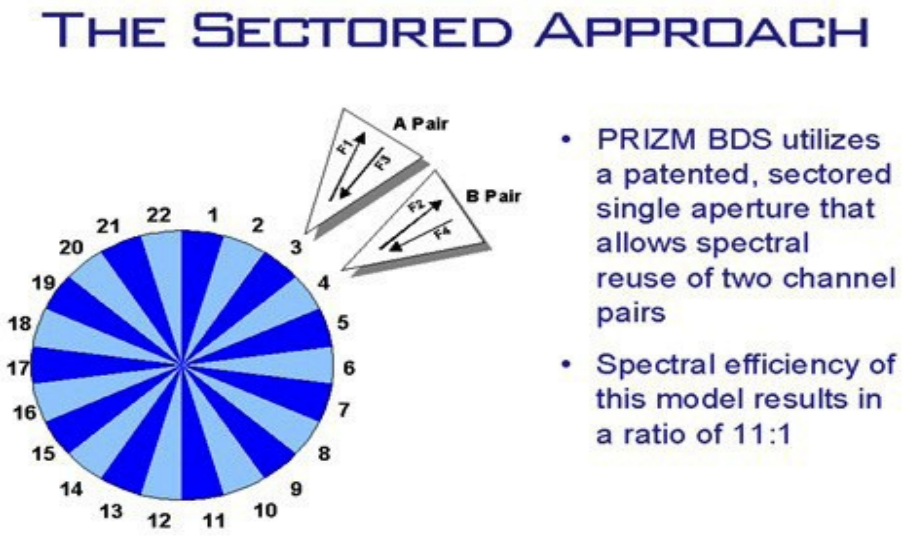
Kembali di Mérida, dengan semakin banyaknya jumlah lokasi, throughput per pengguna menurun. Kami mulai melirik band 2,4 GHz untuk memberikan tambahan kapasitas. Band ini dapat membawa tiga aliran data sekaligus pada 2 Mbps, tetapi jarak efektif lebih rendah daripada apa yang dapat dicapai pada band 900 MHz. Kami sangat sibuk perencanaan pembangunan jaringan tulang punggung menggunakan 2,4 GHz akhirnya kami memulai sebuah perusahaan yang menawarkan solusi baru untuk jarak jauh, dengan throughput yang lebih tingi, dan kemungkinan pemakaian ulang frekuensi mengunakan peralatan microwave yang narrowband.

Broadband sistem penyampaian

Setelah mengunjungi Nashua, New Hampshire, fasilitas dari Spike Technologies, kami yakin bahwa antenna dan sistem radio mereka merupakan solusi terbaik untuk jaringan di negara bagian kami, dengan alasaan sebagai berikut:

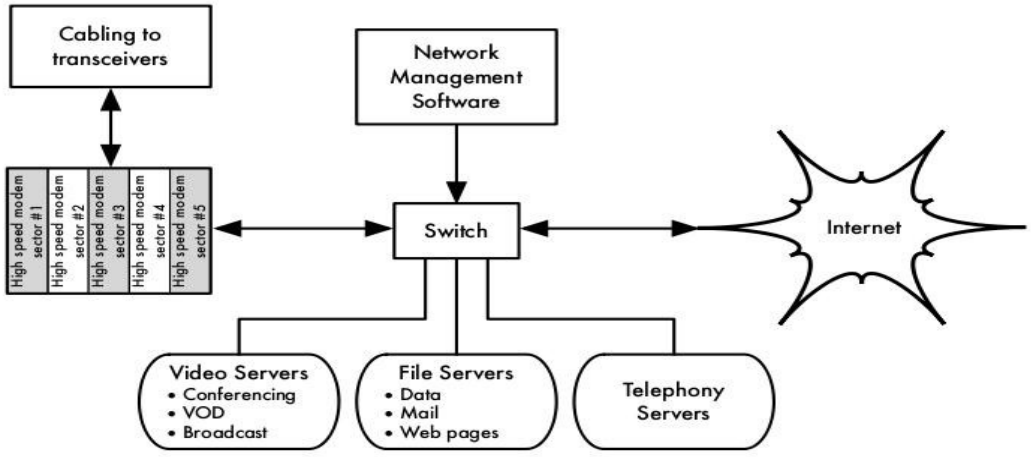
Sistem broadband mereka menggunakan antenna sektoral khusus (**Gambar 11.9**), dengan penguatan 20 dBi dengan pada masing-masing dari 22 sektor yang independen. Setiap sektor akan transmit dan menerima pada kanal independen pada kecepatan 10Mbps full-duplex, dengan total throughput 440 Mbps. Frekuensi digunakan kembali pada sektor yang

tidak saling mengganggu membuat sistem sangat effisien dalam menggunakan spektrum.



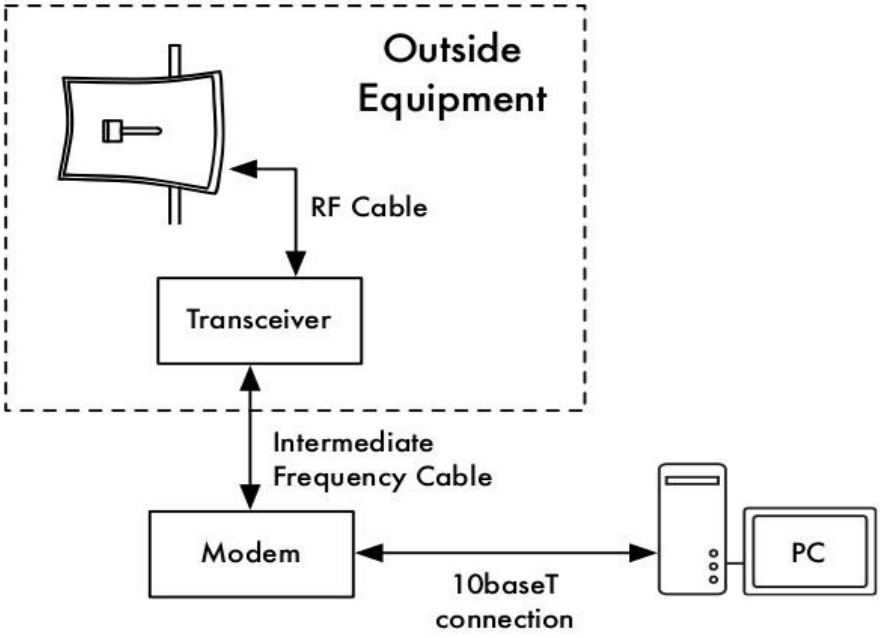
Gambar 11.9: Spike Technologies full duplex, sistem sektoral dengan kepadatan tinggi.

Radio digital narrowband dapat beroperasi di mana saja dari 1 sampai 10 GHz, dengan jangkauan hingga 50 km. Radio tersebut bekerja dengan berbagai modem kabel TV, yang memberikan akses pelanggan melalui kabel LAN standar 10Base-T. Di base station, sektor-sektor terinterkoneksi dengan switch berkecepatan tinggi yang memiliki latensi sangat kecil (lihat **Gambar 11.10**), yang memungkinkan aplikasi seperti streaming video sampai 30 frame per detik. Masing-masing sektor bertindak sebagai Ethernet LAN independen.



Gambar 11.10: Interkoneksi sistem Spike Technologies.

Pada sisi pelanggan, radio yang sama dan modem memberikan sambungan 10BaseT ke Ethernet lokal.



Gambar 11.11: Sambungan di sisi akhir pelanggan.

Dengan dana dari FUNDACITE, sebuah sistem percibaan segera di instalasi di Mérida, dengan base station terletak di atas stasiun cable car La Aguda pada ketinggian 3.600 m.

Gambar 11.12: Instalasi di atas Mérida pada La Aguada, pada 3600 meter.

Pada awalnya hanya 5 sektor terpasang, dengan beamwidth dari masing-masing 16 derajat. Pelanggan pertama adalah lokasi Fundacite, di mana ada sebuah sistem satelit yang

menyediakan akses Internet. Sektor dua memberikan layanan ke istana Gubernur. Sektor ketiga melayani FUNDEM, sebuah organisasi pertolongan dari pemerintah daerah. Sektor ke empat lembaga pemasyarakatan di dekat kota Lagunillas, sekitar 35 km dari Mérida. Sektor kelima memancar ke repeater yang berada di puncak gunung dekat desa La Trampa, 40 km dari La Aguada. Dari La Trampa, sebuah sambungan 41 Km dilakukan untuk memperluas jaringan ke House of Science di kota Tovar.

Pada tanggal 31 Januari 1998, video konferensi antara lembaga pemasyarakatan dan Justice Palace terbukti di Mérida, bahwa selain dari akses Internet, sistem dapat juga mendukung video streaming. Video conference ini digunakan melakukan keputusan pengadilan dari para tahanan, sehingga menghindari risiko penggunaan transportasi bagi mereka.

Keberhasilan percobaan ini telah mendorong pemerintah negara bagian untuk mengalokasikan dana untuk melengkapi sistem untuk memberikan akses Internet kecepatan tinggi negara untuk sistem kesehatan, sistem pendidikan, perpustakaan, pusat masyarakat, dan beberapa instansi pemerintah. Pada bulan Januari 1999 kami telah menyambungkan 3 rumah sakit, 6 lembaga pendidikan, 4 lembaga penelitian, 2 koran, 1 stasiun TV, 1 perpustakaan umum, dan 20 lembaga sosial dan pemerintah agar dapat berbagi informasi dan mengakses Internet. Rencana selanjutnya adalah menyambungkan 400 lokasi dalam tahun ini pada kecepatan 10Mbps full duplex, dan dana telah dialokasikan untuk tujuan ini.

Gambar 11.13 menunjukkan peta negara bagian Mérida. Gelap baris menunjukkan tulang punggung awal, sedangkan garis yang lebih kecil menampilkan pengembangan jaringan.

Gambar 11.13: Jaringan Negara Bagian Mérida

Di antara banyak kegiatan yang didukung oleh jaringan, ada baiknya kami sebutkan beberapa diantaranya:

- **Pendidikan:** sekolah telah menemukan pasokan materi ajar berkualitas tinggi yang tidak habis-habisnya baik bagi murid maupun guru, terutama di bidang geografi, bahasa, dan ilmu pengetahuan, dan sebagai alat untuk berkomunikasi dengan kelompok lainnya yang mempunyai minat yang sama. Perpustakaan memiliki kamar dengan komputer yang dapat diakses oleh masyarakat umum dengan kemampuan internet yang sepenuhnya. Surat kabar dan stasiun TV takjub melihat sumber informasi yang tersedia bagi pemirsa mereka.

- **Kesehatan:** rumah sakit universitas memiliki sambungan langsung ke unit perawatan intensif, dimana ada staf dokter spesialis yang selalu bertugas. Dokter tersebut sekarang menjadi tersedia bagi rekan-rekan mereka di desa-desa terpencil untuk membicarakan kasus-kasus tertentu. Sekelompok peneliti di universitas mengembangkan bebeapa aplikasi telemedicine pada jaringan.

- **Penelitian:** obsevatorium astronomi di Llano del Hato, terletak pada ketinggian 3600 m di pegunungan sekitar 8 derajat dari khatulistiwa akan segera terkait, yang memungkinkan astronomer dari seluruh dunia untuk mengakses foto yang dikumpulkan di obsevatorium tersebut. Peneliti lapangan di pedesaan sangat menikmati akses Internet.

- **Pemerintah:** Sebagian besar instansi pemerintah sudah terhubung dan mulai meletakkan informasi on-line bagi warga. Kami berharap ini memiliki pengaruh yang berarti dalam hubungan antara warga dengan pemerintah. Badan-badan bantuan dan lembaga penegak hukum pengguna jaringan yang sangat aktif.

- **Hiburan dan Produktivitas:** Untuk orang-orang yang tinggal di luar kota, kesempatan yang ditawarkan oleh Internet memiliki dampak yang sangat besar terhadap kualitas kehidupan mereka. Kami berharap bahwa ini akan membantu membalikkan kecenderungan melakukan migrasi keluar dari daerah pedesaan, mengurangi kepadatan di kota. Petani memiliki akses ke informasi tentang harga dan dapat mengontrol harga dari tanaman dan pasokan, serta meningkatkan pertanian.

SUPERCOMM'98, diselenggarakan di Atlanta pada bulan Juni, mengutip jaringan broadband di Mérida sebagai pemenang dalam penghargaan SUPERQuest dalam kategori 8-Remote Access sebagai yang terbaik di bidang tersebut.

Pelatihan

Sejak awal upaya kami untuk membangun sebuah jaringan komputer, kami menyadari bahwa pelatihan adalah kepentingan untuk orang yang terlibat dalam pembangunan jaringan,

manajemen, dan pemeliharaan. Dengan anggaran sangat terbatas, kami memutuskan bahwa kami harus mengumpulkan sumber daya kami dengan orang-orang lain yang membutuhkan pelatihan. Pada tahun 1990, ICTP menyusun Sekolah Internasional pertama tentang jaringan analisis dan manajemen jaringan komputer, yang dihadiri oleh Profesor Silva Jose dan Profesor Luis Nunez dari universitas kami. Sekembalinya ke Mérida, mereka menyatakan bahwa kita harus berusaha mengadakan kegiatan yang sama di universitas kami. Untuk akhir ini, mengambil keuntungan dari cuti panjang saya, saya menghabiskan tiga bulan di Bellcore Morristown, New Jersey, dan lebih tiga bulan di ICTP membantu dalam penyusunan Sekolah Jaringan Kedua pada tahun 1992, dimana saya bisa bergabung dengan rekan saya Profesor Edmundo Vitale. Aku menghabiskan sisa cuti panjang saya di SURANET di College Park, Maryland, di bawah bimbingan Dr Glenn Ricart, yang diperkenalkan untuk saya kepada Dr Saul Hahn dari Organisasi Negara-negara Amerika, yang menawarkan dukungan keuangan untuk kegiatan pelatihan di Amerika Latin . Pengalaman ini memungkinkan kami untuk meluncurkan Sekolah Jaringan Amerika Latin Pertama (EsLaRed'92) di Mérida, dihadiri oleh 45 peserta dari 8 negara di wilayah Amerika Latin, dengan instruktur dari Eropa, Amerika Serikat, dan Amerika Latin. Pelatihan hands-on (praktek) dilaksanakan selama tiga minggu, dan teknologi nirkabel lebih di tekankan.

EsLaRed'95 berkumpul kembali di Mérida dengan 110 peserta dan 20 instruktur. EsLaRed'97 memperoleh 120 peserta, dan ini didukung oleh Internet Society, yang juga mensponsori Spanyol dan Lokakarta Jaringan Pertama Portugis untuk Amerika Latin dan Karibia, diadakan di Rio de Janeiro pada tahun 1998 dengan EsLaRed bertanggung jawab untuk materi pelatihan. Sekarang sepuluh tahun kemudian, EsLaRed terus memperluas upaya pelatihan di seluruh Amerika Selatan.

Penutup

Internet memiliki dampak yang lebih besar di negara-negara berkembang dibandingkan di tempat lain, karena tingginya biaya panggilan telepon internasional, fax, majalah, dan buku. Hal ini jelas diperparah oleh lebih rendah dari pendapatan rata-rata orang. Beberapa penghuni di desa-desa terpencil yang tidak memiliki telepon mengalami peralihan dari abad 19 ke abad 21 terima kasih untuk jaringan nirkabel. Diharapkan ini akan berkontribusi untuk perbaikan gaya hidup di bidang kesehatan, pendidikan, hiburan, dan produktivitas, serta menciptakan hubungan yang lebih adil antara warga dan pemerintah.

Referensi

- 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

Studi kasus: Chilesincables.org

Teknologi pengiriman data nirkabel terbaru memungkinkan pembuatan jaringan berkecepatan tinggi, secara geografis terpisah dengan biaya yang relatif rendah. Jika jaringan ini di bangun dengan ode menghilangkan halangan untuk akses data, kita dapat mengatakan jaringan ini adalah ***free network.*** Jaringan tersebut akan dapat membawa manfaat besar untuk setiap pengguna, mereka independen dari politik, ekonomi, maupun kondisi sosial. Jenis jaringan ini merupakan tantangan secara langsung kepada model jaringan komersial yang banyak mengkungkung masyarakat barat modern.

Agar free network dapat berkembang, teknologi nirkabel harus disesuaikan dan dimasukkan kemungkinan penggunaan yang terbaik. Hal ini dilakukan oleh kelompok hacker yang melakukan penelitian, investigasi, pembangunan dan pelaksanaan proyek, serta mengijinkan semua orang untuk mengakses pengetahuan yang di peroleh secara bebas.

Chilesincables.org berupaya untuk dapat promosikan dan mengatur jaringan nirkabel gratis di Chile secara profesional. Kami melakukan hal ini dengan memberikan pendidikan tentang hukum yang berkaitan dengan aspek teknis dan jaringan nirkabel; mendorong adaptasi dari teknologi baru melalui penelitian yang memadai; dan merangsang penyesuaian teknologi ini untuk memenuhi kebutuhan spesifik komunitas Chili maupun bangsa di dunia.

Keterangan tentang teknologi

Kami menggunakan berbagai teknologi nirkabel, termasuk IEEE 802.11a/b/g. Kami juga mencoba inovasi terbaru di lapangan, seperti WiMAX. Dalam kebanyakan kasus, peralatan yang telah dimodifikasi agar menerima antena eksternal buatan lokal yang memenuhi peraturan telekomunikasi lokal. Walaupun mayoritas nirkabel perangkat keras yang tersedia di pasar akan sesuai dengan tujuan kami, kami mendorong pemanfaatan dan eksplorasi dari beberapa vendor yang memungkinkan untuk kontrol lebih baik dan adaptasi dengan kebutuhan kita (tanpa harus meningkatkan harga). Termasuk card WiFi dengan chipset yang ditawarkan oleh Atheros, Prism, Orinoco, dan Ralink, serta beberapa model dari akses point yang diproduksi oleh Linksys, Netgear, dan Motorola. Komunitas hacker telah mengembangkan firmware yang menyediakan fungsionalitas baru pada peralatan ini.

Untuk jaringan tulang punggung, kami menggunakan sistem operasi Open Source, termasuk GNU/Linux, FreeBSD, OpenBSD, dan Minix. Hal ini sesuai kebutuhan kami dalam bidang routing serta pelaksanaan layanan seperti proxy, web dan FTP server, dll Selain itu, mereka sesuai dengan filosofi proyek yang menggunakan teknologi free dengan kode Open Source.

Penggunaan dan Aplikasi

Jaringan yang diimplementasikan selama ini memungkinkan tugas-tugas berikut:

- Transfer data melalui FTP atau web server
- Layanan VoIP
- Audio dan video streaming.
- Instan Messaging.
- Eksplorasi dan pelaksanaan layanan baru seperti LDAP, resolusi nama, metoda keamanan yang baru, dll.
- Layanan yang disediakan oleh klien. Pengguna bebas menggunakan infrastruktur jaringan untuk membuat layanan mereka sendiri.

Administrasi dan Pemeliharaan

Operasional unit dari sebuah jaringan adalah node. Setiap node memungkinkan pelanggan untuk tersambung ke jaringan dan memperoleh layanan jaringan yang paling dasar. Selain itu, masing-masing node harus dihubungkan minimal satu node lain. Hal ini memungkinkan jaringan untuk tumbuh dan untuk membuat layanan tersedia untuk setiap klien.

Sebuah node dipelihara oleh administrator yang merupakan anggota komunitas yang komit untuk tugas berikut:

- Pemeliharaan untuk uptime yang memadai (lebih dari 90%).
- Menyediakan layanan dasar (biasanya akses web).
- Membuat klien terupdate mengenai layanan node (misalnya, cara mendapatkan akses ke jaringan). Hal ini umumnya diberikan oleh suatu captive portal.

Administrasi umum dari jaringan (terutama, hal yang berkaitan dengan pembuatan node baru, pilihan lokasi, topologi jaringan, dll) dilakukan oleh dewan komunitas, atau oleh teknisi yang terlatih untuk tujuan tersebut. Chilesincables.org saat ini sedang dalam proses perolehan status hukum, sebuah langkah yang akan mengijinkan peraturan dari prosedur administrasi internal dan formalisasi komunitas ke masyarakat.

Pelatihan dan peningkatan kapasitas

Chilesincables.org menganggap pelatihan anggotanya dan klien sangat penting untuk alasan berikut:

- Spektrum radio harus dibuat sebersih mungkin agar menjamin sambungan nirkabel yang baik. Oleh karena itu, pelatihan di teknik komunikasi radio adalah penting.
- Penggunaan material dan metoda yang mentaat peraturan sebagai persyaratan aktifitas pembangunan yang normal.
- Agar sesuai dengan standar Internet, semua administrator jaringan di latih tentang jaringan TCP/IP.
- Untuk menjamin kesinambungan operasi jaringan, pengetahuan tentang teknologi jaringan harus ditransfer ke pengguna.

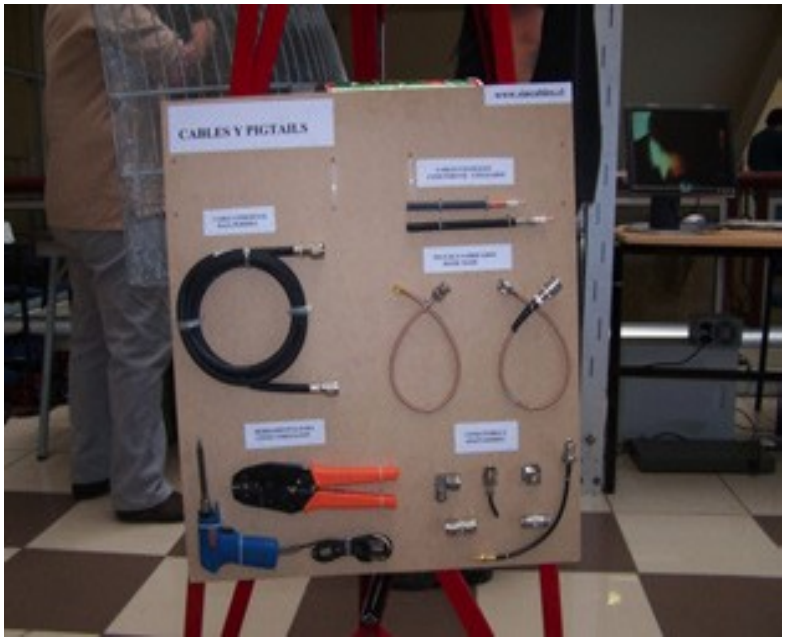
Untuk mendukung prinsip-prinsip tersebut, Chilesincables.org melaksanakan aktifitas berikut:

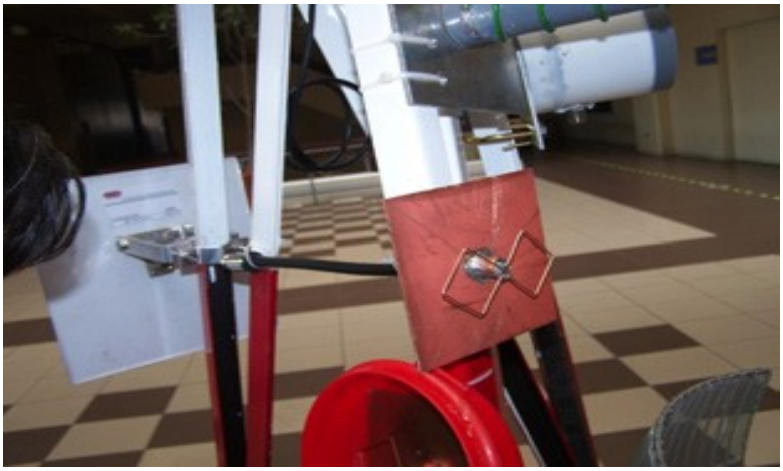
- **Workshop Antena.** Peserta dilatih untuk membuat antenna, dan memperkenalkan konsep komunikasi radio.
- **Workshop Sistem Operasi.** Pelatihan untuk membuat router dan perangkat lainnya berbasis GNU/Linux atau software lainnya seperti m0n0wall atau pfsense. Konsep dasar jaringan juga diajarkan.
- **Promosi dan Iklan.** Acara-acara untuk komunitas berbeda yang mempunyai tujuan yang sama dengan kami di promosikan. Termasuk workshop di kampus-kampus, ceramah, pertemuan teman-teman free software, dll.
- **Memupdate Bahan.** Chilesincables.org me-maintain sejumlah dokumen dan material yang bebas di akses yang tersedia untuk orang-orang yang tertarik pada aktifitas tertentu.

Gambar pada halaman berikut menyajikan beberapa keterangan tentang kegiatan di komunitas kami.

Gambar 11.14: Workshop antenna omnidirectional slotted. Dalam sesi ini, peserta berlajar tentang cara membuat antenna maupun teori terkait.

Gambar 11.15: Salah satu anggota staf kami memberikan kuliah membuat router berbasis m0n0wall dalam mengadmini sebuah node.

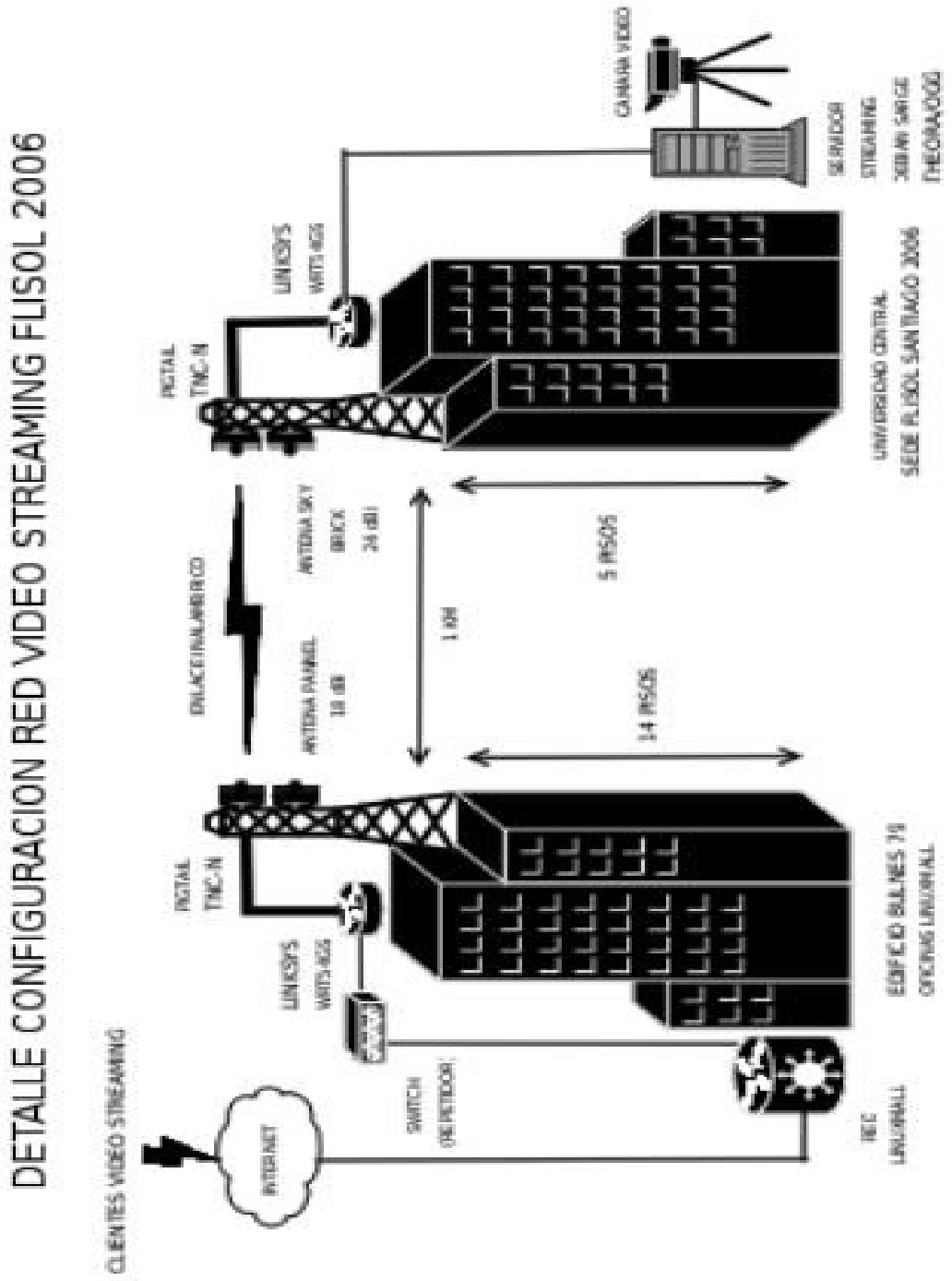




Gambar 11.16: Detail mini tower dengan contoh antena, kabel dan pigtail.

Gambar 11.17: Stasiun wireless dan antena parabolic yang digunakan untuk memancarkan Santiago-2006 FLISOL melalui video streaming.

Gambar 11.18: Lokasi dari ujung sambungan.

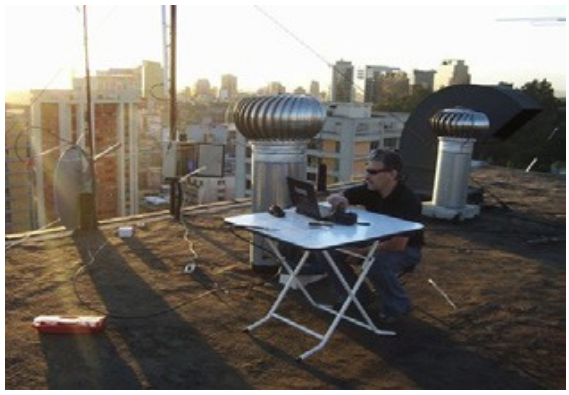


Gambar 11.19: Skematik mewakili transmisi Santiago-2006 FLISOL video streaming, menggunakan free software. Kecepatan transmisi nirkabel yang dicapai adalah 36 Mbps pada jarak 1 km.

Gambar 11.20: Node Quiani. Ini adalah salah satu node tertinggi di dunia. Yang terletak di ketinggian 4000 m, sekitar 2.000 kilometer sebelah utara ibukota negara.

Gambar 11.21: Node di selatan Santiago, yang terdiri dari menara 15 m, sebuah antenna Trevor Marshall 16 + 16, dan 30 klien. Node yang terhubung ke node di pusat kota lebih dari 12 km.

Gambar 11.22: pemandangan alam dari sebuah node dari atas menara.



Gambar 11.23: Node di downtown terhubung ke node di selatan Santiago. Perhatikan antena Parabolic untuk backhaul dan slotted antena untuk menghubungkan klien.

Gambar 11.24: Pemasangan node di atas menara air di Batuco, Wilayah Metropolitan, memberikan backhaul untuk telecenter Cabrati.

Gambar 11.25: Workshop antena Yagi yang diselenggarakan oleh komunitas kami. Peserta sedang membangun sendiri antena.

Kredit

Komunitas kami terdiri dari kelompok relawan yang komit dan layak di perhatikan:

Felipe Cortez (Pulpo), Felipe Benavides (Colcad), Mario Wagenknecht (Kaneda), Daniel Ortiz (Zaterio), Cesar Urquejo (Xeuron), Oscar Vasquez (Mesin), San Jose Martin (paket), Carlos Campano (Campano), Kristen Vasquez (Crossfading), Andres Peralta (Cantenario), Ariel Orellana (Ariel), Miguel Bizama (Picunche), Eric Azua (Bapak Floppy), David Paco (Dpaco), Marcelo Jara (Alaska).

-- Chilesincables.org

Studi kasus: Sambungan Jarak Jauh 802.11

Terima kasih kepada topografi yang baik, Venezuela sudah ada sambungan WLAN jarak jauh, seperti sambungan 70 km yang dioperasikan oleh Fundacite Mérida antara Pico Espejo dan Canagua. Untuk menguji batas dari teknologi ini, perlu untuk menemukan sebuah line of sight yang saling berhadapan tanpa halangan dengan kliring minimal 60% dari zona Fresnel pertama. Sambil melihat daerah di Venezuela, dalam pencarian wilayah ketinggian, saya pertama terfokus pada daerah Guayana. Meskipun banyak tanah yang tinggi yang ditemukan, khususnya yang terkenal "tepuys" (mesa tinggi dengan dinding curam), selalu ada kendala di lapangan.

Perhatian saya dialihkan ke Andes, yang memiliki derajat kemiringan lereng tinggi (naik tiba-tiba dari dataran) terbukti memadai untuk tugas. Untuk beberapa tahun, saya telah melakukan perjalanan melalui kawasan-kawasan yang jarang penduduknya karena minat saya untuk bersepeda gunung. Pada bagian belakang kepala saya, saya mencatat berbagai tempat yang cocok untuk komunikasi jarak jauh.

Pico del Aguila adalah tempat yang sangat baik. Ia mempunyai ketinggian 4200 m dan sekitar dua jam dengan kendaraan dari kota kelahiran saya Mérida. Untuk ujung yang lain, akhirnya saya letakan di kota El Baúl, di negara bagian Cojedes. Menggunakan free software Radio Mobile (tersedia di http://www.cplus.org/rmw/english1.html), saya menemukan bahwa tidak ada halangan pada zona Fresnel pertama (sepanjang 280 km) antara Pico del Aguila dan El Baúl .

Rencana Aksi

Setelah puas dengan keberadaan lintasan yang cocok, kami melihat peralatan yang diperlukan untuk mencapai tujuan. Kami telah menggunakan card Orinoco untuk beberapa tahun. Dengan daya pancar 15 dBm dan ambang batas penerimaan -84 dBm, mereka cukup kuat dan dapat dipercaya. Free Space Loss untuk jarak 282 km adalah 149 dB. Jadi, kita

perlu 30 dBi antena pada kedua sisi itupun hanya menyisakan sedikit margin untuk rugi-rugi lainnya.

Di sisi lain, router wireless populer Linksys WRT54G menjalankan Linux. Komunitas Open Source telah menulis beberapa versi firmware yang memungkinkan untuk penyesuaian setiap parameter transmisi. Khususnya, firmware OpenWRT memungkinkan penyesuaian waktu acknowledge dari lapisan MAC, serta daya output. Firmware lain, DD-WRT, memiliki antarmuka GUI yang sangat nyaman dan utilitas site survey. Selain itu, Linksys dapat diletakan lebih dekat ke antena daripada sebuah laptop. Jadi, kami memutuskan untuk menggunakan sepasang kotak ini. Satu dikonfigurasi sebagai sebuah AP (akses point) dan lain sebagai klien. WRT54G yang dapat beroperasi dengan daya pancar 100 mW dengan linearitas yang baik, dan bahkan dapat di naikan hingga 200 mW. Tetapi di sini, sanga tidak linear dan menghasilkan sinyal spurious / palsu / bayangan, yang seharusnya di hindari. Walaupun ini adalah peralatan kelas konsumen bukan operator telekomunikasi dan cukup murah, setelah bertahun-tahun menggunakannya, kami merasa yakin bahwa peralatan tersebu dapat digunakan untuk mencapai tujuan. Tentu saja, kami menyimpan cadangan untuk berjaga-jaga.

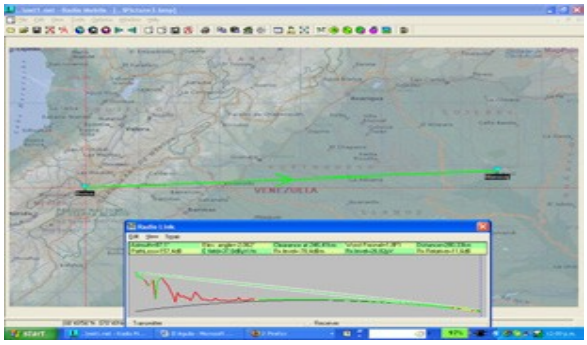
Dengan menetapkan daya pancar ke 100 mW (20 dBm), kami dapat memperoleh keuntungan 5dB dibandingkan dengan kartu Orinoco. Oleh karena itu, kami menetap untuk sepasang WRT54Gs.
Site Survey Pico del Águila

Pada tanggal 15 Januari 2006, saya pergi ke Pico Águila untuk memeriksa situs yang telah cocok berdasarkan perhitungan Radio Mobile. Azimut yang menuju El Baúl adalah 86 °, tetapi karena deklinasi magnetis adalah 8° 16, antenna kami harus mengarah ke arah magnetis 94 °. Sayangnya, saat saya melihat ke arah 94 °, saya menemukan halangan line of sight yang tidak pernah ditunjukkan oleh perangkat lunak, karena keterbatasan resolusi ketinggian peta digital gratis yang tersedia.

Saya mengendarai mountain bike saya unuk beberapa jam memeriksa kawasan sekitar untuk mencari path ke arah Timur yang terbuka. Beberapa tempat yang menjanjikan diidentifikasi, untuk masing-masing tempat saya ambil foto dan mencatat koordinat GPS untuk kemudian memproses dengan software Radio Mobile. Ini menyebabkan saya memperbaiki pilihan path, sehingga memperoleh sebuah gambar seperti pada Gambar 11.26 menggunakan Google Earth:

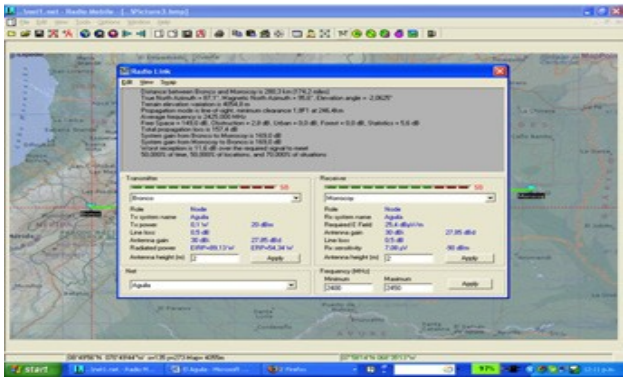
Gambar 11.26: Pemandagan dari sambungan 280 km. Danau Maracaibo di sebelah ke Barat, dan Tanjung Paraguaná di utara Utara.

Profile Radio yang di peroleh dari Radio Mobile ditampilkan dalam **Gambar 11.27:**



Gambar 11.27: Peta dan profil dari usulan path antara Pico Aguila, dan bukit Morrocoy, di dekat kota El Baúl.

Detail sambungan wireless yang ditampilkan dalam **Gambar 11.28:**



Gambar 11.28: Rincian propagasi dari sambungan 280 km.

Dalam rangka untuk mencapai margin yang wajar 12 dB untuk sambungan tersebut, kami memerlukan penguatan antena setidaknya 30 dBi di masing-masing ujung.

Antena

Antenna berpenguaan tinggi untuk band 2.4 GHz tidak tersedia di Venezuela. Biaya impor sangat besar, sehingga kami memutuskan untuk mendaur ulang bekas reflektor parabola (sebelumnya digunakan untuk layanan satelit) dan diganti dengan satu feed yang dirancang untuk 2,4 GHz. Kami membuktikan dengan konsep parabola 80 cm. Penguatan terlalu rendah, sehingga kami mencoba sebuah reflector 2,4m dengan offset fed. Reflector ini menawarkan cukup banyak penguaan, walaupun dengan beberapa kesulitan untuk mengarahkan beam yang hanya 3,5°. Offset 22,5° berarti bahwa parabola akan tampak seperti mengarah ke bawah padahal sebetulnya mengarah horizontal.

Beberapa tes yang dilakukan menggunakan berbagai antenna kaleng dan 12 dBi Yagi sebagai feed. Kami mengarahkan antena di base stasion dari jaringan nirkabel universitas yang berlokasi 11 km pada gunung 3.500 m. Lokasi percobaan berada pada ketinggian 2000 m sehingga sudut elevasinya adalah 8°. Karena menggunakan offset feed, parabola kami arahkan 14° ke bawah, seperti dapat dilihat dalam gambar berikut:

Gambar 11.29: Reflektor offset fed 2,4 m dengan antena 12 dBi di fokusnya, melihat 14 ° ke bawah. Elevasi sebenarnya adalah 8° ke atas.

Kami mampu membuat sambungan dengan base stasion di Aguada, tetapi upaya kami untuk mengukur penguatan dari setup menggunakan Netstumbler tidak berhasil. Ada terlalu banyak fluktuasi pada daya yang diterima pada trafik yang hidup.

Untuk pengukuran yang lebih berarti dari penguatan, kami memerlukan sebuah sinyal generator dan spektrum analyser. Instrumen-instrumen ini juga diperlukan untuk perjalanan di lapangan untuk meluruskan antena yang benar.

Sambil menunggu peralatan yang diperlukan, kami mencari antena untuk digunakan di ujung yang lain, dan juga mengarahkan sistem yang sesuai dengan pancaran radio yang sempit. Pada bulan Februari 2006, saya bepergian ke Trieste untuk mengambil bagian dalam acara tahunan pelatihan nirkabel yang selalu saya hadiri sejak tahun 1996. Pada saat disana, saya menceritakan proyek tersebut ke rekan saya Carlo Fonda, yang segera tertarik dan bersemangat untuk berpartisipasi.

Kerja sama ***Sekolah Networking Amerika Latin s (EsLaRed)*** dan ***Abdus Salam Internasional Center untuk Fisika Teoretis (ICTP)*** telah dilakukan sejak 1992, ketika Jaringan Sekolah pertama diadakan di Mérida dengan dukungan ICTP. Sejak itu, anggota kedua lembaga telah bekerjasama dalam beberapa kegiatan. Beberapa ini termasuk sekolah pelatihan tahunan tentang jaringan nirkabel (di organized oleh ICTP) dan yang lain tentang jaringan komputer (yang diselenggarakan oleh EsLaRed) yang disediakan di beberapa negara di seluruh Amerika Latin. Dengan demikian, tidak sulit untuk meyakinkan Dr Sandro Radicella, kepala dari Laboratorium Aeronomy dan Propagasi Radio di ICTP, untuk mendukung perjalanan Carlo Fonda di awal April ke Venezuela untuk berpartisipasi dalam percobaan. Kembali di rumah, saya menemukan parabolic mesh 2,75 m dengan fed di tengah di rumah tetangga. Bapak Ismael Santos meminjamkan antenna tersebut untuk percobaan.

Gambar 11.30 menunjukkan pembongkaran mesh reflektor.

Gambar 11,30: Carlo dan Ermanno membongkar antene parabola yang dipinjamkan oleh Bapak Ismael Santos.

Kami mengubah feed untuk 2,4 GHz, dan mengarahkan ke sebuah sinyal generator yang berada di atas tangga sekitar 30 m jauh. Dengan spektrum analisa, kami mengukur bahwa maksimum sinyal terletak di fokus. Kami juga menentukan boresight untuk kedua antenna

baik cental fed maupun offset antenna. Hal ini ditunjukkan dalam **Gambar 11.31:**

Gambar 11.31: Mencari fokus dari antena dengan 2,4 GHz feed

Kami juga dibandingkan kekuatan sinyal yang diterima dengan output dari sebuah komersial 24 dBi antena. Ini menunjukkan perbedaan 8 dB, yang menyebabkan kami percaya bahwa penguatan keseluruhan antena adalah 32 dBi. Tentu saja, terdapat beberapa ketidakpastian tentang nilai ini. Kami telah menerima sinyal yang di pantulkan, tetapi nilainya sesuai dengan perhitungan dari dimensi antena.

El Baúl situs survey

Setelah kami puas dengan fungsi dan arah dari kedua antena, kami memutuskan untuk melakukan site survey ke ujung dari sambungan El Baúl. Carlo Fonda, Gaya Fior dan Ermanno Pietrosemoli mencapai lokasi pada 8 April. Hari berikutnya, kami menemukan bukit (selatan kota) dengan dua menara telekomunikasi dari dua operator selular dan satu milik walikota El Baúl. Bukit Morrocoy sekitar 75 m di atas wilayah sekitarnya, sekitar 125 m di atas permukaan laut. Memberikan pemandangann tanpa halangan ke arah El Aguila. Ada jalan setapak ke puncak, yang harus kami lalui untuk tujuan kami, mengingat berat antena.

Melakukan percobaan

Pada hari Rabu 12 April, Javier Triviño dan Ermanno Pietrosemoli pergi ke arah Baúl dengan antena offset yang dimuat di atas sebuah truk four-wheel drive. Pagi 13 April, antenna kami instal di arahkan dengan arah kompas 276 °, mengingat ada deklinasi 8 ° dan oleh karena itu Azimut yang benar adalah 268 °.

Pada saat yang sama, tim lain (terdiri dari Carlo Fonda dan Gaya Fior dari ICTP, dengan bantuan dari Franco Bellarosa, Lourdes Pietrosemoli dan José Triviño) menuju ke area yang pernah di survey sebelumnya di kawasan Pico del Aguila dalam truk Bronco yang membawa mesh antenna 2,7 m.

Gambar 11.32: Peta Pico del Águila dan sekitarnya dengan truk Bronco.

Cuaca buruk sangat umum di ketinggian 4.100 m di atas permukaan laut. Tim Aguila berhasil memasang dan mengarahkan antenna mesh sebelum kabut dan hujan es turun. **Gambar 11.33** menunjukan antena dan tali yang digunakan untuk mengarahkan pancaran radio 3°.

Daya untuk sinyal generator di ambil dari truk menggunakan inverter 12 VDC ke 120 VAC. Pada jam 11 pagi di El Baúl, kami mampu melihat sinyal -82 dBm yang disepakati di frekuensi 2450 MHz menggunakan spektrum analiser. Untuk memastikan kami telah menemukan sumber yang tepat, kami diminta Carlo untuk menonaktifkan sinyal. Betul, spektrum analiser hanya menunjukan hanya noise saja. Hal ini mengkonfirmasikan bahwa kami benar-benar melihat sinyal yang berasal dari jarak 280 km.

Setelah menyalakan sinyal generator lagi, kami melakukan tuning pada elevasi dan azimut pada kedua sisi. Setelah kami puas bahwa kami telah penerimaan sinyal maksimum, Carlo mengganti sinyal generator dengan Linksys WRT54G wireless router dikonfigurasi sebagai jalur akses. Javier digantikan dengan spektrum analiser di ujung lain dengan WRT54G dikonfigurasi sebagai klien.

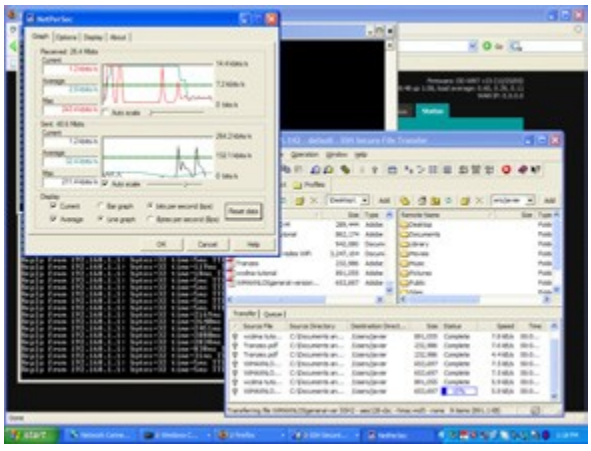
Gambar 11.33: Mengarahkan antenna di el Águila.

Sekaligus, kami mulai menerima "beacon" tapi paket ping tidak tembus. Hal ini dapat di

mengerti, karena waktu propagasi dari gelombang radio pada sambungan lebih dari 300 km adalah 1 ms. Butuh waktu setidaknya 2 ms untuk sebuah acknowledge untuk mencapai pemancar. Untungnya, OpenWRT firmware memungkinkan untuk menyesuaikan waktu ACK. Setelah Carlo menaikan delay waktu acknowledge menjadi 3 order magnitude di atas standar sambungan Wi-Fi, kami mulai menerima paket dengan penundaan sekitar 5 ms.

Gambar 11.34: Instalasi antenna El Baúl instalasi antena. Elevasi sebenarnya adalah 1 ° ke atas,karena antenna memiliki offset 22,5 °.

Kami meneruskan dengan mentransfer beberapa file PDF antara laptop Carlo dan Javier. Hasil akan ditampilkan dalam **Gambar 11.35.**



Gambar 11.35: Screenshot dari laptop Javier menampilkan rincian transfer file PDF dari laptop Carlo pada jarak 280 km, menggunakan dua router nirkabel WRT54G, tanpa Amplifier.

Perlu di catat bahwa waktu ping adalah beberapa milidetik.

Gambar 11.36: Javier Triviño (kanan) dan Ermanno Pietrosemoli mengarahkan antenna El Baúl

Gambar 11.37: Carlo Fonda di lokasi Aguila

Mérida, Venezuela, 17 April 2006

Satu tahun setelah melakukan percobaan ini, kami menemukan waktu dan sumber daya untuk mengulang itu. Kami digunakan antena komersial 30 dBi, dan juga beberapa router wireless yang telah dimodifikasi oleh group TIER yang dipimpin oleh Dr. Eric Brewer dari Berkeley University.

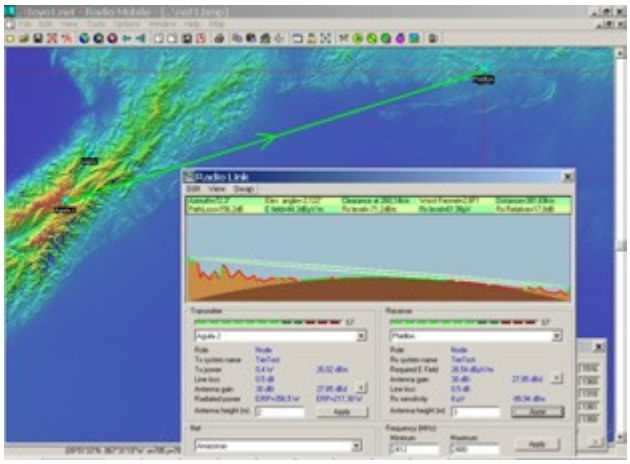
Tujuan dari modifikasi pada WiFi MAC standard adalah agar cocok untuk aplikasi jarak jauh degan cara menggantikan CSMA Media Access Control dengan TDMA. Yang terakhir lebih sesuai untuk sambungan jarak jauh point-to-point karena tidak memerlukan penerimaan ACK. Hal ini menghilangkan kebutuhan untuk menunggu 2ms waktu propagasi round trip pada path 300 km.

Pada tanggal 28 April 2007, sebuah tim dibentuk oleh Javier Triviño, José Torres dan Francisco Torres menginstalasi satu antenna di lokasi El Aguila. Tim lain, terdiri dari Leonardo González V., Leonardo González G., Alejandro González dan Ermanno Pietrosemoli, memasang antenna lainnya di El Baúl.

Sebuah sambungan yang solid berhasil dibentuk dengan cepat menggunakan router Linksys WRT54G. Hal ini memungkinkan pengiriman video dengan throughput 65 kbps. Dengan router TDMA, throughput yang terukur adalah 3 Mbps di setiap arah. Hal ini menghasilkan total 6 Mbps sebagaimana di prediksi oleh simulasi yang dilakukan di Berkeley.

Dapat kami lakukan lebih baik?

Kagum dengan hasil ini, yang telah membuka jalan untuk membuat sambungan jarak jauh broadband yang murah, kedua tim dipindahkan ke lokasi lain sebelumnya diidentifikasi di 382 km dari El Aguila, di tempat disebut Platillón. Platillón adalah 1.500 m di atas permukaan laut dan tidak halangan di zone Fresnel pertama terhadap El Aguila (terletak pada 4200 m di atas permukaan laut). Usulan path ditunjukkan pada **Gambar 11.38:**



Gambar 11.38: Peta dan profil dari path 380 km.

Sekali lagi, sambungan terbentuk dengan cepat menggunakan router Linksys TIER. Sambungan pada Linksys menunjukkan hanya sekitar 1% paket loss, dengan rata-rata round trip time (RTT) hanya 12 ms. Peralatan TIER menunjukkan tidak ada paket loss, dengan waktu propagasi di bawah 1 ms. Hal ini memungkinkan transmisi video, tetapi sambungan tidak stabil. Kami memperhatikan fluktuasi sinyal yang sering memutuskan komunikasi. Namun, jika sinyal yang di terima sekitar -78 dBm, throughput yang di ukut adalah total 6 Mbps bidirectional dengan router TIER yang menerapkan TDMA.

Gambar 11.39: Tim di el Aguila, José Torres (kiri), Javier Triviño (tengah) dan Francisco Torres (kanan)

Meskipun tes lebih lanjut harus dilakukan untuk memastikan batas untuk throughput yang stabil, kami yakin bahwa Wi-Fi memiliki potensi besar untuk komunikasi broadband jarak jauh. Hal ini terutama cocok untuk daerah pedesaan karena spektrum tidak ramai dan gangguan tidak menjadi masalah, asalkan ada radio line of sight yang baik.

Ucapan Terima Kasih

Kami ingin menyampaikan rasa terima kasih kami kepada Bapak Ismael Santos untuk pinjaman mesh antena yang dipasang di El Aguila dan untuk Eng. Andrés Pietrosemoli untuk penyediaan kontruksi untuk instalasi dan transportasi dari antena. Kami juga mengucapkan terima kasih kepada pihak Abdus Salam Internasional Center of Fisika Teoretis untuk mendukung perjalanan Carlo Fonda dari Italia ke Venezuela.

Gambar 11.40: Tim di Platillon. Dari kiri ke kanan: Leonardo González V., Leonardo González G., Ermanno Pietrosemoli danAlejandro González.

Percobaan di tahun 2006 dilakukan oleh Ermanno Pietrosemoli, Javier Triviño dari EsLaRed, Carlo Fonda, dan Gaya Fior dari ICTP. Dengan bantuan Franco dari Bellarosa, Lourdes Pietrosemoli, dan José Triviño. Untuk experimen di tahun 2007, Dr. Eric Brewer dari University Berkeley yang menyediaan wireless router dengan MAC yang dimodifikasi untuk jarak jauh, serta dukungan yang sangat antusias melalui kolaborasi, Sonesh Surana. RedULA, CPTM, Dirección de Pelayanan ULA Universidad de los Andes dan kontribusi Fundacite Mérida untuk percobaan ini.

Pekerjaan ini didanai oleh AKI-IDRC.

Referensi

- Fundación Escuela Latinoamericana de Redes, Latin American Networking School, http://www.eslared.org.ve/
- Abdus Salam International Centre for Theoretical Physics, http://wireless.ictp.it/
- OpenWRT Open Source firmware for Linksys, http://openwrt.org/
- Fundacite Mérida, http://www.funmrd.gov.ve/

-- Ermanno Pietrosemoli

Appendix A: Sumber-sumber

Kami merekomendasikan sumber-sumber ini untuk mempelajari lebih banyak mengenai berbagai aspek pembuatan jaringan nirkabel. Untuk tambahan link dan sumber, lihat website kami di: http://wndw.net/.

Antena dan disain antena

- Makalah teknis Cushcraft pada disain antena dan propagasi radio, http://www.cushcraft.com/comm/support/technical-papers.htm
- Disain antena gratis , http://www.freeantennas.com/
- Hyperlink Tech, http://hyperlinktech.com/
- Pasadena Networks, LLC, http://www.wlanparts.com/
- SuperPass, http://www.superpass.com/
- Arsip kode NEC2 yang tidak resmi, http://www.nec2.org/
- Situs alat modeling radio NEC2 yang tidak resmi, http://www.nittany-scientific.com/nec/
- Disain parabola WiFi USB, http://www.usbwifi.orcon.net.nz/

Alat troubleshooting jaringan

- Alat pengukur throughput bing, http://fgouget.free.fr/bing/index-en.shtml
- Paket pemantauan jaringan Cacti, http://www.cacti.net
- Tes kecepatan bandwidth laporan DSL, http://www.dslreports.com/stest
- Alat spectrum analyzer EaKiu, http://www.cookwareinc.com/EaKiu/
- Pemantau trafik jaringan Ether Ape, http://etherape.sourceforge.net/
- Kolektor NetFlow open source Flowc, http://netacad.kiev.ua/flowc/
- Alat uji kinerja jaringan Iperf, http://dast.nlanr.net/Projects/Iperf/
- Alat diagnostik jaringan iptraf, http://iptraf.seul.org/
- Alat penggambar dan pemantauan jaringan MRTG, http://people.ee.ethz.ch/~oetiker/webtools/mrtg/
- Alat diagnostik jaringan My TraceRoute, http://www.bitwizard.nl/mtr/

- Alat pengumuman event dan pemantauan jaringan Nagios, http://www.nagios.org/
- NetFlowm protocol Cisco untuk mengumpulkan informasi trafik IP, http://en.wikipedia.org/wiki/Netflow
- Utilitas keamanan jaringan ngrep untuk mencari pola dalam arus data, http://ngrep.sourceforge.net/
- Tutorial dan petunjuk implementasi pemantauan jaringan, http://wiki.debian.org/Network_Monitoring
- Alat pemantauan jaringan Ntop, http://www.ntop.org/
- Utilitas gambar database robin bundar RRDtool, http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/
- Pemantau kehilangan paket dan latensi jaringan SmokePing, http://people.ee.ethz.ch/~oetiker/webtools/smokeping/
- Alat analisa jaringan SoftPerfect, http://www.softperfect.com/
- Proxy http transparan HOWTO Squid, http://tldp.org/HOWTO/TransparentProxy.html
- Alat uji kinerja jaringan ttcp, http://ftp.arl.mil/ftp/pub/ttcp/
- Analyzer protocol jaringan Wireshark, http://www.wireshark.org/

Keamanan

- Informasi dan alat bypass proxy http AntiProxy, http://www.antiproxy.com/
- Alat Anti-spyware, http://www.spychecker.com/
- Utilitas pemantauan jaringan Driftnet, http://www.ex-parrot.com/~chris/driftnet/
- Utilitas pemantauan jaringan Etherpeg, http://www.etherpeg.org/
- Pengenalan kepada OpenVPN, http://www.linuxjournal.com/article/7949
- Alat penghapus spyware Ad-Aware Lavasoft, http://www.lavasoft.de/
- Piranti lunak admin dan keamanan Linux, http://www.linux.org/apps/all/Networking/Security_/_Admin.html
- Alat tunneling dan shell aman Open SSH, http://openssh.org/
- Petunjuk setup tunnel terenkripsi OpenVPN, http://openvpn.net/howto.html
- Proxy web filterisasi Privoxy, http://www.privoxy.org/

- Klien SSH PuTTY untuk Windows, http://www.putty.nl/
- Analyzer log Sawmill, http://www.sawmill.net/
- Keamanan algoritma WEP, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
- Wrapper SSL Universal Stunnel, http://www.stunnel.org/
- Router onion TOR, http://www.torproject.org/
- Kelemahan dalam Algoritma Penjadwalan Kunci RC4, http://www.crypto.com/papers/others/rc4_ksaproc.ps
- Klien SCP Windows, http://winscp.net/
- Jaringan Nirkabel 802.11 anda tidak mempunyai Baju, http://www.cs.umd.edu/~waa/wireless.pdf
- Firewall personal ZoneAlarm untuk Windows, http://www.zonelabs.com/

Optimisasi bandwidth

- Hirarki cache dengan Squid, http://squid-docs.sourceforge.net/latest/html/c2075.html
- Penangkap DNS dan server DHCP dnsmasq, http://www.thekelleys.org.uk/dnsmasq/doc.html
- Mengembangkan Akses World Wide Web Internasional di Mozambique melalui penggunaan Mirroring dan Proxy Penangkap, http://www.isoc.org/inet97/ans97/cloet.htm
- Utilitas distribusi file Fluff, http://www.bristol.ac.uk/fluff/
- HOWTO kontrol trafik dan Routing Linux yang lebih baik, http://lartc.org/
- Server Percepatan dan Keamanan Internet Microsoft, http://www.microsoft.com/isaserver/
- Situs sumber Cache dan Firewall server ISA Microsoft, http://www.isaserver.org/
- Mengoptimisasi Bandwidth Internet pada Pendidikan Tinggi Negara Berkembang, http://www.inasp.info/pubs/bandwidth/index.html
- Petunjuk Pusat Supercomputing Pittsburgh untuk Memungkinkan Tranfer Data Berkinerja Tinggi, http://www.psc.edu/networking/perf_tune.html
- Blog Planet Malaysia mengenai manajemen bandwidth, http://planetmy.com/blog/?

p=148

- RFC 3135: Proxy Peningkat Kinerja yang ditujukan untuk Memperbaiki Degradasi berkaitan dengan Link, http://www.ietf.org/rfc/rfc3135
- Cache proxy web Squid, http://squid-cache.org/

Pembuatan jaringan mesh

- Piranti lunak Jaringan Nirkabel Komunitas Champaign-Urbana, http://cuwireless.net/download
- Firmware mesh OLSR Freifunk untuk LinksysWRT54G, http://www.freifunk.net/wiki/FreifunkFirmware
- Proyek Roofnet MIT, http://pdos.csail.mit.edu/roofnet/doku.php
- Daemon pembuatan jaringan mesh OLSR, http://www.olsr.org/
- Viewer topologi OLSR Waktu-nyata, http://meshcube.org/nylon/utils/olsr-topology-view.pl
- Router Mesh AirJialdi, http://drupal.airjaldi.com/node/9

Driver dan sistem operasi nirkabel

- Sistem operasi router nirkabel DD-WRT, http://www.dd-wrt.com/
- Driver nirkabel HostAP untuk Chipset Prism 2.5, http://hostap.epitest.fi/
- Sistem operasi router nirkabel mOnOwall, http://m0n0.ch/wall/
- Driver nirkabel MadWiFi untuk chipset Atheros, http://madwifi.org/
- Sistem operasi router nirkabel Metrix Pyramid, http://pyramid.metrix.net/
- Sistem operasi router nirkabel OpenWRT untuk titik akses Linksys, http://openwrt.org/
- Router nirkabel Tomato untuk titik akses Linksys, http://www.polarcloud.com/tomato

Alat nirkabel

- Portal captive Chillispot, http://www.chillispot.info/

- Utilitas Analisis Disain Jaringan Nirkabel Interaktif, http://www.qsl.net/n9zia/wireless/page09.html
- Pemantau nirkabel KisMAC untuk Mac OS X, http://kismac.macpirate.ch/
- Alat pemantauan jaringan nirkabel Kismet, http://www.kismetwireless.net/
- Alat deteksi jaringan nirkabel MacStumbler untuk Mac OS X, http://www.macstumbler.com/
- Alat deteksi jaringan nirkabel NetStumbler untuk Windows dan Pocket PC, http://www.netstumbler.com/
- Portal captive NoCatSplash, http://nocat.net/download/NoCatSplash/
- Sistem pemesanan tiket prabayar PHPMyPrePaid, http://sourceforge.net/projects/phpmyprepaid/
- Alat modeling kinerja radio RadioMobile, http://www.cplus.org/rmw/
- Alat perhitungan sambungan nirkabel Terabeam, http://www.terabeam.com/support/calculations/index.php
- Alat deteksi jaringan nirkabel Wellenreiter untuk Linux, http://www.wellenreiter.net/
- Portal captive WiFiDog, http://www.wifidog.org/
- Alat Analisa Sambungan Jaringan Nirkabel oleh GBPRR, http://my.athenet.net/~multiplx/cgi-bin/wireless.main.cgi

Informasi umum terkait nirkabel

- Tembakan jarak jauh WiFi DefCon, http://www.wifi-shootout.com/
- Design perangkat keras nirkabel homebrew, http://www.w1ghz.org/
- Informasi titik akses nirkabel Linksys, http://linksysinfo.org/
- Petunjuk sumber WRT54G Linksys, http://seattlewireless.net/index.cgi/LinksysWrt54g
- Grup komunitas nirkabel NoCat, http://nocat.net/
- Perangkat keras sambungan data optik Ronja, http://ronja.twibright.com/
- Grup nirkabel komunitas SeattleWireless, http://seattlewireless.net/
- Halaman perbandingan perangkat keras SeattleWireless, http://www.seattlewireless.net/HardwareComparison
- Kalkulator Daya Lewat Ethernet dari Stephen Foskett,http://www.gweep.net/~sfoskett/tech/poecalc.html

Layanan pembuatan jaringan

- ISP Access Kenya, http://www.accesskenya.com/
- Carrier broadband nirkabel Broadbank Access Ltd., http://www.blue.co.ke/
- Outsourcing Virtual IT, http://www.virtualit.biz/
- Layanan dan konsultasi wire.less.dk, http://wire.less.dk/

Pelatihan dan pendidikan

- Asosiasi untuk proyek konektifitas nirkabel Progressive Communications, http://www.apc.org/wireless/
- Jaringan International untuk Ketersediaan Publikasi Ilmiah, http://www.inasp.info/
- Universitas Makere, Uganda, http://www.makerere.ac.ug/
- Unit Komunikasi Radio Pusat Internasional Abdus Salam untuk Fisika Teoritis, http://wireless.ictp.trieste.it/
- Konferensi tingkat tinggi dunia pada infrastruktur informasi bebas, http://www.wsfii.org/

Link-link lainnya

- Lingkungan serupa Linux untuk Windows, http://www.cygwin.com/
- Alat visualisasi gambar Graphvis, http://www.graphviz.org/
- Simulator bandwidth ICTP, http://wireless.ictp.trieste.it/simulator/
- Perpustakaan dan alat manipulasi gambar ImageMagick, http://www.imagemagick.org/
- Database map pengendali perang NodeDB, http://www.nodedb.com/
- Database Open Relay, http://www.ordb.org/
- Alat partisi Image disk untuk Linux, http://www.partimage.org/
- RFC 1918: Alokasi alamat untuk Internet Privat, http://www.ietf.org/rfc/rfc1918
- Konsep Pembuatan jaringan Linux milik Rusty Russell, http://www.netfilter.org/documentation/HOWTO/ networking-concepts-HOWTO.html
- Linux Ubuntu, http://www.ubuntu.com/
- VoIP-4D Primer, http://www.it46.se/voip4d/voip4d.php
- Alat web wget untuk Windows, http://xoomer.virgilio.it/hherold/
- Database peta pengendali perang WiFiMaps, http://www.wifimaps.com/
- Alat analisis spektrum WiSpy, http://www.metageek.net/

Buku

- 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
- How To Accelerate Your Internet, A free book about bandwidth optimization. http://bwmo.net/. ISBN #978-0-9778093-1-8
- 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

Appendix B: Alokasi Kanal

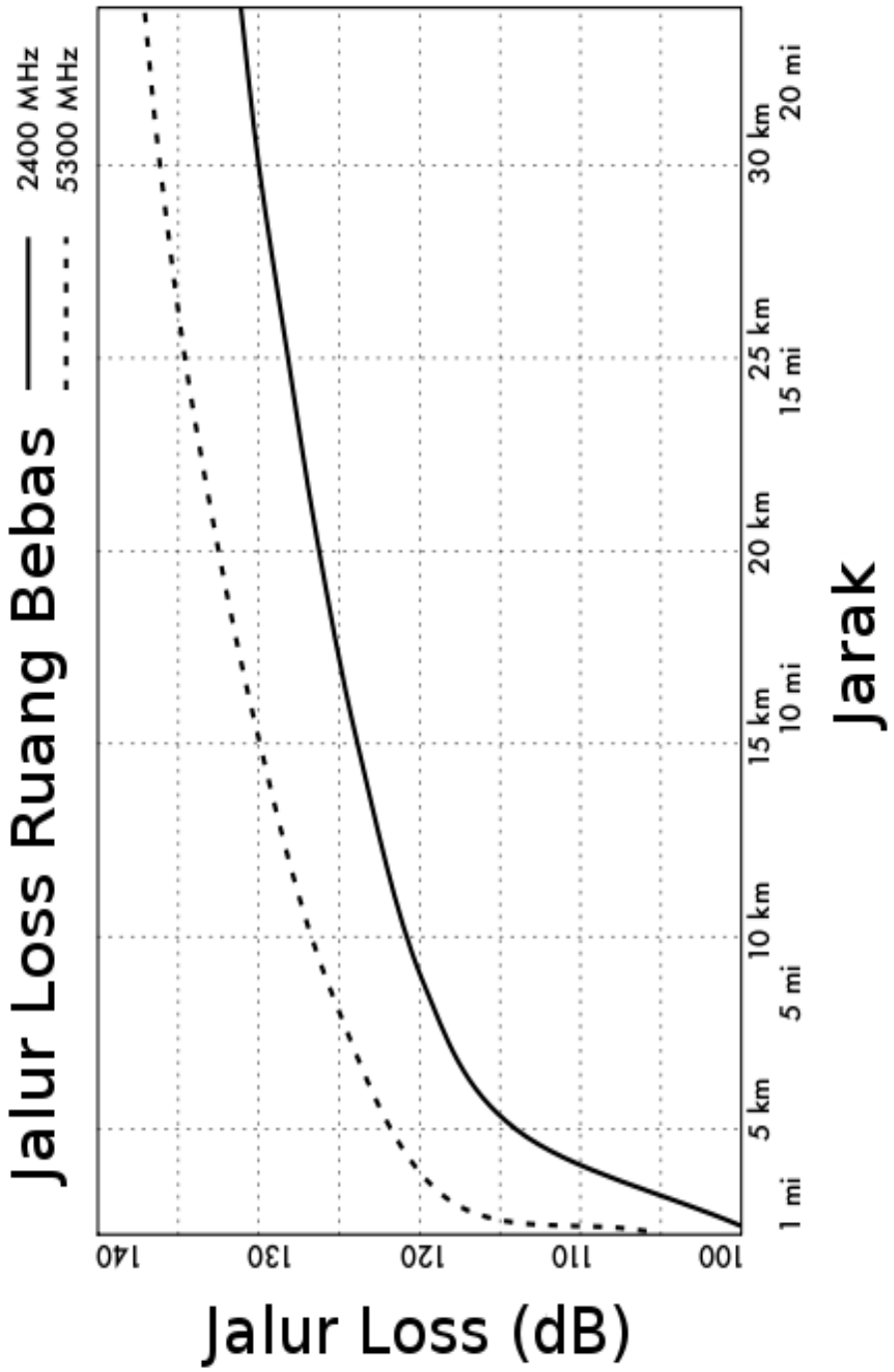
Tabel-tabel berikut menunjukkan nomor saluran dan frekuensi tengah untuk 802.11a dan 802.11 b/g. Perhatikan bahwa sementara semua frekuensi ini termasuk dalam ISM yang tidak berlisensi dan band U-NII, tidak semua saluran tersedia di semua negara. Banyak daerah memberlakukan larangan pada daya output dan penggunaan dalam ruang/ luar ruang pada beberapa saluran. Regulasi ini berubah secara cepat, sehingga selalu ceklah regulasi lokal sebelum memancarkan.

Perhatikan bahwa tabel-tabel ini menunjukkan frekuensi tengah untuk setiap saluran. Saluran selebar 22MHz pada 802.11b/g, dan 20MHz di 802.11a.

802.11b / g			
Saluran #	**Frekuensi Tengah (GHz)**	**Saluran #**	**Frekuensi Tengah (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

Saluran #	Frekuensi Tengah (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

Appendix C: Jalur Loss



Appendix D: Ukuran Kabel

Gauge kabel, diameter, kapasitas arus, dan resistansi di 20°C. Nilai-nilai ini dapat bervariasi dari kabel ke kabel. Jika ragu-ragu, konsultasikan spesifikasi pabrik.

AWG	Diameter (mm)	Ohms / Meter	Max 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

Appendix E: Perencanaan Sumber Daya Tenaga Surya

Gunakan tabel-tabel ini untuk mengumpulkan data yang diperlukan untuk memperkirakan ukuran sistem daya surya anda yang dibutuhkan.

Data umum

Nama tempat	
Garis lintang tempat (°)	

Data penyinaran

Gdm(0), in kWh / m2 per hari)

Jan	Feb	Mar	Apr	Mei	Jun	Jul	Agus	Sep	Okt	Nop	Des
Bulan penyinaran terburuk											

Kehandalan dan Tegangan Operasional Sistem

Hari otonomi (N)	
Tegangan Nominal (V_{NEquip})	

Karakter Komponen

Panel Surya	
Tegangan di Daya Maksimum (V_{pmax})	
Arus di Daya Maksimum (I_{pmax})	
Daya dan Tipe/Model Panel(W_p)	

Baterai

Kapasitas Nominal di 100 H (C_{NBat})	
Tegangan Nominal (V_{NBat})	
Kedalaman Maksimum Pengeluaran Daya (DoD_{MAX}) atau Kapasitas Berguna (C_{UBat})	
Regulator	
Tegangan Nominal (V_{NReg})	
Arus Maksimum (I_{maxReg})	

Inverter DC/AC (jika diperlukan)	
Tegangan Nominal (V_{NConv})	
Daya Seketika (P_{IConv})	
Kinerja di Beban 70%	

Beban

Daya yang Diperkirakan Dikonsumsi oleh Beban (DC)				
Bulan Konsumsi Terbesar				
Deskripsi	**Jumlah Unit**	**X Daya Nominal**	**X Penggunaan Jam / Hari**	**= Daya (Wh/hari)**
ETOTAL DC				

Daya yang Diperkirakan Dikonsumsi oleh Beban (AC)				
Bulan Konsumsi Terbesar				
Deskripsi	**Jumlah Unit**	**X Daya Nominal**	**X Penggunaan Jam / Hari**	**= Daya (Wh/hari)**

ETOTAL DC (sebelum konverter)				
ETOTAL AC (setelah konverter) = ETOTAL AC / 70%				

Mencari Bulan Terburuk

Nama Tempat												
Garis Lintang Tempat (°)												
Tegangan Nominal Instalasi V_N												
(Bulan)	**J**	**F**	**M**	**A**	**M**	**J**	**J**	**A**	**S**	**O**	**N**	**D**
Kemiringan ß												
G_{dm} (ß) (kWh/m2 x hari)												
E_{TOTAL} (DC) (Wh/hari)												
E_{TOTAL} (AC) (Wh/hari)												
E_{TOTAL} (AC +DC) =												
I_m (A) = E_{TOTAL} (Wh/hari) x 1kW/m2/ (G_{dm}(ß) x V_N)												

Rangkuman Bulan Terburuk	
Bulan Terburuk	
I_m (A)	
I_{mMAX} (A) = 1,21 x I_m	
E_{TOTAL} (AC +DC)	

Perhitungan Akhir

Panel		
Panel dalam Rentetan (N_{PS})	**N_{PS} = V_N /V_{pmax} =**	
Panel dalam Paralel (N_{PP})	**N_{PP} = I_{mMAX} / I_{pmax} =**	
Jumlah Total Panel	**N_{TOT} = N_{PS} x N_{PP} =**	

Baterai

Kapasitas yang diperlukan (C_{NEC})	**E_{TOTAL} (BULAN TERBURUK) / V_N x N**	
Kapasitas Nominal (C_{NOM})	**C_{NEC} /DoD_{MAX}**	
Jumlah Baterai dalam rentetan (N_{BS})	**V_N /V_{NBAT}**	

Kabel			
	Panel > Baterai	**Baterai > Konverter**	**Kabel Utama**
Penurunan Tegangan (Va - Vb)			
Ketebalan (Bagian) r x L x ImMAX / (Va - Vb)			

Untuk perhitungan ketebalan kabel, r = 0.01286 Ω mm2/m (untuk tembaga) dan L adalah panjang dalam meter.

Daftar Istilah

0-9

802.11. Walaupun 802.11 sendirinya adalah sebuah protokol wireless, 802.11 seringkali digunakan untuk merujuk pada sekelompok protokol jaringan wireless yang digunakan pada umumnya untuk pembuatan jaringan area lokal. Tiga varian yang terkenal termasuk 802.11b, 802.11g, dan 802.11a. Lihat juga: ***Wi-Fi.***

A

AC lihat Alternating Current

Akses Point (Access Point). Sebuah alat yang menciptakan jaringan wireless yang biasanya tersambung dengan jaringan Ethernet. Lihat juga CPE, master mode.

Akumulator (Accumulator). Sebuah nama lain untuk baterai.

Mode ad-hoc (Ad-hoc mode). Sebuah mode radio yang digunakan oleh peralatan 802.11 yang memungkinkan terciptanya sebuah jaringan tanpa titik akses. Jaringan mesh biasanya menggunakan radio dalam mode ad-hoc. Lihat juga: managed mode, master mode, monitor mode.

Address Resolution Protokol (Address Resolution Protocol atau ARP). Sebuah protokol yang secara luas digunakan pada jaringan Ethernet untuk menerjemahkan alamat IP ke alamat MAC.

Ruang alamat (address space). Sebuah grup alamat IP yang menetap di subnet lojikyang sama.

Jendela yang di sarankan (advertised window). Porsi header TCP yang memspesifikasi seberapa banyak tambahan byte data yang dapat diterima oleh receiver.

Arus bolak balik (Alternating Current atau AC). Arus listrik yang bervariasi sepanjang waktu dalam pola siklis. Arus bolak balik biasanya digunakan untuk penerangan dan alat-alat.

Amortisasi (Amortization). Sebuah teknik akuntansi yang digunakan untuk mengatur perkiraan biaya penggantian dan keusangan alat dalam waktu tertentu.

Amplifier (Amplifier). Sebuah alat yang digunakan untuk menambah daya alat wireless yang dipancarkan.

Amplitudo (Amplitude). Jarak dari tengah gelombang ke yang bagian ekstrim dari salah satu puncaknya.

Pengguna utama (anchor clients). Pengguna bisnis sistem langganan yang dapat dihandalkan dan dianggap berisiko kecil.

Logika AND (AND logic). Operasi logika yang hanya mengevaluasi sebagai sesuatu yang benar jika semua yang dibandingkan juga benar. Lihat juga: OR logic.

Proxy penyembunyi nama (anonymizing proxy). Service jaringan yang menyembunyikan sumber tujuan komunikasi. Proxy penyembunyian nama dapat digunakan untuk melindungi privasi orang dan untuk mengurangi keterbukaan sebuah lembaga terhadap tanggung jawab hukum atas tindakan penggunanya.

Kerahasiaan nama (anonymity). Dalam jaringan komputer, komunikasi yang tidak dapat dihubungkan dengan individu unik bisa disebut keadaan tanpa nama. Nilai timbal balik keadaan tanpa nama terhadap akuntabilitas dalam komunikasi adalah debat online secara terus menerus, dan peraturan mengenai komunikasi tanpa nama bervariasi secara luas di dunia. Lihat juga: authenticated

Antena Diversity (Antenna Diversity). Sebuah teknik yang digunakan untuk mengatasi gangguan multijalur dengan menggunakan dua atau lebih antena penerima yang dipisahkan secara fisik.

Penguatan Antena (Antenna gain). Jumlah daya yang terkonsentrasikan dalam arah radiasi terkuat antena, yang biasanya diekspersikan dalam dBi. Gain antena bertimbal balik, yang artinya efek gain ada pada saat pemancaraan serta penerimaan.

Pola Radiasi Antena (Antenna pattern). Gambar yang mendeskripsikan kekuatan relatif bidang yang diradiasikan dalam berbagai arah dari antena. Lihat juga: rectangular plot, polar plot, linear plot, coordinates, logarithmic polar coordinates

AP lihat Access Point

Lapisan aplikasi (Application layer). Lapisan teratas dalam model jaringan OSI dan TCP/IP.

Argus lihat Audit Record Generation and Utilization System

ARP lihat Address Resolution Protocol

Berasosiasi (associated). Radio 802.11 diasosiasikan dengan titik akses ketika radio itu siap untuk berkomunikasi dengan jaringan. Ini artinya radio tersebut dituning pada saluran yang sesuai, dalam jangkauan AP, menggunakan SSID yang benar dan paramater otentikasi yang benar, dll.

At. Fasilitas Unix yang memungkinkan eksekusi program yang hanya sekali dan diwaktukan. Lihat juga: cron

Atenuasi (attenuation). Pengurangan ketersediaan daya radio karena terabsorbsi sepanjang jalur, seperti melalui pohon, tembok, gedung, dan obyek lainnya. Liha juat: free space loss, scattering

Pembuatan Catatan Audit dan Sistem Utilisasi (Audit Record Generation and Utilization System atau Argus). Sebuah alat pemantauan jaringan open source yang digunakan untuk mengikuti arus antara host. Argus tersedia dari http://www.qosient.com/argus.

Terotentikasi (authenticated). Pengguna jaringan yang telah membuktikan identitasnya kepada sebuah layanan atau alat (misalnya titik akses), biasanya dengan cara kriptografi. Lihat juga: anonymity

azimut (azimuth). Sudut yang mengukur deviasi terkait Selatan di belahan Utara, dan terkait Utara di belahan Selatan. Lihat juga: inclination

B

bandwidth. Pengukuran frekuensi, yang biasanya digunakan untuk komunikasi digital. Kata bandwidth juga biasanya digunakan dengan kapasitas untuk merujuk pada laju data maksimum teoritis jalur komunikasi digital. Lihat juga: capacity, channel, througput

Baterai (battery). Alat yang digunakan untuk menyimpan daya dalam sistem fotovoltaik. Lihat juga: panel solar, regulator, load, converter, inverter

lebar beam (beamwidth). Jarak bersudut antara titik-titik di kedua sisi lobe utama antena, dimana daya yang diterima adalah setengah dari daya lobe utama. Lebar beam antena biasanya dinyatakan untuk bidang horizontal dan vertikal.

Benchmarking. Mengetes kinerja maksimum layanan atau alat. Benchmarking sebuah sambungan jaringan biasanya meliputi membanjiri sambungan itu dengan trafik dan mengukur througput, baik pada pemancaran dan penerimaan.

BGAN lihat Broadband Global Access Network.

Konektor BNC. Konektor kabel koaksial yang menggunakan uliran bayonet menghubungkan/ melepaskan secara cepat. Pada umumnya, mereka ditemukan pada perlengkapan tes dan kabel coaxial ethernet 10base2.

Bridge. Alat jaringan yang menyambungkan dua jaringan di lapisan sambungan data (data

link layer). Bridge tidak mengroute paket di lapisan jaringan (network layer). Mereka secara sederhana mengulang paket antara dua jaringan sambungan lokal (link-local). Lihat juga router dan firewall bridging tranparan (transparent bridging firewall).

Bridge utils. Paket piranti lunak Linux yang dibutuhkan untuk menciptakan bridge Ethernet 802.1d. Http://birdge.sourceforge.net/

Jaringan Akses Global Pita Lebar (Broadband Global Access Network atau BGAN). Satu dari beberapa standar yang digunakan untuk akses Internet satelit. Lihat juga: Digital Video Broadcast (DVB-S) dan Very Small Aperture Terminal (VSAT).

Alamat broadcast (broadcast address). Pada jaringan IP, alamat IP tayang digunakan untuk mengirim data ke semua host dalam subnet lokal. Pada jaringan Ethernet, alamat MAC tayang digunakan untuk mengirim data ke semua mesin dalam domain bentrokan yang sama.

Dioda bypass (bypass diodes). Fitur yang ditemukan pada beberapa panel surya yang mencegah terbentuknya hot-spots pada sel yang terteduh, namun mengurangi tegangan maksimum panel.

C

CA lihat Certificate Authority

Cacti (httpL//www.cacti.net). Alat pemantauan berbasis web yang populer dalam bahasa PHP.

Kapasitas (capacity). Jumlah maksimum teoritis trafik yang disediakan oleh jalur komunikasi digital. Seringkali disamakan dengan bandwidth.

Portal captive (captive portal). Mekanisme yang digunakan untuk secara transparan mengarahkan web browser ke lokasi baru. Portal captive seringkali digunakan untuk otentikasi atau untuk menyela sesi online seorang user (sebagai contoh, untuk menampakan Kebijakan Penggunaan yang Berlaku).

sel (cell). Panel surya dibuat dari beberapa sel individual, yang secara elektrik disambungkan untuk menyediakan nilai khusus arus dan tegangan. Baterai juga dibuat dari sel individual yang tersambung dalam rentetan, yang masing-masing memberikan kontribusi tegangan kira-kira 2 volt ke baterai.

Otoritas sertifikat (Certificate Authority). Entitas yang terpercaya yang mengeluarkan kunci kriptografis resmi. Lihat juga: Public Key Infrastructure, SSL

Kapasitas kanal (channel capacity). Jumlah maksimum informasi yang dapat dikirin menggunakan suatu bandwidth. Lihat juga: bandwidth, throughput, data rate.

Kanal (Channel). Jangkauan frekuensi yang terdefinisikan secara baik yang digunakan untuk komunikasi. Saluran 802.11 menggunakan 22 MHz bandwidth, namun hanya dipisahkan oleh 5 MHz. Lihat juga: Appendix B.

CIDR lihat Classless Inter-Domain Routing

Notasi CIDR (CIDR notation). Sebuah metode yang digunakan untuk mengdefinisikan mask jaringan dengan memspesifikasi jumlah bits yang ada. Sebagai contoh, netmask 255.255.255.0 dapat dispesifikasikan sebagai /24 dalam notasi CIDR.

Polarisasi sirkular (Circular polarization). Bidang elektro-magnetik dimana vektor bidang listrik tampil berputar dengan gerakan melingkari arah propagasi, yang membuat satu putaran penuh untuk setiap siklus RF. Lihat juga: horizontal polarization, vertical polarization.

Jaringan Kelas A, B dan C (Class A, B, and C networks). Untuk beberapa waktu, ruang alamat IP dialokasikan dalam blok tiga ukuran yang berbeda. Ini adalah Class A (sekitar 16 juta alamat), Class B (sekitar 65 ribu alamat), dan Class C (255 alamat). Sementara CIDR telah menggantikan alokasi berbasis kelas, kelas-kelas ini sering kali masih dirujuk dan digunakan secara internal dalam organisasi yang menggunakan ruang alamat privat. Lihat juga: CIDR notation.

Routing Inter-Domain tanpa kelas (Classless Inter-Domain Routing). CIDR dikembangkan untuk meningkatkan efisiensi routing pada backbone internet dengan memungkinkan pengumpulan rute dan mask jaringan ukuran seberapapun. CIDR menggantikan skema pengalamatan berbasis kelas yang lama. Lihat juga: Class A, B, and C networks.

Pengguna (client). Kartu radio 802.11 dalam mode yang sudah diatur atau managed mote. Pengguna wireless akan bergabung dengan jaringan yang diciptakan oleh titik akses, and secara otomatis mengganti saluran untuk menyamainya. Lihat juga: access point, mesh

Jaringan tertutup (closed network). Titik akses yang tidak menayangkan SSID-nya, seringkali digunakan sebagai tindakan keamanan.

Coax. Kabel (koaksial) yang bundar dengan bagian tengah kawat dikelilingi oleh dielektrik, konduktor luar, dan jaket insulasi yang kuat, Kabel antena biasanya terbuat dari coax. Coax adalah singkatan dari “of common axis” (sumbu yang sama).

Bentrokan (collision). Pada jaringan Ethernet, bentrokan terjadi ketika dua alat tersambung dengan segmen fisik yang sama mencoba untuk memancarkan di saat yang sama. Ketika bentrokan terdeteksi, alat menunda pemancaran ulang untuk periode yang sebentar yang dipilih secara serampangan.

Konduktor (conductor). Material yang secara mudah memungkinkan daya termal atau listrik

untuk mengalir tanpa banyak hambatan. Lihat juga: dielektrik, insulator

Protokol tanpa koneksi (connectionless protocol). Jaringan protocol (seperti UDP) yang tidak memerlukan permulaan sesi atau pemeliharaan. Protokol tanpa koneksi biasanya memerlukan sedikit biaya daripada protokol berorientasi sesi, namun biasanya tidak menyediakan perlindungan data atau pengaturan ulang paket. Lihat juga: session oriented protocol.

Platform yang konsisten (Consistent platform). Biaya pemeliharaan dapat dikurangi dengan menggunakan platform yang konsisten, dengan perangkat keras yang sama, dan firmware untuk beberapa komponen dalam jaringan.

Gangguan konstruktif (constructive interference). Ketika dua gelombang yang sama bersatu dan dalam fase yang sama, amplitudo gelombang yang dihasilkan dua kali lebih besar dari masing-masing komponen gelombang tersebut. Ini dinamakan gangguan konstruktif. Lihat juga: destructive interference.

Kontrol (controls). Dalam NEC2, kontrol mengdefinisikan sumber RF dalam model antena. Lihat juga: structure.

Konverter (converter). Alat yang digunakan untuk mengkonversikan sinyal DC menjadi tegangan DC atau AC yang berbeda. Lihat juga: inverter.

CPE lihat Customer Premises Equipment

cron. Fasilitas Unix yang mengijinkan pelaksanaan program yang berulang dan diwaktukan. Lihat juga: at

Peralatan Premis Pelanggan (Customer Premises Equipment). Peralatan jaringan (seperti router atau bridge) yang dipasang di lokasi pelanggan.

D

Lapisan sambungan data (data link layer). Lapisan kedua dalam baik model jaringan OSI maupun model jaringan TCP/IP. Komunikasi di lapisan ini terjadi secara langsung diantara node. Pada jaringan Ethernet, ini juga kadang dinamakan lapisan MAC.

Kecepatan data (data rate). Kecepatan dimana radio 802.11 bertukaran simbol, yang selalu lebih tinggi daripada throughput yang ada. Sebagai contoh, laju data nominal 802.11g adalah 54 Mbps, sedangkan throughput maksimum sekitar 20 Mbps). Lihat juga: throughput

dB lihat decibel

DC lihat Direct Current

Konverter DC/AC (DC/AC Converter). Alat yang merubah daya DC menjadi daya AC, cocok untuk penggunaan dengan banyak alat-alat. Ini juga dinamakan sebagai inverter.

Konverter DC/DC (DC/DC Converter). Alat yang merubah tegangan sumber daya DC. Lihat juga: linear conversion, switching conversion.

Desibel (dB). Unit logaritmik pengukuran yang mengekspresikan besarnya daya relatif terhadap tingkat referensi. Yang biasa digunakan adalah dBi (decibels relatif terhadap radiator isotropik) dan dBm (decibels relatif terhadap satu milliwatt).

Gateway default (default gateway). Ketika router menerima paket yang ditujukan untuk jaringan yang mana jaringan tersebut tidak memiliki rute yang eksplisit, paket diteruskan ke gateway konfigurasi semula . Gateway konfigurasi semula lalu mengulang proses, mungkin mengirim paket itu ke gateway konfigurasi semulanya, sampai paket itu mencapai tujuan akhirnya.

Rute default (default route). Rute jaringan yang menunjukkan gateway konfigurasi semula.

Penolakan Layanan (Denial of Service atau DoS). Serangan pada sumber jaringan, biasanya diperoleh dengan membanjiri jaringan dengan trafik atau mengeksploitasi bug dalam aplikasi atau protokol jaringan.

Depresiasi (Depreciation) Metode akuntansi yang digunakan untuk menghemat uang untuk menutupi biaya yang akhirnya akan muncul dari peralatan.

Gangguan destruktif (destructive interference). Ketika dua gelombang yang sama bersatu dan benar-benar di luar fase, amplitudo gelobang yang dihasilkan adalah nol. Ini dinamakan gangguan destruktif. Liha juga: constructive interference

DHCP lihat Dynamic Host Configuration Protocol

dielektrik (dielectric). Material non-konduktif yang memisahkan kawat konduktif dalam kabel.

Peta ketinggian Digital (Digital Elevation Map atau DEM). Data yang merepresentasikan ketinggian daerah untuk suatu area geografis. Peta ini digunakan oleh program seperti Radio Mobile untuk mengilustrasikan model propagasi elektromagnetik.

Penayangan Video Digital (Digital Video Broadcast (DVB-S). Satu dari beberapa standar yang digunakan untuk akses Internet satelit. Lihat juga: Broadband Global Access Network (BGAN) dan Very Small Aperture terminal (VSAT).

Antena dipole (dipole antena). Antena omnidirectional yang paling sederhana.

Arus Searah (Direct Current atau DC). Arus listrik yang tetap konstan sepanjang waktu. Arus DC ini biasanya digunakan untuk peralatan jaringan, seperti titik akses dan router. Lihat juga: Alternating Current.

Direct Squence Spread Spectrum (Direct Sequence Spread Spectrum atau DSSS). Skema modulasi radio yang digunakan oleh 802.11b.

Antenna Pengarah (Directional antena). Antena yang beradiasi secara kuat dalam sebuah arah tertentu. Contoh directional antenna termasuk yagi, parabola, dan antena pandu gelombang. Lihat juga: omnidirectional antenna, sectorial antenna

Pengarahan (Directivity) adalah kemampuan antena untuk memusatkan energi di arah yang tertentu sewaktu memancarkan, atau untuk menerima energi dari arah yang tertentu sewaktu menerima, atau untuk menerima energi dari arah tertentu ketika menerima.

Diversity lihat antenna diversity

DNS lihat Domain Name Service

Penyimpanan DNS (DNS caching). Dengan memasang server DNS pada LAN lokal anda, permintaan DNS untuk seluruh jaringan mungkin dapat disimpan secara lokal , sehingga meningkatkan waktu tanggapan. Teknik ini disebut DNS caching.

Dnsmasq. Server DHCP dan penyimpanan DNS open source, tersedia di http://thekelleys.org.uk/

Layanan Nama Domain (Domain Name Service atau DNS). Protokol jaringan yang biasanya digunakan secara luas yang memetakan alamat IP ke nama.

Mode dominan (dominant mode). Frekuensi terendah yang dapat dipancarkan oleh pandu gelombang suatu ukuran.

DoS lihat Denial of Service

DSSS lihat Direct Sequence Spread Spectrum

DVB-S lihat Digital Video Broadcast.

Dynamic Host Configuration Protocol (Dynamic Host Configuration Protocol atau DHCP). Protokol yang digunakan oleh host untuk secara otomatis menentukan alamat IP mereka.

E

Mengintip yang tidak diketahui (eavesdropper). Seseorang yang mencegat data jaringan seperti password, email, data suara, atau chat online.

Tepi (edge). Tempat dimana satu jaringan milik organisasi bertemu dengan yang lainnya. Tepi didefinisikan oleh lokasi router external, yang sering kali bertindak sebagai firewall.

Spektrum elektromagnetik (electromagnetic spectrum). Jangkauan luas frekuensi energi elektromagnetik. Bagian-bagian elektromagnetik termasuk radio, microwave, cahaya yang kelihatan, dan X-ray.

Gelombang elektromagnetik (electromagnetic wave). Gelombang yang berpropagasi melalui ruang bebas tanpa perlu menggunakan media propagasi. Gelombang ini meliputi komponen listrik dan magnetik. Lihat juga: mechanical wave.

Ketinggian (Elevation) lihat inclination

Penyuntik jengkal akhir (end span injectors). Alat Power over Ethernet 802.3af yang menyediakan daya melalui kabel Ethernet. Switch ethernet yang menyediakan daya pada setiap port adalah contoh dari penyuntik jengkal akhir. Lihat juga: mid span injectors.

Enkripsi ujung-ke-ujung (end-to-end encryption). Koneksi terenkrip yang dinegosiasikan oleh kedua ujung sesi komunikasi. Enkripsi ujung-ke-ujung dapat menyediakan perlindungan yang lebih kuat daripada link layer encryption ketika digunakan pada jaringan yang tidak dipercaya (seperti Internet).

EtherApe. Alat visualisasi jaringan open source. Tersedia di http://etherape.sourceforge.net/

Ethereal lihat Wireshark

Extended Service Set Identifier (ESSID). Nama yang digunakan untuk mengidentifikasi jaringan 802.11. Lihat juga: closed network.

Trafik eksternal (external traffic). Trafik jaringan yang berasal dari, atau ditujukan pada, alamat IP diluar jaringan internal anda, seperti trafik Internet.

F

Firestarter. Grafis front-end untuk mengkonfigurasi firewall Linux yang tersedia di http://www.fs-security.com/

Filter (filter). Tabel default yang digunakan dalam sistem firewall netfilter Linux adalah tabel filter. Tabel ini digunakan untuk menentukan trafik yang harus diterima atau ditolak.

Firewall. Router yang menerima atau menolak trafik berdasarkan beberapa kriteria. Firewall

adalah alat dasar yang digunakan untuk melindungi seluruh jaringan dari trafik yang tidak diinginkan.

Membuang (flush). Untuk membersihkan semua catatan dalam tabel routing atau netfilter chain.

Penerusan (forwarding). Pada saat router menerima paket yang ditujukan untuk host atau jaringan yang berbeda, mereka mengirim paket ke router berikut yang paling dekat dengan tujuan akhirnya. Proses ini dinamakan forwarding.

Loop penerusan (forwarding loops). Konfigurasi routing yang salah dimana paket diteruskan secara bersiklus antara dua router atau lebih. Kegagalan jaringan yang fatal dicegah dengan menggunakan nilai TTL pada setiap paket, namun loop penerusan harus diatur untuk operasi jaringan yang baik.

Loss di udara (Free space loss). Daya yang dikurangi oleh penyebaran geometris bagian muka gelombang, karena gelombang tersebut berpropagasi melalui ruang. Lihat juga: attenuation, free space loss, Appendix C

Frekuensi (frequency). Jumlah gelombang penuh yang berhasil melewati titik yang tetap dalam periode waktu tertentu. Lihat juga: wavelength, Hertz

Perbandingan depan-ke-belakang (front-to-back ratio). Rasio directivity maksimum antena terhadap directivity pada arah berlawanan.

Duplex penuh (full duplex). Alat komunikasi yang dapat mengirim dan menerima di saat yang sama (seperti telepon). Lihat juga: half duplex.

Fwbuilder. Alat grafis yang memungkinkan anda untuk membuat skrip iptables pada mesin yang terpisah dari server anda, dan kemudian memindahkan mereka ke server tersebut. Http://www.fwbuilder.org/

G

Gain. Kemampuan komponen radio (seperti antena atau amplifier) untuk menambah daya sinyal. Lihat juga: Decibel.

Perpindahan gain (Gain transfer). Membandingkan antena yang sedang dites dengan antena yang umum yang standar, yang memiliki gain terkalibrasi.

Pembuatan gas (gasification). Pembuatan gelembung oksigen dan hidrogen yang terjadi pada saat baterai mengalami pengeluaran daya yang berlebihan.

Routable secara global (Globally routable). Alamat yang diberikan oleh ISP atau RIR yang dapat dicapai dari titik manapun di Internet. Dalam Ipv4, ada kurang lebih 4 milyar alamat IP yang mungkin, walaupun tidak semuanya routable secara global.

H

Duplex setengah (half duplex). Alat komunikasi yang dapat mengirim atau menerima, namun tidak pernah keduanya sekaligus (seperti radio genggam). Lihat juga: full duplex.

Heliax. Kabel koaksial berkualitas tinggi yang memiliki konduktor tengah yang solid dan tubular dengan konduktor luar yang solid dan corrugated yang memungkinkannya untuk fleksibel. Lihat juga: coax.

Hertz (Hz). Ukuran frekuensi, diartikan sebagai sejumlah siklus per detik.

Frekuensi-Tinggi (High-Frequency atau HF). Gelombang radio dari 3 sampai 30 MHz dirujuk sebagai HF. Jaringan data dapat dibuat berdasarkan pada HF yang beroperasi di jangkauan yang sangat panjang, namun dengan kapasitas data yang sangat rendah.

Lompatan (Hop). Data yang melewati satu koneksi jaringan. Server web mungkin beberapa hop dari komputer lokal anda, karena paket diteruskan dari router ke router, yang akhirnya mencapai tujuan akhir mereka.

Polarisasi horizontal (horizontal polarization). Bidang elektromagnetik dengan komponen listrik yang bergerak dalam arah horizontal yang linear. Lihat juga: circular polarization, vertical polarization

hot-spot. Dalam jaringan wireless, hot-spot adalah lokasi yang menyediakan akses Internet melalui Wi-Fi, yang biasanya menggunakan captive portal. Dalam photovoltaic systems, hot-spot terjadi pada saat sel tunggal dalam panel surya tertutup bayangan, yang menyebabkannya untuk bertindak sebagai beban hambatan daripada membangkitkan daya.

Hub. Alat pembuatan jaringan Ethernet yang mengulangi data yang diterima pada semua port yang tersambung. Lihat juga: switch.

Prinsip Huygens (Huygens principle). Model gelombang yang menganjurkan jumlah wavefront yang berpotensi yang tidak terbatas sepanjang setiap titik wavefront yang mendekat.

Hz lihat Hertz

I

IANA lihat Internet Assigned Numbers Authority

ICMP lihat Internet Control Message Protocol

ICP lihat Inter-Cache Protocol

Impedansi (impedance). Quotient tegangan terhadap arus jalur transmisi, yang terdiri dari hambatan dan reaktansi. Impedansi beban harus sama dengan impedansi sumber untuk perpindahan daya maksimum (50Ω untuk kebanyakan alat komunikasi).

Trafik inbound (inbound traffic). Paket jaringan yang berasal dari luar jaringan lokal (biasanya Internet) dan ditujukan pada tujuan di dalam jaringan lokal. Lihat juga: outbound traffic.

Kemiringan (inclination). Sudut yang menunjukan deviasi dari bidang horizontal. Lihat juga: azimuth.

Mode infrastruktur (Infrastructure mode) lihat master mode

Insulator lihat dielectric

Inter-Cache Protocol (Inter-Cache Protocol atau ICP). Protokol kinerja yang tinggi yang digunakan untuk berkomunikasi antara cache web.

Internet Assigned Numbers Authority (Internet Assigned Numbers Authority atau IANA). Organisasi yang mengelola berbagai bagian penting infrastruktur Internet, termasuk alokasi alamat IP, DNS root name servers, dan angka layanan protokol.

Internet Control Message Protocol (Internet Control Message Protocol atau ICMP). Protokol Lapisan jaringan yang digunakan untuk menginformasikan node mengenai keadaan jaringan. ICMP adalah bagian suite protokol Internet. Lihat juga: Internet protocol suite.

Lapisan Internet (Internet layer) lihat network layer

Protokol Internet (Internet Protocol atau IP). Protokol lapisan jaringan yang biasanya paling sering digunakan. IP mengdefinisikan host dan jaringan yang membuat Internet global.

Keluarga Protokol Internet (Internet protocol suite atau TCP/IP). Kelompok protokol komunikasi yang membuat Internet. Beberapa dari protokol ini termasuk TCP, IP, ICMP, dan UDP. Juga dinamakan TCP/IP protocol suite, atau secara sederhana TCP/IP.

Sistem Deteksi Gangguan (Intrusion Detection System atau IDS). Program yang memantau jaringan trafik, mencari data atau pola tingkah laku yang mencurigakan. IDS dapat membuat catatan log, memberitahu administrator jaringan, atau mengambil aksi langsung dalam menanggapi trafik yang tidak diinginkan.

Inverter lihat DC/AC Converter.
IP lihat Internet Protokol

iproute2. Paket alat routing yang sangat maju, yang digunakan untuk membentuk trafik dan teknik berkembang lainnya. Tersedia di http://linux-net/osdl/org/

iptables. Perintah primer yang digunakan untuk memanipulasi aturan firewall netfilter.

Penyinaran (irradiance). Jumlah total daya surya yang menerangi suatu area, dalam W/m2

Pita ISM (ISM band). ISM adalah singkatan untuk Industrial (Industri), Scientific (Ilmiah), dan Medical (Medis). Pita ISM adalah satu set frekuensi radio yang dialokasikan oleh ITU untuk penggunaan tidak berlisensi.

Antena isotropik (isotropic antenna). Antena hipotetis yang secara merata mengdistribusikan daya ke segala arah, yang dikira-kira oleh dipole.

Kurva karakteristik IV (IV characteristic curve). Gambar yang merepresentasikan arus yang disediakan berdasarkan pada tegangan yang dibangkitkan untuk radiasi surya tertentu.

K

Knetfilter. Grafis depan-belakang untuk mengkonfigurasi firewall Linux. Tersedia di http://venom.oltrelinux.com/

Sesuatu yang baik yang diketahui (known good). Dalam troubleshooting, sesuatu yang baik yang diketahui adalah komponen apapn yang dapat digantikan untuk mengecek apakah kembarannya berada dalam kondisi yang baik dan berfungsi.

L

lag. Istilah umum yang digunakan untuk mengdeskripsikan jaringan dengan latensi tinggi.

Lambda (λ) lihat wavelength.

LAN lihat Local Area Network

latensi (latency). Jumlah waktu yang dibutuhkan paket untuk menelusuri sambungan jaringan. Latency seringkali (secara salah) digunakan dengan Round Trip Time (RTT), karena mengukur RTT koneksi area yang luas terlihat jelas dibanding dengan mengukur latensi sesungguhnya. Lihat juga: Round Trip Time.

Baterai timbal-asam (lead-acid batteries). Baterai yang meliputi dua elektroda timbal yang tenggelam dalam solusi elektrolitik air dan asam sulfurik. Lihat juga: stationary batteries

Waktu lease (lease time). Dalam DHCP, alamat IP diberikan untuk periode waktu yang terbatas, yang diketahui sebagai lease time. Setelah periode waktu ini habis, pengguna harus meminta kembali alamat IP yang baru dari server DHCP.

Garis pandang (Line of Sight atau LOS). Jika seseorang beridiri di titik A memiliki pandangan titik B yang tidak berhalangan, maka titik A dapat dikatakan memiliki Garis pandang yang jelas ke titik B.

Koordinat polar linear (linear polar coordinates). Gambar sistem dengan lingkaran konsentris yang bertahap dan berjarak sama yang merepresentasikan nilai absolut pada proyeksi polar. Gambar seperti ini biasanya digunakan untuk merepresentasikan pola radiasi antena. Lihat juga: logarithmic polar coordinates.

Konversi linear (linear conversion). Metode konversi tegangan DC yang menurunkan tegangan dengan merubah kelebihan daya menjadi panas. Switching coversion.

Polarisasi linear (linear polarization). Gelombang elektromagnetik dimana vektor bidang listrik tetap di bidang yang sama sepanjang waktu. Bidang listrik mungkin meninggalkan antena dalam orientasi vertikal, orientasi horizontal, atau pada suatu sudut antara keduanya. Lihat juga: vertical polarization, horizontal polarization.

Link budget (link budget). Jumlah daya radio yang tersedia untuk mengatasi kehilangan jalur. Jika anggaran sambungan yang tersedia melebihi kehilangan jalur, kepekaan penerimaan minimum radio penerima, dan hambatan apapun, maka komunikasi seharusnya mungkin terjadi.

Enkripsi pada lapisan sambungan (link layer encryption). Sambungan terenkrip antara alat link-local, biasanya adalah pengguna dan titik akses wireless. Lihat juga: end-to-end encryption

Sambungan-local (link-local). Alat jaringan yang tersambung dengan segmen fisik yang sama yang berkomunikasi antara satu dengan yang lainnya secara langsung disebut link-local. Sambungan link-local tidak dapat melewati batas router tanpa menggunakan suatu enkapsulasi seperti tunnel atau VPN.

Mendengar (listen). Program yang menerima sambungan pada port TCP dikatakan mendengarkan port tersebut.

Beban (load). Alat dalam sistem fotovoltaik yang memakan daya. Lihat juga: battery, panel solar, regulator, converter, inverter

Jaringan Area Lokal (Local Area Network atau LAN). Jaringan (biasanya Ethernet) yang digunakan dalam organisasi. Bagian jaringan yang berada di belakang router ISP pada umumnya dianggap sebagai bagian dari LAN. Lihat juga: WAN.

Koordinat polar logaritmik (logarithmic polar coordinates). Sistem gambar dengan lingkarang konsentris bertaham dan dijarakan secara logaritmik yang merepresentasikan nilai absolut pada proyeksi polar. Gambar seperti ini biasanya digunakan untuk merepresentasikan pola radiasi antena. Lihat juga: linear polar coordinates.

Jaringan panjang delay tinggi (long fat pipe network). Sambugan jaringan (seperti VSAT) yang memiliki kapasitas tinggi dan latensi tinggi. Guna mencapai kinerja terbaik, TCP/IP harus diatur agar sama dengan trafik pada sambungan seperti ini.

LOS lihat Line of Sight

M

MAC layer lihat data link layer

Alamat MAC (MAC address). Angka 48 bit yang unik yang ditunjukan pada setiap alat pembuatan jaringan ketika dibuat. Alamat MAC digunakan untuk komunikasi link-local.

Penyaringan MAC (MAC filtering). Metode kontrol akses berdasarkan pada alamat MAC alat komunikasi.

Tabel MAC (MAC table). Switch jaringan harus terus mengikuti alamat MAC yang digunakan pada setiap port fisik, guna mengdistribusikan paket secara efisien. Informasi ini disimpan dalam tabel yang dinamakan tabel MAC.

Baterai timbal-asam yang bebas-pemeliharan (maintenance-free lead-acid batteries) lihat lead-acid batteries.

Orang-Di-Tengah (Man-In-The-Middle atau MITM). Serangan jaringan dimana pengguna berbahaya mengganggu semua komunikasi antara pengguna dan server, yang memunkinkan informasi untuk dikopi atau dimanipulasi.

Perangkat keras yang dapat dimanaje (managed hardware). Perangkat keras pembuatan jaringan yang menyediakan antarmuka administratif, penghitung port, SNMP, atau fitur interaktif lainnya dikatakan diatur.

Mode managed (managed mode). Mode radio yang digunakan oleh alat 802.11 yang memungkinkan radio untuk bergabung dengan jaringan yang dibuat oleh titik akses. Lihat juga: master mode, ad-hoc mode, monitor mode.

Browser utama (master browser). Pada jaringan Windows, browser utama adalah komputer yang menyimpan daftar semua komputer, penggunaan file bersama dan printer yang tersedia di Network Neighborhood atau My Network Places.

Mode master (master mode). Mode radio yang digunakan oleh alat 802.11 yang memungkinkan radio untuk membuat jaringan seperti yang dilakukan oleh titik akses. Lihat juga: managed mode, ad-hoc mode, monitor mode.

Kondisi yang sama (match condition). Dalam netfilter, kondisi yang sama memspesifikasi kriteria yang menentukan target akhir untuk suatu paket. Paket mungkin dapat disamakan pada alamat MAC, alamat IP sumber atau tujuan, jumlah port, konten data, atau properti apapun lainnya.

Kedalaman Pengeluaran Daya Maksimum (Maximum Depth of Discharge atau DoD_{max}). Jumlah daya yang diambil dari baterai dalam siklus pengeluaran daya, yang diekspresikan sebagai persentase.

Titik Daya Maksimum (Maximum Power Point atau P_{max}). Titik dimana daya disediakan oleh panel surya adalah maksimum.

Kartu-MC (MC-Card). Konektor gelombang mikro yang sangat kecil yang ditemukan pada alat Lucent/ Orinoco/ Avaya.

Gelombang mekanis (mechanical wave). Gelombang yang terjadi ketika suatu medium atau obyek berayun dalam pola periodik. Lihat juga: electromagnetic wave.

Lapisan Pengontrol Akses Media (Media Access Control layer) lihat data link layer

mesh. Jaringan tanpa organisasi hirarki, dimana setiap node pada jaringan seperlunya membawa trafik satu dengan lainnya. Implementasi jaringan mesh yang baik dapat memperbaiki dirinya sendiri, yang artinya mereka dapat secara otomatis mengdeteksi masalah routing dan memperbaikinya seperlunya.

Tipe pesan (message types). Daripada angka port, ICMP trafik menggunakan tipe pesan untuk mengdefinisikan tipe informasi yang sedang dikirim. Lihat juga: ICMP.

Metode bulan terburuk (method of the worst month). Metode untuk menghitung dimensi sistem fotovoltaik yang mandiri, sehingga sistem itu dapat berfungsi di bulan ketika permintaan daya adala terbesar terkait ketersediaan daya surya. Bulan tersebut merupakan bulan terburuk dalam setahun, karena bulan ini mempunyai rasio tertinggi daya yang dibutuhkan terhadap daya yang tersedia.

MHF lihat U.FL

Pendanaan Mikro (Microfinance). Penyediaan hutang berjumlah kecil, simpanan dan layanan finansial dasar lainnya kepada penduduk miskin dunia.

Penyuntik jengkal tengah (mid span injectors). Alat Daya Lewat Ethernet yang dimasukan

antara switch Ethernet dan alat yang dihidupkan. Lihat juga: end span injectors.

Milliwatts (mW). Satuan daya yang merepresentasikan satu per seribu Watt.

MITM lihat Man-In-The-Middle

MMCX. Konektor gelombang mikro yang sangat kecil yang biasanya ditemukan pada peralatan yang dibuat oleh Senao dan Cisco.

Mode monitor (monitor mode). Mode radio yang biasanya digunakan oleh alat 802.11 yang biasanya tidak digunakan untuk komunikasi yang memungkinkan radio yang secara pasif memonitor trafik radio. Lihat juga: master mode, managed mode, ad-hoc mode

Port monitor (monitor port). Pada switch yang diatur, satu port monitor atau lebih mungkin dapat didefinisikan menerima trafik yang dikirim ke semua port. Ini memungkinkan anda untuk menyambung server monitor trafik dengan port untuk memantau dan menganalisa pola trafik.

Penggambar Trafik Router Multi (Multi Router Traffic Grapher atau MRTG). Alat open source yang digunakan untuk menggambar statistik trafik. Tersedia di http://oss.oetiker.ch/mrtg/

Banyak pantulan (multipath). Fenomena refleksi sinyal yang mencapai target mereka sepanjang jalur yang berbeda, dan oleh sebab itu pada waktu yang berbeda.

Multipoint-to-multipoint lihat mesh

mW lihat milliwatt

My TraceRoute (mtr). Alat diagnosa jaringan yang digunakan sebagai pilihan lain dari program traceroute yang tradisional. Http://www.bitwizard.nl/mtr/. Lihat juga: traceroute/ tracert.

N

Konektor N (N connector). Konektor gelombang mikro yang kokoh yang biasanya ditemukan pada komponen jaringan luar ruang, seperti antena dan titik akses luar ruang.

Nagios (http://nagios.org/) Alat pemantauan dalam waktu nyata yang mencatat dan memberitahu administrator sistem mengenai kekurangan layanan dan jaringan.

NAT lihat Network Address Translation

nat. Tabel yang digunakan dalam sistem firewall netfilter Linux untuk mengkonfigurasikan

Network Address Translation.

NEC2 lihat Numerical Electromagnetics Code

NetBIOS. Protokol lapisan sesi yang digunakan oleh jaringan Windows untuk penggunaan file dan printer bersama. Lihat juga: SMB

netfilter. Kerangka penyaringan paket dalam kernel Linux moderen yang dikenal sebagai netfilter. Netfilter menggunakan perintah iptables untuk memanipulasi aturan filter. Http://netfilter.org/

netmask (network mask). Netmask adalah angka 32 bit yang membagi 16 juta alamat IP yang tersedia menjadi bagian yang lebih kecil, yang dinamakan subnet. Semua jaringan IP menggunakan alamat IP dalam kombinasi dengan netmask kepada grup host dan jaringan secara logis.

NeTraMet. Alat analisa arus jaringan open source yang tersedia di *freshmeat.net/projects/netramet/*

Alamat jaringan (network address). Angka IP terkecil dalam subnet. Alamat jaringan digunakan dalam tabel routing untuk memspesifikasi tujuan yang akan digunakan ketika mengirim paket ke grup alamat IP yang logis.

Penerjemahan Alamat Jaringan (Network Address Translation atau NAT). NAT adalah teknologi jaringan yang memungkinkan banyak komputer untuk secara bersama menggunakan alamat IP routable secara global. Sementara NAT dapat membantu untuk memecahkan masalah keterbatasan ruang alamat IP, NAT menciptakan tantangan teknis untuk layanan dua arah, seperti Voice over IP.

Deteksi jaringan (network detection). Alat diagnosa jaringan yang menampilkan informasi mengenai jaringan wireless, seperti nama jaringan, saluran, dan metode enkripsi yang digunakan.

Lapisan jaringan (network layer). Juga dinamakan lapisan Internet. Ini adalah layer ketiga model jaringan OSI dan TCP/IP, dimana IP beroperasi dan routing Internet terjadi.

Network mask lihat netmask

ngrep. Alat pengamanan jaringan open source yang digunakan untuk mencari pola dalam arus data. Tersedia secara gratis di http://ngrep.sourceforge.net/

node. Alat apapun yang mampu mengirim dan menerima data pada jaringan. Titik akses, router, komputer dan laptop adalah contoh node.

Kapasitas nominal (Nominal Capacity atau C_N). Jumlah daya maksimum yang dapat diambil dari baterai yang terisi penuh. Ini biasanya diespresikan dalam Ampere-jam (Ah) atau Watt-jam (Wh).

Tegangan nominal (Nominal Voltage atau V_N). Tegangan operasi sistem fotovoltaik, yang biasanya 12 atau 12 volt.

Ntop. Alat pemantau jaringan yang menyediakan banyak detil mengenai penggunaan protokol dan sambungan pada jaringan area lokal. Http://www.ntop.org/

null. Dalam pola radiasi antena, null adalah zona dimana daya efektif yang diradiasikan adalah minimum.

Nulling. Kasus spesifik gangguan multipath dimana sinyal di antena penerima ditiadakan oleh destructive interference sinyal yang direfleksikan.

Jumlah hari otonomi (number of days of autonomy atau N). Jumlah hari maksimum dimana sistem fotovoltaik dapat beroperasi tanpa daya yang besar yang diterima dari matahari.

Kode Elektromagnetik Numerik (Numerical Electromagnetics Code atau NEC2). Paket permodelan antena yang gratis yang memungkinkan anda untuk membuat model antena dalam 3D, dan kemudian menganalisa tanggapan elektromagnetik antena tersebut. Http://www.nec2.org/

O

OFDM lihat Orthogonal Frequency Division Multiplexing

Antena omnidirectional (omnidirectional antenna). Antena yang meradiasikan ke segala arah dalam bidang horizontal. Lihat juga: directional antenna, sectorial antenna

Pengulang satu-tangan (one-arm repeater). Pengulang wireless yang hanya menggunakan sebuah radio, pada keluaran yang dikurangi secara luar biasa. Lihat juga: repeater.

Onion routing. Alat privat (seperti Tor) yang secara berulang mementalkan sambungan TCP anda lewat sejumlah server yang tersebar melalui Internet, yang mengemas informasi routing dalam sejumlah lapisan terenkrip.

Logika OR (OR logic). Operasi logika yang mengevaluasi sebagai benar hanya jika salah satu dari yang sedang dibandingkan juga terevaluasi benar. Lihat juga: AND logic.

Orthogonal Frequency Division Multiplexing (OFDM)

Model jaringan OSI (OSI network model). Model komunikasi jaringan yang terkenal yang didefinisikan oleh standar ISO/IEC 7498-1. Model OSI meliputi tujuh lapisan yang saling independen, dari bentuk fisik sampai aplikasinya. Lihat juga: TCP/IP network model.

Trafik Keluar (outbound traffic). Paket jaringan yang berasal dari jaringan lokal dan ditujukan ke tujuan luat jaringan lokal (biasanya di suatu tempat pada InternetO. Lihat juga: inbound traffic).

Penyimpanan Daya Berlebihan (overcharge). Keadaan baterai ketika penyimpan dilakukan melebihi batas kapasitas baterai. Jika daya diberikan kepada baterai melebihi titik penyimpanan maksimumnya, elektrolit mulai hancur. Regulator akan mengijinkan sejumlah waktu penyimpanan daya yang sebentar untuk baterai untuk menghindari gasification, namun akan membuang daya sebelum baterai rusak.

Pengeluaran Daya Berlebihan (overdischarge). Mengeluarkan daya baterai melebihi Kedalaman Pengeluaran Daya Maksimumnya, yang berakibat pada hancurnya baterai tersebut.

Subkripsi Berlebihan (oversubscribe). Untuk mengijinkan lebih banyak pengguna daripada apa yang dapat didukung oleh bandwidth maksimum yang tersedia.

P

Paket (Packet). Pada jaringan IP, pesan yang dikirim antara komputer terbagi menjadi bagian kecil yang dinamakan paket. Setiap paket termasuk sumber, tujuan, dan informasi routing lainnya yang digunakan untuk meng-route paket itu ke tujuan akhirnya. Paket disusun ulang pada ujung lainnya oleh TCP (atau protokol lain) sebelum diteruskan ke aplikasi.

Penyaring paket (packet filter). Firewall yang beroperasi pada lapisan Internet dengan mengecek sumber dan tujuan alamat IP, angka port, dan protokol. Paket diterima atau dibuang tergantung pada aturan penyaring paket.

Partisi (partition). Teknik yang digunakan oleh hub jaringan untuk membatasi dampak komputer yang mengirim secara berlebihkan. Hub akan secara sementara mengeluarkan komputer tersebut (mempartisinya) dari jaringan, dan menyambungkannya kembali setelah beberapa waktu. Partisi menunjukan adanya pengguna bandwidth yang boros, seperti pengguna peer-to-peer atau virus jaringan.

Penyuntik POE pasif (passive POE injector) lihat Power over Ethernet

Loss di jalur (path loss). Kehilangan sinyal radio dikarenakan jarak antara stasiun komunikasi.

Jam Puncak Matahari (Peak Sun Hours atau PSH). Nilai rata-rata penyinaran harian untuk

suatu area.

Pembangkit listrik tenaga fotovoltaik (photovoltaic generator) lihat solar panel.

Daya surya fotovoltaik (photovoltaic solar energy). Penggunaan panel surya untuk mengumpulkan daya solar untuk menghasilkan listrik. Lihat juga: thermal solar energy.

Sistem fotovoltaik (photovoltaic system). Sistem daya yang membangkitkan daya listrik dari radiasi surya dan menyimpannya untuk keperluan nanti. Sistem fotovoltaik yang mandiri melakukan ini tanpa adanya sambungan apapun dengan sumber daya yang sudah ada. Lihat juga: battery, solar panel, regulator, load, converter, inverter

Lapisan fisik (physical layer). Lapisan terendah dalam model jaringan OSI dan TCP/IP. Lapisan fisik adalah medium yang sesungguhnya yang digunakan untuk komunikasi, seperti kabel tembaga, fiber optik, atau gelombang radio.

Pigtail. Kabel gelombang mikro yang pendek yang merubah konektor yang tidak standar menjadi sesuatu yang lebih kuat dan secara umum tersedia.

Ping. Alat diagnosa jaringan yang tersedia dimanapun dan kapanpun yang menggunakan permintaan dan pembalasan pesan berulang ICMP untuk menentukan waktu pulang pergi ke jaringan host. Ping dapat digunakan untuk menentukan lokasi permasalahan jaringan dengan mem-ping komputer pada jalur antara mesin lokal dan tujuan akhirnya.

PKI lihat Public Key Infrastructure

plomb. Sepotong logam besar yang terkubur dalam bumi untuk meningkatkan sambungan ground.

PoE lihat Power over Ethernet

titik-ke-banyak titik (point-to-multipoint). Jaringan wireless dimana beberapa node tersambung dengan lokasi sentral. Contoh klasik jaringan point-to-multipoint adalah titik akses di kantor dengan beberapa laptop yang menggunakannya untuk akses Internet. Lihat juga: point-to-point, multipoint-to-multipoint

titk-ke-titik (point-to-point). Jaringan wireless yang meliputi hanya dua stasiun, yang biasanya dipisahkan oleh jarak yang sangat jauh. Lihat juga: point-multipoint, multipoint-to-multipoint.

Protokol Titik-ke-Titik (Point-to-Point Protocol atau PPP). Protokol jaringan yang biasanya digunakan pada jalur serial (seperti sambungan dial-up) untuk menyediakan sambungan IP.

Plot polar (polar plot). Gambar dimana titik dilokasikan oleh proyeksi sepanjang sumbu yang berputar (radius) terhadap persilangan dengan satu dari beberapa lingkaran konsentris.

Lihat juga rectangular plot.

Polarisasi (polarization). Arah komponen listrik gelombang elektromagnetik sewaktu komponen tersebut meninggalkan antena yang memancar. Lihat juga: horizontal polarization, vertical polarization, circular polarization.

Ketidaksamaan polarisasi (polarization mismatch). Keadaan dimana antena yang memancar dan menerima tidak menggunakan polarisasi yang sama, sehingga mengakibatkan hilangnya sinyal.

Kebijakan (policy). Dalam netfilter, kebijakan adalah aksi konfigurasi semula yang diambil ketika aturan penyaring lainnya tidak berlaku. Sebagai contoh, kebijakan dasar untuk rangkaian apapun mungkin diatur untuk MENERIMA atau MEMBUANG.

Penghitung port. Switch dan router yang diatur menyediakan statistik untuk setiap port jaringan yang dinamakan penghitung port. Statistik ini mungkin termasuk paket inbound dan outbound dan hitungan paket, serta kesalahan dan transmisi ulang.

Daya. Jumlah energi dalam waktu tertentu.

Daya lewat Ethernet (Power over Ethernet atau PoE). Teknik yang digunakan untuk menyediakan daya DC kepada alat yang menggunakan kabel data Ethernet. Lihat juga: end span injectors, mid span injectors.

PPP lihat Point to Point Protocol

Lapisan presentasi (presentation layer). Lapisan ke-enam model jaringan OSI. Lapisan ini berurusan dengan representasi data, seperti enkode atau kompresi data MIME.

Ruang alamat privat (private address space). Serangkaian alamat IP yang sudah diambil yang digambarkan secara garis besar di RFC1918. Ruang alamat privat sering kali digunakan dalam organisasi, bersamaan dengan Network Address Translation (NAT). Jangkauan ruang alamat privat yang diambil termasuk 10.0.0.0/8, 172.16.0.0/12, dan 192.168.0.0/16. Lihat juga: NAT

Privoxy (http://www.privoxy.org/). Proxy web yang menyediakan kerahasiaan nama melalui penggunaan filter. Privoxy seringkali digunakan bersamaan dengan Tor.

Routing proaktif (proactive routing). Implementasi mesh dimana setiap node mengetahui keberadaan mode lainnya pada mesh serta node yang mana yang dapat digunakan untuk mengalihkan trafik ke mereka. Setiap node memelihara tabel routing yang menutupi keseluruhan mesh. Lihat juga: reactive routing.

Penganalisa protokol (protocol analyzer). Program diagnosa yang digunakan untuk memantau dan membongkar paket jaringan. Penganalisa protokol menyediakan detil terbesar

yang mungkin mengenai paket individual.

Tumpukan protokol (protocol stack). Sekumpulan protokol jaringan yang menyediakan lapisan fungsi yang saling independen. Lihat juga: OSI network model dan TCP/IP network model.

PSH lihat Peak Sun Hours

Kriptografi Sandi Publik (Public key cryptography). Bentuk enkripsi yang digunakan oleh SSL, SSH, dan program pengaman yang populer lainnya. Kriptografi kunci publik memungkinkan informasi terenkrip untuk dipertukarkan melalui jaringan tidak dipercaya tanpa harus mengdistribusikan sandi rahasia.

Infrastruktur Sandi Publik (Public Key Infrastructure atau PKI). Mekanisme pengaman yang digunakan bersamaan dengan public key cryptography untuk mencegah kemungkinan serangan Man-In-The-Middle. Lihat juga: certificate authority.

Q

quick blow. Tipe sekering yang dengan segera hangus jika arus yang melewatinya lebih besar daripada ratingnya. Lihat juga: slow blow

R

pola radiasi (radiation pattern) lihat antenna pattern

radio. Porsi spektrum elektromagnetik dimana gelombang dapat dibangkitkan dengan memberikan arus bolak balik kepada antena.

Routing reaktif (reative routing). Implementasi mesh dimana rute dikomputasikan hanya ketika perlu untuk mengirim data ke node tertentu. Lihat juga: proactive routing

Pemantauan waktu nyata (realtime monitoring). Alat pemantauan jaringan yang melalukan pemantauan tanpa supervisi dalam periode waktu yang lama dan dengan segera memberitahu administrator ketika permasalahan muncul.

Keterbalikan (reciprocity). Kemampuan antena untuk menjaga karakteristik yang sama, terlepas apakah antena itu memancarkan atau menerima.

Baterai rekombinasi (recombinant batteries) lihat lead-acid batteries.

Plot persegi (rectangular plot). Gamabr dimana titik dilokasikan pada kisi yan sederhana. Lihat juga: polar plot.

Pendaftar Internet Daerah (Regional Internet Registrars atau RIR). 4 milyar alamat IP yang tersedia diberikan oleh IANA. Ruang dibagi menjadi subnet besar, yang didelegasikan ke satu dari lima register daerah, yang masing-masing dengan otoritas pada area geografis yang luas.

Pengatur (regulator). Komponen sistem fotovoltaik yang menjamin berjalannya baterai dalam kondisi yang baik. Pengatur mencegah overcharging atau undercharging baterai, yang keduanya sangat merusak umur baterai. Lihat juga: solar panel, battery, load, converter, inverter.

Pengulang (repeater). Node yang dikonfigurasikan untuk menayangkan trafik yang tidak ditujukan pada node itu sendiri, yang seringkali digunakan untuk memperpanjang jangkauan berguna jaringan.

Permintaan Komentar (Request for Comments atau RFC). RFC adalah serangkaian dokumen yang berangka yang dipublikasikan oleh Masyarakat Internet yang mengdokumentasikan ide dan konsep terkait teknologi Internet. Tidak semua RFC adalah standar yang sesungguhnya, namun banyak dari mereka secara eksplisit disetujui oleh IETF, atau akhirnya menjadi standar de facto. RFC dapat dilihat online di http://rfc.net/.

Return loss. Rasio logaritmik yang diukur dalam dB yang membandingkan daya yang direfleksikan oleh antena terhadap daya yang diberikan kepada antena dari garis transmisi. Lihat juga: impedance.

Polaritas terbalik (reverse polarity atau RP). Konektor gelombang mikro proprieter, yang berdasarkan pada konektor standar namun dengan jenis kelamin terbalik. RP-TNC mungkin adalah konektor polaritas terbalik yang paling umum, namun yang lainnya (seperti RP-SMA dan RP-N) juga umum.

Jalur transmisi RF (RF transmission line). Sambungan (biasanya coax, Heliax, atau waveguide) antara radio dan antena.

RIR lihat Regional Internet Registrars

Waktu Pulang Pergi (Round Trip Time atau RTT). Jumlah waktu yang dibutuhkan paket untuk dikenali dari ujung sambungan yang jauh. Ini biasanya seringkali disalah kaprahkan dengan latency.

Titik akses tidak sah (rogue akses points). Titik akses yang tidak sah yang terpasang secara salah oleh pengguna resmi, atau oleh oknum yang berniat untuk mengumpulkan data atau merusak jaringan.

Round Robin Database (RRD). Database yang menyimpan informasi dalam cara yang sangat sederhana yang tidak menyebar sepanjang waktu. Ini adalah format data yang digunakan oleh RRDtool dan alat pemantauan jaringan lainnya.

Router. Alat yang meneruskan paket antara jaringan yang berbeda. Proses penerusan paket ke hop yang berikutnya dinamakan routing.

Routing. Proses penerusan paket antara jaringan yang berbeda. Alat yang melakukan ini dinamakan router.

Tabel routing (routing tabel). Daftar jaringan dan alamat IP yang disimpan oleh router untuk menentukan bagaimana paket sebaiknya diteruskan. Jika router menerima paket untuk jaringan yang tidak terdapat di tabel routing, router menggunakan default gatewaynya. Router beroperasi di Lapisan Jaringan. Lihat juga: bridge dan default gateway.

RP lihat Reverse Polarity

RP-TNC. Versi proprieter konektor gelombang mikro TNC yang umum, dengan jenis kelamin terbalik. RP-TN seringkali ditemukan pada peralatan yang dibuat oleh Linksys.

RRD lihat Round Robin Database

RRDtool. Sekelompok alat yang memungkinkan anda untuk membuat dan memodifikasi database RRD, serta membuat gambar-gambar yang berguna untuk menampilkan data. RRDtool digunakan untuk mengikuti data rangkaian-waktu (seperti bandwidth jaringan, suhu ruangan mesin, atau rata-rata beban server) dan dapat menampilkan data itu sebagai rata-rata sepanjang waktu. RRDtool tersedia di http://oss.oetiker.ch/rrdtool/

rsync (http://rsyn.samba.org/). Alat pemindahan file bertahap open source yang digunakan untuk menjaga mirror.

RTT lihat Round Trip Time

S

SACK lihat Selective Acknowledgment

Penyebaran (scattering). Hilangnya sinyal karena adanya obyek pada jalur antara dua node. Lihat juga: free space loss, attenuation.

Antena sektorial (sectorial antenna). Antena yagn beradiasi umumnya di area tertentu. Tembakannya dapat selebar 180 derajat, atau sesempit 60 derajat. Lihat juga: directional antenna, omnidirectional antenna.

Lapisan Soket yang Aman (Secure Sockets Layer atau SSL). Teknologi enkripsi ujung-ke-ujung yang dibuat pada hampir semua web browser. SSL menggunakan public key cryptography dan public key infrastructure yang terpercaya untuk mengamankan komunikasi

data pada web. Kapanpun anda mengunjungi URL web yang berawal dengan https, anda sedang menggunakan SSL.

Pengenalan Selectif (Selective Acknowledgment atau SACK). Mekanisme yang digunakan untuk mengatasi tidak efisiennya TCP pada jaringan berlatensi tinggi, seperti VSAT.

Blok Pesan Server (Server Message Block atau SMB). Protokol jaringan yang digunakan dalam jaringan Windows untuk menyediakan layanan penggunaan file bersama. Lihat juga: NetBIOS.

Service Set ID (SSID) lihat Extended Service Set Identifier

Lapisan sesi (session layer). Layer ke-lima model OSI. Lapisan sesi mengelola sambungan logis antara aplikasi.

Protokol berorientasi sesi (session oriented protocol). Protokol jaringan (seperti TP) yang memerlukan inisialisasi sebelum data dapat dipertukarkan, serta suatu pembersihan setelah pertukaran data sudah selesai. Protokol berorientasi sesi biasanya menawarkan koreksi kesalahan dan penyusunan ulang paket, sedangkan protokol tanpa sambungan tidak. Lihat juga: connectionless protocol.

Medium yang digunakan bersama (shared medium). Jaringan link-local dimana setiap node dapat memantau trafik node lainnya.

Shorewall (http://shorewall.net/). Alat konfigurasi yang digunakan untuk menyeting firewall netfilter tanpa harus mempelajari syntax iptables.

Sidelobes. Tidak ada antena yang dapat meradiasikan energi dalam satu arah yang diinginkan. Beberapa diradiasikan dalam arah-rah lainnya. Puncak yang lebih kecil dirujuk sebagai sidelobes.

Pembangkit sinyal (signal generator). Transmitter yang memancarkan secara terus menerus di frequency tertentu.

Protokol Manajemen Jaringan Sederhana (Simple Network Management Protocol atau SNMP). Protokol yang didesain untuk memfasilitasi pertukaran informasi manajemen antara alat jaringan. SNMP biasanya digunakan untuk memeriksa switch jaringan dan router untuk mengumpulkan statistik operasi.

Simpanan web tempat-luas (site-wide web cache). Sementara semua web browser modern menyediakan cache data lokal, organisasi yang besar dapat meningkatkan efisiensi dengan meng-instal site-wide web cache. Site-wide web cache menyimpan kopi semua permintaan yang dibuat dari dalam organisasi, dan melayani kopi lokal pada permintaan berikutnya. Liha juga: Squid.

Slow blow. Sekering yang memungkinkan arus yang lebih tinggi daripada ratingnya untuk lewat dalam waktu yang singkat. Lihat juga: quick blow.

SMA. Konektor gelombang mikro berkepang yang kecil.

SMB lihat Server Message Block

SmokePing. Alat pengukuran latensi yang mengukur, menyimpan dan menampilkan latensi, distribusi latensi dan kehilangan paket dalam sebuah gambar. SmokePing tersedia di http://oss.oetiker.ch/smokeping/

SNMP lihat Simple Network Management Protocol

Snort (http://www.snort.org/). Sistem deteksi gangguan open source yang sangat populer. Lihat juga: Intrusion Detection System.

SoC lihat State of Charge

Panel surya (solar panel). Komponen sistem fotovoltaik yang digunakan untuk merubah radiasi surya menjadi listrik. Lihat juga: battery, regulator, load, converter, inverter.

Kumpulan panel surya (solar panel array). Sekumpulan panel surya yang tersambung dalam rentetan dan/atau paralel guna menyediakan daya yang diperlukan untuk suatu beban.

Solar power charge regulator lihat regulator

spectrum lihat electromagnetic spectrum

Penganalisa spektrum (spectrum analyzer). Alat yang menyediakan representasi visual specktrum elektromagnetik. Lihat juga: Wi-Spy

Kecepatan (speed). Istilah umum yang digunakan untuk merujuk pada ketanggapan sambungan jaringan. Jaringan berkecepatan tinggi sebaiknya memiliki latensi rendah dan kapasitas lebih untuk membawa trafik penggunanya. Lihat juga: bandiwdth, capacity, dan latency.

DNS horizon terpisah (split horizon DNS). Teknik yang digunakan untuk melayani jawaban yang berbeda kepada permintaan DNS berdasarkan pada sumber permintaan. Horizon terpisah digunakan untuk mengarahkan pengguna internal ke sekumpulan server yang berbeda daripada pengguna internet.

Spoof. Untuk mengimpersonasikan alat, pengguna atau layanan jaringan.

Alat pengecek spot (spot check tools). Alat pemantauan jaringan yang dijalankan hanya

ketika diperlukan untuk mengdiagnosa masalah. Ping dan traceroute adalah contoh alat pengecek spot.

Squid. Web proxy cache open source yang sangat populer. Squid fleksibel, kuat, banyak fitur, dan dapat dirubah skalanya untuk mendukung jaringan berukuran apapun. Http://www.squid-cache.org/

SSID lihat Extended Service Set Identifier

SSL lihat Secure Sockets Layer

Sistem fotovoltaik mandiri (standalone photovoltaic system) lihat photovoltaic system

Keadaan Penyimpanan (State of Charge atau SoC). Jumlah charge yang ada dalam baterai, yang ditentukan oleh tegangan yang ada dan tipe baterai.

Pengecekan berstatus (stateful inspection). Aturan firewall yang sadar akan keadaan yang diasosiasikan dengan suatu paket. Keadaan bukan bagian dari paket yang ditransmisikan melalui Internet, namun ditentukan oleh firewall itu sendiri. Sambungan yang baru dibentuk dan berkaitan mungkin semuanya akan diperhitungkan ketika menyaring paket. Stateful inspection kadang dinamakan connection tracking.

Baterai tidak bergerak (stationary batteries). Baterai yang didesain untuk memiliki lokasi tetap dan dalam skenario dimana konsumsi daya kurang lebih tidak teratur. Baterai tidak bergerak dapat mengakomodasi siklus pengeluaran daya yang dalam, namun mereka tidak didesain untuk menghasilkan arus yang besar dalam periode waktu yang singkat. Lihat juga: lead-acid batteries.

Struktur (structure). Dalam NEC2, deskripsi numerik mengenai dimana bagian antena yang berbeda dilokasikan, dan bagaiman kabel disambungkan. Lihat juga: controls.

Subnet mask lihat netmask

subnets. Bagian yang lebih rendah jangkauan jaringan IP, yang didefinisikan oleh netmasks.

Switch. Alat jaringan yang menyediakan sambungan sementara dan berdedikasi antara alat komunikasi. Lihat juga: hub.

Konversi peralihan (switching conversion). Metode konversi tegangan DC yang menggunakan komponen magnetik untuk secara sementara menyimpan daya dan merubahnya menjadi tegangan lainnya. Konversi peralihan jauh lebih efisien dari[ada linear conversion.

T

target. Dalam netfilter, aksi yang diambil ketika paket menyamai aturan. Beberapa target netfilter yang mungkin termasuk ACCEPT, DROP, LOG, dan REJECT.

TCP lihat Transmission Control Protocol

TCP acknowledgment spoofing

Ukuran jendela TCP (TCP window size). Parameter TCP yang mengdefinisikan seberapa banya data yang mungkin dikirim sebelum paket ACK dikembalikan dari sisi yang menerima. Sebagai contoh, ukuran jendela 3000 berarti dua paket masing-masing 1500 bytes akan dikirim, yang setelah itu ujung penerima akan meng-ACK-kan bagian kecil atau meminta transmisi ulang.

TCP/IP lihat Internet protocol suite

Model jaringan TCP/IP (TCP/IP network model). Penyederhanaan model jaringan OSI yang populer yang digunakan dengan jaringan Internet. Model TCP/IP terdiri dari lima lapisan yang saling independen, dari bentuk fisik sampai aplikasi. Lihat juga: OSI network model.

Tcpdump. Alat analisa dan penangkap paket open source yang populer yang tersedia di http://www.tcpdump.org/. Lihat juga: WinDump dan Wireshark.

Temporal Key Integrity Protocol (Temporal Key Integrity Protocol atau TKIP). Protokol enkripsi yang digunakan seiring dengan WPA untuk meningkatkan keamanan sesi komunikasi.

Energi surya termal (thermal solar energy). Energi yang dikumpulkan dari matahari dalam bentuk panas. Lihat juga: photovoltaic solar energy.

Pembuangan (trashing). Kondisi dimana komputer telah menggunakan RAM yang ada dan harus menggunakan hard disk untuk penyimpanan sementara, sehingga secara luar biasa mengurangi kinerja sistem.

Keluaran (throughput). Jumlah sesungguhnya informasi per detik yang berjalan melewati sambungan jaringan, yang mengabaikan overhead protokol.

Alat testing keluaran (throughput testing tools). Alat yang mengukur bandwidth yang sebenarnya tersedia antara dua titik pada jaringan.

Waktu untuk Hidup (Time To Live atau TTL). Nilai TTL beraksi sebagai deadline atau rem darurat untuk mensinyalkan waktu ketika data seharusnya dibuang. Dalam jaringan TCP/IP, TTL adalah penghitung yang mulai pada suatu nilai (seperti 64) dan berkurang secara sedikit demi sedikit pada setiap hop router. Jika TTL mencapai nol, paket dibuang. Mekanisme ini membantu mengurangu kerusakan yang disebabkan oleh loop routing. Dalam DNS, TTL

mengdefinisikan jumlah waktu dimana catatan zona tertentu sebaiknya disimpan sebelum waktu tersebut di-refresh. Dalam Squid, TTL mengdefinisikan seberapa lama obyek yang tersimpan mungkin disimpan sebelum obyek itu harus diambil kembali dari website awal.

TKIP lihat Temporal Key Integrity Protocol

Konektor TNC (TNC connector). Konektor gelombang mikro berulir yang kuat dan umum.

Tor (http://www.torproject.org/). Alat routing onion yang menyediakan perlindungan yang baik terhadap analisa trafik.

Traceroute/ tracert. Alat diagnosa jaringan kapanpun dan dimanapun yang seringkali digunakan seiring dengan ping untuk menentukan lokasi masalah jaringan. Versi Unix-nya dinamakan traceroute, sedangkan versi Windows adalah tracert. Keduanya menggunakan permintaan berulang ICMP dengan nilai TTL yang bertambah untuk menentukan router mana yang digunakan untuk bersambungan dengan host yang remote, dan juga menampilkan statistik latensi. Varian yang berikutnya adalah tracepath, yang menggunakan teknik yang sama dengan paket UDP. Lihat juga: mtr.

Baterai mobil (traction batteries) lihat lead-aced batteries.

Protokol Pengontrol Transmisi (Transmission Control Protocol atau TCP). Protokol berorientasi sesi yang beroperasi di Lapisan Transport, yang menyediakan penyusunan ulang paket, penghindaran kemacetan, dan pengiriman yang handal. TCP adalah bagian integral yang digunakan oleh banyak aplikasi internet, termasuk HTTP dan SMPT. Lihat juga: UDP.

Daya transmisi (transmission power). Jumlah daya yang disediakan oleh pemancar radio, sebelum gain antena atau kehilangan jalur apapun.

Firewall bridging tranparan (transparent bridging firewall). Teknik firewall yang memperkenalkan bridge yang secara selektif meneruskan paket berdasarkan aturan firewall. Satu keuntungan firewall bridging tranparan adalah bridging tersebut tidak memerlukan alamat IP. Lihat juga: bridge.

Penyimpanan transparan (transparent cache). Metode pelaksanaan site-wide web cache yang tidak memerlukan konfigurasi pada pengguna web. Permintaan web secara diam-diam diarahkan ke cache, yang membuat permintaan itu untuk pengguna. Cache transparan tidak menggunakan otentikasi, yang membuatnya mustahil untul melaksanakan akunting trafik di tingkat pengguna. Lihat juga: site-wide web cache, Squid.

Proxy transparan (Proxy transparent). Proxy caching yang diinstal agar permintaan web pengguna secara otomatis diteruskan ke server proxy, tanpa keperluaan apapun untuk secara manual mengkonfigurasi web browser untuk menggunakannya.

Lapisan transport (transport layer). Lapisan ketiga model jaringan OSI dan TCP/IP, yang

menyediakan metode mencapai layanan tertentu pada suatu node jaringan. Contoh protokol yang beroperasi di lapisan ini adalah TCP dan UDP.

Trending. Tipe alat pemantauan jaringan yang melakukan pemantauan tanpa pengawasan dalam periode waktu yang lama, dan yang mem-plot hasilnya pada gambar. Alat trending memungkinkan anda untuk meramalkan tingkah laku jaringan anda yang akan terjadi, yang membantu anda untuk merencanakan pengembangan dan perubahan,

TTL lihat Time To Live

tunnel. Bentuk enkapsulasi data yang membungkus satu tumpukan protokol di dalam tumpukan lainnya. Ini seringkali digunakan bersama dengan enkripsi untuk melindungi komunikasi dari pendengar yang tidak diketahui, sedangkan mengeliminir keperluan untuk mendukung enkripsi dalam aplikasi itu sendiri. Tunnel seringkali digunakan bersama dengan VPN.

U

U.FL. Konektor gelombang mikro yang sangat kecil yang biasanya digunakan pada kartu radio mini-PCI.

UDP lihat User Datagram Protocol

Pengguna yang tidak sengaja (unintentional users). Pengguna laptop yang secara tidak sengaja tersambung dengan jaringan wireless yang salah.

Pasangan Kepang Tidak Tertutup (Unshielded Twisted Pair atau UTP). Kabel yang digunakan untuk Ethernet 10baseT dan 100baseT, yang terdiri dari empat pasang kabel kepang.

Kapasitas Berguna (Useful Capacity atau C_u). Kapasitas baterai yang dapat digunakan, yang sama dengan perkalian Nominal Capacity dan Maximum Depeth of Discharge.

Protokol Datagram Pengguna (User Datagram Protocol atau UDP). Connectionless yang biasanya digunakan untuk streaming video dan audio.

UTP lihat Unshielded Twisted Pair

V

Baterai timbal asam yang diatur oleh katup (valve regulated lead-acid battery atau VRLA) lihat lead-acid batteries.

Polarisasi vertikal (vertical polarization). Bidang elektromagnetik dengan komponen listrik

yang bergerak dalam arah vertikal yang linear. Kebanyakan alat elektronik konsumen wireless menggunakan polarisasi vertikal. Lihat juga: circular polarization, vertical polarization.

Very Small Aperture Terminal (VSAT). Satu dari beberapa standar yang digunakan untuk akses Internet satelit. VSAT adalah teknologi satelit yang secara luas digelar di Afrika. Lihat juga: Broadband Global Access Network (BGAN) dan Digital Video Broadcast (DVB-S).

Pengirim video (video sender). Transmitter video 2.4 GHz yang dapat digunakan sebagai pembangkit sinyal yang tidak mahal.

Jaringan Private Virtual (Virtual Private Network atau VPN). Alat yang digunakan untuk menggabungkan dua jaringan pada jaringan yang tidak dipercaya (seperti Internet). VPN seringkali digunakan untuk menyambungkan pengguna remote dengan jaringan organisasi pada saat bepergian atau bekerja dari rumah. VPN menggunakan kombinasi enkripsi dan tunneling untuk mengamankan semua trafik jaringan, terlepas apakah aplikasi sedang digunakan. Lihat juga: tunnel.

Suara melalui IP (Voice over IP atau VoIP). Teknologi yang menyediakan fitur seperti telepon yang melalui sambungan Internet. Contoh klien VoIP yang populer termasuk Skype, Gizmo Project, MSN Messenger, dan iChat.

VPN lihat Virtual Private Network

VRLA lihat valve regulated lead acid battery

VSAT lihat Very Small Aperture Terminal

Very Small Aperture Terminal (VSAT). Satu dari beberapa standar yang digunakan untuk akses Internet satelit. VSAT adalah teknologi satelit yang secara luas digelar di Afrika. Lihat juga: Broadband Global Access Network (BGN) dan Digital Video Broadcast (DVB-S).

W

WAN lihat Wide Area Network

Pengendali perang (War drivers). Penggemar wireless yang tertarik dalam mencari lokasi fisik jaringan wireless.

Panjang gelombang (wavelength). Jarak yang diukur dari sebuah titik pada satu gelombang ke bagian yang sama dari yang berikutnya, misalnya dari bagian teratas satu puncak ke yang berikutnya. Ini juga dikenal sebagai lambda (λ)

WEP lihat Wired Equivalent Privacy

wget. Alat baris perintah open source untuk meng-download halaman web. Http://www.gnu.org/software/wget/

Wi-Fi. Merek pemasaran yang dimiliki oleh aliansi Wi-Fi yang digunakan untuk merujuk pada berbagai teknologi jaringan wireless (termasuk 802.11a, 802.11b, dan 802.11g). Wi-Fi adalah kependekan untuk Wireless Fidelity.

Akses yang dilindungi oleh Wi-Fi (WiFi Protected Access atau WPA). Protokol enkripsi lapisan sambungan yang cukup kuat yang didukung oleh kebanyakan alat Wi-Fi yang moderen.

Wi-Spy. Alat analisa spektrum 2.4 GHz yang tidak mahal yang tersedia dari http://www.metageek.net/.

Wide Area Network (WAN). Teknologi jaringan jarak jauh apapun. Leased lines, frame relay, DSL, fixed wireless, dan satelit semuanya biasanya mengimplementasikan wide area network. Lihat juga LAN.

Wiki. Situs web yang mengijinkan pengguna untuk menyunting konten halaman apapun. Satu dari kebanyakan wiki publik yang populer adalah http://www.wikipedia.org/

Skala jendela (window scale). Peningkatan TCP yang didefinisikan oleh RFC1323 yang memungkinkan jendela TCP lebih besar daripada 64KB.

WinDump. Versi Windows tcpdump. Ini tersedia di http://www.winpcap.org/windump/

Wired Equivalent Privacy (WEP). Protokol enkripsi lapisan sambungan yang kurang lebih aman yang diukung oleh hampir semua peralatan 802.11 a/b/g.

Kejituan Nirkabel (Wireless Fidelity) lihat Wi-Fi.

Wireshark. Penganalisa protokol jaringan yang gratis untuk Unix dan Windows. Http://www.wireshark.org/

WPA lihat Wi-Fi Protected Access

Z

Zabbix (http://www.zabbix.org/) Alat pemantauan dalam waktu nyata yang mencatat dan memberitahu administrator sistem mengenai keganjilan layanan dan jaringan.