ROBERT HASKINS

ISPadmin: wireless

Robert Haskins has been a UNIX system administrator since graduating from the University of Maine with a B.A. in computer science. Robert is employed by Shentel, a fast-growing network services provider based in Edinburg, Virginia. He is lead author of *Slamming Spam: A Guide for System Administrators* (Addison-Wesley, 2005).

rhaskins@usenix.org

THIS ARTICLE FOCUSES ON TECH- nologies and hardware that service providers would typically use for deploying wireless networks. Nonlicensed spectrum products are the focus here, since licensed spectrum products are usually beyond the budget of a typical ISP. That doesn't mean licensed products are not used in the service provider market; it just means that licensed spectrum usage is a much smaller segment of that market than is unlicensed spectrum usage.

This article is not meant to be a primer on wireless technologies. The references contain a few pointers to resources where the reader can obtain additional information on wireless technologies [1, 2]. Note that this article is based upon U.S. standards, so readers in other countries should consult their local regulatory agency's rules regarding what is licensed in their particular country.

(Disclaimer: My employer uses many of the products used in this article, including Colubris and Motorola.)

Background

The three applications and frequency ranges typically used (in parentheses) in service provider networks can be broken down as follows:

- Last mile (900 MHz)
- Hotspot, last mile (2.4 GHz)
- Backhaul, hotspot, and last mile (5.x GHz)

In the United States, most of this space is unlicensed spectrum, allocated by the Federal Communications Commission (FCC). One of the major differences between unlicensed and licensed spectrum is that with unlicensed spectrum, the operator of the equipment is required to resolve interference issues. With licensed products, there is no spectrum "sharing," so interference is usually minimal.

One unexpected application of a wireless provider network is in the area of device tracking in metropolitan areas. Often the traditional satellite GPS signal is unusable where there is a lot of interference, such as near a tall building. By triangulating multiple wireless device signals from an ISP's existing wireless network, the location of the device can be determined. Although this will

never replace GPS altogether, it is useful for some metropolitan regions and applications.

Last Mile

Last mile access can be thought of as a DSL or cable modem access replacement. That is, the service provider's POPs connect to the end customer via wireless connection. This "last mile" access eliminates the need for using a local exchange carrier's (LEC's) network, saving cost and possibly time to deployment. One useful application of wireless is allowing access for people living in remote areas whose network access is nonexistent or not more than 128 kbps.

The frequency behind many last mile products is 900 MHz, though 2.4 and 5.x GHz can also be used. As with many wireless technologies, line of site is important but not necessary. Many 900-MHz products are able to get six miles of non-line-of-sight service at 3 Mbps [3]. Typical pricing for the Trango solution is $539 for the customer premises equipment (CPE) and $1595 for the radio and antenna, which can serve 126 CPEs. Motorola Canopy [4] is another offering in this space.

Interference with 900 MHz can be caused by several things: other ISPs running 900 MHz equipment, older wireless phones, scanners, baby monitors, and video senders. Mitigation of the interference is the responsibility of the equipment owner (i.e., the service provider) when unlicensed products are used.

Hotspot

The first widely deployed hotspot IEEE standard was 802.11b, which used the 2.4-GHz frequency at up to 11 MB/s (a maximum of 300 feet from access point to subscriber). Subsequently, the 802.11a standard was developed; it used the 5.x-GHz frequency up to 54 MB/s but was not compatible with 802.11b, because it used a different set of frequencies. Finally, the 802.1g standard allows the 2.4-GHz range up to 54 MB/s and retains compatibility with IEEE 802.11b.

One benefit of deploying 802.11 hotspots (Wi-Fi) is that many portable devices (e.g., laptops) contain embedded 802.11 access devices. This eliminates the need for the provider to ship a CPE device to the subscriber. (Of course, it also eliminates a potential one-time revenue source, but service providers aren't usually focused on selling hardware.)

Hotspots can be deployed using "consumer grade" access points such as Cisco/Linksys or Netgear. However, these devices are often lacking needed features in a service provider's network. The list includes:

- Remote manageability/monitoring (SNMP)
- RADIUS authentication for end-subscriber access
- Wall/ceiling/outdoor enclosure
- Multiple wireless networks (SSIDs) within the same device

One option is for a service provider to build its own access points. Many open source solutions exist for manufacturing your own hardware (see the October 2005 edition of ISPadmin on the topic of embedded systems). However, the cost and trouble involved in a home-grown solution usually makes a commercial solution more attractive. An option for a low-priced gateway would be NoCatAuth [6]. This open source project handles authentication on low-cost hardware.

Along with the radio, a provider will want to control some activities of the subscriber by deploying a gateway that can provide a login screen, authenticate the subscriber, and handle redirection and other similar features. This gateway can be combined with the radio (e.g., the Colubris 3300R) or can be separate (the Colubris MSC-5200/5500 or Nomadix AG3000 [5]). In large deployments, multiple radios can be attached to the 5000-series device, lowering the cost of the project. One manufacturer of service-provider–grade access points is Colubris.

The Colubris 3300R series [7] devices are a good example of what a service provider might use in a combined gateway and radio device. In addition to the necessary but often omitted features in the bulleted list on p. 72, the 3300R series includes, but is not limited to, the following features:

- Multiple radios
- DNS relay and SMTP redirection
- 100 subscriber maximum
- Quality of Service (QoS) management

Backhaul

Backhaul involves moving data between different points on the provider's network. For example, the provider might aggregate all customer traffic at two points in its network. From those two points, the service provider would purchase two connections to the Internet. So the question comes down to how to get all the subscriber traffic to one or both of those Internet connections. This is known as backhaul.

Back in the days before unlicensed wireless, the only option for backhaul was either an LEC-provided data circuit (T1, DS3, etc.) or an expensive license spectrum (RF or microwave-based equipment). The licensed-spectrum solution was not typically an option for an undercapitalized ISP. However, once the nonlicensed spectrum was open and products were available, wireless and the ability to bypass the LEC became a viable option. Also, the ability to reach remote non–LEC-served areas was possible with low-cost wireless backhaul.

Wireless backhaul equipment is normally very similar to the "last mile" equipment, but with an antenna that sends a signal in a narrow range (as opposed to the omnidirectional antenna typically used in last mile applications). Backhaul via wireless is not without the usual issues, however. Some of these issues include:

- Interference with other providers
- Interference with wireless devices
- Line of site
- Power

The Trango Atlas 5010-EXT [8] offers 45 Mbps of bridged Ethernet up to 20 miles at $2795 per connection. This is quite cost-effective when compared to the recurring cost of a DS3 circuit. Another option would be the Motorola Canopy 5430BH product, which offers 60 Mbps line-of-sight to 124 miles.

Troubleshooting

No article on wireless would be complete without covering issues related to deploying wireless networks. A wireless spectrum analyzer is extremely helpful in troubleshooting interference with other devices and networks. Like traditional network analyzers, they come in two types: standalone

dedicated devices, and software (and possibly hardware) that runs on another device such as a laptop or handheld PC. The references list a couple of devices, both dedicated [9] and portable-PC-based [10]. Another tool that is useful for troubleshooting hotspots is a software program such as Netstumbler [11]. This is an application that runs on a Wi-Fi–enabled laptop and tells you what networks are within the range of the wireless radio.

When designing and deploying a wireless network, be sure to check overall throughput and make sure latency doesn't affect performance. Latency can be high if there are a large number of hops or if interference is present. Also, don't deploy wireless networks during the winter when foliage is missing and expect it to work during the summer when everything is in full bloom!

WiMAX

WiMAX (IEEE standards 802.16d and 802.16e) is a next-generation wireless protocol supporting a wide frequency range (2–66 GHz) and fast speeds. It is designed as a "last mile" replacement, offering multi-megabit speeds, with a range of 1–5 miles without line of sight. It may be useful for backhaul applications, but use in this area is currently somewhat limited. The standard could conceivably even replace the 802.11a/b/g wireless "hotspot," though total replacement is unlikely at least over the next few years, owing to the large installed base of 802.11 devices and networks.

WiMAX can be used with either licensed or unlicensed spectrum, making it a flexible choice for spectrum license holders and nonlicense holders as well. It can be deployed as a fixed or mobile (handheld/laptop) configuration. Although it is often hard to distinguish between the hype and news, references [12] and [13] give some good background on the WiMAX arena.

Community Access

Because of the low cost and lack of LEC involvement in deployments, wireless technology is an excellent way for communities to "build their own ISP." In fact, several U.S. cities are sponsoring wireless access deployments within their boundaries. Many other entities are getting into the act as well; sponsors can range from counties and homeowner associations to technologically oriented geeks. Because they operate like a nonprofit, the cost can be less than traditional access methods (DSL and cable modems) and built to serve underutilized and/or remote or rural areas. However, just because these organizations are nonprofit doesn't mean that money-paying subscribers will accept poor service!

Mesh networking [14] is a methodology used by some community-supported enthusiasts (and others) to reduce backhaul costs. Instead of routing all traffic directly to the Internet connections on the network, mesh networks route traffic through several peer (subscriber) nodes prior to hitting a node that is Internet-connected. This has the benefit of potentially reduced cost, depending on how the network is architected. The downside is that it takes specialized software to handle routing (and, potentially, billing) and other tasks that are not widely supported in current consumer firewall/router/access points.

I'd like to thank Bob Alexander of Shentel for his assistance with this article.

REFERENCES

[1] http://www.practicallynetworked.com/pg/wireless_networking_bkgrounder.htm.

[2] *802.11 Wireless Networks: The Definitive Guide*, 2nd ed., Matthew Gast (O'Reilly Media, 2005).

[3] Trango M900S: http://www.trangobroadband.com/products/m900s.shtml.

[4] Motorola Canopy: http://motorola.canopywireless.com/products/specshome.php.

[5] Nomadix AG3000: http://www.nomadix.com/products/platforms/ag3000/.

[6] NoCatAuth: http://nocat.net/.

[7] Colubris 3300R: http://www.colubris.com/downloads/datasheets/DS_MSC_3000.pdf.

[8] Trango Atlas 5010: http://www.trangobroadband.com/products/atlas_5010.shtml?id=bb.

[9] BK Precision Handheld 8.5-GHz Spectrum Analyzer Model #2658: http://www.bkprecision.com/www/np_specs.asp?m=2650.

[10] Fluke Networks AnalyzeAir Wi-Fi Spectrum Analyzer: http://www.flukenetworks.com/fnet/en-us/products/AnalyzeAir/MOA.htm.

[11] Netstumbler: http://www.netstumbler.com/.

[12] ZD Net UK article on WiMAX: http://news.zdnet.co.uk/communications/wireless/0,39020348,39241047,00.htm.

[13] WiMAX Forum: http://www.wimaxforum.org/home/.

[14] Mesh networking page from Wikipedia: http://en.wikipedia.org/wiki/Mesh_network.