;login:
THE MAGAZINE OF USENIX & SAGE
June 2002 volume 27 • number 3

inside:

ISPADMIN
by Robert Haskins

USENIX & SAGE
The Advanced Computing Systems Association &
The System Administrators Guild

ISPadmin

Public Internet Access

by Robert Haskins

Robert Haskins is currently employed by WorldNET Internet Services, an ISP based in Norwood, MA. After many years of saying he wouldn't work for a telephone company, he is now affiliated with one.

rhaskins@usenix.org

Introduction

In this edition of ISPadmin, methods of providing public Internet access are covered. The first area examined is the wired access one might see at hotels, Internet cafes and similar venues. Next, 802.11b fixed public access wireless points are covered. Finally, miscellaneous topics such as access point manufacturers, community networks, and software will be considered.

What exactly is public Internet access? As the name implies, it is allowing Internet access in public or quasi-public locations. Some examples of this would be building lobbies (hotels, airports), hotel rooms, Internet cafes, libraries, and similar locations. It can take the form of wired access (usually indoor locations, such as Internet cafes and hotel rooms) or wireless access (any indoor or outdoor area). The most common form of this type of wireless access is based upon the IEEE 802.11b specification, though other methods/protocols exist.

Public Access (Wired)

Figure 1 illustrates how a provider could deploy a wired public access net in a hotel, for example. The boxes to the left represent subscriber client machines, which could be located in hotel rooms or Internet cafe workstations. These machines would connect to switches (or other aggregation equipment) marked "Switch" via 10Mb or 100Mb Ethernet links. These switches would in turn be connected via Ethernet to a firewall. This firewall would house the appropriate authentication and billing interface to enable access to the Internet, after the subscriber has provided the "go ahead" and/or entered credit card billing information.

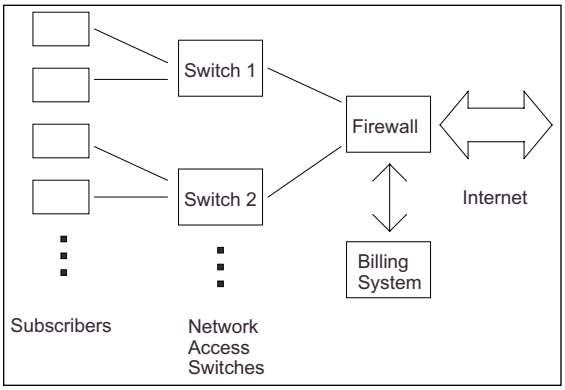

Figure 1

802.11x Background

802.11b is a wireless access standard adopted by the IEEE in 1999. It utilizes the 2.4GHz spread spectrum (unlicensed) to offer 11 megabits per second (Mbps) of bandwidth between two end points. The wireless access point (WAP) will have at least one upstream "wired" port (usually 100Mbps Ethernet) so data not destined for a machine on the WAP network can be delivered. As usual for any evolving technology, WAPs are being integrated into similar products (as well as seeing their price drop). For example, one can purchase a WAP with integrated firewall and 4-port switch for around $150 from Linksys, among other vendors.

There seems to be a lot of confusion between 802.11b and another wireless LAN standard called Bluetooth. Figure 2 illustrates the differences between the two similar technologies: 802.11b is designed for high-speed Internet access with higher radio power and wider range. Bluetooth, on the other hand, is designed for communication between small devices (e.g., cell phones) with low radio power and more limited range.

	802.11b	Bluetooth
Power Consumption	High*	Low
Effective Range	High	Low
Cost	High	Low
Highest ISO Layer**	2	5

*New power-saving mode reduces this to "medium" with appropriate hardware

**ISO layer 2 means protocol requires higher-level software (for example, TCP/IP stack); ISO layer 5 means most functions implemented in protocol.

Figure 2: 802.11b vs. Bluetooth

802.11b wireless access can be used anywhere, indoors or outdoors. However, public access points have been largely deployed up to now in high population density areas (i.e., cities). It is costly

to deploy a wireless technology such as 802.11b in remote areas with limited demand. As deployment costs decline, it will become more cost effective for providers to enable more thorough coverage.

Wireless access is used for point-to-point as well as point-to-multipoint networks. (In this article, WAP will always refer to point-to-multipoint.) The big advantage (and, alternatively, problem) with deploying 802.11b vs. other licensed spectrum products is the fact that 802.11b uses unlicensed spectrum. Of course, the use of unlicensed spectrum may also cause interference problems (from microwave ovens, Bluetooth devices, and wireless phones among others) that have to be corrected. Multipoint to multipoint (or peer to peer) wireless networks exist, though they are not in wide use. Check the References for pointers to additional information on this topic.

There are other wireless standards and products arriving. One is 802.11a, which supports data rates up to 54Mbps in the 5GHz range. The 5GHz spectrum has much less interference than the 2.4GHz band, since it doesn't have nearly the number of uses the 2.4GHz band does. Equipment for 802.11a started hitting the market about January 2002.

Another standard is 802.11g, currently a draft standard that has been the subject of much heated debate. It is 54Mbps (like 802.11a) but is backwards compatible with 802.11b (utilizes the 2.4GHz spectrum) while having 30% greater range than 802.11a. Time will tell which standard "wins," but for now, 802.11b is way ahead of the others simply because it has been around longer and therefore has a much larger installed base. 802.11g chipsets are in the process of being developed, with large-scale shipments scheduled for the third quarter of 2002 (according to a 80211 Planet announcement) by Intersil, a wireless chipset manufacturer.

802.11b Technical Details

The range of 802.11b WAP varies greatly depending upon such factors as transmitter power, antenna type, and the topography between the WAP and client station. The greatest range at full power and clear line of sight with omnidirectional (point-to-multipoint) links is in the neighborhood of 300 meters. The directional antennas (point-to-point links) at full power can exceed 32 km (20 miles).

There are several parameters that can be changed on most WAP models. These include service set identifier (SSID), which associates a WAP with a client. If it is set incorrectly, the WAP will ignore the client packets. Setting this parameter on most client adapters is a manual process, although several aggregators are designing client software to make this transparent to the wireless roamer. Also, the channel (frequency) as well as transmit power and encryption (among other settings) can be adjusted to suit the needs of the WAP owner. Usually these needs are determined by coverage requirements and interference under "Part 15" of the FCC regulations.

Types of 802.11b Networks

The lines between 802.11b network operators are rapidly blurring. For the purposes of this article, wireless networks can be broken down into three types of operators: public, private, and cooperative/community.

Public networks are those installed by service providers for the express intent of reselling/providing access to the public (or quasi-public) user. Private networks are those operators whose primary intent is to run networks for a private entity rather

than provide public access. Finally, the cooperative networks are those operators who build networks in a nonprofit mode (e.g., Seattle Wireless and NYC Wireless).

PUBLIC ACCESS WIRELESS NETWORK

A public access network could be designed as illustrated in Figure 3. Attributes of public wireless 802.11b networks usually take the form of the following:

- Firewall
- RADIUS (Remote Authentication Dial-In User Services) back-end authentication
- No encryption

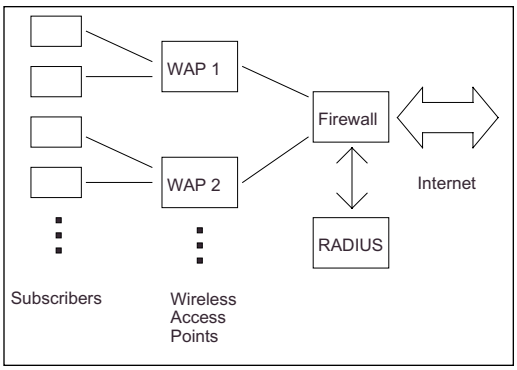

Figure 3

As one might notice, this diagram is very similar to Figure 1 (wired public access network). The only two differences are the wired aggregation points (switches) are replaced with wireless access points, and the billing system is replaced with a RADIUS server. Other than that, the functions remain the same.

PRIVATE WIRELESS NETWORKS

It is difficult to generalize private 802.11b networks. These networks reflect the needs of their owner/operators. They may or may not use firewalls and access control methods. They may or may not participate in a cooperative (Sputnik and Joltage are examples of two such commercial wireless cooperatives). They may or may not utilize encryption, back-end authentication (for example MySQL and/or RADIUS), and MAC address restrictions.

Discovering open wireless networks seems to be a hobby of choice lately (check out Netstumbler and bitshift.org to name two starting points for this activity). To this day, many "private" wireless network owners protect their networks with authentication of some sort (for example, allowing access from certain MAC addresses or authenticating via a database) or with encryption. Also, many opportunities exist for the casual 802.11b network owner to barter/resell access. Participating in such cooperatives may violate the terms of service for the upstream access provider (DSL, cable modem, etc.).

COOPERATIVE WIRELESS NETWORKS

As with private networks, cooperative (co-op) or community wireless networks are very difficult to simplify. There are many co-op wireless networks in operation. Two of the larger and better known ones are Seattle Wireless and NYC Wireless. They focus primarily on point-to-point, but have some point-to-multipoint (public) access as well.

In fact, the NoCatNet co-op group based in Sonoma County, CA, has written one of the few (if only) open source wireless authentication packages available. This code has been modified by Sputnik for use in their hybrid service. (For more on the topic of software, see "802.11b Authentication/Authorization Methods and Software," below.)

802.11b Wireless Access Point Vendors

There are currently a number of 802.11b wireless access point manufacturers. The Network Computing Buyers Guide of November 12, 2001, lists no fewer than 32 WAP models! They range in price from the mid $100s for a Linksys to several thousand dollars for models with integrated management and firewall, among other features. An ISP will likely purchase a less expensive model and attempt to add firewall and man-

REFERENCES

802.11b Networking News: *http://80211b.weblogger.com/*

802.11b vs. Bluetooth: *http://www.imparttech.com/802.11-bluetooth.htm*

bitshift.org: *http://www.bitshift.org/wardriving.shtml*

Bluetooth Special Interest Group: *http://www.bluetooth.com/*

Bluetooth Web log: *http://bluetooth.weblogs.com/*

Boingo: *http://www.boingo.com/*

Building Wireless Community Networks, by Rob Flickenger, O'Reilly, 2001, ISBN 0-596-00204-1

Earthlink: *http://www.earthlink.net/*

Exploiting and Protecting 802.11b Wireless Networks: *http://www.extremetech.com/article/0,3396,s%253D1024%2526a%253D13880,00.asp*

Extreme Tech article on deploying 802.11b access: *http://www.extremetech.com/article/0,3396,apn=5&s=1034&a=13521&app=3&ap=4,00.asp*

Gast, Matthew : 802.11 *Wireless Networks: The Definitive Guide* O'Reilly, 2002, ISBN 0-596-00183-5

GRiC: *http://www.gric.com/*

hereUare: *http://www.hereuare.com/*

IEEE 802.11b standard: *http://standards.ieee.org/reading/ieee/std/lanman/802.11b-1999.pdf*

Internet.com's 802.11 Planet: *http://www.80211-planet.com/*

Intersil 802.11g chipset announcement: *http://www.80211-planet.com/news/article/0,,1481_963341,00.html*

Intersil: *http://www.intersil.com/cda/home/*

IPASS: *http://www.ipass.com/*

Joltage: *http://www.joltage.com/jsp/home/home.jsp*

Linksys multi-function WAP: *http://www.linksys.com/Products/product.asp?grid=23&prid=173*

Linus Router Project: *http://www.linuxrouter.org/*

Mesh Networks: *http://www.meshnetworks.com/*

agement features in a separate firewall box rather than pay for such functionality in a multi-function access point.

One option is to build your own access point. NoCat has a package called WRP (Wireless Router Project, based upon the Linux Router Project). According to the NoCat page, it is "a linux distribution-on-a-floppy that provides wireless support." It appears to be an easy way to reuse old, slow, Pentium-based hardware as a combined wireless access point and chokepoint firewall.

Firewalls

Almost any configurable firewall can be utilized as a public access chokepoint for providers. Most firewalls do not ship with authentication software built in, so this must be developed or perhaps modified if something like NoCatAuth is used. If the site requires multiple WAPs or hardwired networks, all traffic is brought back to a single chokepoint firewall to reduce cost and operational headache. A relatively small box (Pentium 133-class machine) can easily handle the traffic from several active access points. Of course, for very large deployments the traffic would need to be partitioned, but this would not normally be required for a typical rollout involving up to about 250 subscribers.

There are too many firewall vendors to list here, both open source and commercial. An open source firewall can also be utilized and is what most service providers would use to reduce cost and give the ability to customize functionality.

802.11b Authentication/Authorization Methods and Software

As mentioned previously, NoCatAuth is a software package that allows wireless operators to control who accesses their network(s). It is meant for community/cooperative type networks but can be adapted for use in a service provider environment. Its back-end authentication mechanism (as written) can be either text file or a MySQL database. Most service providers require RADIUS authentication for the back end, as that is how existing retail customers usually authenticate. In order for a provider to use NoCatAuth with their existing RADIUS server(s), it must be modified to allow RADIUS authentication. Leveraging existing infrastructure is extremely important these days, with service providers going out of business every week it seems!

NoCatAuth works in conjunction with a firewall to block outside access (by allowing/disallowing MAC addresses through) until the user authenticates. Prior to authentication, "walled garden" access may be granted, which would give the wireless user access to a certain limited set of services. For example, a hotel might allow access to their Web site prior to authentication, but all other access is disallowed.

A version of the NoCatAuth software has been deployed by Sputnik for access to their wireless hot spots (network). See the Sputnik site for more information.

This author is not aware of any commercial off-the-shelf software for deploying WAP authentication mechanisms. However, some WAP manufacturers include authentication/firewall functionality in firmware as an integral part of their access point. This does increase the cost and complexity of the access points in addition to potentially causing interoperability problems with a provider's infrastructure.

Billing

For wired public access, the customer will usually pay up front or be redirected to a Web page that authorizes charges to a hotel room, credit card, or other similar entity.

This functionality can be implemented with most firewalls and an interface (albeit, expensive) to a hotel or credit card billing system.

For 802.11b public access, if RADIUS is utilized as the back-end authentication mechanism, all of the data required for billing should be contained in the RADIUS accounting data. The providers' existing billing system should easily be able to handle these records, once appropriate record filters and billing plans are created. If RADIUS is not utilized, then the process is more difficult and a customized process may be required.

802.11b Aggregators

The state of 802.11b wireless access is very similar to wholesale dial-up at the start of its large-scale deployment a few years ago. Wireless-only aggregators (such as Boingo and hereUare) are joining existing dial aggregators (such as GRiC and IPASS) in this arena. (In fact, the founder of Earthlink, one of the first aggregators of dial-up, is also a founder of Boingo.) Two other aggregators, Sputnik and Joltage, don't seem to fit easily into either category.

Traditional ISP aggregators utilize a settlement process where ISP-A tallies up the amount of usage on its network by ISP-B, and ISP-B adds up usage on its network by ISP-A. The appropriate rate(s) are applied to usage, and whoever ends up owing the other money sends a check. GRiC and IPASS are essentially commercial, third-party implementations of that process. Wireless settlement works in the same manner.

Many of the commercial aggregators develop their own client wireless access software. (In fact, GRiC's software can manage wireless as well as wired and dial connections!) This software manages many of the attributes of the card transparently (SSID being the most relevant) so the subscriber doesn't have to deal with changing them. As additional features are standardized and added to wireless provider networks, this software can be easily upgraded by the subscriber.

Security Considerations

For the end subscriber, security should be of the utmost concern. The fact that critical information (such as credit card data) is traversing open, public access networks and/or radio waves should make one stop and think. If a hardwired public access provider is utilizing hubs (and certain [misconfigured] switches as well), then all ports receive all data destined for one port. Needless to say, this could be hazardous to one's financial well being.

In a similar way, 802.11b access can be "sniffed" out of the air by rogue wireless clients. The encryption standard associated with 802.11b has been proven to be insecure (see the Exploiting and Protecting 802.11b Wireless Networks reference from extremetech.com for a full discussion of security problems and possible solutions). Also, if appropriate access controls aren't in place on each subscriber's machine, one subscriber can hack any other subscriber's machine on the wireless network. This is identical to a subscriber connected to a hardwired hub accessing other subscribers' machines on the same hub, without ever going through the firewall.

Hopefully, future versions of wireless standards and implementations will contain better security. Until then, tread carefully!

Next time, anti-spam mechanisms from a server perspective will be examined in detail. In the meantime, please send me your questions and comments!

Mitre's MobilMesh (Multipoint) project: *http://www.mitre.org/tech_transfer/mobilemesh/*

Multipoint to Multipoint Wiki Wiki Wan in Santa Cruz: *http://wiki.haven.sh/index.php/WikiWikiWan*

MySQL: *http://www.mysql.org/*

Netstumbler: *http://www.netstumbler.com/*

Network Computing article on 802.11a: *http://www.networkcomputing.com/1201/1201ws1.html*

Network Computing WAP Buyers Guide chart: *http://www.networkcomputing.com/ibg/Chart?guide_id=3484*

Network Computing WAP Buyers Guide: *http://www.networkcomputing.com/1223/1223buyers2.html*

NoCat WRP: *http://nocat.net/ezwrp.html*

NoCatAuth: *http://nocat.net/*

NYC Wireless: *http://www.nycwireless.net/*

O'Reilly's wireless starting point: *http://www.oreillynet.com/wireless/*

OpenAP project: *http://opensource.instant802.com/*

Personal Telco, a co-op based in Portland, OR: *http://www.personaltelco.net/*

RADIUS accounting standard: RFC2866

RADIUS authentication/authorization standard: RFC2865

Seattle Wireless: *http://www.seattlewireless.net*

Sputnik: *http://www.sputnik.com/*

Webopedia page for 802.11: *http://www.webopedia.com/TERM/8/802_11.html*

Wireless Anarchy: *http://wirelessanarchy.com/*

Wireless Ethernet Compatibility Alliance: *http://www.wirelessethernet.org/*