

# Have wireless access, will work for food

Wireless networks make any area in your building a workspace, helping employees be productive in conference rooms, colleagues' offices, and the company café. It's a welcoming gesture to offer visitors wireless Internet access while on your site. And the future holds mobile phones that can seamlessly transition from the cellular network onto your Voice-over-IP (VoIP) network when employees enter your building.

Wireless networking is such an important requirement that if you don't implement it, and make it easy to use, you may find your employees doing it themselves. Unfortunately, most employees (and home users) install wireless access points with the default security settings, leaving networks wide open. Some system administrators, unaware of the risks, do the same.

It's trivial to set up a wireless network. Setting up one that's secure and meets all the needs of your enterprise is a totally different beast. To secure a wireless network, you address the same issues that you do when you secure your wired networks. It's always a good idea to start with a policy that covers the following:

- **Access control:** who can access your wireless network and what services they can use. You may classify users by role and allow them access to specific services as dictated by their role. Employees can access internal services, while visitors can only access the Internet. Professors can access the grading system, students can't.
- **Privacy:** how you keep traffic on your wireless network secure so that someone in your parking lot can't view your company secrets.
- **Admission requirements:** what protection mechanisms, such as antivirus software, spyware scanners, and vendor patches, are required before a system can be placed on your network.

## Wireless Ethernet networks

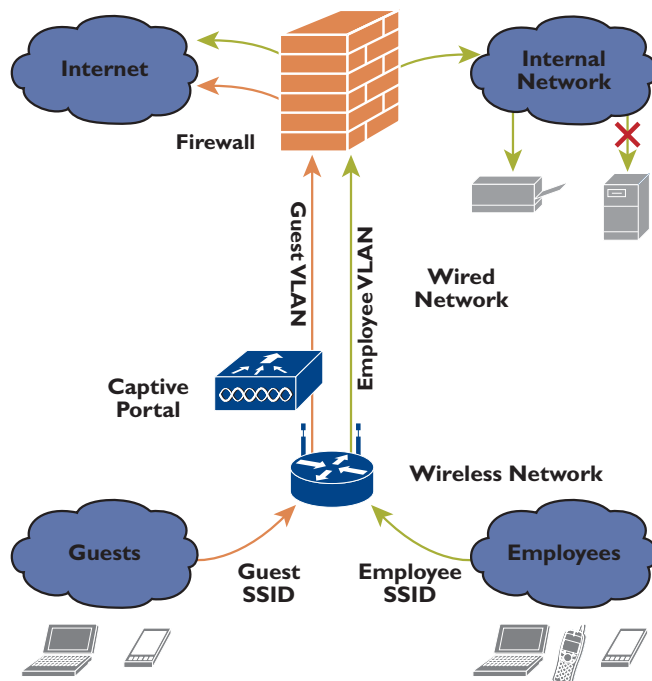
Wireless networking has become popular because of standards that promote interoperability. There are lots of proprietary wireless networks, but the ones that most people actually use are based on the IEEE 802.11 specifications. The WiFi Alliance® allows the WiFi® brand to denote products that comply with the most common standards, hence "wireless networking" and "WiFi networking" are almost synonymous these days.

Devices that follow the 802.11 specifications implement a wireless Ethernet network. The interfaces between wired and wireless Ethernet networks are known as access points. These can be configured as routers or bridges. Routers are often used with NAT and a DHCP server to make it easy for clients to access the network. They can be configured to work with a captive

portal that redirects any Web request to an authentication page, blocking all traffic from the client until she presents the appropriate credentials. Captive portals are particularly useful for guest access — not only does it make your guests feel "special" and make your organization look professional, but it also gives you a way of tracking who is using your guest access. Captive portals are available as open-source or commercial software, and some access points have them built in.

## The wireless popularity contest

The first of the 802.11 standards in wide use was 802.11b, the original 11 Mbps WiFi network. The 802.11g standard later brought the maximum theoretical speed up to 54 Mbps. Because the two standards use the same radio frequencies, most 802.11g-compliant devices are compatible with both b and g networks. The 802.11a standard is the Sony Betamax of the wireless world. It is technologically superior because it uses a broader range of frequencies, making it easier to blanket



an area with access points with less interference where the coverage areas intersect. Unfortunately, it lost the popularity contest because it is incompatible with 802.11b/g equipment. 802.11a-compliant devices are still available, but they'd be a bad choice for your guest network, because most people don't own 802.11a-compliant devices. The 802.11n standard is projected for November 2007, and is expected to offer another six to 10-fold increase in speed (asymmetric) over 802.11g, and up to a 50-fold improvement over 802.11b.

That's the story at the radio-frequency level. A network's *Service Set Identifier* (SSID) differentiates one network from another, and allows clients to choose the network to which they want to connect. Some access points support multiple SSIDs, allowing them to support different networks from the same device. This can be used to separate employee and visitor or professor and student networks. Authentication mechanisms determine who gets access to your network, and what access rights they have. Encryption mechanisms make authentication secure, and they protect traffic from being observed or corrupted. Good encryption uses key rotation with a new key for every packet. Bad encryption uses the same key for all packets, making your network easy to crack.

## Alphabet soup

There are techniques to authenticate you to the network, and techniques for encrypting your network traffic, and some mechanisms do both. When you think about cryptography, consider that the access point and the client must exchange keys that drive the cipher used to encrypt your data. Both must be secure.

WEP, or Wireless Equivalent Privacy, was meant to make wireless networks as secure as wired networks, but unfortunately its designers seemed to design it without consulting cryptography experts. It uses the same key for authentication, encryption, and for every packet. It is very easy to crack, and you shouldn't consider using it for anything. Filtering clients by MAC address is another technique that you should dismiss because of how easy it is to spoof.

WPA™, or WiFi Protected Access™, was a stopgap to WEP's problems until the 802.11i standard could be designed and WPA2™ implemented. WPA works with legacy hardware. Both use a protocol called TKIP to rotate keys for every packet, which is a very good thing.

WPA2 implements the mandatory parts of the 802.11i standard. It uses the AES cipher, stronger than RC4 used by WPA and WEP. Authentication methods include the following:

- *WPA2 Personal* (or PSK mode) uses a single shared key for authentication. Shared keys use passphrases, which are vulnerable to password guessing.
- *WPA2 Enterprise* is based on a per-user key that an 802.11x standard-compliant authentication server manages.
- *EAP*, or Extensible Authentication Protocol, is the framework used by WPA2 to authenticate users and exchange keys. It can be supported with an 802.11x-compliant authentication server such as RADIUS.
- *EAP/TLS* is a flavor of EAP that uses Public-Key Encryption (PKI) to exchange keys securely. It is in wide use.
- *PEAP* is an IETF open standard promoted by Cisco, Microsoft, and RSI that also uses server-side PKI.

The bottom line: always stay away from WEP, and use WPA2

with PEAP. This establishes a mechanism that you can use to grant rights, revoke them, and authenticate on a per-user basis. You might consider using less-secure, but more common, WPA with a pre-shared key (PSK) for your guest network, along with a captive portal to control and monitor who gets access. Captive portals not only handle access control, but also their authentication pages give you a chance to present visitors with information such as a site map, an event schedule, or the daily special in the cafeteria. You've seen captive portals at work in coffee shops, hotels, and airports.

Remember that client devices that connect to your wireless network might be infected with viruses, worms, and Trojan horses, so a firewall between the wireless and wired networks is a must.

## A secure wireless architecture

The first thing you need to develop your own secure wireless architecture is a set of policies that help you to understand what you need to implement. In organizations where you need to support different classes of users, a key principle is to segment traffic, just as you do internally to separate networks such as engineering and finance. Use VLANs, firewalls, and packet filters to make sure that you can control the traffic from each segmented network.

### The guest network

To support visitors to your site, you want to make it as easy as possible for them to use your network, but difficult for people at the coffee shop next door (or hackers in your parking lot). You may want to use a less secure network encryption mechanism (such as WPA) so that most visitors' devices will connect, and a captive portal to control who actually gets to use the network. You should provide them only with access that you give an outside Internet user.

### The employee network

You want to make it as easy as possible for your employees to get onto their network, but since you have more control over the hardware they use, you can select one of the more secure mechanisms such as WPA2 with PEAP. Even these additional authentication and encryption mechanisms aren't impenetrable, and employee laptops might have picked up nasty viruses at home, so you'll want to be careful about what services you open up. Better yet, consider installing a Network Admission Control platform that can perform client posture assessment, to automatically check for protection such as antivirus and anti-spyware tools (as well as patches) before the system is granted access to the network. You might want to provide access to print services, but don't open up your network file servers to the wireless network.

## An example architecture

Here's a simple, one-access-point wireless network that illustrates the points above (Figure 1). Enterprise-grade access points that

support multiple SSIDs can funnel traffic from each SSID onto different VLANs on the wired network, giving you more control over where the traffic can go. Use a good access point with a different SSID for each of your two networks. Route your guest network traffic through your captive portal, to the firewall, and onto the Internet. Route employee network traffic onto the Internet (if that's where it's going) or to specific services that you have protected with an additional layer of security. You can do this based on role so that, for example, finance people can access their network services, including the payroll system, while engineers can access application development systems.

## Implement and verify

As with your wired network, you'll want to verify that the wireless network you've implemented does what you think it should. First use a tool to verify that your wireless networks are visible and accessible as you expect them to be. Use a tool such as *airsnort* ([airsnort.shmoo.com](http://airsnort.shmoo.com)), *netstumbler* ([www.netstumbler.org](http://www.netstumbler.org)), or *macstumbler* to attempt to crack your networks. While you're at it, plan to use them on a continuing basis to watch for rogue access points.

Once you've verified wireless network security, go to the next layer and make sure that your firewall and captive portal are configured properly. Use a port-scanning tool such as *nmap*, and make sure that your captive portal doesn't let any traffic through until you've authenticated. Once you authenticate, make sure that you can't get to any internal services from the guest network. Then check your employee network, and verify that each of the employee roles you've defined allows the access you have granted, and no more.

Wireless networks are an important part of doing business today. Carefully implemented wireless networks are useful business tools, and they don't require you to compromise security. Carelessly implemented wireless networks are not much different than leaving your front door unlocked. ■

## CAPTIVE PORTAL SOLUTIONS

### Open source:

M0n0wall /m0n0spot – [http://www.tomsnetworking.com/2004/09/29/how\\_to\\_monowall\\_portal/](http://www.tomsnetworking.com/2004/09/29/how_to_monowall_portal/)

Wifidog – [www.wifidog.org](http://www.wifidog.org)

Chilispot – [www.chilispot.org](http://www.chilispot.org)

OpenSplash – [www.opensplash.org](http://www.opensplash.org)

Milkeyway – <http://sourceforge.net/projects/milkeyway>

Nocatauth – <http://nocat.net/>

### Commercial:

Rovingplanet – <http://www.rovingplanet.com>

Colubrus – <http://www.colubris.com>

Cisco – [www.cisco.com](http://www.cisco.com)

Proxim – [www.proxim.com](http://www.proxim.com)

This article was reprinted from the Q1 2007 issue of *The Barking Seal*, a publication of Applied Trust. You can subscribe to *The Barking Seal* online at <http://www.appliedtrust.com/barkingseal>. "Applied Trust" and the "Seal on a Rock" Applied Trust Engineering logo are registered service marks of Applied Trust. All other trademarks are registered to their respective owners.