

Securing a Wireless Network

Whether you're using Wi-Fi for an AV controller or a digital signage system, the devices you integrate must be secure—or you could compromise your client's network.

BEFORE YOU BEGIN

Wireless network based on the IEEE 802.11x standards (so-called Wi-Fi), vary greatly in scope and complexity. Depending on whether it's a single-room local area network (LAN) among just a few devices or a wide area network (WAN that's attached to the Internet, your security requirements will vary.



When your AV installation will piggyback a client's existing wireless network, or even connect to its wired network (for AV device management, for instance), you should be extra vigilant to include the client's IT/AV manager in planning and deployment. Many organizations have established protocols and best practices for Wi-Fi security.

QUICK TIPS FOR WIRELESS SECURITY

1. Rename the access point. The wireless access point (AP), or router, comes out of the box with a default SSID (service set identifier). Change it.
2. Stop broadcasting. If the AP is for a certain purpose and isn't meant for people to access whenever they want, turn off the function that broadcasts the AP's SSID to wireless devices. That way a snoop with a notebook won't know it's there.
3. Big MAC attack. For stronger security, consider adopting an approach by which the AP will only acknowledge devices with predetermined IDs, known as a MAC addresses. The MAC address is unique to each device, which makes it a great way to limit access to the network, though it may not be an option at sites where many people link laptops to presentation systems, for example.

ENCRYPT THOSE AIRWAVES

Besides controlling access to wireless and wired networks, it can be important to encrypt information that hops across wireless links. For instance, data that is transmitted wirelessly and then overlaid onto a digital sign (company news, etc.), should be encrypted to ensure the information can't be intercepted or altered.

There are several technologies for encrypting Wi-Fi signals. Your choice will depend on the nature of the information, processing power, and client policies. Among your choices:

Wired Equivalent Privacy (WEP). The oldest, standards-based method is also considered the least secure. It's still available in most wireless products and is, in fact, worth considering in situations where security isn't critical, or where the communicating devices run on battery power and/or use slow processors.

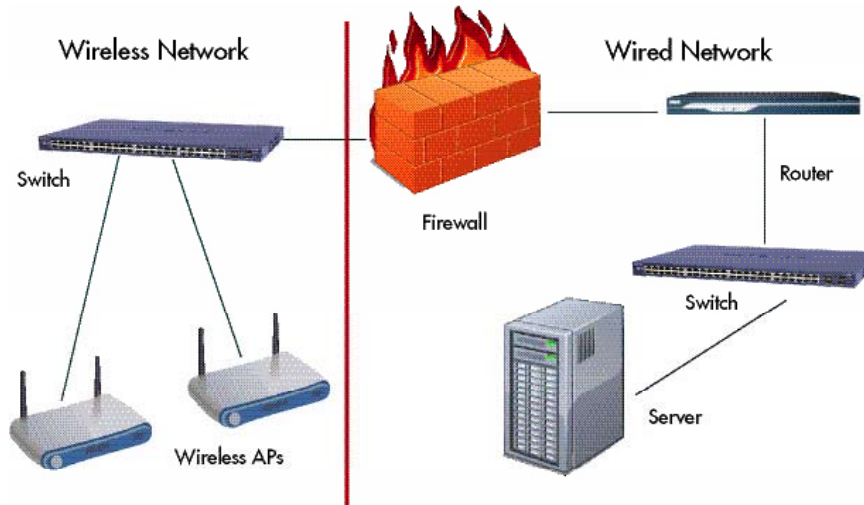
Wi-Fi Protected Access (WPA). An implementation of the IEEE 802.11i security standard, WPA uses randomly generated 128-bit encryption keys and something called Temporal Key Integrity Protocol (TKIP) to take protection up a notch over WEP. In an organization with multiple wireless devices accessing a network, use an authentication server to identify devices and grant access to resources.

Wi-Fi Protected Access 2 (WPA2). Probably overkill in most situations, but WPA2 could be required by government clients, for instance, because it has the 256-bit advanced encryption standard specified by the National Institute of Standards and Technology.

WALL IT OFF

In network situations where you have a combination of wireless and wired segments (common in enterprises), it can be a good idea to have a hardware firewall separating the two segments. The firewall protects against unauthorized access to the wired network, which is where most of an organization's intellectual property resides.

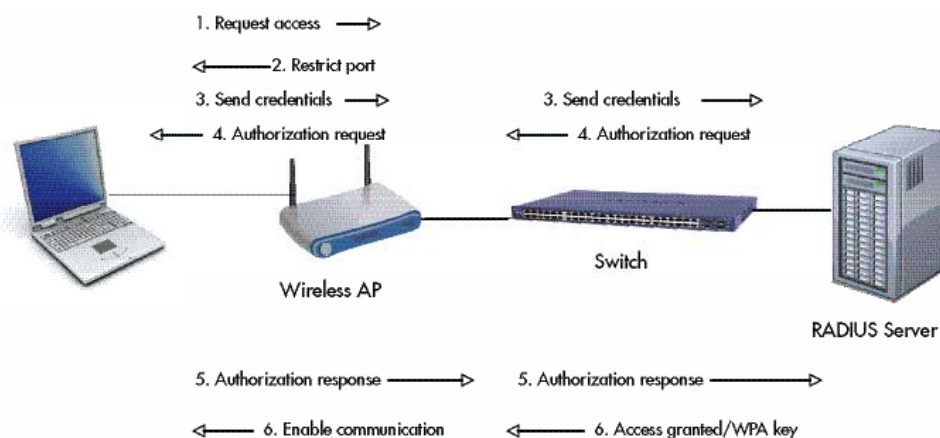
For added security, you could add a virtual private networking (VPN) server attached to the wireless network switch. VPNs are commonly used to encrypt communications sessions with remote users outside the network. When used internally, the VPN treats wireless users as if they were remote, even if they were in the boardroom.



A SECURE RADIUS

Typically in a WPA security situation, you need an authentication server to verify devices attempting to connect and to issue encryption keys. One popular way to do this is through a remote authentication dial-in user service (RADIUS) server. Through a multi-step process (see diagram), a wireless device requests access and seeks authorization.

RADIUS servers can also be used with Extensible Authentication Protocol (EAP) security methods. EAP basically lets organizations employ multiple ways of authenticating a network user, including passwords, smart cards, digital certificates, and biometric identification.



ALPHABET SOUP

When folks talk Wi-Fi, they're talking about wireless devices that conform to 802.11x specifications, including: 802.11a (a media-savvy alternative to 802.11b operating at 5 GHz for higher speeds); 802.11b (which made Wi-Fi a household name); 802.11g (with the range and product selection of 802.11b, plus the speed of 802.11a); and 802.11n (expected to be ratified this year and rated up to 300 Mbps, though 70 Mbps is more likely).