

Wireless Networks

■ Summary

Wireless networks are popular due to their relative convenience and low cost of implementation. However, in an effort by manufacturers to make their wireless devices easy to setup, most wireless routers are shipped with security disabled. Since many assume that if the wireless is working, then it is working properly (securely), few ever go to the effort to implement wireless security techniques. This article discusses wireless networks and how to make them more secure.

■ The Wireless Compromise

Wireless technology is a compromise between convenience and security/performance. If your firm values performance and security over convenience, then quite simply, do not install wireless. A hard-wired network provides the best security with the best performance. If you need network access from a room without a network jack, consider hiring someone to install a network jack ("drop"). Average network drops cost about \$100 each.

■ Understanding Wireless Risks

If you decide that you are interested in installing a wireless network it is important to first understand the risks. Wireless networks send your data into the air. Anytime data goes into the air, others can intercept it. Given time and determination, an attacker could defeat the security and gain access to that data. This article discusses techniques that make wireless networking more secure. (Please note that the phrase "more secure" is not the same as "secure.") A wireless security technique called "WEP" (Wired Equivalency Privacy) has been the standard, and is still relied on by many wireless networks today. However, hackers have figured out how to bypass this security, and gain access to WEP encrypted wireless networks. If you currently have a wireless network, chances are that it is either unsecured or secured by WEP. An enhanced security level, WPA (Wi-fi Protected Access), has been introduced and is now the new standard. True to form, hackers have developed techniques that could allow them to bypass WPA security as well. Consider where you fall on the scale between security and convenience before deciding to implement a wireless network.

■ Installing Wireless

There are two primary reasons firms install wireless access points: (1) guest internet access and (2) internal access to the Local Area Network (LAN).

Guest internet access points are intended to be open and easy to use. For example, hotels, airports and restaurants frequently offer guest wireless internet access. Assuming your computer has an internal firewall, these are generally easy and safe to use. If your computer has no internal firewall, other users of the same wireless access point could gain access to the files on your laptop. As a responsible mobile user, it is critical to turn on internal firewalls whenever connecting to any type of public network, whether wireless or wired. In business, some firms wish to grant internet access to visitors in conference rooms. This can be accomplished installing a wireless access point inside the conference room, normally in the ceiling or otherwise out of view. The most important aspect of this installation is ensuring that the wireless access point is placed on a network segment that does NOT include your servers. To properly segment your network when using a firewall, use the DMZ (Demilitarized Zone) as shown in Figure 1 below; when using a managed network switch, use VLAN (Virtual LAN).

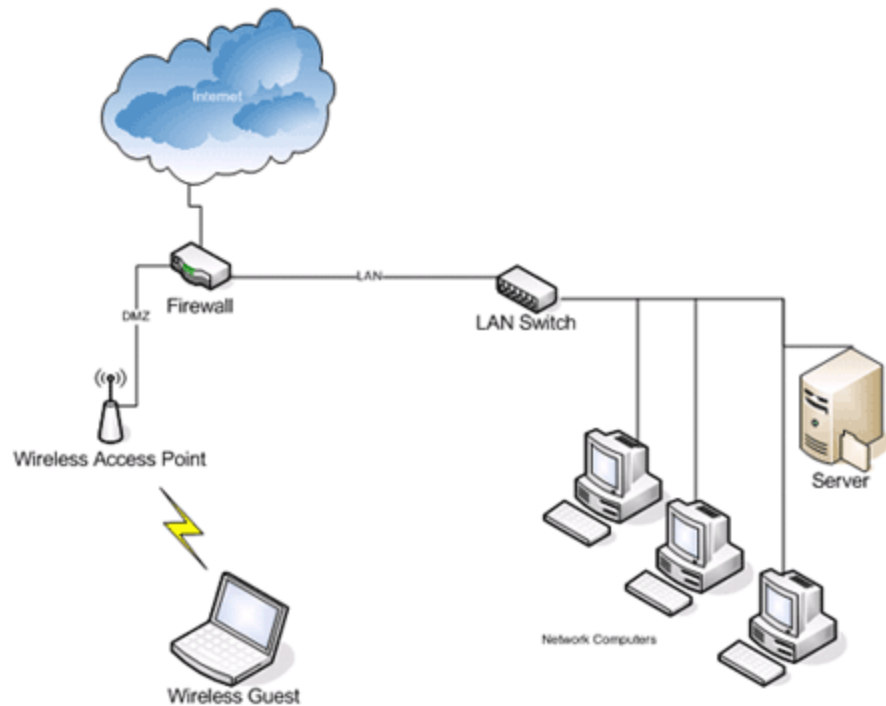


Figure 1

By placing the wireless access point on its own network segment, you ensure that guest users can not gain access to your confidential data files located on your servers and internal LAN.

■ Increasing Wireless Network Security

The other type of wireless installation is designed to provide wireless access to the local area network (LAN) & the network's resources, shared folders, printers, and so on. This should be done securely, if at all.

There are two levels of wireless security we will discuss: third-party and those that are built-in to most generic wireless routers. The highest security levels are obtained via add-ons to most generic wireless routers, such as RADIUS, and IPsec VPN, and others. The SonicWall (www.sonicwall.com) line of wireless routers have built-in IPsec VPN support, which provides enhanced security. Given the variety of choices, and implementation alternatives, the installation of third-party security products is outside the scope of this article. We will focus on implementation of security features built-in to most generic wireless routers.

Specifically, we will discuss the implementation of the following security features, which are standard on most wireless routers sold today:

- Enable WPA (do not rely on WEP)
- Use MAC address filtering
- Change the default SSID
- Change the default password

■ Enable WPA (Do not rely on WEP)

WPA is the newest security standard for wireless networks. If your existing router does not support it, either upgrade the firmware or buy a new router. Do not rely on WEP, it is hackable. In addition, when choosing a W passphrase, use a strong passphrase that contains numbers, letters and special characters. One technique hackers use to bypass WPA security is to attempt to login with hundreds, thousands, or an entire dictionary of passwords. So, make your passphrase strong.

■ Use MAC Address Filtering

A MAC address is the unique serial number of your network adapter. Most wireless routers allow you to specify which MAC addresses are allowed wireless access. Remember, a sophisticated wireless attacker could spoof their MAC address and gain access to your network.

■ Change The Default SSID

The SSID is the wireless network name. The default SSID (as established by the manufacturer) should be changed to a non-descriptive name. For example, do not use your company name, your name, or any other name that associates the wireless network back to you or your firm. Back in the "old days" disabling SSID broadcast entirely was recommended, however, the tools available to hackers today allow them to detect wireless network even when SSID broadcasting is disabled.

■ Change The Default Router Password

Change the default router password to a strong password so that a sophisticated wireless attacker will have a more difficult time gaining direct access to the router configuration.

■ Conclusion

Your decision to install wireless depends on your comfort on the scale between security and performance on one side, and convenience on the other side. At least now you better understand the risks and several techniques increase the security of your wireless network.

Jeff Lenning, CPA CITP is an AICPA Certified IT Professional. His Seal Beach, CA based firm, Click Consulting specializes in network support and application development. For further information, visit clickconsulting.com or email jeff@clickconsulting.com