



# Technology Matters

## Office Networking Basics

by Ken Knight



**M**ore people are discovering the advantages of connecting multiple computers together to share various resources. These resources can be databases, images, word processing documents, spreadsheets and just about anything else you can imagine. Let's discuss the two most commonly used methods to create an office network: wired and wireless.

### WIRED

The first is using wires to connect your computer to a device known as a "switch." A network switch operates in a similar manner as phone operators of days gone by that handled calls coming to their "switchboard" by connecting wires between the caller and the person being called. Unlike the phone operator, the network switch handles this traffic at incredible speeds so you shouldn't have to worry about delays or outages in your network due to coffee breaks.

Depending upon the type of work you perform with your computers, the speed of your network can have a significant impact. A wired network will always be much faster than a wireless, so if you plan on running applications from a central computer (also known as a server), then a wired network might be your best investment.

The speed of networks can be measured and wired networks currently start at 100 Mbps (megabits per second) and go up to 1000 Mbps (pronounced gigabit) for most Local Area Networks (LANs). And if you have not already noticed, technology comes with a plethora of acronyms. In fact it might be said that if a geek cannot do anything else, they can bury you in acronyms. To put this in a perspective that is more understandable, let's substitute 100 mph for the 100 Mbps specification. Now think about the difference between going 100 mph and 1000 mph. Desktop computers shipped today typically are equipped with a network adapter capable of 100 Mbps or 1000 Mbps. Computer notebooks normally have two network adapters, one for wired and one for wireless. Most notebooks are still sold with 100 Mbps adapters and 54 Mbps wireless adapters. If you are planning a gigabit network and are in the process of purchasing new notebooks, check the wired adapter on the notebook to ensure it fits your needs.

### WIRELESS

The second method of connecting computers together is known as "wireless." This is currently the most popular and least expensive method to get a network up and running, however, be aware that while this method is absolutely wonderful, it does have a few downsides compared to the wired method.

The types of wireless devices you will find in stores today come in two types. The first is known as an Access Point or AP. The other type is actually several devices combined into one and is called a "wireless router." This piece of equipment plays the role of an access point, a switch, and a router (which we will discuss shortly).

The wireless router is what you will find in most homes and small offices today, and allows you to connect via wired or wireless. Downside? It is also the first point of attack by hackers. Unlike a wired network where the person has to be physically inside your office to connect to the network, your wireless AP or Router is like an FM Radio Station. It is broadcasting a signal 24 hours a day, 7 days a week for wireless clients to connect to. So be aware that hackers have no problem sitting in a parking lot nearby attempting to break into your network, especially if they feel you have



---

*"...if you have not already noticed, technology comes with a plethora of acronyms. In fact it might be said that if a geek cannot do anything else, they can bury you in acronyms."*

---

something of value to them. With that said, it is imperative that you turn on the security features of your wireless device. At a bare minimum you should use the Wireless Encryption Protocol (WEP) and if you really want to increase the security, use Wi-Fi Protected Access (WPA) and turn on Media Access Control (MAC) filtering. Every network adapter in the world has a globally unique address known as a MAC address, so when you use MAC filtering you are telling the wireless AP / Router that only specific MAC addresses are allowed to connect to this device.

Other issues with wireless? Wireless is susceptible to radio interference. For example, a cordless phone might be broadcasting on a frequency close to the one your network wireless is using. One customer in California would lose their network connection every time they entered a particular office. It turned out to be a Panasonic cordless phone. Once the phone was turned off; their network connection popped right back up.

Another disadvantage is the speed of wireless networks. They currently operate at 54 Mbps which is divided among all of the users connected via wireless. So again, if you are trying to run a large application across the network and you have more than a few people in your office using this same application you might want to consider the wired method.

## **ROUTERS**

Now, let's talk about routers. A router can be a standalone device or, as we mentioned earlier, a combination network device known as a "Wireless Router." This will give you the ability to plug in between four and eight computers directly by wire, along with allowing users to connect via wireless. But the third part, the router, is probably one of the most important parts of your entire network as this is what is going to protect you from the "Internet Boogie Man" (i.e. Hacker).

A router is your "Network Traffic Cop" directing traffic between your internal network and the rest of the world. If you request a web page from your browser, the router will forward that request to the correct server out on the Internet and then return the page back to your browser. Because this request originated from your internal network, the router knows it is OK to send the response traffic back to your computer's browser, however, all other traffic originating from the Internet attempting to get back into your network will be denied access and that traffic will be dropped, unless you explicitly allow certain traffic to enter your network. A mail server would be an example of something on your internal network that would need to be accessible from the Internet. The first thing for you to do is to change your router's manufacture default password. Sadly, leaving the default password on the router has been the latest widely publicized vulnerability which means that even a "wannabe" hacker will check for this.

So to sum all this up, you can go wired or wireless. Wired will provide the most speed, while wireless will provide the most convenience. Most, if not all, of the equipment needed can be purchased at your local computer or office supply store. If you go wireless, first make sure to turn on wireless security and second change your router default password.



**Ken Knight** is an application specialist for PropertyBoss Solutions, a provider of property management software solutions that empower your business. He has over twenty years experience providing networking, software and web development solutions for customers throughout the United States and Canada. Ken started programming at the age of 14 on a TRS-80 Level II from Radio Shack. For more information about Ken or PropertyBoss Solutions, visit the company website at [www.propertyboss.com](http://www.propertyboss.com) or call Ken at 864-297-7661 x44.