

Wired or Wireless?

By Gregory S. Michaels

Wireless is one of the hottest technologies available today for home and small business networking. The idea of being able to roam with your laptop around the office, living room or backyard while still being connected is a very appealing concept. With no holes to cut or cable to run, some service companies are quick to push a wireless solution without even mentioning some of the major issues and concerns. So before you blindly take the leap into wireless networking there are a few things you need to know.

A wireless network requires a wireless base station such as a router, hub, or wireless access point and computers with wireless capability. Most of today's laptops come ready for wireless. This is not the case with traditional desktop computers. However, the traditional desktop computer can be made wireless ready with the addition of a wireless network card or USB device.

Wireless networking devices come in several flavors including 802.11a, 802.11b, 802.11g, and 802.11n. The 802.11a flavor operates in the 5-GHz frequency band and has a theoretical maximum throughput of 54 megabits per second (Mbps). The 802.11b and 802.11g flavors both operate in the 2.4-GHz frequency band and have a theoretical maximum throughput of 11Mbps and 54Mbps respectively. You cannot mix 802.11a devices with 802.11b or 802.11g devices because of the difference in the frequency bands they operate in. The newest standard in the Wi-Fi category is 802.11n. It improves on 802.11g in the amount of bandwidth supported by utilizing multiple wireless signals and antennas instead of one. This is sometimes referred to as MIMO. An 802.11n connection should support data rates of over 100 Mbps. 802.11n offers somewhat better range over other Wi-Fi flavors due to its increased signal intensity. 802.11n equipment is backward compatible with 802.11g gear. Right now the 802.11g devices are the most popular and widespread with 802.11n being the up and coming technology.

Unfortunately, the theoretical maximum throughput is not realistically achievable for any flavor of wireless device. Performance is based on the signal strength and will degrade as the distance increases between your PCs and the base station. Structural issues such as concrete and steel walls can also interfere with signal strength and can even result in complete dead spots. The realistic throughput ends up being about half of what is advertised. In addition the 802.11b and 802.11g devices operate in the same frequency band as some portable phones, microwaves ovens, and other common devices that can also cause interference. Some of these issues can be mitigated with strategic placement of the wireless devices or the installing of additional base stations, signal boosters, and signal boosting antennae.

There are also some serious security concerns surrounding wireless devices. The traditional wired network can easily be secured from hackers with a firewall device because there is only a single access point between the network and the outside world. In a wireless network all that is needed to hack the network is physical proximity to the wireless network signals, which can travel several hundred feet. All wireless devices do have built-in security provisions. However, many products require activation of the security features by the user who may not realize this is their responsibility. Using the default settings when setting up wireless access usually results in an unsecured network open to everybody within reach. So, if you don't mind sharing your network with the neighbors or worse the hackers, stick with the default settings.

Compared to wireless networks, a wired network has a consistent throughput of 100Mbps, is easier to secure, uses devices that cost less, and is not subject to the same distance limitations and interference problems as wireless. The additional cost of running cable must be weighed against the higher cost of the wireless devices. In may surprise you to learn that from a cost standpoint it can turn out to be a wash.

So, how does one decide on wired versus wireless? If security is a major issue, wired is the best choice. If your office or home is under constant rearrangement or running cable is cost prohibitive then wireless is the better choice. You don't want to have to run new cabling every time you reconfigure your workspace. If you are planning to move in the near future then go wireless. You can take your entire network with you when you go. If your workstations never move, can be easily wired, and you are not moving any time soon, then wired is the better choice. You may also want to consider a wired solution for part of your network with wireless as an extension for those hard to wire areas. For example, you can have all of the PCs in your basement workspace wired while also having a wireless access point on the first or second floor where it is difficult to run cable. But if you just have to live that dream of working on your laptop from the deck in your backyard, wireless is the only way to go.

By Line:

Gregory Michaels is President of TekTrek Computer Services providing on-site computer services for home and business. For more information email info@tektrekcomputer.com or call 303-438-9365.