Atlantic Cabling, Ltd.
North Lodge
Teddington, TW11 0NP
0800-0935-150
www.atlanitc-cabling.com

A Word about Wireless

Wireless Zones and Communication

All wireless technologies use bandwidth that is shared amongst all users communicating through their access point. There is a limit as to how many devices can communicate through any single access point. This limit may be lower for some access points than others depending on the workstations' use of the bandwidth and each user's need for network services. Typical access points can serve 10-20 users due to network traffic's "bursty" nature. However, heavy users or those with absolutely mission critical connection needs may not find it acceptable to share this bandwidth.

It is also important to note that as radio is a radiated signal, the farther away you are from the access point, the slower your connection speed; like any radio signal, a wireless network signal weakens over distance. As the signals are radio signals, environmental and building conditions will impact range. Combined with the fact that WiFi transmitter are legally restricted to 100 mili-watts of output power, if a building is heavily reinforced with metal, stone, brick, concrete block, or very dense wood, the radio signals may not be strong enough to provide connectivity through these barriers.

Wireless devices also are limited by law to specific frequency ranges that are also assigned to other consumer items like microwave ovens, Bluetooth and cordless telephones, making this frequency range very congested.

Why use Wi-Fi?

Wi-Fi certainly has advantages for small offices and transient workforces. It allows for users to be provided with network access when workers do not have a fixed desk for their regular use. Wi-Fi is also a good solution for conference rooms, meeting rooms and dorm rooms where users may need to share services and files while on the move. In cases where cabled network connections are not available or for some reason would be very expensive to install, WiFi can be an attractive option. Hearing this, one might think that WiFi offers a large savings over network cabling: this may not be the case.

Users that are regularly in the office and accustomed to 100Mbps switched networks, where the bandwidth is not shared may not find even the highest shared 54Mbps speeds acceptable. Actual throughput will be 40-70% of the speed for a single user and possibly less depending on their distance from the WAP. New devices and users will require the addition of WAPs to the network. PDA's, phones and other equipment are being introduced to Wi-Fi as well; each will eat into the bandwidth of the network. At the point of saturation, the network must be expanded.

With each new WAP comes additional cable installation. Each access point must be hard-wired to a network switch to allow to access to hard-wired network resources. As companies increase the number of access points to overcome bandwidth and other issues, new cabling drops are required. Other network equipment that is already hardwired will probably not be retrofitted with wireless cards. In short, WiFi is actually far from eliminating cable.

Wireless Security

WiFi security considerations will require organizations to carefully consider their wireless plans. 802.11b provides a mechanism called WEP (Wireless Equivalent Privacy). This mechanism provides for an encrypted key to be exchanged between the PC card and the access point. While not perfect, it does provide for some level of security. This key can be changed as often as necessary. Bearing in mind that access points advertise services and PC cards scan for the services, this is different than a wired network. In a wired network, users must first have a connection or access. In a wireless network, one could actually sit outside of a window and obtain access to the network with a simple card if the network is not secured.

Changing your network name and SSID (Service Station Identifier) and manually administering the MAC (Media Access Control) addresses that can attach to your network will close your network to unwanted trespassers. But because it is a broadcast environment, this may not provide the level of protection required by corporate users.

Encryption on wireless networks has already been broken. Newer standards addressed by the IEEE 802.11i working group work towards better mechanisms for wireless security. TKIP (Temporal Key Integrity Protocol) was the recommended encryption standard for some time. However, the newer RSN (Robust Secure Network) standard goes above and beyond the previously breakable encryption methods by changing keys and providing harder to break keys, while still providing backwards compatibility to TKIP. The RSN is a better method of security, but as long as a network has any other devices that do not support RSN, the entire wireless network can still be compromised. It is also not known how long this encryption method will provide the level of protection needed for sensitive communications. One must assume that the ability to break security protocols will progress nearly as quickly as the protocols themselves.

Any wireless network must be designed and planned with the best security offerings available. Network managers will need to monitor known security flaws to assure that their wireless network is not compromised. A policy about the types of files and communications allowed on wireless networks will also help to assure that sensitive documents do not fall into the wrong hands. Like any network, a combination of security strategies is the best method for secure communications.

Emerging Wireless Technologies

802.11n

One problem with 802.11 networks outside of security is speed. The IEEE has approved a new task group - 802.11N. This task group is working to provide speeds of 100Mbps minimum. This technology is expected to be incorporated not only into PC's, but also into consumer electronics, handheld devices and major enterprise, public and even residential hotspot environments. This standard will be backward compatible to the other 802.11 standards.

Wi-Max

Wi-Max (Worldwide Interoperability for Microwave Access) is the newest wireless communication method and was standardized by the IEEE 802.16 (Broadband Wireless Access) working group. This provides for point to multi-point architectures that operate in the spectral range between 2 GHz and 66 GHz. Transmissions can go to distances of up to 30 miles with shared data rates at 70Mbps. For the higher frequencies, line of site is required. It requires antennas with much higher gain than a typical WiFi antenna, but for broadband wireless access to rural areas and in a campus environment, it can provide significant benefit due to the fact that communications can occur with multiple devices like a radio station broadcast to multiple radios. For those in areas where broadband internet access is not an option, Wi-Max is certainly one solution. A new amendment to the standard will allow for fixed and mobile access through Wi-Max antennas.

Mesh & Spread Spectrum

IEEE 802.15 is a newly developed standard for Personal Area Networks and short distance wireless networks. The ZigBee Alliance, whose members include: Motorola, Samsung, Honeywell, Mitsubishi & Philips, are developing very low-cost, low-power consumption, two-way, wireless communications applications for use with remote controls and monitoring applications based upon the 802.15 standard.

However the 802.15 standard also uses the congested 2.4 Ghz frequency range. In order to address these congestion issues, Mesh and Spread Spectrum technologies are being developed that move signals in a series of small hops, from device to device, from source to destination within a "fabric" of similarly enabled and closely spaced devices.

Summary

While there are benefits to WiFi technology, it will not replace cabled networks in mainstream corporate environments. With faster computing, growing applications and greater demand on network resources, a cabled environment for most core applications will provide the appropriate speed for full and secure functionality. The additional security measures and administrative time WiFi requires in implementation and maintenance may, in fact, outweigh any cabling savings.

Further, as the spectrum that wireless uses is unlicensed, it can be saturated and susceptible to interference, causing additional problems. The largest hurdle to solving these problems is that the effects are generally intermittent and therefore, harder to troubleshoot. Signals can also be jammed, creating a new denial of service type attack. It is not likely that Wi-Fi will replace cabled systems, but will provide complementary services where technically feasible.