SIEMON™

IT Infrastructure Solutions

Note:

The following technical article was current at the time it was published. However, due to changing technologies and standards updates, some of the information contained in this article may no longer be accurate or up to date.

Wi-Fi - Why for?

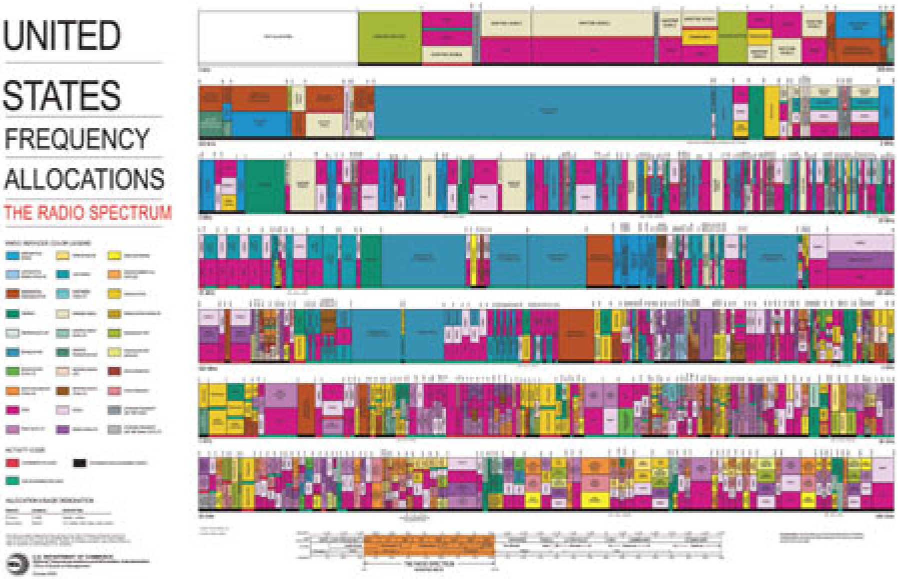
Wireless networking has made tremendous progress from its early iterations to the today's Wi-Fi (Wireless Fidelity) throughput of 54 Mbps (megabits per second). The original IEEE 802.11 standard allowed for wireless network transmissions with data rates up to 2 Mbps in the ISM (Industrial-Scientific-Medical) band. The newer adaptations of these standards are a bit different and not all are inter-compatible. 802.11a operates in the 5GHz U-NII (Unlicensed National Information Infrastructure) band and provides for throughput of 1Mbps, 2Mbps, 5.5Mbps, 11Mpbs with a maximum of 54 Mbps. 802.11b operates in the same ISM band as the original and allows for 11Mbps throughput. The latest of the standards is 802.11g. This standard, approved in June of 2004, allows data speeds up to 54Mpbs and operates in both bands. This dual band capability makes it backward compatible with 802.11b (not 802.11a). In digesting this, it is important to note that 802.11b equipment was less expensive and first to market and therefore gained significant market share over its 802.11a counterpart.

Sound confusing? You're certainly not alone. It was equally baffling for many of the original WiFI implementers as well. It is a new mindset for many network professionals, accustomed to "plugging in" network equipment that smoothly interoperates with other devices. In these cases, speed and protocols were the only concern. But WiFi standards are a bit different due to encoding and the fact that they are transmitted in different frequencies without wires.

A Word About Spectrum

To better understand WiFi implementation, one should have a basic knowledge of spectrum. Spectrum is licensed and governed by the FCC. Wi-Fi products utilize frequencies in the unlicensed spectrum bands opened by the FCC for data communications. What does unlicensed mean? In short, it means ability to transmit without requiring a license. In order to possess a portion of licensed spectrum, one must apply for the license and agree to transmit only within that frequency range. The advantage of a licensed wireless spectrum is that bandwidth can be controlled and guaranteed. Where these companies have transmission towers as part of their BTA (Business Trade Area), they must broadcast in their frequency, in their spectrum 24 x 7, much like a TV station or radio station.

Unlicensed spectrum is different in that it operates as an open license available to any manufacturer whose equipment is certified as complying with the frequency requirements within the spectrum. The spectrum is not policed for abuse and thereby; users must understand that they may be subject to interruptions and data contamination from unwanted signals. In the US, the 1-100MHz spectrum is "public airwaves," carrying marine, police and fire communications, HAM radios, Class D CB radios, VHF channels 2-6 and a Government Aeronautical Marker at 75MHz as well as all of the AM and some of the FM radio bands.



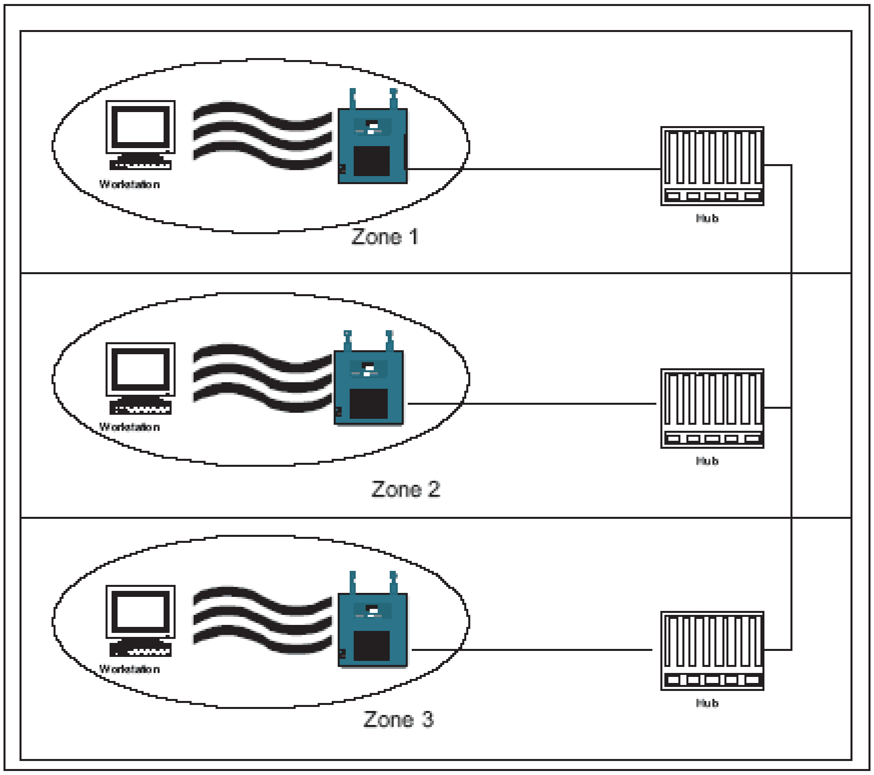
Enlarge this image

Figure 1 - FCC Spectrum Chart

The chart above represents the US Frequency allocations that are governed by the FCC and the NTIA (for government frequencies only). As you can see, the number of frequencies and the channels within them are quite extensive. Included in the frequency maps are Television, Data and Radio signals.

How do Wireless Networks Work?

PCs and other wireless network devices are equipped with a wireless network card. This card contains a radio. Early versions of these cards would work with one wireless technology only (i.e. 802.11b only). Newer versions offered by some manufacturers can seek through all of the available frequency ranges to find a network that is either 802.11a, 802.11b or 802.11g. This card scans the airwaves for a wireless network by transmitting via its radio in the different frequency ranges. The network services are advertised via a Wireless Access Point (WAP) which acts as a base station for the radio signals. The transmitter (PC) and receiver (WAP) in any frequency transmission must understand each other and operate in the same frequency range to allow for communication. Once a network is found, it assigns information to the wireless card allowing communications on the network.



Enlarge this image

Figure 2 - Wireless Zones and Communication

The WAP handles the signaling between the wireless devices and the hard-wired network. Each WAP operates on a different channel within the frequency. As shown in Figure two, each is also hardwired to the network. This allows for transmission outside of the network, for example, internet services. The bandwidth 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.

Zones are generally defined by the square footage of a building and the capabilities of the Wireless Access Point. In designing a wireless network, you first must know the the coverage area of your WAP, typically 100-300 feet indoors. As the signals are radio signals, some building conditions may impact the range. If a building is constructed or 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. 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. Depending on signal strength, a user attaching to an 11Mbps network may negotiate a speed of only 1Mbps due to distance and/or other transmission weaknesses.

A single WAP can service only a limited number of users. That number can vary greatly depending on 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 bandwidth, and additional WAPs may be required to assure that they are close enough to the signal to receive the highest available level of bandwidth.

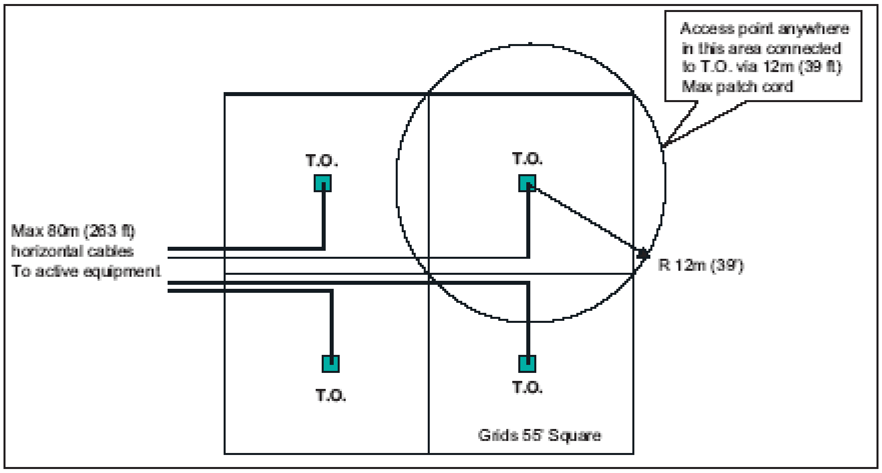
	Maximum Range	**Range At 11 Mbps**
Outdoors / open space with standard antenna	750-1,000 ft	150-350 ft
Office / light industrial setting	250-350 ft	100-150 ft

Residential setting	125-200 ft	60-80 ft

Figure 3 - Typical Range settings (Provided by the Wi-Fi alliance)

The New TIA WLAN Standard

A new WLAN cabling standard is under development with the TIA. This standard does not provide any coverage guarantees and is designed to be non-vendor specific. Rather, it utilizes a grid system within the ceiling to assure that maximum configuration options are available for location of wireless access points. The grid breaks an area into 55' square sections with a telecommunications outlet in the center of each grid. A patch cord with a maximum distance of 12m (30') allows an access point to be moved anywhere within the grid section. This will provide excellent coverage and configuration options for access point locations. See figure 4 below.


Access point anywhere in this area connected to T.O. via 12m (39 ft) Max patch cord
T.O.
T.O.
Max 80m (263 ft) horizontal cables To active equipment
R 12m (39')
T.O.
T.O.
Grids 55' Square

Enlarge this image

Figure 4 - Coverage Areas

Supporting this developing standard is the trend towards providing technically ready buildings that include both work area outlets as well as pre-wired grids in the ceiling of office space. Telecommunications outlets that are not used for access points can be used for other purposes such as IP cameras. If Power over Ethernet (PoE) were utilized, electrical circuits would not be needed in these locations. New access points are on the market that can be combined into a grid where connections are switched from one point to-another lowering home run cable counts to the telecommunications room. However, these configurations provide for a single point of failure and are not recommended.

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 without having finding a hard-cabled connection. Wi-Fi is also a good solution for conference rooms, meeting rooms and dorm rooms where users may need to share services and files. In cases where network connections are not available or for some reason would be very expensive to run (filled concrete block walls, for instance), WiFI can be an attractive option. Hearing this, one might think that WiFi offers a large savings on 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.

A Brief Word About 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. Many SOHO networks today use wireless networking. Neighbors can log on to your network services and consume your bandwidth if the administrator is not careful.

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. This method provided mitigation to most known attacks, but not all. 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.

Newer 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. The task force is working on MIMO (multiple in - multiple out) as a possible solution to increase speed while still remaining compatible with 802.11a/b/g networks. This provides multiple channels for communications through multiple antennas.

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 for them. A new amendment to the standard will allow for fixed and mobile access through Wi-Max antennas.

Summary

While there are benefits to WiFi technology, it is not expected to replace networks in mainstream corporate environments. This technology will probably remain as a transient or SOHO solution. 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.

As bandwidth is shared on a Wi-Fi network, the connectivity solutions incorporated for the cabled portion should provide the highest bandwidth possible with the least amount of interference possible. This will assure that any degradation of speed is kept to a minimum.

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 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 it is technically feasible.

The Siemon Company
Siemon Business Park
101 Siemon Company Drive
Watertown, CT 06795-0400 USA
Phone: (1) 860.945.4200
Fax: (1) 860.945.4225