Way to the wireless technology

How do you retrofit an older building with today's networking infrastructure? If the building is built with thick interior walls, or with bricks, or is otherwise architecturally unique, your options to run network cabling on the surface of walls may be limited. And the installation of either copper wire or fiber cabling may require thousands of feet of cable and many hours of painstaking labor to connect. Are there any alternatives to the installation of physical wiring? Five years ago the answer would have been a resounding no! but due to advancement in wireless technology, today we can

safely answer the same question with an emphatic yes. The PC is the center of ones digital Universe and it ties this Universe together with the tangled cables of the information age. The mess of wiring behind ones computer could be all gone, the cable sticking out of ones PC Card, Ethernet adapter could be unnecessary, the PDA cradle sitting on ones desk could be counting sheep in the bottom drawer. Every single cable on ones desk has a wireless equivalent itching to replace it.

Spectrum of wireless technology

Information connectivity is conceptually divided into three zones, based on the distance it needs to span.

The first and the shortest zone is one around ones personal space. Considering an example for the same, assume that one has a cell phone in the pocket and an MP3 player hooked on ones belt. Now suppose one needs to HotSync the PDA and backup the phonebook and also download fresh music to the MP3 player. For this one first has to disentangle the cables and then connect the cables for each of the mobile devices. The same things can be achieved by simply pointing and clicking if one possesses a PAN (personal area network) powered with say Bluetooth. A wireless PAN is like a next generation Infrared, far more sophisticated and capable, that creates a kind of 'Data Island' over a short radius for ones information. It connects all personally accessible devices, plus eliminates all wires from the desktop for the printer, scanner or digital camera or any other device that needs to exchange data with any other.

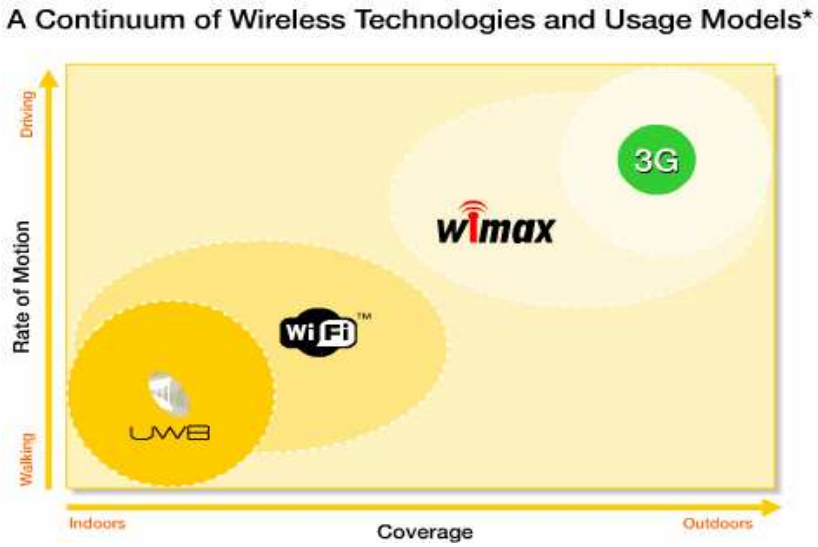
- **IR (Infrared Radiation):**
  Refers to energy in the electromagnetic radiation spectrum at which the wavelengths are longer than those of visible light, but shorter than those of radio waves.

- **Ultra-Wide Band**
  Wireless Personal Area Networks (WPANs) are very small networks within a confined space, such as an office workspace or room within the home. Ultra Wideband (UWB) technologies, offering WPAN users a much faster, short-distance connection, are currently under development.

Local area networks with wires continue to be the center of networking infrastructure. But now one can carry any computing device like a laptop around ones office and get automatically connected to the company's network. This is possible using IEEE 802.11 wireless technology. This is the technology included in the second zone of information connectivity.

- **Wi-Fi**
  Wireless Local Area Networks (WLANs) have broader range than WPANs, typically confined within office buildings, restaurants, stores, homes, etc. WLANs are gaining in popularity, fueled in part by the availability of devices optimized for wireless computing such as Intel Centrino Mobile Technology.

With the launch of digital GPRS services, data connectivity over long distances is much more convenient. Connections over long distances are the domain of Wide Area Networks (WAN) those connect far-flung devices, and even complete networks to each other. One of the most convenient things would be a laptop that connects to the WAN/LAN in the office as one walks in, and seamlessly switches to GPRS as one walks out, leaving one permanently connected wherever one goes!



• **WiMAX**
Wireless Metropolitan Area Networks (WMANs) cover a much greater distance than WLANs, connecting buildings to one another over a broader geographic area. The emerging WiMAX technology (802.16d today and 802.16e in the near future) will further enable mobility and reduce reliance on wired connections.

• **3G**
Wireless Wide Area Networks (WWANs) are the broadest range wireless networks, and are most widely deployed today in the cellular voice infrastructure although they also have the ability to transmit data. Next-generation cellular services based on various 3G technologies will significantly improve WWAN communications.

• **EDGE**
This topic is reserved for EDGE (Enhanced Data GSM Environment) infomation and products. EDGE is designed to deliver data at faster rates than Global System for Mobile (GSM) wireless service, while offering other wireless broadband applications such as multimedia.

• **Spread spectrum**
Spread spectrum is a type of wireless communications in which the frequency of the signal varies resulting in greater bandwidth than the signal would have if its frequency were not varied.

FHSS (Frequency Hopping Spread Spectrum) relies on frequency variance to combat interference with the transmitted signal.
DSSS (Direct Sequence Spread Spectrum) combines a data signal at the sending station with a higher data rate bit sequence to reduce interference in the signal transmission.
CDMA (Code division multiple access) is a wireless communications technology that uses the principle of spread spectrum communication. Instead of using frequencies or time slots, it uses mathematical codes.

• **UMTS** (Universal Mobile Telecommunications System) is a wireless broadband, packet-based standard for transmitting text, voice, video, and multimedia.

The best part about all of this wireless business is that it's a snap to set up and use. As the end user, you need not consciously twiddle with switches and configuration options- it's all automatic. Bluetooth devices find each other, exchange their capabilities and set up private connections. Laptops with wireless connectivity authenticate themselves and join the nearest open WANILAN's or any other computers that wish to exchange data. However, as with any technology it's always good to know what's going on under the hood.

Quick Connect with Bluetooth

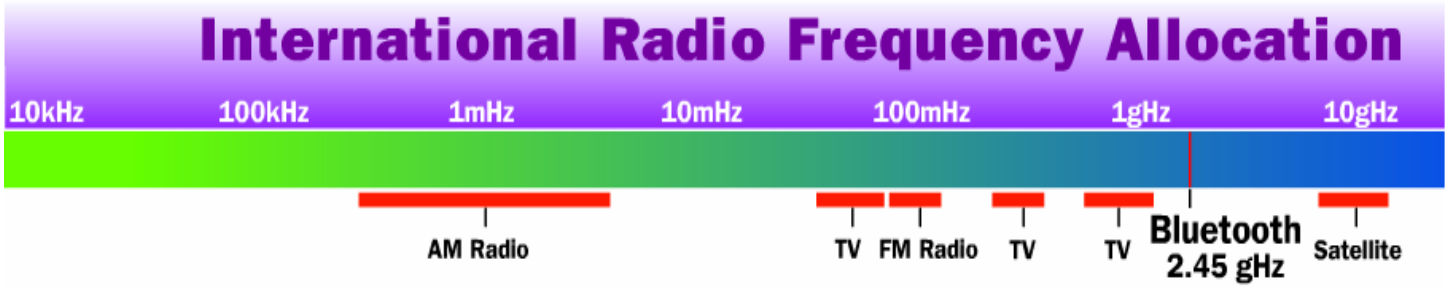
The Blue Truth: Announced in early 1998 by Erricson, IBM, Intel, Nokia and Toshiba, Bluetooth was initially designed as a simple low-cost and low power way to connect headsets to cell phones. The five founders later formed the **Bluetooth SIG**, quickly attracting players in the computing and telecom industries. No longer had a replacement for headset cables, many of these vendors seen Bluetooth as a way to connect all the electronic gadgets carried by a person or installed in a home or office.

As things stand today Bluetooth rules for wireless connectivity. Now, Bluetooth is managed by a large association including all major cell phone manufacturers and many hardware and software companies, with dozens of products available for a variety of purposes. Bluetooth has a clearly defined zone of activity- it connects personal devices.

The True Part of It:

When two Bluetooth devices are brought within the range of each other they automatically negotiate a network. More devices can be added to the network or removed at will. One of the - devices becomes the Master and regulates the traffic over the ad-hoc network. Up to eight devices can form one network sharing communications and bandwidth in a configuration called a 'piconet' - a tiny network. In any given area there can be multiple such piconets, and where they need to communicate with other piconets, thy can do so across designated devices like gateways. These larger networks are called 'Scatternets'.

Bluetooth also operates in the 2.4GHz frequency band but uses the band in the frequency Hopping mode. It uses 79.1MHz bands, with each transmission lasting less than a second over any band. The next transmission is over another band. Thus by rapidly jumping around, Bluetooth avoids interference problems between piconets or other devices in the same band.



An Example:

Let's take a look at how the Bluetooth frequency hopping and personal-area network keep Systems from becoming confused. Let's say you've got a typical modem living room with the typical modern stuff inside. There's an entertainment system with a stereo, a DVD player, a Satellite TV receiver and a television; there's a cordless telephone and a personal computer. Each of these systems uses Bluetooth, and each forms its own Pico-net to talk between main unit and peripheral.

The cordless telephone has one Bluetooth transmitter in the base and another in the handset. The manufacturer has programmed each unit with an address that falls into a range of addresses it has established for a particular type of device. When the base is first turned on, it sends radio signals asking for a response from any units with an address in a particular range. Since the handset has an address in the range, it responds, and a tiny network is formed. Now, even if one of these devices should receive a signal from another system, it will ignore it since it's not from within the network. The computer and entertainment system go through similar routines, establishing networks among addresses in ranges established by manufacturers. Once the networks are established, the systems begin talking among themselves. Each Pico-net hops randomly through the available frequencies, so all of the Pico-nets are completely separated from one another.

Now the living room has three separate networks established, each one made up of devices that know the address of transmitters it should listen to and the address of receivers it should talk to. Since each network is changing the frequency of its operation thousands of times a second, it's unlikely that any two networks will be on the same frequency at the same time. If it turns out that they are, then the resulting confusion will only cover a tiny fraction of a second, and software designed to correct for such errors weeds out the confusing information and gets on with the network's business.

Limitations of Bluetooth:

- There are interference problems between Bluetooth and most currently installed WAN / LAN's and many members of SIG once promoted Bluetooth for applications that are better off with 802.11.
- As a system for linking computers together, Bluetooth isn't attractive. Its maximum speed is about 700 bits/sec-only one tenth that of 80211.
- Its range is usually less, again by a factor of around ten, though this varies depending on how the standard is implemented.
- Bluetooth chips still haven't reached the price points that its proponents hoped for, and 802.11's popularity has brought its costs down. WiFi cards and access points are now even cheaper than their Bluetooth equivalents.

What is Bluetooth good for?

- Uses radio signals so can pass through walls and does not require line of sight. Lower power consumption. Won't drain your battery.
- 2.5 GHz radio frequency ensures worldwide operation.
- No thinking required. The devices find one another and connect without any user input at all.

Wi Fi

Wi-Fi (or Wi-fi, WiFi, Wifi, wifi), short for "Wireless Fidelity" is the wireless way to handle networking. It is also known as 802.11 networking and wireless networking. The big advantage of WiFi is its simplicity. You can connect computers anywhere in your home or office without the need for wires. The computers connect to the network using radio signals, and computers can be up to 100 feet or so apart.

Wifi is a set of product compatibility standards for wireless local area networks (WLAN) based on the IEEE 802.11 specifications. There are currently four deployed 802.11 variations: 802.11a, 802.11b, 802.11g, and 802.11n. The b standard permits up to 11Megabits/second, while both a and g allow up to 54Mbs. The new n specification will allow even higher speeds (up to 100Mbs and beyond). The 802.11a standard works in the 5GHz frequency band, and the others work in the 2.4GHz band.

Wi-Fi was intended to be used for mobile devices and LANs, but is now often used for Internet and wireless VoIP phone access. It enables a person with a wireless-enabled computer, a personal digital assistant (PDA), or a wireless VoIP phone to connect to the Internet when in proximity of

an access point. The geographical region covered by one or several access points is called a hotspot.

Advantages of Wi-Fi

- Unlike packet radio systems, Wi-Fi uses unlicensed radio spectrum and does not require regulatory approval for individual delayers.
- Wi-Fi products are widely available in the market. Different brands of access points and client network interfaces are interoperable at a basic level of service.
- Many Wi-Fi networks support roaming, in which a mobile client station such as a laptop computer can move from one access point to another as the user moves around a building or area.
- Many access points and network interfaces support various degrees of encryption to protect traffic from interception.
- Wi-Fi is a global set of standards. Unlike cellular carriers, the same Wi-Fi client works in different countries around the world.

Disadvantages of Wi-Fi

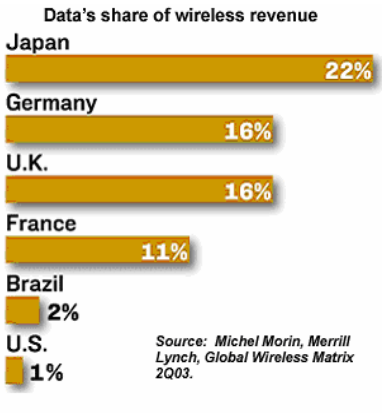
- The 802.11b and 802.11g flavors of Wi-Fi use the 2.4 GHz spectrum, which is crowded with other devices such as Bluetooth, microwave ovens, cordless phones (900 MHz or 5.8 GHz are, therefore, alternative phone frequencies one can use to avoid interference if one has a Wi-Fi network), or video sender devices, among many others. This may cause a degradation in performance. Other devices which use these microwave frequencies can also cause degradation in performance.
- Power consumption is fairly high compared to other standards, making battery life and heat a concern.
- The most common wireless encryption standard, Wired Equivalent Privacy or WEP, has been shown to be easily breakable even when correctly configured. Although newer wireless products are slowly providing support for the Wi-Fi Protected Access (WPA) protocol, many older access points will have to be replaced to support it. The adoption of the 802.11i (aka WPA2) standard in June 2004 makes available a rather better security scheme for future use — when properly configured. In the meantime, many enterprises have had to deploy additional layers of encryption (such as VPNs) to protect against interception.
- Free access points (or improperly configured access points) may be used by a hacker to anonymously initiate an attack that would be impossible to track beyond the owner of the access point.

Are wireless networks secure?

Wireless networks are inherently less secure than wired connections, since anything transmitted over the air can be intercepted. But some relatively simple precautions can make the network safe for home or small-business use. The first generation of Wi-Fi gear used a badly flawed security system called Wired Equivalent Privacy. Most equipment being sold today uses a much improved system called Wi-Fi Protected Access (WPA) that provides reasonably strong encryption of the data transmitted over the air.

Wimax

The two driving forces of modern Internet are broadband, and wireless. The WiMax standard combines the two, delivering high-speed broadband Internet access over a wireless connection. Because it can be used over relatively long distances, it is an effective "last mile" solution for delivering broadband to the home, and for creating wireless "hot spots" in places like airports, college campuses, and small communities.

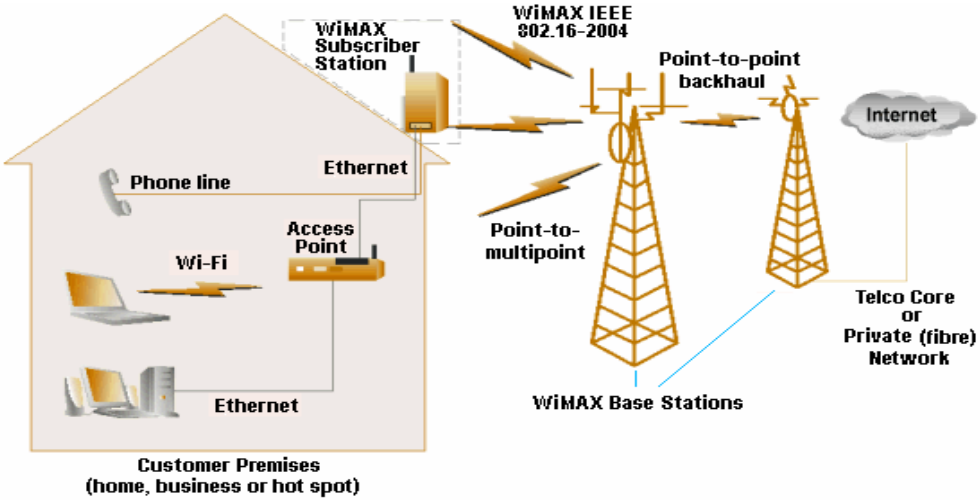


Based on the IEEE 802.16 Air Interface Standard, WiMax delivers a point-to-multipoint architecture, making it an ideal method for carriers to deliver broadband to locations where wired connections would be difficult or costly. It may also provide a useful solution for delivering broadband to rural areas where high-speed lines have not yet become available. A WiMax connection can also be bridged or routed to a standard wired or wireless Local Area Network (LAN).

The so-called "last mile" of broadband is the most expensive and most difficult for broadband providers, and WiMax provides an easy solution. Although it is a wireless technology, unlike some other wireless technologies, it doesn't require a direct line of sight between the source and endpoint, and it has a service range of 50 kilometers. It provides a shared data rate of up to 70Mbps, which is enough to service up to a thousand homes with high-speed access.

WiMax offers some advantages over WiFi, in that it offers a greater range and is more bandwidth-efficient. Ultimately, WiMax may be used to provide connectivity to entire cities, and may be incorporated into laptops to give users an added measure of mobility.

WiMax requires a tower, similar to a cell phone tower, which is connected to the Internet using a standard wired high-speed connection, such as a T3 line. But as opposed to a traditional Internet Service Provider (ISP), which divides that bandwidth among customers via wire, it uses a microwave link to establish a connection.



Because WiMax does not depend on cables to connect each endpoint, deploying WiMax to an entire high-rise, community or campus can be done in a matter of a couple days, saving significant amounts of manpower.

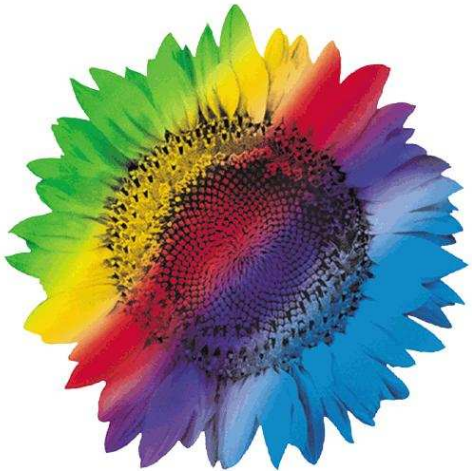
Wimax promises

- Up to a ten (10) mile range without wires
- Broadband speeds without cable or T1
- Handles "last mile" access in remote areas
- Licencing and equipment due in 2005
- Affordable technology

Wipro adopts WiFi on campus

Wipro recently went live with WiFi at its Bangalore HQ. It plans to roll out WiFi across all new locations.

Wipro's primary business goal behind going in for a wireless campus is to provide mobility to upper management. The second objective is to use WLAN as an overlay network at Wipro's 18 offshore development centres (ODCs) for providing additional seats or connections at short notice by deploying additional wireless access points when a project needs to be ramped up. Use of WLAN in sales offices or branch offices as a replacement for wired LAN will help set up such



offices faster. Sunil P Rangreji, general manager-Global IT Infrastructure at Wipro Technologies says, "We treat WLAN as a overlay network and not a replacement for wired access. But we are treating WLAN as part of our disaster recovery strategy by building redundancy for wired ports and ensuring business continuity for our mobile users."

Wipro's immediate two-point strategy with WiFi has been to use WLAN as an overlay to wired LAN infrastructure and give mobility and flexibility to accommodate additional users at a short notice. This is limited to senior executives.

Wipro Technologies evaluated wireless LAN technology as a solution in 2000. To see how the WLAN technology could improve productivity and mobility and to meet its future needs, Wipro decided to set up a small pilot project wherein it created two hotspots at its Electronic City facility on the outskirts of Bangalore in early 2002. These two hotspots were created in a conference room. The company had to put the WLAN rollout on hold at that point because of restrictions in using the 2.4 GHz frequency in a campus environment that required a special permit.

Security

WLAN security being a area of concern, Wipro has taken elaborate steps to stop unauthorised access. It uses a pre-configured default SSID (Service Set Identifier) and password for the first level of security (authentication). The secret SSID is configured by an IMG engineer on each notebook and access to the WLAN is denied if the SSID is changed. Only notebooks configured with an ID are allowed to proceed to the next level of authentication. Wipro is also using LEAP (Lightweight Extensible Authentication Protocol), an authentication protocol from Cisco, configured on the notebooks and wireless access points. Data transferred between notebooks and access points is encrypted.

Sunil P Rangreji, general manager-Global IT Infrastructure at Wipro Technologies says, "We have designed WLAN access points in such a way that the wireless network cannot be accessed beyond the restricted area—there is no leakage of signals. We are using Cisco Works, an enterprise software management component, to monitor all wireless access points." There is a separate VLAN for mobile users where access level controls are defined.

Comparison – Finding the winner

Each technology have its own merits and demerits, same is the case of WiFi, WiMax and Fixed Wireless.

Strengths

We first examine what are strengths of these technologies.

WiFi

- Convenience: continuous, wireless connection to a corporate network or the Internet from a variety of sites - airports, hotels, restaurants, offices, hospitals, homes etc. - improving worker connectivity and, therefore, productivity.
- Compatibility: connections to PCs, laptops and PDAs with a wireless LAN card adhering to IEEE's 802.11b (or other) standard
- Interoperability: a non-proprietary, standardized solution
- Ad Hoc mode: direct communication between two compatible 802.11 devices without an access point (base station)
- Installation speed and flexibility: fast and easy to install, eliminating the need to cable the desktop
- Scalability: modular configurations to suit changing density requirements

WiMax

- Cost: by enabling standards-based products with fewer variants and larger volume production, it will drive the cost of equipment down
- Competition & Choice: having standardized equipment will also encourage competition, making it possible to buy from many sources.
- Ease to deploy: Due to certified and standard equipments it makes a excellent case for plug and play installation
- Reach: Can serve to distances up to 25-30 Kms
- Spread: can scale to support thousands of users with a single base station.

Weakness

Along with strengths, these three technologies also have fair share of weaknesses also.

WiFi

- Security: opens up your network to the public any one with WiFi compatibility has access to network. A number of problems like "War chalking" and "war driving" are new phenomenon becoming apparent only recently. This is when hackers "drive" around and "chalk" the frequency of a WiFi onto the ground for other hackers. Theoretically, anyone with an 802.11b/WiFi client device can tap into your network via a non-secure access point.
- Cost: low volume chip production for client device makes cost of solution high, as cost depends a lot on client device which in turn depends on chip
- Range: short range 200meters (can be enhanced using high cost proprietary devices) for standardized solution

WiMax

- Availability: not yet widely available, encouraging numbers possible only by 2006
- Infrastructure: requires additional backhaul to feed wireless network, base stations etc
- Spectrum: Uses both licensed and unlicensed band

Conclusion :

As seen above as such no technology is a clear winner, but each one supplements or complements each other. If WiFi is a strong contender for high mobility indoor enterprise application then WiMax is just about perfect for multiple site mass metropolitan applications, while cellular fixed wireless provides a more than appealing solution for remote area or rural data connectivity requirements.

Another interesting aspect of BWA landscape is that WiMax is a lot like WiFi, but unlike WiFi's 200 Meter range, WiMax has a reach of one to 25 to 30 KM, offering a way to bring the Internet to entire communities without having to invest billions of dollars to install phone or cable networks. One thing worth a mention here is that though in its very early stages WiMax, if can deliver what it is promising then because of compelling reasons like Cost, Reach, Security, and Usability it will defiantly have a edge over other technologies.