Introduction
As part of the IT Architecture Initiative, the Office of Information Technologies (OIT) is producing a series of papers outlining directions in information technology architecture. In the spirit of RFCs, the papers are intended to facilitate understanding of and open dialogue about information technology trends at Cornell, with the ultimate goal of improving the utilization and interoperability of information technology services throughout Cornell.

Synopsis
This document outlines OIT recommended directions for “wireless” data networking at Cornell. It includes:

- An overview of wireless networking.
- Reviews of relevant wireless technologies.
- A description of wireless implementation issues.
- A brief review of wireless security issues.
- Recommendations for wireless deployment at Cornell.
- Practical implications.

What is Wireless Networking?
Generally wireless data networks use the electromagnetic spectrum\(^1\) (radio, micro & light waves) to carry data. Wireless networks carry data from transmitters and receivers attached to computers to fixed transmitters and receivers connected to the campus network infrastructure via devices known as wireless access points. Access points are placed at locations dictated by coverage needs and the nature of the signal requirements of a given wireless technology. While some wireless applications are focused point-to-point connections, others provide a general area of coverage.

The advantage of wireless data networking is readily apparent. Wireless data network users are not confined to the locations of “wired” data jacks, and so enjoy connectivity that is less restrictive and therefore well suited to meet the needs of today's mobile faculty, staff and students.

---
\(^1\) [http://www.ntia.doc.gov/osmhome/allochrt.pdf](http://www.ntia.doc.gov/osmhome/allochrt.pdf)
An important form of wireless data networking to be outlined in this paper is known as cellular. Cellular service consists of many radio cells coordinated with each other. In the ideal case, users of a cellular wireless data network service can move from cell to cell throughout the coverage area without degradation of performance or loss of service. The advantage of a cellular approach is the ability to cost effectively tune radio coverage over time to meet changing demands. This “cellular” approach to service provision has been made familiar through mobile “cell phone” services leveraged throughout the world.

**Wireless Network Deployment Technologies**

Wireless network deployment issues can be best understood if placed into the following three service classifications:

- Wireless Personal Area Networking (WPAN)
- Wireless Local or Campus Area Networking (WLAN)
- Wireless Wide Area Networking (WWAN)

Today, the core technology behind the wireless service in each of these service classifications is unique and more importantly, not an inherently integrated seamless networking strategy. For example a user of a PDA, such as a PALM (XXX) connecting to the Internet via a “Wide Area Network” service provider will not be able to directly connect to Local or Campus area wireless service currently being implemented at Cornell. Simply stated, they are different services, with different hardware requirements, and have fundamentally different service limitations.

**WPAN Technology**

WPAN systems have evolved from “cord” replacement technologies. Some examples are:

- Cordless communication between your keyboard and computer.
- Cordless communication between your Personal Productivity Device (PDA) and your computer.
- Cordless communication within your home between your cell phone and your home phone.

Because of their initial function focus, WPAN wireless implementations to date have been low-powered and offer limited coverage range.

The most hyped of all WPAN wireless technologies today is called “Bluetooth.” Bluetooth is a product of the telecommunications and computer industry “Bluetooth Special Interest Group” and is rapidly gaining wide acceptance throughout the industry.

Bluetooth is a low power wireless system initially designed as a supplement to infrared-based cable replacement communications systems that have been used for years. The capabilities are:

- Data transmission speeds of 732 Kbps or less.
- Range limited to ~ 10 meters.
- No support for application roaming. (The ability to maintain connection to the network when walking from one Bluetooth cell into another.)

Though not initially a standard as defined by the IEEE, the IEEE now has a formalized standards development in process for Bluetooth known as: 802.15.1. In turn, the IEEE is exploring the enhancement of 802.15.1 with a high data rate Bluetooth standard: 802.15.3. A high power / high-speed version of Bluetooth may someday be seen as a viable WLAN service.

---

3 [http://grouper.ieee.org/groups/802/15/index.html](http://grouper.ieee.org/groups/802/15/index.html)
WLAN Technology

WLAN systems are designed to supplement and in some cases replace traditional wired-based Local Area Networks. The predominant standards-based WLAN technology being deployed in the United States and at Cornell today is based on the IEEE 802.11b standard. (802.11b is the “upgrade” to the prior 2 Mb IEEE 802.11 standard.) The capabilities are:

- Transmission speeds up to 11 Mbs.
- Target range is ~ 30 meters.
- Limited support for roaming.

Supported implementation topologies include overlapping cells and integration of remote cells via an existing network infrastructure.

The next generation 802.11 wireless standards under development are:

- 802.11g: Near term 20 Mb enhancement to 802.11b. Like 802.11b and Bluetooth, 802.11g broadcasts on the 2.4 GHz radio frequency.
- 802.11a: 54 Mb. Based on 5 GHz frequency. Not downwardly compatible with 802.11b/g. Likely available within 2 years, but high initial component cost is expected and deployments may require denser access point placement for equivalent coverage of an 802.11b/g systems due to the nature of 5 GHz vs. 2.4 GHz radio signal propagation.

One disadvantage of 802.11 systems is their relatively high power consumption need. Given this power requirement, many believe relative battery size/life requirements of 802.11 services make this an impractical technology to support small PDA class devices.

Competing WLAN/WPAN technologies of note: HiperLAN2 and HomeRF.

802.11x and Bluetooth are not the only widely deployed and/or planned wireless systems. Hiperlan2 is a 5 Ghz high-speed wireless standard under consideration that has many compelling features. Included among these are:

- Automatic AP configuration.
- Differentiated service levels to support limited QoS.
- A strategy for integration into WPAN / WWAN environments.

HomeRF, a 2.4 Mhz system, also has a strong following. It is a WPAN “priced” service with many features needed in small WLAN environments.

All that can be said at this time about these systems is that the “popular wisdom” today suggests these strategies will lose out to retooled Bluetooth (802.15.x) and 802.11x systems over time. Regardless, it is worth maintaining a watchful eye on these systems in case of a change in industry and patron convictions.

WWAN Technology (Cellular)

Wireless phone corporations are using a broad range of technologies to transmit voice and data in the United States and even more technologies are in use across the globe. “Second generation” (2G) wireless Cellular phone systems deployed in the United States today include those based on: “GSM,” “CDMA,” and “TDMA” technologies. All these systems are currently limited to datarates of ~ 9.6 Kbps. Within the next

---

4 http://grouper.ieee.org/groups/80211/index.html
5 http://www.hiperlan2.com/web/
6 http://www.homerf.org/
few years industry plans are to supplement and/or replace these with second generation “upgrades” to support data rates between ~ 170 Kbps to ~ 300 Kbps. Over the next 5 years third generation (3G) standards-based solutions supporting data rates in excess of 2 Mbs are expected.  

While the pervasive nature of WWAN systems are enticing relative to the needs of small mobile devices such as PDA’s, the broader utility of the systems remains limited. Clearly the available data rate of the provisioned cellular infrastructure today is not sufficient to provide network services to traditional laptop and desktop computers. In fact it is so limited that cellular phone companies have developed esoteric protocols and related gateway services, to compress traditional web information so it can better be delivered over their cell networks.

The Wireless Access Protocol (WAP) Forum is the major industry consortium. WAP is a compiled and compressed protocol distilled from source Wireless Markup Language (WML) content. (WML is a standards spin-off of Extended Markup Language (XML).) Simply put, WML is similar to HTML but enables the design of Web pages that can be displayed on the small view screens of phones and PDA’s. In turn, WMA is compiled in WAP “gateways” where it is greatly compressed into the WAP protocol and then transmitted across the wireless network to WAP enabled clients. All this processing is done simply to allow the transmission of information over a very low bandwidth wireless pipe.

There is a huge trend in the wireless industry to support WAP. Understanding the ramifications of this direction is important for Cornell departments interested in extending information across the cellular phone network to connected devices. The prime issue deserving thought is the design of web content conforming to WML structure in parallel with standard HTML, SHTML, and XML pages. Then, web portal technology must be deployed to automatically detect the nature of the requesting client and direct the appropriately formatted page in response.

Satellite Based Wireless Systems

Although they are wireless, satellite based wireless systems are outside the practical intent of this document to some degree. Nevertheless, satellite based systems can be viewed as an augmentation to WWAN services. However the cost value of service is often limited to specific applications, most notably those applications that benefit from one-direction broadcasting of content or communication to locations on the globe not serviced by other means. Bi-direction communication using satellites to support highspeed and/or pervasive connectivity on the Cornell campus simply is not a practical approach today. But the use of fixed location satellite receiving stations on the Cornell campus to receive broadcast information from content providers is an important resource to leverage.

Wireless Implementation Issues

There are several key points to keep in mind when outlining the deployment of wireless services.

- Because of the “churn” in the wireless industry, any system deployed today has a limited “state of the art” life span.
- Each of the different types of wireless technology is targeted at a slightly different user base and/or coverage targets.
- Inherent interoperability of WPAN, WLAN, and WWAN systems is non-existent today.
- Each type of system has limits.

In short, the vision of a ubiquitous and integrated wireless service for Cornell comprised of a selected suite of solutions is not likely in the near term.

8 http://www.wapforum.org/
9 http://www.w3.org/
Wireless also has limitations when compared to the wired network infrastructure. There tends to be a fair amount of discussion of the potential for wireless to replace all needs for wired a network at Cornell. This is not a viable argument today. Wireless is simply no match for the high data speeds (in excess of 1 Ggbs) and service quality levels deliverable on modern wired networks.

The wireless systems under consideration for Cornell currently enable shared 11 Mb resource. (The 11 Mb rate is a function of the proximity of the receiving client: the weaker the signal, the slower the connection.) Even with expected enhancements to wireless data rates, wireless systems will not have the same quality of service, or network application potential of wired systems. To place this into practical context, wireless data rate services are, at best, the equivalent of 10-year old twisted pair wired networking technologies.

Other wireless limitations include:

- No current provisions for quality of service, thus eliminating support for voice and video services.\(^\text{10}\)
- Interference prone nature of the radio spectrum makes guaranteed service problematic.
- Short "state of the art" technology life spans.

Regardless, users of 11Mb wireless services worldwide find excellent utility within current data rate limitations - and wireless allows a wonderful form of connectivity that wired systems cannot afford – mobility. Today, wireless networking has become a desired service class enhancement, to the broader wired network at Cornell.

If one of the great values of wireless is client mobility, deploying many uncoordinated “one-off” implementations may be shortsighted. Enabling a larger campus-wide service, however, is far more challenging. Challenges include:

- IP number allocation to mobile devices.
- Coordination of wireless network deployment.

IP number allocation is complicated by the mobile nature of wireless users. IP numbers at Cornell are mostly bound to a physical location. (An IP number is the unique Internet Identity of your host, not unlike the phone number of your phone.)

In most standard routed network configurations, you would not be able to unplug your computer, walk to another building on campus, plug it in, and expect the IP number to work. You would be on a different part of the network and each part only supports a certain specific list of IP numbers (a subnet).

Dynamic Host Configuration Protocol (DHCP)\(^\text{11}\), can solve the problem of having a static IP number assigned to your computer, but DHCP servers still need to allocate a number that will work within the subnet of the computer’s given connection. To work around this issue for “mobile” computers requesting IP numbers from DHCP servers, organizations have two options. One is to leverage the installed campus routers’ ability to create a campus wide “virtual” network (VLAN) and forge a single dedicated network and broadcast domain for projected wireless usage, thus allowing IP numbers to work regardless of the router hardware they ultimately pass through. Another approach is to consider the implementation of Mobile IP\(^\text{12}\).

Interference caused by other devices using the same part of the radio spectrum is another issue of concern for wireless network systems. 802.11b/g services use the same spectrum allocation as Bluetooth, many cordless phones, and other wireless devices. Users of wireless service should keep this in mind when setting their expectations for service quality. Additionally, wireless networks based on 802.11x must be coordinated. Two or more access points need to work in concert with each other. While 802.11b/g has 11 channels, cell to cell coordination requires at least 3 and popular deployment wisdom recommends an unused channel between each. In short, all 11 channels can be consumed by one integrated wireless system. In an attempt to assure reasonable wireless service quality many peer universities have strong central control over

---

\(^{10}\) IEEE 802.11e work group is defining 802.11 QoS standards.

\(^{11}\) http://www.dhcp.org/

\(^{12}\) http://www.ietf.org/html.charters/mobileip-charter.html
the use of the electromagnetic spectrum and related wireless deployments. Many universities have policies banning independent deployments and specific types of “offending” technologies. Given Cornell’s independent spirit, the notion of central control of wireless air space may be distasteful, however lack of coordination would be far worse. It will remain an important IT architecture goal to figure out the best means to coordinate and resolve these conflicts. The simple desire to work together may foster the greatest returns.

Wireless and Security

Unlike data on wires, which can remain inaccessible in walls, barred underground, and locked behind doors; data carried on general coverage wireless networks is there for all to receive. Open access to wireless data means that if a transmission is of a sensitive nature, precautions must be taken to protect the information. Most wireless technologies offer data encryption to protect data from being read by an unintended recipient. However, users of wireless networks should not assume all configurations have enabled or effective security services.

Currently interoperable "standards based" 802.11 systems, as defined by the Wireless Electronic Computability Alliance (W-Fi) requires support for Wired Equivalent Privacy (WEP) encryption services. However WEP is of little to no value in large open deployments as is envisioned for Cornell. WEP uses static "keys" that any user of the wireless system must know. Once a master key code is disseminated to a large campus, it is silly to assume any value in encrypting streams that anyone with the key can simply decrypt. In turn, many pockets of small wireless nets, each with their own "keys," would not allow roaming. This WEP limitation and other sever security weakness of the 802.11 security services are well understood by the 802.11 development community and hardware manufactures. The IEEE 802.11e (task group E) is in the progress of defining enhanced 802.11 security tools. However it is not clear when these will be available or declared a universal requirement of inter operable 802.11 wireless deployments as certified by Wi-Fi. In the interim individual vendors are beginning to market vendor specific enhancements to their 802.11 offerings. The disadvantage of this approach is the requirement of a sole manufacture source infrastructure to take advantage of the products enhanced security features.

Wireless and Authentication

Eavesdropping is possible on a wireless network which means precautions must be taken to prohibit unauthorized use of the service. In order to restrict illicit consumption, additional authentication procedures are required. Most are based on procedures requiring the pre-registration of legitimate 802.11 clients. A more sophisticated approach could be via an authentication server that challenged user access before data packets could be transmitted to the general campus resource. Not only is authentication an issue relative to limiting access to the net, it is also important for users of a wireless network to be assured the access point to which they are connecting is really a legitimate agent of the expected service provider. It is conceivable that anyone with a current 802.11 access point and relevant hardware could easily "spoof" the legitimate campus network and those devices within! As with the limitations with basic WEP, the need for broader 802.11 security resources is being addressed through the 802.11e process and one off vendor solutions.

Deployment Directions at Cornell

Keeping in mind the technologies and limitations outlined above, Cornell must make a balanced investment in wireless services. Because wireless is a new network utility, it also represents a new expense. Wireless deployments will not lower the support costs of the wired system, nor will wireless systems be able to deliver all the network services available on wired networks. Given this, initial wireless deployments at Cornell should be targeted where wireless utility is seen to have the greatest value, i.e., at those locations

13 http://www.wi-fi.org/
14 http://gruper.ieee.org/groups/80211/
where patrons will utilize en masse insecure networking to support mobile computing devices. These locations are likely to be locations such as University Libraries, dining halls, and other finite locations conducive to wireless’s value.

Ongoing and recommended installations of wireless services at Cornell are based on the WLAN technology 802.11b/g. After much practical review of WPAN/WLAN development in the United States, 802.11x is the mainstream “commodity” product of choice with a growing base of industry providers. But again, by implementing one form of wireless you do not enable all classes of wireless services. Users of an 802.11b enabled laptop computer will not be able to use that same wireless system as their cell phone. Or, users of a Bluetooth or WAP enabled palm will not be able to directly connect with the 802.11b network.

Until there is a convergence in wireless strategies, or effective gatewaying tools, a unified vision of wireless is not a reality. This is not to say the Cornell should ignore the expected increase in Bluetooth, WAP enabled devices, and future high-speed 3G cellular services or the infrastructure required to support them. But the value of the service must be balanced against the cost. Cornell should keep abreast of ongoing development to assure due diligence investment in new wireless systems at optimal times.

Regarding IP numbers, the current plan at CIT is to implement a DHCP service to allocate IP numbers to registered hardware. This is the simplest and most straightforward means to resolve IP allocation today. But it will not resolve the long term desire to permit Cornell IP number allocation to wireless devices outside of Cornell’s wireless system, and it may be problematic to provide service to tens of thousands concurrent users.

**Practical Implications**

Departments interested in 802.11b wireless services should be aware of the limitations and unique benefits when considering deployment. In review these are:

Current Limitations and Deployment notes:

- 802.11 is not a Bluetooth or a cellular phone class service.
- 802.11 will not provide the same data rates and quality of service as a wired network.
- Current "public" 802.11x transmissions at Cornell are not secure!
- High power consumption wireless means larger battery needs for many mobile devices.\(^{15}\)
- Wireless systems are prone to interference. Be prepared for frustrated users.
- Wireless systems must be coordinated if patrons expect campus wide mobility.
- Wireless systems require a network configuration to support a roaming IP number.
- Future wireless security systems being outlined by the IEEE 802.11e work group will require campus wide coordination to be effective.
- Churn in the wireless industry means demands for better/new wireless services in the near term.

Current Benefits:

- Mobility.
- Extending network to areas that are cost prohibitive to run wire.
- Current 802.11b deployments will have valued utility for an extended period despite new "state of the art" wireless developments.

Perceptions of cost savings that may be afforded by wireless systems to extend network connectivity to locations that are cost prohibitive for traditional wired services must be realistically tempered. First it is

---

\(^{15}\) There is conflicting opinion on the practicality of 802.11 for PDA class devices.
important to note that the users of WLAN's will still use the campus backbone and Internet resources just as much as those connected via traditional wired network. In turn, wireless hubs do not remove the obligation of users to pay their fair share for the cost associated with the larger campus and Internet services leveraged.

On the surface, using wireless hubs to deliver network services to currently wired stationary hosts may seem to be a way to reduce the total cost of networking. In reality, replacing existing wired repeaters with wireless only lowers the network quality to your patrons and reduces the network’s ability to support enhanced services such as video on demand or video conferencing.

**Closing Thoughts**

Despite limitations, the benefits of a coordinated, focused deployment of a wireless network at Cornell is resolutely encouraged. The benefit of allowing user mobility and extending the research and teaching value of network accessible information to new locations is seen to have clear value by the Office of Information Technology.

Ideally, departments will see the inherent value of a coordinated implementation — an implementation that enhances mobility, the primary value of the technology. In fact, there is a defensible argument to be made that in order to take advantage of future enhancements in wireless technology that will afford a secure and mobile wireless resource, deployments must be coordinated. Minimally this would require:

- Campus wide VLAN and DHCP services for wireless.
- Campus wide coordination of radio spectrum allocation.
- Common security and authentication strategy.

In parallel with this initial deployment, Cornell Information Technologies and interested departments must keep a vigilant eye on industry trends and be prepared to retrofit the wireless system when appropriate. The long-term goal is to create an integrated, seamless wireless system capable of supporting the full range of network devices in use or envisioned.