

# Methodology for the Deployment of Effective Campus Wireless Environment Infrastructures

Riad Lemhachheche, J. David Porter, Thanit Puthpongsiriporn  
Department of Industrial and Manufacturing Engineering  
Oregon State University  
Corvallis, OR 97331, USA

## Abstract

The utilization of wireless local area networks in campus settings to enhance instructor-student interaction is quickly gaining acceptance throughout the world. The deployment of such network infrastructures in an educational environment imposes challenges that are significantly different from similar systems typically deployed at enterprises or commercial settings (i.e., Hotspots). This paper presents a methodology for the deployment of effective campus wireless environment infrastructures that was developed based on the results of a web-based survey conducted by the authors in collaboration with Intel Corporation. Institutions surveyed were asked to provide information on different categories related to their wireless deployment including deployment and management strategy, types of user categories, hardware infrastructure, security and cost of ownership.

## Keywords

Campus wireless deployment, SOHO, Wi-Fi, WLAN

## 1. Introduction

The networking technology known as Wireless Local Area Network (WLAN) has experienced a tremendous growth over the last ten years [1]. WLAN technology enables the connection of network devices over an air-based interface with the use of radio frequency communications. The standardization efforts by the IEEE under the IEEE 802.11 family name and the interoperability efforts by the Wi-Fi Alliance have helped the widespread adoption of WLANs by businesses, Small Office Home Office (SOHO) and the general public. The ease of deployment of WLANs to extend existing wired networks or to build new networks from the ground-up coupled with advances in the Internet have made it the logical choice for public hotspot, conferences centers and home networking.

## 2. Background and Motivation

The deployment of WLAN-based infrastructures in educational environments poses challenges to IT architects that are significantly different from those found in similar systems deployed at enterprises or in commercial settings (i.e., Hotspots). For example, services offered through a HotSpot are normally subject to a fee whereas in a campus setting these services are free of charge. Also, a variety of users with different needs (e.g., students, faculty, administrators, etc.) have to be considered in the design resulting in different applications and security requirements per user category.

A first approach in the deployment of a campus wireless environment could be to try to separate higher education institutions in tiers based on their size (e.g., small, medium and large campuses) and then define common characteristics and needs for each individual tier. However, the results of the on-line survey conducted with 12 institutions of higher education coupled with information found in 38 campus wireless user guides indicate that campuses cannot be easily classified in tiers based solely on size. A wide variety of factors play a role in the definition of a campus wireless environment including campus size, type of users, and security and performance requirements among others. Therefore, a design methodology is needed to help IT architects to successfully deploy a campus wireless environment based on the institution's specific requirements and limitations.

### 3. Campus Wireless Network Requirements

Home users normally use wireless networking to obtain more comprehensive access to the Internet or to share files and printers. The small number of devices connected to the home wireless network makes it feasible to implement simple authentication and security schemas like medium access control (MAC) addresses filtering or the Wired Equivalency Privacy (WEP) protocol, both widely available on low-cost commercial access points. While MAC addresses filtering restricts wireless network access to specific devices, WEP allows authentication and secure transmissions between the access point and any device who share the same secret key.

Corporate wireless network are aimed at providing added coverage to the corporate wired network in areas such as meetings rooms. In most cases, corporate wireless networks users are assumed to possess the credentials necessary to physically gain access to the wireless network. Indeed, well-designed corporate wireless networks are only available within the corporation's building and therefore only accessible to employees and visitors allowed inside the building.

Contrary to home or corporate wireless networks' users, campus wireless network users are highly mobile during the day and expect to be able to use computing resources regardless of their location on campus. Ease of use to access resources from residence halls, classrooms, and library or study rooms can bring valuable benefits to students and faculty in their day-to-day activities. Table 1 shows a comparison among home, corporate and campus wireless environments (developed by the authors) based on six different requirements. It is clear that campus wireless networks are a more challenging environment for the deployment of WLAN technology.

Table 1. Issues and Concerns with Different Types of Wireless Local Area Network

Requirement	Home	Corporate	Campus
Security of Transmissions	Low	High	High
Management Issues / Policy	Low	Medium	High
Secure Physical Access	Low	Low	High
Variety of Users	Low	Low	High
Coverage	Low	Low/Medium	High
Usage pattern (peak)	Low	Medium/High	Medium/High

EDUCAUSE, a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology, surveyed its members in 2001 in regard to campus wireless networks [2]. The survey revealed that smaller campuses (less than 10,000 full-time students) are more likely to implement campus-wide wireless networks from the start, whereas larger institutions will roll out deployment progressively in specific buildings. According to the results of our survey as well as campus wireless connectivity user's guide available online, small to medium institutions are more likely to deploy a campus-wide wireless network managed by a central IT structure. Larger institutions, on the other hand, will start the deployment earlier at one of their colleges or departments (generally computer science or electrical engineering) and use it as a test bed for the rest of the institution.

Results from our survey as well as publicly available information indicate that there is no direct correlation between the size of the institution (i.e., number of students) and the extent of wireless coverage on the campus. For example, the University of Twente in the Netherlands deployed in 2001 "Europe's largest Wi-Fi Hotspot" with campus-wide deployment for its 7,100 students while the University of Texas – Austin, the campus with the largest number of students in the US, does not currently offer comprehensive wireless coverage to its 50,000 students. Table 2 shows the scale of coverage for a sample of different size institutions in the U.S.

Table 2. Deployment Scale in Various Universities

Institution	Type	Scale of Coverage	Enrollment	Size (Acres)
Dartmouth College	Private	100 %	5,700	200
University of Twente	Public	100%	7,100	346
Oregon State University*	Public	30-50%	19,000	500
University of British Columbia	Public	100%	39,300	982
University of Texas – Austin*	Public	50-70%	50,000	350

\*: coverage estimates as of Jan 2005

#### 4. Campus Wireless Environment Deployment Methodology

Most educational institutions follow the steps shown in Table 3 to deploy a campus wireless environment. The following sections of this paper will describe some of these steps in more detail.

Table 3. Campus Wireless Network Deployment Process

<b>1. Collect Requirements</b>	User Requirements
	Management Requirements
	Network Requirements
<b>2. Perform Site Survey</b>	
<b>3. Develop the Initial Design</b>	Network design
	Choice of wireless link technologies
	Authentication and security mechanism
	Services supported
<b>4. Deploy Wireless Network</b>	Install hardware
	Test connectivity and performance
<b>5. Make Network Live</b>	
<b>6. Monitor Performance</b>	Adjust settings as appropriate

##### 4.1 Define Requirements

A campus wireless network needs to satisfy different types of requirements:

1. **User requirements.** These include issues related to the performance of the WLAN from the point of view of the user. Examples include the minimum number of users that access points must support, roaming/mobility expectations and access to resources on the wired network (e.g., shared network drives, printers, and classroom resources through direct or VPN connection).
2. **Management Requirements.** These are requirements that the institution that owns the campus wireless environment must take into consideration in providing wireless access services. Examples include access control (who can and cannot access the network), maintenance requirements, remote management capabilities and wireless network availability.
3. **Network Requirements.** These requirements are essentially derived from the user and management requirements and include characteristics that must exist on the network. Examples include mechanisms for the user to provide credentials for the purpose of login into the system, network backhaul requirements, network backbone requirements and IP address management.

Universities usually form a committee including experts in wireless networking, IT staff and a project manager. An example of this process can be found in the description of the deployment of the campus wireless network at the University of British Columbia, considered the largest campus wireless deployment in Canada to date [3].

## 4.2 Perform Site Survey

A site survey is run prior to deploying the wireless infrastructure in order to optimize the coverage of the campus in regard to the radio frequency signal. Site surveys in campuses are particularly important since it is not unusual to have campus buildings with different age, design and layout. Also, wireless network requirements and usage can vary greatly from hallways to amphitheaters that accommodate 200 plus students. Site surveys can be performed in three main ways:

1. **Basic approach.** No site survey is performed prior to the deployment. Wireless access points are deployed in a logical manner such as at regular geographic interval. This approach usually does not take into account the specifics of radio frequency propagation and requires adjustments in order to provide comprehensive coverage of the target area.
2. **Ad hoc approach.** Simple tools such as laptops or personal digital assistants (PDA) are used to prepare for the wireless deployment. Once the deployment is done, these same tools are used to validate the design and adjust access point's location to provide a complete geographic coverage of the target area.
3. **Full coverage approach.** The site survey is run using advanced equipment such as a computer on a cart, which will make precise measurement of radio signal propagation throughout the buildings to be covered. After deployment, a second phase consisting in wireless traffic measurements needs to be performed to match wireless usage with bandwidth made available.

Table 4 shows the type of site survey and the equipment utilized at three different institutions. More details on site surveys and these three institutions' deployment specifics can be found in Intel's guide on campus wireless networks [4].

Table 4. Site survey approaches in campus wireless network deployment

	<b>Basic Approach</b>	<b>Ad Hoc Approach</b>	<b>Full Coverage</b>
<b>Example</b>	Saint Joseph's Academy HS Baton Rouge, LA	Oregon State University Corvallis, OR	Carnegie Mellon University Pittsburgh, PA
<b>Site Survey Equipment</b>	-	PDA site survey Trial and Error	Computer Cart Usage pattern
<b>AP placement</b>	Regular interval	Optimal geographic coverage	Optimal geographic coverage + Minimum data rate guaranteed

## 4.3 Network Design

### 4.3.1 Network Authentication

The responsibility assumed by the access point in the wireless infrastructure can differ from one deployment to another. In small deployments where the wireless infrastructure will mostly be used to provide access to the Internet, access points will assume most of the responsibility towards the wireless client and will need to be configured for all tasks related to the wireless connectivity. These tasks assumed by these 'smart' access points include:

1. Provide wireless signal to the client and broadcast information about the wireless network such as identification data (i.e., service set identifier or SSID).
2. Associate to the mobile client.
3. Encrypt the communication between the access point and the client (optional).

4. Authenticate the mobile client (optional) and grant access to the local network/ the Internet.

However, in a campus wireless environment with hundreds of access points, managing these ‘smart’ access points can become really complex. Indeed, security and identity management has been recognized as the number two issue for campus IT administrators in 2004 [5]. A network design more adapted to such a large scale deployment is to limit the responsibilities assigned to access points. Oregon State University, for example, limits the role of the access points in its wireless network design to only providing information and signal from the wireless network. Once the client is associated with the wireless network, the access points hands down the rest of the tasks to other devices on the local network.

The client will be redirected by the access point to an authentication platform that will require the entry of credentials through a web browser interface. The authentication platform is located behind a firewall, which would block all other type of traffic until the user gets authenticated, as shown on Figure 1. The credentials required are the account login identification and password; these credentials are the same throughout the OSU campus to access computing services. This authentication is made secure by using the secure sockets layer (SSL) protocol to encrypt the information transmitted within the web pages. The authentication platform will then record client information such as hardware addresses (i.e., MAC addresses) to let the client access the wireless network without re-identifying for a specified amount of time (i.e., 24 hours).

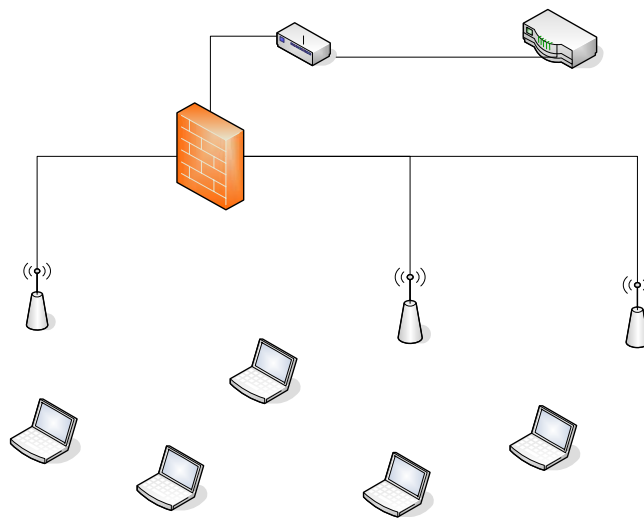


Figure 1. Example of Oregon State University Network Design Architecture

Access to basic services (e.g., e-mail and web browsing) is granted to all the wireless users authenticated on the network. To access advanced services such as network drives, MS Outlook, printing, OSU requires users to open a VPN session after being connected to the wireless network.

#### 4.3.2 Security Mechanisms

The technology deployed to secure the wireless transmission can vary greatly between institutions. The main reasons are the known issues with the security protocols included in the IEEE 802.11 standard and the difficulties to implement them on a large scale. Most universities currently do not provide encryption and rely on usage policy or other security schema.

Table 5 shows the different approaches taken by a sample of institutions with regards to securing the transmission on their campus wireless networks. Information enclosed in parenthesis indicates optional features. The institutions listed in Table 5 were selected from the 12 respondents to our online survey and a sample of 38 universities whose online connectivity guide is publicly available online.

Bridge / Authenticat

Table 5. Security schema implemented in campus wireless networks

Institution	Security Mechanism
Carnegie Mellon University	VPN
Columbia University	N/A
Princeton University	N/A
University of Maryland	(VPN)/ MAC
University of Michigan	WPA
University of New Mexico	WEP / MAC
University of Tennessee	WEP / (VPN) / MAC
University of Texas	N/A
University of Utah	802.1x
University of Washington	N/A
University of Wisconsin	N/A

#### 4.4 Cost

The financial data available from the campus wireless network deployment at Oregon State University, Carnegie Mellon University [6] and Saint Joseph's Academy High School made it possible to define an estimated cost for the deployment. Estimated costs to deploy a campus wireless network are \$600 per access point with power over Ethernet. This estimate includes the networking equipment, power and data cable, and labor costs for installation only. Planning, backhaul or wired backbone costs, software or hardware upgrade costs are not included. Additional costs are associated to user and security management and are dependent of the implementation scale.

## 5. Conclusions

This paper presented the specifics of deploying a campus wireless network. Even if each institution is different in terms of needs, resources and expectations, common design 'best practices' can be learned from the experiences of institutions who already went through the process of designing and implementing a campus wireless environment. A more comprehensive survey of educational institutions at different levels of implementation will hopefully provide more common characteristics and 'best practices' to be used by campus IT staff in their deployment.

## Acknowledgements

The authors wish to acknowledge the support of Intel Corporation in providing the funding necessary for this research.

## References

1. Kapp, S. "802.11: Leaving the Wire Behind", *IEEE Internet Computing Online*, January/February, 2002
2. R. Boggs and P. Arabasz, 2002, The move to wireless networking in higher education. Research Bulletin of the EDUCAUSE Center for Applied Research, April 2002.
3. J. Martell, D. Michelson, S. Mair, and D. Zollmann, 2003, "Deployment of Canada's Largest Campus Wireless Network at the University of British Columbia" Information Technology: Research and Education, 2003. Proceedings. ITRE2003. International Conference on Information Technology, 11-13 Aug. 2003 Pages:360 – 364
4. Juan Rivero, J. David Porter, Thanit Puthongsiriporn, William M. Layton, Riad Lemhachheche, 2005, "Campus Wireless Environment Deployment Guide", Intel White Paper (draft), 2005
5. Donald Z. Spicer, Peter B. DeBlois et al, 2004, Fifth Annual EDUCAUSE Survey Identifies Current IT Issues, EDUCAUSE Quarterly Articles (2004)
6. Paul Arabasz, Judith Pirani, 2002, Wireless Networking at Carnegie Mellon University, Case Study from the EDUCAUSE Center for Applied Research, 2002