



# Empowering Wi-Fi™ Networking in

EDUCATION

December, 2005

The logo for XIRRUS, featuring the word "XIRRUS" in a bold, blue, sans-serif font. A small orange circle is positioned above the letter "I".

### Executive Summary

The primary purpose of educational institutions is the advancement of knowledge. To be successful, schools must intelligently select and deploy technologies that will attract the best and brightest students and faculty. Delivering a powerful Wi-Fi™ solution as the primary network in an easy, cost-effective, and scalable manner has been challenging for limited IT staffs – until now.

Xirrus has developed the next generation in high-performance Wi-Fi networking equipment to easily deliver maximum Wi-Fi capacity campus-wide. At the heart of this revolutionary solution is the Wireless LAN Array – combining a Wireless LAN Switch and up to 16 Integrated Access Points to deliver 864Mbps of Wi-Fi bandwidth over a large coverage area.

This innovative approach simplifies the deployment and management of Wi-Fi networks while maximizing Wi-Fi bandwidth and coverage, creating confidence in your network's abilities today and tomorrow.

### Introduction

Competition among educational institutions is hotter than ever. To attract the best and brightest, schools must offer state-of-the-art learning facilities including campus networks that continually adapt to enable open learning and collaboration among its members. Technologies such as the Internet, campus intranets, e-mail, and databases link individuals to their studies, research, work, must be accessible on- or off-campus. The trend for increased learning anytime, anywhere has fueled the growing demand for technologies such as campus-wide Wi-Fi networks.

This paper details the issues surrounding the deployment of Wi-Fi networks on educational campuses and describes how Xirrus' innovative Wireless LAN Array architecture addresses these issues; enabling a powerful campus-wide network.

### Technological Realities on Campus

There is a long standing partnership between Information Technology (IT) and Education. For example, Education created the technology that led to the Internet, and continues to utilize the Internet today for applications such as online collaboration and distance learning. Over the past decade, schools have invested heavily in technology to enrich student experience and administrative functionality. However, campus IT has realized that not all technologies benefit the advancement of knowledge. Today, schools are approaching technology more carefully and strategically. As part of their technology strategy, schools must deal with the following forces:

#### Increasing Expectations

Students, faculty, administrators, and staff expect on-demand services such as online collaboration, instant access to research, self-serve administration, and distance learning. As an example, there are a growing number of schools offering online access to lectures and course material both on-and off-campus to provide greater convenience and flexibility for students. The National Center for Education Statistics calculated that students taking at least one online course grew nearly 50% over the past four years. Networks are playing a critical part to facilitate these growing demands.

### Fierce Global Competition

There is escalating competition among schools to attract the brightest students, educators, and researchers in order to enhance the stature of the institution and draw funding for the schools. A student's ultimate goal is to find a rewarding career and to better society. Whatever career they choose, students will be using computers and other information technologies. How they use technology in their degree programs will affect them in that chosen career, so schools are working harder to intelligently adopt the right technologies that will ensure their competitiveness.

*"You're not just a student; you're a consumer too...and should know what you're paying for, so ask."*

Educause Website

### Financial and Staff Resource Restraints

Let's face it; IT staff is stretched thin with daily tasks of planning, managing, and upgrading networks. IT is being asked to do more with less. Schools are frantically looking for ways to push their campus network beyond the current stagnant locations. Campus IT needs alternative technologies to lighten their work load, save money, and provide a positive experience to campus stakeholders.

### Security, Regulatory, and Policy Demands

Students are very creative leveraging technological tools for entertainment and social ends, which can consume bandwidth and inadvertently compromise network security. According to the 2005 Campus Computing Project survey conducted earlier this year, "College and university IT officials identify network and data security as the single most important IT issue affecting their institutions over the next two-three years."

IT needs a simplified approach to implement and manage security on campus and in dormitories. Beyond security concerns, campus IT must also deal with government regulations and institutional policies from all levels.

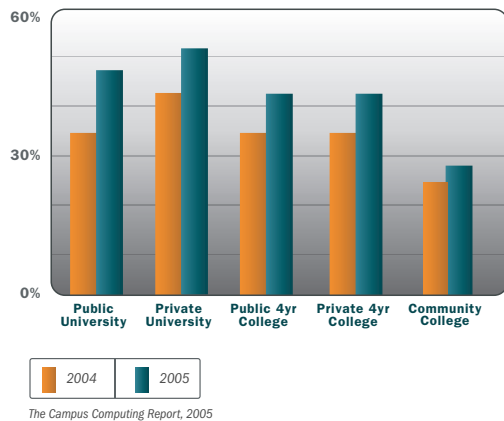
### Challenges of a Campus Network



### Benefits of a Wireless Campus

One of the fastest growing technologies being adopted by education is Wi-Fi networking. The trend towards mobile communications among students, faculty, administrators and staff has pressed the migration from stagnant wireless hot spots to more ubiquitous wireless coverage campus-wide. The 2005 Campus Computing Project survey found that campuses with strategic plans for Wi-Fi networks increased 164 percent, from 24.3 percent in 2001 to 64 percent (nearly two-thirds) in 2005. Wireless service in college classrooms increased 6.7 percent over the past year according to this same study. Private universities are leading the way with 53.8 percent (up 47.4 percent year-over-year) offering Wi-Fi in classrooms, while public universities and community colleges follow close behind. There are several benefits of Wi-Fi that positively affect students, faculty, administrators, and staff.

### Wireless Classrooms, 2004-2005



### Mobile Connectivity

Anytime, anywhere network access provides students with the ability to participate in learning while sitting in the classroom, lecture hall, student lounge, library, dormitory, cafeteria, etc. They can freely move about the campus, able to search for materials both in and out of the institution's knowledge base.

#### Where to Deploy Wi-Fi?

Libraries	Lecture Halls
Classrooms	Study Areas
Cafeterias	Faculty Offices
Conference Rooms	Dormitories
Lounges	Remote Classrooms
Stadiums	Outdoors

### Online Communication and Collaboration

Wi-Fi networks turn classrooms and lecture halls into real-time, interactive learning centers allowing students and teachers to collaborate and input comments directly into course materials. Students can communicate with classmates across campus to discuss projects while traveling to and from class. Instructors can deliver assignments, course materials, and institute online activities outside the classroom to create an integrated learning experience. Administration can implement 24/7 systems such as online class registration, course management, and financial assistance. By fostering collaborative learning, Wi-Fi networks enable the institution to better support its mission of advancing knowledge.

### Wi-Fi LAN Applications

E-Mail	Internet Access
Intranet Access	Network Access
Interactive Lectures	Library Research
Project Collaboration	Temporary Networks

### Global Competitiveness

We live in a digital age when high-speed access to networks is expected. Students and faculty are more technically savvy than ever before. Providing a persistent connection throughout the campus and living areas will positively affect the school.

### Cost-effective Network Deployment

Hard-wiring a campus LAN is both difficult, costly, and in cases of older historic buildings, nearly impossible. A Wi-Fi network can be deployed more quickly and with less operational overhead. While the Wi-Fi equipment may be more costly upfront than a traditional wired network, overall installation expenses and life-cycle costs are usually considerably less. Further, operational overhead associated with new Ethernet cable pulls and changes are virtually eliminated. For example, the remote or portable classroom in need of a network connection – Fixed connections are expensive and rarely practical, while a Wi-Fi network offers a cost-effective solution.

### Challenges of a Wireless Campus

Despite the benefits gained from wireless, deploying a campus-wide Wi-Fi network has distinctive challenges for IT to resolve:

#### Varying Population and Traffic Flow

Population and traffic flow is unpredictable requiring a scalable Wi-Fi network. This problem becomes even more critical as wireless grows in popularity and versatility—clients will include not only PCs and handheld devices, but also phones and streaming video devices. Like any shared network, more users equal less bandwidth. Due to the collision rates among clients seeking access, performance drops as more clients associate to a given access point creating the challenge to address high density areas (lecture halls, dormitories, and libraries).

The typical response from traditional Wi-Fi vendors is to place more access points in a general area; however, this creates co-channel interference, especially 802.11b/g networks, which only have three non-overlapping channels. Channel planning for dense areas traditionally require RF expertise and a significant investment for additional wireless components, without getting the bandwidth needed for student requirements.

### Expansive Coverage Area

Schools typically consist of large buildings sprawled over hundred of acres making RF coverage difficult. No matter what type of Omni-directional access point is used (“fat” or “thin”) blasting RF energy in all directions becomes a barrier to performance. A number of issues arise that limit high-performance deployments: cell size, channel reuse, hidden Wi-Fi nodes, and multi-path. (For more information on the limitations of Omni-directional access points, please refer to the “Sectorized Wi-Fi Architecture Benefits” Whitepaper by Xirus.)

### Too Many Devices to Deploy and Manage

Traditional Wi-Fi vendors try to resolve issues with dense deployments and limited bandwidth by increasing the number of infrastructure devices (switches, access points, security monitors, software, etc). This increases the complexity, deployment, management, and overall cost of the network, while adversely decreasing the network’s capacity and performance due to continued co-channel interference and the ability to efficiently use all non-overlapping channels. Throwing more devices at the problem increases the burden and cost to IT– this is not a solution.

### Challenges in Wi-Fi Networking



### Multiple Security Levels

Varying levels of network access and permissions are needed for undergraduate and graduate students, teacher assistants, faculty, administrators, and senior staff. Some applications require heavy security and policies while others are accessible to guests. Deploying multiple security levels is required for any network.

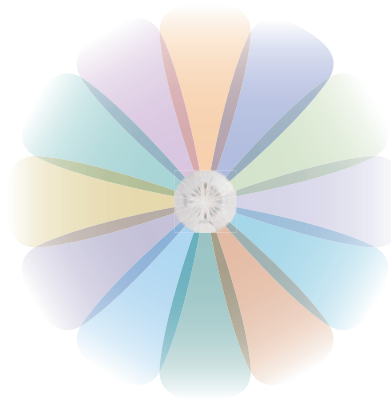
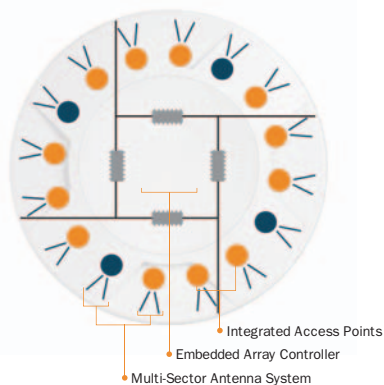
### Planning for Tomorrow

The explosive growth of Wi-Fi creates the challenge of meeting the needs of current coverage and client capacity while being able to scale in the future to accommodate higher user densities and new applications. Adding more infrastructure devices and more planning software exasperates the challenge of managing and meeting the needs of a growing network.

### The Xirrus Approach

The Xirrus Wireless LAN Array enables educational institutions to intelligently deploy a cost-effective Wi-Fi solution that maximizes Wi-Fi bandwidth and coverage, creating confidence in their Wi-Fi network's abilities today and tomorrow. With Xirrus, Wi-Fi networks no longer require a sea of "inconsiderate" access points that limit channel reuse, and that create hidden node and multi-path issues yielding poor performing networks.

#### Wireless LAN Array: Sectorized Antenna System



#### Bandwidth to Support Wi-Fi Growth

The Wireless LAN Array can deliver up to 864Mbps of Wi-Fi bandwidth. By integrating up to 16 separate Integrated Access Points in a single platform, Xirrus has created a solution for today and tomorrow's bandwidth intensive applications. Each Xirrus Wireless LAN Array can take the place of up to 16 separately installed legacy access points and handle hundreds of simultaneous users. Additionally, one integrated access point can be used as a dedicated full-time RF sensor for the detection of rogue access points and other security threats.

#### Sectorized Approach Simplifies Deployment

Most legacy access points today make use of Omni-directional antennas. Omni-directional antennas transmit and receive RF energy in all directions much like a light bulb. The Xirrus Wireless LAN Array incorporates a Multi-sector Antenna System focusing RF energy into single directions across multiple radios providing 360 degrees of Wi-Fi coverage.

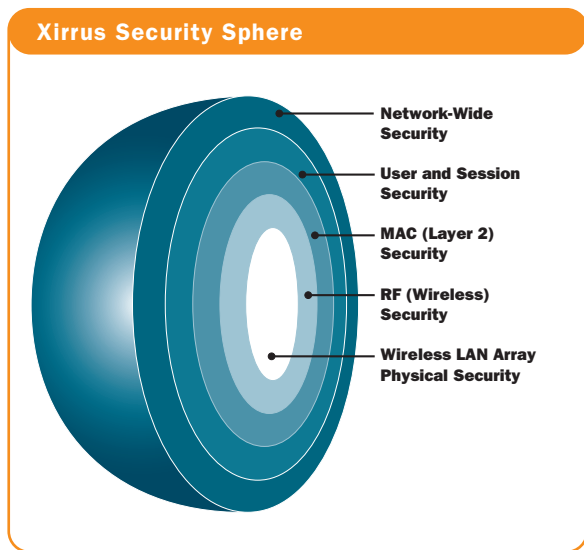
Sectorizing the antennas intensifies the strength of the RF signal that is transmitted, much like a flashlight directing a strong beam of light in the direction that it is pointed, thereby providing the ability to transmit further and "listen better" to the signals of wireless clients.

#### Delivering a Cost-effective Alternative

The Wireless LAN Array delivers more bandwidth and a larger coverage area at a fraction of the cost. Instead of installing large numbers of access points, each requiring its own Ethernet connection, a single Wireless LAN Array can be installed. The Xirrus approach frees IT staff from the hassles of managing a sea of legacy access points, switches, and software packages. The ongoing expenses of network management and maintenance are costly; the fewer devices to manage, maintain, troubleshoot, and upgrade—the better.

### Multi-level Approach to Security

The Wireless LAN Array incorporates a state-of-the-art multi-level approach to address security requirement for Wi-Fi networking on the campus: Physical Security (Chassis), Radio (RF) Layer Security, MAC (Layer 2) Security, User Layer Security, and Network-Wide Security.



### Physical Security

To secure the chassis of the Wireless LAN Array, the power switch is concealed beneath the unit; the chassis can be locked to prevent removal of the unit with a Kensington™ lock slot. For additional chassis security, there is a separate console port for CLI and a separate Ethernet port for out-of-band management.

### Dedicated RF Security

The Wireless LAN Array contains a dedicated Integrated Access Point to continuously monitor and alert the presence of an unauthorized "rogue" access points or unauthorized client station on the Wi-Fi network. In addition, the Wireless LAN Array can scrutinize every Wi-Fi packet, identifying over 135 intrusions (Detect Jamming attacks, DoS Techniques, Session Hijacking, Soft APs, Attack Tools, Day-Zero Attacks and many more). Xirrus is the only solution with full analysis within the built-in sensor, supporting 500 sensors with a single server.

### MAC Security

At the MAC layer, the Wireless LAN Array has complete 802.1x authentication protocol support including EAP-TLS, EAP-TTLS, or PEAP for use with external enterprise-class RADIUS servers ensuring only authorized users gain access to the Wi-Fi network. It also supports strong, government-grade wireless data encryption standards including Wi-Fi Protected Access (WPA) with both TKIP and AES-CCM that eliminates any eavesdropping of wireless packets.

### User Security

Several levels of access control for users can be implemented by defining which Wi-Fi networks each user is allowed to connect to. Administrators can also define which VLANs are assigned to each Wi-Fi network such that physical network separation is achieved for specific network resources. This can restrict user access to specific portion of the network. For smaller deployments, the Xirrus WLAN Array contains an integrated RADIUS server for use with up to 1,024 users to eliminate the cost and administration of an external RADIUS server.

### Network-wide Security

The Xirrus solution provides for secure administration of the Wi-Fi network. All management interfaces are secured with multi-level password protected administrative accounts and assignable privileges. Secure management over the network is done through secure protocols such as secure http (https), secure shell (SSH) and SNMP. Each Wireless LAN Array is authenticated with the Xirrus XM-3300 Central Management System ensuring that only authorized devices are apart of the trusted Wi-Fi network infrastructure.

To secure against stolen clients, MAC addresses can be entered into a special list that will block access for those devices and create an alert to the fact that attempts to access the network are being done with those devices.

Additionally, the use of the Xirrus Central Management System (XM-3300) default policies can be created such that newly deployed Wireless LAN Arrays are automatically configured in compliance with security policies. The use of the XM-3300 will alert the presence of other types of wireless security issues including denial of service attacks, man-in-the-middle attacks, the presence of peer-to-peer Wi-Fi networks and other issues. Further, the XM-3300 can automatically trace these security issues on both the wired and wireless side of the network and automatically contain or eliminate such threats.

Detailed logs that capture network access intrusion along with other security threat alerts are captured on each Wireless LAN Array.

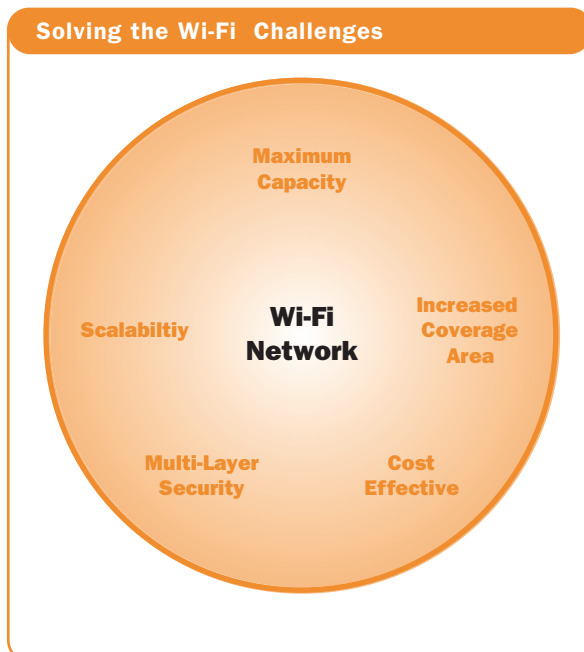
These event logs can be forwarded to an existing enterprise Syslog server, or aggregated to the Central Management System. Logs can then be reviewed and should be part of a periodic compliance audit.

#### **Deploy It Once and Forget About It**

Due to the fact that the Wireless LAN Array makes use of every available non-overlapping Wi-Fi channel, the best possible channel plan can automatically be created and modified as conditions warrant. Legacy architectures force the need to continuously re-architect, rewire and re-deploy the Wi-Fi network and manage even more devices when additional capacity is needed. Xirrus eliminates the need to re-architect and re-deploy Wi-Fi networks by providing the maximum possible bandwidth—“deploy it once and forget it.”

### **Summary**

This Whitepaper has shown the challenges facing educational institutions deploying technologies, specifically in relation to Wi-Fi networks. Today’s traditional Wi-Fi equipment cannot keep pace with the trajectory of needed wireless capacity and coverage. By combining the Wireless LAN Switch, Integrated Access Points, and Multi-Sector Antenna System into one easy to manage device, the Xirrus architecture confidently puts campus IT ahead of demand and creates a high-performance Wi-Fi network that is simple to deploy, easy to manage and flexible enough to handle anything that gets thrown at it. ●





Xirrus, Inc.  
370 North Westlake Blvd.  
Suite 200  
Westlake Village  
California 91362  
805.497.0955 Corporate Office  
805.497.0955 x300 Sales  
805.449.1180 Fax  
[www.xirrus.com](http://www.xirrus.com)

Copyright 2005 Xirrus, Inc. All Rights Reserved. The Xirrus logo is a registered trademark of Xirrus, Inc. All other trademarks and registered trademarks are the property of their respective owners. Content subject to change without notice.  
December 2005