

Wireless Networking

Helpful information and practical strategies for planning, setting up and running your institution's wireless network

TABLE OF CONTENTS

- 2** The Benefits of a Wireless Network
- 2** Selecting the Right Equipment
- 4** Conducting Your Site Survey
- 5** Bandwidth Capacity Planning
- 5** Beefing Up the Backbone
- 6** Content Filtering
- 7** Encryption and Authentication
- 7** Failover and Redundancy
- 8** Wireless Networking Best Practices

Executive Summary

Over the past few years, higher education institutions have begun to place increasing importance and value on their wireless networks. Wireless technology is changing the way students, faculty and staff communicate and interact on campus.

Some colleges are offering courses online via their wireless network. Other universities are utilizing the wireless network to facilitate instructor-to-student and student-to-student dialogues on coursework — outside of the lecture hall.

And students are embracing — if not pushing the limits of — the transformation in the way that knowledge is communicated on campus. Many students are now taking into consideration a school's IT infrastructure as a factor when choosing a college to attend.

The changes taking place on campus should be noted by colleges and universities, and prompt those schools that have not yet begun to explore the many ways that a wireless network can enhance their campus to catch up before it's too late. For those higher education institutions that have already begun to grasp and explore the extraordinary value that their wireless networks can provide, it may be time to consolidate and reassess the role of the wireless network in their mission.

Wherever your organization is at with its wireless network, this white paper has something to offer you. In its pages you will find relevant information about setting up and equipping your wireless network, as well as some best practices for making the most of this valuable resource.

The Benefits of a Wireless Network

Over the past few years, many higher education institutions have begun to adopt wireless technology as the primary means of user connectivity to the network. Much of the motivation behind this adoption is because of the additional benefits afforded by a wireless network, including increased security, mobile Voice over IP (VoIP), easy guest access and asset tracking capabilities.

Such advances help institutions operate more efficiently and productively. As far as budget investments go, colleges would be hard-pressed to find a smarter return on investment.

This increased dependency on wireless communication has resulted in the building of more robust wireless networks capable of delivering voice, video and data in a secure and reliable manner throughout an entire campus. These networks deliver services and applications that were impossible in the past; they grant students, staff and faculty access to needed data and resources, anywhere and at any time.

Increasing the services provided by a wireless network greatly increases an organization's dependency on it. Thus, wireless networks have become an essential element of a university's operational infrastructure.

Consolidated, Simplified, Holistic Administration

Previously, one of the inhibitors of large-scale wireless deployments had been autonomous access points (APs). With autonomous APs, each AP is capable of functioning independently. However, individual maintenance was required on each device. Large deployments became very difficult to manage. Dedicated staff was often needed to provide the wireless local area network (WLAN) with the attention it required.

In recent years, the introduction of centralized wireless architecture has largely resolved this maintenance issue. Utilizing centralized WLAN controllers (discussed later in this white paper), these unified wireless networks have made the deployment and maintenance of robust wireless networks easier than ever.

The solution offers a single point of contact from which administrative personnel can monitor and manage the entire Wi-Fi network. No matter where access points may be located, they can be managed from the same interface. This innovation led to more widespread adoption of wireless networking on college campuses.

Selecting the Right Equipment

The first step when setting up a college's WLAN is deciding what equipment to use. You may not know how many access points or controllers you will need at this time, but you can determine that later when conducting the wireless site survey.

Installing or upgrading a wireless network is a major investment in your infrastructure and shouldn't be taken lightly. Proper planning, equipment selection and proper implementation will ultimately determine the success or failure of your WLAN.

When in doubt, ask other schools what equipment they are using and how satisfied they are. Taking a short trip to see a WLAN system in action may be the best way to help narrow down your choices.

When shopping for wireless equipment, there are a few key features that you will want to keep in mind. The first is radio frequencies. The 802.11n standard is not expected to be approved until November 2009. Keeping this in mind, you need to decide whether you want to purchase "pre-n" equipment that may or may not meet the standard when it is released.

Modal Ops

Most wireless equipment manufacturers offer 802.11 access points that function in several operational modes. Get to know what those are:

MIXED MODE: This lets 802.11n devices coexist and interoperate with legacy 802.11a/b/g devices on the same wireless LAN. Most enterprise WLAN equipment will use mixed mode by default to ensure legacy compatibility. This is because most organizations will concurrently use legacy and 802.11n devices for the foreseeable future.

LEGACY MODE: In this mode, the AP behaves like an 802.11a/b/g AP with improved performance because it uses some of the 802.11n physical layer enhancements. This configuration could be used when an institution buys new 802.11n APs but does not yet want to enable 802.11n operation.

802.11N MODE: Some manufacturers' access points can be configured to accept association requests only from other 802.11n devices. Some IT departments may choose this configuration to achieve the best possible throughput.

Source: Burton Group

802.11n Considerations

All IT managers want the performance improvements of up to 600 megabits-per-second throughput and the increased coverage that the new 802.11n wireless standard promises. But with the IEEE standard still not fully resolved, and prestandard products on the market, it's important to do your homework and consult with your network manufacturer before moving forward.

Here are five points to consider when you plan to implement or upgrade to 802.11n:

1. USE MODULAR ACCESS POINTS. While all indications are that any final changes to the draft 2.0 standard will be upgradeable with software, there's no guarantee that this will be the case for every change. This means you may need to replace your access points when the 802.11n standard is finally issued.

Before buying, ask the manufacturer what kind of replacement policy they have and how easy or hard it is to swap out the gear. You may want to look for modular products that let you more easily swap out the networking cards.

On the other hand, note that the current generation of 802.11n products don't yet support the full theoretical potential of 600Mbps speeds. You may find yourself upgrading hardware in a few years anyway if the higher speeds are important to your organization.

Many manufacturers are guaranteeing the equipment will be "flash upgradeable" to the ratified standard, but make sure you can get those updates for no additional fees. It will be hard to go back to the budget director six months after you purchase the WLAN and ask for money to upgrade it again.

If you decide to go with "n" equipment, you will certainly need a gigabit connection to each AP in order to provide the increased bandwidth that it will require. There is nothing wrong with purchasing wireless networking equipment that meets the current standards (802.11a/b/g) and upgrading some APs in a year or two when the standard has been ratified.

2. CHECK TO SEE IF YOUR WIRELESS ACCESS POINTS REQUIRE MORE THAN 15.4 WATTS. Most Power over Ethernet (PoE) switches support the 802.3af standard and can supply a theoretical maximum of 15.4 watts of power to PoE-capable devices. After loss from cabling and power supplies, however, the real power output may be closer to 12 to 13 watts.

Power requirements of 802.11n access points are all over the map: Some manufacturers require more than 15.4 watts, others claim to

work within the current standard. If you're using APs that claim to work with standard 802.3af power, be sure you understand exactly how much power the AP requires and how it behaves if it gets less than that.

For example, some 802.11n APs start scaling back functionality if they don't receive enough power. If your manufacturer's APs require more power than 802.3af can deliver, your options include prestandard 802.3at switches from manufacturers such as Cisco and ProCurve, or midspan PoE injectors from companies such as PowerDsine.

3. CONSIDER HOW AESTHETIC CONCERNS MAY AFFECT PERFORMANCE. Wireless gear used to be fairly simple, with a single antenna, or two at most. Today, some of the new products are downright cumbersome, with as many as six antennas.

This may sound trivial, but you don't want to put ugly gear on the walls or ceilings of a coveted historic building on campus. You may also have to hide APs in a drop ceiling, which could become an issue if it interferes with the wireless signal, putting a damper on performance.

4. UNDERSTAND POTENTIAL NETWORK DESIGN ISSUES.

There has been debate for the past few years about whether an 802.11x wireless network should be based on stand-alone "thick" or "thin" APs powered by a central controller.

The earliest wireless networks were primarily thick, meaning that most of the intelligence resided in each access point. As wireless networks expanded, the industry moved toward a thin model; the APs were essentially dumb radios, and all the intelligence resided in centralized controllers.

5. FOCUS ON SPECTRUM AND CHANNEL PLANNING.

The growing consensus is that the 5 gigahertz spectrum is best for enterprise wireless because it is a much cleaner space than 2.4GHz. 802.11n complicates the issue by allowing you to run in either the 2.4GHz or 5GHz space.

You'll need to decide which frequencies to use, and whether you want to support the legacy 802.11a/b/g protocols. Many of the 802.11n APs on the market feature dual radios, a good choice at least for the next few years because many of the notebooks you'll support will work only with those legacy standards.

If you haven't deployed 802.11a widely on campus, consider using one radio to run 802.11n in 5GHz and the other to run 802.11b/g in 2.4GHz. You could also add 802.11n to the mix in 2.4GHz, but keep in mind that it limits your ability to enable channel bonding,

Who's On the Network?

It's a good idea to occasionally audit the users that are accessing your wireless network. Fortunately, there are a number of easy ways to do this.

Some administrative consoles feature wireless-client shortcuts that will show you who is currently connected; others have a Dynamic Host Configuration Protocol clients table that displays the network names and media access control (MAC) addresses of connecting devices.

Enabling your wireless router's logging feature can also offer a wealth of information that can help you track your wireless network's activity.

a performance-enhancing feature in 802.11n that lets you "bond" two 20-megahertz channels into one 40MHz channel.

Because 2.4GHz allows for only three non-overlapping channels, you'll be able to run only one 40MHz bonded channel, which would severely limit your deployment options.

Central Control

The second key feature that you will want to look for is a wireless controller that allows for one central point of management of your WLAN. Try to imagine needing to change a setting on your APs and having to change 50 of them, one at a time.

A controller can offer huge time savings, but it may cause a performance bottleneck on the network. Different controllers require different network architectures and are worth investigating.

Wireless controllers from Trapeze Networks and Enterasys allow the APs to handle local switching and not route all traffic back to the controller (whereas some controllers route all traffic to the controller, potentially causing a bottleneck). One last point to consider is that when selecting your WLAN equipment, you will need to decide if you are going to provide outdoor access to make your entire campus wireless.

There's now some concern that with the increased throughput of 802.11n, the centralized controllers (and the uplinks to them) won't be able to handle all the traffic. Whether or not this is an issue on your campus will depend on your deployment size, the location of your controllers and the usage patterns on your network. While there's no right or wrong answer, it's an issue you should understand and monitor as you roll out 802.11n.

Conducting Your Site Survey

Now that you have selected your equipment, you are ready to start your site survey. The site survey could be the single most important phase of your deployment. The purpose of the site survey is to determine coverage areas and locate dead spots in the buildings on your campus.

Often a site survey will indicate areas where you may need to place additional access points, or areas where you can forego an access point or two. If you already have an existing WLAN, you may be able to improve your network by using some wireless analysis tools and examining your coverage area.

It's important to find site survey tools that can handle 802.11n. The 802.11n standard offers much greater coverage than the existing 802.11g and 802.11a standards. Because it achieves this through new technologies such as multiple input/multiple output (MIMO) and channel bonding, it's important that your site survey tool understands 802.11n to get an accurate survey.

Active survey products such as AirMagnet have been updated to communicate with 802.11n networks. Many wireless manufacturers are in the process of upgrading their predictive survey tools to understand 802.11n, but you need to be sure — so ask.

One workaround if you are using an older survey tool is to do a site survey for 802.11a, which will give you the access point density you need for 802.11n. This makes good sense, especially if you want to support legacy protocols. However, if you're doing a greenfield installation and plan to support only 802.11n, you'll be best served by a newer site survey tool.

There are other options for analyzing a wireless network, both free and purchased. NetStumbler is an open-source product that many network administrators use when tracking down wireless issues. NetStumbler will allow you to see the different access points, the channels they are operating on and the signal strength that is being observed.

Fluke Networks has an entire line of products designed to help you troubleshoot or design your wireless infrastructure. The InterpretAir software from Fluke Networks is site survey software that you can use to map your network, as well as determine coverage areas based on the WLAN equipment you are using.

Trapeze Networks has a site survey tool that can tell you exactly where to place your APs after you run through a wizard that asks you about your building construction and user locations.

If you opt to go the professional route for your site survey, be sure to get references from other sites that have been surveyed, and see how those networks are performing. There is a possibility that you could cut the costs for your network by having a professional site survey conducted.

Bandwidth Capacity Planning

When setting up your school's WLAN, keep in mind the number of users who may be accessing that AP at any one time. Early to midmorning may be the busiest time of day for the network at many colleges as students are getting online to submit homework, check e-mail and catch up with their friends.

Many WLAN access points claim to support a theoretical maximum of 256 clients, but real-world performance is about 10 percent, or 25 clients. Networks that experience slow performance are most likely suffering from not enough APs though offering plenty of coverage area.

Having a higher concentration of APs is important. In the event of a failure, other APs may pick up the slack and increase their broadcast levels to accommodate for the outage. A higher concentration of APs will allow the network administrator to restart an AP in the event of a malfunctioning unit.

Fast and Faster

Standards bodies and equipment manufacturers are hammering out 40-gigabit-per-second and 100Gbps Ethernet for server interconnects and backbones.

Alan Weckel, director of Ethernet-switch market research for the Dell'Oro Group, says component manufacturers are hard at work developing 40Gbps. He predicts the technology will begin ramping up in 2011. As for 100Gbps, don't count on seeing it until 2012 or 2013.

"Those will be really popular in research environments where there's a lot of link aggregation and core oversubscription," Weckel says. "When these uplinks begin shipping, it will help the performance of the network and help them collapse the network."

Beefing Up the Backbone

While they've been deployed in research labs in engineering, science and medical departments for many years, 10 gigabit-per-second Ethernet switches are now proliferating in campus data centers. Colleges are upgrading their backbone in order to carry their increasingly bandwidth-heavy operations applications, not to mention increased wireless traffic.

Colleges can expect many gains from adopting 10Gbps including an elimination of bottlenecks and stronger built-in redundancy. Faster bandwidth speeds also let universities more easily comply with security policies calling for traffic filtering without losing any packets or experiencing latency.

Upgrading the network's bandwidth can open up all sorts of new opportunities for schools. Whether it's an increased use of video conferencing for administrative functions or greater utilization of streaming video in the classroom, colleges are discovering all sorts of applications on campus that can take advantage of 10Gbps capacity and increase teaching and learning opportunities.

Get In Line for Online

Still not sure about whether investing in a more robust wireless network will pay off? Greater demands on your wireless network may be coming sooner than you think.

Gartner research director Marti Harris says that many universities are now considering asking students to take at least one course completely online per semester. Ten years ago, such a request would have sparked protests from the faculty, but Harris says faculty members have several reasons to go along today:

- In some situations, not offering online courses harms the college's reputation with potential students.
- A growing percentage of faculty members are less suspicious of teaching with technology, appreciate its value and are already interacting with their students in an online collaborative mode.
- Technology can make teaching easier for professors. For example, online learning could make it possible to avoid teaching classes on late Friday afternoons when energy, attention and attendance are low among students.

Content Filtering

As more wireless devices and notebooks come online on college campuses, IT departments are finding that they need to rethink their network management processes. One area in particular, Internet content filtering, will have to be revisited with the increased use of wireless access. Here are five strategies to help.

1. DON'T USE MANUAL PROXY SETTINGS. If your students have to manually enable an Internet proxy when they come on campus and turn it off when they leave, then you are bound to see more help desk calls as a result. Consider a filtering solution that uses pass-by technology or a gateway filtering system, or automate the proxy settings for them.

If you need to set manual proxies, then push out Web Proxy AutoDiscovery settings via Dynamic Host Configuration Protocol.

Keep in mind that not all browsers support WPAD settings and that students could run another browser from a USB thumb drive or from a download.

2. TO FILTER OFF CAMPUS, OR NOT TO FILTER OFF CAMPUS? This may be one of the hardest issues on which to achieve consensus. Should you filter the Internet content on computers when students take them off campus?

If you are going to filter students' activity while off campus, is your administration prepared to take disciplinary action based on inappropriate web surfing as it would if the same surfing was done on campus?

Not many filtering systems offer content filtering for mobile users. 8e6 Technologies uses agent technology that validates each and every request before allowing access. Such systems may impact your Internet bandwidth, depending on the architecture of the system you are considering.

Open-source fans can configure a proxy server with Squid and open it up to the Internet so that students can access it from home. But beware: You will want to consider setting up authentication so you aren't running a proxy for hackers on the Internet.

3. FIND A FILTER THAT CAN STOP MALWARE. When students have 24x7 access to a computer, you are bound to see more malware than on computers that stay on campus. As most technology personnel will tell you, students will click on absolutely anything.

Peer-to-peer file sharing programs often can be grouped with malware because of the disruption they can cause on educational networks. Most content filters should be able to prevent this while notebooks are being filtered. Any worthwhile Internet filter will help you identify and stop those mobile devices infected with malware.

4. WHAT USER AUTHENTICATION AND REPORTING DO YOU NEED? Nearly all Internet content filtering systems provide some degree of reporting. For it to be effective, you need to correlate user names to web activity.

Some systems require that a program be launched upon network login (often via script); others require that a pop-up window remain open; and still others check against your logon servers and correlate user names to IP addresses.

There are pros and cons to each authentication mechanism, and you will need to compare them to see which one will work best in your

environment. For example, if authentication depends on a program that runs upon login, then students who restart their notebooks at home will not have the program running when they get to class.

The simple solution is to have the students reboot the computer once they get to school, which is also a great time for other scripts or utilities to run. Whichever system your filter uses, make sure that you test it in your environment during your evaluation period.

5. DO YOU HAVE THE CACHE? Some Internet filtering systems will let you cache content that is frequently downloaded. If you have a professor who asks all students to visit the same website, then each student's computer has to reach out to the Internet and download the content.

If you are using a caching engine, only one computer goes to the Internet while the rest pull content from the caching engine. Some schools have seen 30 percent to 40 percent of their Internet activity come from cache. For schools that have a slower Internet connection, a cache engine is critical.

Encryption and Authentication

There are currently two main types of encryption used on WLANs: Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP encryption is substantially weaker than WPA, but depending on what kind of data you are trying to protect, it still may be a good fit.

If you are using WEP to encrypt student data, you may be fine. However, staff members who may be accessing your student information system (SIS) or online gradebook application may benefit from the added strength of WPA encryption.

WPA encryption is much stronger and can be managed with randomly changing keys via the 802.11x standard. Each time a notebook changes APs, it has to reauthenticate against the system, which in the case of 802.11x has to hit your RADIUS or authentication servers and may cause logon delays.

If you determine that you are going to go with 802.11x, you may need to add additional logon servers and/or RADIUS servers to handle the authentication and keep the rest of your network performing adequately. This is because of the nature of a college campus: Students are constantly moving from class to class during the day, causing them to have to reauthenticate several times a day.

Navigating Network Downtime

There are so many new devices and technologies on college campuses these days that some IT managers readily admit that their networks may go down at times and that the school just has to live with it.

Case in point: During the NCAA Final Four tournament of 2008, the IP network at the University of North Carolina at Chapel Hill went down when students opted to watch the UNC game on ESPN Online rather than on cable TV.

Larry Conrad, vice chancellor and CIO at UNC, says, "We thought about the downtime long and hard, but came to the conclusion that the interruption was an isolated incident," and that it wasn't necessary for the university to upgrade its network at the time.

Failover and Redundancy

One of your last but most crucial steps to setting up a wireless network is determining how much redundancy or failover you will need. Consider purchasing multiple wireless controllers so that if one of them has a problem or needs to be rebooted during the school day then interruptions are kept to a minimum.

Check to see whether the APs can have a "master" and a "slave" controller so they will automatically switch over to the controller that is online. As mentioned earlier, having a strong concentration of APs will allow for them to be rebooted if necessary while still providing service to your users.

Wireless Networking Best Practices

To ensure the success of campus users once the WLAN is set up, IT departments should focus on providing users with three things: a consistent end-user experience, good help desk support and strong security measures. All three are critical to making sure mobile users are as productive and protective of sensitive information off campus as they are on campus.

A Consistent User Experience

Universities should plan to provide users with access to the same network applications and data, regardless of whether they are on campus or off. One way to help create a consistent user experience is to assign mobile users a notebook that they can use all the time, regardless of their location.

One of the benefits of a one-to-one computer program that offers organization-issued notebooks is that the IT department can install uniform security safeguards, such as antivirus software, on every computer. This will go a long way toward firming up the campus's network security.

Institutions should carefully consider the network bandwidth and IT infrastructure ramifications before rolling out a one-to-one mobility initiative. To provide users with fast access to the same applications and data when off campus may require the organization to rearchitect, upgrade or invest in new infrastructure.

Good Help Desk Support

Help desk support is an important piece of the mobility puzzle. The productivity gains of a mobility initiative can easily evaporate if the devices are not functioning properly. Offering extended help desk hours will allow mobile users to quickly address any problems that come up with their mobile devices.

The use of a standard software image and standardized configurations for mobile devices will also help simplify troubleshooting. Standardization allows the help desk staff to quickly diagnose and resolve any problem that comes up.

Strong Security Measures

Security is an essential issue with any mobility rollout. Multiple layers of security, including antivirus software, virtual private networks, encrypted hard drives on notebook computers and password-protected handheld devices are all important for bolstering mobile worker security. In addition, institutions should consider requiring two-factor authentication before users can log onto the network.

One often overlooked aspect of mobile security is properly training users on the risks and what they can do to counter attacks on their mobile devices. The security of the network can be greatly improved when mobile users have an awareness of the dangers and what they can do to protect themselves and the university itself from threats to their mobile devices.

Banding Together

Iowa State University is continuously upgrading its network infrastructure to stay ahead of growing demand. One way that the university is able to stay on top of bandwidth demand is its participation in a consortium of four schools (along with the University of Iowa, the University of Minnesota and the University of Wisconsin-Madison) that pooled resources to build a regional voice, data and video fiber-optic network.

“We built a ring around the Midwest, including dedicated research circuits,” says Jim Davis, CIO of ISU. “It’s not endless, but it serves us well.”