Toolkit: Checklist: Choosing Wireless Broadband Technologies for the Enterprise Campus

Robin Simpson

Wi-Fi mesh solutions are mature enough for enterprises, but other technology choices, such as 3G and WiMAX, may be suitable. Our decision framework includes factors to consider such as campus geography, application, work style and bandwidth requirements.
WHAT YOU NEED TO KNOW

Colleges and universities pioneered large-scale deployment of Wi-Fi mesh networks to provide Internet and intranet access for their students and staff across campus. They showed that Wi-Fi mesh is a practical and inexpensive way of providing ubiquitous wireless coverage of large outdoor areas, but that it must be supplemented with conventional wireless LAN (WLAN) for indoor areas or anywhere large numbers of users congregate.

Voice over WLAN will remain problematic until 802.11 standards for roaming and quality of service are ratified. Organizations with high mobile phone penetration (whether or not the phones are paid for by the enterprise) should consider working with mobile operators to improve outdoor and indoor 3G cellular coverage for voice and data.

Mobile WiMAX today is immature, but, by 2008, it will complement Wi-Fi and Wi-Fi mesh as a backhaul technology. By 2009, it will be a viable alternative to Wi-Fi as an access technology if the consumer premises equipment (CPE) cost approaches zero in laptops.

These technologies can also be applied to any large business area — a head office, a sprawling campus, a factory, a shopping mall or an airport.

ANALYSIS

The Way People Work Is Changing

Today's new employees have a completely different set of expectations from those of the past. Most have grown up owning a cellular phone since they were 11 or 12 years old; they have long experience of communicating and collaborating with their friends via e-mail, instant messaging, Skype — even the virtual worlds of online gaming. Thus, the tools and processes that they would prefer to use at work or study are different from those the previous generation expected when it entered the workforce.

In parallel with this "youth demographic" change, there is change in the way our current workforce wants to work. Working from home for an hour or two each night — or for two or three days a week — is becoming an important lifestyle choice. Working while traveling (both locally and internationally) is an increasing requirement. Collaborating with others — who may not be in the same room, the same campus, the same time zone or even the same country — is a growing work requirement.

Employees want and need access to their online tools, anytime, anywhere. Providing wireless broadband mobility in all the places that they work and play (including across the enterprise campus) helps to meet these objectives.

A Campus Wireless Network Technology Checklist

1. Evaluate End-User Application and Mobility Needs

The most important driver for deployment of an enterprise campuswide wireless network is the business need for mobility. Therefore, any campus wireless strategy must begin with a thorough analysis of the mobility needs of the intended end users. This involves segmenting the mobile workforce by its work style category, usage patterns, work locations and degree of mobility, and application and device requirements. The resulting mobility matrix can usually be simplified down to four or five different user profiles, each with its own set of application, device and connectivity needs. These profiles — and the number of employees that fall into each category — then
become an extremely useful tool in defining the coverage, capacity and functionality of the campus network — and even the budget priorities.

2. Understand the Application Bandwidth and Latency Requirements

The most-popular mobile applications used in enterprises today are e-mail, instant messaging, Web browsing and access to administrative systems, such as training, scheduling and appointment systems, directories, and expense management. None of these applications is very demanding on network traffic, and a well-designed wireless network can provide adequate shared bandwidth.

However, a new class of more-demanding enterprise applications will emerge during the next five years. They include:

- Voice over IP (VoIP) over wireless
- Audio and video streaming (live and on-demand)
- Videoconferencing and remote collaboration
- Video monitoring for security
- Telematics and remote control of plant and equipment
- Backhaul for radio frequency identification readers for asset tracking, maintenance and management

Each of these applications has different requirements for campus coverage, bandwidth, latency and quality of service, and these requirements must be planned for. Latency is often as important as bandwidth — for example, for VoIP and media streaming.

3. Determine Who Owns the Devices and Who Pays for the Services

The cellular phone is pervasive in our business and personal lives today. It is, by definition, mobile, always with us and often much more usable than a desk phone. Cellular operators may already be providing good voice (and sometimes data) coverage of the campus without the enterprise having to build any infrastructure.

Enterprises that own or control large campuses should understand that real estate for antennas and base stations and for right of way for backhaul (for example, access to trenches and cable conduits) is a precious commodity to operators trying to build out coverage — especially if they can serve a wider community from these cell sites — and so they may be in a good position to negotiate improved campus coverage with the operator in return for access to cell sites.

The lesson for enterprises is that, for a large campus and where many users already own a mobile phone, building a converged network that supports voice as well as data may not be the best option — especially if a significant proportion of mobile-originated calls are to recipients outside the campus network. By understanding usage profiles, cell phone ownership and calling patterns, it may be possible to negotiate an enterprise-wide calling plan with a mobile operator that greatly reduces the cost of on-campus calls, without building infrastructure.

However, if the enterprise is moving strongly toward IP telephony and plans to issue company-owned VoIP-capable terminals for business purposes, then a converged campuswide mobile voice and data network may make financial sense. If the enterprise supports dual-mode unlicensed mobile access (UMA) handsets, then end users can still retain all the functionality and convenience of a cell phone for calls when traveling outside the campus area. However, it should
be remembered that the main purpose of converged voice and data services is to enhance mobility and productivity, not reduce costs.

4. Manage Campus Spectrum to Take Control of Your Airspace

A key element of any campus wireless plan is how the basic radio resource or frequency spectrum ("airspace") will be used. If the enterprise is not able to control, allocate and protect this resource — inside buildings and, especially, outside them — it will be impossible to deliver applications to end users at the desired levels of service and quality.

WLANs commonly operate in two separate spectrum "regions" or frequency bands that are approved for wireless use by governments worldwide — the industrial, scientific and medical (ISM) bands at 2.4GHz and 5.8GHz. These bands are open to virtually any type of wireless device, including cordless telephones, provided that the devices used comply with the power levels and approval requirements established by the regulatory authorities. Because no spectrum license is required, anyone can set up and operate a WLAN with approved equipment. With only three available channels in the 2.4GHz band, the potential for interference from adjacent networks operated by different users is high, and, because both are following the ISM rules, neither has a case to take action to mitigate the resulting interference. This is a difficult issue to manage in a multitenant high-rise office building, but in a campus environment, the enterprise should take charge of the ISM spectrum and manage channel allocation.

Spectrum management for cellular, WiMAX and proprietary wireless broadband networks is more straightforward, because they typically operate in a spectrum that requires a license, and the license is normally granted for a specific geographic area. However, spectrum can be expensive.

5. Choose the Right Wireless Architecture

Fixed WLAN networks consist of access points — typically placed in the ceiling — and controllers that offload some of the work from these access points to a central device. This approach, like any centralized computer architecture, can help to improve manageability and reduce costs. The wireless products themselves fall into three broad categories — second, third and fourth generation — with the fundamental difference between the categories being how devices access the network. Few mainstream vendors have yet made significant investments in fourth-generation products, partly because of anticipated standards improvements that will enhance the performance of third-generation (3G) systems, and 3G systems are typically adequate for current enterprise needs.

Mesh networks involve the use of wireless for their backhaul and service links. Wireless backhaul — which is typically Wi-Fi — is especially important for organizations that wish to deliver service outdoors, because it is often impossible or too expensive to run data cabling outdoors to connect the access points to the wired network. The term "mesh network" is used because the backhaul does not need to follow a single path. If one path is overloaded or its wire connection is not working, a mesh network's software can find alternative paths. We will increasingly see meshing as an integral part of all vendor offerings.

Most campus wireless networks will likely be a mixture of fixed and mesh architectures.

6. Consider Campus Geography and Building Layout

Given the broad range of application, bandwidth and mobility needs across a typical campus, no single fixed or wireless infrastructure will fulfill all needs, and a hybrid solution will make the most sense.
University and college experience has shown that Wi-Fi mesh is most suitable for broad outdoor areas, for car parks and to penetrate from both sides of long narrow buildings. If this is not possible, these areas may be covered by operator-provided 3G cellular voice and data services. Ultimately, mobile WiMAX networks will be a practical solution once zero-cost WiMAX chips are included by laptop manufacturers, but this is not likely to happen before 2009. WiMAX may also be suitable for the backhaul for fixed WLAN and Wi-Fi mesh access points, and we expect that hybrid mesh access points that use Wi-Fi for the access layer and WiMAX for backhaul will emerge by mid-2007.

Fixed 3G Wi-Fi will be most suitable for indoor areas requiring mobility or portability and, especially, for higher capacity where large numbers of users gather — for example, cafeterias, meeting rooms, boardrooms, large meeting halls, sports facilities, visitor areas, and reception and waiting areas.

Operator-provided 2G and 3G networks may be suitable for voice services in all public areas, supplemented by indoor microcells, picocells or enterprise-owned distributed antenna systems, unless handsets are to be used only on campus, when Wi-Fi handsets or dual-mode UMA handsets can reduce costs by offloading all campus-originated cellular calls from the operator networks to the enterprise network.

 Femtocells are an emerging technology to boost indoor 2G or 3G reception using existing carrier-owned spectrum, but connected to the operator's core network via the customer's own broadband Internet service (for example, DSL or cable). Unlike the expensive UMA handsets, femtocells can connect any standard 2G or 3G handset to the operator's network, but they typically only service a few users with a range of about 200 m. Again, campus owners may be able to make a deal with an operator to boost indoor and outdoor coverage to make 3G data more viable and ubiquitous across campus.

7. Use Site Surveys and Wireless Network Planning Tools

Perhaps the most important lesson learned by the institutions pioneering campus wireless mesh networks is the importance of conducting comprehensive site surveys. Because such surveys are expensive and time-consuming, some organizations skimp on this step. However, experience has shown that they are essential if the desired coverage, performance and quality of service are to be realized. For example, modern building materials, such as steel framing used in plasterboard walls and office partitions, aluminum and galvanized steel roofing materials, and even decorative steel structures, can have a big impact on coverage and optimal antenna siting.

Many vendors can provide site surveys as part of a contract bid, but if in-house skills exist, several tools are available to help deliver optimal infrastructure performance. These site survey tools permit building diagrams to be input along with the expected densities of users and materials found in the environment. They will recommend placement of access points for optimal performance. For example, Wireless Valley from Motorola makes it possible to use computer-aided design diagrams of buildings and other locations — which may include building materials and other characteristics, as well as user profiles for different areas — in planning the wireless deployment. This enables planners to establish where access points should go, and to create "heat maps" that show the bandwidth in different areas and where it can leak out. This is useful not only in the initial planning stages, but also when changes are made later.

Once the initial network is in place, management tools and sensors are available to monitor the traffic on a wireless network to identify anomalies and spot potential user problems. For example, if too many users are congregating in one area, some of those users can automatically be moved to another access point. Management tools should also make it possible to upgrade firmware on all products, keep them up-to-date, and overcome outages caused by failed access points.
RECOMMENDED READING

"Toolkit: Tutorial: Comparing Wireless Broadband Technologies for the Enterprise Campus"
"Campus Wireless Mesh Network Offers Challenges, Opportunities"
"Mobility, Not Cost Savings, Is the Driving Force for 'Cutting the Cord'"
"Pick the Right WLAN Architecture for Your Organization"
"Planning Tips for WLANs in Higher Education"
"Whirlpool's Network Transformation Delivers Business Value"

Acronym Key and Glossary Terms

3G The third-generation cellular wireless networks, which support increased voice capacity and peak data speeds up to 2 Mbps in fixed locations and up to 384 Kbps at pedestrian speeds.

UMA Unlicensed Mobile Access — an industry standard designed to support seamless connectivity between cellular networks and unlicensed spectrum networks, such as Wi-Fi or Bluetooth. Requires two wireless transceivers in the handset (a "dual-mode" handset).

Wi-Fi Wireless Fidelity — certification by the Wi-Fi Alliance of 802.11a, b or g standards compliance and interoperability.

WiMAX Worldwide Interoperability for Microwave Access — broadband wireless technology based on the IEEE 802.16 standards.

Wireless Mesh A mesh topology network based on Wi-Fi standards but typically linked together by proprietary extensions today. The Wi-Fi Alliance Task Group 802.11s is developing a proposal for consideration as an IEEE standard.

WLAN Wireless LAN — a network that connects devices or LAN segments using radio (the unlicensed 2.4GHz and 5GHz bands), instead of physical cables.
REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9º andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509