

tions are available virtually across the entire campus. In addition, 2,500 employees work with university-supplied cell phones, 20,000 individuals take advantage of special university discount programs, and just about all students use cell phones as their primary means of communications. So it is not a surprise that the university has been eyeing FMC developments.

“FMC has the potential to make communications between our network and WiFi hotspots seamless,” noted David Morton, director of mobile communication strategies at the University of Washington. However, the university has not moved to this area because it has not been able to build a sound business case.

A number of factors are at play in the university’s cost-benefit analysis. The cellular carriers have been aggressively cutting service pricing. In some cases, users can make an unlimited number of calls for about \$50 per month.

“Without the add-on charges, the price differential between using cellular or WiFi connections is not as great as the vendors have portrayed,” said Morton. In addition, the new system can create unforeseen costs. Because traffic constantly increases on academic WiFi networks, upgrades may be needed. To accommodate more traffic, institutions may have to increase their number of WiFi access points by as much as 25 percent.

Creating New Management Challenges

Management can also present new challenges. Users now move between two different networks, and network technicians may not be able to troubleshoot problems down to the phone.

Security has been an ongoing concern with WiFi connections, which offer various techniques to ensure that only authorized individuals gain network access. However,

many smartphones were not designed to support security check, such as IPsec. Consequently, individuals’ personal identifiers (password, user ID) can be transmitted in the open air. Recently, phones, such as Apple’s iPhone, have been outfitted with IPSec. However, even that feature may not be enough, since cellular-to-WiFi hand-offs open up new security holes. Vendors have been tweaking their products so security functions pass from the cellular to the WiFi network, but their approaches may not be 100 percent effective.

Lost functionality is another deterrent. Customers may not have as much functionality with FMC applications as they would with a PBX. The telecommunications industry has spent decades developing the features found with their systems, while VoIP systems are still in a relatively nascent stage of development. For instance, FMC systems often do not allow five-digit dialing.

Voice over WiFi (VoWiFi) networks introduce another level of complexity. (Note: VoWiFi is actually VoIP over a switched Ethernet WLAN.) Quality of service (QoS) is very important to voice calls, and packet networks just aren’t engineered with the right stuff...at least not right out of the box. Sufficient bandwidth has to be reserved for the anticipated level of voice traffic and committed to each call for the entire duration (off-hook to on-hook) in order to ensure that latency, jitter, and loss are within limits. Supporting stationary users is relatively straightforward, but that’s not the real world. Mobile users walking around a building or campus present a considerable challenge, as the network has to deal with call hand-off issues between WiFi access points (APs), just as a cellular network has to deal with hand-offs between base stations. That translates to additional investment in infrastructure in the form of either VoWiFi-capable fat APs or central-

ized VoWiFi switches and controllers. Once designed and configured properly, the network also must be monitored and managed properly to ensure QoS levels over time. That means investment in management tools, including probes and network management and optimization software, and the skill sets necessary to make proper use of them.

Closing Up Their Systems

Functionality can also vary by device. In order for FMC equipment vendors to enable phones to toggle between networks, they must map functions to a device’s application program interfaces (APIs). In some cases, the handset suppliers have been reluctant to expose their APIs for fear of losing their competitive advantage. Standards would help address such limitations, but to date, cell phone vendors have been trying to differentiate their product designs rather than coalesce around different feature sets.

In sum, FMC has the potential to ease wireless communications management functions at academic institutions, but the underlying infrastructure is immature. Consequently, colleges are taking a look at the technology, but few are implementing it. Some of the shortcomings should be addressed as the market matures. For instance, product pricing should drop as more units are sold, and stronger security features are expected to be put in place. These changes may pique universities’ interest. “FMC should help academic institutions simplify their networks, so it just makes sense that sooner or later they will move to it,” concluded Farpoint Group’s Mathias.

Paul Korzeniowski is a freelance writer who specializes in communications issues and is based in Sudbury, Massachusetts. He can be reached at paulkorzen@aol.com.

Solar Chargers: A Bright (Green) Idea

For students or faculty on-the-go, keeping electronic devices like cell phones, PDAs, iPods, and even laptops charged can be a challenge. “There are many budget-friendly portable charging devices on the market that harness the power of the sun—a free

and totally clean energy source,” notes Paul Holstein of CableOrganizer.com.

One example is the JuiceBar Solar Charger. It’s equipped with solar cells that begin to charge immediately upon contact with light. It includes 12 of the most com-

monly used adapters for cell phones, iPods, MP3 players, portable gaming systems, and more, and it sells for less than \$50.

More info: <http://cableorganizer.com/pocket-solar-charger>. Solar power is a hot idea!