



**Wireless WAN/LAN solutions
for schools using
WiMax, WiFi and
*Secured Access and Content***

Halestar, Inc.
Hartford Connecticut
Virginia Beach, Virginia

Prepared by:

Kevin Dowd, October 2008

Copyright © 2008, Halestar, Inc.

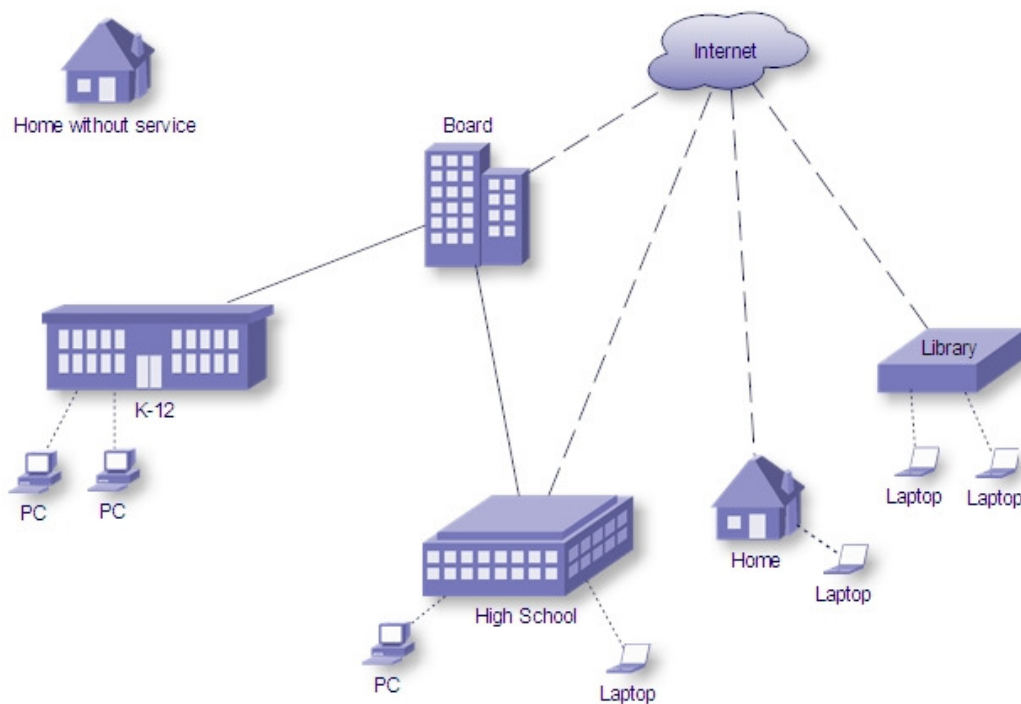
Introduction

Wireless wide area network (WAN) and local area network (LAN) technologies provide revolutionary savings and flexibility for regionally distributed organizations, like schools. Network access can be provisioned to a whole school building in just a few hours. An integrated private network, spanning a city or county, can be erected in a week. The cost savings justify the effort within a few months. And, if desired, the school network can be extended wirelessly to the student at home.

This paper discusses the technologies and components that will revolutionize a school district's touch to its schools, faculty and students.

Changes in the Wired Model

The network model for most school systems and distributed businesses is a combination of wide area networking, site distribution and switched LANs. There may be WiFi in use as well.





The diagram above depicts this model. Leased lines form the school WAN. Each school has some local servers and some district-based servers. There may be multiple internet connections. In most cases, student access to school resources is limited to the time the student spends in school.

Periodically, portions of the network require a refresh in order to keep up with bandwidth and management demands.

Among the reasons:

- Migration from older copper technologies to gigabit or fiber, both for end-user access and distribution.
- Network segmentation for security.
- Authentication and client security, particularly campus management and network access control (NAC).
- Addition of VoIP telephony.
- Addition of security, including cameras
- Addition of wireless LANs.

The costs of a network refresh can be significant. Wireless is becoming attractive from technological and cost perspectives. A wired port density of $\frac{1}{4}$ that of a few years ago is sufficient to support fixed devices, such as printers and servers. The rest can be wireless. User experience for mobile devices is as good as or better than for yesterday's fixed wire network.

Wireless LAN, WAN and Wireless Distribution

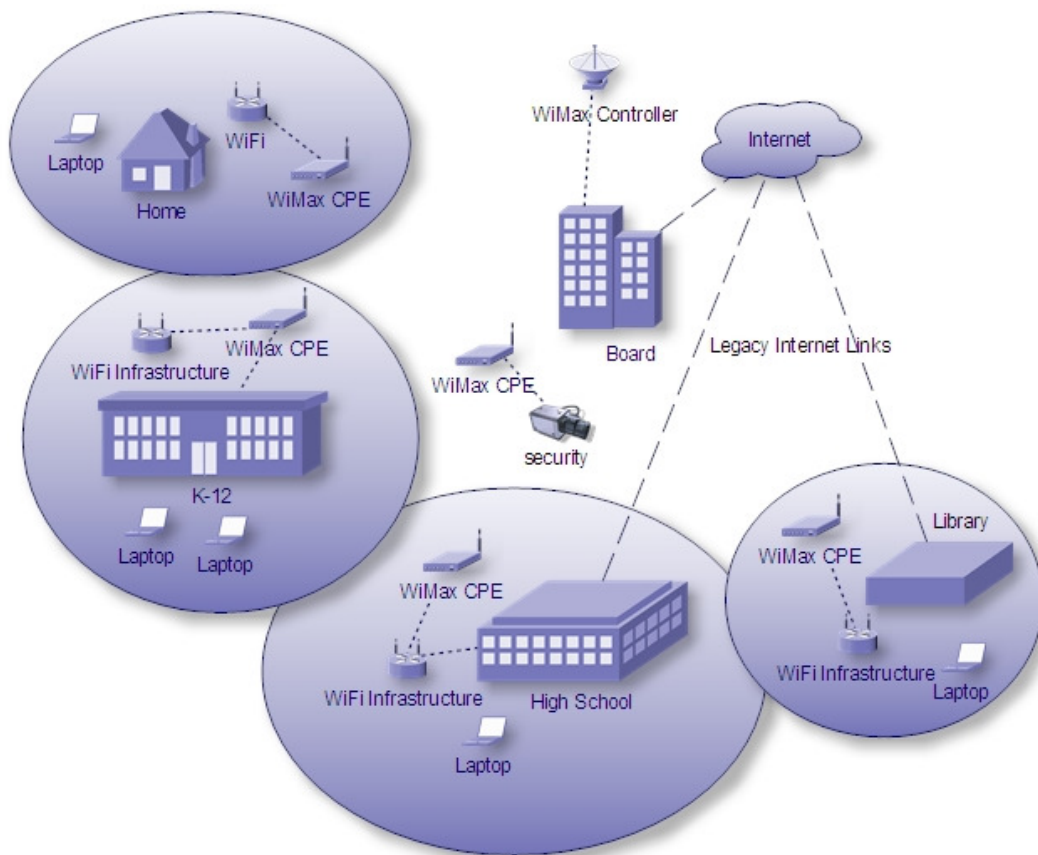
You have likely heard of WiMax.

WiMax is a wireless *broadband* or *wide area network* technology. Its purpose is to provide an alternative to wired WAN technologies, such as DSL, cable or leased lines. Any organization may erect its own WiMax network across a town or county. The radio spectrum is lightly licensed, and free of distribution charges; a school system creating a WiMax-based wide area network does not have to pay a carrier. Furthermore, WiMax can be deployed quickly and without a great deal of prior planning; any new building, trailer, library or neighborhood can be added to the network in about an hour, simply by provisioning a WiMax transceiver.

WiFi, on the other hand, is a wireless *local area network* technology, providing distribution and service to end-user devices in a smaller footprint, such as a campus or a school building. A WiFi *infrastructure* may accommodate many access points all at once—possibly hundreds. WiFi can be further used for network backhaul and local network extension via bridge or mesh technology

For end-user access, wireless can be a reliable and convenient alternative to traditional wired networks. The cost and flexibility are attractive. Wireless networks can provide hundreds of Mbit/s service. And wireless networks are arguably more secure than wired.

Deployments of WiMax, WiFi and WiFi-based bridging and backhaul provide attractive alternatives to wired infrastructure—particularly when considered in lieu of a wired LAN refresh or WAN deployment. Wired networks (and fiber networks) have their place in network infrastructure, particularly where speed and contention-free access is paramount. But wireless alternatives for WAN and LAN delivery should be considered.





The diagram above depicts a school district serviced by a combination of terrestrial WAN links for Internet service and WiMax for district service. Naturally, a hybrid of wired and wireless WAN is possible. However, the important element in this diagram is the notion of ad-hoc links; anyplace that one wishes to place a WiMax customer premises transceiver, one can extend the school network. Used in combination with a WiFi infrastructure, WiMax distribution with WiFi local delivery can provide on-the-spot service with identical security and access as is available within the schools. This can be extended cheaply to libraries, neighborhoods and temporary structures.

WiFi Infrastructure

Modern wireless infrastructures are overlays to an existing wired network. Access points are deployed to cover the air space at the edges of the network, but managed centrally at controllers. Wireless management, security access, firmware updates, service and radio tuning are managed by the controllers for all of the access points, all at once. Once an access point is installed, there is likely no need to revisit it.

Centralized management of all access points (APs) means that the infrastructure can tune radios to fill dead spots, or avoid interference. The APs can “hear” one another, and can coordinate in triangulation for security, or for simply locating a missing wireless device.

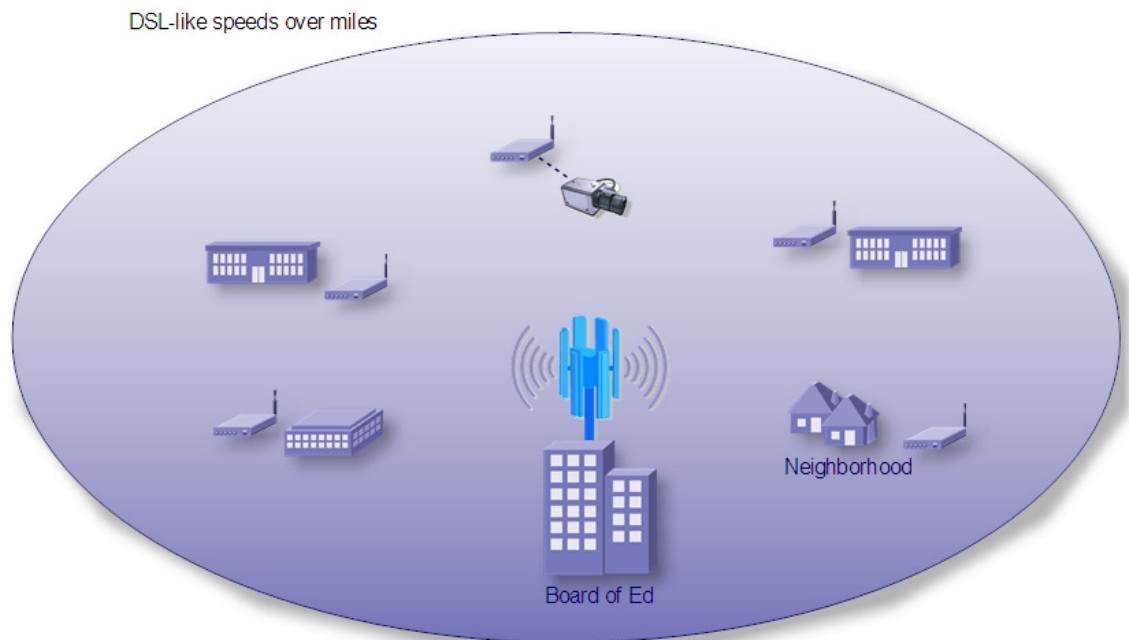
Wireless networks are more secure than wired networks. This is because traffic need never pass in the clear, and a wireless connection cannot be established without the proper credentials. A single wireless system typically supports a full range of encryption, security and authentication capabilities, including captive logon pages for guests, and network-authenticated access for known users.

Current WiFi technologies provide for raw bit rates of up to 540 Mbit/S. The costs range from a few hundred dollars for a lone access point to tens of thousands for a complete wireless infrastructure with many access points.

WiMax

The term 'WiMax' is applied to two basic forms of wireless broadband service, loosely termed as *fixed (802.16d 2004)* and *mobile (802.16e 2005)* WiMax. The WiMax standards define modulation methods and network management technology. These standards can be deployed on different portions of the RF spectrum. Some WiMax networks are in licensed spectra, secured by telecoms at auction. Others are in 'lightly' licensed spectra, which can be accessed by schools or service providers for a couple hundred dollar fee. Still other parts of the RF spectrum are set aside for schools, or provisioned for unlicensed use.

Reliable and cost effective WiMax infrastructure components are available from a number of vendors. A deployment consists of one or more base station controllers and customer premises equipment (CPE).



The cost of a controller and antennas is in the range of ten to fifteen thousand dollars. The cost of CPE is in the range of \$500, and dropping quickly. CPE can be combined with WiFi to provide complete wireless delivery.

WiMax links are encrypted. They can be regarded as old-style WAN links, with added features for Quality of Service and



abstractions that can make a link appear circuit-switched, like a phone line. Speeds are DSL-like over distances of miles.

Combined WiMax/WiFi infrastructure

WiMax can provide long distance distribution. WiFi can provide local delivery. Between the two technologies, a school system can quickly deploy service that is captive and unique to the student or faculty experience, wherever students or faculty may be—the same wireless SSIDs, the same directory logins, the same URL filtering, content security and user controls. Telephony can be extended too, so that a user's telephone number rings 'locally,' anywhere the network reaches.

Naturally, WiMax can be fed into local area wired service as well.

WiFi, by virtue of the fact that 'ports' are virtual, allows for network access control for an arbitrary number of ports at arbitrary distances, when extended across the WAN. Combined with authenticated wireless access, portal products or a campus manager, WiFi can be configured to authenticate, secure and restrict connections based on *who, where, when, and what hardware*. PC health can be factored into the access grant.

Content security for prevention of viruses, malware, proxied internet connectivity and spam can be provided at the head end of the mobile WiFi/WiMax deployment. This means that access can be 'sanitized' for students with school-owned laptops, reducing the district's exposure to unsanctioned use.

Halestar's Solutions

Halestar provides secure wired and wireless access for businesses, government and schools across the country. Halestar's data security customers include the state of Connecticut, many universities and private schools and some very large school districts in Virginia. Halestar has deployed many tens of wireless networks for universities, private and public schools.

Halestar carries all of the technologies discussed in this paper.



This discussion about Wireless WAN and LAN technology is from Halestar, Inc. See www.halestar.com.