Designing and Building a Campus Wireless Network

For the K-12 Community of North Carolina

Version 2

8/2012

Designing and Building a Campus Wireless Network

For the K-12 Community of North Carolina

Overview

This document is intended to provide technical guidance to LEAs within North Carolina for Wireless LAN (WLAN) deployments. The LEAs within the state each have unique characteristics such as student population, number of schools, budget constraints, IT staff, etc. Furthermore, individual schools within an LEA may have very different needs for wireless connectivity. For example, a school that implements a 1:1 computing initiative will have very different connectivity requirements than a school that simply has a few mobile carts for labs. As a result, there is no single set of best practices that will encompass every LEA or every school within an LEA. Instead, this document covers the general areas that each LEA should consider with respect to their current/future deployments of WLANs.

Define the Requirements

Different schools have different needs. A WLAN should be designed to meet the requirements of the prospective users. Here are a few basic questions that should be considered when gathering requirements:

- **WHO** needs wireless connectivity? Faculty/staff, students or guests?
- **WHAT** computing devices will service be provided for? Laptops, Desktops, Point-Of-Sale devices, cell phones/PDAs, IP phones, etc? What applications will need to be supported (general Internet data, streaming video, IP multicast, voice, etc)?
- **WHERE** do users need wireless connectivity? Classrooms, offices, outdoors, etc?
- **HOW MANY** devices need wireless access in each location? Classrooms, cafeteria, library, offices, etc? How much bandwidth will be needed to support various applications?
- **WHEN** is connectivity needed? Will many devices require concurrent access as might be seen in online testing? Is connectivity needed outside school hours?

These areas will drive basic design principles such as coverage, capacity and security. It is absolutely essential to define the requirements up front as they will they will dictate the entire design.

WLAN Architectures

WLANs consist of devices called Access Points (APs) which convert wired Ethernet frames to wireless RF signals. Clients associated with the AP receive the RF signals which are then converted and processed as appropriate. At a basic level, there are two main approaches to deploying WLANs – (1) using autonomous APs (also known as "fat" APs) and (2) using lightweight APs (also known as "thin" APs). This paper will not discuss single channel vs. multi-channel (cell) RF architectures, but it is notable that some vendors have different RF engineering philosophies.

Autonomous Access Points

Autonomous APs are completely self-sufficient and are deployed as stand-alone devices that connect multiple clients to an upstream wired network. Each fully-featured autonomous AP is managed independently. This approach is the most basic deployment model. Many districts have deployed autonomous APs because they are cheap and available off-the-shelf. Figure 1 shows a sample architecture using autonomous APs. Because the APs are autonomous, there can be a wide variety of vendors and configuration sets in a given location.

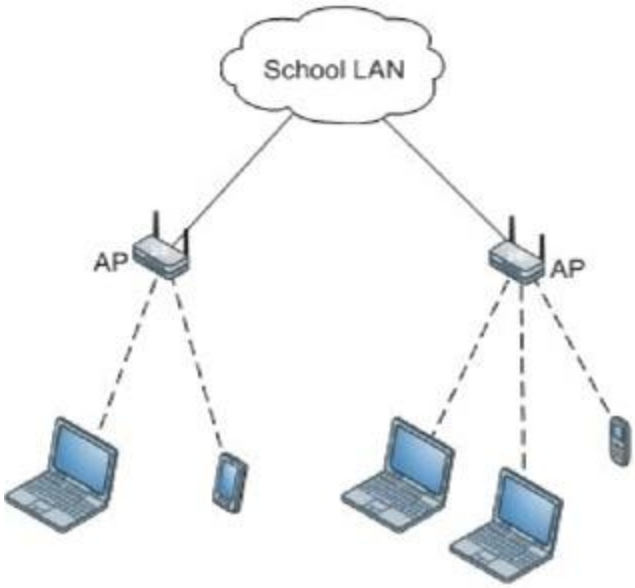


Figure 1: AUTONOMOUS/"FAT" AP ARCHITECTURE

Lightweight Access Points (LAPs)

Lightweight Access Points (LAPs) are under the control of central management by a cloud controller or a premise-based Wireless LAN Controller (WLC) which provides scalability

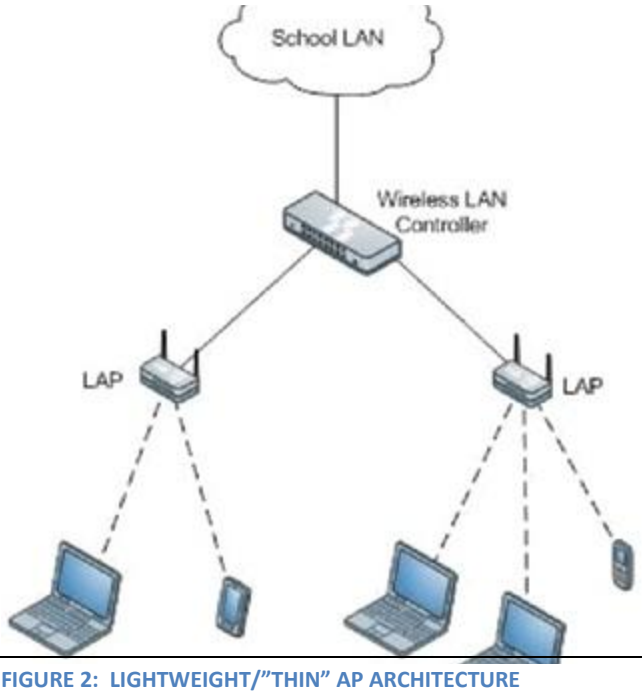


FIGURE 2: LIGHTWEIGHT/"THIN" AP ARCHITECTURE

and increased manageability. Typically the controller will have several key functions including enforcing configuration policies (security, RF thresholds, QoS), managing software, and enabling client authentication. While all APs convert wired Ethernet frames to wireless RF signals, the data traffic may be handled only at the AP level or by the AP in conjunction with the controller. The degree of AP autonomy depends on the wireless vendor and configuration, with APs often able to perform some combination of functions without the controller. The LAPs may append some management data to the frames sent to the controller which describe RF conditions and other WLAN data. Many districts are moving towards LAPs/controllers because of the increased scalability, management and features/functionality available. These deployments use a single vendor solution throughout the district, require significant planning, and can be fairly expensive.

Wireless Basics

There are a few technology principles that need to be considered when building a wireless infrastructure. This paper will not go in depth on wireless engineering concepts. Rather, the goal is to simply highlight basic ideas to assist with planning and general guidance.

1. **Different Technologies**: There are several different flavors of wireless technology to date as summarized in Table 1. This is no single flavor that is the "best" because technical requirements and budget constraints vary widely.

Table 1: WLAN TECHNOLOGY SUMMARY

Technology	Frequency (GHz)	Channels (US)		Data Rates (Mbps)		Throughput (typical, Mbps)	Standard Ratified	Typical indoor Range (m)*
		Total	Non-overlapping	Max/ channel	Supported			
802.11b	2.4	11	3 (1, 6, 11)	11M	1, 2, 5.5, 11	5	1999	35
802.11g	2.4	11	3 (1, 6, 11)	54M	1, 2, 5.5, 11, 6 ,9, 12, 18, 24, 36, 48, 54	23	2003	25+
802.11a	5	24	24	54M	6, 9 ,12, 18, 24, 36, 48, 54	23	1999	25
802.11n	2.4 or 5	Uses a/b/g bands	Uses a/b/g bands	300M	6, 9, 12, 18, 24, 36, 48, 54, others	100	2009	50
802.11ac	5	Uses 'a' (5GHz) band	Uses 'a' (5GHz) band	500M	6, 9, 12, 18, 24, 36, 48, 54, others	N/A	In progress	N/A

**Note: Distance is impacted by many variables including power, interference, antenna type, etc.*

2. **Interference**: RF interference is a major challenge to deploying wireless networks. Interference can be caused by other wireless devices operating within the same frequency range (i.e. think of two radio stations broadcasting different content at the same frequency). Sources of interference could include other WLAN devices in close proximity or technologies that happen to emit RF in the same frequency bands (i.e. Bluetooth, cordless phones, microwaves, and many others). The 2.4GHz range is generally viewed as more prone to interference as more devices share that frequency range.
3. **Channel Allocation**: As noted in Table 1, the 2.4 and 5GHz bands have different frequency ranges. There are several channels that subdivide a given range. Figure 3 shows how the channels are assigned for 802.11b/g. The important concept here is that some channels overlap. Using non-overlapping channels is a critical part of avoiding interference. Note that 802.11b/g has 3 non-overlapping channels while 802.11a has up to 24, depending on factors including vendor support and use of dynamic frequency selection (DFS) channels.

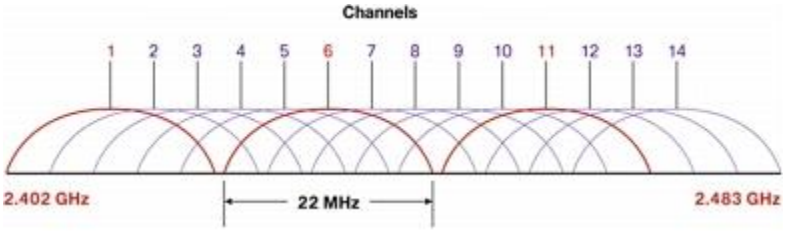


Figure 3: IEEE 802.11b/g CHANNEL ALLOCATION (SOURCE: CISCO SYSTEMS)

4. **Channel Bonding**: With more current technologies such as 802.11n and 802.11ac, adjacent channels may be combined to provide increased bandwidth. While channel-bonding is feasible on the 5GHz band, it is not recommended on the 2.4GHz band due to the limited number of channels and amount of overlap. Bonding 2 channels together to form a 40MHz band is supported with 802.11n. The proposed 802.11ac standard may allow bonding of as many as 8 channels. Use of single channels to form bonded channels affects the number of actual available channels.
5. **Shared Access**: Today's wireless technology operates as a half-duplex shared medium – very similar to an Ethernet hub. Bandwidth is shared across users, collisions are possible, and only one device can transmit at a time.
6. **Distance Constraints**: The greater the distance between communicating devices, the lower the data rate (see Figure 4). The higher the frequency, the shorter the possible distance. Adding power to the transmitter and using different types of antennas will help increase distance. The downside to increasing power/distance is that it potentially results in interference issues or security concerns (increasing reach to unwanted clients).

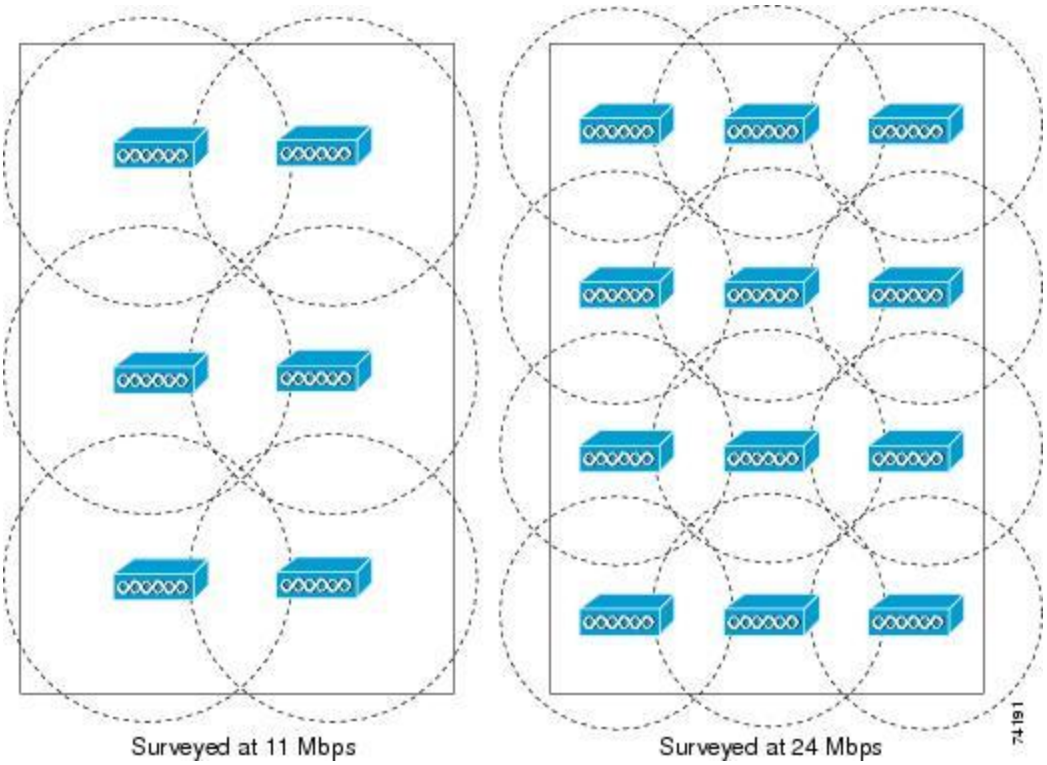


Figure 4: AP DENSITY WITH DIFFERENT DATA RATES (SOURCE: CISCO SYSTEMS)

7. **Multiple Data Rates**: As noted in Table 1, the different 802.11 technologies support different data rates based on the quality of the signal. The higher the signal quality and shorter the distance, the greater the possible data rate. APs transmit at the rate of the slowest associated client. A user associated to an AP at a low data rate will slow down all other clients associated at higher rates to the same AP. The higher the required data rate, the more APs will be needed due to both capacity and coverage, as shown in Figure 4.
8. **Physical Obstacles**: Wireless signals have different properties at different frequencies. Generally, a signal at 5GHz will have more signal degradation through walls and floors than a signal at 2.4GHz. Other objects in school locations such as filing cabinets, mirrors, plumbing, duct work and many others can significantly alter RF characteristics.

Design and Deployment Best Practices

1. **Site surveys are critical**. The survey output will determine AP placement and channel selection for optimal coverage and capacity. Several commercial tools can assist with performing site surveys. It is critical that the same model of equipment be used during the survey as is deployed in production. Network requirements must be defined prior to performing the site survey. Many LEAs have opted not to have site surveys performed prior to a deployment due to cost constraints. The long-term operational costs associated with a poor layout/design will far outweigh the costs of a proper survey.

a. Surveys must utilize the same equipment that will be used in production.
b. Surveys should be performed using the minimum data rates required. For example, if clients must be associated at 6Mbps, then APs should be placed where 6Mbps can be maintained by clients.
c. Surveys should be performed in a school environment that is ready for students. In other words, performing a survey during construction or without objects in the classroom will not provide a valuable dataset.
d. Surveys should be performed with client-types in mind. If VoIP handsets are to be used, that will have a significant impact on the survey and overall design of the network.
e. Consider a post-installation site survey to validate that the actual deployment is indeed meeting design goals.

2. **Use Non-Overlapping channels**. In 802.11b/g environments in particular, use channels 1, 6, and 11. Use of channel bonding in newer technologies such as 802.11n and 802.11ac will affect the channel layout in the 802.11a band. Always avoid use of channel bonding on the 802.11b/g band. Proper surveys and controllers can assist with channel selection.
3. **Ensure Capacity**. For areas that have high bandwidth and a concentrated area of users (i.e. classrooms in a 1:1 computing school), plan for approximately 15-25 data users per AP. When wireless devices are used for high bandwidth applications or concurrent use such as online testing, an even greater number of APs may be required to achieve a density closer to 10-15 users per AP. If a 'bring your own device' (BYOD) initiative is planned, non-school-owned devices should also be factored into the bandwidth needs. This could equate to one or more APs per classroom. General BYOD recommended practices can be found at: https://edspace.mcnc.org/confluence/download/attachments/10027773/BYOD+MCNC+White+Paper.pdf?version=1&modificationDate=1345514718353
4. **Consider leveraging 802.11a or 802.11n and use the 5GHz bands.** This applies more for deployments focused on capacity such as 1:1 computing schools and is dependent upon budget and client interoperability. The 5GHz spectrum is less crowded with other devices and has many more non-overlapping channels than 802.11b/g. While 802.11a does not travel as far and is degraded significantly through walls/floors, that may be a positive in the classroom setting. 802.11n can utilize both 2.4GHz and 5GHz bands and allows for much higher bandwidth and client capacity. Use of the 5GHz band will become more critical when the 802.11ac standard is ratified.
5. **Avoid the use of autonomous access points. Use Wireless LAN Controllers with Light-weight APs, Wi-Fi arrays with integrated controllers, or other control architectures.** For environments with over ten APs, it makes sense to move towards centralization. The management features will allow for a much easier deployment as complex RF engineering tasks can be automated (i.e. channel selection, power levels,

triangulation of individual clients, roaming features, etc). Controllers also help detect rogue/unauthorized APs as well as mobile devices serving as access-points on campus which could be a problem for some schools to otherwise track down.

6. **Make Roaming Easy**:
    a. Use a single SSID for each group of users throughout the school campus. Using multiple SSIDs at different locations will make roaming tedious.
    b. Use a maximum subnet size of /23 (510 hosts) to limit the amount of broadcast on the network. Presence of unencrypted SSIDs as well as non-school-owned devices can deplete available addresses. If there are more than 510 devices at the school, most controller vendors offer seamless roaming features that work on networks with multiple VLANs/subnets.
7. **Use Power Over Ethernet** switches to connect APs back to the network. This will allow for remote power cycling, ease of deployment, and energy savings. The alternative is to have power injectors that are bulky and difficult to incorporate within cable management.
8. **Use gigE-capable Switches**. While 802.11n APs can negotiate lower speeds, as the amount of wireless bandwidth increases with newer standards, the wired ports must be able to accommodate the increased wireless throughput on the wired side.
9. **Set minimum signal and data rate thresholds**. This will prevent a single user from associating to an AP with a weak signal and degrading the performance of all other users connected to that AP. This can be accomplished by not allowing users to associate to an AP at rates/signals below configured thresholds. If 802.11b/g is chosen, a district needs to decide whether or not to support 802.11b clients. Allowing 802.11b clients will reduce overall WLAN performance.
10. **Implement User Authentication**. Most vendors offer a wide variety of authentication methods including 802.1X, RADIUS, LDAP and others. It is suggested that a district's existing authentication infrastructure be considered when choosing a vendor to ensure ease of integration. Authentication measures may be implemented at the controller or AP level depending on the solution. General K-12 recommended practices can be found at: https://edspace.mcnc.org/confluence/download/attachments/10027773/NCET+Security+Considerations+for+K12+rev1.pdf?version=1&modificationDate=1319914759000
11. **Implement Encryption**. Not all schools will find it necessary to encrypt traffic, however it is recommended that encryption be implemented. There are several options for encryption. WEP is not a viable option as it is easily cracked. Use wpa2/aes if possible. Districts should ensure that a chosen encryption method is compatible between wireless vendor and wireless clients.
12. **Create a separate SSID for guests**. If guest access will be permitted, connectivity should be controlled. This could include any wireless device not managed by the LEA (i.e. student cell phones/PDAs, parent laptops, etc). Guests may not be required to authenticate, but they should have to agree to an Acceptable Use Policy. Guests should be placed on a separate network and treated as "untrusted" from a security perspective.

Districts will need to decide what services will be allowed to guest users. Some LEAs may wish to rate-limit guest access to prevent saturation of Internet bandwidth.

13. **Become familiar with vendor feature/functionality options**. Many LEAs simply deploy network infrastructure using default values and rarely spend the time to optimize the environment. For WLANs, many vendors have specific features that need to be customized to work in specific environment. For example, if multicast is required for some applications, there may be some features available to enhance multicast delivery. Simply deploying a system using default values will not translate into positive results for either autonomous APs or LAPS. Each vendor has their own set of best practices that should be followed.
14. **User management and monitoring features of controllers to be proactive**. For example, some solutions will send SNMP traps if the number of users connected to an AP goes over a configured threshold. The identification of rogue APs including BYOD hot spots on the campus could also generate an alert to IT staff. Some vendor solutions will triangulate the physical location of various clients and/or provide real-time coverage maps. Using the proper management/monitoring will ensure the maximum availability and quality for users.

Appendix A – Links to Additional Information

Design Guides

Enterprise Mobility Design Guide (Cisco Systems)
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/emob41dg-wrapper.html

Wireless and Network Security Integration Solution Design Guide (Cisco Systems)
http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/secwlandg20/sw2dg.html

Planning a Wireless Network (HP)
http://www.hp.com/rnd/pdfs/802.11technicalbrief.pdf

Site Survey Information

Wireless LAN Site Assessment (HP)
http://www.hp.com/rnd/pdf_html/wirelessLANsite_assessment.htm

Site Survey Best Practices (Fluke Networks)
http://www.cellgain.com/Wireless_Site_Survey_Best_Practices.pdf

Indoor Access Points: Site Survey and Planning (Aruba Networks)
http://www.arubanetworks.com/pdf/technology/DIG_Aruba_Site_Survey.pdf

K-12 Specific Resources

Wireless LAN Best Practices Guide (K-12 Schools of Alberta, Canada)
http://education.alberta.ca/media/822010/wirelessbestpracticesguid.pdf

Lessons in Wireless for K-12 Schools (Aruba Networks)
http://www.arubanetworks.com/pdf/technology/whitepapers/wp_K12.pdf

50 Questions K-12 School Districts Should Ask WLAN Vendors (Blog)
http://wifijedi.com/2009/02/16/50-questions-k-12-school-districts-should-ask-wlan-vendors/

Security Best Practices for Grades K-12
https://edspace.mcnc.org/confluence/download/attachments/10027773/NCET+Security+Considerations+for+K12+rev1.pdf?version=1&modificationDate=1319914759000

Bring Your Own Device (BYOD) – Supporting Personal Devices on the LEA Network

https://edspace.mcnc.org/confluence/download/attachments/10027773/BYOD+MCNC+White+Paper.pdf?version=1&modificationDate=1345514718353

Appendix B – Vendor Information

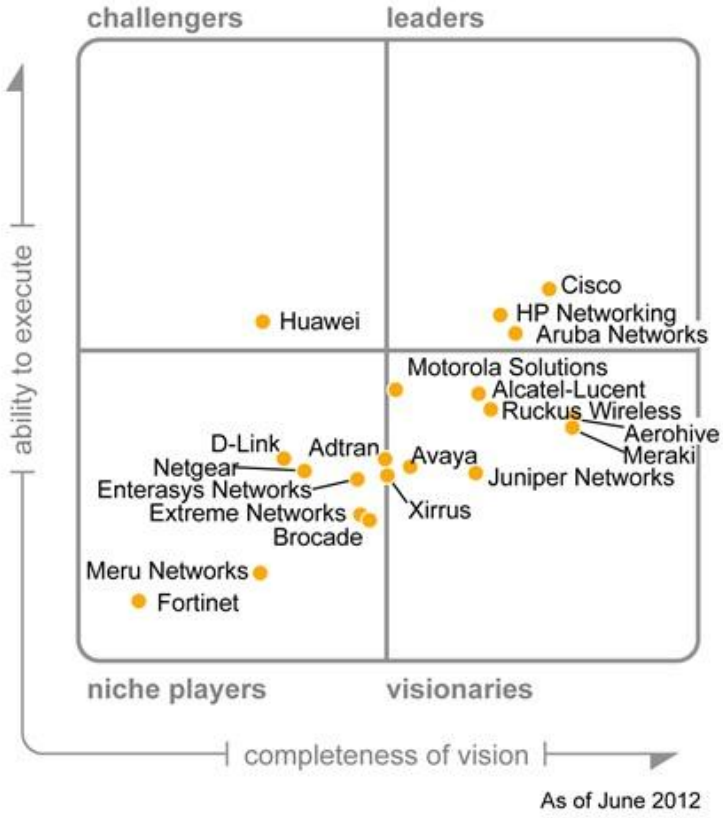
While the following list is not inclusive of every WLAN manufacturer, this list should provide a starting point to popular players in the current marketplace.

Adtran www.adtran.com
Aerohive Networks www.aerohive.com
Alcatel-Lucent www.alcatel.com
Aruba Networks www.arubanetworks.com
Avaya www.avaya.com
Bluesocket www.bluesocket.com
Brocade www.brocade.com
Cisco Systems www.cisco.com
D-Link www.dlink.com
Enterasys Networks www.enterasys.com
Extricom www.extricom.com
Extreme Networks www.extremenetworks.com
Fortinet www.fortinet.com
Hewlett-Packard/Colubris www.hp.com
Huawei www.huawei.com/en/
Juniper www.juniper.net
Meraki www.meraki.com
Meru Network www.merunetworks.com
Motorola www.motorola.com
Netgear www.netgear.com
Nortel Networks www.nortel.com
Proxim Wireless www.proxim.com
Ruckus Wireless www.ruckuswireless.com
Siemens www.siemens.com
Symbol Technologies/Motorola www.symbol.com
Trapeze Networks www.trapeze.com
Vernier www.vernier.com
Xirrus www.xirrus.com

Gartner market overview with vendor summaries, strengths, and cautions can be found here:

http://www.gartner.com/technology/reprints.do?id=1-1AYV4GJ&ct=120619&st=sb&mkt_tok=3RkMMJWWfF9wsRojuqvBZKXonjHpfsX%252F7%252BQqXKag38431UFwdcjKPmjr1YAASMR0dvycMRAVFZl5nQ1KD%252BKUcoVU7fpPAFI%253D

Figure 1. Magic Quadrant for the Wired and Wireless LAN Access Infrastructure



Source: Gartner (June 2012)

Figure 5: Gartner Magic Quadrant for the Wired and Wireless LAN Access Infrastructure