# DATA NETWORKING SYSTEMS
# WIRED VS. WIRELESS REPORT

## Antelope Valley Community College
## Health and Sciences Building

02/17/2010

Prepared for:

Antelope Valley Community College


Vantage Technology Consulting Group
201 Continental Blvd. • Suite 120
El Segundo • California 90245
310 536 7676 • fax 310 536 7677 • www.VantageTCG.com

TABLE OF CONTENTS

## EXECUTIVE SUMMARY

At the request of the College, Vantage has put this report together to outline the capital cost savings and operational cost implications of removing hard-wired voice and data cabling in the labs and classrooms, while deploying wireless coverage throughout the new Health and Sciences building. In doing the study, Vantage reviewed the implications of deploying IEEE 802.11 a/b/g/n wireless technology as the primary access to the data network (in lieu of more typical wired connections) at Antelope Valley Community College within the new Health and Sciences Building. More students and faculty are equipped with laptop computers and mobile devices capable of wireless connection to the internet and wireless is becoming the primary means of network access for these users. Uses include:

- Downloading classroom materials
- Collaborating on class work and projects
- Streaming recorded and live video

The wireless environment can also offer cost savings to the College. This report provides a basis for a Cost Analysis Model which compares the Wired vs. Wireless costs, will detail assumptions and risks associated with this approach, and offers a recommendation to the College.

The table below summarizes the associated costs of a Wired vs. Wireless implementation at Antelope Valley Community College's Health and Sciences Building:

| Summary | Capital Costs | Operational (Annual) Costs | Total Cost (5 year duration) |
|---|---|---|---|
| Wireless Installation | $79,600 | $30,300 | $231,100 |
| Wired Installation | $423,590 | $1,150 | $429,340 |
| **Cost Difference between Wired and Wireless Solutions** | **-$343,990** | **$29,150** | **-$198,240** |

As can be seen from the above table, the use of wireless technology rather than wired connections can result in a significant overall cost saving to the College, with a reduction in capital costs than is not offset by the increase in operational costs. However, investment in operational costs will be required in order to maintain the same level of service as the wired equivalent.

# WIRED AND WIRELESS NETWORKS

## I. PURPOSE

As a result of a meeting between Antelope Valley College, Klassen Corporation, tBP Architecture, and Vantage, Vantage was asked to assist the College in providing a report in which it reflects the capital cost savings introduced by removing the voice and data cabling within the floorboxes and desks in each of the labs and classrooms and deploying full wireless for the new Health and Sciences building, as well as outlining the operational cost implications as the College ITS feels as though they do not have the resources nor the personnel to support wireless at this time.

## II. OVERVIEW

Networking technologies that allow users to share data, applications, and peripherals are constantly evolving, offering higher connection speeds and larger bandwidth capacities. In today's educational environment many devices require network connections, including desktop computers, laptops, tablets, cellular and mobile phones, PDAs (Personal Digital Assistants) and other devices. These network connections facilitate access to inform stored on the College's local area network (LAN) as well as the Internet. Users and their devices today rely on, and expect, a connection for information more than ever before which poses the overall networking question: How should Antelope Valley College provide a LAN connection to the users and systems?

This report looks at wired vs. wireless connection methods to determine the most cost effective and prudent installation, configuration, and support of our basic requirement which is a connection to the network.

## III. OPTIONS

Two primary methods of providing a network connection exist; wired (via cable) and wireless. Wired networking has traditionally been deployed for stationary computers and machines which do not require mobility. Wireless networking allows the user to roam wire free where the wireless network exists while never dropping the connection to the network. Traditionally, wired connections have been the primary means of access to the network, with wireless connectivity offering a secondary means of connection for mobile devices.

### A. Wired Networking:

Wired networking connections provide the foundation of the Local Area Network. Incoming connections, Data Center interconnections, IT closet facilities, and stationary computing devices have all traditionally been connected to the network via a series of cables. The primary benefit to a wired connection is that the wire provides a standard level of service (performance, security, reliability) which can be relied upon in all situations. Typically, wired connections (correctly installed) have an extremely low failure rate and provide a standard of service which helps provide a very low cost for support per connection. Once the connection is configured, very little needs to be done in order to maintain the system.

1. Wired Advantages

   - Standard level of service guaranteed to each user/device
   - High bandwidth capable (1GB/10GB)

- Low cost of support
- Higher level of security
- Modular, standardized connectivity with backwards compatibility
- Minimally impacted by radio-frequency interference

2. Wired Disadvantages

- High cost of initial installation
- Difficult to install in some locations
- Number of connections limited by number of cables installed

## B. Wireless Networking:

Wireless networking technology is relatively new to the enterprise and education markets. Although individual consumers have been using wireless routers and access points for some time, systems capable of providing wireless services to a large number of users across a campus began maturing about five years ago. With the ratification of the IEEE 802.11n wireless specification (which offered significantly higher performance and backward compatibility), the proliferation of wireless technologies has significantly increased in all markets.

Wireless networking is deployed for a number of reasons; the primary purpose being mobility allowing laptop users to roam the facility freely and not rely on a wired connection. Although the freedom to roam the facility and always be connected to the LAN can be a great advantage for network users, the amount of support needed to manage the system and users is much higher than that required by a wired network. Due to the broadcasting nature of a wireless system, security is an important concern and provisions should be made for guest / unauthorized users to use the system in a limited and controlled way. Additional support by the IT Team is often required to configure a user to use the wireless network, to ensure the wide variety of disparate hardware will work with the College's wireless system, and to provide Help Desk support for wireless issues.

The College's wireless network is a shared resource meaning all users share the available bandwidth from the access point they are connected to. This can create connection and throughput problems when a high number of wireless-attached users congregate in the same place. Another issue occurs when a user tries to use a network intensive application which could hoard the bandwidth from the wireless access point. For this reason, wireless networks are not recommended as the primary connection for high bandwidth intensive applications.

1. Wireless Advantages

- Supports user mobility
- Provides network connectivity in locations without wired ports
- Significant capital cost savings over a wired network

2. Wireless Disadvantages

- Additional support and management of the wireless system and users leads to higher operational costs

- More susceptible to security breaches
- Shared bandwidth system which can limit performance
- Connectivity not always guaranteed
- Impacted by radio frequency interference

ASSUMPTIONS & RISKS

## IV. ASSUMPTIONS

The following assumptions have been used to create the Cost Analysis Model for wired and wireless connectivity options in the Health & Sciences Building:

**Wired Costs**

- Capital costs include (952) Cat 6 Cables for classroom and lab space. This includes all labor and materials costs. Costs for network electronics including switches to support the (571) active ports.
- Operational costs for the wired network assume $1,150 per year for maintenance and support. Hourly labor is assumed at $50/hr.

| Wired Costs | Unit | Cost | Total |
|---|---|---|---|
| Cabling | 952 | $295 | $280,840 |
| Network Electronics | 571 | $250 | $142,750 |
| **Total Capital Cost** | | | **$423,590** |
| Administrative Support | 23 | $50 | $1,150 |
| **Total Operational Cost** | | | **$1,150** |

**Wireless Costs**

- Capital costs include (40) additional access points required to provide sufficient coverage throughout the building (procurement and installation), with (2) Cat 6 cables to each access point (including labor and materials). Costs also include network electronics to support the (40) active ports. In addition, 120 hours for Initial Setup, Training and Policies are included. Hourly labor is assumed at $50/hr.
- Operational costs assume $30,300 for maintenance and support for the wireless network per year. This includes additional user support costs as the campus' helpdesk will experience a higher quantity of user support calls. An estimate of 1200 users with 3 calls each at 10 minutes per call for the support of wireless at the Health and Science building. Hourly labor is assumed at $50/hr.

| Wireless Costs | Unit | Cost | Total |
|---|---|---|---|
| Access Points | 40 | $1,000 | $40,000 |
| Cabling | 80 | $295 | $23,600 |
| Network Electronics | 40 | $250 | $10,000 |
| Initial Setup | 120 | $50 | $6,000 |
| **Total Capital Cost** | | | **$79,600** |
| Administrative Support | 6 | $50 | $300 |
| User Support / Helpdesk | 600 | $50 | $30,000 |
| **Total Operation Cost** | | | **$30,300** |

## V. RISKS

Wireless networks can present a number of risks to end-users and Network Administrators.

End-user risks include issues with performance, interference and reliability. In terms of network services, a Wireless Local Area Network (WLAN) provides data rates slower to that of wired networks. A typical laptop user can access files at a data transmission speed of 1 Gigabit per second (Gbps) or 1000 Megabits per second (Mbps) through the Local Area Network (LAN) wired connection, however through the WLAN, the maximum data transmission speed is theoretically 300 Mbps for each access point (although in all likelihood actual throughput will be significantly less than that.) This rate is also dependent on how many users are associated with one access point. For example, if 20 users are associated with one access point, then each user will only be able to utilize a maximum theoretical speed of 15 Mbps (with actual throughput considerably lower.) Accordingly, wireless performance limitations typically manifest themselves in two forms:

- Problems with large files. Large files typically take longer to download on a wireless network than from a wired connection.
- Problems with multiple access of the same file. It may not take one person long to download a spreadsheet over a wired connection, but it can take considerably longer to download the same file when twenty students all try to download it at the beginning of a class.

In addition, the WLAN is susceptible to multiple forms of interference and signal attenuation, including losses from the materials that the building is made to, interference from other radio frequency generating devices (including microwave ovens), and co-channel interference. Any of these sources of interference can result in weaker wireless signals and slower data transmission speeds.

Administrator risks deal with security and management. Unlike a wired network, a wireless network is susceptible to attack by intruders who could be located inside or outside of the building. Unencrypted messages can be picked up through eavesdropping tools which can put sensitive information at risk of being acquired and there are many readily-available software packages that can detect and reveal passwords and encryption keys. Attackers can also shut down the College's wireless network by deploying a Denial of Service attack that floods the wireless network with meaningless traffic leaving no capacity for real users.

The WLAN also requires additional resources to support network maintenance and troubleshooting. Wired connections are standardized and easy to manage and maintain, but wireless connections are supported by many differing vendors and equipment and have more settings that must be administered to create a secure managed environment.

## CONCLUSION

Moving to a wireless solution does appear to provide cost savings to the College and (potentially) additional convenience to its users. However, as stated above wireless does present additional risks and requirements. Accordingly, it is important that expectations of the wireless network are managed by the College to be at a lower level than the equivalent wired network. Users should be educated to expect slower transfer rates and increased time to access online materials. Administrators should expect increased helpdesk calls and a higher involvement in managing the network to protect from potential security threats. The Cost Analysis Model includes the cost of these additional resources within the annual operational cost of the WLAN. To appropriately mitigate the risks identified and plan for the increased level of management needed, it is recommended that the College invest in the appropriate technical personnel to maintain, troubleshoot, and secure the wireless network.