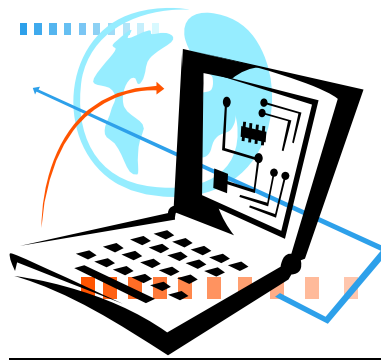


# Wireless Networking for K-12 Education in B.C.

July 2007



# INDEX

<b>TABLE OF CONTENTS .....</b>	<b>2</b>
<b>EXECUTIVE SUMMARY .....</b>	<b>3</b>
<b>CURRENT WIRELESS TECHNOLOGIES .....</b>	<b>5</b>
<b>WIRELESS SECURITY IMPLICATIONS AND OPTIONS.....</b>	<b>9</b>
<b>WIRELESS CONSIDERATIONS AND QUESTIONS FOR K-12 EDUCATION.....</b>	<b>11</b>
<b>SECURITY ISSUES FOR K-12 EDUCATION IN BC .....</b>	<b>15</b>
<b>RECOMMENDATIONS AND POSSIBLE MODELS .....</b>	<b>17</b>
<b>FUTURE DIRECTIONS FOR WIRELESS .....</b>	<b>18</b>
<b>CASE STUDIES .....</b>	<b>19</b>
SD72 CAMPBELL RIVER.....	21
SD23 CENTRAL OKANAGAN .....	23
SD43 COQUITLAM .....	25
SD92 NISGA'A.....	28
SD67 OKANAGAN SKAHA.....	30
SD 28 QUESNEL.....	32
SD36 SURREY.....	34
<b>GLOSSARY OF TERMS .....</b>	<b>38</b>
<b>BIBLIOGRAPHY .....</b>	<b>41</b>
<b>APPENDICES AND REFERENCES .....</b>	<b>42</b>
PLNET BULLETIN: WIRELESS LAN ACCESS POLICY .....	42

## Executive Summary

Today, wireless technology is pervasive in all aspects of people's personal and business lives. In the education environment, where the customers are young, 'millennial' students, there is a strong expectation that the technology environment will provide services and infrastructure to support the ways they work and interact. The proliferation of mobile devices such as cell phones, PDAs and laptop computers is placing huge stress on educational institutions, both in providing the connectivity required and offering learning environments that align with the ways students think, learn and work.

Those under 25 years of age have never been without electronic communications; they grew up using computer technology. The past five years have seen an explosion of social software products facilitating instant communication, 24/7 availability and the ability to multi-task effectively. The Internet has provided online access to a research library of staggering proportions, rendering many of the more traditional resources obsolete. Students, teachers and parents are challenged to demonstrate not only search skills, but also the ability to assess and determine value from the multitude of online resources.

Along with the benefits online services and devices provide, there is an inevitable 'dark side' which is common to any service offering an opportunity for anonymous access to people and resources. Security and safety have expanded from the pure physical realm to include the myriad of online services and opportunities wireless devices --which are accessible anywhere, any time-- provide.

For many school districts, network connectivity within schools, between sites, and to the Internet has been a major challenge for the past 10 years. Funding and technical support continue to compete with other priorities, but the Provincial Learning Network (PLNet) has provided significant bandwidth and connectivity, addressing many of BC school districts' Wide Area Networking needs. While there are still numerous challenges in wiring and connecting school sites, particularly in older buildings, the majority of school buildings have some or most teaching and administrative areas serviced by wired network connections. These wired networks typically provide connection speeds of between 10 Mbps and 100 Mbps, with sophisticated router and switching capability for managing traffic and security.

Early adoption of wireless connections was introduced by Apple prior to 2000. To date, however, the implementation of wireless technologies in schools and districts has been somewhat limited. In many cases, wireless LAN technology is an overlay to wired networking, often providing expanded access to teaching areas with limited or no physical connections. In some older facilities, wireless has been used to avoid costly infrastructure wiring or to provide access in areas where cabling is difficult or impossible to install.

While it may be tempting to ignore or refuse to support wireless technology in schools, that option has passed. Virtually all laptops, PDAs and other personal technology devices have wireless capability and many offer default settings with little or no security. Users will try to connect these devices to building and corporate networks, or will bypass the existing supported networks and security if they are perceived to be blocking effective use of individuals' personal technology.

This white paper will address a number of the challenges associated with the implementation and management of wireless technologies, with particular focus on Wi-Fi (local area network) technology. The paper outlines the technology and terminology of wireless, along with the challenges and issues inherent in installing and supporting these networks. As with other technologies, there are specific considerations inherent to the school and educational environment. It is our hope that this paper will aid readers in becoming more informed and help them to ask the right questions, make appropriate decisions, and be successful in implementing wireless technology.

This report is intended to serve as an introduction to the wireless world and offers a significant amount of information and advice, numerous suggestions and some BC-based examples of current wireless installations. It should not, however, be considered the complete or final solution to districts' wireless challenges. Finally, while several products are mentioned or discussed in some detail, the report does not express a preference for any specific vendor or product. Further, the presence or absence of any vendor or product does not imply any bias, positive or negative.

## Current Wireless Technologies

Wireless technology is pervasive in today's society. A large proportion of the population carries cellular telephones and virtually every laptop and PDA has either a built-in wireless antenna or a wireless card (PCMCIA) that can be inserted into the device to provide connectivity. Staff and students in schools use and expect to be provided with consistent, accessible connections to their e-mail, websites, text and voice-mail systems. It is no longer considered a frill, but a necessity, to be connected anywhere, anytime. Schools and districts that cannot or will not provide such services risk alienating or frustrating their clients and staff.

Wireless connectivity is not an obvious choice or priority for many school and district buildings, as some districts are still working to establish basic wired network connections. Regardless of the type of wireless being considered, current wireless technologies are not able to provide the type of data speed experienced with wired connections, typically running at 100Mbps or faster. Thus wireless is still not an obvious replacement for a wired environment, and each case must be considered on its own circumstances. The best answer to the question, 'Should I install wireless' is usually, 'It depends'!

Wireless technologies can be grouped by type of technology and coverage area served. Common acronyms for wireless include WWAN, WMAN, WLAN, and WPAN. While each of these will be covered below, the majority of this document will focus primarily on the WLAN, also called Wi-Fi or IEEE 802.11. It is important to remember that each of these types uses a specific, sometimes proprietary technology, and the ability to switch between various networks with a common device is almost impossible. Significant developments are under way, however, and it is expected that such devices and network interoperability will be commonly available within the next three to five years.

WWAN, or Wireless Wide Area Networks, have traditionally been supplied as subscription services by major suppliers such as telephone or cable vendors. They typically rely on large scale services similar to cellular phones, with the same issues around coverage and poor connectivity in more remote areas. Devices like the RIM Blackberry or the Sony TREO operate in this space. Current technologies use acronyms like 2G, 3G, GSM, CDPD, and CDMA. Many of the second generation (2G) technologies are incompatible with each other, causing limited roaming capabilities for those who must travel outside their carrier's service area. Third generation (3G) technologies are anticipated to follow a global standard and offer wider, if not world-wide roaming abilities.

WMAN, or Wireless Metropolitan Area Networks, are used to establish relatively high-speed connectivity between multiple locations within a metropolitan area. Wireless connections using radio or infrared light are often used when locations span water or other boundaries to wired connections, and are often used as backups to wired links. Recently, vendors have begun providing broadband wireless services with much faster network access. Several communities have moved towards such coverage across their entire metro area, but connecting to such a service still has a subscription cost, either monthly or per connection. It can be an excellent choice for users who stay within the metro area that's covered.

WPAN, or Wireless Personal Area Networks are almost always ad-hoc wireless communications for devices like cellular phones, PDAs, or laptops, used within a personal operating space less than 10 meters in distance. Two key technologies in this space are infrared and Bluetooth. Both technologies can be used to communicate between devices, often through walls, pockets and backpacks.

WLAN, or Wireless Local Area Networks are the main focus of this report. The group of technologies in this category, commonly known as Wi-Fi or 802.11, have been in use since the late 1990s. A series of improved standards have evolved out of IEEE in the last decade. WLAN technology can be used as a temporary service, in spaces where wired connections are cost prohibitive, or as a means to expand the number of connections in a given space, such as a classroom or lab. WLAN technology can be used as an extension to a wired infrastructure, where access points (APs) act as a bridge between user devices and the existing wired backbone. With current laptop wireless abilities, small groups of users can also form a temporary network in a limited area without the use of an AP, or by using a standalone AP unit not connected to any other network resources. This set-up is often called ad-hoc or peer-to-peer networking.

WLAN technology is three dimensional in nature, not unlike a ball or sphere with the access point in the centre. Any receiver within range (inside the walls of the ball) can communicate with the access point, and thus establish a network connection. In order to picture how this technology provides the maximum coverage within a building or area, imagine a shoe box filled with tennis balls. Each ball will represent the coverage area of a single access point. Note that there will be space between each ball, representing areas where network connectivity will not be available, or will be very poor. The benefit of working in three dimensions is that a given access point can provide service between floors and through walls, subject to the construction material. Like cellular technology, there may be places that wireless frequencies have great difficulty penetrating. If wireless connectivity is necessary in almost all the corners of a given space, it will be necessary to overlap the coverage of two or more APs. There are some technical limitations to this, depending on which 802.11 standard you choose to support. In most larger installations, it is advisable to have a site survey done by a company that specializes in wireless configurations and networks, in order to determine connection requirements and challenges.

All network technology, whether wired or wireless, is rated with a theoretical maximum data rate, usually only achieved in a lab setting with ideal circumstances. The reality in any reasonable environment will be substantially less than the maximum rating. For example, current wired links are rated at 100Mbps or higher. Average user connections will be considered excellent if they actually run at a quarter to half of that speed. Throughput across a network connection is never constant and consistent: typical user communications happen in bursts, with significant wait periods while systems at either end process or retrieve data, or delay for a myriad of reasons. The same issues arise when considering the rated speeds of the various wireless protocols. In addition, wireless APs must share their full bandwidth with all the connections currently communicating with them. This means the maximum bandwidth available to a group of eight simultaneous users would be one-eighth of the total capacity. Adding more connections will further reduce the connection speed for all other users of that AP. This limitation is probably one of the largest reasons for dissatisfaction with wireless connection speed and reliability.

The main technology types for WLAN are a series of IEEE ratified standards with the number 802.11 followed by a lower case letter such as a, b, g, or i. The letter signifies a version or release improving in some manner on the original standard. The Institute of Electrical and Electronics Engineers (IEEE) ratified the original 802.11 standard in 1997, but this version ran at less than 2 Mbps, and was not good enough to support even voice applications.

The 802.11b standard evolved in 1999, increasing the data rates to an aggregate of 11 Mbps and running in the 2.4 GHz frequency band. This is still one of the most commonly used protocols, with almost all current wireless devices capable of running this version. The APs and wireless receivers are inexpensive and very easy to source. Access points using 802.11b have the capability to run on 11 different channels, but only three can overlap their coverage areas without causing interference. The practical range indoors for access point coverage is 50 to 100 meters, depending on the materials in walls, floors and ceilings. In addition, the 2.4 GHz band is shared with a number of devices, such as wireless telephones and even some microwave ovens. Locating an AP near a lunch area can create some interesting, intermittent connectivity issues. As noted above, sharing a network link of this type with more than about six to eight simultaneous users will probably result in very slow response times and poor connectivity.

The 802.11a standard was also ratified in 1999, and provided up to 54 Mbps data rates in the 5 GHz band. This enhancement not only increased the data rate, but the RF channels in this band do not overlap. This allows more APs to be located in overlapping coverage patterns without interference. There are 12 channels available; up to eight are able to overlap coverage areas. There are far fewer other devices in this band, but the coverage area for an access point is reduced to 20 to 30 meters. This means more APs are needed to cover the same area. The technology is more expensive, less available, and has not seen a significant uptake in market share at this point. 802.11a is also incompatible with 802.11b equipment.

The 802.11g standard was ratified in 2004, and appears to provide the best of both of the previous versions. It provides up to 54 Mbps data rates, while keeping the wider coverage pattern. It is fully backward compatible with 802.11b equipment. This is the current standard for most wireless laptops and new handheld devices, but it will support older equipment that still uses the 'b' version. This standard still runs in the 2.4 GHz band and therefore encounters the same interference risks with other devices.

The 802.11i standard is a recent improvement in the security of the protocols, adding much stronger encryption and authentication mechanisms.

Other standards in the 802.11 family will include 802.11e which addresses quality of service issues for voice over wireless networks, and 802.11n which will offer 100 Mbps or better data rates.

Wireless networks are composed of one or more access points, client devices with wireless capability to match the AP, a connection to a wired LAN/WAN, and some method of managing and securing the connections.

Access points come in two basic varieties – ‘thin’, where the AP has little or no intelligence in the unit, and ‘fat’ or ‘smart’, where the AP has everything necessary to manage the wireless connection and connect to any Ethernet switch. Many personal or small business networks use the latter, ranging from companies such as D-Link and Linksys to Netgear and Apple. These devices are robust, very inexpensive, and have great appeal for small group or ad-hoc networks. They do require individual configuration and management, which can be time consuming and complicated when changes are needed or an AP fails. Consistent policy and practise across multiple locations can be difficult to define and maintain. Some current intelligent APs can be converted to thin, with an upgrade to the firmware.

Thin APs and companion controller/management systems are becoming the preferred enterprise or large network choice. The individual APs are inexpensive, while robust management controllers provide centralized, scalable security, throughput, and authentication. Thin APs can be added or replaced as needed with minimal configuration. Consistent security and access management is provided centrally and can be monitored from one location. Vendors with enterprise solutions based on thin AP technology include 3Com, Cisco, Nortel, and Aruba.

Regardless of the choice of AP, each device must ultimately connect back to a wired network connection, usually a router or switch in a central location. In addition, each AP requires power, provided through a normal electrical plug or via the wired data connection (called Power over Ethernet or PoE). The latter option requires switch equipment capable of providing PoE to each port, but eliminates the need to locate the nearest plug-in or use extension cords.

Client devices are predominantly laptop computers, with current models containing built-in wireless adapters for communication with 802.11a/b/g networks. If users require connections to metro, or other wide area networks, plug in cards (PCMCIA) are available. Specific information will be required from the supplier of the service offering the connection. Other types of handheld devices, such as PDAs, also come with built-in wireless, but present some unique challenges with connectivity and security capabilities.

Most laptops provide a switch to enable/disable wireless connections, as well as an auto-sensing capability which searches for any network it can see. In many instances this may be other laptops in the area, which can create unintentional access to ad-hoc networks, many of which are totally unsecured. Ideally, client wireless connections should be configured for the highest supported connection speed available, as opposed to the default which is likely to be 802.11b. Client computers using wireless connections should always be aware of the networks they are connected to, and must ensure that security tools are in place to maintain the integrity of district networks. More specifics and guidelines for security of wireless networks and devices follow in the next section.

## Wireless Security Implications and Options

Security for networks and equipment in the wired world has been a concern for quite some time, with regular reports of hacking, data tampering and theft, malware, and inappropriate use of corporate resources. Network managers (and Superintendents) fear the day a school district becomes front page news due to some significant intrusion or data loss.

The introduction of wireless networks, and the proliferation of devices with built-in, activated Wi-Fi devices, has added a new level of worry and potential for security lapses. In its default settings, most laptops will have their wireless adapter active, broadcasting the user's network and computer access to anyone close enough to see it. Wireless networks, by their definition, beg to be used, and offer their services to all comers with compatible connections. While using a wireless device or access point unprotected may seem obviously insecure, the fact remains that many such networks exist, and continue to be used and abused while their owners are blissfully unaware. Take a laptop to a conference, meeting, or just start up a wireless session at home one evening. You will be amazed at the number of network identities that show up, most with little or no security. An entire new practice, called 'Wardriving', involves cruising around streets and neighbourhoods searching for available wireless networks.

Many of the inexpensive, basic wireless routers purchased for home, small business, or classroom use are almost always set to fully open access. Despite the best efforts of district or school network managers, such a router can be plugged into any wired network port and become a glaring hole in the network. There are a number of security practices that can be put in place to reduce or eliminate the risks of connecting wireless equipment to school or district networks. Using various levels and layers of defence will offer sufficient protection that casual attackers will not bother to try to penetrate the network.

Every wireless network router or access point has an assigned name called a Service Set Identifier (SSID) which is configured to a default name right in the factory. In addition, the router will have an administrative username and password, used for management of the device, which will have defaults that are easy to figure out. These should all be changed to make it a bit more difficult for attackers and unauthorized users to guess.

Where small numbers of regular users are connecting to limited APs, the MAC addresses of each wireless device can be entered in each AP filter table, allowing connection only to those devices with access. Regardless of the other measures taken, it is critical that encryption be enabled on all devices. Early equipment used WEP, which, users discovered, was easy to crack. Current equipment will likely support WPA or WPA2 for even stronger and stricter security requirements. Network managers should ensure that all equipment being connected can utilize the security level they select, as older devices may not support the newer standards. Individual laptops should also disable ad-hoc connections, selecting infrastructure access points only.

With the appearance of many public wireless hot spots in airports, coffee shops, bookstores and restaurants, a new level of exposure and risk has emerged. The trust factor of connecting to a known wired network is gone and the exposure to malicious factors increases substantially. Laptop users who purchase or use such services should ensure that local data on their hard drives is protected, preferably by encryption and definitely backed up off line. A personal firewall and current anti-virus software are also highly recommended.

Recently 'Evil Twin' attacks have begun to appear, where a Wi-Fi hot spot appears to be a legitimate one offered on the premises, but is actually set up by a hacker. If users need to connect to secure networks, use a Virtual Private Network (VPN) to create a secure tunnel between your laptop and the corporate service.

Regardless of the size of the wireless network, schools and districts need to ensure that someone is responsible for policy and implementation of security practices. Configuration of access points needs to be consistent, timely, and accurate. New and replacement units must be set up and must conform to existing criteria. All devices connecting to wireless networks should be configured as per a policy that is enforced. It only takes one device left unsecured to provide a hole into an otherwise secure network. Many organizations have isolated wireless networks from the rest of the wired infrastructure, using VLAN capability or by separating corporate and public segments entirely.

## Wireless Considerations and Questions for K-12 education

Considering the implementation of any new or different technology should generate a series of questions which should result in answers that are satisfactory to district governance, prior to proceeding. These questions include, but are not limited to, why, who, what, where, and how much. The case studies of districts that have implemented wireless programs have offered their answers, included below.

### Why do we need wireless?

Needing, as opposed to ‘wanting’ wireless is usually driven by infrastructure cost or unavailability of a wired network solution. It is impractical to provide individual wiring to many areas of schools where mobile devices are an integral part of curriculum or instructional method. In some cases, physical impediments such as asbestos or inaccessible walls, or power source limitations, make wireless the obvious solution.

### Why do we want wireless?

While some may argue that ‘need’ and ‘want’ are interchangeable, there are excellent arguments for wanting wireless to improve the integration of mobile technologies into the curriculum and classroom environment. District respondents all indicated that wireless was implemented and supported by district-level initiatives. Answers to why wireless is a necessary technology direction included:

- It provides for the integration of technologies in the classroom
- Laptops are convenient for many users and purchase price is becoming comparable with desktop computers.
- Technicians in the field are able to work more efficiently.
- Laptops, laptops, laptops.
- Learning anywhere, anytime; cost savings; revenue potential.
- Move to mobile computing is ubiquitous – future of computing in education – imperative to have good, reliable wireless infrastructure in schools.
- Fundamental to the on-to-one philosophy. We want to build student-centred learning. It’s not normal for laptops to be standalone; they are portable, personal and connected.
- Improve technology literacy and student performance, so students are prepared to be successful in the 21<sup>st</sup> century.

### Who will use it, and where?

The simplistic answer to these questions is ‘everyone’ and ‘everywhere’. Students, teachers, school-based and district staff, technical support, and even the public will make use of wireless resources, provided they have access to laptops or other devices, and the network is reliable and fast enough to satisfy their needs. The case study respondents identified laptop programs in many responses. Mobile laptop labs were cited; they may be wheeled into classrooms for specific projects. Others spoke of secondary students with school or district-provided laptops, or even personal devices, connected throughout school buildings.

Elementary implementations seem to trend toward smaller, zoned wireless areas, while secondary schools seem to prefer full building coverage, including courtyards and other exterior areas on school property. Almost all respondents indicated use by district or itinerant staff, including technical IT resources doing support in the buildings.

### What will wireless enable, and what are the risks?

Some of the answers to wireless' ability to enable can be found in the 'why' questions above. Aside from the fundamental flexibility to connect laptops in various locations, and use multiple devices in non-lab settings, it should be noted that wireless technology provides a window to more creative, innovative kinds of teaching and more engaged, interested students. Given the tools and availability, educators and students can do amazing things.

Many of the risks associated with wireless have been addressed in other sections of this document. Reliability, slow speed of connections, interference from other devices, cost, security, manageability, compatibility, scalability and consistency of technology implementation were all cited by case study districts.

### How long will it last?

Like all technology, new standards and advances in hardware and protocol may quickly render current equipment obsolete or less than state-of-the-art. Planning a multi-year implementation can be extremely difficult, when access to the same models of equipment is not possible. While not guaranteed, dealing with larger vendors can alleviate this condition, as they often provide a longer cycle of support before products become completely obsolete. Cheaper technology is not always the best solution for a long-term investment. Several respondents discouraged purchase of inexpensive, consumer-grade equipment. They suggest that while more expensive, a commercial product with good management and centralized control and security is more robust and last longer. Upgrading thin APs and installing new versions of software tends to be easier and cheaper with such products.

### How much will it cost?

The answer to this question will vary from district to district and from school to school. It will almost always be higher than available funding, but respondents have warned that those making the change should resist the urge to 'do it cheap'. They suggest that districts develop a district plan, set standards for equipment and implementation, and choose a timeline that is affordable and can be achieved successfully. Most respondents indicated a strong preference for solutions with a centralized management capability, managed by trained IT support resources. Thin APs, often powered by PoE switches, are the preferred direction for large building coverage. Smaller areas in elementary schools seem to trend towards APs with onboard management, although maintaining and following district standards can be a challenge.

### What's Required in Policy and Standards?

The successful implementation of any technology relies on a series of best practices, including district-wide policy, standards, support, and effective use.

All the case study respondents indicated that their wireless initiatives were partially or completely initiated at the district level, regardless of size. District-level support, both for funding and programs, will make wireless networking and associated laptop support a more stable, ongoing project. Individual schools have implemented a number of wireless programs independently, but are at risk for loss of funding or support if student numbers drop or a critical school staff resource leaves. In addition to district support for wireless initiatives, there should be standard policy and communication of expectations for use for this, and indeed any, use of technology. There are plenty of examples available, often called ‘Acceptable Use of Technology’ policies or guidelines.

In addition to policy, it is critical that districts engaging in wireless programs establish a set of standards that is common to all sites, equipment, and users. Ensure that wireless APs are compatible with district network infrastructure, follow existing security and authentication protocols and, ideally, are configured exactly the same way in each installation. Standards should extend to the laptops being connected, and must address issues such as access, security, and connectivity.

### Laptop Devices

This white paper will not attempt to articulate the educational rationale for using laptops in schools. The numerous reasons have been documented by other sources. For the purposes of this discussion, it is sufficient to say that the use and growth of laptops in schools will continue unabated and with increasing demand.

Laptop devices must have a consistent network configuration, including acceptable district network security, adapter settings, and local user identification (such as a MAC address). In addition, laptops, like other computers, must maintain current operating system patch levels and current anti-virus software. ERAC offers districts access to several anti-virus products at excellent pricing. Ideally, district IT technicians should define, load and update critical patches via automated services.

Increasing numbers of personal or public laptops are seeking connection to school and district wireless networks. These may be brought by students, staff, or the general public attending functions or courses in buildings. These devices add an additional level of complexity to a wireless network, as well as offering significant security considerations. In almost all cases, such units require a connection to public Internet resources, which can be offered in a number of ways without compromising the security of school and district secure systems. Users often cannot be identified (for secure login), may only use the network occasionally or one time, and require a simple, easy-to-use interface and instructions. In addition, personal laptops offer a much larger risk of introducing virus or Trojan activity into the network or onto other computers connected at the same time. Many sites that allow public connections have restricted access with separate subnets, firewalls, captive portals and pre-connect scans to ensure laptops have current patches and anti-virus software. While it may be more convenient to ignore and block public laptop access, this is an area of increasing demand and sites that are able to provide such access will find it sends a very positive message to the community. Those attending evening classes and public seminars will appreciate the ability to use the wireless connectivity without worrying about finding a lab, setting up authorized users and configuring software.

It should be remembered that even though network connectivity is wireless, laptops still require substantial electrical provisions. Large concentrations of laptops in a classroom or localized space will find significant numbers needing to plug in, as batteries may be low or drained by periods of heavy use. Battery life is being improved, but it is still not sufficient to support several hours of computer use. The lack of power outlets is becoming a common criticism of spaces where power users of laptops do their work.

## Security Issues for K-12 education in BC

When addressing security in any networking situation, more is always better than less. By the nature of their clientele, schools and districts are exposed to a wide range of security risks from children, teachers, staff, and the general public, who use the facilities during the evenings and weekends. Technology has provided such a rich spectrum of opportunity for either intentional or unintentional exposure to risk, from virus/Trojan infections to serious hacking, denial of service, or botnet attacks. Confidential or critical records and data files can be exposed, revealed or stolen for any number of illegal or embarrassing purposes.

Security for districts is a multi-tier issue that must be dealt with at the Internet connection site, building WAN connection, local network, individual access point, and connecting devices.

Almost all districts are connected to the world, through public Internet via PLNet, the government-provided network for education in BC. This is a traditional wired connection, supported and managed by external resources. As the carrier for many different user groups, PLNet has established policy to address its expectations for both wired and wireless security. The PLNet bulletin [Wireless LAN Access Policy](#) dated June 17, 2005 lists expectations and recommended logical controls for wireless access. A copy of the policy appears in the appendix of this report.

Larger districts will often have firewalls, routers, and segmented networks (VLANs) defined, to separate and protect internal systems and data. Educational access required to Internet and other teaching resources would be on one segment and protected operational data on the other. Authentication systems for computers directly connected to the wired network(s) ensure that access to both segments is properly controlled and logged. These same systems can and should be used to authenticate wireless connections as well. Enterprise WANs that need stronger controls can deploy 802.1x to authorize and audit wireless connections permitted to reach the corporate network. Used in conjunction with server certificates, it can ensure clients get to the services they intended. In larger networks, one or more specialized wireless controllers will offer additional security for connections through authorized access points. These devices will allow connections from registered APs, while blocking and identifying 'rogue' or unregistered devices. In a larger building, this management function may be implemented locally, or shared between local and district devices. Wireless Intrusion Prevention systems should be considered if misuse or attacks are going to adversely affect speed or risk access to critical systems. Guest access to wireless networks should be routed through a captive portal, to track use and enforce time and bandwidth limits.

Individual access points must also be configured and managed, preferably by a district-level technical resource. This will ensure consistency and integrity of the security measures defined by district policy. If applied properly and uniformly, 802.11 protocols and standards offer significant security. Wi-Fi-certified products offer either WPA using Temporal Key Integrity Protocol (TKIP) or WPA2, using 802.11i and AES to secure data in a stronger, more efficient manner. Under no circumstances should APs still be using the original WEP security, and only older legacy APs should still be using WPA. Access points should always be configured with non-default, descriptive SSIDs. In some cases, SSID names may be hidden by not broadcasting their service to all network adapters. For small numbers of clients, registering MAC addresses will add additional security, but the addresses must be added to each AP, and can be spoofed fairly easily.

In summary, there are security risks when using wireless networking, but such risks are manageable and capable of being reduced to an acceptable level, if not eliminated completely. It should be understood, however, that security is not something put in once and ignored; further, it is not advisable to settle on a single security measure. It is strongly advised that districts have policy in place, as well as centralized network expertise to ensure that security is maintained and monitored.

## Recommendations and Possible Models

1. Define a district policy on wireless networking. Include security specifics, as well as appropriate usage of network resources.
2. Define and ensure that standards are upheld at all sites. Purchases should be made, or at least advised on, by central network specialists who can ensure compatibility and appropriateness for the site's needs. If a district has not defined policy and standards, it is guaranteed that school sites will have purchased their own wireless APs and have installed them without telling anyone outside their building. These are absolutely the biggest security risks, as they have likely been installed without the benefit of any of the security measures discussed above.
3. Avoid consumer-grade equipment, unless wireless installations are very small or the APs have been vetted and approved by IT support.
4. Seriously consider a district-wide solution. Investing in thin APs and an enterprise-grade controller, switches, firewalls, and authentication will pay dividends in terms of support and scalability. Most case study districts recommend this method of deployment even though, at times, it means higher initial costs and slower implementation.
5. If large wireless installations are involved, consider getting a site survey and evaluation done by a company that specializes in wireless engineering.
6. Use a multi-level security model with as many different components as are feasible within your district or school. Guest access should be isolated and secured as much as possible, using separate SSID and/or a captive portal with defined access to services.
7. Don't put wireless in and leave it. Regularly monitor traffic, speed, reliability, and usage. If the numbers are good, this is a metric that indicates success. If the numbers are poor, the installation can be revisited in the hope that improvement can be made.
8. There should be periodic audits of both wired and wireless networks. Searches for rogue access points, failed connection attempts and other hacks will offer some reassurance of the integrity of the network. Districts should ensure that a formal external security audit is done every two to three years, to address audit concerns and provide an unbiased look at the network.
9. Research the current wireless technologies available and get the most current equipment compatible with your laptops and network infrastructure. The majority of vendors in the wireless arena are fairly compatible with mainstream router and switch manufacturers.
10. There is no absolute best solution to recommend, as each district will have different needs, resources and infrastructures. The case studies included in this paper offer examples of various sizes of districts, from very small to large. Talk with the contacts listed and use the advice and services of the infrastructure vendors already supplying your district.

## Future Directions for Wireless

Districts implementing wireless technologies should be aware that the industry continues to evolve very quickly. This section includes several issues to observe and consider in the next few years.

To date, each of the wireless technologies has been built on a unique platform, with anywhere from limited to no interoperability. Watch for adoption of wider, more generic standards allowing more shared services and automatic sensing/switching between services.

Increasing numbers of communities are providing widespread coverage for metropolitan WAN service. One such technology, called WiMAX, offers broadband network speeds over wide areas, modeling the current cellular telephone services. While still subscription based, it will offer options and alternatives to wired connections and specialty Wi-Fi services in metro areas. Such services also offer a good disaster recovery backup solution for wide area network connections.

Mesh networks are another growing trend, with 802.11s recently defining a standard routing protocol to allow wireless devices to interconnect, forming a large ad-hoc network.

802.11n, while still a work in progress, will define the next generation of Wi-Fi devices and connectivity. It is expected to deliver data rates in the order of 248 Mbps, compared to 54 Mbps for 802.11g. This technology makes use of multiple transmit and receive antennas, and operates in both 2.4 and 5 GHz bandwidths. This will likely require a complete replacement of switches and access points and, in some cases, probably controllers as well.

Ultra-Wideband (UWB) is a short-range, high-speed technology that will likely replace Bluetooth. This technology is capable of data rates approaching 500 Mbps, with relatively low power consumption.

Network adapters in mobile devices will continue to evolve, allowing devices to move more seamlessly across multiple access points and between LAN/WAN/MAN services.

Handheld devices such as PDAs will continue to grow in use, as software interfaces for small screen size and limited architecture become mainstream options for popular software packages and services. Multi-function network adapters will allow choice of network service, either manual or according to signal strength.

Voice over wireless will continue to grow, as wireless technology, bandwidth and quality of service improve. Cellular telephone devices will evolve to switch seamlessly between local and metro services, as well as evolving further into multi-function communication devices.

## Case Studies

ERAC extends its thanks to all the school districts that took the time to respond to our request for information on their wireless implementations. They have agreed to share their models and experiences with this white paper's readers. A comparative summary is provided, along with each district's specific responses. In some cases, districts have requested that data considered sensitive or security related be edited or removed.

## District Wireless Summary

District	#	Students & Schools	Apple %	PC %	Other %	Tech Support Model	Network Support Model	Wireless Penetrat'n	Wireless Protocols/Speeds	Wireless Security in Use	Project Initiated By	Success? Measures Metrics
Surrey	36	Stud:55,000 Elem:100 Sec: 20	50%	50%	Nil	Combined Teachers & IT staff	Central IT staff	Some Elem - partial coverage. Second - full coverage	Thick APs 802.11b and 802.11b/g	Encrypted. Controlled Guess Access	District. Started as 8 school pilot program	Yes. Measure support calls, connections, ease of use
Quesnel	28	Stud: 4,100 Elem: 14 Sec: 3	Nil	100%	Nil	Centralized	Central IT staff	All schools. Limited coverage	Sonicpoint APs 802.11g	Firewall controllers WPA keys	District staff	Yes.
Campbell River	72	Stud: 5,000 Elem: 15 Middle: 3 Second: 2	5%	70%	25% Linux	Combined Central and school based techs	Combined Central and school based techs	All middle & high done. Elem to start Fall 2007	3Com thin APs. 802.11g	WPA and AES	District, with schools push	Yes. Measure connectivity and support ability
Central Okanagan	23	Stud: 22,180 Elem: 29 Middle: 6 Second: 5	3%	97%	Nil	Centralized	Centralized	5 Elem All Middle Second over next 2 years	Cisco 1131 thick AP with PoE & WLSE engine 802.11a/g	WPA-PSK using TKIP or AES encryption	District	Yes. Student and parent satisfaction. Student achievement
Okanagan Skaha	67	Stud: 6,725 Elem: 11 Middle: 4 Second: 3	Nil	100%	Nil	Centralized	Centralized	All sites	Cisco thin APs. 802.11b/g	Authen, certif, MAC add, ACS, NAC, firewall	District	Yes. Anecdotal evidence
Coquitlam	43	Stud: 30,500 Elem: 45 Middle: 13 Second: 8	10%	90%	Nil	Combined Central and school based techs	Combined Central and school based techs	Elem and middle done. All second done by 2008	D-Link. Cisco thin APs in Second & Dist Ofcs 802.11b/g	Certif, user auth, WPA	Combined effort	Yes. Anecdotal feedback, demand, expectations
Nisga'a	92	Stud: 575 Elem: 4 Second: 1	65%	33%	2%	Centralized	Centralized	All sites	Apple Airport APs	MAC address, managed logins	District	Mixed, leaning to Yes.

## SD72 Campbell River

### Primary Technology Contact

*Geoff Wilson 250-830-2320 [geoff.wilson@sd72.bc.ca](mailto:geoff.wilson@sd72.bc.ca)*

District Student Population (Ministry FTE from Sept 2006) 5,000

Number of Schools:  
*Elementary - 15  
Middle - 3  
Secondary - 2*

Computer Technology by %:  
*Apple – 5%  
PC – 70%  
Other (Linux) – 25%*

### Technology Support Model

*1 manager of IT, 1 lead hand IT, 1 developer, 2 school based techs middle/high, 1 school based tech elementary, 1 tech helper.*

### Network Support Model

*1 manager of IT and 1 lead hand IT are primary support; IT technicians are partners in this support.*

### WAN Connections

*All in-town sites linked by 100MB fibre optic connection. Upstream PLNet connection leaving Campbell River to Nanaimo is 100MB.*

### Wireless Technology Model

*Centralized software controlling managed switches and managed access points. We have selected 3COM as the single vendor. District- wide deployment near completion for middle/high; elementary deployment to commence Oct. 2007 and be complete by Dec. 2007. It is used by any staff and students, and often by guests.*

### Network Technology Specifics

*All AP's are thin and use POE switches. High/Middle/board office use 3COM WX1200 wireless switches with AP2750 maps. Elementary use 3COM WXR100 wireless switch and AP2750 maps. Every switch and map is centrally managed by 3COM wireless switch manager software, which is client - server based. All wired and wireless network is part of the same layer 2 VLAN and fully routable.*

## **SD72 Campbell River, Continued**

### Wireless Devices, Protocols, and Speeds

*Primarily Window- based laptops using 802.11g and WPA. We are consistently getting around 20MB/s throughput. Is this acceptable to users? Users don't understand the limitations, and don't care to either. So we just tell them "that is the way it is".*

### Wireless Security Specifics

*We are using WPA and AES. This will not support older devices, so this summer we will be regressing to WEP and TKIP to support the legacy devices.*

### Other Questions

How did the wireless initiative get started in your district?

*It was initiated by need, as the schools thought they would just go down to London Drugs or Staples and buy a consumer-grade router. IT worked very hard to inform management about the problems associated with this model, and won approval for a district- wide, centrally managed solution.*

Why is wireless a necessary technology direction for schools and districts? Under what circumstances?

*Laptops, laptops, laptops.*

What are the future plans for wireless networks in your district?

*Completion of elementary roll-out. Would like to work towards 802.1x authentication.*

Do you consider the wireless implementation a success? What measurements are you using to determine the level of use or success?

*Yes; users can connect, we can support it.*

Do you have any advice for other districts considering wireless technology?

*Stay away from the idea of a consumer-grade router on top of a laptop cart. Cheaper is NOT better. If you really want a supportable solution, be prepared to pay for it and select a single vendor, central solution such as Cisco, Nortel, 3COM, etc. Legions of D-Link, Linksys, etc. will end up sinking you.*

## SD23 Central Okanagan

### Primary Technology Contact

*Jon Rever 250-860-9729 ext. 4103 jrever@sd23.bc.ca*

District Student Population (Ministry FTE from Sept 2006) 22,180

Number of Schools:

<i>Elementary</i>	<i>29</i>
<i>Middle</i>	<i>6</i>
<i>Secondary</i>	<i>5</i>

Computer Technology by %:

<i>Apple</i>	<i>3</i>
<i>PC</i>	<i>97</i>

### Technology Support Model:

*Centralized support for technology through the Learning Technology Department. Twelve fields techs, 1 Help Desk, 1 e-mail admin / programmer, 1 coordinator, 3 co-op students.*

### Network Support Model

*Same as above.*

### WAN Connections

*Hollywood Road Data Center – 100 Mbps  
Secondary and Middle schools, SBO, Operations – 10 Mbps  
Elementary Schools – ADSL 1.5Mbps down / .5Mbps up*

### Wireless Technology model

*Cisco wireless infrastructure implemented at all iLearn (student laptop initiative) sites. Currently at all Middle schools and five elementary schools. Will be implemented in all Secondary schools over the next year or two. Wireless network is monitored and supported by the Learning Technology Department. Currently used by all Grades 7 and 8 students and teachers. Grade 9 students will be using in fall / 07. All Grade 7 to 12 students and teachers will be using wireless by fall 2010.*

### Network Technology Specifics:

*Generally, we use 1 Cisco 1131 Access Point per classroom, which is plugged into an existing Ethernet jack in each classroom. We currently have 322 wireless access points installed. Wireless network is on a private network which is routed through a server at each school and out through the PLNet router to the WAN. AP's are thick and powered by Cisco 3560 PoE switches or PoE injectors. Wireless network is centrally managed through a WLSE (wireless LAN solution engine) server.*

## **SD23 Central Okanagan, continued**

### Wireless Devices, Protocols and Speeds

*Only laptops are connecting to the wireless network. Currently around 3,000 wireless laptops being used and another 2,000 will be added to the network by the fall of 2007. Protocols being used are 802.11a and 802.11g. Speeds start at 54Mbps and go down based on number on computers per wireless access point. We've had up to 35 laptops on one wireless access point at the same time without complaints about speed.*

### Wireless Security Specifics

*We use Cisco Security Agent (CSA), Netsweeper and Deepfreeze on all iLearn laptops. Traffic is monitored and web access is filtered both at school and at home. Clients are not authenticated to the wireless network but we are using a WPA-PSK pre-shared key using TKIP or AES encryption.*

### Other Questions

How did the wireless initiative get started in your district?

*It was a district initiative.*

Why is wireless a necessary technology direction for schools and districts?

*To enhance and support the teaching and learning process and to allow better access to learning resources.*

What are the future plans for wireless networks in your district?

*All middle and secondary schools and district offices.*

Do you consider the wireless implementation a success? What measurements are you using to determine the level of use or success?

*Yes, based on student and parent satisfaction and student achievement.*

Do you have any advice for other districts considering wireless technology?

*Visit a school or classroom that is using it for student learning.*

## SD43 Coquitlam

### Primary Technology

*Brian Kuhn, 604-939-2901, bkuhn@sd43.bc.ca*

District Student Population (Ministry FTE from Sept 2006) *30,500*

Number of Schools:                      *Elementary – 45 as of Jul/1/07*  
*Middle - 13*  
*Secondary - 8*

Computer Technology by %:              *Apple - 10*  
*PC - 90*

### Technology Support Model:

*10 IT (secondary school, curriculum centre, board office)*

- a. 6 IT (“zone” – middle/elementary)*
- b. 4 team leaders*
- c. 1 supervisor*
- d. 2 web technologists*
- e. 2 BCeSIS technologists*
- f. 1 IT (assistive / adaptive)*
- g. 1 permanent relief*
- h. 2 service desk*

### Network Support Model

*One team leader (security & networks)*

*Individual ITs at sites support what is designed / delivered and participate in design and, implementation*

### WAN Connections

*Mostly ADSL for middle, elementary, E10 for half middles, all secondary, E100 for curriculum centre, board office*

### Wireless Technology Model

*District-wide, consumer-grade devices supplied by district with common SSID*

*Enterprise sol’n is controller based (Cisco) and in three secondary schools, board office (not necessarily full coverage).*

*Summer 2007 will implement ent. Sol’n in five more secondary plus curriculum centre (not full coverage yet.)*

## **SD43 Coquitlam, continued**

### Network Technology Specifics

*Consumer-grade units are D-Link. Enterprise-grade are Cisco light-weight PoE AP's managed by controller at site. Centralized console to view / manage all controllers.*

### Wireless Devices, Protocols, and Speeds

*Mostly "g" devices (some are PDA's on "b")*

*Currently, around 1,000 devices district-wide*

*Speed is dependent on single / location in building etc. – consumer-grade devices are poor and very poor when concentrations of devices occur*

*Speed for Cisco system is very good and high concentration of devices works well – coverage is good*

### Wireless Security Specifics

*Used by staff and students and based on computer in our AD and user authenticated via AD already*

*Push config via Group Policy to computers that are authorized (basically any district-owned laptop)*

*Filter on security group for users (basically by default all staff and students but can be excluded as needed)*

*Allow privately owned computers (second SSID with AD authentication)*

*Allow guest (third SSID with simple 24h authentication)*

*Enterprise: District clients are machine authenticated (certificate pushed via AD)*

*Private clients are user authenticated*

*Uses WPA*

*Consumer: Simple WPA-2 PSK key*

*No proactive monitoring. No quarantine in place. No known security issues to date*

### Other Questions

How did the wireless initiative get started in your district?

*It was a combination of individuals, schools, and district staff.*

Why is wireless a necessary technology direction for schools and districts? Under what circumstances?

*The move to mobile computing is ubiquitous – this is the future of computing in education – it is imperative to have good reliable wireless infrastructure in schools*

## **SD43 Coquitlam, continued**

What are the future plans for wireless networks in your district?

*Ubiquitous enterprise, full coverage*

*Fill-in density as device count increases*

*No structural budget / project yet – piecemeal so far focus on secondary then middle then elementary*

Do you consider the wireless implementation a success? What measurements are you using to determine the level of use or success?

*Absolutely – the user experience for enterprise is very good overall (anecdotal feedback)*

*Demand is increasing constantly*

*People expect wireless in buildings now and question why it's not there – this is good*

*In-service sessions with teachers and administrators are 50 % (or more) laptop-based in many cases – wireless is expected*

Do you have any advice for other districts considering wireless technology?

*Go with a solid enterprise solution from a vendor with a solid networking reputation*

*Just do it!*

## SD92 Nisga'a

### Primary Technology Contact

*Robert J. Wahl, District Principal, Education Technology  
Phone 250-633-2937 Fax 250-633-2333*

District Student Population (Ministry FTE from Sept 2006) 575

Number of Schools: *Elementary 4  
Secondary 1*

Computer Technology by %: *Apple 65%  
PC 33%  
Other (Linux) 2%*

### Technology Support Model:

*Support is centralized to permit technicians to specialize and function as a team. Network is monitored, trouble calls result in best option dispatch. No special status by usage type. Technicians and administrators may have roles in other departments. 1.0 FTE Apple Repair/Laptop Tech 1.0 FTE Network Services Engineer, 0.8 Workstation Support, Help Desk, and Media Production, 0.4 FTE BceSIS/0.4 FTE Admin Support. Admin—  
Total approximately 4.6 FTE among five people for on-site. Teachers/Principals not used for technical support.*

### Network Support Model

*Schools on fibre backbone supplied by local ISP. PLNet routes all traffic through central district firewall. Networking services supplied by about 10 major Linux (Debian) servers, one per school/office and five in DMZ. Mandatory proxy. Additional buildings wireless. Ubiquitous wireless in all buildings. One-thousand network attached devices.*

### WAN Connections

*10Mb bandwidth between schools and to PLNet. 100 Mb from network centre to ISP core.*

### Wireless Technology Model:

*Wireless networking assigned to one primary technician. Managed POE hubs, custom ethernet cabling to Apple Airport Basestation A/Ps.  
Central monitoring and dispatch, POE hubs permit re-boot.*

## **SD92 Nisga'a**, continued

### Network Technology Specifics

*AP's are Apple Airport / Thin or transparent.*

*Servers/Firewall are DELL/Debian*

*Switches and Hubs, no standard, currently using Actin POE, Cisco and 3com.*

*Directory Services: LDAP/Open Directory*

### Wireless Devices, Protocols, and Speeds

*802.11b/g, 55Mb per station means about 2Mb per user and this seems fine.*

### Wireless Security Specifics

*We use MAC address filtering and managed logon privilege. All users have own accounts, which are required to get past firewall. We'd like to improve but we have reasonable security.*

### Other Questions

How did the wireless initiative get started in your district?

*We built a link from computers to literacy. There's more money in literacy than in computers. Superintendent was supportive and management was able to convince the board.*

Why is wireless a necessary technology direction for schools and districts? Under what circumstances?

*Wireless technology is fundamental to the one-to-one philosophy. We want to build student-centred learning. I don't think it's normal for laptop computers to be stand alones. They are portable, personal and connected.*

What are the future plans for wireless networks in your district?

*We've pretty much done all that can be done for now. We're working on adding online services and training users and teachers in integrating technology into instruction.*

Do you consider the wireless implementation a success? What measurements are you using to determine the level of use or success?

*Depends how you measure success. We are neither a success or a failure, but we continue to expect and see positive results.*

Do you have any advice for other districts considering wireless technology?

*Don't go ad-hoc. Work up a comprehensive plan and than do it all at once. If that's too much, minimally do a whole school at once. Be ready for a shakedown period of about six months.*

## SD67 Okanagan Skaha

### Primary Technology Contact

*Ron Shongrunden, 250-770-7705, [rs@summer.com](mailto:rs@summer.com)*

District Student Population (Ministry FTE from Sept 2006) 6,725

Number of Schools:  
*Elementary 11  
Middle 4  
Secondary 3*

Computer Technology by %:  
*Apple 0%  
PC 100%*

### Technology Support Model:

*Presently have three but will have four CUPE district technicians. One IT excluded manager. District technology is 100% centralized.*

### Network Support Model

*Included in technicians' duties listed above.*

### WAN Connections

*PLNet and Telco connections to the outside - network is run internally on dark fiber at gigabit speeds.*

### Wireless Technology model:

*Centrally managed wireless mesh in all buildings indoors and outdoor pilot for full city-wide coverage next year. Available to all staff, students and public.*

### Network Technology Specifics :

*Cisco centrally managed WISM blades in 6509 chassis switches, PoE thin access points, fiber backhaul. PLNet not involved.*

### Wireless Devices, Protocols, and Speeds

*Devices connected include laptops, video projectors, VoIP phones and cameras. Quantity in the hundreds. Mostly 802.11 b/g. Speed similar to cable modem or DSL which is acceptable for most tasks, but not for video high-density situations.*

### Wireless Security Specifics

*Various layers including passwords, certificates, WPA, MAC addresses, Cisco ACS and NAC, and firewalls.*

## **SD67 Okanagan Skaha, continued**

### Other Questions

How did the wireless initiative get started in your district?

*District initiative*

Why is wireless a necessary technology direction for schools and districts?

*Learning anywhere, anytime. Provides operational and infrastructure cost savings.  
Potential for revenue generation related to providing services to users outside the district.*

What are the future plans for wireless networks in your district?

*Completion of Okanagan Valley network*

Do you consider the wireless implementation a success?

*Yes. Not scientifically proven (anecdotal evidence)*

Do you have any advice for other districts considering wireless technology?

*Nothing ever works as advertised.*

## SD 28 Quesnel

### Primary Technology Contact

*Mark Ekelund 250-992-8802 markekelund@sd28.bc.ca*

District Student Population (Ministry FTE from Sept 2006) 4,100

Number of Schools: *Elementary 14  
Secondary 3*

Computer Technology by %: *Apple 0%  
PC 100%*

### Technology Support Model:

*Centralized support and purchasing with one technology coordinator and four technicians.*

### Network Support Model

*Included in the above duties.*

### WAN Connections

*Wireless connections to all schools, ranging from three MB shared between three elementary to 24 MB to a secondary school.*

### Wireless Technology model:

*Each school has a firewall which also controls the wireless access points. Management of both firewalls and access points is done centrally at the district office. Wireless coverage will completely cover all schools within the next year. Usage is quite limited at this point, with a small number of laptops in each school or used by district staff. We have no 1:1 laptop projects. Laptops tend to be used for staff, mobile presentations and special education students.*

### Network Technology Specifics:

*Firewalls are Sonicwall, wireless access points are Sonicpoint. One Firewall/AP controller per school. APs are connected to a separate segment/IP network; traffic between wired and wireless network is routed through SonicWall. APs are configured as thin devices, and do not use PoE.*

### Wireless Devices, Protocols, and Speeds

*Laptops are 802.11 g (54 MB) and speed is not a problem.*

## **SD 28 Quesnel**, continued

### Wireless Security Specifics

*Security set-up is district-wide so a laptop (or a user) set up for one location can log in at any location. Firewalls have a separate network segment for wireless devices, which is separated from wired devices within the school. Wireless security is provided by pre-shared WPA keys - future possibilities include a RADIUS server tied to our LDAP backend.*

*We are able to control access to network on a per-user basis but we cannot control access to the Internet on a per-user basis. That would be a useful improvement.*

### Other Questions

How did the wireless initiative get started in your district?

*Planned and implemented by district technology staff.*

Why is wireless a necessary technology direction for schools and districts? Under what circumstances?

*Laptops are very convenient for many users and purchase price is becoming comparable to desktop systems. Technicians in the field are able to work more efficiently if they can access the network without having to hunt for a cable.*

What are the future plans for wireless networks in your district?

*Gradual increase in use. No plans for 1:1 projects at this time due to lack of sustainable funding. Possible integration between wireless authentication and our LDAP/Samba user database.*

Do you consider the wireless implementation a success? What measurements are you using to determine the level of use or success?

*Yes, it is successful. Scalability is yet to be determined.*

Do you have any advice for other districts considering wireless technology?

*Carefully consider needs before making first purchases since solutions are often incompatible with each other. This produces vendor 'lock-in' as we all hate to throw everything out and start again.*

## SD36 Surrey

### Primary Technology Contact

Wayne Arseneault 604-590-9348

District Student Population (Ministry FTE from Sept 2006) 55,000

Number of Schools: Elementary - 100  
Secondary - 20

Computer Technology by %: Apple 50%  
PC 50%

### Technology Support Model:

#### *Elementary Schools (including Learning Centres):*

- 1 x designated teacher volunteer who works as Technical Contact.  
They provide varied levels of technology user-level support, depending on individual expertise and experience.  
Act as single contact for school staff and liaison with district IT staff.*
- 6 x Info. Services Technicians IT staff.  
They provide first-level, on-site and remote technology support.*

#### *Secondary Schools (including Continuing Education):*

- 1 x designated teacher volunteer who works as Technical Facilitator.  
They provide varied levels of technology user-level support, depending on individual expertise and experience.  
Act as single contact for school staff and liaison with district IT staff.*
- 4 x Info. Services Technicians IT staff  
They provide first-level, on-site and remote technology support*

#### *Administration Sites:*

- 1 x designated management staff volunteer who works as Technical Facilitator/Contact.  
They provide minimal levels of technology support, depending on individual expertise and experience.  
Act as single contact for school staff and liaison to district IT staff.*
- 4 x Info. Services Technicians IT staff  
They provide first-level, on-site and remote technology support*

### Network Support Model

*Multiple Info. Services technicians IT staff (see above) provide first-level, on site and remote support for wired and wireless networks and WAN connections.  
Two second-level support Lan technicians act as support and troubling-shooting contact for multiple info services technicians for both wired and wireless networks  
One senior-level network technician acts as the PLNet technical contact*

## **SD36 Surrey, continued**

### WAN Connections

*Elementary - ADSL, Secondary - 10Mb, Administration - 10Mb*

### Wireless Technology model:

*Multi generations in use, moving toward district standard:*

*Apple wireless mobile carts*

*Primarily utilized in elementary schools*

*Usually 20-30 wireless laptops, 1-3 APs, 1 printer*

*District standard*

*Initial implementation in secondary schools only*

*Fixed thick access points, POE switch*

*Provides 'guest' access*

### Network Technology Specifics:

*Wired: PLNet WAN connection and Router (1/ site)*

*800 switches*

*Fibre Optic vertical wiring (secondary schools) connecting wiring closets.*

*UTP Cat5 vertical wiring (elementary schools) connecting wiring closets  
(if more than one)*

*UTP Cat5 horizontal data wiring (all sites)*

*Wireless: 264 – Intelligent Access Points*

*155 - fixed wireless, PoE Access Points*

*50- PoE switches*

*District managed computers connecting to wireless networks have access via secured connections to the Internet and district services, such as home folders, websites, and district servers.*

### Wireless Devices, Protocols, and Speeds

*Primarily wireless Laptops connect to the wireless network.*

*Approx 4,200 Access points installed*

*Elementary schools have between 1 and 5 mobile carts, with 20-30 laptops per cart.*

*Secondary schools have between 1 and 4 mobile carts, with 20-30 laptops per cart.*

*The wireless connection speed for users can be an issue, as well as the reliability of the wireless networks. The shared medium and cross protocol effect on access points along with channel interference can cause speed acceptability issues for users.*

## **SD36 Surrey, continued**

### Wireless Security Specifics

*Specifics removed at District request. See district contact for more details.*

*Guest wireless network connections are limited to Internet access and authorized district services that are available from the Internet.*

*Wireless Security controllers are configurable to allow or disallow specific wireless network access.*

*Sources of problems include frequency over crowding, interference by other devices, client configuration issues, network configuration and reliability, rogue devices, and security.*

### Other Questions

How did the wireless initiative get started in your district?

*District initiated via Curriculum Instructional Services Center initiative – eight schools each received a single Apple 10 unit mobile lab as part of a pilot project .*

Why is wireless a necessary technology direction for schools and districts? Under what circumstances?

*Primarily to provide for the integration of technologies into the classroom*

What are the future plans for wireless networks in your district?

*Complete wireless coverage at all sites*

Do you consider the wireless implementation a success? What measurements are you using to determine the level of use or success?

*Yes. Implementation in full campus deployments is considered a success.*

*We have confirmed numerous client connections daily with few support calls. Mobile carts at these sites are able to roam without having to trouble shoot access point issues as no access points are located on the carts. All access points are statically configured and placed strategically in the ceiling. Client connectivity is configured via preset standard so very few support calls relating to client configuration issues are logged . The wireless network coverage on full campus installations are surveyed to paint the entire school or site and to date we have not had any calls relating to coverage issues.*

*Network reliability is a success based on the number of user connections and limited call volume related to full campus installations.*

*Ease of use: No client configuration for district managed devices in these sites is required.*

## **SD36 Surrey**, continued

Do you have any advice for other districts considering wireless technology?

*Compare the reliability, manageability, and operation costs of thin AP technology being used in Enterprise environments today. Also, explore the possibility of two or three radio access point technology. The cost of this newer technology may appear higher but, in the long term, operations, management and reliability for the users may offset the higher cost. The wireless network connection speeds are increasing and new standards are being developed. Keep a close eye on the up and coming 'to be ratified' standards that will take wireless networks to a new era in networking.*

## Glossary of Terms

Technology documentation and articles are littered with specialized words and acronyms that are completely foreign to the average person. This glossary attempts to define some of the terms that you may encounter in this and other readings on networks and wireless. An excellent online source of assistance can be found at [www.wikipedia.org](http://www.wikipedia.org).

802.11a – IEEE standard with maximum speed of about 54 Mbps, running in the 5GHz range. This standard is less prone to interference, but has a shorter range and requires more APs to cover the same area as 802.11b/g. Not backward compatible with 802.11b/g.

802.11b – IEEE standard with maximum speed of about 11 Mbps, running in the 2.4 GHz range. This standard has a theoretical range of approximately 100 meters indoors and 300 meters outdoors. Prone to interference from some cordless phones and microwaves.

802.11g – IEEE standard with higher transmission speed of 54 Mbps, but operating in the 2.4 GHz range. Backwards compatible with 802.11b, with the same distance range and risk of interference.

802.11i – IEEE wireless security standard with much stronger encryption and authentication mechanisms than the initial standards.

802.1x – See EAP

Access Point or AP – a hardware device which provides wireless connections to a wired LAN. Each device contains one or more antenna which sends and receives signals from one or more compatible wireless stations (laptop, PDA)

Ad-hoc network – common term for a peer-to-peer connection between two or more devices where they communicate without the benefit of a network controller, server, or intelligent access point. Typically very insecure environment, and often the default network setting for wireless laptop devices.

AES – Advanced Encryption Standard – newest security protocol (802.11i) for encryption of wireless data.

Bluetooth – short-range wireless technology using radio waves to transmit data up to 10 meters, through walls, pockets, and briefcases. Usually seen in cell phones and PDAs.

Controller – a device which manages and controls authentication, access, security, and performance of a wireless network.

EAP – Extensible Authentication Protocol - also known as standard 802.1x

Ethernet – a large, diverse family of frame-based computer networking technologies that operates at many speeds for local area networks (LANs). The name comes from the physical concept of the ether. It defines a number of wiring and signaling standards for the physical layer, through means of network access at the Media Access Control (MAC)/Data Link Layer, and a common addressing format. The combination of the twisted pair versions of Ethernet for connecting end systems to the network, along with the fibre optic versions for site backbones, has become the most widespread wired LAN technology. It has been in use from the 1990s to the present, largely replacing competing LAN standards such as coaxial cable Ethernet, token ring, FDDI, and ARCNET.

Firewall - a firewall's basic task is to transfer traffic between computer networks of different trust levels. Typical examples are the Internet which is a zone with no trust and an internal network which is a zone of higher trust. A zone with an intermediate trust level, situated between the Internet and a trusted internal network, is often referred to as a "perimeter network" or Demilitarized zone (DMZ).

GHz or Gigahertz – the frequency band for wireless data transfer. Two common standards for WLAN technologies are 2.4 and 5 GHz bands.

Hub - a device for connecting multiple twisted pair or fibre optic Ethernet devices together, making them act as a single segment. Hubs work at the physical layer (layer 1) of the OSI model. The device is thus a form of multiport repeater.

Intelligent or Fat AP – access point with security and limited management capability in the unit itself. Most often used in ad-hoc or small group wireless networks, or where centralized controllers are not available/necessary.

Mbps – Megabits per second – a measurement of the number of bits (0 or 1) transmitted over a wireless frequency or wired connection. A megabit is one million bits, or approximately 100,000 characters of information.

MAC – Media Access Code – the unique address that identifies a device's network adapter. Can be used to restrict access to wireless networks based on only recognized MAC addresses.

PoE – Power over Ethernet - a system to transmit electrical power, along with data, to remote devices over standard twisted-pair cable in an Ethernet network. This technology is useful for powering IP telephones, wireless LAN access points, webcams, Ethernet hubs, embedded computers, and other appliances where it would be inconvenient, expensive (mains wiring must often be done by qualified and/or licensed electricians for legal or insurance reasons) or infeasible to supply power separately.

Router - a junction between two or more networks to buffer and transfer data packets among them. Wikipedia has an excellent 'street analogy' which explains the relationships between routers, switches and hubs.

SSID – Service Set Identifiers – a group name or identifier for authorized connections to a wireless network.

Switch – a data link layer networking device. Switches perform transparent bridging (connection of multiple network segments with forwarding based on MAC addresses). Typical port speeds on an Ethernet switch are 10, 100, 1000 or 10000 megabits per second (Mbit/s), and half or full-duplex.

Thin AP – access point with little or no intelligence in the unit. Unit cost is very low, but requires management and security by a central controller on the network.

TKIP – Temporal Key Integrity Protocol – used by WPA to deter eavesdropping, forgery, and replay of data.

VLAN – Virtual Local Area Network - a method of creating independent logical networks within a physical network. Several VLANs can co-exist within such a network. This helps in reducing the broadcast domain and aids in network administration by separating logical segments of a LAN (like company departments) that should not exchange data using a LAN (they still can exchange data by routing).

VPN – Virtual Private Network - a private communications network often used by companies or organizations, to communicate confidentially over a public network.

WEP – Wired Equivalent Privacy – encryption system using static keys. Basic security between AP and wireless device, where each side has the same fixed encryption key. Easily cracked and replaced by WPA/WPA2.

Wi-Fi – general industry term for IEEE 802.11 series of standards, and most often 802.11b/g.

WiMAX – general industry term for IEEE 802.16 standards. Broadband wireless service over wide areas and high speeds

WLAN – Wireless local area networks – technologies enabling users to establish wireless connections within a local area. IEEE has approved the 802.11 standard for WLANs, with work continuing on a series of security and bandwidth improvements. These technologies are often referred to as Wi-Fi.

WMAN – Wireless metropolitan area networks – technologies enabling users to establish wireless connections between multiple locations in a metropolitan area, such as multiple office buildings, campus locations, etc). Current technologies use radio wave or infrared light, but carriers are building broadband networks to service this growing demand.

WPA – Wi-Fi Protected Access – improved encryption system using dynamic keys. Better and newer than WEP.

WPA2 – Wi-Fi Protected Access 2 - security supported by Wi-Fi devices produced since late 2004, as defined in the 802.11i standard. Uses AES to secure data in a stronger, more efficient manner. Better and newer than WPA.

WPAN – Wireless personal area networks – technologies enabling users to establish ad-hoc, wireless communications for devices (PDAs, cell phones, laptops) that are used within a personal operating space, usually a distance of 10 meters or less. Two current technologies are infrared and Bluetooth.

WWAN – Wireless wide area network – technologies enabling users to establish wireless connections over remote public or private networks, over large geographical areas. Currently telecom providers offer these types of services, based on several second and third generation technologies.

## **Bibliography**

Advances in Wireless LAN Architecture. Ashland, MD: Farpoint Group White Paper 227.1, May 2007.

An Overview of Wireless Technology in the Enterprise. 2007. TechTarget. 10 May 2007. <[http://www.bitpipe.com/data/web/bpmd/wireless/wireless\\_overview.jsp](http://www.bitpipe.com/data/web/bpmd/wireless/wireless_overview.jsp)>.

Davis, Jeff. “Centralized Wireless LAN: Thin vs. Fat Technology”. Cabling Business Magazine. November 2004. p. 14+.

Hill, Gene T. and Miller, Benjamin. Eleven Myths about 802.11 Wi-Fi Networks. Global Knowledge Training LLC. 2006.

IEEE 802.11. 24 June 2007. Wikipedia.org. 25 June 2007. <[http://en.wikipedia.org/wiki/IEEE\\_802.11](http://en.wikipedia.org/wiki/IEEE_802.11)>.

Kirk, Jeremy. Double trouble – ‘Evil twin’ Wi-Fi attacks on the rise. 25 April 2007. IT World Canada. 07 June 2007. <http://www.itworldcanada.com/mobile>.

McKeag, Louise. Access Points – beyond the Thin/Fat spat. 08 April 2004. Techworld. 17 May 2007. <<http://techworld.com/features/index.cfm?featureID=477>>.

Microsoft Windows XP – Wireless networking overview. 2007. Microsoft Corporation. 10 May 2007. <[http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/wireless\\_networking\\_overview.mspx](http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/wireless_networking_overview.mspx)>.

Phifer, Lisa. Five-Step Plan for Securing your Enterprise WLAN. Core Competence Inc. November 2006.

Phifer, Lisa. Wireless Security – Defending Wi-Fi clients. 24 May 2007. TechTarget. 24 May 2007. <<http://searchnetworking.techtarget.com/tip>>.

Wireless Network Security. 10 Sept 2006. Syngress Publishing. 10 May 2007.

# Appendices and References

## PLNet Bulletin: Wireless LAN Access Policy

**DATE: June 17, 2005**

### OBJECTIVE

This bulletin defines the circumstances, terms and conditions by which PLNet clients provide wireless connectivity to PLNet.

### BACKGROUND

This document attempts to outline the basic requirements and security precautions expected of PLNet customers deploying wireless (802.11) access technology. This establishes standards for access to PLNet with this technology. This policy does not apply to dedicated point-to-point wireless solutions.

### GENERAL POLICY

PLNet is part of SPAN/BC. Together they support 2000 educational institutions, 1500 government offices, and 300 other agencies and programs. Security and reliability of the Network is a collective responsibility. No single organization should permit activity that jeopardizes the operations of the Network.

This standard governs the controls that are required when allowing users to connect to the Network wirelessly. This Policy is also recommended for all LAN access regardless of how it is achieved.

### EXISTING SERVICES

Where a PLNet client has an existing wireless network, they must ensure that their existing service meets this updated policy, as soon as practical.

### STANDARDS

1. A secure location is required for the communications equipment and communications server (e.g. no unauthorized access).
2. Logical Controls for wireless LAN access must include a minimum of three (3) of the following:
  - a. Media Access Control (IEEE 802 data link layer) (MAC) address controls
  - b. Hidden Service Set Identifier (SSID)
  - c. Wireless Encryption Protocol (WEP) (minimum) or Wi-fi Protected Access (WPA) (preferred) access control
  - d. LAN authentication using a robust standard such as Kerberos or RADIUS
  - e. Disabling user identifiers after no more than six (6) consecutive unsuccessful password attempts

3. Passwords used shall include common practices to avoid the authentication system being compromised, such as:
  - a. pseudo-random in nature or verified by an automated process designed to counter triviality or repetition
  - b. of sufficient length to avoid brute-force cracking
  - c. changed at least every 40 days
  - d. contain a mixture of characters, both upper and lower case, numbers, punctuation, and special symbols
  - e. not be a dictionary word
  
4. Local Administrative policy shall specify those individuals who are authorized to perform security functions for the management of the wireless service, such as resetting passwords, providing security guidance and advice for users.  
Internal audit procedures, such as all changes being clearly documented, ensure administration functions and help identify security problem sources.

## **INDEMNITY**

Nothing in this document should be taken as a recommendation as to the suitability or security of wireless services. Furthermore, the PLNet client agrees to indemnify PLNet, the Province, its employees and agents against all claims, demands, losses, damages, costs and expenses made against or incurred, suffered, or sustained by the Province arising out of connections provided locally and agrees that in no event will the Province be liable for any damages, including but not limited to any incidental, special or consequential damages, arising out of or in connection with the use or inability to use these services.

The PLNet Helpdesk will not be responsible for fielding trouble calls regarding end users accessing VPN, or wireless LAN access provided locally.

In the event of a security incident, the PLNet Helpdesk will advise the customer as soon as practical. The PLNet site should remove the equipment that is the source of the incident until the problem can be remedied. If there is an imminent security threat, CITS Network Operations has been authorized to block access from the offending IP address or from that entire site depending on the nature of the threat. Such blocking may occur prior to contacting the site.

**Responsibility Centre: PLNet**

**FOR MORE INFORMATION CONTACT: PLNet Help Desk 1-888-769-5678 or  
send an email to [plnetbc@eds.com](mailto:plnetbc@eds.com)**