MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

Technology in Schools

School Wireless LAN Guidelines – Building and Maintaining a Wireless Network

Version 1.2

May 2015

Document Information

Acknowledgements

The Ministry of Education, New Zealand, acknowledges with thanks the assistance and contribution of a number of organisations, institutions, statutory bodies, and individuals in the preparation of these Standards. In particular, the assistance of the following parties is acknowledged:
Torque IP, Connector Systems, Allied Telesis,
New Zealand offices of Ruckus Wireless, Aerohive, Aruba Networks.

Table of Contents

Table of Figures

1 Introduction

This document is part of the Education Infrastructure Services: Technology in Schools, School Wireless LAN Guidelines 2015. It has been prepared by the Ministry of Education for use by New Zealand schools and other organisations, which participate in the design, supply, and implementation of information technology infrastructures for New Zealand schools. The document addresses deployment of wireless access to computer networks in New Zealand schools in a way that is complementary to existing wired infrastructures.

Overall, the Guidelines aim to inform in the following areas:

- What is a Wireless LAN (a brief description)
- How does a WLAN work
- What are the benefits of wireless access
- Current wireless access technology and standards (technical details)
- Security issues, threats, and standards
- Deployment of wireless access (planning, installation and integration and avoiding problems)
- Product and integrator selection

The Guidelines will be updated as standards change. Prior to using this document please confirm that it is the latest version. The latest version of each of the Guidelines documents may be obtained at www.education.govt.nz/ict-standards

1.1 Audience

There are two documents that make up the Guidelines, please see the documentation map below.

This document is the “Building and Maintaining a Wireless Network”. It provides guidance for a school IT support person who is implementing and maintaining a school wireless LAN (WLAN). This document outlines the standards available for building and securing a WLAN, technical considerations for implementation, and requirements for ongoing maintenance.

The other document is the “Understanding Wireless Guide” which introduces the overall concepts of a Wireless LAN, and summarises the content required when commissioning an RFP process.

1.2 Documentation Map

The Education Infrastructure Service: Technology in Schools, School Wireless LAN Guidelines 2015 consists of three documents:

1.2.1 School Wireless LAN Guidelines – Understanding Wireless Guide

Intended to provide guidance to principals, board members and other stakeholders who would like an introduction to the issues around selecting and procuring wireless LAN technology for their school.

1.2.2 School Wireless LAN Guidelines – Building and Maintaining a Wireless Network

This document – described above.

1.2.3 Recommended Specifications for School Wireless LAN Systems

Intended to provide guidance for the selection of wireless network technologies and features.

1.3 Scope

The Schools ICT LAN Infrastructure Standards and Guidelines Project aims to inform schools as they make changes to their Information and Communication Technology (ICT) infrastructure.

In Scope	Outside Scope
Wireless networks supporting learning and research within schools	Community Wireless which might be based around a school
General considerations for wireless network installation	Use of wireless technologies for point to point connections between buildings
Wireless connection between a ‘user device’ and the school network	Detailed connectivity between school LAN and WAN
Additional security required for a school wireless network	General school network security, including firewall configuration and other network issues
	Bandwidth management of external Internet access
	Teaching pedagogy required to make use of an expanded wireless network
	Selection of, and management of, wireless devices, beyond connection to the network
	Detailed specification of a school Wireless Network RFP

2 What are the standards relating to WLANS?

There are two distinct sources of standards that are relevant to a WLAN installation national/international and IEEE.

Various national and international standards are maintained by national standards bodies. New Zealand standards are generally developed is association with Australia, and are referred to as A/NZ standards.

The Institute of Electrical and Electronics Engineers (IEEE) is an international body that, among many other things, creates and maintains the technical standards used in WLANs.

2.1 New Zealand and International Standards

The work covered by this document shall comply with relevant New Zealand and International Standards, Specifications and Technical Bulletins.

For a list of those documents, and details regarding how they should be interpreted and applied, please refer to the Ministry of Education Information and Communications Technology (ICT) Cabling Infrastructure: Policy and Standards for Schools. This is available at www.education.govt.nz/ict-standards

2.2 Ratification and Certification

The standards for 802.11 WLAN are typically developed by IEEE where they move through working groups and are finally ***ratified*** as a standard.

Once a standard is ratified, a manufacturer can submit a device that supports that standard to the Wi-Fi Alliance for ***certification***. The Wi-Fi Alliance is a non-profit organisation that tests manufacturers' 802.11 devices for compliance with the IEEE standards. Devices that pass the compliance test are **certified** and are able to display the Wi-Fi Logo (a registered trademark which can only be displayed on equipment that has been tested and certified).

Most 802.11 manufacturers are members of the Wi-Fi Alliance, but for cost reasons some manufacturers are not. A device that has not been certified may still be compliant with the IEEE standard, but it is highly recommended that schools only purchase certified devices to ensure compatibility and compliance.

2.3 IEEE Wireless LAN Standards

A summary of the current relevant IEEE 802.11 WLAN network standards is tabulated below:

Figure 1 – 802.11 Network Standards, March 2015

802.11 network standards						
Protocol	**Release Date**	**Freq.**	**Bandwidth**	**Maximum Data rate per stream**	**Allowable MIMO streams** (see School Wireless LAN Guidelines – Glossary.).	**Approximate indoor range**
		(GHz)	**(MHz)**	**(Mbit/s)**		**(Metres)**
802.11a	Sep-99	5	20	54	1	35
		3.7				
802.11b **(no longer in common use)**	Sep-99	2.4	20	11	1	35
802.11g	Jun-03	2.4	20	54	1	38
802.11n	Oct-09	2.4/5	20	72.2	4	70
			40	150		70
802.11ac	Dec-13	5	80	433	8	35
			160	Between 1.73 Gbit/s and 6.93 Gbit/s		35

Brief, non-technical, descriptions of these terms are defined in School Wireless LAN Guidelines – Glossary (at the end of this document).
Based on http://en.wikipedia.org/wiki/IEEE_802.11

2.3.1 Description of Current Technologies & Standards

This section describes the standards commonly in use in early 2015. Note that many client devices have multiband wireless hardware that supports combinations such as a/g/n or a/b/g/n/ac.

Further definition of many of the terms used in this section is provided in the glossary.

2.3.1.1 IEEE 802.11a

The 802.11a standard was ratified by the IEEE in 1999 and gradually adopted worldwide. It was slow to become adopted due to cost and shorter-range signals (compared to 802.11b) and was more common in business rather than home environments. 802.11a operates in the 5GHz frequency range, which is less “crowded” than the 2.4GHz frequency range, and so is not as susceptible to interference as 802.11b or 802.11g. 802.11a is now increasingly being replaced with 802.11n and ac.

Advantages (when released) were faster maximum speed and less susceptibility to interference than 802.11b.

Disadvantages were cost, shorter range and signals that were more easily absorbed by objects such as walls (due to 802.11a having higher frequency signals).

2.3.1.2 IEEE 802.11b

The 802.11b standard was also ratified by the IEEE in 1999 and was rapidly adopted worldwide (particularly in home environments) as a result of its low cost. It is now largely obsolete – being replaced by 802.11g,n and ac.

802.11b operates in the unregulated (and somewhat crowded) 2.4MHz band along with other devices including cordless phones, baby monitors, bluetooth devices and microwave ovens – all of which can cause interference. The 2.4GHz band also has few options for channels that do not overlap so interference from other Wireless Access Points (APs) is also common.

Advantages (when released) were low cost, good signal range, and not easily absorbed by walls and other objects (compared to the higher frequency 802.11a).

Disadvantages were slow speed and susceptibility to interference.

2.3.1.3 IEEE 802.11g

The 802.11g standard was ratified in 2003. It was intended to offer the same data rates as 802.11a (54Mbps), whilst working in the same frequency range as 802.11b (2.4GHz) for backwards compatibility and range. While 802.11g is still widely used in wireless equipment, it is rapidly being replaced with 802.11n and ac.

Some low-cost end user devices are still being sold with 802.11g wireless networking only, so backwards compatibility with 802.11g is normally a requirement for WLAN deployments.

Advantages (when released) were backwards compatibility with the popular 802.11b standard, fast maximum speed, good signal range, and not easily absorbed by obstructions.

Disadvantages are susceptibility to interference (still uses crowded 2.4GHz band) and reduced speed from an AP if older end user devices are also connected to it (e.g. if any 802.11b end user device connects to an 802.11g AP the speed for all 802.11g devices that are connected to that AP is reduced).

2.3.1.4 IEEE 802.11n

Introduced in 2009, 802.11n was intended to improve network throughput over the 802.11a and g standards.

802.11n devices can operate on 2.4GHz, 5GHz, or both frequency ranges.

The 802.11n standard uses additional radio frequency manipulation techniques to extend the usable distance of an AP when compared to earlier standards.

Some lower end 802.11n APs have a single radio that can operate on both the 2.4GHz or 5GHz frequency range (but only one a time) while higher end APs have dual radio which allows them to use both frequency ranges simultaneously (i.e. communicate with a client on 2.4GHz and with a client on 5GHz at the same time).

802.11n further improved on 802.11a and g by introducing MIMO to provide multiple simultaneous radio spatial streams to a single client and thereby increase both signal range and maximum data rates. Up to 4 MIMO streams are supported by the standard, although in practice devices supporting 4 MIMO streams are rare and most devices sold to date support either 2 or 3 streams.

802.11n supports channel bonding in the 5GHz frequency, where two adjacent 20MHz channels are combined to make a single 40MHz channel to increase data rates – at the expense of the number of channels available.

802.11n has a theoretical maximum data rate of 150 Mbps per MIMO stream over a 40MHz channel, so with 4 MIMO streams the maximum data rate is 600 Mbps. A realistic actual data rate that could be expected on an 802.11n wireless LAN is approximately half of that (i.e. 300 Mbps).

Advantages (when released) were fastest maximum speed, best signal range, and least susceptibility to interference.

The major disadvantage (when released) was higher cost than 802.11g

2.3.1.5 IEEE 802.11ac

IEEE ratified 802.11ac in December 2013.

Wave 1 and Wave 2

At the time 802.11ac was ratified, most vendors had products that supported the mandatory features of 802.11ac, but very few chipsets were available for the optional advanced features (particularly multiple-user MIMO, 160MHz channel bonding and 4 MIMO streams per channel).

As a result, most 802.11ac devices to date have been Wi-Fi Alliance certified for the mandatory features only and they are known as Wave 1 devices. Devices that are certified with the advanced optional features are known as Wave 2 devices.

At the time of writing the chipsets that support the advanced optional features of Wave 2 have been developed and provided to the mainstream device manufacturers who are building and testing Wave 2 products ready for Wi-Fi Alliance certification. It is expected Wave 2 devices will become readily available in the second half of calendar 2015.

Note that some 802.11ac client devices which have been purchased in the last 12 months will support MU-MIMO via a driver update, but the majority will not.

Almost all high-end smart phones and tablets now ship with 802.11ac Wave 1 wireless capability and the cost of Wave 1 APs, which initially sold at a premium over 802.11n APs, has now tumbled to almost the same cost as 802.11n APs.

Frequency Range

802.11ac only operates in the 5GHz range, although most 802.11ac APs have “dual-band” radios that run simultaneously at both 2.4GHz and 5GHz to allow them to support all earlier standards - so an 802.11ac AP will support 802.11ac features for 802.11ac clients over 5GHz, and 802.11n and 802.11g features are supported on the 2.4GHz radio.

Channel Width and Bonding

802.11ac introduces two new channel sizes: 80MHz (Wave 1) and 160 MHz (Wave 2). As with 802.11n, wider channels increase speed. In some areas, 160MHz of contiguous spectrum will be hard to find, so 802.11ac introduces two forms of 160MHz channels: a single 160MHz block, and an “80+80MHz” channel that combines two non-contiguous 80MHz channels and gives the same capability.

Using 160MHz may be more likely to be used in the home environment where typically only a single AP is used - in school and business environments with multiple APs the small number of non-overlapping 160MHz channels available is likely to lead to interference issues.

MIMO and MU-MIMO

Wave 1 (mandatory 802.11ac) supports single user MIMO, and up to 4 spatial streams of data over the same channel to the same client (as with 802.11n), although most Wave 1 APs (like 802.11n APs) only support 2 or 3 streams.

Wave 2 devices will increase the number of spatial streams over a single channel from 4 to 8 and will add a feature called multi-user MIMO (MU-MIMO) whereby the streams may be to different clients. This means Wave 2 APs will be able to simultaneously communicate with multiple clients at the same time (unlike 802.11n and Wave 1 802.11ac APs which support multiple streams, but only to a single client).

The difference between single user MIMO and MU-MIMO is similar to the difference between a hub and a switch. With the ability to transmit at high speeds to multiple clients simultaneously, 802.11ac will speed up networks even more than might be apparent from simply looking at the data rate and this needs to be considered carefully during network design.

Beamforming

Beamforming was optional in 802.11n with several variants – but the different variants were incompatible with each other and in order to function, each variant needed both the AP and client to have the same variant – and the market never settled on a particular variant. Beamforming is a technique where an AP with multiple antennae increases the signal strength in a specific direction to provide better wireless reception to a wireless station.

Maximum Data Rate

802.11ac has a theoretical maximum data rate of 200 Mbps per MIMO stream over a 40MHz channel, 433 Mbps over an 80MHz channel and 867 Mbps over a 160MHz channel; so with 8 MIMO streams the maximum data rate is 6.93 Gbps.

2.3.2 Multiple Channels in One Area

Each frequency range used by 802.11 wireless (2.4GHz and 5GHz) is split into channels each of which a subset of the frequency range.

To enable the highest device compatibility it is advisable to select the US/Canada Radio Frequency policy on installation of a WLAN system.

2.4GHz Channels

The 2.4GHz band (used in 802.11b, g, and optionally n) is divided into 14 channels. Different countries have different regulations as to what 2.4GHz channels are permitted – NZ allows channels 1 through 13, while the US allows 1 through 11.

The frequency (mid-point) of each 2.4GHz channel is only 5MHz away from the mid-point of the next channel (with the exception of channel 14 which is 12MHz away from channel 13). Since the 802.11b,g and n standards require a 20MHz wide channel, adjacent channels overlap and interfere with each other. There are effectively only three non-overlapping channels (channels 1, 6 and 11) and when wireless is deployed each AP is typically set to one of these 3 channels. Care must be taken to ensure APs set to the same channel do not have overlapping coverage areas or interference will occur (e.g. if two adjacent APs are both set to channel 6 and they have overlapping coverage areas, interference will occur potentially causing poor reception and slow performance).

Since there are only 3 non-overlapping channels to choose from, 2.4GHz wireless design can be challenging.

Note that a school may carefully design and deploy a wireless network that minimises overlapping channels, but then have another user or organisation close by deploy APs that use the same channels that then cause interference. This may require changes to be made to the channels used by the school.

5GHz Channels

The 5GHz band (used in 802.11a, n and ac) has far more channels specified in the IEEE standards, but again the channels permitted vary by country. Typically there are 8 non-overlapping 20MHz channels available.

The 5GHz channels that are permitted in most countries are typically 20MHz apart so there is no channel overlap if 20MHz MIMO spatial streams are used, but if channel bonding is used for a higher speed a 40MHz, 80MHz or 160MHz channel would be needed so there may be issues with channel overlap. This becomes a significant design consideration.

NZ and the USA allow channels 36 through 64 and 149 through 165

2.3.3 Wireless Standards and Performance

In order to maintain optimum wireless speed for client devices, 802.11ac Wave 1 with Wi-Fi Protected Access version 2 (WPA2) should be the minimum standard for all new APs. The AP should also support 802.11n (both 2.4GHz and 5GHz).

Devices using older wireless standards, such as 802.11g, can connect to an 802.11n compatible AP, however when a slower device (which might be a device using an older standard, or be further from the AP, or be behind a wall) is using the network, all other devices are forced to wait for it. This wait time is in the order of tens of milliseconds and, over time, it can cause a significant delay to other network users.

In a similar way, the 802.11n standard dictates that devices using WEP or WPA (not WPA2) encryption are only allowed to connect at 54Mbps. Note that as well as having speed limitations, WEP and WPA are not recommended choices from a security perspective (refer section 3.1.6 Encryption Techniques), and it is recommended they be avoided.

Handling of slow devices should be addressed during the planning process for a school wireless network environment.

2.3.4 MIMO

MIMO (multiple-input and multiple-output) is a technique that uses multiple antennae and radios in wireless devices to exploit multipath propagation so that multiple wireless data streams can be sent/received simultaneously over a single channel.

MIMO capable APs have a descriptor (mode) that designates the number of transmit and receive antennae and the number of data streams it is capable of supporting. The mode is denoted as:

Nt x Nr: Ns

where Nt is the number of transmit antennas, Nr is the number of receive antennas and Ns represents the number of transmitted data streams.

Common combinations of MIMO mode are:

2x2:2

2x3:2

3x3:2

3x3:3

Up to 4x4:4

MIMO was first introduced in 802.11n which defines single-user MIMO whereby up to 4 spatial streams of data can be sent over the same channel to the same client. Each stream requires a separate antenna in the sending and receiving device and, because of the cost and physical space required for each antenna, most 802.11n APs only support either 2 or 3 streams. Almost all tablets and smart phones only support 1 or 2 streams, and almost all laptops support a maximum of 3 streams, so the extra cost for 4 stream devices is seldom justified, as the 4th stream is typically never used.

Wave 1 802.11ac also provides for up to 4 single user MIMO streams and virtually all Wave 1 APs support a maximum of either 2 or 3 streams only for the same reasons outlined above.

Wave 2 802.11ac optionally increases the number of spatial streams over a single channel from 4 to 8 and adds an optional feature called multi-user MIMO (MU-MIMO) where the streams over a single channel may be to different clients. This means Wave 2 APs will be able to simultaneously communicate with multiple clients at the same time – for example an 8 stream AP could communicate simultaneously with 4 different smart phones that each support 1 stream and 2 tablets that each support 2 streams.

While it is typically not cost effective to buy an 802.11n or 802.11ac Wave 1 AP that supports more than 3 streams (since they only support single user MIMO and virtually no mobile client devices support more than 3 streams) the same does not apply to Wave 2 APs as the extra streams can communicate with other devices.

A Wave 2 AP effectively acts like a switch rather than a hub, and the significant additional data transfer rates this potentially allows requires careful network design.

2.3.5 Multiple Radio Access Points

APs can come with either single radio or dual radio hardware.

Some single radio APs only support a single frequency range (2.4GHz or 5GHz) while others can support both frequency ranges, but they can only operate on one frequency range at any one time.

Dual radio APs are able to operate on both frequency ranges simultaneously.

Dual radio APs are more expensive, but are now more commonly deployed because of their greater versatility.

When a solution has dual radio access points i.e. one radio operating in the 2.4GHz spectrum and one in the 5GHz it may also offer band steering as an efficient way of ensuring client devices are connected to the most suitable radio. See Glossary below for further reading.

3 Security and Access Management

Network security is critical to the reliable and safe functioning of a wireless network. Steps must be taken to secure each device on the network, as well as securing the 'edge' where the internal network connects with other networks, such as the Internet.

The depth of security necessary in a school environment will vary, depending on the size of the school, and the way in which it uses its network.

This document uses the term security to cover the technical implications of a range of physical and logical security options. Access management is often described in terms of Authentication, Authorisation and Accounting (AAA). AAA security is described in the glossary below for further reading.

Security concepts are critical in defining the objectives of a wireless deployment project. Security and access management need to be considered at all stages of the project. Once the network is running, it should be monitored on an ongoing basis to detect and mitigate security and access risks.

3.1.1 Key Security Concepts

In a school network, security should be applied to all APs. For most schools, configuration should be completed on a Wireless Network Management System (WNMS) and/or Controller (see section 5.1 below) which then propagates that configuration to the APs.

3.1.2 Device or User Authentication

Some authentication techniques authenticate the user of a device; others authenticate the device itself, regardless of who is using it.

Device authentication is simple to configure on a wireless network and, when used with WPA2 (see below), can provide sufficient security for a school that tightly controls the specific wireless devices that are allowed to connect, such as limiting use to school-owned devices.

A school that anticipates widespread wireless use (such as BYOD) should consider user authentication rather than device authentication. This is usually provided using the 802.1X protocol or via a Captive Web Portal.

These authentication methods use a database of authorised users (such as a school's existing directory service). The person connecting to the wireless network will enter their username and password to verify their identity.

Some vendors have additional methods of authentication based on the current standards such as Unique Per User Pre-Shared Keys.

3.1.3 MAC address filtering

A common technique used to authenticate a device is to use the device's Media Access Control (MAC) address. If the device attempting to connect to the WLAN has a MAC address that matches one of the allowable addresses then it is allowed to connect.

MAC address authentication is not a recommended access method (unless combined with other authentication techniques) for the following reasons:

- While the MAC address is, in theory, unique to each device, in most wireless devices the MAC address can easily be 'spoofed', or changed. This makes it very unreliable for identification.

- MAC address authentication adds an additional overhead by requiring the administration of a database containing the MAC address of every device that is permitted to access the WLAN.

3.1.4 Pre-shared Key or Password

A network can be configured so that devices are prompted to enter a ‘Pre-Shared Key’ (PSK) before being allowed to connect.

This technique works well for small networks or networks where only school staff and school-owned devices are connected. This offers more security than MAC address filtering, but it is easy for a password to be ‘shared’ further than desired. Ideally, the password should be changed regularly, but this can cause issues in securely notifying all users of the new password.

Innovations from some vendors use proprietary techniques to extend this authentication method to provide granular per-user PSK’s in order to provide per-user authentication and authorisation.

Some devices might only be able to use less secure protocols. An example might be a hand-held barcode scanner that communicates over a wireless network and is used for tracking books in a school library. In this case, access should be firewalled to communicating with one application only, with no Internet access. Any device authenticated using a MAC address only should be allowed access to its specific need only, as it is relatively easy to make any wireless device take over a connection set up in this way.

3.1.5 Encryption Techniques

Encryption is important in wireless networks as unencrypted wireless signals can easily be intercepted and ‘read’ by third parties.

Early wireless systems commonly used Wired Equivalent Privacy (WEP). WEP is an encryption method that operates at Layer 2 based on the RC4 Cipher. WEP uses a static key and nowadays tools that can rapidly break (decrypt) the encryption used by WEP are easily obtained on the Internet, making WEP unacceptable for almost all wireless networks.

To overcome the security shortcomings of WEP, Wi-Fi Protected Access (WPA) was introduced in 2004 as an interim snapshot of the IEEE 802.11i security amendment (pending the development of WPA2). WPA only supports RC4 and TKIP dynamic key management and has a number of security vulnerabilities.

WPA2 was introduced in 2004 and provides strong encryption using the Advanced Encryption Standard (AES) using the CCMP encryption method and incorporates the mechanisms defined in the IEEE 802.11i standard. This is the industry accepted best practice for robust wireless security and performance.

WPA2 is provided in two modes. WPA2-Personal is based on Pre Shared Key passphrase authentication and WPA2-Enterprise mandates the use of 802.1X authentication with mutual validation.

NB. In addition to being well out of date, and providing low security, using WEP or WPA will limit the throughput of a wireless network. Both should be avoided.

3.1.6 WPA2 Authentication

WPA2 Personal

WPA2 Personal uses a PSK passphrase to provide authentication and authorisation. PSK authentication, described in 0, works well for a home and some small school networks, but managing the shared key is difficult when there are many users.

WPA2 Enterprise

WPA2 Enterprise mandates the use of mutual user authentication and authorisation via 802.1X/EAP (Extensible Authentication Protocol) and while more complex to initially set up, this is the recommended approach for medium and large sized schools.

802.1X is a port based access control standard that restricts access to network resources until user authorisation has been completed.

There are various components to this framework, including the client device (Supplicant), Authenticator (AP) and Authentication Server (RADIUS server).

There are a variety of EAP methods, which can be confusing, and it should be noted that a number are proprietary to certain vendors.

The major factor to consider in selecting the appropriate method is that the method used on the client device (supplicant) and the Authentication Server (AS) must be the same.

For example Microsoft Windows XP/Vista/Win7/Win8 support EAP-TLS, PEAP-TLS /MS-CHAP and are widely used for this reason.

The difference between TLS and MS-CHAP is the method in which user credentials are presented. TLS is based on Client and Server Digital certificates and requires a Public Key Infrastructure (PKI) in order to generate and manage the digital certificates. MS-CHAP is based on user name and password.

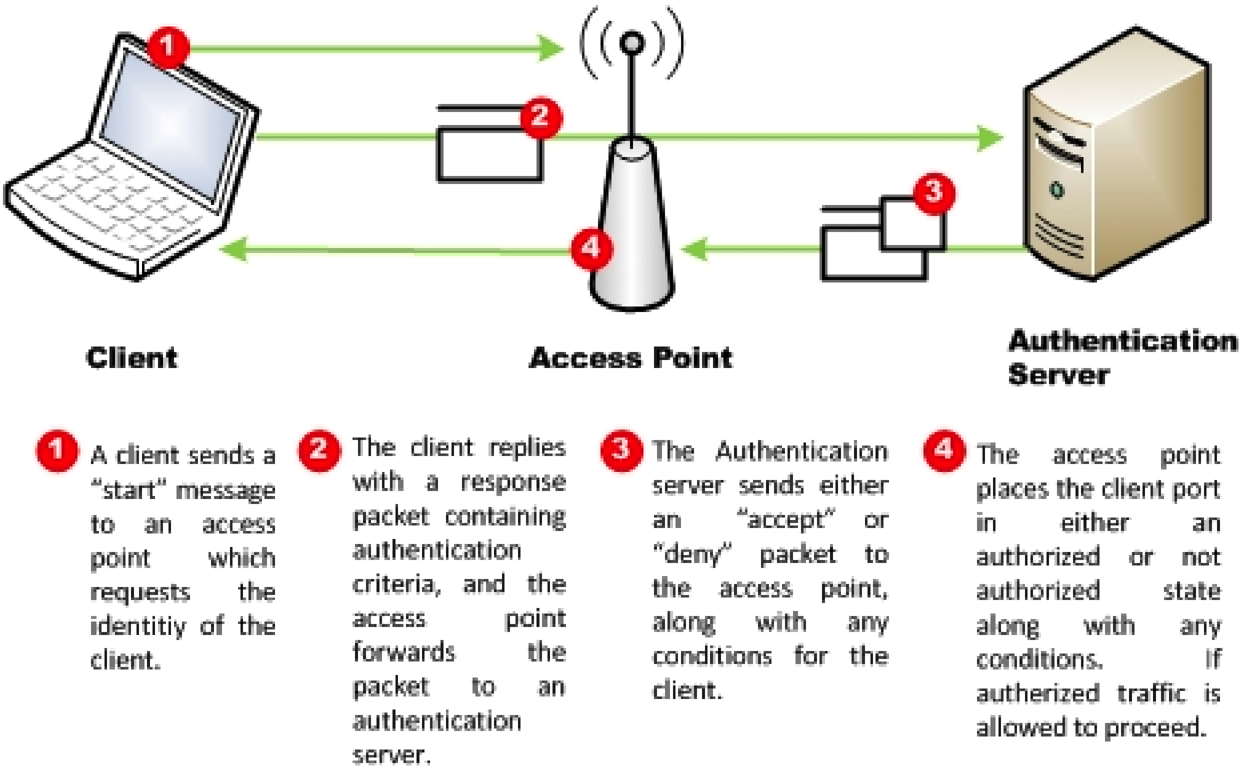
The reasons for the different methods are generally security based. It is technically harder to obtain a digital certificate than it is to obtain a username and password via social engineering, therefore the industry best practice is to use EAP-TLS or PEAP-TLS with non-exportable certificates for client authentication, however this may be impractical for some environments due to the administrative overhead it adds.

There are a number of Authentication Server options available. Examples are Microsoft Internet Authentication Services (IAS) and more recently Network Access Policy Services (NPS). These are services that are part of Microsoft Windows Server and are integrated into Active Directory.

Other network systems from Apple, Novell, or Linux can provide the ‘RADIUS’ protocol required for 802.1X/EAP.

Figure 2 outlines 802.1X/EAP authentication.

Figure 2 – Highly Simplified Description of 802.1X



1 A client sends a "start" message to an access point which requests the identitiy of the client.

2 The client replies with a response packet containing authentication criteria, and the access point forwards the packet to an authentication server.

3 The Authentication server sends either an "accept" or "deny" packet to the access point, along with any conditions for the client.

4 The access point places the client port in either an authorized or not authorized state along with any conditions. If autherized traffic is allowed to proceed.

3.1.7 Captive Portal

The authentication techniques outlined above focus on controlling connection to a wireless network at the Data Link Layer (refer Glossary below for further reading).

A captive portal can offer some control and security by allowing any device to connect to a network at this lower Data Link layer, but then requiring authentication before the device can access the Internet or any network services.

With a captive portal, users typically cannot access anything until they start a web browser session and they are then redirected to a special web page called a Captive Web Portal (CWP) where they are required to enter a username and password before continuing further (this technique is often used to provide wireless access in airports, coffee bars etc.).

Captive portals can be provided either with or without Access Layer authentication (e.g. Open or with PSK). In the case of an Open SSID, the captive portal should be delivered via Secure Sockets Layer (SSL) in order to encrypt the user's credentials.

Authentication is typically queried against a centralised user directory in order to leverage existing user information. Authentication methods can be via RADIUS, LDAP, Active Directory etc. Once the user is authenticated, the services available to them will depend on what has been allowed by the school. In some circumstances this might only be simple browsing or the ability to create a VPN to get more functionality with associated better security.

3.2 Summary of School Wireless Security

It is recommended that APs be installed in general accordance with this document by inclusion of these requirements in requests for proposals and contract documents.

In the event of conflict between these requirements and other regulations, codes or standards the order of precedence should be:

- Statutory Codes and Regulations
- Standards or Specifications within the tender or contract
- This document
- Referenced New Zealand and International Standards

Figure 3 - Summary of Common Wireless Security Components

Note: ease of use and setup difficulty need to be weighed against WLAN security, generally the two are generally inversely proportionate

	Open	Captive Portal only	Virtual Private Network only	WPA2-PSK + AES	WPA2-EAP with 802.1x	WPA2 with Captive Portal	WPA2+AES+ 802.1x + Per User PSK
Authentication	No	Yes – user (Device authentication is available but not secure)	Yes – user	Yes – device	Yes – user	Yes – user, device or both	Yes - user and device
Authorisation	No	Yes	Yes	Yes – for any user of the device Vendor dependant.	Yes	Yes – for user or device depending on authentication used	Yes - user and device
Encryption	No	No CWP is generally encrypted but Data link is not unless PSK is used.	Yes	Yes	Yes	Yes	Yes

Scalable **– can more devices be added to the network with little change to the security infrastructure?**	Yes	Yes, depending on how it is implemented	No – requires hardware support which will need to be enhanced as number of users increases	Limited – OK for deploying multiple classroom laptops at once Depends on solution.	Yes – assuming each user has a network login, they use that login for wireless	Yes – depending on type of WPA2	Yes - assuming each user has a network login, they use that for login to wireless
Traffic Separation can be based on login	No	Depends on Vendor	Yes	Depends on Vendor	Yes	Depends on Vendor	Depends on Vendor
Ease of use setting up infrastructure **Indicative only,** **1 (easiest) to** **6 (more complicated))**	1	2	5	2	6	6	6
Ease of use for person using device	1	2	3	2	3	4-6	3

Ease of use for ongoing Administration	1	3	2	3-5	1	3-5	2
Security Level [0 (least)-6(most)]	0	1	2	3	5	4	6

4 Building a Wireless LAN

School wireless networks have evolved from being predominately ad-hoc deployments in small areas through becoming part of school-wide infrastructure, to BYOD deployments where staff and students expect the network to always work, in all parts of the school campus. Early WLAN deployments focused on coverage. Over time, wireless standards and speeds have changed and there has been a mass increase in the availability of wireless capable client devices. WLAN deployments are now also about planning for client density, supporting the varied type of client devices (BYOD) and management of the WLAN for optimal performance and security.

The rapid widespread deployment of smart phones and tablets has placed significant demands on wireless networks – particularly with uploading photos and videos to the cloud for storage, apps transferring data in the background, substantial use of social media, and the proliferation of video content and multi-media websites.

This section describes some of the technical considerations for wireless implementation. Non-technical issues are described in School Wireless LAN Guidelines – Understanding Wireless (refer to section 1.2 – Documentation Map).

4.1 Network Requirements

As wireless network technology has matured there has been a proliferation in manufacturer offerings of both equipment and management tools. At the same time there have been a number of architectural developments in the industry that are driving forward innovation as the industry moves to 802.11ac and beyond.

The initial planning for a wireless LAN is critical in determining criteria for choice of hardware and integrator. The integrator should be responsible for ensuring that the chosen solution fulfils the school requirements.

School teaching and administrative requirements should be articulated and recorded clearly before technical requirements can be finalised. The Understanding Wireless document can assist with defining this process.

4.1.1 Logical Network Design Considerations

A school should consider the effect on their IP address range when deploying a wireless LAN (e.g. a BYOD policy will mean a significant number of new devices joining the network and requiring IP addresses). It can be an expensive (and frustrating) exercise for a school to discover it needs to create a new IP addressing scheme part way through a wireless deployment.

While small schools may not need to invest heavily in detailed design, a medium or large school is likely to benefit from a detailed network design, including the use of traffic separation. This technique can improve network security and performance. As a general rule, a school campus with greater than 250 connected network devices in the present, or near future, should give consideration to network traffic segmentation or VLANs

Traffic separation is best accomplished by including the use of Virtual Local Area Networks (VLANs). As the name suggests, a VLAN is a virtual network and it is created within software on network switches. A VLAN shares most of the characteristics of a physical Local Area Network (LAN), except that multiple VLANs can share a single physical cable. A network can be deployed so a user can select between multiple networks available from each AP (each different wireless network would have a different SSID). The network they choose (via the SSID) determines which VLAN(s) they belong too. Each VLAN can have a unique set of characteristics (such as services available, network speed and priority, monitoring etc.) applied to network activity.

For optimum WLAN and network performance it is recommended that network traffic segregation and management is performed using VLANs within the minimum possible number of SSIDs.

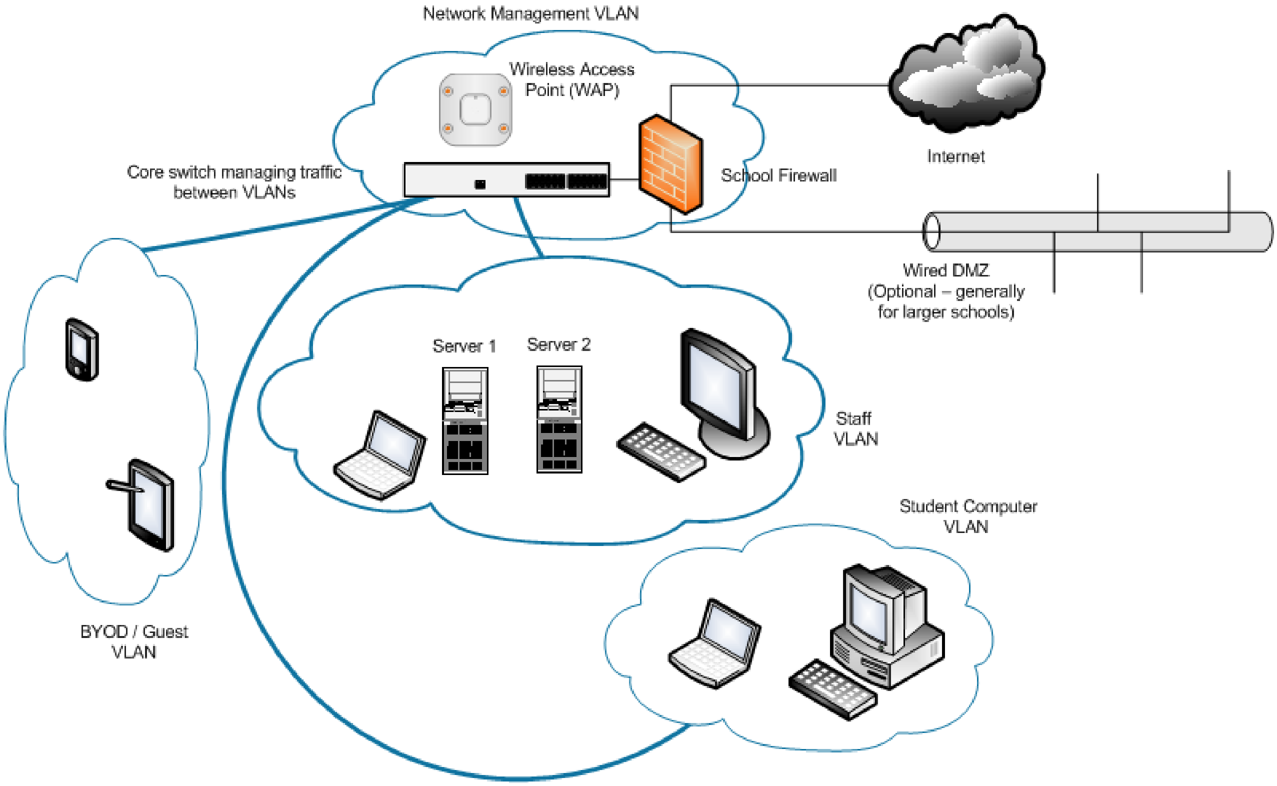
This would serve to maximise available ‘beacon time’ for each radio and offer granular network traffic control through the optimisation of media level data flow within each network segment. Multiple VLANs can be assigned to single SSIDs

Simply put – in most school campus scenarios at most three SSIDs would be required;

- trusted STAFF device network
- semi-trusted BYOD STUDENT device network
- un-trusted GUEST network

- A logical network diagram is shown in Figure 4 – Logical (VLAN) Diagram of Simple Network with Wireless. This diagram has similar parts to a network diagram, but suggests logical relationships within the network, which can be quite different to the physical network.

Figure 4 – Logical (VLAN) Diagram of Simple Network with Wireless


Network Management VLAN
Wireless Access Point (WAP)
Internet
Core switch managing traffic between VLANs
School Firewall
Wired DMZ (Optional – generally for larger schools)
Server 1
Server 2
Staff VLAN
Student Computer VLAN
BYOD / Guest VLAN

The planning and configuration of VLANs needs to be considered carefully by a network architect. Details are beyond the scope of this document.

4.2 Equipment Requirements

Once the high-level plan is in place, various options can be considered for the infrastructure that will best accomplish that plan.

4.2.1 Determining Location of Wireless Access Points

A site survey is the process of measuring the radio frequency (RF) coverage of a test AP or the existing WLAN infrastructure. It can also be useful to measure other RF signals, both from wireless networks, and conflicting ‘RF noise’ from other devices that might interfere with the school’s new APs.

There are two aspects to a survey, which each contribute to the positioning of APs. Coverage determines the locations in a school campus where the wireless network can be used. Saturation describes the number of devices that can be used in a particular location. Coverage and saturation must both be specified in the wireless network requirements.

A wireless infrastructure scoping document should be used to define the performance specification for an installation. It should include the proposed wireless applications, the total number and type of devices to be connected, the number of simultaneous connections required, and the bandwidth performance requirements broken down into areas of the school campus. This document is a critical part of the tendering process. The network supplier should be held to deliver to these requirements.

4.2.1.1 Coverage

There are two site survey coverage strategies that can be considered:

i. The most reliable, but most expensive, approach is to perform a complete site survey before any deployment to choose the best locations for the APs. Typically with this method, site survey professionals temporarily place APs in different locations, take measurements, and adjust their settings and locations as necessary. Once the optimum location for the APs has been determined, they will be permanently installed, and the system tested again to confirm installation quality. This method is the most reliable way to deploy a wireless network; however, it can be expensive and time consuming. It also requires specialist hardware/software for taking the measurements.

ii. An alternative strategy is to make initial estimates, with the help of a software planning tool, to determine the AP locations. The tool needs to be configured with a school site map (floor plans etc.), indications of wall construction, and types of APs being considered. After the planning, the installers deploy APs according to the plan, then check to confirm that the network meets the requirements specified by the school. If there are coverage issues, additional APs can be deployed. If there is interference, or similar issues, the AP locations can be adjusted.

The second strategy is usually less costly to implement. There should be few changes required for complete coverage. Any money saved though spending less time doing the survey can be invested in one or two more APs. Either strategy should result in the school getting a wireless network that meets the requirements they have specified.

4.2.1.2 Capacity Planning

Sometimes there is a requirement for a very large number of user devices to connect wirelessly in one area. An example is a lecture theatre where dozens of students may be simultaneously using BYOD devices wirelessly.

Capacity planning, especially for high density areas, is a critical part of wireless implementation planning. This is covered further in Appendix A.

Typically most 802.3 Wave 1 APs allow for two 1-Gbps switch ports either for resilience or for “bonding” together to support the higher data rates of the AP. This needs to be considered when allocating switch ports.

Note also that 802.11ac Wave 2 APs with MU-MIMO and higher data rates may dramatically increase bandwidth and overwhelm 1-Gbps switch ports.

4.2.1.3 Roaming

In addition to being able to connect to the wireless network from any part of the school, devices should also be able to move seamlessly from one part of the school to another while using network services without the need for re-authentication. This is especially important when authentication is provided by 802.1X. The selected infrastructure needs to support Fast Roaming with key caching and Layer 3 mobility to facilitate inter-subnet roaming. This allows users to move about freely and remain connected to the network without their applications/services dropping out.

During the design phase the network should provide overlapping coverage in areas where seamless roaming is required and this should be validated during the post implementation survey phase. If a service is ‘broken’ by moving around in this way, the integrators should diagnose why, and rectify any problems within the wireless network.

4.2.2 Power over Ethernet (PoE)

Enterprise class APs support Power over Ethernet (PoE). PoE is a mechanism for sending power over standard Ethernet cabling to run remote devices, such as wireless APs, VoIP phones and CCTV/IP cameras.

The relevant IEEE PoE standards are 802.3af, which provides a maximum of 15W of power per port and 802.3at which provides a maximum of 30W per port.

PoE allows for flexibility in WLAN deployment as it means APs do not require power outlets, and can be easily moved to meet requirements.

The power is provided either by a PoE capable data switch, PoE Midspan Injector, or a singular power injector. The PoE switch looks exactly like any other switch, and provides power along with the Ethernet signal, over standard Cat 5 or better copper cable. An injector is a separate device that looks much like a regular ‘power brick’ often used to power electronic equipment. The injector has two RJ45 ports. One is connected to the network switch, and the other port connects to the Ethernet cable running to the device requiring power.

A PoE switch can power a number of devices from one central point. Injectors are useful where there are only one or two devices that need to be powered from a particular data cabinet. There are a wide range of considerations to determine the best device to use. Considerations include topography of a school, existing wireless and wired equipment, quality and type of cabling.

With 802.11ac the power requirements of APs have increased and 802.3af switches or injectors are unlikely to have sufficient power, so typically 802.3at switches/injectors are required.

PoE capable switches are more expensive than non-PoE capable switches, consume more power and generate more heat.

4.3.2 IPv6 Readiness

The current version of the Internet Protocol (IP) being used in almost all networks is known as version 4, or IPv4. A new version of IP, IPv6, is being increasingly deployed, and is likely to be a very important upgrade option for schools over the typical lifetime of an AP purchased now.

All IT equipment purchased by a school should be IPv6 compatible. Vendors can verify the standards their equipment is built to, and supply records of IPv6 compliance testing or provide information on when IPv6 compatibility will be available. This information will give the school confidence that equipment will be able to use IPv6 as it becomes common. Most vendors will add IPv6 support in future software updates.

5 Network Management

Schools will need to allocate resources for network management in the same way as they would for a wired network. This section describes ways that the additional workload of a carefully planned and implemented wireless network can be minimised.

The concept and security features of Wireless Infrastructure management software are described in section 5.1 below.

A Network Management System (NMS) provides the centralised monitoring, configuration and reporting on the network infrastructure. While wireless controller based solutions can provide a range of management functions, this should not be confused with the function of an NMS. A controller based solution may require additional reporting tools/software for the data logging required for comprehensive troubleshooting.

5.1 Wireless Access Point Management

Setup information for a wireless network can be configured on each AP individually (also known as Autonomous Access Points), configured via an AP controller, or a centralised NMS can provision devices collectively.

If a school has more than two APs, a solution that includes centralised management should be considered – the more APs installed, the more essential this becomes.

There are a number of ways management can be implemented. The main options are compared below.

Figure 5 – Summary of Wireless Management Systems

	Autonomous	Controller-Less	Physical – controlling all traffic	Physical – monitoring	Virtual - monitoring	Software Service
Description	Each Wireless Access Point (AP) is manually configured and monitored	Intelligent AP devices with centralised network management either on-premise or cloud based	A physical controller is purchased It is then physically connected to each AP, using the school's standard network cabling Some controllers can receive and process traffic from anywhere on the school network	A physical controller is purchased	A new virtual server is deployed to run controller software (typically VMware or Microsoft Hyper-V)	Software is installed on an existing (physical or virtual) school server
				In each case, the controller communicates with each AP, sending configuration, update, and control information. The AP can send back information about its usage		
Advantages	• Very Simple concept to configure each AP individually, repeating the same configuration steps each time • Many low-cost APs only support this method • No controller cost	• No single point of failure • Linearly scalable • No Controller Cost	• Simple configuration • Adding additional APs is a relatively trivial task • Controller might include PoE	• Can monitor all APs regardless of where they are in the school	• No separate hardware cost. • Can monitor all APs regardless of where they are in the school	• No separate hardware cost • Software might be provided at no cost to school • Can monitor all APs regardless of where they are in the school

	Autonomous	Controller-Less	Physical – controlling all traffic	Physical – monitoring	Virtual - monitoring	Software Service
Disadvantages	• Requires configuration and monitoring to be repeated for each AP in a school Having to configure each AP individually does not scale well. • APs that only support this method tend to be lower quality than those recommended for a school	• If cloud based, loss of internet access means no ability to manage or update AP configurations	• Cost of physical controller. • Single point of failure with one controller • Can create a network bottleneck if many APs are all directing traffic through one controller	• Cost of physical controller	• Reliability depends on reliability of underlying hardware and virtualisation software • Uses resources on existing school virtual server. • Some additional overhead for school IT support	• Reliability depends on reliability of server it is running on. • Uses minimal resources on existing school server. • Some additional overhead for school IT support

Enterprise class wireless vendors typically provide management tools and usually support remote management. These management tools are often proprietary and rely on all APs being from the same vendor. Alternatively, some third party management and WLAN monitoring tools can work with products from a variety of manufacturers. Such third party tools can often be used to configure other network devices such as switches and firewalls.

5.2 Authentication

Access rules can be changed using network management software. A specific user or AP configuration can be changed to prevent or allow a particular connection. Once the wireless network has been configured, anyone with an appropriate account will be able to connect to any AP on the network.

5.3 Managing Wireless Performance

Ideally, each AP should monitor the radio environment it is in, and periodically report on neighbouring signal and interference levels. This function is a part of the control plane and with some vendors' products, this information can be used to modify the signal strength of each AP to maximise network efficiency and avoid APs interfering with each other.

5.4 Wireless Intrusion Prevention System

A standard feature of most wireless solutions is a Wireless Intrusion Prevention System (WIPS) where the APs are able to detect 'rogue' devices which are not part of the network. Some enterprise APs can vary their radio characteristics to minimise the negative effects of rogue APs and in some cases mitigate against threats.

There are also many free software tools available to scan for rogue devices. They are readily available for a wide variety of operating systems.

Specialised hardware tools can be used to give much more accurate and detailed information. These tools are generally only used by those installing or maintaining wireless installations. There are broadly two security objectives in using these tools:

- They can help identify other wireless networks that might interfere
- They can be used to analyse the wireless network to help identify any security risks

Scanning can also pinpoint the source of performance issues caused by interference between APs, and interference caused by other devices.

6 Wireless LAN Issues

After the completion of a wireless installation, there will be further considerations for the ongoing operation of the network. An overview of the costs of installing and maintaining a wireless network is included in School Wireless LAN Guidelines – Understanding Wireless. Refer to section 1.2 – Documentation Map, above. The following section describes ongoing technical considerations.

6.1 Security Practice

Security is always a balance between risks (perceived and actual) and mitigation costs. Various factors need to be considered including the vulnerability of the network, the threat of attack, the value of the data to be secured and the costs involved. Wireless networks are often perceived as particularly vulnerable because anyone with a suitable wireless device can detect the presence of a wireless LAN. Some risks are specific to wireless, but in general a security plan that provides good protection to a wired network will also mitigate many risks with wireless. Securing WLANs, as with all networks, needs to be seen as a continuous process rather than a one-off step. Any security solution needs to be consistently and properly implemented with regular monitoring.

The WLAN should be configured so that anyone trying to access the WLAN has at least the same access restrictions as they would if they sat down at a wired network workstation. Schools should be implementing a comprehensive security policy and incorporating best practice standards including WPA2. Section 6.3 – Common Security Issues and Mitigations, lists many common WLAN security issues, and suggests mitigations for each.

6.2 User Support Requirements

A support plan should be in place for supporting school staff, students, and any other wireless users. This needs to cover two very distinct areas:

Technical support – to ensure the client devices are attached to the wireless network and performing to expectation.

Pastoral care - to ensure the safe use of the network. Many schools will already have a support structure in place to help develop confident, safe, and responsible online activity. This should be reviewed, and extended, to cover specific issues with wireless devices, such as having less control over where and when a device is used. Netsafe (www.netsafe.org.nz) is a valuable resource to help with this. Netsafe provides a downloadable kit for schools to help students learn to stay safe online, and also offers the myLPG site which contains a range of online content, covering topical areas of online safety. Schools should also consider incorporating an Acceptable Use Policy or Digital Citizenship practice.

6.3 Common Security Issues and Mitigations

Issue	Mitigations
- Performance and security is compromised by devices using old standards	- 802.11n and WPA2 should be the minimum standard required to connect to the school's primary wireless network. A second network, using a different VLAN, may be provided for older or less capable wireless devices. Ensure that less secure devices are upgraded to WPA2
- Easily guessed management username and password	- Change default settings on APs. It is preferable to also use a central directory service to authenticate management access to any device if the school is using a directory service for user authentication.
- Anyone with a wireless device can be tempted to try to break into any wireless network they can 'see' on their device	- The security configuration should mitigate against unwanted malicious access - Using techniques like SSID Schedules, Intrusion Detection and Alerting are all best practice methods of mitigation
- Wireless network signals can be visible over a wider area than the school would like	- Consider changing the position, or in some cases rotation, of APs, to concentrate the radios in the desired directions - Use of directional antenna technology could be considered
- Wireless access is available for longer hours than is necessary or desirable	- If a school wishes to restrict access hours, or have 'device free days', authentication can be disabled on the infrastructure making the wireless LAN unavailable at those times - Most vendors have features that provide schedules to automatically control this requirement

Issue	Mitigations
• Someone on the school campus can plug an additional AP in to the school network, bypassing standard school security	• Make sure that the network is regularly checked to ensure that only legitimate wireless APs and devices are connected. Many vendor solutions can periodically scan for WIPS events; otherwise it can be tested manually by walking around with a wireless device and software tools such as inSSIDer • Shut down or secure unused switch ports • Educate users about security and implement an organisation wide policy. Ensure that users know not to plug in their own APs to avoid compromising the network
• Lack of control over BYOD devices increases risk in a wide range of areas	• Establish separate VLANs for BYOD devices and apply stronger security rules, compared to the rules for school-owned devices • Implement Mobile Device management functionality if appropriate
• Security issues can be discovered on AP hardware • APs can be underperforming due to firmware bugs	• Regularly update the firmware of all wireless equipment
• Monitoring might determine that an unexpectedly high number of devices are connecting to one or two APs	• Consider moving APs, or purchasing additional ones, to cover saturated areas • Where there is more than one AP in range of a saturated area, set a maximum number of clients for each AP to spread clients evenly • Consider features such as load balancing and band steering to maximise performance

Issue	Mitigations
Users might attempt to gain management control of network devices, including AP controllers	Disable the ability to manage APs from any VLAN other than the VLAN reserved for management Impose additional security on the management VLAN, such as not allowing wireless access, or restricting management VLAN access to school IT support staff
Some ‘visitors’ to the school (e.g. relieving teachers, Ministry staff or contractors) need more access to the school network than a visitor would normally have	Ensure User Role Based Access Control is a requirement to provide different levels of access to the network based on Identity
Students might be exposed to inappropriate content, either accidentally, as the result of student experimenting, or as part of a bullying pattern of behaviour	Provide students and staff with appropriate training to avoid, and to deal with, this behaviour The Ministry of Education is one of a number of organisations that are members of the NetSafe group. NetSafe claims to be “… an independent non-profit organisation that promotes confident, safe, and responsible use of online technologies.” Ensure that all student traffic is appropriately delivered through content control Implement fine-grained policy to only allow required services
There is a concern among some parents that wireless networks may present a health risk	The Ministry of Health can provide scientifically validated research on this topic

7 Appendix A – Special Requirements

The issue of extending coverage to remotely located, moveable/portable buildings and special usage or temporary buildings is the subject of this Appendix. .

Although each school site is unique, this Appendix will aim to outline appropriate best practice for common challenges, including:

- Remote buildings
- Special usage buildings
- Temporary buildings
- Mobile/moveable buildings
- High-density environments

7.1 Wireless Backbone Connectivity Solutions

In addition to supporting user devices, wireless networks can be used to deliver backbone network connectivity, particularly where a cabled solution is either not feasible or not cost effective. This can be used to connect remote, temporary and mobile buildings to the LAN in a school environment.

Two common ways of delivering wireless backbone connectivity are;

- Point to Point connections
- Wireless mesh connections

7.1.1 Point to Point

Point to Point (P2P) wireless connectivity is based on using either unlicensed spectrum (typically the 5GHz band) or licensed spectrum used by digital microwave (a licensed spectrum P2P link would be extremely costly for a school to deploy).

Many wireless vendors have APs that can be deployed as P2P transmitter/receivers, and by using special directional antennae they can connect over distances in excess of 5km.

An AP connected to the school’s wired LAN would be set up as a P2P device and its antenna pointed at another AP in the remote building to create a P2P link over the 5GHz frequency range. If the AP in the remote building has a second radio, this could be used to support client devices in the 2.4GHz range. If single radio access points are used for the P2P link then an additional access point would be required to support end users. If the cost of the two APs to deliver this solution is lower than the cost of cabling this may well be a viable alternative. It also has the flexibility of easily being redeployed – either as a P2P link to another remote building or else the P2P APs can be redeployed as standard APs.

Disadvantages of a wireless P2P link to a remote building are:

- Subject to interference (e.g. by other 5GHz APs using the same channel)
- Line of sight only - will not penetrate landforms (hills etc.) or dense vegetation

7.1.2 Wireless Mesh

Using standard 802.11 technologies, wireless vendors have developed proprietary routing protocols to create self-forming, self-healing resilient mesh networks in order to extend a LAN or connect devices such as VoIP or video equipment. Not all solutions are created equal with some vendors requiring centralised controllers in order to support this functionality while others are able to provide distributed control and data planes with no single points of failure.

The wireless mesh technology chosen should be capable of managing multiple on and off ramps to the wired network and be able to mitigate loops and broadcast traffic to maximise performance.

Most mesh technology operates in the unlicensed spectrum, and in some cases 5GHz is dedicated for backhaul and the 2.4GHz radio for client access. Some vendors support client and backhaul on the same radios. Typically omni-directional antennas are used.

The advantages of mesh technology are the same as with P2P but with the added benefit of resiliency and survivability. In a fully distributed mesh, no one node can take down the entire network as traffic is routed around the outage.

Disadvantages are generally performance. As wireless is a half duplex shared medium, each mesh hop will result in a decrease in throughput unless dual bonded radio technology is used. In most cases the benefits of a resilient, flexible infrastructure outweigh any performance limitations.

It should be noted that there is no current IEEE standard for mesh interoperability; therefore all vendor solutions are proprietary. The 802.11s standard is in progress to address this.

Mesh links in the unlicensed spectrum can offer a cost effective solution to bringing LAN connectivity to groups of remote, re-locatable and temporary buildings. Dependent on the vendor technology, the mesh nodes (APS) may support client devices in addition to providing backhaul to the LAN. If not, additional APs can be deployed off the node.

7.2 User Density on a Wireless Network

Many school wireless networks are no longer ad-hoc deployments in small areas. More commonly schools are adopting a BYOD policy which drives a staff and student expectation that the network should always work at acceptable performance levels and in all parts of the school campus.

Early WLAN deployments focused on coverage. Whilst coverage is still important, what is also critical in delivering on these new expectations is planning for client density. With the proliferation of wireless capable devices including iPads, iPods, SmartPhones, Netbooks, laptops and other tablet devices, it is possible that many typical school network users will have more than one device on hand and connected to the network simultaneously. A simple plan for coverage will not deliver on the expectation of the network always working and at acceptable performance levels in this case.

Wireless networks, unlike wired networks, are a shared medium at the access level. An AP will potentially provide a maximum specified amount of bandwidth so if ten users are simultaneously using the network, each will have to share and may get somewhat less than 10% of the total available - depending on the behaviour of the user, their device, other users' behaviour, and the AP.

Users who only send and receive e-mail or use the wireless connection in short bursts may never notice a slow down even when sharing it with 50 or more other users. On the other hand, a small group of wireless users who access high-resolution multimedia or download large files over a single access point may find network performance so frustrating that a wired solution is required.

In some cases there may be a very large number of devices in one area. An example is an assembly hall with all students using BYOD devices simultaneously.

Catering for a high density of users can be more effective if the power of each AP is lowered, as higher powered APs can interfere with each other's radio signals. This lowers coverage per AP, so there may need to be more APs to compensate. Lowering the power of an AP does not negatively affect saturation.

Most wireless technologies provide a variety of techniques to ensure that adequate capacity is available to the users. Examples include Quality of Service configurations, use of AirTime Fairness as well as load balancing and band steering to make maximum use of the available medium. See the glossary at the end of this document for an explanation of these terms.

It is critical to consider and plan for any expected high density wireless use areas in a school campus.

8 Appendix B – Cost Effective Transitioning to Wireless

This appendix is to provide guidance for school principals, board members and IT support people looking for options to cost effectively transition from wired to wireless technology –particularly in the case where a school has a number of non-wireless legacy PCs connected to old cabling and data switches.

8.1 Background to the Issue

The SNUP programme will replace a school's old cabling and switching infrastructure and will typically provide 4 x 1Gbps data ports per standard classroom. Cabling infrastructure in excess of this is not likely to be required as high performance WLANs become more prevalent. Each AP needs to connect to a data outlet (ideally 2 outlets for 802.11ac), so in the future (where the expectation is almost all user devices will be wireless capable) this number of outlets should be sufficient for classroom requirements in almost all cases.

The challenge is that for budgetary reasons many schools will need to transition to wireless over a period of a year or more and so they still need to retain legacy PCs that are not wireless capable. Each of these legacy PCs needs a data outlet to connect to the network. In some cases there are 20 or more legacy PCs and so the SNUP cabling refresh project will not provide sufficient data outlets to cater for the transition period.

There are five different options described in this appendix to address this situation:

- Replace legacy PCs
- Add additional data outlets
- Use wireless USB adapters
- Use wireless PCI cards
- Use a hybrid cabling interim solution

Each of these options, along with their advantages and disadvantages, is described in more detail below.

8.2 Replace Legacy PCs

Option Description:

This option is to immediately replace legacy non-wireless PCs with wireless enabled devices, replace all legacy cabling/switching infrastructure with the standard SNUP cabling/switching upgrade (the wireless option), and deploy a Wireless LAN (WLAN).

Advantages:

- Meets the current SNUP programme criteria
- Will provide sufficient data connectivity to meet all immediate and medium term future requirements
- School will be able to take immediate advantage of wireless deployment
- Higher speed and more robust connectivity for all devices

Disadvantages:

- Significant up-front cost to deploy WLAN and replace all legacy PCs.
- Very short transition period from old environment to new environment (days or weeks at most)

Evaluation of Option:

This option is unlikely to be a viable option for schools with large pools of legacy PCs and very little funding available for replacement.

This option is probably the most appropriate for schools that have few legacy PCs and/or the majority of legacy PCs are about to be replaced and they have sufficient funds available for immediate replacement of these legacy PCs.

8.3 Add Additional Data Outlets

Option Description:

This option is to replace all legacy cabling/switching with sufficient new cabling/switching to provide new data ports for all legacy PCs and any additional outlets required (e.g. for APs)

Advantages:

- Legacy PCs will be able to be used until the end of their lifecycle
- No requirement for school to immediately fund new PCs
- Will provide sufficient data connectivity to meet all immediate and medium term future requirements
- School will be able to deploy wireless if required – as and when they are ready
- Higher speed and more robust connectivity for all devices

Disadvantages:

- The school (or the SNUP project) will need to fund the additional cabling and switching infrastructure to provide the additional data ports needed for the legacy PCs
- Most of the additional cabling and switching needed for the legacy PCs will become a stranded asset – it will become redundant as the legacy PCs are replaced by wireless devices, so it is unlikely to be a prudent use of funds
- If the legacy PCs need to be relocated to other areas, the new area is unlikely to have sufficient data outlets to accommodate them and so the problem recurs

Evaluation of Option:

While additional cabling and switches could be provided to cater for the legacy PCs, this option is likely to be a poor investment choice as switches and cabling are expensive, and the additional data outlets will only be used for the transition period while the school moves to wireless

This option may also be appropriate for schools with small numbers of legacy PCs that need to be available for a few more years before replacement. Such schools should consider whether the number of ports the SNUP programme delivers per classroom, potentially supplemented with a few additional data outlets, will be sufficient to cover the number of legacy PCs they have (remembering there must also be sufficient data ports to connect any APs required)

8.4 Use Wireless USB Adapters

Option Description:

This option is to deploy a WLAN and plug wireless USB adaptors into each legacy PC so they can connect wirelessly.

Advantages:

- Legacy PCs will be able to be used until the end of their lifecycle
- No requirement for school to immediately fund new PCs
- Meets the current SNUP programme criteria
- Will provide sufficient data connectivity to meet all immediate and medium term future requirements
- School will be able to take immediate advantage of wireless deployment

Disadvantages:

- USB adaptors are very simple to remove, and are small enough to be easily concealed, so there is a high risk of theft
- Signal strength of USB adaptors may be considerably weaker than that of a PCI card (refer next option). In most cases this will not be an issue
- Some legacy PCs may not have a spare USB port
- School will need to fund the purchase of the wireless USB adaptors and the time required to install and test them. Installation is generally fairly simple (less than 15 minutes per device) but there is a possibility (fairly small) of having driver conflicts or other issues that would increase this time. Wireless USB adaptors typically sell for around $50
- If lower cost 802.11g USB adaptors are used, they will slow the wireless network down for all 802.11n devices using the same AP
- If 802.11n USB adaptors are used the PCs will need a minimum of USB 2 to support the 802.11n data rates
- USB adaptors may become a stranded asset once the legacy PCs are replaced
- Requires a WLAN to be deployed. While it is almost certain that all schools will eventually move to wireless, many schools may not be in a position to do this initially when they are upgraded under SNUP

Evaluation of Option:

The major drawback to this option is the risk of the USB adaptors being stolen. They are very easy to remove and conceal, and it is very difficult to guard against this occurring. As a result, there is likely to be few schools for whom this would be a viable option

This is also only a viable option for schools that are ready (and have the funding) to upgrade to wireless at the time of the SNUP rollout

8.5 Use Wireless PCI Cards

Option Description:

This option is to deploy a WLAN and install wireless PCI/PCI-E cards into each legacy PC so they can connect wirelessly. Wireless PCI/PCI-E cards get installed into a PCI slot inside the PC, so the cover will need to be removed from the PC, the card installed, and software drivers installed and tested

It should be noted that PCI and PCI-E expansion slots are physically different and special care should be taken to ensure that the correct wireless card is purchased for the correct PC expansion slot

Advantages:

- Legacy PCs will be able to be used until the end of their lifecycle
- No requirement for school to immediately fund new PCs
- Meets the current SNUP programme criteria
- Will provide sufficient data connectivity to meet all immediate and medium term future requirements
- School will be able to take immediate advantage of wireless deployment

Disadvantages:

- Some PCs may not have a spare PCI slot.
- School will need to fund the purchase of the wireless PCI cards and the time required to install and test them. Installation is generally fairly simple (less than 30 minutes per device) but there is a possibility (greater than for USB adaptors) of having driver conflicts or other issues that would increase this time. Wireless PCI cards typically sell for around $50
- PCI cards may become a stranded asset once the legacy PCs are replaced
- If lower cost 802.11g PCI cards are used, they will slow the wireless network down for all 802.11n devices using the same AP
- Requires a WLAN to be deployed. While it is almost certain that all schools will eventually move to wireless, many schools may not be in a position to do this when they are upgraded under SNUP

Evaluation of Option:

This is likely to be a viable option for schools that are ready (and have the funding) to upgrade to wireless at the time of the SNUP rollout

The time and expertise involved in installing and testing the PCI cards needs to be considered. The expertise required is not particularly high unless issues such as driver conflicts occur. For schools with strong IT capability this should not pose a major issue and they may find this option attractive, but other schools may find the task of installing PCI cards rather more daunting.

8.6 Use a Hybrid Cabling Interim Solution

This option is to deploy the new SNUP cabling and switching infrastructure and also retain the current legacy cabling and floor switching infrastructure – but only retain legacy cabling in those rooms where the standard SNUP deployment will not provide sufficient data outlets to connect all the legacy PCs.

This is shown diagrammatically in Figures 4 and 5 below. Figure 4 shows a simplified diagram of a typical school environment prior to upgrading as part of SNUP and Figure 5 shows the same school after the upgrade.

Figure 6 – Before Upgrade

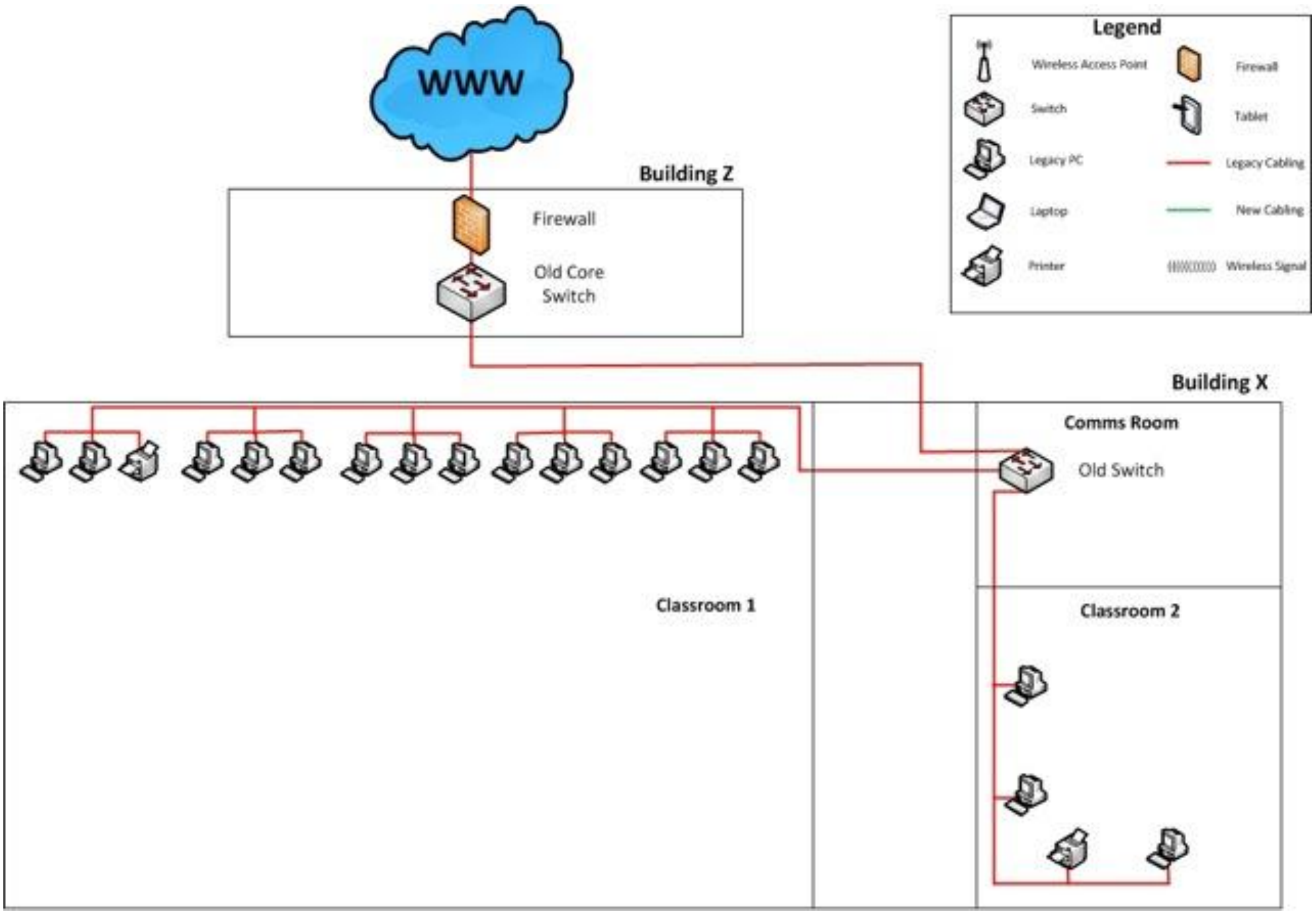
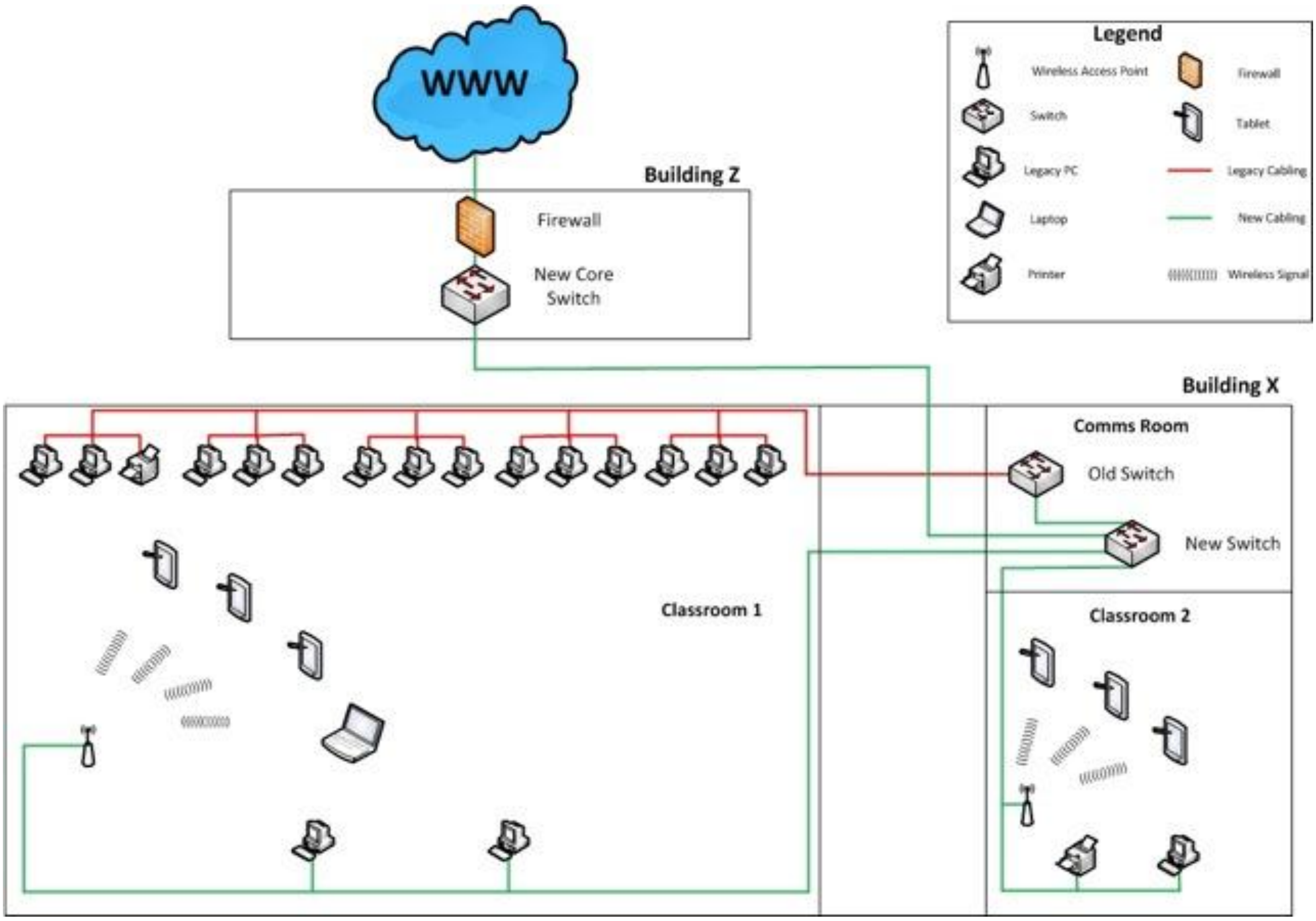


Figure 7 – After Upgrade



The diagrams show a classroom block (Building X) with two classrooms and the building where the core campus IT infrastructure is housed (Building Z). The legacy cabling is shown in red, and new SNUP cabling is shown in green. Classroom 1 has many legacy PCs, while classroom 2 only has two devices that need a wired connection.

The approach for the hybrid cabling option is to replace all old cabling and switching infrastructure that is not compliant with the SNUP policy and standards with new infrastructure in all areas except for classrooms where there are more legacy PCs than available data outlets under the SNUP upgrade criteria. In the diagrams, classroom 1 would get 4 new SNUP outlets and would also retain the old legacy cabling and outlets; while classroom 2 would get 4 new SNUP outlets and have all legacy cabling removed (or disabled).

The legacy PCs in classroom 1 will remain connected to the same wall outlets as before, and the legacy switch that connects to these outlets will in turn be linked to a new SNUP building switch and then back to the core network.

The retention of legacy cabling and switching should be minimised and confined to being as close to the legacy PC classrooms as possible. Note that this is the only option described in this document that retains any of the legacy cabling and switching infrastructure.

Since both classroom 1 and 2 are wired with 4 outlets as per the SNUP policies and criteria, these outlets can support new wireless infrastructure whenever this is required as well as legacy PCs or other wired devices if required – the limitation is the number of outlets, not their functionality.

Figure 5 shows APs installed in both classrooms after the upgrade, but schools may wish to defer the wireless deployment until sometime after the SNUP upgrade.

Advantages:

- Legacy PCs will be able to be used until the end of their lifecycle.
- No requirement for school to immediately fund new PCs.
- Meets the current SNUP programme criteria.
- Will provide sufficient data connectivity to meet all immediate and medium term future requirements.
- School will be able to deploy wireless without additional cabling.
- No additional costs involved in connecting legacy PCs.

Disadvantages:

- Legacy cabling and switching infrastructure has an increasing risk of failure due to its age and the significantly less stringent quality assurance and manufacturing tolerances during its manufacture compared with current good practice. Note that this risk exists today regardless of any SNUP work, and adding the new SNUP cabling in parallel does not increase the risk, but one of the original intentions of SNUP was to get rid of all non-compliant cabling and switching infrastructure to avoid this issue.
- Legacy cabling and switching will not support higher data speeds reliably. This can be mitigated by not using the legacy cabling for anything other than legacy PCs.
- Legacy cabling may not be suitable to connect APs as it may not support PoE – so all APs should be connected to new cabling/switching.
- The legacy PC classrooms will end up with two different types of wall data outlets that both look the same – the legacy outlets (which should not be used for anything other than legacy PCs) and the new SNUP outlets. Confusion may occur over which outlets are which – particularly as time passes and personnel change. Once the legacy PCs are finally decommissioned the legacy switches can be removed and blank faceplates (that cover the outlet sockets) could be purchased to cover the legacy data outlets to reduce future confusion.
- Both the legacy and new switch(es) need to be accommodated in the comms cabinets (see Figure 2) – this may create issues with space and cooling (particularly if there is a need for several PoE ports).
- If the legacy PCs need to be relocated to other areas, the new area is unlikely to have sufficient data outlets to accommodate them, and will either not have legacy cabling or (if it did have) the legacy cabling would have been replaced under SNUP, and so the problem recurs.

Evaluation of Option:

This option provides a way to retain legacy PCs (albeit by retaining the increasingly unreliable cabling and switching infrastructure they utilise) without additional expenditure as well as ensuring all classrooms are wired for the future.

The major drawback to this option is that some classrooms (the ones with large numbers of legacy PCs) will have two different types of wall data outlet – one type that meets the needs of the future, and one type that will become increasingly unreliable and has significant restrictions on what it can do. These outlets will look the same and so there may be future confusion over which is which. In many cases this will be offset by the ability to retain legacy PCs for their useful lifetime without incurring any additional expenditure.

This option is likely to be attractive to most schools that have significant numbers of legacy PCs – particularly if they do not have the budget to replace these PCs in the short term.

8.7 Assessment of Options for Different Scenarios

If a school has only a few legacy PCs, the option of adding wireless PCI cards may be the most appropriate. For small numbers of PCs the impact of adding PCI cards may be acceptable and the PCs will then be able to connect to the network from any location where there is wireless coverage (or where there is a new data outlet available).

If a school has a large number of legacy PCs that are likely to remain in their current location until they are retired, the hybrid cabling option may be the most appropriate (i.e. leave the PCs on their existing cabling infrastructure until they are retired).

If a school has a large number of legacy PCs that are likely to move from their current location before they are retired, the situation is less obvious. Installing PCI cards will provide portability for the PCs but may not be a trivial operation. Another option is to use the hybrid cabling option and then move the legacy switch with the old PCs when they are relocated (a new switch or switches will need to be purchased if the PCs are to be split into more than one location). Note that this may require the use of temporary low cost cabling from the switch to the PCs in the new location(s). The most pragmatic solution may be to deploy the hybrid cabling option initially and wait until the PCs are relocated before making the decision as to what to do in the new location.

9 Appendix C - Glossary of Terms

Term, Acronym, or Abbreviation	Definition
10/100 Mbps (or Mb/s)	100 megabits per second Ethernet. Can switch 'back' to the older 10 megabit standard.
10GbE	10 Gigabit (per second) Ethernet
1GbE	1 Gigabit (per second) Ethernet. When using copper cabling, can switch 'back' to the older 100 or 10 megabit standards.
802.11 protocols .	A set of standards created by the Institute of Electrical and Electronics Engineers (IEEE). Each standard is created by a specially convened committee of the IEEE. Each committee is designated by a letter. The letter then becomes part of the standard name.
802.11 protocols – Allowable MIMO streams	Equipment that uses Multiple Input / Multiple Output technology transmits multiple radio signals at the same time. Each individual radio signal is transmitted by a unique radio and antenna. More streams provides increased data capacity. Note that the number of usable streams is equal to the lower of the number of streams supported by the AP or client.
802.11 protocols – Approximate indoor range	An indication, in metres, of the likely distance within which the AP will deliver reasonable performance indoors. There are numerous things that can interfere with the RF transmission, which weakens the signal. This effectively lowers the actual data rate. Outdoor range can vary tremendously, up to several kilometres, for most protocols. Actual distances achieved depend heavily on the type of antennae used, height of the AP, and geography of the region being covered.
802.11 protocols – Bandwidth	While the standard frequency provided is a 'reference', the actual frequency used varies around the reference. Bandwidth is a measurement in megahertz (MHz) of 'spread' of the actual RF transmission. A wider bandwidth allows faster data flow.
802.11 protocols – Frequency	This is a technical reference point, describing the mean radio frequency (RF) used to carry data, in Gigahertz. (GHz) Of particular note is that lower frequencies travel further, and are less susceptible to certain environmental considerations (such as wall construction). Higher frequencies provide more data capacity but do not travel as far as 2.4GHz.
802.11 protocols – Maximum data rate	The theoretical data transfer rate per stream, expressed in megabits per second (Mbit/s). A stream describes one logical connection between the AP and client device. The 802.11 specification and amendments specify transmission rates not actual throughput. Due to different access methods to the RF medium the typical throughput is half or less the data rate.

Term, Acronym, or Abbreviation	Definition
802.11 protocols – Release Date	The date each standard was confirmed by the IEEE. Note that standards tend to be implemented in ‘draft’ form before this date, and manufacturers release products based on the draft. Draft implementations might not work properly between different manufacturers or with standards compliant equipment once the standard has been confirmed.
802.11i	802.11i is a security amendment that has been ratified by the IEEE and is now part of the 802.11-2007 standard. 802.11i mandates the use of strong authentication and authorization via 802.1X/EAP (Extensible Authentication Protocol) – Enterprise or Pre Shared Key – Soho (small office/home office) use. Enhanced Data Privacy is addressed with the use of a strong encryption method called Counter Mode with Cipher Block Chaining Method Authentication Code Protocol (CCMP) using Advanced Encryption Standard (AES). The Supplement also defines the optional use of Temporal Key Integrity Protocol (TKIP) using the RC4 cipher for older clients that do not support AES.
802.1X	IEEE 802.1X-2004 is a port based access control standard that allows or disallows traffic to pass through a port and therefore access network resources. When implemented with Wireless LAN the 802.1X authentication framework uses an Extensible Authentication Protocol (EAP) type with an authentication server to provide strong mutual authentication between the client and authentication server via the Wireless Infrastructure. In this mode, each user is assigned a unique key mechanism for access to the WLAN. This affords a high level of individual privacy. For WPA, TKIP encryption is used. For WPA2, AES encryption is used. AES is stronger than TKIP, thus providing additional network protection.
AAA **A**uthentication **A**uthorisation **A**ccounting	Common terms used to describe security infrastructure. These are three services commonly provided by a directory service. Authentication is the process of determining, with some agreed level of confidence, the current user of a wireless device. Often it is desirable to authenticate the user of the device. Alternatively, authentication can be applied to the device itself. Authorisation determines what the authenticated user or device is allowed to do on the network. For a small school, it might be sufficient simply to give each wireless device the same network access as a wired device. A school with a larger, or more complicated, network might provide different access depending on who the user is. Accounting is the tracking of network resource usage by end users to assist will capacity planning, billing etc. A school security solution will generally have some way to measure how much use is made of various services provided on the network.

Term, Acronym, or Abbreviation	Definition
AES	Advanced Encryption Standard AES is a strong block cipher used to encrypt 802.11 Wireless Data. AES uses CCMP and encrypts data in fixed blocks with the choice of 128, 192 and 256 bit keys. AES is a mandatory part of the 802.11i security standard and is stronger and more efficient than older TKIP based on RC4.
Air Time Fairness	Airtime fairness is a technique used to reduce the impact the slowest clients on a wireless network have in slowing down other users by reducing the number of opportunities the slow clients have to transmit data. On a wireless network, once a client (or AP) starts to transmit a wireless frame, all other wireless devices on the same channel must wait until the transmission is finished before they can transmit. If a device is transmitting, the period of time that another device needs to wait before trying to transmit is determined by the size of the frame being transmitted and the transmit and receive data rates between the client and its AP. For example, a wireless frame transmitted to or from a client connected at a low data rate may utilize 10 milliseconds of airtime, whereas it may take only 100 microseconds for a client connected at a high data rate, so the high speed client could have sent 100 frames in the time the slow client takes to send one frame. Unfortunately this means that a single low speed client can slow down all of the other clients on the WLAN. The traffic to the lower speed client consumes much more airtime than the faster client and prevents the fast client from benefiting from its higher data rate. The 802.11 standards allow for all wireless devices within range and on the same channel to compete equally for an opportunity to transmit a data frame, so a fast client can spend most of its time sitting idly waiting for a slow client to finish transmitting a frame so they can have another chance to transmit. With airtime fairness, the 802.11 standard of equal opportunity for all clients is not used; rather the wireless system dynamically determines the exact amount of airtime each client is consuming in microseconds. It then adjusts the number of opportunities each client gets to transmit using algorithms that account for each client's characteristics, such as current throughput, distance from the AP etc. As a result slower clients get fewer opportunities to transmit than faster clients. This results in improved speeds for the faster client with little or no impact on the slower client. Note that airtime fairness does not form part of the 802.11 standards. Not all vendors support airtime fairness and those that do have different methods of deploying it.
Anywhere, any-time, computing.	An expression sometimes used to refer to the increased portability of computing devices and services.
Band Steering	Some wireless vendors have developed band steering. This is the ability for an access point to offload a client from one radio to another based on the client's capabilities. E.g. an 802.11n capable client may be offloaded to a 5Ghz radio to ensure maximum performance for that client and to reduce the likelihood of the 2.4Ghz radio becoming overloaded.

Term, Acronym, or Abbreviation	Definition
Beamforming	Beamforming was first supported in the 802.11 standards in 802.11n and was refined in 802.11ac. It is a technique that focuses the power of the wireless signal sent out by a transmitting device in the direction of the receiving device. Beamforming improves both range and throughput. Typically 802.11 AP radios radiate the wireless signal from the antenna evenly in all directions (like the ripples in a pond when a stone is thrown in) so the signal coverage map is a circle. With beamforming, the radio has two or more antennae and by changing the phase difference between the signal being sent from each antenna it is possible to focus the radio power in the direction of the client (radio waves, like all other waves, from two or more different sources create interference patterns when they meet, and this can increase or decrease the amplitude of the resulting wave). This results in a coverage map that is not a circle, but instead has a lobe (or lobes). APs that support beamforming typically modify the antenna phase differences electronically each time the AP communicates with a new client – and also changes the phase differences dynamically as the client physically moves about during the communication session, so the coverage map for the AP can be continuously changing. Beamforming is either ***explicit*** or ***implicit***. Explicit beamforming is where the AP and client work together by sharing information on the radio channel characteristics to modify the radio signal for best performance, so both the AP and client must have beamforming capability. Implicit beamforming is when only the AP has beamforming capability and it decides the best way to modify the signal based on dropped data packets. Explicit beamforming has the advantage of better performance but has the disadvantage that it will not work unless both the AP and client support the same version of beamforming. Implicit beamforming has the advantage that as long as the AP has beamforming capability it will work with any client, but has the disadvantage of not having the same level of performance as explicit beamforming. Beamforming was first supported in 802.11n which defined several optional methods for explicit beamforming. Explicit beamforming requires both the AP and client to support the same beamforming method and since the 802.11n standard had several optional methods, the market did not standardise on any method and so beamforming was not widely deployed (although some vendors did provide APs that had proprietary implicit beamforming). With 802.11ac implementing beamforming on devices is still optional for manufacturers, but if implemented a single beamforming method is prescribed so it is likely to become ubiquitous.
Bring Your Own Device (BYOD) (or Bring Your Own Technology BYOT etc.)	Often used to refer to an environment (e.g. school or workplace) that provides wireless network access of some sort (typically carefully secured internet) for people to use with privately owned devices such as laptops, netbooks, iPads, tablets and smartphones.

Term, Acronym, or Abbreviation	Definition
BSS	Basic Service Set Part of the 802.11 standard service set – the Basic Service Set refers to the communication between a single wireless access point and a wireless station.
Building backbone cabling	Cable that connects the building distributor to a floor distributor.
Building distributor	A device (typically a 10/100 Mbps or 1Gbps switch) that is the connection point to the campus backbone and connects (distributes) to all floor distributors
Campus	A facility with two or more buildings in a relatively small area e.g. a school.
Campus backbone cabling	Cable that connects the campus distributor to the building distributor(s).
Campus distributor	A device (typically a gigabit Ethernet switch) that is the central point for a campus (or school) network. The campus distributor connects to the external telecommunications network and also interconnects all the campus buildings (via "campus backbone cabling" to each of the "building distributors")
Captive Web Portal	A Captive Web Portal is used to capture a users HTTP request and redirect to a specific webserver for such purposes as Authentication, registration or Policy acceptance. CWP are largely used for hotspots and guest networks (e.g. in airport terminal lounges)
Category 5 (Cat 5)	A definition of cabling components that provides AS/NZS 3080 class d performance.
Category 5e	Any reference to category 5e shall be interpreted as category 5.
Category 6 (Cat 6)	A definition of cabling components that provides AS/NZS 3080 class e performance.
CCMP	Counter Mode with Cipher Block Chaining Method Authentication Code Protocol (CCMP) is the default encryption method defined in 802.11i amendment. CCMP uses AES encryption and uses 128bit encryption in fixed length blocks. An 8 Byte Message Integrity Check (MIC) is used to ensure data integrity.

Term, Acronym, or Abbreviation	Definition
Channel	Each frequency range used by 802.11 wireless (2.4GHz and 5GHz) is split into channels each of which a subset of the frequency range. For example, the 2.4GHz band (used in 802.11b, g, and optionally n) is divided into 14 channels. The frequency (mid-point) of each 2.4GHz channel is 5MHz away from the frequency of the next channel (with the exception of channel 14 which is 12MHz away from channel 13). **2.4GHz Channels** Not all 2.4GHz channels are permitted to be used under local regulations in many countries. In most of the world (including NZ) channel 14 is not permitted, and in the US channels 12, 13 and 14 are not permitted. As a result, some wireless equipment from US vendors does not support channels 12, 13 and 14. For this reason it is strongly recommended that channels 12 and 13 are not used in schools as some user devices may have these channels disabled. Since the 802.11g and n protocols require a 20MHz channel width, adjacent channels overlap and cause interference with each other. To overcome this, it is recommended that only channels 1, 6 and 11 be used as they do not overlap. **5GHz Channels** In the 5GHz frequency range there are far more channels specified in the IEEE standards, but again the allowable channels varies by country. The 5GHz channels that are permitted in most countries are typically 20MHz apart so there is no channel overlap using 802.11n in the lower speed 20MHz mode, but if channel bonding is used for higher speed a 40MHz channel is needed so there are issues with channel overlap. With 802.11ac the channel width required can be up to 160MHz for the fastest data speeds, so channel overlap becomes a significant design consideration.

Term, Acronym, or Abbreviation	Definition
Channel Bonding	Channel bonding is a technique where adjacent contiguous 20MHz wireless channels are combined into a wider channel to enable higher data rates. Channel bonding is typically only used in the 5GHz range as there are insufficient non-overlapping channels available in the 2.4GHz range. **802.11a,b and g Channel Bonding** 802.11a, b and g do not support channel bonding. **802.11n Channel Bonding** 802.11n supports bonding of two adjacent 20MHz channels to form a 40MHz channel. **802.11ac Channel Bonding** 802.11ac supports bonding of adjacent 20MHz channels to form 40MHz, 80MHz and 160MHz channels. The 160MHz channels can be either two adjacent 40MHz channels or an “80+80” configuration where two non-adjacent 80MHz channels are bonded together.
Data Link Layer	The Data Link Layer is the 2nd layer of the OSI model. Its function is to provide reliable transit of data across a link between two devices. The data link layer groups the stream of bits of information being transmitted into units called “frames” (e.g. an Ethernet frame), adds checksums to the frames so the receiver can ensure the frame has been received without errors (if the checksum does not match it is discarded), provides an acknowledgement back to the sender that the frame was correctly (or incorrectly) received, and provides flow control to ensure a fast sender does not overwhelm a slow receiver. In most school networks the data link layer function will be performed by the network interface adapter (which also manages the physical layer).

Term, Acronym, or Abbreviation	Definition
Data Rate	Data rate is the rate that data is transmitted over a link and is measured in bits per second (bps) or bytes per second (Bps). A 1 Bps data rate is the same as an 8bps rate (1 Byte = 8 bits). The 802.11 standards determine maximum data rates (e.g. 802.11a has a maximum data rate of 54Mbps). These maximum data rates are a theoretical maximum only and actual throughput in practice is significantly less due to network and security overheads, interference, distance, obstacles and user congestion. An AP with a single client and good real world conditions will typically have a throughput between half and two-thirds of the maximum data rate. With two clients trying to simultaneously transfer large files through the same AP, this throughput per client would typically be halved, and quartered for 4 clients. **802.11b Data Rate** The maximum data rate for 802.11b is 11 Mbps. **802.11a and g Data Rate** The maximum data rate for 802.11a or g is 54 Mbps on a 20MHz channel. **802.11n Data Rate** The maximum data rate for 802.11n depends on the number of MIMO streams used (can be 1 – 4) and on the channel width used (can be 20MHz or 40MHz). For a 20MHz stream the maximum data rate is 70 Mbps while for a 40MHz stream it is 150 Mbps. So for 4 streams over a 40MHz channel the maximum combined data rate is 600 Mbps. **802.11ac Data Rate** The maximum data rate for 802.11ac depends on the number of MIMO streams used (Wave 1 can have 1 - 4 streams and Wave 2 can have 1 - 8) and on the channel width used (Wave 1 can be 20MHz, 40MHz, or 80MHz and Wave 2 includes 160MHz). For a 20MHz stream the maximum data rate is 96 Mbps, for a 40MHz stream it is 200 Mbps, for an 80MHz stream it is 433 Mbps and for a 160MHz stream it is 867 Mbps. So the maximum combined data rate for a Wave 1 AP with 4 streams over an 80MHz channel is 1.73 Gbps and the maximum combined data rate for a Wave 2 AP with 8 streams over a 160MHz channel is 6.93 Gbps.
Device	In the context of this document, the term ‘device’ refers to any equipment that is part of a wireless or wired network. This can include a router, switch, PC, laptop computer, netbook, tablet, iPod, smartphone, PSP console, or any one of many other types of equipment.

Term, Acronym, or Abbreviation	Definition
Directory Service	A directory service is a network-based service that can maintain information about all network users and devices, and provides that information to devices on the network with appropriate security (see AAA). Directory services in common use are Microsoft's Active Directory (AD), Apple Open Directory, Novell eDirectory, various Linux options, or possibly an externally provided secure Identity and Access Management (IAM) service.
DSSS	Direct Sequence Spread Spectrum (DSSS) is a technique originally developed for military use to make wireless signals more secure and less susceptible to interference and jamming. The original signal is multiplied with pseudo random noise resulting in a scrambled signal that appears to be just noise. 802.11b uses DSSS
EAP-TLS	EAP-TLS is an EAP (Extensible Authentication Protocol) method from Microsoft used in the 802.1X authentication framework. EAP-TLS requires a client side digital certificate. The digital certificate is used for identity validation instead of User Name or Password. Digital Certificates are considered a strong form of authentication as they can be marked as non-exportable and therefore difficult to forge.
EMC	EMC (electromagnetic compatibility) is the ability of electronic components and devices to work correctly when they are close together without being impacted by EMI. Typically it means limiting the electromagnetic disturbances from devices that generate EMI and having an adequate level of immunity in devices that are exposed to EMI
EMI	EMI (electromagnetic interference) is the electrical disturbances caused by rapidly changing electrical currents. High frequency EMI is often called RFI. Wireless networks are susceptible to high frequency EMI.
Encryption	The process of transforming data using an encryption cipher in order to render the data stream unreadable except with the key.
Floor distributor	A device (typically a 10/100 Mbps or 1Gbps switch) that is the connection point to the building backbone and connects (distributes) to data outlet ports in rooms
Frequency Ranges used by IEEE Wireless Standards	The frequency range is a key characteristic of a wireless standard, and is the mid-point of a range of radio frequencies used by that standard. The '2.4GHz' frequency range is used by 802.11b, g, and (optionally) n standards. The 5 GHz frequency range is used by 802.11n and ac.
Gbps	Gigabits per second
Horizontal cabling	Cable connecting the floor distributor to the telecommunications outlets (wall data ports).
ICT	Information and Communication Technology
IEEE	IEEE (Institute of Electrical and Electronics Engineers) is the world's largest professional association dedicated to advancing technological innovation and excellence for the benefit of humanity. IEEE and its members inspire a global community through IEEE's highly cited publications, conferences, technology standards, and professional and educational activities.

Term, Acronym, or Abbreviation	Definition
IP	Internet Protocol – A Layer 3 Protocol that allows the assignment of IP addresses to devices in a network for routing purposes.
IPv4	IPv4 is the most widely used version of the Internet Protocol. It defines IP addresses in a 32-bit format, which looks like 123.123.123.123. Each three-digit section can include a number from 0 to 255, which means the total number of IPv4 addresses available is 4,294,967,296 (256 x 256 x 256 x 256 or 2^32).
IPv6	IPv6, also called IPng (or IP Next Generation), is the next planned version of the IP address system. While IPv4 uses 32-bit addresses, IPv6 uses 128-bit addresses, which increases the number of possible addresses by an exponential amount. For example, IPv4 allows 4,294,967,296 addresses to be used (2^32). IPv6 allows for over 340,000,000,000,000,000,000,000,000,000,000,000,000 IP addresses.
IETF	The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The IETF Mission Statement is documented in RFC 3935.
IPSec	IP Security, a set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPSec has been deployed widely to implement VPNs
ITIM Framework Information Technology Investment Management Framework	A framework developed by the United States General Accounting office, it can be used for both assessing the maturity of an organisations investment management process and as a tool for organisational improvement. http://www.gao.gov/new.items/d04394g.pdf
L2TP	The Layer Two Tunneling Protocol (L2TP) provides a dynamic mechanism for tunneling Layer 2 (L2) "circuits" across a packet-oriented Layer 3 data network (e.g., over IP). L2TP, as originally defined in RFC 2661, is a standard method for tunneling Point-to-Point Protocol (PPP) [RFC1661] sessions. L2TP has since been adopted for tunneling a number of other L2 protocols. L2TP is largely used with VPN access technologies.
Load Balancing	Often in a wireless network, many users will unknowingly be connected to the same AP, or even the same radio on the same AP, while neighbouring APs may be underutilised. This can have a significant impact on client performance and may cause users to have an unsatisfactory experience. It is logical, therefore, that clients be encouraged to move from the more heavily loaded APs to the lightly loaded ones. Some wireless vendors have developed load balancing to optimise the distribution of clients among access points.
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Control, a hardware address that uniquely identifies each node of a network
Mbps	Megabits per second

Term, Acronym, or Abbreviation	Definition
Ministry	Ministry of Education.
MIMO and MU-MIMO	MIMO (multiple-input and multiple-output) is a technique that uses multiple antennae and radios in wireless devices to exploit multipath propagation so that multiple wireless data streams can be sent/received simultaneously over a single channel. MIMO was first introduced in 802.11n. Both 802.11n and 802.11ac Wave 1 permit up to 4 simultaneous data streams over a single channel and they can only be used for a single client at a time. 802.11ac Wave 2 devices will support up to 8 data streams over a single channel and the streams may be sent to multiple clients simultaneously – a technique called multi-user MIMO (MU-MIMO)
MOE	Ministry of Education
Network-Based Applications and Services	Applications include Student Management Systems, Learning Management Systems, financial systems, ePortfolio, email, etc. Services include file storage, printing etc.
NIC	A NIC (Network Interface Controller) is a computer hardware component that connects a computer to a data network. The most common network protocol supported by NICs today is Ethernet.
NMS	An NMS (Network Management System) is a combination of hardware and software used to monitor, report on and administer a network.
PCI	PCI (Peripheral Component Interconnect) is a local bus standard developed by Intel Corporation for attaching hardware devices (typically PCI cards) to a computer.
PCMCIA	PCMCIA (Personal Computer Memory Card International Association) is a standard for small, credit card-sized devices, called PC Cards to connect to computers to add functionality
PEAP-TLS/MS-CHAP	Protected EAP is a Microsoft EAP method that uses TLS to provide an outer tunnel that is mutually validated prior to user credentials being submitted to the authentication server. PEAP-TLS uses a Digital Certificate for user identification; PEAP-MS-CHAP uses User Names and Passwords.
PKI	PKI (Public Key Infrastructure) is mechanism to enable users of a basically unsecure public network such as the Internet to securely and privately exchange data (and money) through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. PKI provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.
PoE	PoE (Power over Ethernet) is a network standard for sending DC power over data cabling to provide power for networked devices. The first PoE standard (IEEE 802.3af) provided up to 15 watts for a device. A new standard (IEEE 802.3at-2009) provides for up to 30 watts per device.
P2P	Point to Point

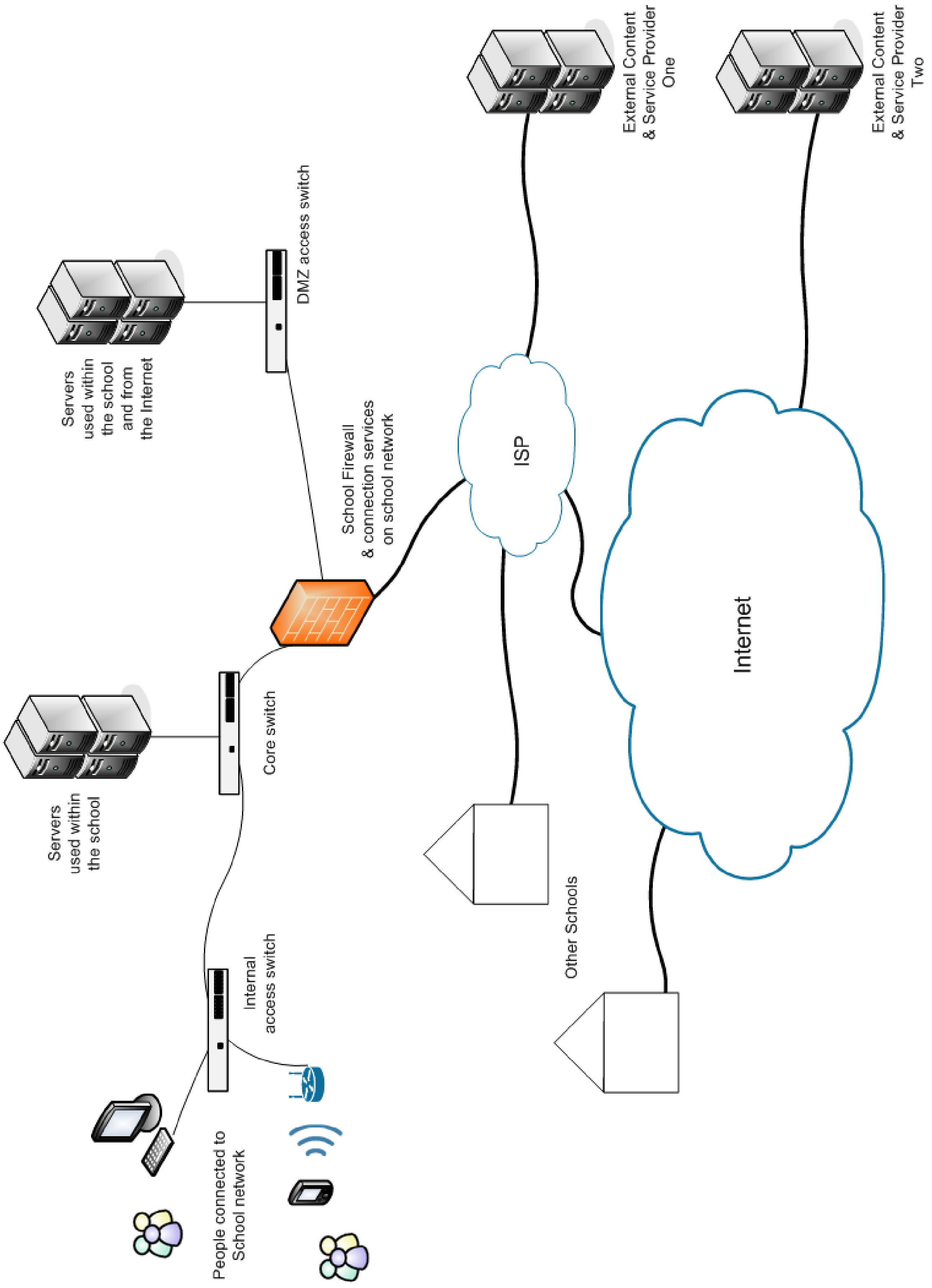
Term, Acronym, or Abbreviation	Definition
PPTP	The Point-to-Point Tunnelling Protocol (PPTP) is the most widely supported VPN method among Windows clients. PPTP is an extension of the Internet standard Point-to-Point protocol (PPP), the link layer protocol used to transmit IP packets over serial links. PPTP uses the same types of authentication as PPP (PAP, SPAP, CHAP, MS-CHAP v.1/v.2 and EAP).
P2P	Point to Point
PSK	PSK (Pre Shared Key) is a shared secret (passphrase or “key”) that has been shared using some secure method by two parties prior to the key being used. A PSK typically needs to be entered into a device in order to authenticate to an AP.
QoS	QoS (Quality of Service) is the ability to provide different priorities to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. QoS is important if the network becomes congested, especially for real-time streaming multimedia applications such as voice over IP, online games realtime video, since these are delay sensitive.
RADIUS	RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralised AAA management for devices to connect and use a network service.
RC4	RC4 is a streaming cipher used in SSL as well as 802.11 Wireless LAN WEP and TKIP.
RF	Radio frequency
RFI	RFI (Radio Frequency Interference) is high frequency EMI. Wireless networks are susceptible to RFI at certain frequencies.
RFP	Request For Proposal
Roaming	The ability for client devices to seamlessly transition from one AP and BSS to another (e.g. when moving from one location to another) while maintaining network connectivity for upper layer applications.
SFP	Small Form-factor Pluggable (connector)
SNMP	Simple Network Management Protocol
SNUP	School Network Upgrade Project http://www.minedu.govt.nz/snup
SSID	SSID (Service Set Identifier) is a 32-character unique identifier for a WLAN. To communicate, all wireless devices (APs and end user devices) on a specific WLAN must use the same SSID.
Structured Cabling System	A set of cabling and connectivity products that are constructed according to standardised rules to facilitate integration of voice, data, video, and other signals.
TCP/IP	Transmission Control Protocol/Internet Protocol are two protocols developed in the early days of the Internet by the U.S. military. TCP is associated with the assembling of data into packets and verifying delivery of the packets while IP is associated with the address part of each data packet so it gets to the correct destination. TCP/IP has become the foundation of the Internet. TCP/IP software is built into all major operating systems, such as Unix, Windows, and the Mac OS.

Term, Acronym, or Abbreviation	Definition
TDM	TDM (Time Division Multiplexing) is the process of combining multiple sources of data into one larger stream of data by allocating a time period to each source.
TKIP	TKIP (Temporal Key Integrity Protocol) is an enhancement to WEP encryption designed to address the weakness of WEP. TKIP mandates dynamic keys and Message Integrity Check (MIC) however it is still based on the RC4 cipher and offers lower performance.
TO	Telecommunications Outlet (typically a wall data port)
Traffic Separation	Network traffic from wireless devices can be combined with wired traffic, however, security can be improved by treating different types of traffic in a way that is appropriate for each type. Common criteria are the degree to which the device generating traffic is known and trusted, and any special requirements of that type of device. Traffic separation is usually implemented by the use of VLANs. Categories of traffic might include: • Standard data traffic including staff • Other school-owned devices • Visitor wireless access • Student wireless access (BYOD) • Management of network devices • VoIP Phone connections • Streaming video, or video conferencing • Security cameras
Unique Per User Pre Shared Key	Unique PSKs are unique WPA/2 PSKs created for each individual user/device on the same SSID. They offer the key uniqueness and policy flexibility that 802.1X provides with the simplicity of WPA/2-PSK.
UPS	Uninterruptible Power Supply
UTP	Unshielded Twisted Pair
Virtual Server	Software that provides services on a network in the same way as a physical server. Multiple virtual servers can share the resources of one physical server.
Visitors	In this document, a visitor is anyone who might use a wireless network, but is not on the school staff, or regularly at the school. The implication is that these people will be welcome to use the school wireless Internet, but not other school network services such as file storage, or printing. Examples might be parents, students from other schools attending technology classes, Ministry of Education or ERO visitors, and contract workers. In a wider context, the term ‘guest’ is often used with a similar meaning when discussing wireless networks.
VLAN	A VLAN (Virtual Local Area Network) is a virtual network created within software on network switches. Multiple VLANs can share a single physical cable but are effectively separate networks. VLANs are typically used for traffic separation
VoIP	Voice over Internet Protocol

Term, Acronym, or Abbreviation	Definition
VPN	A VPN (Virtual Private Network) is secure (encrypted) private network created over any other (often unsecure) network.
AP	Wireless Access Point
WEP	WEP (Wireless Equivalent Privacy) is a Layer 2 encryption method that uses the RC4 streaming cipher. The original 802.11 standard defined 64 and 128 bit keys. WEP should not be used, as it is relatively easy to “crack”.
Wi-Fi	Wi-Fi (Wireless Fidelity) is used generically to refer to any type of 802.11 network
Wi-Fi Alliance	A non-profit organisation that tests manufacturers’ 802.11 devices for compliance with the IEEE standards. Devices that pass testing are certified and are permitted to display the trademarked “Wi-Fi Certified” logo.
Wireless Station	All components connected into wireless networks are referred to as wireless stations. All stations are equipped with a WNIC
WLAN	Wireless Local Area Network
WNIC	Wireless Network Interface Controller
WNMS	Wireless Network Management System
WPA2	WPA2 (Wi-Fi Protected Access 2) is a standards-based wireless security specification. It is often implemented with EAP for authentication and integrity checking and with TLS to provide encryption.
WPA2 Enterprise	Used to describe WPA2 implemented using a directory service, specifically a RADIUS server.
WPA2 Personal	The simpler way of implementing WPA2 is with a shared key, where each wireless device uses the same key. This essentially means the device is authenticated, rather than the user.

10 Appendix D - Typical School Network End to End Diagram

Note: Where Network for Learning (N4L) is available for a school's internet connection, a web and application layer firewall and content filtering system is available through the cloud on an opt-in basis. This could reduce infrastructure complexity and ongoing costs for the school by obsolescing the requirement to purchase and manage these systems independently


People connected to School network
Internal access switch
Servers used within the school
Core switch
School Firewall & connection services on school network
Servers used within the school and from the Internet
DMZ access switch
Other Schools
ISP
Internet
External Content & Service Provider One
External Content & Service Provider Two

11 Conclusion

Thank you for reading the School Wireless LAN Guidelines 2015 - Building and Maintaining a wireless network. We hope you have found these documents useful and that they have met their aim of informing on best practice solutions for deploying wireless LAN in schools.   However, every school and campus is unique. Be sure to plan well and discuss your specific requirements with either your RFP consultant or your integrator to ensure the schools needs are clearly understood and addressed.