MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

# Technology in Schools

## Recommended Specifications for School Wireless LAN Systems

**Version 2.2**

**May 2015**

## Table of contents

# 1 INTRODUCTION

## 1.1 Instructions

This document serves to inform vendors, wireless system integrators and schools of the recommended technological specifications when selecting a wireless network product suite.

It is best used in conjunction with the following documents;

School WLAN Guidelines – Understanding WLANs
School WLAN Guidelines – Build and Maintain WLANs

Which can be found at www.education.govt.nz/ict-standards

# 2 SYSTEM OVERVIEW

**The proposed system should be:**

a) From a single vendor.
b) A purpose-built managed wireless system. No PC-based open source solutions are acceptable.

**The proposed system should have at a minimum:**

c) The ability to support 802.11ac 5GHz and 802.11ng 2.4GHz MIMO
d) The ability to display users, laptops and general location of devices on a management console.
e) The functionality to support all current wireless standards including the older 802.11a/b/g and the 802.11n standard in both the 2.4 & 5.0GHz bands.
f) The ability to initiate rate limiting of individual SSIDs or user profiles (if individual user profiles are available on the management interface).
g) The ability to configure time-based access policies is a requirement for any compliant solution e.g. Student WLAN operates only between 8:30am – 3:30pm and Staff WLAN operates 24/7.
h) The ability to support various levels of QoS, at a minimum, 802.1p and DiffServ.
i) Access Points rated for 802.3af and/or 802.3at Power over Ethernet and defined in the response matrix.

**The proposed system should support or provide the following:**

j) A wireless system with a centralised (on or offsite) controller, management system or both.
k) Dual Concurrent Radio 3x3:3 MIMO (in both 2.4GHz and 5GHz) Access Points at a minimum.
l) Options for fibre interface, N+1 redundancy on the controller interfaces (if applicable).
m) High Availability functionality for controller-based solutions.

n) VLAN support.
o) Up to 8 SSIDs per radio to support tiered service architecture.
p) A.D, RADIUS, eDirectory, LDAP and/or Open LDAP integration for secure client logon.
q) Individual Guest Access for school visitors.
r) Individual Pre-Shared Keys per user to allow for user tracking on the network.

# 3 PERFORMANCE

## 3.1 Air Interface

| Item # | System Feature | Importance |
|---|---|---|
| 3.1.A | Conforms to all current applicable air interface standards for Wi-Fi including 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac | Mandatory |
| 3.1.B | The WLAN system access points and controller (if applicable) must carry the Wi-Fi Alliance Wi-Fi interoperability certification at a minimum for IEEE 802.11a, 802.11b, 802.11g, 802.11n and 802.11ac. If the certificate is 'in process' the vendor must state where the company is in the process and what sections are completed. It is not sufficient that a vendor's product be a member of the Wi-Fi alliance | Mandatory |
| 3.1.C | If some of the vendor's products are certified but not the product(s) being put forward the vendor must supply a letter stating the reasons why that product(s) is not certified | Mandatory |
| 3.1.D | Conformance to the radio spectrum policies for spread spectrum devices operating in the 2.4 GHz band and 5 GHz bands. Please state all applicable certifications relevant to NZ so that your product complies with government regulations for radio transmitters and electromagnetic interference | Mandatory |
| 3.1.E | Frame aggregation support (MSDU/MPDU) | Mandatory |

## 3.2 Access Points

The desired outcome should be to integrate a wireless solution that is capable of performing to the highest level possible and as such, 3x3:3 units are seen as the de facto AP baseline of performance.

| Item # | System Feature | Importance |
|---|---|---|
| 3.2.A | Each access point shall have a minimum of two radios able to operate concurrently, one radio assigned to 2.4GHz operation, the other radio to 5GHz operation. Access points with a single radio covering both bands are not acceptable | Mandatory |
| 3.2.B | The access point must support 802.11ac operation in the 2.4GHz and 5GHz bands concurrently | Mandatory |
| 3.2.C | Load balancing between:<br>➢ Access Points<br>➢ 2.4GHz & 5GHz radios on any given AP | Mandatory |
| 3.2.D | Up to 8 SSIDs per radio to support tiered service architecture | Mandatory |
| 3.2.E | AP Meshing – ability to expand or bridge network via AP Meshing. Confirm if your 802.11ac compliant product supports this feature | Highly Desirable |
| 3.2.F | AP Meshing – ability to self-heal and auto-fail in the event of LAN link loss | Mandatory |
| 3.2.G | Beam forming – specify current provisions, whether it's chip or antenna based, and if your system beam forming is considered unique or proprietary | Highly Desirable |
| 3.2.H | Antenna signal gain (specify dB value and band) | Mandatory |
| 3.2.I | Auto-channel selection | Mandatory |
| 3.2.J | Additional features such as MRC and CDD (specify additional features in your matrix response) | Highly Desirable |
| 3.2.K | Distributed intelligence (i.e. Fat APs) | Highly Desirable |
| 3.2.L | Adaptive resource management (i.e. air time allocation) to fairly manage legacy and current client devices | Highly Desirable |
| 3.2.M | Omni-directional antennae | Highly Desirable |

| | | |
|---|---|---|
| 3.2.N | Band Steering ability based on client | Mandatory |

### *3.3* 3x3:3

Must support all other features unless specifically indicated:

| Item # | System Feature | Importance |
|---|---|---|
| 3.2.1.A | The number of antennas per radio must be 3x3 MIMO minimum | Mandatory |
| 3.2.1.B | The number of spatial data streams per radio must be three (for 1300Mbps at 5GHz and 450mbps theoretical throughput per 2.4GHz radio) | Mandatory |
| 3.2.1.C | Access Points must be capable of running 3x3 MIMO concurrently on both radios | Mandatory |

### 3.4 WLAN Roaming

| Item # | System Feature | Importance |
|---|---|---|
| 3.3.A | User equipment should be able to seamlessly roam from one area to another and one access point to another fast enough to provide a voice conversation on a Wi-Fi connection, inside the specified coverage zones | Mandatory |
| 3.3.B | Must provide intelligent support for clients that do not support roaming tendency settings, or are either too “sticky” or too “loose” with their AP association | Mandatory |
| 3.3.C | Users should not have to reconnect to the network when they roam from one area to another within the school coverage zones | Mandatory |
| 3.3.D | Laptops shall not have to re-authenticate as they move from access point to access point | Mandatory |

### 3.5 Controller

| Item # | System Feature | Importance |
|---|---|---|
| 3.4.A | High availability feature via secondary controller | Highly desirable |
| 3.4.B | Ability to share license blocks between multiple controllers | Highly desirable |

# 4 SYSTEM FEATURES

## 4.1 VLAN & Policy Support

| Item # | System Feature | Importance |
|---|---|---|
| 4.1.A | The wireless controller (if required) and access points must provide IEEE 802.1q VLAN support | Mandatory |
| 4.1.B | The solution must be able to support all existing VLANs in the air without changing any existing router configurations, adding any new routing protocols to the network, or modifying any client configurations | Mandatory |
| 4.1.C | Enforcement of VLANs via WLAN management policies | Mandatory |
| 4.1.D | Enforcement of existing network policies including access control lists (ACLs), class of service (CoS), quality of service (QoS) and routing policies. | Mandatory |
| 4.1.E | The WLAN system is required to isolate user-to-user traffic, even if they are on the same VLAN on the same AP or across multiple APs | Mandatory |

## 4.2 Ethernet Support

| Item # | System Feature | Importance |
|---|---|---|
| 4.2.A | Access points and controllers must comply with IEEE 802.3 10/100/1000 Ethernet | Mandatory |
| 4.2.B | The connection between the access point and the controller (if applicable) and or the Ethernet network must comply with 802.3 specifications. Proprietary line protocols are not acceptable as access points must interface with school Ethernet switching equipment | Mandatory |

## 4.3 Traffic Management

| Item # | System Feature | Importance |
|---|---|---|
| 4.3.A | Ability to choose traffic pathways e.g. all traffic tunnelled via controller (if applicable), or direct to gateway from AP | Mandatory |
| 4.3.B | Should support a minimum of 30 concurrent clients on a single multicast stream per AP | Mandatory |

# 5 SECURITY

A significant requirement is the breadth of security measures supported by the proposed WLAN system. The following requirements are designed to determine standards adherence, the range of security protocols supported and future-proofing of the system.

## 5.1 Encryption

| Item # | System Feature | Importance |
|---|---|---|
| 5.1.A | The WLAN system at a minimum must support the following encryption types:<br>a. WEP with 64-bit and 128-bit encryption<br>b. WPA/WPA2 (TKIP and AES-CCMP) with pre-shared keys<br>c. WPA/WPA2 (TKIP and AES-CCMP) with 802.1X.<br>d. **The vendor must also state any client number limitations that exist per AP for each encryption method** | Mandatory |
| 5.1.B | The catch-all encryption requirement is that the WLAN system must comply with 802.11i in addition to the above. Wi-Fi alliance certification is required for WPA/WPA2 and the above authentication methods | Mandatory |

## 5.2 Authentication

| Item # | System Feature | Importance |
|---|---|---|
| 5.2.A | The WLAN system must support IEEE 802.1x authentication | Mandatory |
| 5.2.B | The WLAN System should have a RADIUS proxy function available | Mandatory |
| 5.2.C | The WLAN system must support MAC-based authentication | Mandatory |
| 5.2.D | The WLAN system must support web-based authentication (captive portal) | Mandatory |
| 5.2.E | The WLAN system must support the following Extensible | Mandatory |

| Item # | System Feature | Importance |
|---|---|---|
| | Authentication Protocols (EAP): EAP-TLS, EAP-TTLS PEAPv0-MSCHAPV2, and PEAP-TLS | |
| 5.2.F | The WLAN system must support bonded authentication, tying the device together with the authenticated user | Highly Desirable |
| 5.2.G | Device OS fingerprinting – ability to offer network features based on device OS | Highly Desirable |
| 5.2.H | Authentication mechanisms used by schools vary greatly; at a minimum vendor's solutions must be able to authenticate against:<br>i. RADIUS (Window and open source versions)<br>ii. A.D<br>iii. LDAP<br>iv. OpenLDAP<br>v. eDirectory | Mandatory |

## 5.3 Wireless Intrusion Protection, Detection (WIP/WID) & Counter Measures

| Item # | System Feature | Importance |
|---|---|---|
| 5.3.A | Active background rogue AP detection service, with automated emails to the administrator upon identification | Highly Desirable |
| 5.3.B | Stateful Firewall | Highly Desirable |
| 5.3.C | Implement counter-measures to address rogue APs | Highly Desirable |
| 5.3.D | Ability to identify and disable Peer-2-Peer networks | Highly Desirable |

## 5.4 End Point Integrity Checking – Network Access Control

| Item # | System Feature | Importance |
|---|---|---|
| 5.4.A | Product contains NAC functionality, or can integrate with a NAC solution | Highly Desirable |
| 5.4.B | Part of a certified partner program with a NAC device. Please provide details | Highly Desirable |
| 5.4.C | Does your NAC solution use a software agent or is it an agent-less solution? | Highly Desirable |
| 5.4.D | Remediation via quarantine or captive portal | Highly Desirable |

## 5.5 Guest Access & Control

| Item # | System Feature | Importance |
|---|---|---|
| 5.5.A | Ability to generate and manage guest users on the network via unique Pre-Shared Keys | Highly Desirable |
| 5.5.B | Captive portal available | Mandatory |
| 5.5.C | Network Address Translation protocol for deployment in Proxy/TMG server environment (or statement of how your system deals with Proxy/TMG server) | Highly Desirable |

# 6 SCALABILITY

## 6.1 Expansion

| Item # | System Feature | Importance |
|---|---|---|
| 6.1.A | Linear licensing mechanism that allows 1:1 purchasing of Access Points and Licenses | Highly Desirable |
| 6.1.B | “Plug and play” approach that allows end users to plug in new Access Points and pick up configurations automatically | Highly Desirable |
| 6.1.C | Ability to set up branch offices with the Access points? | Highly Desirable |

## 6.2 IPv6 Support

| Item # | System Feature | Importance |
|---|---|---|
| 6.2.A | IPv6 support is mandatory in both the controller (if applicable) and Access Points | Mandatory |

# 7 MANAGEMENT

The WLAN solution will provide a wireless management interface for Moves/Adds/Changes as well as WLAN network wide monitoring.

## 7.1 WLAN Management Software

| Item # | System Feature | Importance |
|---|---|---|
| 7.1.A | Visibility and management of all WLAN equipment: Controller and Access Points | Mandatory |
| 7.1.B | Web GUI | Mandatory |
| 7.1.C | Visibility of WLAN users and their devices on the network | Mandatory |
| 7.1.D | Visibility of WLAN users:<br><br>i. User name<br>ii. IP address & MAC address<br>iii. Roaming history<br>iv. Bandwidth usage<br>v. Location (to nearest AP at a minimum)<br>vi. Equipment 'host name' if resolvable | Highly Desirable |
| 7.1.E | Visibility of RF Performance | Mandatory |
| 7.1.F | Event Logging | Mandatory |
| 7.1.G | Critical incident email reporting | Mandatory |
| 7.1.H | RF Planner | Highly Desirable |
| 7.1.I | Spectrum Analyser | Highly Desirable |
| 7.1.J | Visibility and management of security features | Mandatory |

## 7.2 Users & SSID

| Item # | System Feature | Importance |
|---|---|---|
| 7.2.A | Time-based access policies per SSID | Mandatory |
| 7.2.B | User-based WLAN policies to throttle or restrict access | Highly Desirable |
| 7.2.C | Options to adjust SSID visibility | Mandatory |

# 8 WARENTEE AND SUPPORT

| Item # | System Feature | Importance |
|---|---|---|
| 8.1.A | 5 year Advanced Replacement Warranty on Controllers and Access Points (specify whether it is included as standard, or requires additional licensing/purchasing).<br>Outline replacement process in an XLS matrix | Mandatory |
| 8.1.B | 5 year Support Licenses available for Controllers and Access Points (specify whether it is included as standard, or requires additional licensing/purchasing) | Mandatory |
| 8.1.C | Unlimited vendor helpdesk (specify whether it is included as standard, or requires additional licensing/purchasing) | Mandatory |