Dynamic wireless

Wireless Consulting Services

Dynamic Wireless Pty Ltd

Technical Review of iiNet's Free Public Wi-Fi Proposal

ACT Government

16th December 2013

Contents

Document Control

Action	Name	Position	Date
Prepared by:	David Renaud	Principal Consultant	15/12/13

Release

Version	Date Released	Pages Affected	Remarks
1.0	15/12/13		Draft Release
2.0	16/12/13	p7-8 (Summary Updated, Completed Risk Scores Added) p56 (RF Prediction Maps for Rx Sensitivity Added) p56-58 (Cost Accuracy Review Added) p59-61 (Implementation Timeframe Review Added)	Final Release

Distribution List

Name	Organisation	Title
Mark Lightfoot	Digital Canberra | Economic, Regional and Planning | **Policy and Cabinet Division** | Chief Minister and Treasury Directorate | **ACT Government**	

1. INTRODUCTION

Dynamic Wireless was contracted by the ACT Government for the purposes of providing a technical review of one of their free public Wi-Fi proposals, submitted by iiNet, as part of a recent tender for providing free Wi-Fi across Canberra.

This report is the deliverable to the ACT Government, of which the purpose is to evaluate the risks associated with their proposal, risks associated with individual items within their proposal, and provide an overall recommendation based on the total risk.

An overview of the evaluation criteria used to review iiNet's proposal and assign risks, is provided below:

- **Executive Summary**
- **Technical Review**
  - Solution Quality Review
    - i. Wi-Fi Technology Design
    - ii. Radio Specifications Evaluation
      1. Receive (RX) Sensitivity
      2. 802.11n MIMO Capability
    - iii. Hardware Environmental Ratings/Suitability for Outdoors
    - iv. Wireless Network Management System
    - v. Additional Features
  - Solution Upgradeability
    - i. Hardware Upgradeability
    - ii. Firmware Upgradeability
  - Client Security Features
    - i. Wireless Encryption and/or Authentication
    - ii. Firewalls
    - iii. Filtering Capability (Viruses and Malware)
  - Solution Scalability
    - i. Coverage Scalability
    - ii. Client Capacity Scalability
  - Open Network Standards Compliance
    - i. Wireless Technology based on Open Standards
    - ii. Integration with Open Network Standards
  - Technical Feasibility
    - i. Proven Technology or Cutting-Edge Technology
    - ii. History of Technology being used in Wireless Broadband Deployments
- **Non-Technical Review**
  - Vendor Suitability
    - i. Local Hardware Vendor Support Availability
    - ii. Hardware Vendor Size and Stability
    - iii. Number and size of deployments globally
    - iv. Wireless/Radio Technology Patent Search
    - v. Vendor Commitment to Product Development and Firmware Updates
    - vi. Warranty and Expected Equipment Lifetime
- **Cost Accuracy Review**
  - Hardware and Installation Cost
  - Maintenance Cost
- **Implementation Timeframe Review**

2. SUMMARY OF EVALUATION

2.1 RISK ANALYSIS METHODOLOGY

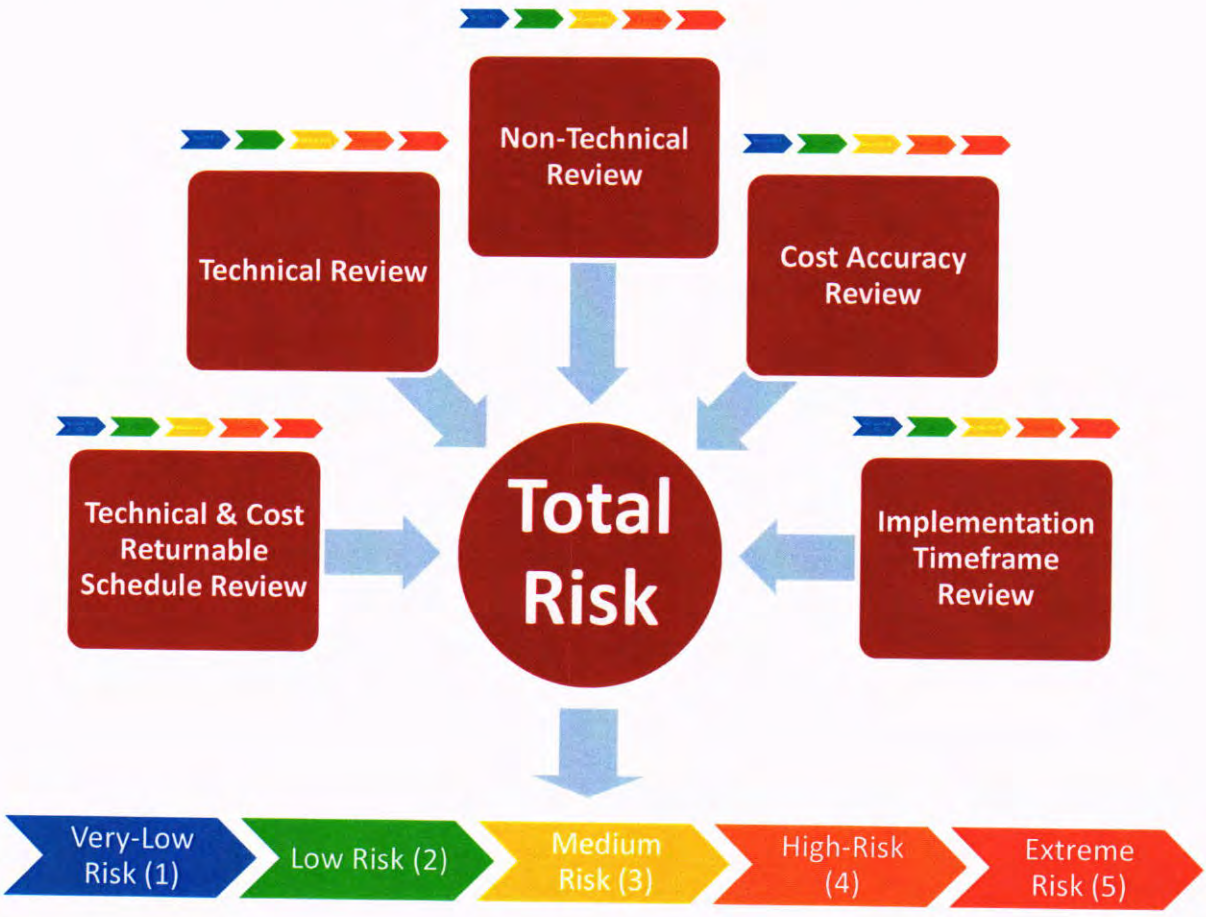
Dynamic Wireless has chosen a five-fold risk analysis method, whereby the following five reviews were conducted, and a risk assigned to each type of review, based on the average of the individual review items within each risk review. The sum of all five risk reviews were then added together and the average taken, in order to arrive at a total risk score representative of all the risks. A diagram allowing you to visualise what this looks like is provided on the following page. Furthermore, this risk review also allows the reviewers of this report to delve further down into each risk review and individual risk items as required.

Dynamic Wireless believes that such a methodical risk evaluation, where the average is taken of the sum of all risks, provides for a more granular approach and hence more accurate final risk calculation.

The five risk reviews are listed in the table below, with a further explanation about each type:

Review Type	Purpose	# Individual Risk Review Items
Technical & Cost Returnable Schedule Review	To review iiNet's each and every response to the 'Attachment 1 - Technical and Cost Returnable Schedule' document.	All 49 response items were reviewed and assigned a risk from 1 (Very-Low) to 5 (Extreme)
Technical Review	To review a selection of technical specifications and criterion deemed important to the ACT Government's Free Wi-Fi Project, pertaining to iiNet's proposed hardware (Huawei, and Cisco as their alternative proposal)	16 technical review items assigned a risk from 1 (Very-Low) to 5 (Extreme)
Non-Technical Review	To review a selection of non- technical criterion deemed important for the purposes of evaluating iiNet's chosen vendors (Huawei, and Cisco as their alternative proposal)	7 non-technical review items assigned a risk from 1 (Very-Low) to 5 (Extreme)
Cost Accuracy Review	To review iiNet's proposed costs and determine whether it represents value for money and whether it is above or below the expected industry benchmark.	Assigned a risk from 1 (Very-Low) to 5 (Extreme), based on Dynamic Wireless cost calculations.
Implementation Timeframe Review	To review iiNet's proposed implementation timeframe and determine whether it is reasonable by industry standards, and whether the month-by-month rollout schedule is reasonable.	Assigned a risk from 1 (Very-Low) to 5 (Extreme), based on Dynamic Wireless cost calculations.

A diagram showing Dynamic Wireless's Five-Fold Risk Review Methodology is provided below:



2.2 SUMMARY

Important Note:

Please note that due to iiNet essentially having an N+1 proposal, whereby if their Huawei proposal is not accepted then they will offer an alternative backup Cisco proposal; it is not possible to review their proposal without reviewing the risks associated with Huawei and Cisco separately. Therefore for whichever risk items were affected by the hardware being either Huawei or Cisco, these were recorded and then added up separately in order to arrive at separate overall risk scores for both Huawei and Cisco solutions.

Based on the calculated risk scores below, iiNet's proposal (either Huawei or Cisco) represent a Low-Risk solution and Dynamic Wireless recommends their proposal to the ACT Government. However our recommendation would be to not choose Huawei, until such a time as iiNet is able to provide detailed technical and radio specifications for the proposed Huawei access points, controller and wSight management software. Only after these items have been submitted by iiNet, can the technical evaluation be completed in its entirety and an informed decision made. If it is not possible to gain access to this information, Dynamic Wireless recommends the ACT Government obtain a copy of iiNet's alternative Cisco proposal for review.

- iiNet proposes *"to build Australia's most technologically advanced Wi-Fi network in Canberra, using technology borrowed from gigabit-speed LTE standards that have not yet been deployed outside of trials at this time."* As there is no publicly available information (no data sheets or other information that Dynamic Wireless could find at the time of this review), nor has this information been supplied by iiNet as part of their proposal; there is no way of evaluating these latest APs from Huawei in order to determine how exactly they have borrowed technology from gigabit-speed LTE standards,

and to also evaluate and compare their AP radio specifications (RSSI, transmit power, environmental ratings etc) against other leading carrier-grade wireless mesh hardware in the market.

- As the Huawei technology being proposed by iiNet has not been deployed outside of China, it does represent a risk like all cutting-edge technology with limited deployments do.

- Huawei's existing mesh AP (AP6610DN-AGN) receive sensitivity levels are 3-4 dBm lower than Cisco's mesh AP, which can potentially results in a mesh AP density, and capital expenditure increase of up to 30% depending on the terrain.

- iiNet's response does not address how they include levels of protection for viruses. They do not mention any hardware appliances or methods used to filter and protect users from viruses. Cisco and other well known vendors do provide such hardware appliances. Cisco for example provides it's IronPort Sophos Anti-Virus Technology. As this is a mandatory requirement for the ACT Government, this has been assigned an Extreme risk level.

- iiNet states that *"iiNet will use its own internal customer experience measurement systems to determine the service levels for customers, including those that use the Wi-Fi networks."* This statement however, contradicts this ACT Government's clause which states *"These minimum contract management service levels will be developed in conjunction with the successful supplier and will be designed to ensure that the network functions as proposed."* On the facts, it appears that iiNet are going to use their own performance metrics, and not take into account any ACT Government input into defining performance metric levels and how they will be measured. For this reason, a risk level of 5 (extreme) has been assigned, until such a time as this is clarified. The ACT Government should enquire into this.

3. TECHNICAL AND COST RETURNABLE SCHEDULE REVIEW

Each of iiNet's responses to the criteria items within the Technical and Cost Returnable Schedule were thoroughly evaluated for any technical risks and assigned either a 'Compliance Risk Rating' of either 1 (Very-Low Risk), 2 (Low Risk), 3 (Medium Risk), 4 (High Risk) or 5 (Extreme Risk). Comments as to why the risk rating was given are provided, along with any anomalies discovered within iiNet's response, which the ACT Government should review and raise with iiNet if necessary.

Evaluation Criteria	Compliance Risk (1--Very Low,2-Low, 3-Medium Risk, 4- High Risk, 5-Extreme Risk)	Comments
2. Technical Requirements		
1. Mandatory Requirements	**1**	No Comments
2.2 General Wi-Fi Requirements (Essential)	**1**	• Although the Wi-Fi services on 20 buses is an R&D exercise, iiNet states that coverage will not be integrated with the greater Wi-Fi service to avoid interference issues. Although this is fine for the initial R&D exercise, in the longer term if the Canberra-wide Free Wi-Fi network expands, then the onboard bus router's Wi-Fi should also be used as a backhaul to the Canberra-wide Free Wi-Fi network. Thus the mobile router can become backhaul-agnostic and switch between either 3G and Wi-Fi depending on what coverage the bus receives. For example, when a bus passes through a Wi-Fi coverage area such as the bus stations, or public parks, passengers data will be transmitted over Wi-Fi instead of the 3G network, thus saving data and therefore money. • The entire network will support 2.4 GHz and 5 GHz bands, which is a must nowadays. • Dynamic Wireless agrees that 802.11b clients should not be allowed on the network, as they can slow down all other clients on the wireless network should they connect. • Dynamic Wireless agrees that 802.11ac does not currently represent good value for pubic Wi-Fi, as there are simply very client radios in the market which support this new standard. However this is changing rapidly, more details are provided on this later in the report. • Dynamic Wireless agrees with the target platform for compatibility will be an Apple iPhone5 or Samsung S4, as iOS and Android represent 92.5% of the world-wide smart phone OS market, as of 2Q13, according to IDC. Source: http://www.idc.com/getdoc.jsp?containerId=prUS24257413 • Ease of Use - The free network will be open, making it easier to connect to. This is the best method of allowing free users onto a network as it minimizes support issues. • Corporate users will use WPA2/Enterprise, and be standards based. iiNet are referring to such standards based authentication such as RADIUS which is an industry standard for providing secure access to wireless.

		• Commercial and free users will use different networks, which is a good practice which ensures segregation of sensitive/confidential commercial client data, from free client data.
2.3 Services and Support (Essential)	**2**	• Although the Wi-Fi services on 20 buses is an R&D exercise, a download limit of 10 MB per device per day does not seem a reasonable amount of data transfer by today's standards. According to the website HTTP Archive, which regularly studies the top 10,000 most-visited sites online, the average web page now weighs in at about 1.3 megabytes, up about 35 per cent in the last year. HTTP Archive suggests the average web page when browsing on a mobile device – accounting for the fact that some websites have mobile-optimized pages and others don't – is about 720 kilobytes[1]. Considering that most passengers take return journeys on buses, 10 MB will get used up very quickly on a smart phone or tablet. This equates to viewing about 7 web pages for each one-way journey. Somewhere between 25-50 MB would be more suitable. Dynamic Wireless recommends that ACT Government staff conduct their own tests using their smart phones built-in data usage statistics (or 3rd part data usage tracking application) to track how much data is being used across a sample of bus journeys, using regular websites which passengers are likely to use such as Facebook, Instagram, News sites, mobile banking etc. Based on these tests, an accurate download limit can be set, as this limit should be intended to block high usage (youtube etc) users, and not every passenger who is simply viewing a few websites on their journey each way. [1] Source: http://www.theglobeandmail.com/technology/tech-news/bloated-web-pages-costly-for-smartphone-users/article9355125/
2.4 Network and Technology		
2.4.1 Wireless Standards (Essential)	**1**	• • Dynamic Wireless agrees that 802.11ac does not currently represent good value for pubic Wi-Fi, as there are simply very few client radios in the market which support this new standard. However, it is important to note that 802.11ac is expected to rapidly gain traction, and according to a study done by CNET (an American tech media website that publishes reviews, news, articles, blogs, and podcasts on technology and consumer electronics globally), devices with the 802.11ac specification are expected to be common by 2015 with an estimated one billion spread around the world. Source: http://news.cnet.com/8301-30685_3-20030964-264.html?part=rss&subj=news&tag=2547-1_3-0-20 Therefore, although no outdoor mesh APs are yet available with 802.11ac radios yet, and not a risk to this project currently, the technology could be 2 years away from large-scale proliferation and should be monitored. However as indoor APs from Huawei and Cisco are now shipping with 802.11ac radios, iiNet's proposal to install an 802.11ac capable AP in a public library as a demo site is highly recommended by Dynamic Wireless, not just for the purposes of satisfying user curiosity, but for ACT

		Government to closely monitor and record the percentage statistics of 802.11ac clients connecting to the wireless network. Only in this way can the ACT Government monitor 802.11ac trends on the Free Wi-Fi Network, to enable planning for future upgrades. Considering the speed at which 802.11ac may proliferate, it would be advisable to have more than just one site with an indoor 802.11ac capable AP installed, for example maybe 5 APs at 5 different types of sites such as business centre, park, bus station, educational precinct etc. This would allow 802.11ac trending to be performed across a wider audience variety, than those that just go to the library. • • FYI - iiNet states that Today, approximately 2% of usage occurs on 5GHz. This figure seems exceptionally low, as due to the latest smart phones and tablets now being shipped with dual-band 2.4/5 GHz radios, usage in the 5 GHz spectrum is increasing dramatically and can be as high as 50% of total users. Dynamic Wireless has witnessed this statistic when monitoring thousands of connected wireless clients for a major University.
2.4.2 Technology, Capacity and Capability (Essential)	4- If Huawei chosen 1- If Cisco chosen	As the Huawei technology being proposed by iiNet has not been deployed outside of China, it does represent a risk like all cutting-edge technology with limited deployments do. Also, due to the unavailability of detailed radio specifications and data sheets for these new access points, Dynamic Wireless was unable to conduct an evaluation on this new hardware, and instead has based its evaluation on Huawei's previous/older wireless mesh APs, which are already deployed around the world.
2.4.3 Connectivity Type (Highly-Desirable)	1	No Comments
2.4.4 Handoff (Essential)	1	Seamless handoff (i.e. roaming) between APs using centralised controllers has been well-proven over the past decade, by such vendors as Cisco.
2.4.5 Supported Applications (Essential)	1	No Comments
2.4.6 Traffic Prioritisation (Highly-Desirable)	1	No Comments

2.4.7 Quality of Service (Essential)	2	• • iiNet states that *"It is very challenging to deliver iiNet's quality expectations to buses. This is because mobile network coverage is not perfect, and a bus may have enough passengers on it to overload a mobile network connection."* This can be mitigated by having dual-sims in the mobile wifi router, thereby providing backhaul-agnostic bandwidth over 2 wireless carrier networks. Although it does cost more, it ensures a more stable backhaul connection and experience to users, and if both sims are used concurrently, provides double the bandwidth. An example of this is the University of Queensland's deployment on all CityCat boats along the river, where each carrier they tested had coverage holes around the river, hence they decided to use multiple sim cards connecting to two carriers in order to even out the coverage and provide the best experience possible. Icomera has a product which even supports up to 8 sims, so all 3 mobile networks (Telstra, Optus, Vodaphone) could be used as backhaul if required. The real issue here is cost. A good compromise would be to find which combination of two carriers in Canberra will provide the best coverage in the Free Wi-Fi network coverage areas across Canberra, and use the two that provide the best converged coverage.
2.4.8 Roaming Agreements (Essential)	1	• • and as stated by The Canberra Times *"The top five source markets for international visitors to Canberra in terms of visitor numbers were China (12.1 per cent), the US (11.8 per cent), Singapore/Malaysia/Thailand/Hong Kong (10.7 per cent), the United Kingdom (9.6 per cent) and New Zealand (8.0 per cent)."* http://www.canberratimes.com.au/act-news/capital-tourism-figures-best-in-a-decade-20130607-2nvu0.html
2.4.9 Security and Filtering (Mandatory)	5	

2.4.10 Privacy (Essential)	**1**	No Comments
2.4.11 Congestion (Essential)	**1**	No Comments
2.4.12 Architecture and Design (Essential)	**2**	• • iiNet states that *"Roaming and meshing will be proprietary as there is not yet an industry supported open standard for Wi-Fi meshing."*This is correct, as all mesh vendors have developed their own proprietary meshing algorithms. The best wireless mesh vendors have proprietary mesh protocols incorporating powerful smart meshing algorithms, such as Cisco's Adaptive Wireless Path Protocol (AWPP). Dynamic Wireless was unable to find much information about how Huawei's meshing protocols and algorithms differ from the other vendors in the market. However this is only a slight risk as all vendors algorithms follow similar optimal path calculation rules, so for this reason a risk of 2 was assigned.
2.4.13 Spectrum (Essential)	**1**	• Like licensed microwave links, a point to point wireless Ethernet bridge in the 24 GHz unlicensed wireless band provides carrier grade wireless backhaul. 24 GHz wireless backhaul is ideal for point to point wireless bridges in areas where there is a lot of wireless interference.
2.4.14 Regulatory and Legal Requirement (Essential)	**1**	• iiNet's response accepted Prima Faci. No other way to check this.
2.4.15 Wireless Network Equipment (Essential)	**4- If Huawei chosen 1- If Cisco chosen**	• As the Huawei technology being proposed by iiNet has not been deployed outside of China, it does represent a risk like all cutting-edge technology with limited deployments do. Also, due to the unavailability of detailed radio specifications and data sheets for these new access points, Dynamic Wireless was unable to conduct an evaluation on this new hardware, and instead has based its evaluation on Huawei's previous/older wireless mesh APs, which are already deployed around the world. However iiNet has mitigated this risk by preparing an option for a similar state-of-the-art Cisco hardware at a higher cost. should the ACT consider Huawei equipment to be unsuitable. • The proposed alternative Cisco solution hardware is exactly what Dynamic Wireless would also propose for the ACT Government's Free Wi-Fi Project. In providing wireless consulting services to airports and

		mining sites in Australia, the above Cisco wireless infrastructure has been previously recommended by Dynamic Wireless as being suitable for such large campus/municipal deployments.
2.4.16 Operating Hours (Highly-Desirable)	**1**	No Comments
2.4.17 Reliability (Highly-Desirable)	**1**	No Comments
2.4.18 Scalability and Technology Upgrade (Highly-Desirable)	**1**	No Comments
2.4.19 Network Maintenance (Highly-Desirable)	**1**	No Comments
2.4.20 Health and Safety (Essential)	**1**	As long as Huawei or Cisco wireless mesh APs are compliant with the mandatory ARPANSA Standard EME Exposure Limits, via complying with ACMA's Radiocommunications (Electromagnetic Radiation — Human Exposure) Standard 2003, then iiNet will be compliant. The fact that such hardware is imported into Australia by the vendors, implies compliance to these standards, as the fines are very high for non-compliance.
2.4.21 Subscription Levels (Highly-Desirable)	**1**	• Dynamic Wireless has always advised its own wireless customers to limit the number of simultaneous connections per AP to 30 (15 per 2.4 and 5 GHz radio) in order to ensure 1+ Mbps of throughput (from a 54 Mbps radio) to each client, assuming all clients are downloading at the same time. This is the worst case scenario at maximum capacity, which will likely never occur. Typically it is safe to assume a 20% network utilisation ratio at any point in time. Therefore 31 clients per AP x 20% = ~6 clients, which equates to 3+ Mbps for each client. iiNet has allowed for 2 Mbps for each free client, which equates to a network utilisation of around 30%. Therefore in summary, iiNet has designed the network to support a high number of simultaneous connections, exceeding the generally accepted minimum of 20% utilisation.