



## **MOBILE & WIRELESS TECHNOLOGY (CT090-3-2)**

**UC2F1808IT**

**ASSIGNMENT TITLE : GROUP ASSIGNMENT**

**HANDOUT DATE : 8 October 2018**

**SUBMISSION DATE : 15 November 2018**

**LECTURER'S NAME : DAVID TAN GEI KAR**

<b>NAME</b>	<b>TP NUMBER</b>
MOLDOBAEVA MUNARA	TP042788
NUR AFIQAH BINTI BAKAR	TP043448
NADZIRAH BINTI RASOL	TP048345
MOUSI AHMED ABDULHAFITH	TP047417

[Table of Contents](#)

1.0 Introduction.....	4
1.1 Company Background.....	4
1.2 Scope and Limitations.....	5
2.0 Overview Layout.....	6
3.0 Content Body.....	7
3.1 Standards, Site Surveys & Other Considerations.....	7
3.1.1 Site Survey Types and Process.....	7
Justification and Recommendation for Site Survey Types.....	9
3.1.2 Software and Hardware tools.....	10
Justification and Recommendation for Hardware and Software Tools.....	12
3.1.3 Floorplan.....	13
3.1.4 Wi-Fi Standard and other considerations.....	15
Justification and Recommendation for Wi-Fi Standard.....	19
3.2 WLAN -Hardware & Software Requirements.....	20
3.2.1 Hardware Requirements.....	21
Access Point.....	21
Justification and Recommendations for Access Point.....	30
Controller.....	31
Justification and Recommendations for Controller.....	40
Wireless Bridge.....	41
Justification and Recommendations for Wireless Bridge.....	49
3.2.2 Software Requirements.....	50
Justification and Recommendations for Software Requirements.....	51
3.3 Security Implementation Requirements.....	52

3.3.1 Potential Threats Affecting WLAN.....	53
Justification and Recommendations for Security Threats.....	55
3.3.2 Algorithms.....	56
Authentications.....	56
Encryption.....	59
Comparison between the encryption methods.....	61
Justification and Recommendations for Authentication and Encryption.....	62
3.4 WLAN - Monitoring and Maintenance Considerations.....	63
3.4.1 Monitoring WLAN.....	63
Justification and Recommendations for Monitoring Tools.....	67
3.4.2 Maintaining WLAN.....	68
3.4.3 Wireless LAN Optimization.....	71
4.0 Appendices.....	73
4.1 Gantt Chart.....	73
4.2 Workload Matrix.....	74
5.0 Conclusion.....	75
5.1 Learning Outcomes and Future Enhancements.....	75
6.0 References.....	76

## 1.0 Introduction

### 1.1 Company Background

The aim of this project is to launch and maintain wireless LAN connection between Bario Health Clinic and Tele-Centre. Team of four was assigned as a network assisting consultants to help a clinic to link with their telecentre through satellite antennas and whole network technology behind it. The distance between these two buildings accounted as 200 meters. Inside of the clinic only one desktop PC located; In future clinic may grow in scale together with number of devices in it.

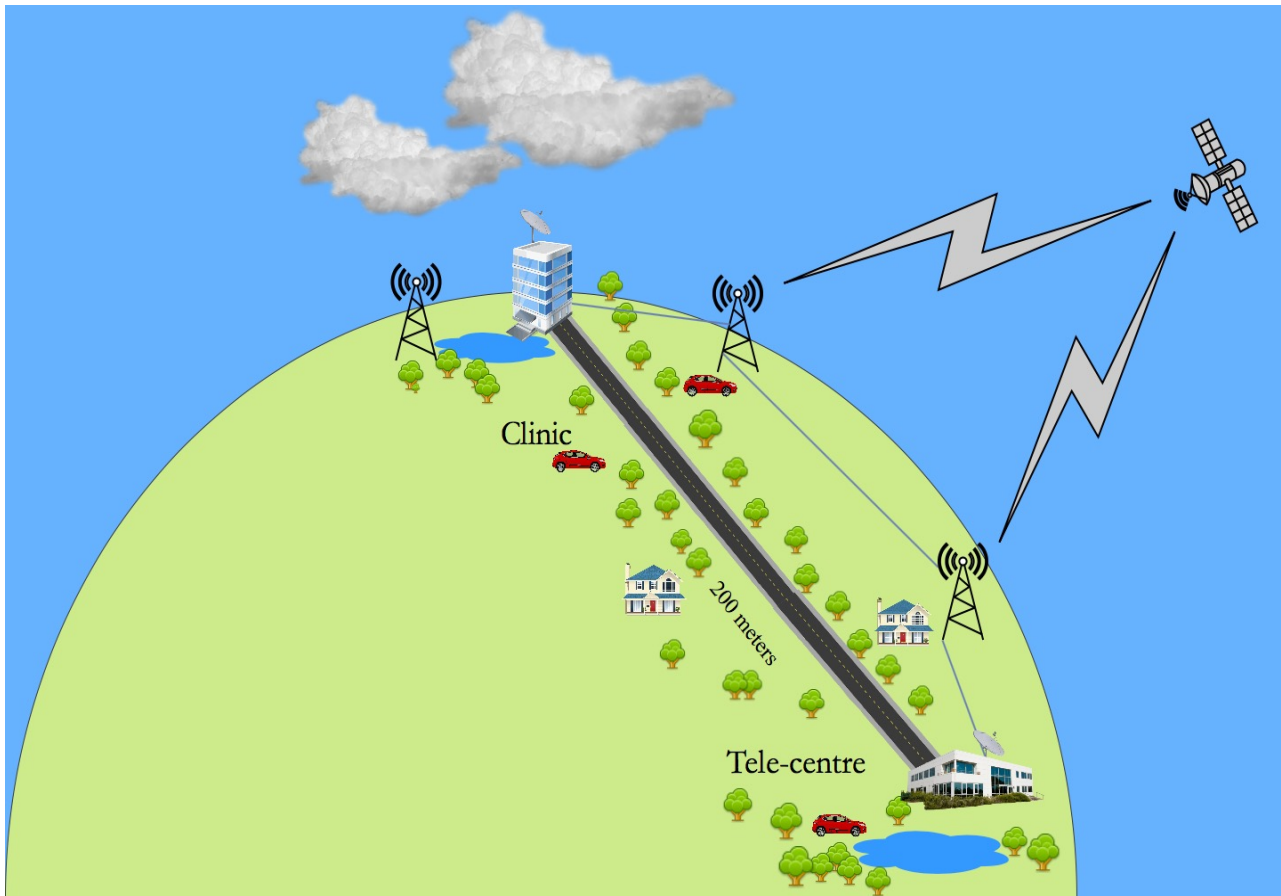
First goal of networking team is to base strong WLAN connection, preventive from any security attacks, easily monitorable and maintainable in future perspective. In order, to reach current goal this project has been separated to several tasks as: get list of solutions and options to deploy WLAN connection for clinic and telecentre. Then, representation of accurate site survey with list of every chosen Hardware and Software with their following recommendation and requirements. Other than that, team was considered to provide clinic with strong network security system with following preventive solutions. And lastly, monitoring and maintenance procedures was required to support and develop further high performance of wireless LAN in further period of time. All mentioned points were taken under consideration and assigned among team members accordingly.

## **1.2 Scope and Limitations**

The scope of the study involves the overall process of implementing a WLAN from doing the survey, choosing the hardware and software, determining the types of security needed for the connection and the types of maintenance needed for the WLAN after its being implemented. The general budget for implementing WLAN for Bario Community Clinic and Telecentre are roughly between RM100,000 to RM 200,00 which depends on the hardware and software chosen. The time range of implementing the WLAN is about 2 to 3 weeks depending on the size of area of the Bario Clinic and Bario Telecentre.

This study is limited to implementing a WLAN only and not to consider of implementing a wired cable for the connections between Bario Clinic and Bario Telecentre. The limitations are that the connections at Bario Telecentre are up to 35 personal computers (PCs) only whereas for the Bario Clinic, it is up to 5 personal computers (PCs) only.

## 2.0 Overview Layout



*Figure 1: An overview layout of Barrio Clinic and Barrio Telecentre*

### 3.0 Content Body

#### 3.1 Standards, Site Surveys & Other Considerations

##### 3.1.1 Site Survey Types and Process

Site survey is the most important task before starting the practical work to avoid any trouble and potential dangers to the task. The two main goals for wireless site survey are to determine the most suitable location to place the access points and to determine the feasibility of building a WLAN on the site [ CITATION Jim14 \l 1033 ]. There are three types that are commonly used in the industry are active site surveys, passive site surveys and predictive site surveys. Below is the comparison of the three types of surveys.

Types of survey	Predictive Surveys	Active Surveys	Passive Surveys
<b>When to conduct</b>	Optional but usually conducted before any deployment to plan the WLAN and simulate its characteristic	Optional and it is used to conduct when measurement of real-world performance characteristic of the WLAN is required	Highly recommended at all times as it is the most comprehensive survey type that covers the most important WLAN characteristics and metrics
<b>Hardware requirements</b>	<ul style="list-style-type: none"><li>• No wireless adapter is required</li><li>• A fast-multi-core, Intel i7 is highly recommended</li></ul>	<ul style="list-style-type: none"><li>• A compatible wireless adapter to Windows or macOS</li></ul>	<ul style="list-style-type: none"><li>• A compatible wireless adapter to Windows or macOS</li></ul>
<b>Additional software configuration requirements</b>	None	For Windows, must create a profile to test the WLAN  For macOS, the WLAN	None

		to be tested must be listed under preferred network.	
<b>Data collecting</b>	No-on site data collection is performed. Data is simulated based on the virtual environment of the floorplan.	The application connects the Wi-Fi adapter to the wireless network that is desired to measure actual throughput rates and a few other metrics.	The application will passively listen for packets and does not attempt to connect to any WLANs.
<b>Available visualization</b>	<ul style="list-style-type: none"> <li>• Signal Level</li> <li>• Signal-to-Noise Ratio</li> <li>• Signal-to-Interference Ratio</li> <li>• AP Coverage Areas</li> <li>• Number of APs</li> <li>• Expected PHY Rate</li> <li>• Frame Format</li> <li>• Channel Bandwidth Requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Actual PHY Rate</li> <li>• TCP Upstream Rate *</li> <li>• TCP Downstream Rate *</li> <li>• UDP Upstream Rate *</li> <li>• UDP Downstream Rate *</li> <li>• UDP Upstream Loss *</li> <li>UDP Downstream Loss *</li> <li>Round-trip Time</li> <li>Associated AP</li> <li>Requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Signal Level</li> <li>• Signal-to-Noise Ratio</li> <li>• Signal-to-Interference Ratio</li> <li>• AP Coverage Areas</li> <li>• Number of APs</li> <li>• Expected PHY Rate</li> <li>• Frame Format</li> <li>• Channel Bandwidth Requirements</li> </ul>
<b>List of access points and their characteristic</b>	Yes	No	Yes




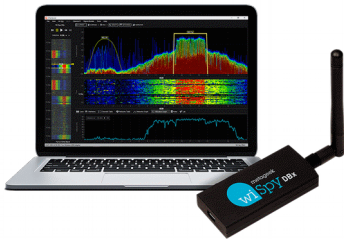
***Table 1: A comparison between Active, Predictive and Passive surveys[ CITATION Tam18 \l 1033 ]***

#### Justification and Recommendation for Site Survey Types

In terms of operational and technical feasibility, active site survey is the most efficient compared to the others as it will measure the actual throughput rates of the desired location on site. Therefore, the chances of having a problem related to the location of the access point can be avoided. On the other hand, predictive site surveys are the most economical one as it only requires the blueprints and floorplans to perform the measurements by using only software tools. Therefore, our team have decided on performing active site surveys for Bario Clinic and Bario Telecentre as it is only required one a single test and can get accurate measurements from the survey.

#### 3.1.2 Software and Hardware tools

To conduct a wireless survey, there are some hardware and software tools that are needed to help confirm that all the requirements for optimal performance are met [ CITATION Jim14 \l 1033 ]. For the hardware components, it consists of an analyzer dongle whereas for the software components, it consists of a site survey software. Below is the comparison of USB dongle analyzer and the software from Wi-Spy DBx Spectrum Analyzer and Ekahau Spectrum Analyzer.

<b>Product</b>	<b>Ekahau Spectrum Analyzer</b>  [ CITATION Eka18 \l 17417 ]	<b>Wi-Spy DBx Spectrum Analyzer</b>  [ CITATION Met18 \l 1033 ]
<b>Compatible Software</b>	Ekahau Site Survey Pro	Chanalyzer 5
<b>Company</b>	Ekahau	Metageek
<b>Interface</b>	USB	USB
<b>Amplitude Range</b>	-100 dBm to -6.5 dBm	-100 dBm TO -6.5 dBm
<b>Amplitude Resolution</b>	0.5 dBm	0.5 dBm
<b>Antenna</b>	External, RP-SMA	External, RP-SMA
<b>Default Frequency Range</b>	2.400 GHz to 2.495 GHz, 5.150 GHz to 5.850 GHz	2.400 GHz to 2.495 GHz, 5.150 GHz to 5.850 GHz
<b>Wi-Fi Radio Supported</b>	802.11ac, 802.11n and 802.11a/b/g	802.11ac, 802.11n
<b>Price</b>	Ekahau Wi-Fi Spectrum Analyzer with Survey Integration <ul style="list-style-type: none"> <li>• Ekahau Spectrum Analyzer</li> <li>• Ekahau Site Survey Pro</li> <li>• 1year software support</li> <li>• Total (RM7882.40)</li> </ul>	Chanalyzer Essential <ul style="list-style-type: none"> <li>• Wi-Spy DBx</li> <li>• Chanalyzer with Report Builder</li> <li>• Device Finder Antenna</li> <li>• 1year software support</li> <li>• Total (RM 4158.60)</li> </ul>

--	--	--

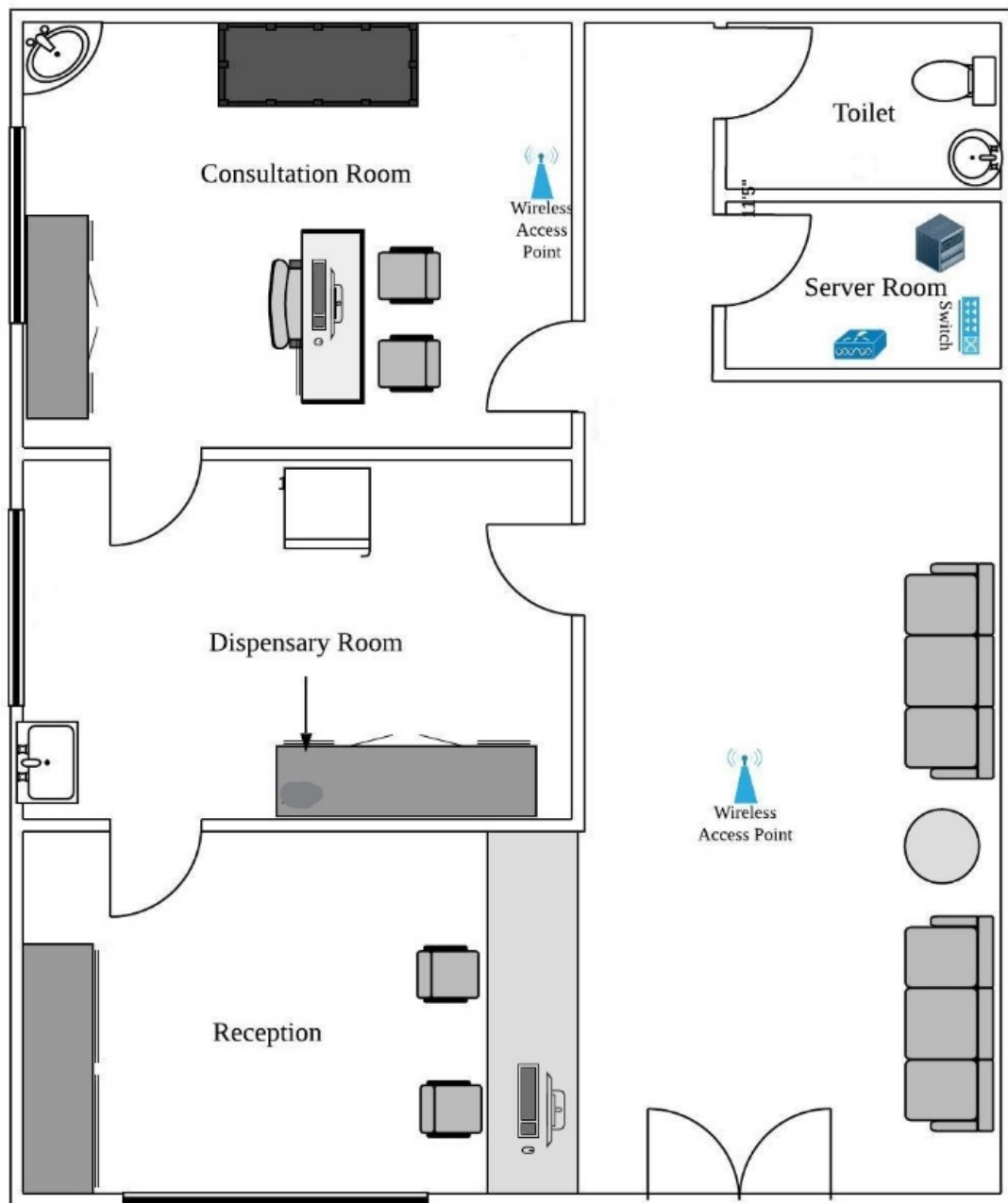
***Table 2: Comparison of Ekahau Spectrum Analyzer and Wi-Spy Spectrum Analyzer***

#### Justification and Recommendation for Hardware and Software Tools

In terms of economic feasibility, Wi-Spy DBx Spectrum Analyzer is much cheaper than Ekahau Spectrum Analyzer when both are offering the same functionalities. As for the operational feasibility, Ekahau Spectrum Analyzer is more efficient as it can be used to test more ranges of wireless standard compared to the Wi-Spy DBx Spectrum Analyzer, where else the other features that both products offers are just the same. The system requirements for Ekahau Spectrum Analyzer is more reliable as it can be supported in more versions of Windows operating system and has a higher resolution. Therefore, as our team have decided on choosing the Ekahau Spectrum Analyzer to help perform the active site surveys on both Bario Clinic and Bario Telecentre. Although the price is much higher than the other one, the operational and technical feasibility of Ekahau Spectrum Analyzer offers much more, and it is worth the money.

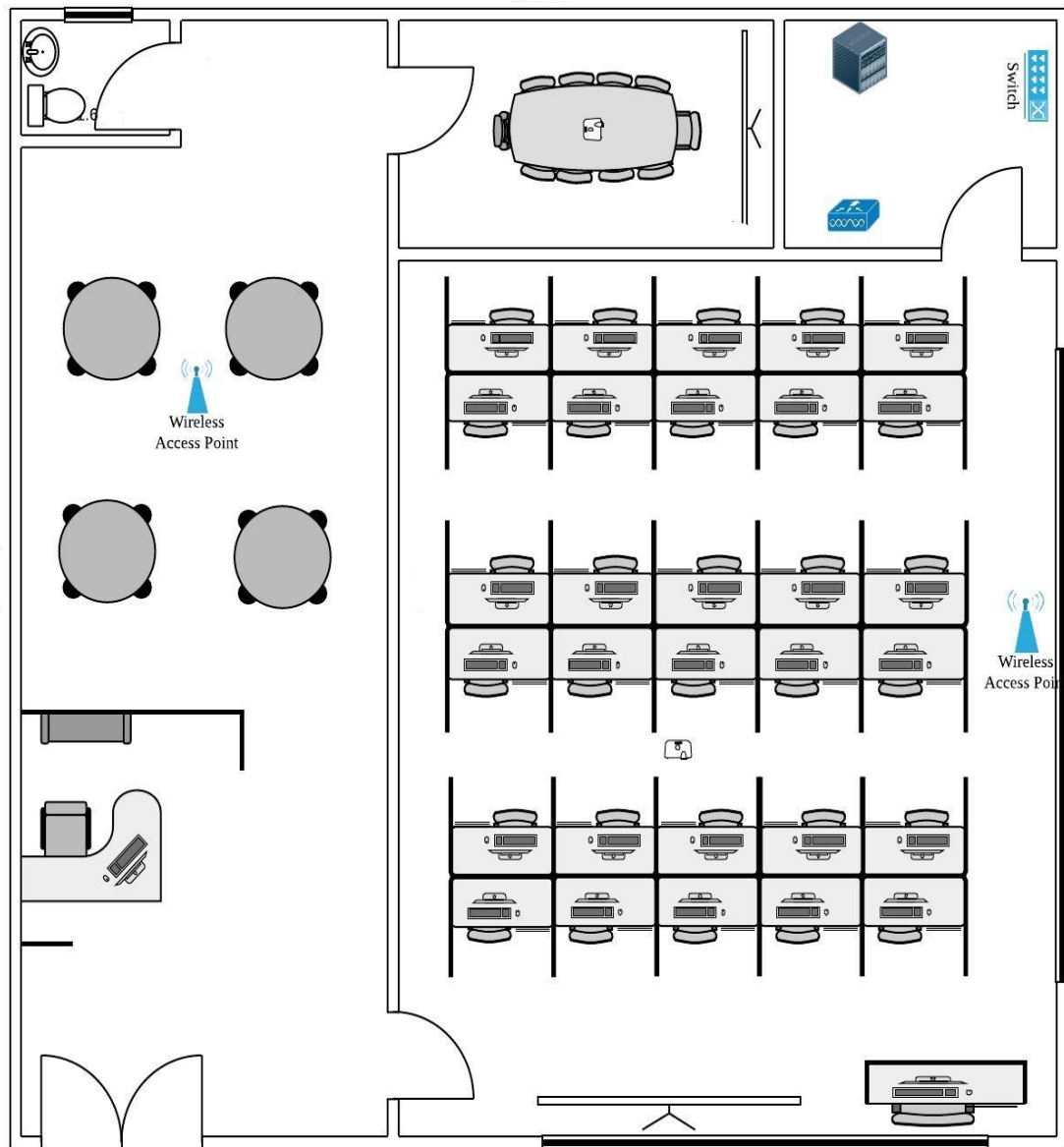
### 3.1.3 Floorplan

#### a) Bario Clinic Floorplan



**Figure 2: Bario Clinic floorplan**

b) Bario Telcentre Floorplan



*Figure 3: Bario Telecentre floorplan*

### 3.1.4 Wi-Fi Standard and other considerations

Wireless Fidelity or know as ‘Wi-Fi’ was first released in 1997 and the standards have been continually evolving since then as to keep up with the higher throughput. The technical name for Wi-Fi standard is IEEE 802.11 and it covers not only wireless, but all kind of Local Area Networks (LAN) and Metropolitan Area Network (MAN) [ CITATION Mat18 \l 1033 ]. The latest Wi-Fi standard are 801.11ac and its predecessor 802.11n where both of it allows a high throughput. These standards have some similarities and differences, therefor, below is the comparison between 802.11ac and 802.11n

<b>Wi-Fi Standard</b>	802.11ac	802.11n
<b>Published Year</b>	2015	2009
<b>Frequency Band</b>	5 GHz	2.5 GHz and 5 GHz
<b>Bandwidth</b>	20 MHz	20 MHz
	40 MHz	40 MHz
	80 MHz	
	160 MHz	
<b>Multi-user MIMO</b>	Yes	No
<b>Max Data Rate</b>	7 Gbps	600 Mbps
<b>Number of Spatial Streams</b>	1 to 8 totals	1 to 4
	Up to 4 per client	
<b>Single Stream (1x1) Maximum Client Data Rate</b>	450 Mbps	150 Mbps
<b>Two Stream (2x2) Maximum Client Data Rate</b>	866 Mbps (80MHz channel)	270 Mbps (40MHz channel)

***Table 3: A comparison between 802.11ac and 802.11ad [ CITATION Mat18 \l 1033 ]***

To achieve the desired safe and reliable WLAN, there are some recommendations that needs to be kept in mind. The surveyor needs to know what the clients' needs and they need to fulfil all those requirements[ CITATION Net181 \l 1033 ]. Basically, there are few factors that need to be considered by the surveyor during the planning and deploying the WLAN. Though the considerations may vary with each project, the basic process and considerations will always remain the same. Below is the list of what need to be considered before deploying WLAN connection in Bario Clinic and Bario Telecentre.

**a) Coverage**

The ability for user to connect to the wireless connection with a good signal and strength are defined by the coverage of the WLAN. The coverage will be the biggest concern as there will be many client devices that will connects to the WLAN.

<b>Signal strength</b>	-70.0 dBm
<b>Signal – to – noise ratio at least</b>	15.0 dB
<b>Data rate at least</b>	50 Mbps
<b>Number of access points</b>	1
<b>Ping round trip time at most</b>	200.0 ms
<b>Packet loss at most</b>	5.0%

***Table 4: Coverage considerations specification***

**b) Size of Area**

The size of area will help the surveyor to determine the amount of access points needed to cover the whole area. Based on Bario Clinic and Bario Telecentre, two access points will be used for each of the building.

**Bario Clinic (Size of area = 124 m<sup>2</sup>)**

Dimension	Size in metre (m)
X (width)	15.5 m
Y (length)	8 m

***Table 5: The width and length of the Bario Clinic***

**Bario Telecentre (Size of area = 250 m<sup>2</sup>)**



Dimension	Size in metre (m)
X (width)	25 m
Y (length)	10 m

***Table 6: The width and length of the Bario Telecentre***

### **c) Numbers of Users**

Number of users will be the major factor that affects the capacity of the network. Data rate is mostly affecting the delay performance of the WLAN. Hence, is important to know the number of users to determine the maximum data rate.

### Justification and Recommendation for Wi-Fi Standard

On the operational side, 802.11ac is the most effective to be implemented for the Bario Community as it utilizes dual-band wireless technology which mean that it supports 2.4GHz and 5GHz simultaneous connections and is also backward compatible. As for the technical side, 802.11ac are more reliable to use now as more devices are now have been manufactured to support this standard to fulfil people needs in seeking for the best speed for their connections. In terms of economic feasibility, implementing 802.11n is less expensive than 802.11ac as it is not the latest one in the market. However, as years passed by, the prices of 802.11ac have dropped to the point where it will not be a barrier to anyone who wants to implement it. Based on the critical researches, our team has decided to choose 802.11ac to be implemented for the Bario Clinic and Bario Telecentre WLAN as it has more advantages than any other standards.

### **3.2 WLAN -Hardware & Software Requirements**

Hardware and software are the fundamental element to make sure the deployment of WLAN can be done successfully. The basic hardware components needed are the access point, controller, and wireless bridges. Access point connects devices to other devices within the network and it can also serve as the point of interconnection between a WLAN and wired network. In other words, it is a station that receives and transmits data and information. Access point is the main part in order for the WLAN to be fully functional [CITATION Mar10 \l 17417 ]. Another vital component is controller. Controller helps in providing multiple of the access points with easy and quick configurations without having to configure each of the AP manually. It focuses more on the management for the entire wireless network in a particular place. Certain types of access point nowadays do function even without controller, but most of them need it for a more convenient network management [ CITATION Dan16 \l 17417 ]. Besides, wireless bridge also is needed in this situation to connect the network from the telecentre to clinic which is approximately 200 metres away from each other. The list of possible option for the components to be installed at Bario Community are as shown below.

### 3.2.1 Hardware Requirements

#### Access Point



***Figure 4: Ruckus R610 Access Point***

Model	Ruckus R610 Indoor 802.11ac 2 Access Point
Features / Specifications	<p>Stunning Performance</p> <p>Provide a great user experience no matter how challenging the environment with BeamFlex+ adaptive antenna technology and a library of 512 directional antenna patterns.</p> <p>Serve More Devices</p> <p>Connect more devices simultaneously with three MU-MIMO spatial streams and concurrent dual-band 2.4/5GHz radios while enhancing non-Wave 2 device performance.</p> <p>Get Optimal Throughput</p> <p>ChannelFly dynamic channel technology uses machine learning to automatically find the least congested channels. You always get the highest throughput the band can support.</p> <p>Multiple Management Options</p>

	<p>Manage the R610 from the cloud, with on-premises physical/virtual appliances, or without a controller.</p> <p>Better Mesh Networking</p> <p>Reduce expensive cabling, and complex mesh configurations by checking a box with SmartMesh wireless meshing technology to dynamically create self-forming, self-healing mesh networks.</p> <p>Expanded Backhaul</p> <p>Pair two onboard 1GbE ports with link aggregation (LACP) to maximize throughput between the AP and wired switch.</p>
Data Rate	<p>1,300 Mbps (5GHz)</p> <p>600 Mbps (2.4GHz)</p>
Capacity	512 concurrent devices
Frequency	<ul style="list-style-type: none"> <li>• ISM 2.4-2.484GHz</li> <li>• U-NII-1 5.15-5.25GHz</li> <li>• U-NII-2A 5.25-5.35GHz</li> <li>• U-NII-2C 5.47-5.725GHz</li> <li>• U-NII-3 5.725-5.85GHz</li> </ul>
Mechanical	<p>Physical Size</p> <ul style="list-style-type: none"> <li>• 20.1(L), 19.5(W), 5.1 (H)cm</li> <li>• 7.9 (L), 7.68 (W), 2.00 (H)in</li> </ul> <p>Weight</p>

	<ul style="list-style-type: none"> <li>• 578g (1.3lb)</li> </ul> <p>Mounting</p> <ul style="list-style-type: none"> <li>• Wall, Drop ceiling, Desk</li> <li>• Secure bracket (sold separately)</li> </ul>
Environmental	<p>Operating Temperature</p> <ul style="list-style-type: none"> <li>• 0°C (32°F) - 40°C (104°F)</li> </ul> <p>Operating Humidity</p> <ul style="list-style-type: none"> <li>• Up to 95%, non-condensing</li> </ul>
Price (per unit)	RM 3703.00

**Table 7: Ruckus R610 access point** [CITATION Ruc18 \l 17417 ]



**Figure 5: Aruba 300 Series Access Point**

Model	Aruba 300 Series Entry-level 802.11ac Wave 2 Access Points
Features / Specifications	<ul style="list-style-type: none"> <li>• AP-304 (controller-managed) and IAP-304 (Instant): <ul style="list-style-type: none"> <li>- 5GHz 802.11ac 3x3 MIMO (1,300 Mbps max rate) and</li> <li>- 2.4GHz 802.11n 2x2 MIMO (300 Mbps max rate) radios,</li> <li>- three dual-band RP-SMA connectors for external antennas.</li> </ul> </li> <li>• AP-305 (controller-managed) and IAP-305 (Instant): <ul style="list-style-type: none"> <li>- 5GHz 802.11ac 3x3 MIMO (1,300 Mbps max rate) and</li> <li>- 2.4GHz 802.11n 2x2 MIMO (300 Mbps max rate) radios,</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>- three integrated omni-directional down tilt dual- band antennas</li> </ul>
Data Rate	<ul style="list-style-type: none"> <li>- Supports up to 1,300 Mbps in the 5GHz band and up to 300 Mbps in the 2.4GHz band</li> </ul>
Capacity	<ul style="list-style-type: none"> <li>• Support for up to 256 associated client devices</li> </ul>
Frequency	<ul style="list-style-type: none"> <li>• Supported frequency bands (country-specific restrictions apply):</li> <li>- 2.400 to 2.4835GHz</li> <li>- 5.150 to 5.250GHz</li> <li>- 5.250 to 5.350GHz</li> <li>- 5.470 to 5.725GHz</li> <li>- 5.725 to 5.850GHz</li> </ul>
Mechanical	<ul style="list-style-type: none"> <li>• Dimensions/weight (unit, excluding mount accessories):</li> <li>- 165mm x 165mm x 38mm</li> <li>- 460g</li> <li>• Dimensions/weight (shipping):</li> <li>- 205mm x 205mm x 52mm</li> <li>- 620g</li> </ul>
Environmental	<ul style="list-style-type: none"> <li>• Operating:</li> <li>- Temperature: 0° C to +50° C (+32° F to</li> </ul>

	+122° F) - Humidity: 5% to 93% non-condensing • Storage and transportation: - Temperature: -40° C to +70° C (-40° F to +158° F)
Price (per unit)	RM2466.89

***Table 8: Aruba 300 Series [ CITATION Aru18 \l 17417 ]***





**Figure 6: Ubiquiti UAP-AC-PRO Access Point**

Model	Ubiquiti UniFi UAP-AC-PRO 802.11ac Access Point
Features / Specifications	<ul style="list-style-type: none"> <li>• Support Guest Traffic Isolation</li> <li>• Advanced QoS</li> <li>• Wireless security: <ul style="list-style-type: none"> <li>-WEP, WPA-PSK, WPA-Enterprise (WPA/WPA2, TKIP/AES)</li> </ul> </li> <li>• 3 Dual-band antennas, 2.4 GHz: 3dBi, 5GHz: 3dBi</li> </ul>
Data Rate	6.5 Mbps to 1300 Mbps (MCS0 - MCS9 NSS1/2/3, VHT 20/40/80)
Capacity	<ul style="list-style-type: none"> <li>• 250+ devices</li> </ul>
Frequency	2.4 GHz  5 GHz
Mechanical	Dimension <ul style="list-style-type: none"> <li>• 196.7 x 196.7 x 35 mm (7.74 x 7.74 x 1.38")</li> </ul> Weight <ul style="list-style-type: none"> <li>• 350 g (12.4 oz)</li> </ul>

	<ul style="list-style-type: none"> <li>• 450 g (15.9 oz) – with mounting kits</li> </ul>
Environmental	<ul style="list-style-type: none"> <li>• Operating Temperature</li> </ul> <p>-10 to 70° C (14 to 158° F)</p> <ul style="list-style-type: none"> <li>• Operating Humidity</li> </ul> <p>5 to 95% Noncondensing</p>
Price (per unit)	RM885.00

***Table 9: Unifi UAC-AP-Pro [ CITATION Ubi18 \l 17417 ]***

### Justification and Recommendations for Access Point

Based on some consideration and research done, Aruba 300 Series access point has been chosen to be deployed at the Bario Clinic and the telecentre. Aruba has been well-recognised among technology company for being one of the brands that provide good quality of product. For this 300 Series access point, its scalable feature suits very well with the condition and environment at Bario community as it supports a capacity of up to 256 devices [ CITATION Aru18 \l 17417 ]. Bario is assumed to be a medium scale community and is not well-developed yet in terms of its technology, therefore as for now the capacity provided by this access point is sufficient to cover all users at a time. In economic terms, it is cheaper compared to some other brands, but it is not the cheapest. As one knows, a good quality product is not always cheap, and it is worth the price because it has a reliability of 127 years if it is operating at a temperature of +25°C, and a warranty for one year is also given upon purchasing of the access point. Aruba 300 series can be delivered with the current technology and can be use in a long term as it supports the standard of up to 802.11ac which is a common standard being use at the moment. Another benefit of deploying Aruba 300 Series AP is it equipped with a multiuser MIMO and supports up to 300Mbps in the 2.4GHz band, with 2SS/HT40 clients, and up to 1,300 Mbps for the other 5GHz band, with 3SS/VHT80 clients [ CITATION Aru18 \l 17417 ]. This can ensure the user's connection and the efficiency of the network.

## Controller



**Figure 7: Ruckus ZoneDirector 1200 Series Enterprise-Class Smart Wireless Lan Controller**

Model	Ruckus ZoneDirector 1200 Series Enterprise-Class Smart Wireless Lan Controller
Power	External power adapter Input: 110 - 240V AC Output: 12V DC, 1A
Ethernet Port	2 Ethernet ports, auto MDX, autosensing 10/100/1000 Mbps 1 Console RJ-45 port
Environmental Conditions	Operating temperature: 32° F (0°C) - 104°F (40°C) Operating humidity: 20% - 90% non-condensing
Capacity	Managed Aps: Up to 75 WLANs (BSSIDs): 256 Concurrent Stations: Up to 2,000
Applications	Hotspot: WISPr Guest Access: Supported

	<p>Captive Portal: Supported</p> <p>Mesh: Supported</p> <p>Voice:</p> <ul style="list-style-type: none"> <li>-802.11e/WMM</li> <li>-U-APSD</li> <li>-Tunnelling to AP</li> </ul>
Security	<p>Standards: WPA, WPA2, 802.11i</p> <p>Encryption:</p> <ul style="list-style-type: none"> <li>-TKIP, AES</li> <li>-Ruckus Dynamic Pre-Shared Key</li> </ul> <p>Authentication: 802.1x, MAC address</p> <p>User Database:</p> <ul style="list-style-type: none"> <li>-Internal database up to 2,000 users</li> <li>-External: RADIUS, LDAP, Active Directory</li> </ul> <p>Access Control:</p> <ul style="list-style-type: none"> <li>-L2 (MAC address-based)</li> <li>-L3/4 (IP and Protocol based)</li> <li>-L2 client isolation</li> <li>-Management interface access control</li> <li>-Time-based WLANs</li> </ul> <p>Wireless Intrusion Detection (WIDS)</p> <ul style="list-style-type: none"> <li>-Rogue AP detection</li> <li>-DoS attack prevention</li> <li>-Evil-twin/AP spoofing detection</li> </ul>

	-Ad hoc detection -Password guessing protection
Price (per unit)	RM4579.90

**Table 10: Ruckus ZoneDirector 1200[ CITATION Ruc181 \l 17417 ]**



**Figure 8: Aruba 7000 Series Mobility Controller**

Model	Aruba 7000 Series Mobility Controller
Power	190 W (with PoE)
Ethernet Port	2 SFP Gigabit Ethernet port 2 USB 2.0 Console port (micro-USB/RJ-45)
Environmental Conditions	Operating temperature: 0° C to 40° C Storage temperature: -40° C to 70° C Humidity/storage humidity: 10% to 95%, non-condensing Operating altitude: 10,000 feet
Capacity	Maximum concurrent users/devices: 2048 Maximum campus AP licenses: 32 Maximum remote AP licenses: 32
Security	32,768 active firewall session 4 Gbps firewall throughput 2.4 Gbps Encrypted throughput (3DES, AES-CBC) 3.4 Gbps Encrypted throughput (AES-CCM)

Price (per unit)	RM1463.88
------------------	-----------

**Table 11: Aruba 7000 Series [ CITATION Aru181 \l 17417 ]**





**Figure 9: Cisco 3504 Wireless Controller**

Model	Cisco 3504 Wireless Controller
Power	<p>Power adapter: Input power: 100 to 240 VAC, 50/60 Hz</p> <p>Heat dissipation (without PoE): 47W, 160BTU/hr</p> <p>Heat dissipation (with PoE): 98W, 335BTU/hr</p>
Ethernet Port	<p>1x Multigigabit Ethernet interface (up to 5 Gigabit Ethernet) + 4x 1 Gigabit Ethernet interfaces (RJ-45)</p> <p>1x service port: 1 Gigabit Ethernet port (RJ-45)</p> <p>1x redundancy port: 1 Gigabit Ethernet port (RJ-45)</p> <p>1x console port: Serial port (RJ-45)</p> <p>1x console port: Serial port (mini-B USB)</p> <p>1x USB 3.0 port</p>
Environmental Conditions	<p>Operating Temperature: 32 to 104 °F (0 to 40°C)</p> <p>Storage Temperature: -4 to 158 °F (-20 to 70°C)</p>

	<p>Operating Humidity: 5% to 95% RH non-condensing</p> <p>Storage Humidity: 0% to 95% RH non-condensing</p>
Capacity	<p>Supports up to 150 APs</p> <p>Up to 3000 clients</p>
Applications	<p>Cisco VideoStream technology optimizes the delivery of video applications across the WLAN</p> <p>Simplified GUI wizard for quick setup, and intuitive dashboards for monitoring and troubleshooting</p>
Security	<p>Standards:</p> <ul style="list-style-type: none"> <li>● Wi-Fi Protected Access (WPA)</li> <li>● IEEE 802.11i (WPA2, RSN)</li> <li>● RFC 1321 MD5 Message-Digest Algorithm</li> <li>● RFC 1851 Encapsulating Security Payload (ESP) Triple Data Encryption Standard (3DES) Transform</li> <li>● RFC 2104 HMAC: Keyed Hashing for Message Authentication</li> <li>● RFC 2246 Transport Layer Security (TLS) Protocol Version 1.0</li> <li>● RFC 2401 Security Architecture for the Internet Protocol</li> <li>● RFC 2403 HMAC-MD5-96 within ESP and Authentication Header (AH)</li> <li>● RFC 2404 HMAC-SHA-1-96 within ESP and AH</li> <li>● RFC 2405 ESP DES-CBC Cipher Algorithm with Explicit IV</li> </ul>

	<ul style="list-style-type: none"> <li>● RFC 2407 Interpretation for Internet Security Association and Key Management Protocol (ISAKMP)</li> <li>● RFC 2408 ISAKMP</li> <li>● RFC 2409 Internet Key Exchange (IKE)</li> <li>● RFC 2451 ESP Cipher Block Chaining (CBC)-Mode Cipher Algorithms</li> <li>● RFC 3280 Internet X.509 Public Key Infrastructure (PKI) Certificate and Certificate Revocation List (CRL) Profile</li> <li>● RFC 4347 Datagram Transport Layer Security</li> <li>● RFC 5426 TLS Protocol Version 1.2</li> </ul> <p>Encryption:</p> <p>Wired Equivalent Privacy (WEP) and Temporal Key Integrity Protocol-Message Integrity Check</p> <p>(TKIP-MIC):</p> <ul style="list-style-type: none"> <li>● RC4 40, 104 and 128 bits (both static and shared keys)</li> <li>● Advanced Encryption Standard (AES): CBC, Counter with CBC-MAC (CCM), Counter with CBC Message Authentication Code Protocol (CCMP)</li> <li>● Data Encryption Standard (DES): DES-CBC, 3DES</li> <li>● Secure Sockets Layer (SSL) and TLS: RC4 128-bit and RSA 1024- and 2048-bit</li> <li>● DTLS: AES-CBC</li> <li>● IPsec: DES-CBC, 3DES, AES-CBC</li> </ul>
--	---

	<ul style="list-style-type: none"> <li>● 802.1AE MAC sec encryption</li> </ul>
Price (per unit)	RM10,340.00

**Table 13: CISCO Wireless 3504 [ CITATION cis17 \l 17417 ]**

#### Justification and Recommendations for Controller

A good controller can manage and support all the access point in the particular network. As for Bario clinic and telecentre, the preferred controller is Aruba 7000 Series Mobility Controller as it is the more compatible device in terms of its technical, operational and economic factors. One of the reasons for proposing this particular controller is because of its compatibility with the access point that has been recommended earlier. Some controller will not be able to be functioning well with access point from a different brand due to some configuration and manufacturing reasons. Hence, choosing devices from the same company seems to be more suitable and can avoid any unnecessary problems afterwards. At the same time, this controller helps to eliminate the need to re-architect the available network at both Bario telecentre and clinic every time if there is any additional or changes applied because it able to manage light-weight access points in large quantities, a maximum of 64 access points and 2048 concurrent devices to be more specific [ CITATION Aru181 \l 17417 ]. Addition of the relevant and compatible access point is the only thing involves in the future if the clinic is to be upgraded into a bigger organization, in this case it may be develop into a medium-sized hospital. The configuration for the access points and other related devices and addresses can be done just at the controller instead of having to configure on each of the access points. This saves a lot of time and energy. Moreover, both the clinic and telecentre at Bario can gain benefits with a high-quality product at a very affordable price which is only around RM1,000 to RM2,000. Aruba 7000 Series also offers a quite great security for the network despite its ability to support over 4,000 users. The secure IP tunnels protect the traffic across the transport network to data centre. It also can perform stateful firewall policy enforcement, secure VPN, and threat management with content filtering [ CITATION Aru181 \l 17417 ].



## Wireless Bridge



***Figure 10: Ruckus P300 Wireless Bridge***

Model	Ruckus P300 Wireless Bridge
Features	<p>802.11ac Point to Point or Point to Multi Point Bridge</p> <ul style="list-style-type: none"><li>• 5GHz operation</li><li>• 20MHz, 40MHz, and/or 80MHz channelization</li><li>• 14dBi internal directional antenna</li><li>• 2 external N-Type antenna connectors</li><li>• 802.3af Power over Ethernet</li><li>• Maximum link distance 12 km (using internal antenna)</li><li>• Dedicated radar avoidance pre-scan (DFS)</li></ul>

	<ul style="list-style-type: none"> <li>• PD-MRC for reliable bridge connections</li> <li>• Simple installation with mounting brackets included</li> <li>• Automatic pairing and easy aiming between bridges</li> <li>• Optional accessories available to enhance range &amp; performance</li> </ul>
Power	802.3af Power over Ethernet
Antenna	<ul style="list-style-type: none"> <li>• 14 dBi internal directional antenna</li> <li>• 30degree 3dB beam width</li> <li>• Two external N-Type antenna connectors</li> </ul>
Maximum Link Distance	• 12 kilometres
Wireless Security	• WPA2 AES
Target UDP Throughput	<ul style="list-style-type: none"> <li>• Up to 500Mbps</li> <li>• Up to 250Mbps at 2.6 km/1.6 mi</li> <li>• Up to 100Mbps at 8 km/5 mi**</li> </ul>
Environment	<ul style="list-style-type: none"> <li>• IP-67 rated</li> <li>• Operating air temperature: -40°C to 65°C (-40°F to 149°F)</li> </ul>
Price (per unit)	RM3717.76

**Table 14: Ruckus P300 Wireless Bridge [ CITATION ruc17 \l 17417 ]**



**Figure 11: Aruba 501 Wireless Client Bridge**

Model	Aruba 501 Wireless Client Bridge
Features	<ul style="list-style-type: none"> <li>• Radios (built-in): 802.11 a/b/g/n/ac</li> <li>• Radio operation modes: Client bridge</li> <li>• Wi-Fi Alliance Certification: a/b/g/n/ac Wi-Fi Certified</li> <li>• Antenna connector: Three RP-SMA</li> <li>• Antenna: 2dBi dual-band omnidirectional</li> <li>• Number of external antennas: 3</li> <li>• Three spatial streams for up to 1.3 Gbps PHY rate</li> <li>• Three RP-SMA connectors for a range of antenna options</li> </ul>
Power	<ul style="list-style-type: none"> <li>• 9 W from external DC power source</li> <li>• 11 W from PoE power source</li> </ul>
Antenna	<ul style="list-style-type: none"> <li>• 2dBi dual-band omnidirectional</li> <li>• Number of external antennas: 3</li> </ul>



Maximum Link Distance	Up to 9 kilometres
Security	<ul style="list-style-type: none"> <li>• IEEE 802.1X support</li> </ul> <p>Provides user authentication with support for EAP-TLS and PEAP—with choice of Advanced Encryption Standard</p> <p>(AES), Temporal Key Integrity Protocol (TKIP), and Wired</p> <p>Equivalent Privacy (WEP) encryption for protecting wireless</p> <p>traffic between authenticated clients and the access point</p> <ul style="list-style-type: none"> <li>• Choice of IEEE, WPA2, WPA, or WEP</li> </ul> <p>Secures the data integrity of wireless traffic, using robust</p> <p>AES or TKIP encryption</p>
Environment	<ul style="list-style-type: none"> <li>• Operating temperature: 32°F to 122°F (0°C to 50°C)</li> <li>• Operating relative humidity: 5% to 95%, noncondensing</li> <li>• Nonoperating/Storage temperature: -40°F to 158°F (-40°C to 70°C)</li> </ul>

	<ul style="list-style-type: none"> <li>• Nonoperating/Storage relative humidity: 5% to 95%, noncondensing</li> <li>• Shock and vibration: EN 61373</li> <li>• Altitude: 10,000 feet (3,048 meters)</li> </ul>
Price (per unit)	RM1543.35

**Table 15: Aruba 501 Wireless Client Bridge [ CITATION Aru182 \l 17417 ]**



**Figure 12: Ubiquiti PowerBridge M10 (10 GHz Carrier Class airMAX PtP Bridge with Dish Antenna)**

Model	Ubiquiti PowerBridge M10 (10 GHz Carrier Class airMAX PtP Bridge with Dish Antenna)
Features	Innovative Industrial Design - Only a screwdriver and adjustable wrench are needed for radio installation and pole-mounting.

	<p>Licensed Band Advantage - The PowerBridge M10 is the ideal solution for crowded wireless environments. For more capacity and reliability, the 10 GHz licensed band has significantly less noise than the 2.4 and 5 GHz unlicensed bands.</p> <p>Powerful airOS Features - Ubiquiti's versatile airOS firmware technology enables high-performance, outdoor multi-point networking. airOS provides features such as custom wireless settings, bridge or routing configuration, and system management services.</p>
Power	24V, 1A PoE Supply included
Maximum Link Distance	Capable of high speed 20km+ links.
Security	WEP, WPA, WPA2
Target UDP Throughput	Up to 150+ Mbps
Environment	<p>Operating Temperature -40 to 80° C</p> <p>Operating Humidity 5 to 95% Condensing</p>
Price (per unit)	RM2923.59

**Table 16: Ubiquiti Powerbridge M10 [ CITATION ubi11 \l 17417 ]**

### Justification and Recommendations for Wireless Bridge

The recommendation of a suitable wireless bridge to be deployed for Bario clinic and telecentre is Aruba 501 Wireless Client Bridge. This bridge performs in linking distant access points together. Since the clinic is located about 200 metres away from the telecentre, there is a high probability that the wi-fi signal transmitted from the telecentre not reaching the clinic. As this wireless bridge's maximum link distance is approximately 9 kilometres, it is indeed can aid in connecting the network. It can link up to 15 devices to the specific wireless network at high speeds. This device supports for IEEE 802.11b/g/n and also 802.11a/n/ac WLAN networks [ CITATION Aru182 \l 17417 ]. This shows that this bridge can support with other device on the WLAN including the access point. Its cost-effective feature also one of the justifications for choosing it instead of other wireless bridge. The price for each unit of it is only about RM1,500, which is cheaper than the others. Aruba 501 Wireless Bridge provides user authentication with choices that include Advanced Encryption Standard (AES), Temporal Key Integrity protocol (TKIP), IEEE, WPA, WPA2 and Wired Equivalent Privacy (WEP) encryption [ CITATION Aru182 \l 17417 ]. In simple words, it ensures the protection of the wireless traffic and secures the integrity of the user's data.

### 3.2.2 Software Requirements

At the same time, software requirements need to be taken into account too. This includes the firmware or operating system for the devices related in the WLAN deployment such as the access point, controller and wireless bridge. Firmware is permanent or fixed software programmed into a read-only memory of the device, either erasable read-only memory (EROM) or electrically erasable programmable read-only memory (EEPROM). It serves as the fundamental software for the system or device. The firmware usually comes with extra features including error correction technology, playback control technology and secure burning technology [ CITATION Mar06 \l 17417 ]. This firmware or software specification is highly depending on the devices or the hardware. For the hardware that has been chosen, the software required are ArubaOS 8.3.0.0 and V2.0.0.2-Aruba 501-B0019. ArubaOS 8.3.0.0 or also known as AOS8.3.0.0 works with the access point and also controller while the V2.0.0.2 is needed for the wireless bridge.

- **AOS 8.3.0.0**

AOS 8.3.0.0 is a newer version released and it is technically better than the previous AOS 8.2.0.2 version. Many enhancements have been done to this operating system. One of them are the load balancing of the active APs. This is done to make sure that fewer APs failover when a managed device fails. Another enhancement for this particular version of operating system is AP fast recovery, where one can configure this feature from the AP system profile. It is applicable with Aruba 300 Series; the same access points as recommended in the hardware part. When a firmware asserts is detected, this feature aims to minimize the AP downtime [CITATION Pac18 \l 17417 ].

- **V2.0.0.2-Aruba 501-B0019**

On the other hand, V2.0.0.2-Aruba 501-B0019 software is installed in Aruba 501 Client Bridge. The adoption of this software into the wireless bridge stated in hardware section can fix bugs and issues that has arisen before including issue in which the MAC Translation table was not updated when the Aruba 501 was rebooted, the device stopped

bridging traffic across the wireless uplink when the radio mode was set to Auto, and an issue in which if the Aruba 501 roamed to a different AP that had no network connectivity. Despite being able to fix some issues, it also arises with another issues. Issues exists in this version are related with an error occurs when selecting SSID that contains a backslash (\) from the station profile drop-down list, a fixed channel cannot be specify when taking a wireless trace on the Aruba 501. However, some enhancements are included in this software version despite of this issues. This consists of the updated DHCP client behaviour when the Aruba 501 does not get a DHCP IP address. When it disassociates from one AP and associates with a new AP, the Aruba 501 allows DHCP to run, acquires a DHCP address in less than 30 seconds, otherwise it uses the static IP address for the network. It also can disable DHCP and then enables the MAC cloning [CITATION Hew18 \l 17417 ].

#### Justification and Recommendations for Software Requirements

As mentioned above, both operating system and firmware are going to be installed and deployed to the Bario clinic and telecentre as the hardware specifies requires them. Moreover, AOS 8.3.0.0 and V2.0.0.2-Aruba 501-B0019 are the newer version release so far and it assist the network to be well-functioning and reduce the downtime of the network. Up-to-date version of software usually is reliable as it helps in detecting and fixing bugs or any issues and it is more secured.

### **3.3 Security Implementation Requirements**

As the wireless technology is growing to be widely used in different fields of business, because of the ease of using it, since it just depends on the signal that broadcast through the air, which will allow the user to freely roam around while still connected to the network. However, this feature can also cause some security threats. Because the signal is not confined within a wall of a building, an unauthorised user can pick the signal from outside the building, for example if an attacker is in the car parking of a company, he might pick the signal and then tries to access the secure internal network and steal some sensitive information. So, it is important for Bario Clinic and Tele centre to take the necessary action and prober security method to secure the WLAN network against those attacks and threats. First, we need to deeply understand the main security threats that Bario Clinic wireless LAN might face, to set up the most prober security method to overcome them.

### 3.3.1 Potential Threats Affecting WLAN

There are lots of different attacking methods that hackers would use to trick any organization. Down we will be discussing some of these security threats, then we will conclude by providing some possible solutions that Bario Clinic and the Tele -centre may implement to prevent and defend against those threats.

Threat	Description
Rogue Access points	A rogue access point is a wireless AP that attackers tend to install within the range of a secured network without the authorization of the network administrator. The idea of that is to trick some legitimates devices to connect to this fake access point over the real legitimate access point. The extreme dangerous part in this method is when the attacker succeeds to gain an access to a physical port on the wireless network, then hook the rogue access point into this port, lots of devices would get associated with that rogue access point which enables the attacker to capture data through it for long period of time without grapping their attention (Ph.D, 2014).
Eavesdropping Attack	It is an attack where someone tries to steal information that is been transmitted through an unsafe network. And these types of attacks are mostly hard to detect, because there is no abnormality identified in network transmissions. It is mostly dangerous for those who are using public networks, because the protection level is so low, but even for private wireless networks which is our case in Bario clinic and the telecentre, Eavesdropping Attack is not something to be ignored and it might cause problems, if the right security protocols are not implemented properly. This attack is categorized under Man in



	<p>the Middle threats (MiM). In our Barrio clinic and telecentre, since employees will be sending and receiving lots of emails, so it is attracted to attackers listen to this data and interrupt it using eavesdropping attack (Journals.sagepub.com, 2018).</p>
--	---

***Table 17: List of threats***

## Justification and Recommendations for Security Threats

A rogue access point, and Eavesdropping have been serious problems for lots of companies that are implementing a wireless network, but still there are some policies and solution that can be taken to detect, protect and prevent from these types of threats. The most popular method is called NAC appliances, stands for Network Access Control, which is normally used in protecting and defending against such attacks. The way this method works is that it allows network administrator to validate identities, which mean, they will get to know all the devices that are connected to the network and who are the users of those devices. Plus, checking wither those users exist in the directory services. if not, then it is most probably a rogue device. For Eavesdropping, NAC can help in preventing unauthorised users getting onto your network in the first place, so it will give eavesdropping attackers tough time.

Another method in detecting the rogue access point is to use some special sensor called wireless probe, which is a device that can monitor the airwaves for traffic. However, in our case for Bario clinic and telecentre, they will not really need to worry about implementing those mention methods and security appliances, due to the security features that our chosen AP (Aruba 300 series) provides. One of the main security specifications that (Aruba 300 series) has, is the Integrated wireless intrusion protection that offers protection and mitigation for the network, as well reduces and eliminates the need for separate RF sensors or security appliances such as NAC appliances we mentioned earlier. We must also put into consideration the importance of implementing prober authentication and encryption methods, which we will be discussing in detail later (Aruba, 2018).

### 3.3.2 Algorithms

Two important aspects in the process of wireless network security are authentication and encryption.

#### Authentications

Authentication is distinct from authorization, which is mainly the process of allowing user to access the network by connecting to the AP based on validating their username, password along with their MAC address. There are several types of wireless authentication methods, but we will be mainly focusing on three of them, which are Open authentication, Shared key authentication and EAP authentication.

Authentication method	Description
Open authentication	<p>Open system authentication is the default authentication protocol for 802.11 standard. It basically contains a simple authentication request which includes the station ID, as well an authentication response which includes success or failure data. Once the authentication is successfully done, both stations are to be mutually authenticated.</p> <p>On other words once, the client gets to know the SSID of the AP intending to connect to, they will send an authentication frame(request), then the other station(AP) will receive this request and responds back with an authentication response.</p> <p>This kind of authentication usually used with WEP (Wired Equivalent Privacy) protocol to help in providing better security for communication. However, it is important to put into consideration that the main disadvantage of using open authentication method is that the management frames are still sent in clear text during authentication process, which means that WEP is only used to encrypt data once the client is authenticated and associated. That means in conclusion that anyone can send their station ID in attempt to associate with the AP that</p>

	<p>implements the open authentication, which leads us to know that indeed no authentication is done (Ph.D, 2014).</p>
Shared key authentication	<p>Shared Key Authentication is a standard challenge and response mechanism. The way this method works is that the client will first sends an authentication request as it happens in the open authentication method. However, the difference is that the other side station (AP) will not directly send an authentication response. Instead it will send challenge text that asks for the shared secret key. Once the client resends the encrypted challenge text. The AP will decrypt the text and the authentication succeeds if the same shared secret key is decrypted. After that the client will be connected to the network (Ph.D, 2014).</p> <p>The diagram below illustrates the shared key authentication process.</p> <p><b>802.11 Authentication Shared Key Steps</b></p> <ol style="list-style-type: none"><li>1) Authentication request sent to AP</li><li>2) AP sends challenge text</li><li>3) Client encrypts challenge text and sends it back to AP</li><li>4) AP decrypts, and if correct, authenticates client</li><li>5) Client connects to network</li></ol> <p>The diagram shows a client attempting to connect to an Access Point (AP). The AP is connected to a network with servers and PCs, and also to the Internet via a cable or DSL modem.</p>

(Figure 13: Key Shared authentication)

<p>Extensible authentication protocol</p>	<p>EAP is a framework that helps structuring security protocols to provide a shape of request\response environment over which we implement specific authentication algorithms. EAP has couple of different methods, the common used ones are: EAP-MD5, EAP-TLS, and EAP-PEAP.</p> <p>For the best security performance, the EAP-TLS is used, which is based on the Transport layer security.</p> <p>The way that EAP types implements the authentication process is by providing mutual authentication between the client/supplicant, authenticator/AP, and the RADIUS server. The figure below illustrates the steps involving in implementing the Extensible authentication protocol process (Ph.D, 2014).</p> <div data-bbox="503 835 1274 1438"> <pre> sequenceDiagram     participant Client as Client (VLAN 10)     participant Switch as Switch     participant RADIUS as RADIUS Server (VLAN 1)      Client-&gt;&gt;Switch: EAP Identity Request     Switch-&gt;&gt;Client: EAP Identity Response     Switch-&gt;&gt;RADIUS: RADIUS Access Request     RADIUS-&gt;&gt;Switch: RADIUS Challenge Req.     Switch-&gt;&gt;Client: EAP Challenge Request     Client-&gt;&gt;Switch: EAP Challenge Response     Switch-&gt;&gt;RADIUS: RADIUS Challenge Resp.     RADIUS-&gt;&gt;Switch: RADIUS Access Accept </pre> </div> <p>(Figure 14: EAP)</p>
---	--

**Table 18: Description of authentication**

## Encryption

Traffic Encryption is data passing between the access point and clients must be protected from interception and eavesdropping.

Encryption method	Description
Wired Equivalent Privacy (WEP):	Wired Equivalent Privacy (WEP) is a security protocol designed to ensure that only authorized clients can view transmitted wireless information. WEP uses RC4 algorithm to encrypt the data once it is sent out from the user laptop wireless network card or the access point. Each byte of data will be encrypted using a different packet key. That means, even if a hacker manages to crack a specific packet, he still can't get access into the network, because the information that are leaked is only the one contained in that packet Ph.D, 2014).
Wi-Fi Protected Access (WPA)	It is a type of security protocol which has been developed by Wi-Fi Alliance purposely to secure wireless networks with better data encryption and user authentication comparing to wired equivalent privacy, which is the original Wi-Fi security protocol. WPA ensure better authentication by using two protocol standards, RC4, as well Temporal Key Integrity Protocol(TKIP) Ph.D, 2014).
Wi-Fi Protected Access 2 (WPA2)	In September 2004 the Wi-Fi Alliance introduced to the world Wi-Fi Protected Access 2 (WPA2), that was the second generation of WPA security protocols. WPA2 use the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) and Advanced Encryption Standard (AES) technology to implement encryption Ph.D, 2014).

RC4.	<p>RC4 is one of the most popular and commonly used software stream chipper, which is mainly used in protocols, such as WEP, WPA for encryption. It is used due to its high speed and the simplicity of software. The way it works is that it generates a pseudo-random stream of bits (key stream) just like other stream chippers. Then, It does the encryption and decryption process by combining that generated key stream with the plaintext using an exclusive OR (XOR) operation. RC4 in fact could be used as block cipher as well. However, it is pretty much known that it is not so effective when it is used as block cipher (VOCAL Technologies, 2017).</p>
AES	<p>AEC Advanced Encryption Standard is a symmetric encryption algorithm. It was developed by two Belgian cryptographer Joan Daemen and Vincent Rijmen. AES takes plaintext and convert it to cipher text. In June 2003, U.S government announce that AES could be used to protect classified and sensitive information. As of today, AES become the most used and secure encryption algorithm. The AES algorithm uses a 128-bit key, so it is kind of so hard for an attacker to hack into the network. That is why so far, no practicable attack against AES exists (Boxcryptor.com, 2018).</p>
RC4 VS AES	<p>in comparison between RC4 and AES, we would say that RC4 is very old and simple, whereas AES is very new and complex. Another difference is that RC4 is stream chipper whereas AES is a block chipper. AES is extremely secure whereas RC4 is not so. Lastly, RC4 is away faster than AES (Joan, 2010).</p>

***Table 19: Description of encryption***

### Comparison between the encryption methods

<b>Types of encryption methods</b>	WEP	WPA	WPA2
<b>Name</b>	Wired Equivalent Privacy	Wi-Fi Protected Access	Wi-Fi Protected Access 2
<b>Authentication</b>	Uses WEP key	Uses 802.1x & EAP	Uses 802.1x & EAP
<b>Encryption</b>	Uses RC4	RC4/ TKIP	Uses AES
<b>Security</b>	Weak	Stronger	Strongest

***Table 20: Comparison of encryption methods***

### Justification and Recommendations for Authentication and Encryption

Speaking of both Bario telecentre and Bario clinic Wireless network security, our team has recommend using WPA2 with AES for encryption, along with using EAP for authentication, due to the fact that it is more secure and stronger and feasible than using WPA with TKIP/ RC4 and WEP with IV, RC4. Intruders are always looking for week Wireless networks but with setting up the right configurations and strong Password for the wireless network Bario telecentre's and clinic's communication and data will be protected against any harmful attacks. EAP authentication might be a bit difficult to implement due to its complexity but because it is better to focus more on breach containment, it is suggested that they stick with it since it is the most common method in terms of securing the Wireless network. Since AP (ARUBA 300 SERIES) and bridges have been utilized, they are supported by WPA2 protocol Standard, so it is



a way better to use this security method for both Barrio clinic and telecentre whether it is in the indoors or outdoors communication as well to secure the data transferred for the reason that WPA2 offers strong encryption using 128-bit key.

### **3.4 WLAN - Monitoring and Maintenance Considerations**

#### **3.4.1 Monitoring WLAN**

It is a method of monitoring, scanning and analyzing wireless data communication among end-user devices within WLAN area. In order to reach failure free wireless network performance with high availability and strong security system, several methods do exist. Network monitoring is generally carried out through software applications and tools. These tools allow network administrator to make wired and wireless network monitoring, web mailing and browsing, network traffic monitoring and many more. Monitoring WLAN implemented, in order to reach stage of high efficiency, affordability and failure free status. (Technopedia, 2017)

As any other methods it has own implementation difficulties and functioning issues. These monitoring issues such as covering entire WLAN infrastructure which includes software and hardware monitoring, it comes difficult to monitor whole if it has huge scales. Besides, several issues can occur while scanning and troubleshooting enterprise wireless network. And lastly, identifying network weakness and documenting correct statistics of traffic, bandwidth and overall WLAN performance. (Lifewire, 2017)

## Monitoring Tools of Software and Hardware:

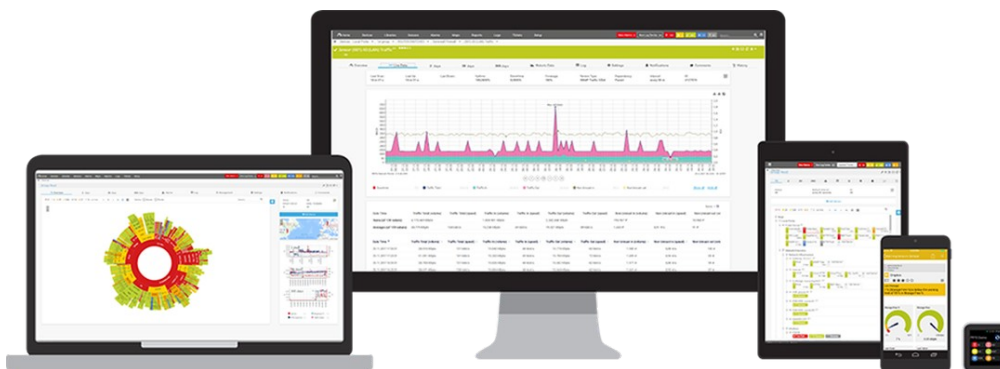
- **PRTG Network Monitor Tool**

Amount of existing monitoring tools, software and applications in IT market is very wide. And this marketplace is being developed and expanded by each year and competition between manufacturers is pretty high. Among huge variety of monitoring applications one of the top tools been considered which are Zabbix an open source monitoring tool, ConnectWise cloud-based monitoring app, OP5 Monitor an enterprise level monitoring software and lastly, PRTG Network Monitor tool. (Wilson, 2017).

Compare to other mentioned monitoring applications PRTG Network Monitor was selected for Bario Health Clinic as main WLAN monitoring tool due to the huge variety of offered featural advances, cost affordability and known practical efficiency.

PRTG (Paessler Router Traffic Grapher) is a network monitoring software by Paessler AG company. This software able to monitor, collect statistics from hosts like switches, routers, servers and classify system conditions as bandwidth usage, network mapping etc. PRTG Monitor provides auto- discovery mode which scans given area of enterprise network and makes device list from scanned data. (Paessler, 2018)

Current tool is working based on sensors which are adjusted for different specific tasks. It has application and hardware sensors particularly for switches, routers and servers. After sensors monitor system for response time, bandwidth, memory etc., all details will be converted to statistics and provide network status.



**Figure 15: PRTG Monitoring**

PRTG Network Monitor allows to monitor entire IT infrastructure and categorizes data traffic within a network to show accurate results of network traffic and usage trends. It displays the results in various easy to read tables and graphs. One of the main monitoring options of this software are listed below:

- Bandwidth Monitoring
- Port Monitoring
- Network Mapping
- Database Monitoring
- Wi-Fi Monitoring
- WLAN Diagnosis

In terms of feasibility, operational, technical and economical feasibility studies were considered to estimate overall feasible performance of represented tool. A feasibility study aims to objectively and rationally observe the strengths and weaknesses of presented enterprise; To calculate its expenses, in order to, estimate further benefit and coverage of spend cost. (Investopedia, 2016).

PRTG Monitor Tool considered as economically feasible according to its affordable price within company's operational budget. Coming to the operational feasibility, current application is highly suitable in long term use and working on high level performance as well as further usage benefits to monitor the WLAN and the Internet connection. According to the following reasons, this application considered as feasible for usage in future perspectives.

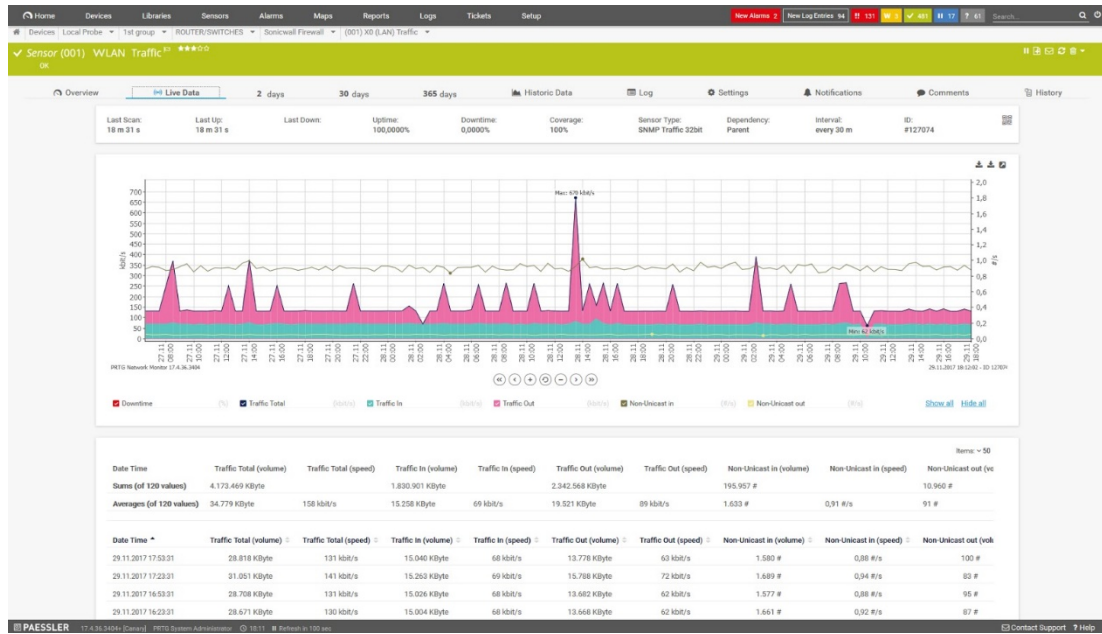


Figure 16: PRTG WLAN Traffic Scaling

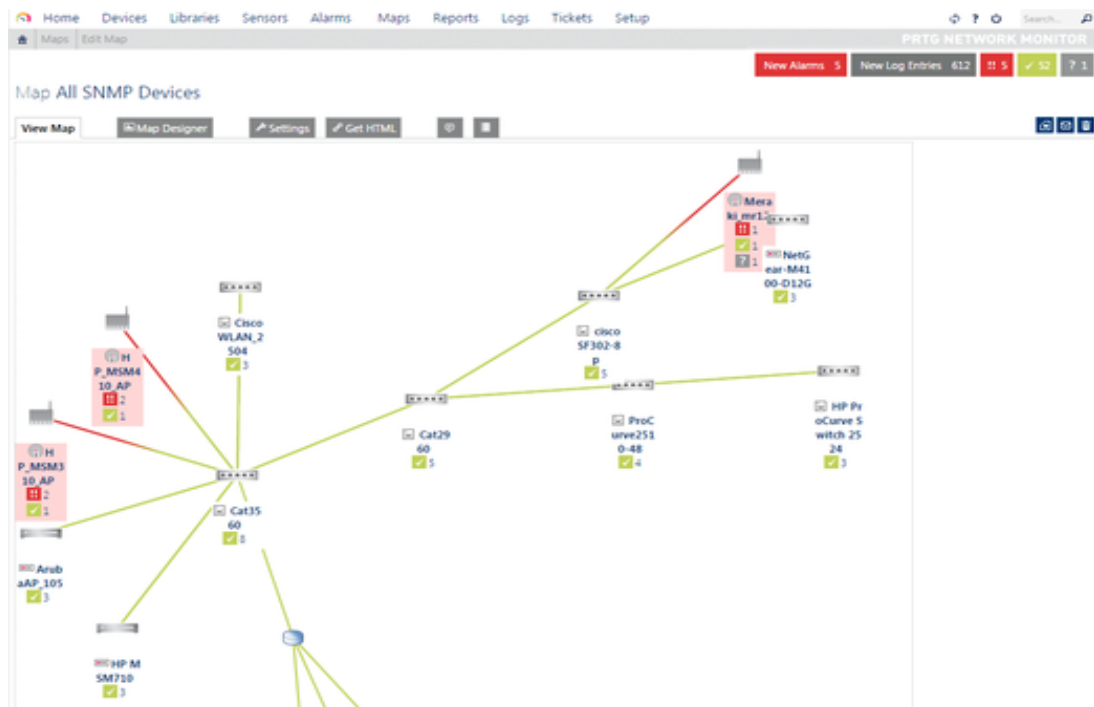


Figure 17: PRTG Network Mapping

### Justification and Recommendations for Monitoring Tools

PRTG Monitor Tool highly suitable option for WLAN network monitoring of Bario Health Clinic system due to the software's features as: capacity to support wide range of technologies, ability to optimize clinic's wireless network efficiently and functionality in every platform. In comparison with other existing monitoring tools, PRTG has long years of experience in market space and high level of positive reviews from enterprise clients.

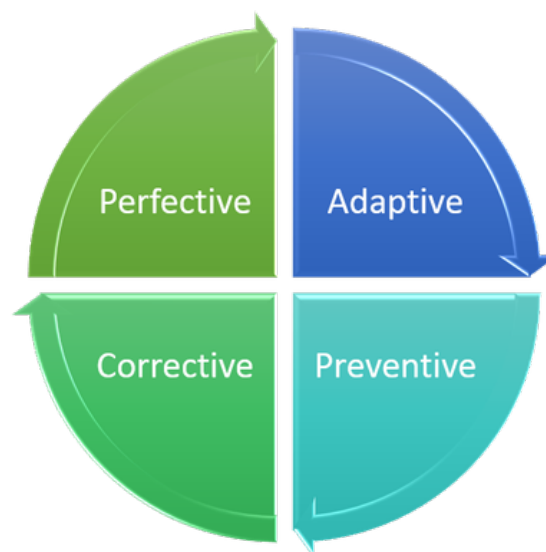
For system administrator this tool will help to get better network management and gain wide understanding of clinic's wireless network bandwidth and resource consumption. Other than that, PRTG can be easily installed in Bario Clinic's operating system and in case of later platform changes, it still will keep functioning. In addition, the beneficial point of using current monitoring tool is ability to monitor not only enterprise applications but also scan network hardware and identify the performance issue. Lastly, is affordable price for PRTG Monitor Tool; most of this software versions, which can support up to 100 integrated sensors are available free of charge.

### 3.4.2 Maintaining WLAN

It is a process of managing and supporting Wireless Network for high performance and fault tolerance of WLAN. It includes regular hardware and software updates which should be handled by network administrator. Moreover, it is continuous operation where constant network configuration, network system check-up and assistance are required. In addition, WLAN maintenance involves resolving extra and urgent wireless network issues which may appear during WLAN operational lifetime. (TechHub, 2015)

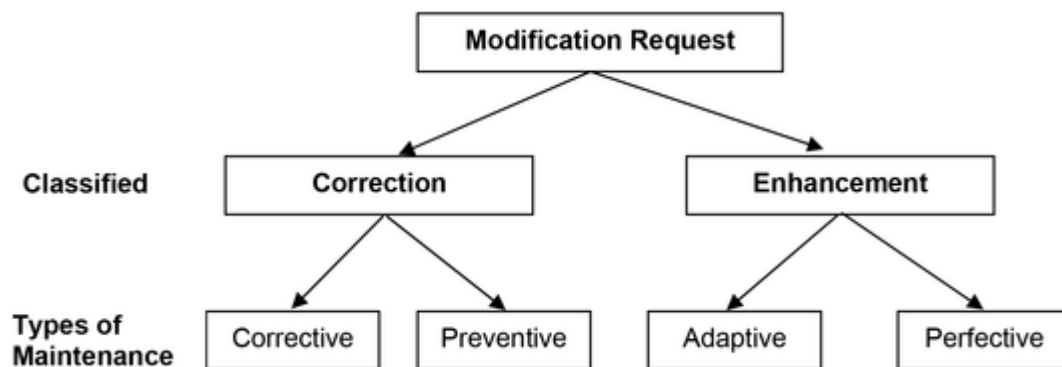
#### Procedures performed during WLAN maintenance

The need for maintenance is to oversee the system failure – ideally, maintenance is performed to keep equipment and systems functioning efficiently during its designed lifetime. (Prokowski, 2015). Four main types of maintenance exist which are corrective, adaptive, perfective, and preventive. Corrective maintenance is focuses on fixing errors that are displayed when the software is in use. Adaptive maintenance is focuses with the changes in the system that takes place to make it adaptable to new environment. Adaptive maintenance accounts for 25% of all the maintenance activities. (Thakur, 2016). Perfective maintenance is concerned with the change in the system. Preventive maintenance involves implementing changes to prevent the occurrence of errors.



***Figure 18: Types of maintenance***

Each of these types was broken into particular categories and can be applied into different scenario cases and system structure specifications. (Course, 2017)



**Figure 4.0: Maintenance categorization**

For Barrio clinic and telecentre adaptive maintenance was chosen because of its ability to implement changes in a part of the system, which has been affected by a change that occurred in other parts of the system. This type is the most suitable option for clinic maintenance because in continuous changing environment and conditions like: new business rules, work patterns, and environmental conditions etc., it is important to keep wireless network system ready and adopted to any external changes. Adaptive maintenance includes following procedure steps:

- Identifying new changes and its solution
- Referring to previous changes
- Coming with new proposed plan
- Adjusting to the new environment
- Documenting

As Barrio clinic and telecentre newly started WLAN functioning it is recommended to adopt adaptive maintenance type, set it ready for any external changes and modifications. So, the wireless network performance of clinic will have strong support in front of changes due to the adaptive nature and ability to adjust in new environment.



In order to, finalize justification of chosen maintenance for clinic and telecentre following scenario represented. Government declared about new project to build several university campuses in area between telecentre and clinic which is 200 meters. This situation causes interference issue and prevents smooth signal transmission. To solve current problem adaptive maintenance was selected and explained its procedure steps:

- First of all, management and network consultants should discuss with government parties about the planned project. Propose them occurring interference problem due to the new building construction between signal transmission area.
- Secondly, have agreement with government side about the height of new university buildings. In case, if their side would not agree to limit the height of constructions, then ask for sponsorship to supply clinic with extra technical hardware for WLAN.
- Thirdly, discuss solution options in future perspectives with network consultant team, in case if similar situation occurs network team would be ready to resolve interference issue. It should include proper documentation, solution and prevention options to avoid WLAN problems in future.

-

### 3.4.3 Wireless LAN Optimization

It is the category of technologies and techniques used to maximize the efficiency of data flow, bandwidth across a wide area network of wireless LAN. (Margarret, 2016). In Bario clinic and telecentre the goal of optimization WLAN is to increase the speed of Internet connection, in order to, provide access to applications and information.

- **Increasing Signal Power**

One of the effective methods to improve wireless network signal. This method can be radical in some case but the most effective due to the fact that it allows to pass strong signal power despite external interference and distance. Current instance should be considered in case if other optimization methods could not give expected result. Moreover, Signal increasing should be done with proposed agreement of clinic's management and networking consultants.

- **Routers and AP positioning**

Counted as one of the main and most practical ways to optimize WLAN is to well design location of routers and AP's placement. Suggested solution enables to get high functionality and performance of wireless network. In Bario clinic and telecentre placement of AP's and routers were especially designed in specific topology what allows to avoid WLAN problems with weak signal.

- **Interference Solution**

Caused issues with interference significantly making difficult to reach level of high wireless network signal. So, one of the solutions if to reduce external obstacles from WLAN area, in Bario clinic and its telecentre case, it is located buildings, vehicles between clinic and tele-centre distance. Besides that, increasing antenna gain and ensuring that there inside of buildings no metal filing rooms and microwave ovens are not nearby routers which may to bring signal interference. Bario clinic, as well as, telecentre used spectrum analyzer to catch the source of interference and further eliminate it.

- **Reducing Number of Devices**

Another proposed solution to optimize clinic WLAN is reducing amount of assigned number of devices in wireless network. It can be realized by implementing restriction to enter the network connection only for authorized amount of people and check for authentication. Represented method would highly secure and strength the clinic wireless network.

- **Use Wi-Fi Repeater**

In addition, to extend strong Wi-Fi signal in Barrio clinic and nearby telecentre system admin suggested to use repeaters. Wireless repeaters should be placed in-between wireless router and the computers which are having connection problems. Devices can connect wirelessly to the repeater, and the repeater connects wirelessly to the router. However, this method is not the very optimal but, it can be good solution to fix weak signal in WLAN area.

## 4.0 Appendices

### 4.1 Gantt Chart

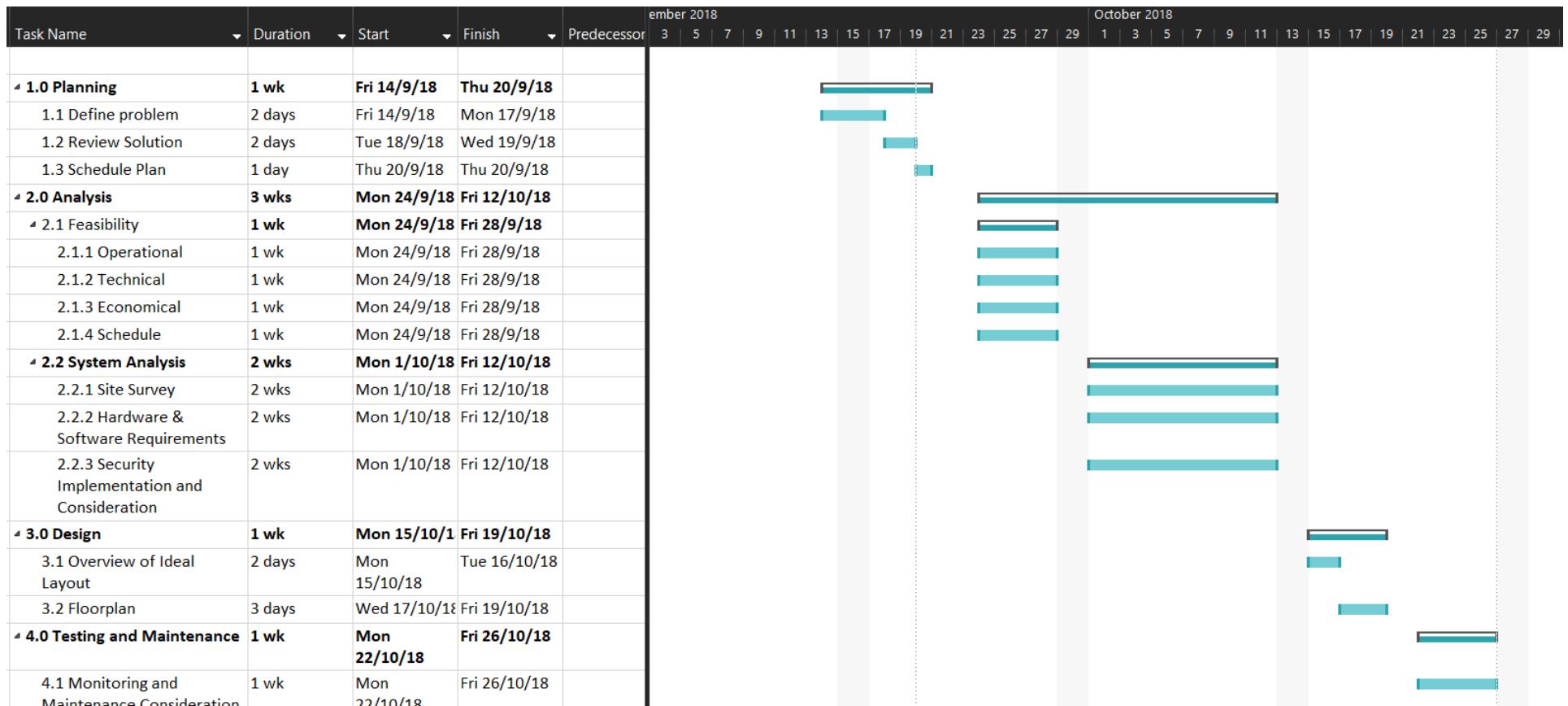


Figure 19: Gantt Chart

## 4.2 Workload Matrix

Group Member	TP Number	Assigned Component	Signature
Nur Afiqah Binti Bakar	TP043448	<ul style="list-style-type: none"><li>• Scope and Limitations</li><li>• Gantt chart</li><li>• Standards, site survey</li></ul>	
Nadzirah Binti Rasol	TP048345	<ul style="list-style-type: none"><li>• Introduction</li><li>• Workload Matrix</li><li>• Hardware &amp; software requirements</li></ul>	
Moldobaeva Munara	TP042788	<ul style="list-style-type: none"><li>• Introduction</li><li>• Overview layout</li><li>• Monitoring&amp; maintenance</li></ul>	
Mousi Ahmed Abdulhafith	TP047417	<ul style="list-style-type: none"><li>• Conclusion</li><li>• Security implementation</li><li>• Future enhancements</li></ul>	

## 5.0 Conclusion

### 5.1 Learning Outcomes and Future Enhancements

In conclusion, the procedure of establishing both Bario community telecentre and a Bario clinic wireless network has been described. By going through some steps, which are: implementing proper site survey, choosing the right software and hardware, discussing the different security protocols, and lastly, illustrating the monitoring and maintaining methods. The communication within and between the two buildings will be established by using wireless LAN instead of wired LAN. During the phase of doing this assignment, we have learnt and gained huge knowledge by conducting a feasibility study that had to match specific criteria. We also got to learn the process of developing a wireless LAN network and what are the important aspects, which needed to put into consideration when do so. When it comes to the enhancement features for the coming years, we strongly recommend for the clinic to practice 802.11ax standard with WPA3 encryption methods, in case they are willing to expand their business, which will in order increase the number of hardware devices and software programs. Furthermore, upgrading, as well keeping the hardware and software up to date.

## 6.0 References

- 1) Anon., 2018. *Wi-Fi survey software for SOHO and hoem users*. [Online]  
Available at: <https://www.ekahau.com/products/heatmapper/overview/>  
[Accessed 20 October 2018].
- 2) Aruba, 2018. *Aruba 300 Series*. [Online]  
Available at: <https://www.arubanetworks.com/products/networking/access-points/300-series/>  
[Accessed 10 November 2018].
- 3) Aruba, 2018. *arubanetworks*. [Online]  
Available at: [https://www.arubanetworks.com/assets/ds/DS\\_AP300Series.pdf](https://www.arubanetworks.com/assets/ds/DS_AP300Series.pdf)  
[Accessed 22 October 2018].
- 4) Aruba, 2018. *arubanetworks*. [Online]  
Available at: [https://www.arubanetworks.com/assets/ds/DS\\_7000Series.pdf](https://www.arubanetworks.com/assets/ds/DS_7000Series.pdf)  
[Accessed 25 October 2018].
- 5) Aruba, 2018. *arubanetworks*. [Online]  
Available at: [https://www.arubanetworks.com/assets/ds/DS\\_501WirelessClientBridge.pdf](https://www.arubanetworks.com/assets/ds/DS_501WirelessClientBridge.pdf)  
[Accessed 1 November 2018].
- 6) Boxcryptor, 2018. *AES and RSA Encryption*. [Online]  
Available at: <https://www.boxcryptor.com/en/encryption/>  
[Accessed 10 November 2018].
- 7) Buckowski, M., 2018. *Wi-Fi STandard Evolution*. [Online]  
Available at: <https://www.grandmetric.com/2018/05/29/wi-fi-standards-evolution/>  
[Accessed 20 October 2018].

- 8) Buczkowski, M., 2018. *IP and Mobile Trends Education*. [Online]  
Available at: <https://www.grandmetric.com/2018/05/29/wi-fi-standards-evolution/>  
[Accessed 10 10 2018].
- 9) cisco, 2017. *cisco*. [Online]  
Available at: <https://www.cisco.com/c/en/us/products/collateral/wireless/3504-wireless-controller/datasheet-c78-738484.html>  
[Accessed 25 October 2018].
- 10) Course, S., 2017. *System Development. Retrieved from Computing*. [Online]  
Available at: <https://mis.uhcl.edu/rob/Course/SAD/Lectures/Systems%20Maintenance.htm>  
[Accessed 10 November 2018].
- 11) Dai, H.-N., Wang, Q., Dong, L. & Wong, C.-W., 2013. *On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas*. [Online]  
Available at: <https://journals.sagepub.com/doi/full/10.1155/2013/760834>  
[Accessed 10 November 2018].
- 12) Ekahau, 2018. *Ekahau Heatmapper Features*. [Online]  
Available at: <https://www.ekahau.com/products/heatmapper/overview/>  
[Accessed 20 October 2018].
- 13) Ekahau, 2018. *Ekahau Spectrum Analyzer*. [Online]  
Available at: <https://www.ekahau.com/products/spectrum-analyzer/overview/>  
[Accessed 20 October 2018].
- 14) Geier, J., 2014. *How to: Conduct a Wireless Site Survey*. [Online]  
Available at: [http://www.wireless-nets.com/resources/tutorials/conduct\\_wireless\\_site\\_survey.html](http://www.wireless-nets.com/resources/tutorials/conduct_wireless_site_survey.html)  
[Accessed 17 10 2018].



- 15) Joan, B., 2010. *Difference Between AES and RC4*. [Online]  
Available at: <http://www.differencebetween.net/technology/internet/difference-between-aes-and-rc4/>  
[Accessed 10 November 2018].
- 16) Lifewire, 2017. *WLAN Monitoring*. [Online]  
Available at: <https://www.lifewire.com/infrastructure-mode-in-wireless-networking-816539>  
[Accessed 10 November 2018].
- 17) Mareco, D., 2016. *securedgenetworks*. [Online]  
Available at: <https://www.securedgenetworks.com/blog/controller-vs-controllerless-wifi-whats-the-difference>  
[Accessed 21 October 2018].
- 18) Metageek, 2018. *MetaGeek Spectrum Analysis Hardware*. [Online]  
Available at: <https://www.metageek.com/products/hardware/>  
[Accessed 20 October 2018].
- 19) NetScout, 2018. *Site Survey Best Practices*. [Online]  
Available at: <https://enterprise.netscout.com/edocs/site-survey-best-practices>  
[Accessed 20 October 2018].
- 20) Netspot, 2018. *Netspot Your Wi-Fi Survey app for Windows and Mac*. [Online]  
Available at: <https://www.netspotapp.com/features.html>  
[Accessed 20 October 2018].
- 21) Netspot, 2018. *Top 5 Best Wi-Fi Heatmap Software Tools*. [Online]  
Available at: <https://www.netspotapp.com/best-wifi-heatmap-software.html>  
[Accessed 20 October 2018].

- 22) Packard, H., 2018. Aruba 501 802.11ac Wireless Client Bridge V2.0.0.2 release notes. *Aruba*, pp. 5-6.
- 23) Packard, H., 2018. Arubanetwork. *Release Notes*, April.pp. 19-28.
- 24) Paessler, 2018. *PRTG Monitoring Tool*. [Online]  
Available at: <https://www.paessler.com>  
[Accessed 10 November 2018].
- 25) Prokowski, 2015. *Types of Maintenance Programs*. [Online]  
Available at: [https://www1.eere.energy.gov/femp/pdfs/OM\\_5.pdf](https://www1.eere.energy.gov/femp/pdfs/OM_5.pdf)  
[Accessed 10 November 2018].
- 26) Rouse, M., 2006. *TechTarget*. [Online]  
Available at: <https://searchmicroservices.techtarget.com/definition/software>  
[Accessed 4 November 2018].
- 27) Rouse, M., 2010. *TechTarget Search Mobile Computing*. [Online]  
Available at: <https://searchmobilecomputing.techtarget.com/definition/access-point>  
[Accessed 21 October 2018].
- 28) Rouse, M., 2010. *WAN optimization (WAN acceleration)*. [Online]  
Available at: <https://searchenterprisewan.techtarget.com/definition/WAN-optimization>  
[Accessed 10 November 2018].
- 29) ruckus, 2017. *ruckus*. [Online]  
[Accessed 25 October 2018].
- 30) Ruckus, 2018. *ruckuswireless*. [Online]  
Available at: <https://ruckus-www.s3.amazonaws.com/pdf/datasheets/ds-zonedirector-1200.pdf>  
[Accessed 24 October 2018].

- 31) Ruckus, 2018. *Ruckuswireless*. [Online]  
Available at: <https://ruckus-www.s3.amazonaws.com/pdf/datasheets/ds-ruckus-r610.pdf>  
[Accessed 22 October 2018].
- 32) Tamo Oft, 2018. *Understanding Survey Types: Passive, Active and Predictive*. [Online]  
Available at: [https://www.tamos.com/htmlhelp/tg/understanding\\_survey\\_types\\_pas.htm](https://www.tamos.com/htmlhelp/tg/understanding_survey_types_pas.htm)  
[Accessed 20 October 2018].
- 33) TechHub, 2015. *Wireless LAN Maintenance*. [Online]  
Available at: <https://education.govt.nz/assets/Documents/School/Running-a-school/Technology-in-schools/technical-info/MoE-School-WLAN-Guidelines-Build-and-Maintain-May-2015-v1.2.pdf>  
[Accessed 10 November 2018].
- 34) TPI, 2010. *RF Spectrum Analyzer for Wireless Site Surveys*. [Online]  
Available at: <https://www.tpi1.com/rf-spectrum-analyzer-wireless-site-surveys/>  
[Accessed 20 October 2018].
- 35) ubiquiti, 2011. *ubnt*. [Online]  
Available at: [https://dl.ubnt.com/datasheets/powerbridgem/PowerBridge\\_M10\\_datasheet.pdf](https://dl.ubnt.com/datasheets/powerbridgem/PowerBridge_M10_datasheet.pdf)  
[Accessed 1 November 2018].
- 36) Ubiquiti, 2018. *ubnt*. [Online]  
Available at: [https://dl.ubnt.com/datasheets/unifi/UniFi\\_AC\\_APs\\_DS.pdf](https://dl.ubnt.com/datasheets/unifi/UniFi_AC_APs_DS.pdf)  
[Accessed 21 October 2018].
- 37) VOCAL Technologies, 2018. *RC4 Encryption Algorithm*. [Online]  
Available at: <https://www.vocal.com/cryptography/rc4-encryption-algorithm/>  
[Accessed 10 November 2018].

