FIT9135 Data Communications

Assignment 1: PART A

Modernized Computer Lab Infrastructure for Melbourne Technology University (MTU)

Assignment 1: PART B

WLAN Design and Security

Tutor's name:
Sameela Suharshani Wijesundara
Faculty of Information Technology,

Submitted by:
Farhad Ullah Rezwan
ID: 30270111

Submission date: April 29, 2019
Due date: April 29, 2019

Assignment 1: PART A

1. Executive Summary

This technical report describes the plan for modernised computing infrastructure for labs of Melbourne Technology University (MTU) at hardware and software level. This report examines and differentiates options like keeping existing lab classrooms, introducing bring your own device (BYOD), and giving loan laptop to the enrolled MTU students. By conducting the cost-benefit analysis of BYOD option this report suggests that for university setting of 8000 students, BYOD option is the most cost-efficient. This report also describes the technology such as Virtualization and Mobile Device Management to successfully implement BYOD in lab setting. Finally, this report suggests how security in BYOD environment can be improved.

2. Introduction

Melbourne Technology University (MTU) with 8000 students wants to implement bring your own device (BYOD) to replace their existing computer laboratory model. There are three options for MTU to decide. First option is to keep the existing lab where students are provided with personal computer in big classroom setting. Second option for MTU to make their students bring their own devices to the classroom which is known as BYOD. Third option for MTU is they can provide loan devices to the students for the time they are enrolled in courses. For the purpose of increased students' satisfaction, better security and comfortless, effective learning ecosystem, I think BYOD option with Virtualization and MDM technology is best among three options.

3. Existing lab technology

Traditional lab technology involves installing multiple devices in classroom lab environment. Most educational institutions spend huge amount of resources for establishing and maintaining computer labs. For this case of MTU, the cost basically related to the maintenance of lab computers, updating and replacing hardware and most importantly updating the existing software to the latest ones. Besides, with the evolution of modern technology-based learning system the need for computer labs and engagement of non-IT courses with computer labs has increased, which lead to overload operations in labs, and shortened time to maintain the labs properly (Shi, Zhao, & Zhang, 2015).

Devices involved and its functions:

To design and maintain the existing lab facility, network devices like routers, hubs, switches and wireless access points, cabling , patch panels, computing devices like nodes, personal computers , and laptops, network interface card (NIC) are required (Caicedo & Cerroni, 2009). Universities require extensive cabling, routers, switches and access points in different patch panels to connect between campuses, buildings and lab classes.

WLAN/ LAN technology required:

For existing lab technology strong LAN connection is required, as a result high cabling cost and network maintenance systems need to be implemented.

Strategies for controlling devices and network components:

- **Eliminate bottlenecks to improve throughput:** Dropped packets in data transfer can be solved by eliminating bottlenecks. There could be three possible areas where bottlenecks can happen- server, circuit or nodes. If the bottleneck is in the circuit, MTU can use newest technology like switched 1000 base -T cables instead of old ones. For server level bottle necks new server could be added or old server's processors can be updated. Beside doing segmentation, splitting the LAN into two Lan can solve server level bottlenecks. Segmentation of network includes two tasks adding new NIC to the server and adding more parallel paths between lab computers and the main server. And slow personal computers in labs can be replaced with fasters pc for eliminating node level bottleneck.
- **Improving the security:** In the existing laboratory system MTU can audit what are the devices that are connected to each switch, install antivirus and firewall software to reduce malware and virus infections.
- **Connectivity and cable management:** According to Caicedo and Cerroni (2009) for each lab class three kind of connections are required such as Laboratory Network (LNET), Management Network (MNET), and Workbench to core (WK).

How devices can be controlled and updated:

In existing classroom lab setting a management workstation is provided with the administrative privilege to make these changes and control all the applications of lab devices (Caicedo & Cerroni, 2009). Caicedo and Cerroni (2009) indicated that administrator or course tutors can install updates and software patches and shut down or restart devices when required. These changes are done with the help of Management Plane Topology system.

4. BYOD technology

Bring your own device or BYOD in educational institution refers to the strategy where students carry their mobile devices like laptop, tablet, or smartphones to carry out study purposes(Chau, Chang, & Lin, 2017). The reasons of BYOD getting popular in Universities and colleges includes smartphones and devices getting cheaper and readily available to students, less resources and expenses for educators, students' and teachers' awareness of newest technologies engaging students in studies more(Johnson, 2012). Furthermore, BYOD classroom environment helps socialization in the classroom environment aside with learning topics this helps less spoken students to participate (Forbes Technology Council, 2018). For MUT re-innovating the existing lab could be more expensive and solution could be implementing BYOD.

Devices involved and its functions:

In BYOD classroom different operating system devices are involved. As most of the devices in BYOD need wireless connectivity, high speed access points and strong WLAN networking system devices required to meet the infrastructure requirement.

WLAN/ LAN required

According to Mareco (2016), for a successful BYOD environment in lab setting both WLAN and LAN Network access all over the campus is required. High speed wireless connection with minimum standard of 802.11ac is mandatory. High speed backbone network is needed to connect different campuses or buildings. Appropriate and secure VPN is also needed for the students who study online (Diogenes & Gilbert, 2015).

Strategies for controlling devices and network components:

- Policies for BYOD: To implement BYOD in MTU there are some policies that has to be made. According to Bruder (2014), such policies may include- Informed tech department, ensure all students who does not have a compatible device can loan from the university, proper authentication system and testing various devices with cloud-based technology.
- Site survey: Access points of same location should minimize the overlaps in between them and must ensure interference avoidance of same frequency channel.

How devices can be controlled and updated:

In BYOD lab environment technologies like Virtualization can be used to update remote devices with software patches. Other technology like Mobile Device Management (MDM) is used to remotely lock and unlock student devices.

Advantages and disadvantages of BYOD:

Advantages of BYOD can be said to be the comfortableness of students, however the drawback is related to the security of the system (Disterer & Kleiner, 2013). Other pros and cons by Garba, Armarego, Murray, and Kenworthy (2015) are summed up in this table-

Advantages of BYOD	Disadvantages of BYOD
Cost reduction	Privacy and security risk
Increased user productivity and contentment	Supporting various OS/devices
Improved flexibility and convenience	Problem of scalability
Online accessibility of data for clients	Difficulties in monitoring devices

5. Loan laptop technology

The third option for MTU is giving loan laptops to the enrolled students, this option is extremely expensive as new devise with a good specification could cost most at any time. According to the online survey by W. Wang, Dermody, Burgess and F. Wang (2014) in Ryerson University Library and Archives (RULA), a library of Ryerson University in Canada, famous for its technology lending services. Suggests us that the top five features technology lending program could be speed in functioning and processes, enough and adequate devices available, and loan period maximum and lightweight and easily manageable to work in home and in university legibility of battery life.

Devices involved and its functions:

To implement Loan Laptop computer lab setting devices need wireless connectivity, high speed access points and strong WLAN networking system required to meet the infrastructure requirement.

WLAN/ LAN required:

High speed WLAN network is required. Recommended standard could be IEEE 802.11ac.

Strategies for controlling devices and network components:

- **Policies for loan laptop facility:** Gu (2011) suggested some policies for successful student loan lab facility, a. Applying loan agreement, b. Security and login authentication c. Equipment specification and software requirements has to be matched, managing device enrolment profiles.
- **Controlling data access:** Device Access Control (DAC) technology enables who can access particular data and makes logs of users who accessed the data from servers (Diogenes, & Gilbert, 2015).
- **Device management:** Cloud based management system: Microsoft Intune, helps to enable students to use particular apps, without damaging important information of university.

How devices can be controlled and updated:

Some of the disadvantages and challenges for loan laptop can be summed like – unit specification and keeping up to date course software requirement, fixing technical problem for each laptop can be cumbersome, updating the softwires can be difficult, and applying appropriate power source to charge laptop etc. (Gu, 2011). However, introducing Mobile Device Management (MDM) is used to remotely lock and unlock student devices.

6. Comparisons between three options for MTU

Comparison in terms of technological aspects:

For loan laptop and BYOD option high speed Wi-Fi network is necessary. On the other hand, for existing lab option strong LAN connection is required as devices are directly connected to the LAN network. For implementing BYOD in MTU technology team should give focus on university level, application level and device level security measures.

	Existing Lab	**BYOD**	**Loan Laptop**
LAN/WLAN	▪ Strong LAN connection is required.	▪ Strong WLAN connection is required	▪ Strong WLAN connection is required
Devices/components Involved	▪ Network devices- router, switches, access points etc. ▪ Clients- pc, laptops. ▪ Others- cables, patch panels, NIC, NOS	▪ Network devices- router, switches, access points ▪ Client computers owned by students	▪ Network devices- router, switches, access points ▪ Client computers owned by MTU
Proposed Technology	▪ Virtualization	▪ MDM ▪ Virtualization ▪ Cloud computing	▪ MDM
Security	▪ Most secure option	Least secure option	▪ Moderate secure option

Table: Comparison Between 3 options for MTU

Comparison in terms of cost:

The most cost-efficient option for MTU should be BYOD option. There is minimal device maintenance cost for BYOD option whereas, for existing lab and loan laptop option the maintenance cost is high. updating software and hardware another source of major cost for existing lab option and loan laptop option for MTU.

	Existing Lab	**BYOD**	**Loan Laptop**
Cost	▪ Maintenance of Lab Computers ▪ Updating software and hardware	▪ Cost related to WLAN technology	▪ Maintenance of loan Computers ▪ Updating software and hardware

Table: Comparison Between 3 options for MTU

7. Proposed new technology for MTU

By looking at the above comparison, it is evident that BYOD option can be worth trying for Melbourne Technology University. BYOD has benefits like sustainability, user friendliness, and low-cost comparative to other options. However, maintaining security and controlling the devices could become a challenge.

Technologies required for implementing BYOD in MTU:

Mobile Device Management (MDM): For MTU MDM technology could help to monitor and configure administrative settings in student devices. Some of the reputed MDM tools available are- IBM MaaS360, VMware AirWatch, Microsoft Exchange ActiveSync, Apple Profile Manager etc. Some of the key advantages of MDM includes- Remote lock and wipe technology, apply administrative policies in devices and manage all student devices and servers using same tool (Garba et al., 2015).

Virtualisation: For MTU Virtualisation could be another handy technology to successfully implement BYOD in the campus. Some of the advantages pointed out by Garba et al. (2015) includes, virtual software to operate on university servers instead of student devices helping centralized strategy to update software, securing access of data from resources, and improved security as viruses cannot be sent through virtualised apps.

Cost Benefit Analysis of proposed BYOD Technologies (Virtualization and MDM):

Project goals:

Cost reduction for MTU, secure, comfortable and productive environment for students.

Alternatives:

loan laptop options and existing computer lab option

Net Present Value of the project:

A$ 2m.

Assumptions:

Among 8000 students 6000 students are enrolled in computer lab-based unit and standard laptop buying value is A$ 1300.

Outcome:

- **Cost for BYOD is lowest:** The cost per year of MDM, and Virtualization solution from two different vendors is 1.7M (Apple Profile Manager = 6000* (A$ 51 / device) + VMware workstation 15 player = 6000* (A$224 /device). On the other hand, lending each student with loan laptop could cost more approximately 7.8M in initial investment.

8. Recommendation

I would recommend MTU to choose BYOD option as it is most cost-efficient, secure and it improves student engagement. Though it has security concerns, three level security measures could mitigate the risk as suggested by (Vignesh & Asha, 2015). First of all, at university level measures are controlling the access of data for students and multiple user differentiation like guest-user, administrating stuff etc. Secondly, application level approach includes implementing MDM to reduce the security risk with authentication for student devices, troubleshooting software related problems and managing and deleting content when the device is lost or stolen(Mareco, 2016). Finally, device level security should be implemented where students have credentials installed in their devices for mitigating unauthorized access of data.

References

Bruder, P. (2014). Gadgets go to school: The benefits and risks of BYOD (Bring your own device), *The Education Digest; Ann Arbor, 80*(3), 14-18. Retrieved from: https://search-proquest-com.ezproxy.lib.monash.edu.au/docview/1619303677?accountid=12528

Caicedo, C. E., & Cerroni, W. (2009). Design of a computer networking laboratory for efficient manageability and effective teaching. *2009 39th IEEE Frontiers in Education Conference* (pp. 1-6). San Antonio, TX, USA. doi: 10.1109/FIE.2009.5350782

Chou, P., Chang, C., & Lin, C. (2017). BYOD or not: A comparison of two assessment strategies for student learning, *Computers in Human Behavior, 74*, 63-71. doi: 10.1016/j.chb.2017.04.024

Diogenes, Y., Gilbert, Jeff. (2015). *Enterprise mobility suite managing byod and company-owned devices* (1st ed.). Retrieved from https://learning.oreilly.com/library/view/enterprise-mobility-suite/9780735698444/?ar

Disterer, G., & Kleiner, C. (2013). BYOD Bring Your Own Device, *Procedia Technology 9*, 43-53. Doi: 10.1016/j.protcy.2013.12.005

Forbes Technology Council. (2018). Cutting-edge education: 13 ways to leverage technology for learning. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/03/28/cutting-edge-education-13-ways-to-leverage-technology-for-learning/#1a7a7d153919

Garba, A. B., Armarego, J., Murray, D., & Kenworthy, W. (2015). Review of the information security and privacy challenges in bring your own device (BYOD) environments. *Journal of Information Privacy & Security, 11*(1), 38-54. Retrieved from https://search-proquest-com.ezproxy.lib.monash.edu.au/docview/1691289631?accountid=12528

Gu, F. (2011). The Campus-Wide Laptop Loan Service and the Library's Role, *Library Management, 32*(1-2), 6-21. Retrieved from: http://www.emeraldinsight.com.ezproxy.lib.monash.edu.au/info/journals/lm/lm.jsp

Johnson, D. (2012). Power Up! / On Board with BYOD, *Students Who Challenge Us, 70*(2), 84-85. Retrieved from: http://www.ascd.org/publications/educational-leadership/oct12/vol70/num02/On-Board-with-BYOD.aspx

Mareco, D. (2016). How to Build the Perfect BYOD Solution: 5 Must-Have Components. Retrieved from https://www.securedgenetworks.com/blog/how-to-build-the-perfect-byod-solution-5-must-have-components

Shi, L., Zhao, H., & Zhang, K. (2014). Research of Computer Virtual Laboratory Model Based on Cloud Computing. *Applied Mechanics and Materials, 687*,3027-3031. doi:10.4028/www.scientific.net/AMM.687-691.3027

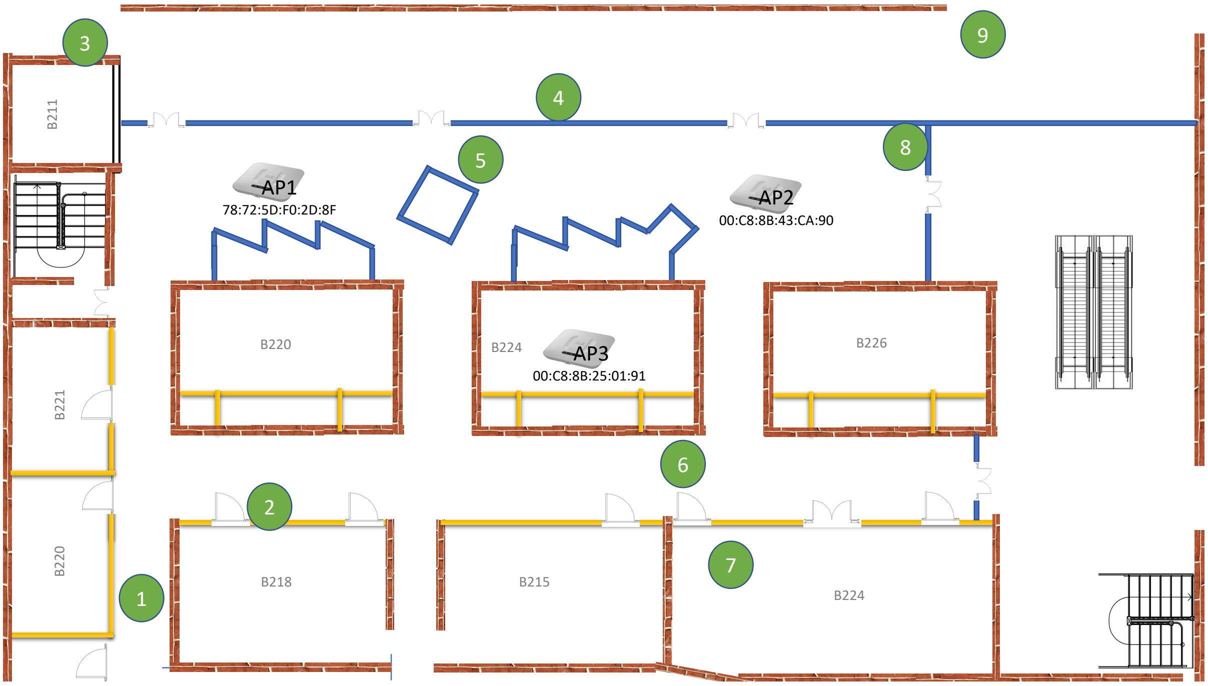
Vignesh, U., & Asha, S. (2015). Modifying security policies towards BYOD, *Procedia Computer Science. 50,* 511-516. Doi: 10.1016/j.procs.2015.04.023

Wang, W., Dermody, K., Burgess, C., and Wang, F. (2014). From a Knowledge Container to a Mobile Learning Platform: What RULA Learned from the Laptop Lending Program, *Journal of Access Services. 11*(4), 255-281. doi: 10.1080/15367967.2014.945118

Assignment 1: PART B:

This report represents the WLAN site survey of the second floor of Building B of Monash University, Caulfield campus. This report assumes that the floor contains only three access points (AP's).

Section A: WLAN site survey



Locations of access points (AP)

● Locations of measurements

Glass

Brick Wall

Plasterboard wall

	Network Name (SSID)	Mac Address (BSSID)	802.11 Version	Band	Channel
AP 1	eduroam	78:72:5D:F0:2D:8F	ac	5 GHz	64,-1
AP 2	eduroam	00:C8:8B:43:CA:90	g/n	2.4 GHz	11
AP 3	Monash Free WiFi	00:C8:8B:25:01:91	g/n	2.4 GHz	11

Signal strength in dBm for different locations									
	Location 1	Location 2	Location 3	Location 4	Location 5	Location 6	Location 7	Location 8	Location 9
AP 1	-87	-87	-81	-75	-69	-88	-90	-84	-87
AP 2	-86	-77	-80	-72	-61	-65	-84	-71	-74
AP 3	-86	-86	-77	-82	-84	-74	-84	-85	-

Signal to Noise Ratio (SNR)									
	Location 1	Location 2	Location 3	Location 4	Location 5	Location 6	Location 7	Location 8	Location 9
AP 1	8	6	16	21	23	7	3	8	-4
AP 2	7	14	16	26	33	29	11	21	9
AP 3	8	9	17	12	11	20	10	10	-

Fig: WLAN site survey for Building B, MU, Caulfield.

Section B: Observation Analysis

Channel Occupancy:

AP 2 and AP 3 have similar bands of 2.4 GHz and competing on the same channels which is 11. So, there can be a problem of overlapping channels as they are relatively closer. The configuration could be improved if the position of AP 1, which has different bandwidth(5 GHz) is swapped with the position of AP 2.

Interference from Different Objects:

1. Interference from glass: The interference from glass for AP 1 can be found in location 4 which is outside the glass boundary. The signal strength for this location is -75 dBm, which is lower than signal strength of location 5(-69 dBm), which is inside the glass boundary.

2. Interference from plasterboard wall: Interference from the plasterboard wall can be seen in location 7. The signal strength of location 7 is -84 dBm from AP 2. On the other hand, at location 6, which is in quite nearer to location 7 and no plasterboard wall in between, has the signal strength of -65 dBm from the same AP.

3. Interference from wall: Between AP 1 and location 3 there are a wall and a glass. For that reason, the signal strength is lower at -81 dBm, whereas the signal strength for location 4 from the same AP is comparatively good (-75 dBm) with no walls in between them.

- Difference in attenuation for two different AP's: For the AP 1 (with higher bandwidth = 5 GHz) the signal strength outside the glass area (location 4) is -75 dBm and inside glass area (location 5) is -69 dBm. So, the signal loss is 6 dB. On the other hand, For the AP 2 (with lower bandwidth = 2.4 GHz) the signal strength outside the glass area (location 9) is -74 dBm and inside glass (location 8) is -71 dBm. So the signal loss is 3 dB. In sum, the attenuation is higher for higher bandwidth WLAN networks.

Attenuation caused by own body:

At location 5, I measured the attenuation loss for my own body for two different AP's (AP1 & AP 2). Initially the signal strength for AP1 and AP 2 was -69 dBm and -61 dBm and percentage values of signal strength was 51 % and 64 % respectively. The signal strength loose for the attenuation caused by human body at 13%(-88 dBm) and 32 %(-79 dBm) .

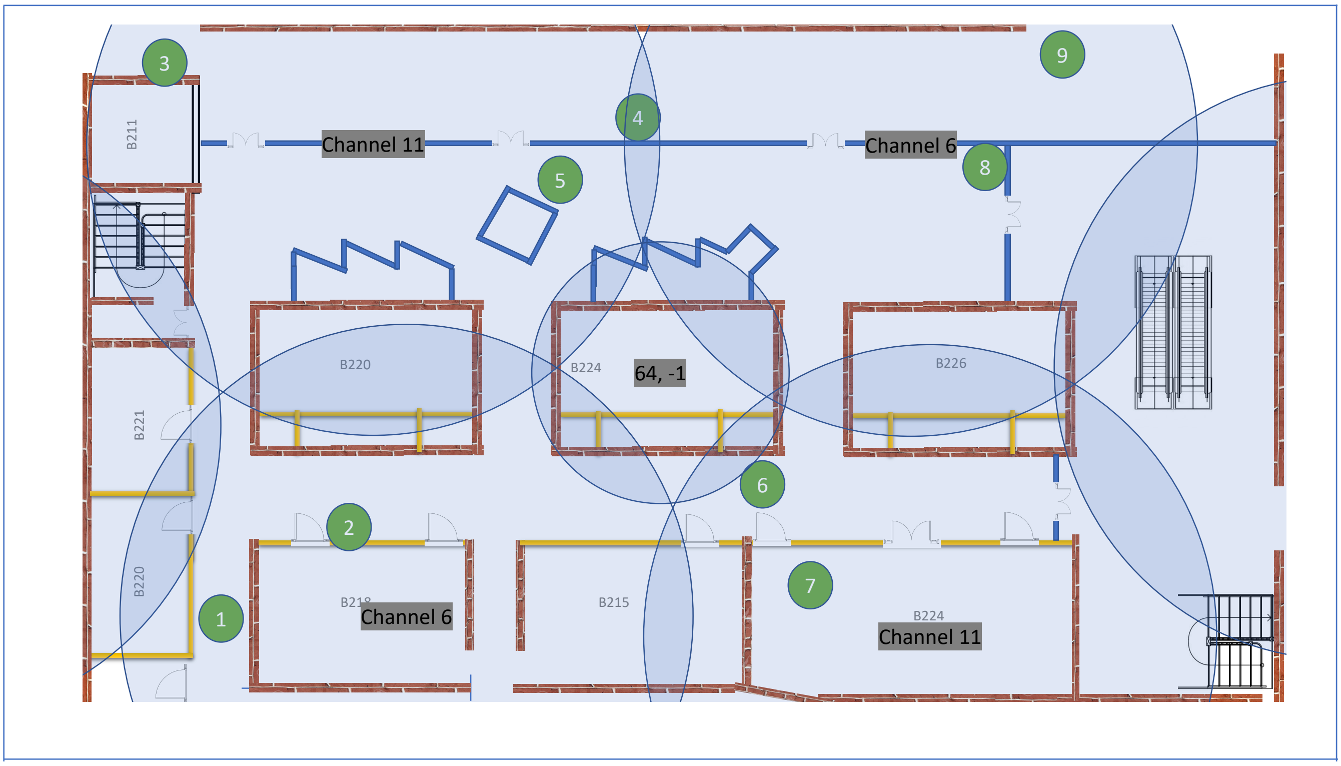
Attenuation for AP1: is 6db for location 5. As current signal strength percentage is about ¼ of previous signal strength percentage. And,
Attenuation for AP2: is 3db for location 5. As current signal strength percentage is about ½ of previous signal strength percentage.

Here we can realize that attenuation is higher for 5GHz band then 2.4GHz band.

Coverage:

I think the 3 access points do not cover all the areas properly. For example, location 1 and location 2 do not have enough signal strengths. The optimal design for this consideration should include these changes-

a. installing AP 3 near the empty place of location 1 and location 2.
b. as AP 2 and AP 3 has similar channel and band, AP 1 should be placed in Room no B224 replacing AP 3, this will ensure interference avoidance of similar channel.
c. Installing more AP's and also making sure that overlaps are minimized.


3
9
B211
Channel 11
4
Channel 6
8
5
B220
B224
64, -1
B226
B221
6
2
B220
7
1
B218
Channel 6
B215
B224
Channel 11